Preprint typeset in JHEP style - HYPER VERSION

Chapter 1: Abstract Group Theory

Gregory W. Moore

ABSTRACT: Very Abstract.May 1, 2020

Contents

1. Introduction

Historically, group theory began in the early 19th century. In part it grew out of the problem of finding explicit formulae for roots of polynomials. [1]. Later it was realized that groups were crucial in transformation laws of tensors and in describing and constructing

[1] For a romantic description, see the chapter "Genius and Stupidity" in E.T. Bell's *Men of Mathematics*. For what is likely a more realistic account see chapter 6 of T. Rothman's *Science à la Mode*.

geometries with symmetries. This became a major theme in mathematics near the end of the 19th century. In part this was due to Felix Klein's very influential Erlangen program.

In the 20th century group theory came to play a major role in physics. Einstein's 1905 theory of special relativity is based on the symmetries of Maxwell's equations. The general theory of relativity is deeply involved with the groups of diffeomorphism symmetries of manifolds. With the advent of quantum mechanics the representation theory of linear groups, particularly $SU(2)$ and $SO(3)$ came to play an important role in atomic physics, despite Niels Bohr's complaints about "die Gruppenpest." One basic reason for this is the connection between group theory and symmetry, discussed in chapter ****. The theory of symmetry in quantum mechanics is closely related to group representation theory.

Since the 1950's group theory has played an extremely important role in particle theory. Groups help organize the zoo of subatomic particles and, more deeply, are needed in the very formulation of gauge theories. In order to formulate the Hamiltonian that governs interactions of elementary particles one must have some understanding of the theory of Lie algebras, Lie groups, and their representations.

In the late 20th and early 21st century group theory has been essential in many areas of physics including atomic, nuclear, particle, and condensed matter physics. However, the beautiful and deep relation between group theory and geometry is manifested perhaps most magnificently in the areas of mathematical physics concerned with gauge theories (especially supersymmetric gauge theories), quantum gravity, and string theory. It is with that in the background that I decided to cover the topics in the following chapters.

2. Basic Definitions

We begin with the abstract definition of a group.

Definition 2.1: A *group* is a quartet $(G, \mathbf{m}, \mathbf{I}, e)$ where

1. G is a set.
2. $\mathbf{m} : G \times G \to G$ is a map, called the *group multiplication map.*
3. $\mathbf{I} : G \to G$ is a map, called the *inverse map*
4. $e \in G$ is a distinguished element of G called the *identity element.*

These data $(G, \mathbf{m}, \mathbf{I}, e)$ are required to satisfy the following conditions:

1. $\mathbf{m}$ is *associative*: For all $g_1, g_2, g_3 \in G$ we have

$$\mathbf{m}(\mathbf{m}(g_1, g_2), g_3) = \mathbf{m}(g_1, \mathbf{m}(g_2, g_3)) \tag{2.1}$$

2.

$$\forall g \in G \qquad \mathbf{m}(g, e) = \mathbf{m}(e, g) = g \tag{2.2}$$

3.
$$\forall g \in G \qquad \mathbf{m}(\mathbf{I}(g), g) = \mathbf{m}(g, \mathbf{I}(g)) = e \tag{2.3}$$

The above notation is unduly heavy, and we will not use it. Thus, we give the definition again, but more informally:

$\forall a, b \in G$ *there exists a unique element in* G*, called the product, and denoted* $a \cdot b \in G$ in other words, we streamline notation by writing $a \cdot b := \mathbf{m}(a, b)$.

The product is required to satisfy 3 axioms:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

2. Existence of an identity element: $\exists e \in G$ such that:
$$\forall a \in G \qquad a \cdot e = e \cdot a = a \tag{2.4}$$

3. Existence of inverses: Again, we streamline notation by writing $a^{-1} := \mathbf{I}(a)$. so that $a \cdot a^{-1} = a^{-1} \cdot a = e$

Remarks

1. We will often denote e by 1, or, when discussing more than one group at a time, we denote the identity in a particular group G by 1_G. The identity element is also often called the *unit element*, although the term “unit” can have other meanings when dealing with more general mathematical structures such as rings.

2. Also, we sometimes denote the product of a and b simply by ab.

3. We can drop some axioms and still have objects of mathematical interest. For example, a *monoid* is a set M with a multiplication map $\mathbf{m} : M \times M \to M$ which is associative. And that’s all. If there is an identity element $e \in M$ which functions as the identity for this multiplication then we speak of a *unital monoid.* The further assumption of inverses turns the monoid into a group. The definition of a group seems to be in the Goldilocks region of having just enough data and conditions to allow a deep theory, but not having too many constraints to allow only a few examples. It is <u>just right</u> to have a deep and rich mathematical theory.

4. We can also put further mathematical structures on the data $(G, \mathbf{m}, \mathbf{I}, e)$. For example, if G is a topological space and $\mathbf{m}$ and $\mathbf{I}$ are both <u>continuous</u> maps, then we have a *topological group.* If G is furthermore a manifold and $\mathbf{m}$ and $\mathbf{I}$ are real analytic in local coordinates, then we have a *Lie group.*

Exercise

a.) Show that e unique. [2]

b.) Given a is a^{-1} unique?

c.) Show that axioms 2,3 above are slightly redundant: For example, just assuming $a \cdot e = a$ and $a \cdot a^{-1} = e$ show that $e \cdot a = a$ follows as a consequence.

Example 2.1: As a set, $G = \mathbb{Z}, \mathbb{R}$, or $\mathbb{C}$. The group operation is ordinary addition:

$$\mathbf{m}(a, b) := a + b \tag{2.5}$$

The reader should check all the axioms.

Example 2.2: A simple generalization is to take n-tuples for a positive integer n: $G = \mathbb{Z}^n, \mathbb{R}^n, \mathbb{C}^n$, with the operation being vector addition, so if $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$ then

$$\mathbf{m}(\vec{x}, \vec{y}) := (x_1 + y_1, \ldots, x_n + y_n) \tag{2.6}$$

Example 2.3: $G = \mathbb{R}^* := \mathbb{R} - \{0\}$ or $G = \mathbb{C}^* := \mathbb{C} - \{0\}$ Now if $x, y \in G$ then $\mathbf{m}(x, y) := xy$ is ordinary multiplication of complex numbers. Check the axioms.

Definition 2.2: Suppose $(G, \mathbf{m}, \mathbf{I}, e)$ is a group and $H \subset G$ is a subset so that $\mathbf{m}$ and $\mathbf{I}$ preserve H, that is, the restriction of $\mathbf{m}$ takes $H \times H \to H$ and the restriction of $\mathbf{I}$ maps $H \to H$. (It then follows that $e \in H$.) In this case we say that $(H, \mathbf{m}, \mathbf{I}, e)$ is a *subgroup of* $(G, \boldsymbol{m}, \boldsymbol{I}, e)$.

Exercise *Subgroups*

a.) $\mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$ with operation $+$, define subgroups.

b.) Is $\mathbb{Z} - \{0\}$ a monoid (with $\mathbf{m}$ given by standard multiplication).

c.) Is $\mathbb{Z} - \{0\} \subset \mathbb{R}^*$ a subgroup?

d.) Let $\mathbb{R}^*_{>0}$ and $\mathbb{R}^*_{<0}$ denote the positive and negative real numbers, respectively. Using ordinary multiplication of real numbers, which of these are subgroups of $\mathbb{R}^*$?

e.) Consider the negative real numbers $\mathbb{R}_{<0}$ with the multiplication rule:

$$\mathbf{m}(x, y) = -xy \tag{2.7}$$

Show that this defines a group law on $\mathbb{R}_{<0}$, but that $(\mathbb{R}_{<0}, \mathbf{m}, ...)$ is not a subgroup of $\mathbb{R}^*$.

Definition 2.3: The *order* of a group G, denoted $|G|$, is the cardinality of G as a set. Roughly speaking this is the same as the "number of elements in G." A group G is called a *finite group* if $|G| < \infty$, and is called an *infinite group* otherwise.

[2] *Answer*: Suppose that two elements $e_1, e_2 \in G$ behave as units. Consider the product $e_1 \cdot e_2$. Using e_1 as a unit we can say this is e_2. On the other hand, using e_2 as a unit we can say this is e_1. Therefore $e_1 = e_2$.

The groups in Examples 1,2,3 above are of infinite order. Here are examples of finite groups:

Example 2.4: The group of N^{th} roots of unity. Choose a natural number N. [3] We let $Res(N)$ be the set of complex numbers z such that $z^N = 1$. Thus we could write

$$Res(N) = \{1, \omega, \dots, \omega^{N-1}\} \tag{2.8}$$

♣Need a better notation for this group. How about μ_N ? ♣

where $\omega = \exp[2\pi \mathrm{i}/N]$. This is a finite group with N elements, as is easily checked.

Exercise

Does $Res(137)$ have any nontrivial subgroups? [4]

Exercise

In example 4 show that if N is even then the subset of classes of even integers forms a proper subgroup of $Res(N)$. What happens if N is odd?

Already, with the simple concepts we have introduced, we can ask nontrivial questions. For example:

Does every infinite group necessarily have proper subgroups of infinite order?

It is actually not easy to think of counterexamples, but in fact there are infinite groups all of whose proper subgroups are finite. [5]

So far, all our examples had the property that for any two elements a, b

$$a \cdot b = b \cdot a \tag{2.9}$$

One cannot use just the group axioms above to prove the equation (2.9). But nothing forbids that it could happen in some examples. So, this is a special situation. When equation (2.9) holds for two elements $a, b \in G$ we say "a and b commute." If a and b commute for every pair $(a, b) \in G \times G$ then we say that G is an *Abelian group*:

[3] The *natural numbers* are the same as the positive integers.

[4] *Answer*: We will give an elegant answer below.

[5] One example are the *Prüfer groups.* These are subgroups of the group of roots of unity. They are defined by choosing a prime number p and taking the subgroup of roots of unity of order p^n for some natural number n. Even wilder examples are the "Tarski Monster groups" (not to be confused with the Monster group, which we will discuss later). These are infinite groups all of whose subgroups are isomorphic to the cyclic group of order p.

Definition 2.4: If a, b commute for all $a, b \in G$ we say "*G is Abelian.*"

Example 2.5: **The residue classes modulo N, also called "The cyclic group of order N."**

As a set we can take $G = \{0, 1, \dots, N-1\}$. [6] If n is an integer then we can write $n = r + Nq$ in a unique way where the quotient q is integral and the *remainder* or *residue modulo N* is the integer $r \in G$. The group operation on G is defined to be:

$$\mathbf{m}(r_1, r_2) := (r_1 + r_2)\mathrm{mod}N \tag{2.10}$$

This group, which appears frequently in the following, will be denoted as $\mathbb{Z}/N\mathbb{Z}$ or $\mathbb{Z}_N$. For example, telling time in hours is arithmetic in $\mathbb{Z}_{12}$, or in $\mathbb{Z}_{24}$ in railroad/military time. The reader should note that it "resembles" closely the group $Res(N)$. We will make that precise in the next section.

Note: Note that our abbreviated notation $a \cdot b$ for the group multiplication $\mathbf{m}(a, b)$ would actually be quite confusing when working with $\mathbb{Z}_N$. The reason is that it is also possible to define a *ring structure* (see Chapter 2) where one multiplies r_1 and r_2 as integers and then takes the residue. This is *NOT* the same as $\mathbf{m}(r_1, r_2)$!! For example, if we take $N = 5$ then $\mathbf{m}(2, 3) = 0$ in $\mathbb{Z}_5$ because $2 + 3 = 5$ is congruent to 0 modulo 5. Of course, multiplying as integers $2 \times 3 = 6$ and 6 is congruent to 1 mod 5. Thus, often when considering Abelian groups we prefer to use the abbreviated notation

$$a + b := \mathbf{m}(a, b) \tag{2.11}$$

When we use this additive notation for Abelian groups we will write the identity element as 0 so that $a + 0 = 0 + a = a$. (Writing "$a + 1 = a$" would look extremely weird.) Note that we will not <u>always</u> use additive notation for Abelian groups! For example, for $Res(N)$ the multiplicative notation is quite natural.

There are certainly examples of nonabelian groups.

Example 2.6: *The General Linear Group*

Let $\kappa = \mathbb{R}$ or $\kappa = \mathbb{C}$. Define:

♣κ will be our official symbol for a general field. This needs to be changed from k in many places below. ♣

$$GL(n, \kappa) = \{A | A = n \times n \text{ invertible matix over } \kappa\} \tag{2.12}$$

$GL(n, \kappa)$ is a group of infinite order. It is abelian if $n = 1$ and nonabelian if $n > 1$. There are some important generalizations of this example: [7] We could let κ be any field. If κ is a finite field then $GL(n, \kappa)$ is a finite group. More generally, if R is a *ring* $GL(n, R)$ is the subset of $n \times n$ matrices with entries in R with an inverse in $M_n(R)$. This set forms a

[6] It is conceptually better to think of G as the integers modulo N, using the notation of equivalence relation of §7.1 below. Then we denote elements by $\bar{0}, \bar{1}, \bar{2}, \cdots$. Thus, e.g. if $N = 2$ then $\bar{1} = \bar{3}$. The group operation is simply $\overline{r_1} + \overline{r_2} := \overline{r_1 + r_2}$.

[7] See Chapter 2 for some discussion of the mathematical notions of fields and rings used in this paragraph.

group. For example, $GL(2,\mathbb{Z})$ is the set of 2×2 matrices of integers such that the inverse matrix is also a 2×2 matrix of integers. This set of matrices forms an infinite nonabelian group under matrix multiplication.

Definition 2.5: The center $Z(G)$ of a group G is the set of elements $z \in G$ that commute with all elements of G:

$$Z(G) := \{z \in G | zg = gz \qquad \forall g \in G\} \tag{2.13}$$

$Z(G)$ is an Abelian subgroup of G. (Why? You prove it - NOW!!) As an example, for $\kappa = \mathbb{R}$ or $\kappa = \mathbb{C}$ the center of $GL(n,\kappa)$ is the subgroup of matrices proportional to the unit matrix.

Example 2.7: *The Classical Matrix Groups*

A *matrix group* is a subgroup of $GL(n,\kappa)$. There are several interesting examples which we will study in great detail later. Some examples include:

The special linear group:

$$SL(n,\kappa) \equiv \{A \in GL(n,\kappa) : \text{det} A = 1\} \tag{2.14}$$

The orthogonal groups:

$$\begin{aligned} O(n,\kappa) &:= \{A \in GL(n,\kappa) : AA^{tr} = 1\} \\ SO(n,\kappa) &:= \{A \in O(n,\kappa) : \text{det} A = 1\} \end{aligned} \tag{2.15}$$

Another natural class are the unitary and special unitary groups:

$$U(n) := \{A \in GL(n,\mathbb{C}) : AA^{\dagger} = 1\} \tag{2.16}$$

$$SU(n) := \{A \in U(n) : \text{det} A = 1\} \tag{2.17}$$

Finally, to complete the standard list of classical matrix groups we consider the standard symplectic form on $\mathbb{R}^{2n}$:

$$J = \begin{pmatrix} 0 & 1_{n\times n} \\ -1_{n\times n} & 0 \end{pmatrix} \in M_{2n}(\mathbb{R}) \tag{2.18}$$

Note that the matrix J satisfies the properties:

$$J = J^* = -J^{tr} = -J^{-1} \tag{2.19}$$

Definition A *symplectic matrix* is a matrix A such that

$$A^{tr} J A = J \tag{2.20}$$

We define the symplectic groups:

$$Sp(2n,\kappa) := \{A \in GL(2n,\kappa) | A^{tr} J A = J\} \tag{2.21}$$

Remark: As an exercise you should show from the definition above that the most general element of $SO(2,\mathbb{R})$ must be of the form

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \qquad x^2 + y^2 = 1 \tag{2.22}$$

where the matrix elements x, y are real. Thus we recognize that group elements in $SO(2,\mathbb{R})$ are in 1-1 correspondence with points on the unit circle in the plane. We can even go further and parametrize $x = \cos\phi$ and $y = \sin\phi$ and ϕ is a coordinate provided we identify $\phi \sim \phi + 2\pi$ so the general element of $SO(2,\mathbb{R})$ is of the form:

$$R(\phi) := \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \tag{2.23}$$

This is familiar from the implementation of rotations of the Euclidean plane in Cartesian coordinates. Note that the group multiplication law is

$$R(\phi_1) R(\phi_2) = R(\phi_1 + \phi_2) \tag{2.24}$$

so, in ϕ "coordinates" the group multiplication law is continuous, differentiable, even (real) analytic. Similarly, taking an inverse is $\phi \to -\phi$. What we have just said can be generalized to all the classical matrix groups: They can be identified with manifolds. There are parametrizations of these manifolds, so the group multiplication and inverse are smooth operations. Moreover, the groups "act" naturally on various linear spaces. (See Section 4.2 for the notion of "group action.") This is part of the theory of Lie groups. Lie groups have vast applications in physics. For example, $G = SU(3)$ is the gauge group of a Yang-Mills theory that describes the interactions of quarks and gluons, while $G = SU(3)\times SU(2)\times U(1)$ is related to the standard model that describes all known elementary particles and their interactions. The general theory of Lie groups will be discussed in Chapter 8(?) below, although we will meet many many examples before then.

Example 2.8 *Function spaces as groups.*

Suppose G is a group. Suppose X is any set. Consider the set of all functions from X to G:

$$\mathcal{F}[X \to G] = \{f : f \text{ is a function from } X \to G\} \tag{2.25}$$

We claim that $\mathcal{F}[X \to G]$ is also a group: We define the product $f_1 \cdot f_2$ to be that function whose values are defined by:

$$(f_1 \cdot f_2)(x) := f_1(x) \cdot f_2(x) \tag{2.26}$$

The inverse of f is the function $x \to f(x)^{-1}$.

If both X and G have finite cardinality then $\mathcal{F}[X \to G]$ is a finite group. If X or G has an infinite set of points then this is an infinite order group. If X is a positive dimensional manifold and G is a Lie group (notions defined below) this is an infinite-*dimensional* space.

In the special case of the space of maps from the circle into the group:

$$LG = \mathcal{F}[S^1 \to G] \tag{2.27}$$

we have the famous "loop group" which has many wonderful properties. (It is also the beginning of string theory.) In some cases if X is a manifold and G is a classical matrix group then, taking a subgroup defined by suitable continuity and differerentiability properties, we get the *group of gauge transformations of Yang-Mills theory.* As a simple example, you are probably familiar with the gauge transformation in Maxwell theory:

$$A_\mu \to A_\mu + \partial_\mu \epsilon \tag{2.28}$$

where A_μ is the vector potential so that $F_{\mu\nu} = \partial_\mu A_\nu - \partial_\nu A_\mu$ is the fieldstrength tensor. Here $\epsilon : \mathbb{M}^{1,3} \to \mathbb{R}$ is a function on 1+3 dimensional Minkowski space. (In a more careful account one would put restrictions on the allowed functions - they should be differentiable and satisfy suitable boundary conditions - etc.) The more canonical object is

$$f : x \mapsto e^{\mathrm{i}\epsilon(x)} \tag{2.29}$$

and this is a function from spacetime, $\mathbb{M}^{1,3}$ to $U(1)$, so $f \in \mathcal{F}[\mathbb{M}^{1,3} \to U(1)]$. This is a better point of view because it generalizes in interesting ways to other spacetimes. Note that the gauge transformation law can be written as:

$$(-\mathrm{i}\partial_\mu + A'_\mu) = f^{-1}(-\mathrm{i}\partial_\mu + A_\mu)f \tag{2.30}$$

For many reasons this is a conceptually superior way to write it.

Example 2.9: *Permutation Groups.*

Let X be any set. A *permutation* of X is a one-one invertible transformation $\phi : X \to X$. The composition $\phi_1 \circ \phi_2$ of two permutations is a permutation. The identity permutation leaves every element unchanged. The inverse of a permutation is a permutation. Thus, composition defines a group operation on the permutations of any set. This group is designated S_X. It is an extremely important group and we will be studying it a lot. In the case where $X = M$ is a manifold we can also ask that our permutations $\phi : M \to M$ be continuous or even differentiable. If ϕ and ϕ^{-1} are differentiable then ϕ is a *diffeomorphism.* The composition of diffeomorphisms is a diffeomorphism by the chain rule, so the set of diffeomorphisms $\mathrm{Diff}(M)$ is a subgroup of the set of all permutations of M. The group $\mathrm{Diff}(M)$ is the group of gauge symmetries in General Relativity. Except in the case where $M = S^1$ is the circle, remarkably little is known about the diffeomorphism groups of manifolds. One can ask simple questions about them whose answers are unknown.

Example 2.10: *Power Sets As Groups.*

Let X be any set and let $\mathcal{P}(X)$ be the power set of X. It is, by definition, the set of all subsets of X. If $Y_1, Y_2 \in \mathcal{P}(X)$ are two subsets of X then define

$$Y_1 + Y_2 := (Y_1 - Y_2) \cup (Y_2 - Y_1) \tag{2.31}$$

This defines an abelian group structure on $\mathcal{P}(X)$. The identity element 0 is the empty set $\emptyset$ and the inverse of Y is Y itself: That is, in this group

$$2Y := Y + Y = \emptyset = 0 \tag{2.32}$$

Exercise *Due diligence*

Check that each of the above sets (2.14),(2.15),(2.16), (2.21), are indeed subgroups of the general linear group.

Exercise *Apparent Asymmetry In The Definitions*

In (2.15) we used $AA^{tr} = 1$ but we could have used $A^{tr}A = 1$. Similarly, in (2.16) we used $AA^{\dagger} = 1$ rather than $A^{\dagger}A = 1$. Finally, in (2.21) we could, instead, have defined $Sp(2n, \kappa)$ to be matrices in $M_{2n}(\kappa)$ such that $AJA^{tr} = J$. In all three cases, writing things the other way defines the same group: Why?

(Careful: Just taking the transpose or hermitian conjugate of these equations does not help.)

Exercise $O(2,\mathbb{R})$ *vs.* $SO(2,\mathbb{R})$

a.) Show from the definition above of $O(2,\mathbb{R})$ that the most general element of this group is the form of (2.22) above, OR, of the form

$$\begin{pmatrix} x & y \\ y & -x \end{pmatrix} \qquad x^2 + y^2 = 1 \tag{2.33}$$

b.) Show that no matrix in $O(2,\mathbb{R})$ is simultaneously of the form (2.22) and (2.33). Conclude that, as a manifold, $O(2,\mathbb{R})$ is a disjoint union of two circles.

Exercise *Symplectic groups and canonical transformations*

Let q^i, p_i $i = 1, \dots n$ be coordinates and momenta for a classical mechanical system.

The **Poisson bracket** of two functions $f(q^1, \dots q^n, p_1, \dots p_n)$, $g(q^1, \dots q^n, p_1, \dots p_n)$ is defined to be

$$\{f, g\} = \sum_{i=1}^{n} \left(\frac{\partial f}{\partial q^i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial q^i} \right) \tag{2.34}$$

a.) Show that

$$\{q^i, q^j\} = \{p_i, p_j\} = 0 \qquad \{q^i, p_j\} = \delta^i{}_j \tag{2.35}$$

Suppose we define new coordinates and momenta Q^i, P_i to be linear combinations of the old:

$$\begin{pmatrix} Q^1 \\ \vdots \\ Q^n \\ P_1 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1,2n} \\ \vdots & \ddots & \vdots \\ a_{2n,1} & \cdots & a_{2n,2n} \end{pmatrix} \cdot \begin{pmatrix} q^1 \\ \vdots \\ q^n \\ p_1 \\ \vdots \\ p_n \end{pmatrix} \tag{2.36}$$

where $A = (a_{ij})$ is a constant $2n \times 2n$ matrix.

b.) Show that

$$\{Q^i, Q^j\} = \{P_i, P_j\} = 0 \qquad \{Q^i, P_j\} = \delta^i_j \tag{2.37}$$

if and only if A is a symplectic matrix.

Exercise *Direct Product Of Groups*

Definition Let G_1, G_2 be two groups. The *direct product* of G_1, G_2 is the set $G_1 \times G_2$ with product:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2') \tag{2.38}$$

a.) Check the group axioms.

b.) Generalize this to arbitrary products: Given a map $\mathcal{G}$ from a set I to the set of all groups define the product over I as a group.

c.) Interpret the direct product G^n of a group with itself n times as a group of the form $\mathcal{F}[X \to G]$ for some X.

Exercise *The Quaternion Group And The Pauli Group*

When working with spin-1/2 particles it is very convenient to introduce the standard Pauli matrices:

$$\sigma^1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.39}$$

$$\sigma^2 := \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \tag{2.40}$$

$$\sigma^3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.41}$$

a.) Show that they satisfy the identity, valid for all $1 \leq i, j \leq 3$:

$$\boxed{\boxed{\sigma^i\sigma^j = \delta^{ij} + \mathrm{i}\epsilon^{ijk}\sigma^k}} \tag{2.42}$$

b.) Show that the set of matrices

$$Q = \{\pm 1, \pm\mathrm{i}\sigma^1, \pm\mathrm{i}\sigma^2, \pm\mathrm{i}\sigma^3\} \tag{2.43}$$

forms a subgroup of order 8 of $SU(2) \subset GL(2, \mathbb{C})$. It is known as the *quaternion group.*

c.) Show that the set of matrices

$$P = \{\pm 1, \pm\mathrm{i}, \pm\sigma^1, \pm\sigma^2, \pm\sigma^3, \pm\mathrm{i}\sigma^1, \pm\mathrm{i}\sigma^2, \pm\mathrm{i}\sigma^3\} \tag{2.44}$$

forms a subgroup of $U(2) \subset GL(2, \mathbb{C})$ of order 16. It is known as the *Pauli group.*

Remark: [8] The Pauli group is often used in quantum information theory. If we think of the quantum Hilbert space of a spin 1/2 particle (isomorphic to $\mathbb{C}^2$ with standard inner product) then there is a natural basis of up and down spins: $v_1 = |\uparrow\rangle$ and $v_2 = |\downarrow\rangle$. Thinking of these as quantum analogs $|0\rangle$ and $|1\rangle$ of classical information bits $0, 1$ we see that $X = \sigma^1$ acts as a "bit flip," while Z acts as a "phase-flip." Y flips both bits and phases. These are then quantum error operators. Note that if we have a chain of N spin 1/2 particles then the N^{th} direct product

$$P^N = \underbrace{P \times \cdots \times P}_{N \text{ times}} \tag{2.45}$$

acts naturally on this chain of particles. [9] This group is useful in quantum information theory. For example if $H \subset P^N$ is a subgroup such that $(-1, ..., -1)$ is not in H then we can study the subspace of Hilbert space $\{\psi | g\psi = \psi, \quad \forall g \in H\}$. For astutely chosen subgroups these are useful quantum code subspaces, known as *stabilizer codes.*

---

3. Homomorphism and Isomorphism

Definition 3.1: Let $(G, \mathbf{m}, \mathbf{I}, e)$ and $(G', \mathbf{m}', \mathbf{I}', e')$ be two groups,

1.) A *homomorphism* from $(G, \mathbf{m}, \mathbf{I}, e)$ to $(G', \mathbf{m}', \mathbf{I}', e')$ is a mapping that preserves the group law. That is, it is a map of sets $\mu : G \to G'$ such that, for all $g_1, g_2 \in G$ we have:

$$\mu(\mathbf{m}(g_1, g_2)) = \mathbf{m}'(\mu(g_1), \mu(g_2)) \tag{3.1}$$

[8] Many terms used here will be more fully explained in Chapter 2.

[9] See 4.2 for the formal definition of a group action on a space.

2.) If μ is 1-1 and onto it is called an *isomorphism*.

3.) One often uses the term *automorphism* of G when μ is an isomorphism and $G = G'$, that is G and G' are literally the same set with the same multiplication law.

Remarks

1. We will henceforward be more informal and simply say that $\mu : G \to G'$ is a homomorphism of groups if, for all $g_1, g_2 \in G$:

$$\mu(\underbrace{g_1 g_2}_{\text{product in G}}) = \overbrace{\mu(g_1)\mu(g_2)}^{\text{product in G}'} \tag{3.2}$$

2. A common slogan is: "isomorphic groups are the same."

3. For each integer k we can define a homomorphism $\mu : Res(N) \to Res(N)$ by $\mu(\omega^j) = \omega^{jk}$. We will see later that this is an automorphism when k and N are relatively prime.

4. An example of a nontrivial automorphism of a group is to consider the integers modulo N, additively, $G = \mathbb{Z}/N\mathbb{Z}$. Now, for any integer k we can take

$$\mu(\bar{r}) := \overline{kr} \tag{3.3}$$

where on the right hand side $\overline{kr}$ is defined by first taking the ordinary multiplication of integers $k \times r$ (e.g. $2 \times 3 = 6$) and then reducing modulo N. As we will see later, when k is an integer relatively prime to N this is in fact an automorphism of G. For example in $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ if we take $k = 2$, or any even integer not divisible by 3, then μ exchanges $\bar{1}$ and $\bar{2}$. (Check that such an exchange is indeed a homomorphism!) We will discuss this kind of example in greater detail in Section §12 below.

♣This example is a bit out of place. Easier after we have quotient groups. ♣

5. One kind of homomomorphism is especially important:

Definition 3.2: A *matrix representation* of a group G is a homomorphism

$$T : G \to GL(n, \kappa) \tag{3.4}$$

for some positive integer n and field κ. (One can also have matrix representations in $GL(n, R)$ where R is a ring.)

Exercise *Preservation Of Structure*
Show that, for <u>any</u> group homomorphism μ we always have:

$$\mu(1_G) = 1_{G'} \tag{3.5}$$

$$\mu(g^{-1}) = \mu(g)^{-1} \tag{3.6}$$

Exercise *The Stupid Homomorphism*

Consider the map $\mu : G \to G'$ defined by $\mu(g) = 1_{G'}$. Show that this is a homomorphism.

Exercise *Some Simple Isomorphisms*

a.) Show that the exponential map $x \to e^x$ defines an isomorphism between the additive group $(\mathbb{R}, > 0)$ and the multiplicative group $(\mathbb{R}_+^*, \times)$.

b.) Use the exponential map to show that $Res(N)$ is isomorphic to $\mathbb{Z}_N$. Henceforth we will tend to use these groups interchangeably and often just use the notation $\mathbb{Z}_N$.

Exercise *The Quaternion Group*

Construct a homomorphism

$$\mu : Q \to \mathbb{Z}_2 \times \mathbb{Z}_2 \tag{3.7}$$

where Q is the Quaternion group (2.43).

Exercise *Subgroups of $\mathbb{Z}_N$*

a.) Show that the subgroups of $\mathbb{Z}_N$ are isomorphic to the groups $\mathbb{Z}_M$ for $M|N$.

b.) For $N = 8, M = 4$ write out H.

Exercise

Let S_2 be any set with two elements

a.) Show that there are exactly two possible group structures on S_2, and in each case construct an isomorphism of S_2 with $Res(2) \cong \mathbb{Z}_2$.

b.) Consider the matrix group of two elements:

$$\hat{S}_2 = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \} \tag{3.8}$$

with multiplication being matrix multiplication. Construct an isomorphism with S_2. [10]

Exercise *Some Simple Representations Of Res*(N)

Let $\omega = e^{2\pi i/N}$.

a.) Show that for any integer k

$$\mu(\omega^j) = \omega^{jk} \tag{3.10}$$

defines a representation of $Res(N)$ by 1×1 matrices.

b.) Show that

$$\mu : \omega^j \mapsto R(\frac{2\pi j}{N}) := \begin{pmatrix} \cos(\frac{2\pi j}{N}) & \sin(\frac{2\pi j}{N}) \\ -\sin(\frac{2\pi j}{N}) & \cos(\frac{2\pi j}{N}) \end{pmatrix} \tag{3.11}$$

defines a two-dimensional matrix representation of $\mathbb{Z}_N$.

c.) Let P be the $N \times N$ "shift matrix" all of whose matrix elements are zero except for 1's just below the diagonal and $P_{1,N} = 1$. See equation (10.19) below. Show that

$$\mu(\omega^j) = P^j \tag{3.12}$$

is an $N \times N$ dimensional representation of $Res(N)$.

Exercise *Two Characterizations Of Abelian Groups*

Let G be a group.

a.) Consider the map: $\mu : G \to G$ given by squaring: $\mu(g) = g^2$. Show that μ is a group homomorphism iff G is Abelian.

b.) Consider the map:

$$G \times G \to G \tag{3.13}$$

[10] *Answer*: Write $S_2 = \{e, \sigma\}$ with e the identity and $\sigma^2 = e$. Define $\mu : S_2 \to \hat{S}_2$

$$\begin{aligned} \mu(e) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \mu(\sigma) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned} \tag{3.9}$$

defined by group multiplication: $\mu(g_1, g_2) = \mathbf{m}(g_1, g_2) = g_1 g_2$. Show that μ is a group homomorphism iff G is Abelian.

Exercise *Fiber Products*

Given groups G_1 and G_2, and homomorphisms $\psi_1 : G_1 \to H$ and $\psi_2 : G_2 \to H$ one can define a subset of $G_1 \times G_2$ known as a *fiber product*:

$$G_1 \times_{\psi_1,\psi_2} G_2 := \{(g_1, g_2)|\psi_1(g_1) = \psi_2(g_2)\} \ . \tag{3.14}$$

Show that the fiber product is in fact a subgroup of $G_1 \times G_2$, where $G_1 \times G_2$ has the direct product group structure.

---

4. Equivalence Relations, Group Actions On Sets, And Orbits

4.1 Equivalence Relations

A very elementary, but very basic idea that we will use repeatedly is that of an *equivalence relation.*

A good reference for this elementary material is I.N. Herstein, *Topics in Algebra*, sec. 1.1.

Definition 4.1.1 . Let X be any set. A binary relation $\sim$ is an *equivalence relation* if $\forall a, b, c \in X$

1. $a \sim a$
2. $a \sim b \Rightarrow b \sim a$
3. $a \sim b$ and $b \sim c \Rightarrow a \sim c$

Example 4.1.1 : $\sim$ is $=$.

Example 4.1.2 : $X = \mathbb{Z}$, $a \sim b$ if $a - b$ is even.

Definition 4.1.2: Let $\sim$ be an equivalence relation on X. The *equivalence class* of an element a is

$$[a] \equiv \{x \in X : x \sim a\} \tag{4.1}$$

In the above two examples we have

Example 4.1.1' : $[a] = \{a\}$

Example 4.1.2' :

$[1] = \{n : n \text{ is an odd integer}\}$

$[4] = \{n : n \text{ is an even integer}\}$.

Here is a simple, but basic, principle:

The distinct equivalence classes of an equivalence relation on X decompose X into a union of mutually disjoint subsets. Conversely, given a *disjoint* decomposition $X = \amalg X_i$ we can define an equivalence relation by saying $a \sim b$ if $a, b \in X_i$.

For example, the integers are the disjoint union of the even and odd integers, and the corresponding equivalence relation is the one mentioned above: $a \sim b$ iff $a - b$ is even.

4.2 Group Actions On Sets

Recall that we defined:

Definition 1: Let X be any set. A *permutation* of X is a 1-1 and onto mapping $X \to X$. The set S_X of all permutations forms a group under composition.

In addition we say that

Definition 2: A *transformation group* on X is a subgroup of S_X.

This is a very important notion, and we will return to it extensively when discussing examples. If the following discussion seems too abstract the reader should consult the beginning of Chapter 3 for several concrete examples.

Another way to think about transformation groups is to define a *left G-action on a set* X to be a map $\phi : G \times X \to X$ compatible with the group multiplication law as follows:

$$\phi(g_1, \phi(g_2, x)) = \phi(g_1 g_2, x) \tag{4.2}$$

We would also like $x \mapsto \phi(1_G, x)$ to be the identity map. Now, equation (4.2) implies that

$$\phi(1_G, \phi(1_G, x)) = \phi(1_G, x) \tag{4.3}$$

which is compatible with, but does not quite imply that $\phi(1_G, x) = x$. Thus in defining a group action we must also impose the condition:

$$\phi(1_G, x) = x \qquad \forall x \in X. \tag{4.4}$$

Exercise

Give an example of a map $\phi : G \times X \to X$ that satisfies (4.2) but not (4.4). [11]

Yet another way to say this is the following: Define the map $\Phi : G \to S_X$ that takes $g \mapsto \phi(g, \cdot)$. That is, for each $g \in G$, $\Phi(g)$ is the function $X \to X$ taking $x \mapsto \phi(g, x)$. Clearly $\Phi(g_1) \circ \Phi(g_2) = \Phi(g_1 g_2)$ because of (4.2). In order to make sure it is a permutation we need to know that $\Phi(g)$ is invertible and therefore we need to impose that $\Phi(1_G)$ is the

[11] *Answer*: As the simplest example, choose any element $x_0 \in X$ and define $\phi(g, x) = x_0$ for all g, x. For a slightly less trivial example consider $G = S_2$ and let $\phi(e, x) = \phi(\sigma, x) = f(x)$. Then if $f \circ f(x) = f(x)$ the condition (4.2) will be satisfied, but there certainly exist functions with $f \circ f = f$ which are not the identity map.

identity transformation. This follows from (4.4). Then $\Phi(g) \in S_X$. So, to say we have a group action of G on X is to say that Φ is a homomorphism of G into the permutation group S_X. We will discuss G-actions on sets and their properties extensively in Chapter 3.

Definition: If X has a group action by a group G we say that X is a G-set.

Example: Let $G = GL(n, \kappa)$ and $X = \kappa^n$, the n-dimensional vector space over κ. Then the usual linear action on vectors defines a group action of G on X.

♣Give some other simple examples ♣

The following general abstract idea is of great importance in both mathematics and physics: Suppose X and Y are any two sets and $\mathcal{F}[X \to Y]$ is the set of functions from X to Y. Now suppose that there is a left G-action on X defined by $\phi : G \times X \to X$. Then, automatically, there is also a G action $\tilde{\phi}$ on $\mathcal{F}[X \to Y]$. To define it, suppose $F \in \mathcal{F}[X \to Y]$ and $g \in G$. Then we need to define $\tilde{\phi}(g, F) \in \mathcal{F}[X \to Y]$. We do this by setting $\tilde{\phi}(g, F)$ to be that specific function whose values are defined by:

$$\tilde{\phi}(g, F)(x) := F(\phi(g^{-1}, x)). \tag{4.5}$$

Note the inverse of g on the RHS. It is there so that the group law works out:

$$\begin{aligned} \tilde{\phi}(g_1, \tilde{\phi}(g_2, F))(x) &= \tilde{\phi}(g_2, F)(\phi(g_1^{-1}, x)) \\ &= F(\phi(g_2^{-1}, \phi(g_1^{-1}, x)) \\ &= F(\phi(g_2^{-1} g_1^{-1}, x)) \\ &= F(\phi((g_1 g_2)^{-1}, x)) \\ &= \tilde{\phi}(g_1 g_2, F)(x) \end{aligned} \tag{4.6}$$

and hence $\tilde{\phi}(g_1, \tilde{\phi}(g_2, F)) = \tilde{\phi}(g_1 g_2, F)$ as required for a group action. It should also be clear that $\tilde{\phi}(1_G, F) = F$.

In the above discussion we could impose various conditions, on the functions in $\mathcal{F}[X \to Y]$. For example, if X and Y are manifolds we could ask our maps to be continuous, differentiable, etc. The above discussion would be unchanged.

As just one (important) example of this general idea: In field theory if we have fields on a spacetime, and a group of symmetries acting on that spacetime then that group also acts on the space of fields.

Exercise *When Y Is A G-Set*

Suppose there is a left G-action on a set Y and X is any set. Show that there is a natural left G-action on $\mathcal{F}[X \to Y]$.

4.3 Orbits

If G acts on a set X then we can define an equivalence relation on X by saying that two elements $x_1, x_2 \in X$ are equivalent, $x_1 \sim x_2$ if there is some $g \in G$ with $\phi(g, x_1) = x_2$. The reader should check that this is indeed an equivalence relation. The equivalence class $[x]$ with this equivalence relation is known as the *orbit of G through a point x*. So, concretely it is the set of points $y \in X$ which can be reached by the action of G:

$$O_G(x) = \{y : \exists g \quad \text{such that} \quad y = g \cdot x\} \tag{4.7}$$

The notion of orbits is very important in geometry, gauge theory and many other subjects.

The *set of orbits* is denoted X/G. We will discuss many examples below.

5. The Symmetric Group.

The symmetric group is an important example of a finite group. As we shall soon see, all finite groups are isomorphic to subgroups of the symmetric group.

Recall from section 2 above that for any set X we can define a group S_X of all permutations of the set X. If n is a positive integer the symmetric group on n elements, denoted S_n, is defined as the group of permutations of the set $X = \{1, 2, \dots, n\}$.

In group theory, as in politics, there are leftists and rightists and we can actually define *two* group operations:

$$\begin{aligned}(\phi_1 \cdot_L \phi_2)(i) &:= \phi_2(\phi_1(i)) \\ (\phi_1 \cdot_R \phi_2)(i) &:= \phi_1(\phi_2(i))\end{aligned} \tag{5.1}$$

That is, with $\cdot_L$ we read the operations from left to right and first apply the left permutation, and then the right permutation. Etc. Each convention has its own advantages and both are frequently used.

In these notes we will adopt the $\cdot_R$ convention and henceforth simply write $\phi_1\phi_2$ for the product.

We can write a permutation symbolically as

$$\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix} \tag{5.2}$$

meaning: $\phi(1) = p_1, \phi(2) = p_2, \dots, \phi(n) = p_n$. Note that we could equally well write the same permutation as:

$$\phi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p_{a_1} & p_{a_2} & \cdots & p_{a_n} \end{pmatrix} \tag{5.3}$$

where $a_1, \dots, a_n$ is any permutation of $1, \dots, n$. With this understood, suppose we want to compute $\phi_1 \cdot_L \phi_2$. We should first see what ϕ_1 does to the ordered elements $1, \dots, n$, and then see what ϕ_2 does to the ordered output from ϕ_1. So, if we write:

$$\begin{aligned}\phi_1 &= \begin{pmatrix} 1 & \cdots & n \\ q_1 & \cdots & q_n \end{pmatrix} \\ \phi_2 &= \begin{pmatrix} q_1 & \cdots & q_n \\ p_1 & \cdots & p_n \end{pmatrix}\end{aligned} \tag{5.4}$$

Then

$$\phi_1 \cdot_L \phi_2 = \begin{pmatrix} 1 & \cdots & n \\ p_1 & \cdots & p_n \end{pmatrix} \tag{5.5}$$

On the other hand, to compute $\phi_1 \cdot_R \phi_2$ we should first see what ϕ_2 does to $1, \dots, n$ and then see what ϕ_1 does to that output. We could write represent this as:

$$\begin{aligned} \phi_2 &= \begin{pmatrix} 1 & \cdots & n \\ q'_1 & \cdots & q'_n \end{pmatrix} \\ \phi_1 &= \begin{pmatrix} q'_1 & \cdots & q'_n \\ p'_1 & \cdots & p'_n \end{pmatrix} \end{aligned} \tag{5.6}$$

and then

$$\phi_1 \cdot_R \phi_2 = \begin{pmatrix} 1 & \cdots & n \\ p'_1 & \cdots & p'_n \end{pmatrix} \tag{5.7}$$

Exercise

a.) Show that the order of the group is $|S_n| = n!$.

b.) Show that if $n_1 \le n_2$ then we can consider S_{n_1} as a subgroup of S_{n_2}.

c.) In how many ways can you consider S_2 to be a subgroup of S_3? [12]

d.) In how many ways can you consider S_{n_1} to be a subgroup of S_{n_2} when $n_1 \le n_2$? [13]

Exercise Show that the inverse of (5.2) is the permutation:

$$\phi = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ 1 & 2 & \cdots & n \end{pmatrix} \tag{5.8}$$

It is often useful to visualize a permutation in terms of "time evolution" (going up) as shown in 1.

Exercise *Left versus right*

[12] *Answer*: There are three subgroups of S_3 isomorphic to S_2. They are the subgroups that fix $1, 2, 3$ respectively.

[13] *Answer*: for any subset $T \subset \{1, \dots, n_2\}$ of cardinality $n_2 - n_1$ we can consider the subset of permutations that fix all elements of T. This subset of permutations will be a subgroup isomorphic to S_{n_1}. So there are $\binom{n_2}{n_1}$ distinct subgroups isomorphic to S_{n_1}.

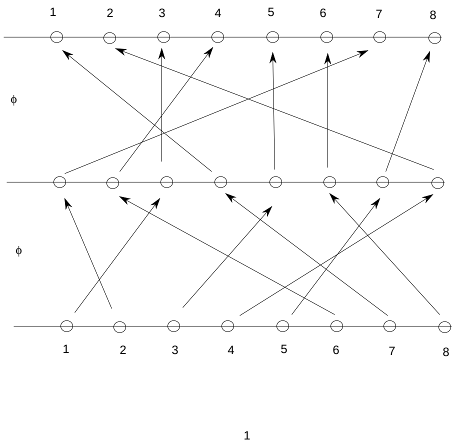

Figure 1: A pictorial view of the composition of two permutations ϕ_1, ϕ_2 in S_8. Thus $1 \to 3, 2 \to 7$ etc. for the group product $\phi_2 \cdot \phi_1$.

a.) Show that in the pictorial interpretation the inverse is obtained by running arrows backwards in time.

b.) Show that the left- and right- group operation conventions are related by

$$\phi_1 \cdot_L \phi_2 = (\phi_1^{-1} \cdot_R \phi_2^{-1})^{-1} \tag{5.9}$$

c.) Interpret (5.9) as the simple statement that $\phi_1 \cdot_R \phi_2$ puts ϕ_2 in the past while $\phi_1 \cdot_L \phi_2$ puts ϕ_1 in the past.

5.1 Cayley's Theorem

As a nice illustration of some of the concepts we have introduced we now prove Cayley's theorem. This theorem states that *any* finite group is isomorphic to a subgroup of a permutation group S_N for some N.

To prove this we begin with an elementary, but important, observation known as the

The rearrangement lemma: Consider a totally ordered group, that is, we can list the group elements in order

$$G = \{g_1, g_2, \dots, \} \tag{5.10}$$

Consider this as an ordered set, with all the g_i distinct. The set can be finite or infinite. Then, for any $h \in G$ consider the ordered set:

$$h \cdot G = \{h \cdot g_1, h \cdot g_2, \dots, \}. \tag{5.11}$$

With a little thought you can (and should) convince yourself that (5.11) is a a permutation of (5.10): No two elements coincide (since the $g_i \neq g_j$ for $i \neq j$) and every element of G must appear in the list $h \cdot G$.

To put this differently, there is a left-G-action of G on itself: For $h \in G$, define the map $L(h) : G \to G$ by the rule:

$$L(h) : g \mapsto h \cdot g \qquad \forall g \in G. \tag{5.12}$$

This map is one-one and invertible so $L(h) \in S_G$, the group of permutations of the set G. (In fact, there is no need to assume G is totally ordered.) Now note that

$$L(h_1) \circ L(h_2) = L(h_1 \cdot h_2) \tag{5.13}$$

so the map $\mathcal{L}$ defined by $\mathcal{L} : h \mapsto L(h)$ is a homomorphism

$$\mathcal{L} : G \to S_G \tag{5.14}$$

This is an example of a group action on a set. In this case $X = G$ and G is acting on itself by left-multiplication and $\mathcal{L}$ is the quantity denoted by Φ above. Furthermore, if $L(h_1) = L(h_2)$ then $h_1 = h_2$. Therefore $\mathcal{L}$ is an isomorphism of G with its image in S_G. [14]

The above remarks apply to any group. However, now consider any finite group G with $N = |G|$ then S_G is isomorphic to S_N. Therefore, any finite group is isomorphic to a subgroup of a symmetric group S_N for some N. This is Cayley's theorem. Note that which subgroup of S_N we obtain depends on how we choose to order G, that is, it depends on the choice of isomorphism $S_G \cong S_N$.

Exercise *Concrete Example*

By Cayley's theorem the cyclic group $\mathbb{Z}_n$ of order n is isomorphic to a subgroup of a permutation group. Exhibit such an isomorphic subgoup. [15]

Exercise *Right Action*

There are other ways G can act on itself. For example we can define

♣This is redundant with some material on group actions below. ♣

$$R(a) : g \mapsto g \cdot a \tag{5.15}$$

a.) Show that $R(a)$ permutes the elements of G.

b.) Show that $R(a_1) \circ R(a_2) = R(a_2 a_1)$. Thus, $a \mapsto R(a)$ is not a homomorphism of G into the group S_G of permutations of G.

c.) Show that $a \mapsto R(a^{-1})$ is a homomorphism of G into S_G.

---

[14] This last step actually assumes the result in equation (10.10) below.

[15] *Answer*: Choose any cyclic permutation of length n (Cyclic permutations are defined in Section 5.2 below.) Then it generates a subgroup of S_N of length n for any $N \geq n$.

5.2 Cyclic Permutations And Cycle Decomposition

A very important class of permutations are the *cyclic permutations of length ℓ*. Choose ℓ distinct numbers, $a_1, \dots, a_\ell$ between 1 and n and permute:

$$a_1 \to a_2 \to \cdots \to a_\ell \to a_1 \tag{5.16}$$

holding all other $n - \ell$ elements fixed. This permutation is denoted as

$$\phi = (a_1 a_2 \dots a_\ell). \tag{5.17}$$

Of course, this permutation can be written in ℓ different ways:

$$(a_1 a_2 \dots a_\ell) = (a_2 a_3 \dots a_\ell a_1) = (a_3 \dots a_\ell a_1 a_2) = \cdots = (a_\ell a_1 a_2 \dots a_{\ell-1}) \tag{5.18}$$

So:

$$S_2 = \{1, (12)\} \tag{5.19}$$

$$S_3 = \{1, (12), (13), (23), (123), (132)\} \tag{5.20}$$

but it is not true that all permutations are just cyclic permutations, as we first see by considering S_4:

$$\begin{aligned} S_4 = \{1, (12), (13), (14), &(23), (24), (34), (12)(34), (13)(24), (14)(23), \\ (123), (132), (124), (142), &(134), (143), (234), (243) \\ &(1234), (1243), (1324), (1342), (1423), (1432)\} \end{aligned} \tag{5.21}$$

Now a key observation is:

Any permutation $\sigma \in S_n$ can be uniquely written as a product of disjoint cycles. This is called the cycle decomposition of σ.

For example

$$\sigma = (12)(34)(10, 11)(56789) \tag{5.22}$$

is a cycle decomposition in S_{11}. There are 3 cycles of length 2 and 1 of length 5.

The decomposition into products of disjoint cycles is known as the *cycle decomposition.*

Remarks

1. S_2 is abelian.
2. S_3 is NOT ABELIAN[16]

$$\begin{aligned} (12) \cdot (13) &= (132) \\ (13) \cdot (12) &= (123) \end{aligned} \tag{5.23}$$

   and therefore so is S_n for $n > 2$.

[16] Note that $(12) \cdot_L (13) = (123)$.

Exercise *Decomposition as a product of disjoint cyclic permutations*

Prove the above claim: every permutation above is a product of cyclic permutations on disjoint sets of integers. [17]

Exercise

a.) Let ϕ be a cyclic permutation of order ℓ. Suppose we compose ϕ with itself N times. Show that the result is the identity transformation iff ℓ divides N.

b.) Suppose ϕ has a cycle decomposition with cycles of length $k_1, \dots, k_s$. What is the smallest number N so that if we compose ϕ with itself $\phi \circ \cdots \circ \phi$ for N times that we get the identity transformation?

5.3 Transpositions

A *transposition* is a permutation of the form: (ij). These satisfy some nice properties: Suppose i, j, k are distinct. You can check as an exercise that transpositions obey the following identities:

$$\begin{aligned} (ij)\cdot(jk)\cdot(ij) = (ik) &= (jk)\cdot(ij)\cdot(jk) \\ (ij)^2 &= 1 \\ (ij)\cdot(kl) = (kl)\cdot(ij) & \qquad \{i,j\}\cap\{k,l\} = \emptyset \end{aligned} \tag{5.24}$$

The first identity is illustrated in Figure 2. Draw the other two.

We observed above that there is a cycle decomposition of permutations. Now note that

Any cycle $(a_1, \cdots, a_k)$ *can be written as a product of transpositions.* To prove this note that

$$(1,k)(1,k-1)\cdots(1,4)(1,3)(1,2) = (1,2,3,4,\dots,k) \tag{5.25}$$

Now, consider a permutation that takes

$$1 \to a_1, \quad 2 \to a_2, \quad 3 \to a_3, \cdots, k \to a_k \tag{5.26}$$

For our purposes, it won't really matter what it does to the other integers greater than k. Choose any such permutation and call it ϕ. Note that

$$\phi \circ (1\ 2\ \cdots\ k) \circ \phi^{-1} = (a_1\ a_2\ \cdots\ a_k) \tag{5.27}$$

[17] *Answer*: Use induction: Consider any element, say $n \in \{1, \dots, n\}$ and let ϕ be a permutation. Consider the elements $n, \phi(n), \phi(\phi(n)), \dots$. This must be a finite set C, so we get a cyclic permutation of the elements in C. Then ϕ must permute all the elements in $\{1, \dots, n\} - C$. But this has cardinality strictly smaller than n. So, use the inductive hypothesis.

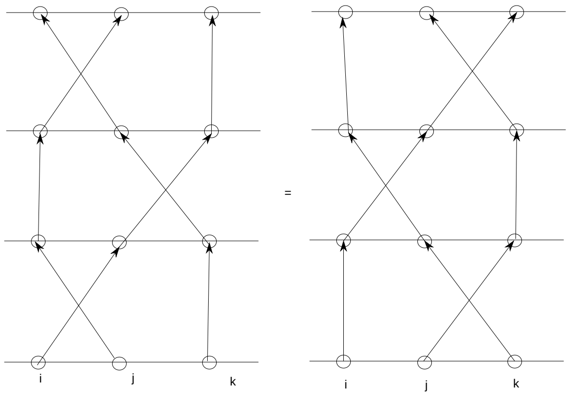

Figure 2: Pictorial illustration of equation (4.21) line one for transpositions where $i < j < k$. Note that the identity is suggested by "moving the time lines" holding the endpoints fixed. Reading time from bottom to top corresponds to reading the composition from left to right in the $\cdot_R$ convention.

so now conjugate the above identity by ϕ to get a decomposition of $(a_1\ a_2\ \cdots\ a_k)$ as a product of transpositions.

Therefore, *every element of S_n can be written as a product of transpositions, generalizing* (5.23)*.* We say that the transpositions *generate* the permutation group. Taking products of various transpositions – what we might call a "word" whose "letters" are the transpositions – we can produce any element of the symmetric group. We will return to this notion in §6 below.

Of course, a given permutation can be written as a product of transpositions in many ways. This clearly follows because of the identities (5.24). A nontrivial fact is that the transpositions together with the above relations generate precisely the symmetric group. [18] It therefore follows that all possible nontrivial identities made out of transpositions follow from repeated use of these identities.

Although permutations can be written as products of transpositions in different ways, the number of transpositions in a word *modulo 2* is always the same, because the identities (5.24) have the same number of transpositions, modulo two, on the LHS and RHS. Thus we can define *even, resp. odd, permutations* to be products of even, resp. odd numbers of transpositions.

Definition: The *alternating group* $A_n \subset S_n$ is the subgroup of S_n of even permutations.

Exercise

[18] This follows once one has shown that the Coxeter presentation given below gives precisely the symmetric group, and not some larger group (requiring the imposition of further relations) since the above relations all follow from the Coxeter relations.

a.) What is the order of A_n ? [19]

b.) Write out A_2, A_3, and A_4. Show that A_3 is isomorphic to $\mathbb{Z}_3$.

Exercise

When do two cyclic permutations commute? Illustrate the answer with pictures, as above.

Exercise *A Smaller Set Of Generators*

Show that from the transpositions $\sigma_i := (i, i+1)$, $1 \leq i \leq n-1$ we can generate all other transpositions in S_n. These are sometimes called the elementary generators.

Exercise *An Even Smaller Set Of Generators*

Show that, in fact, S_n can be generated by just two elements: (12) and $(1\ 2\ \cdots\ n)$. [20]

Exercise *Center of S_n*

What is the center of S_n? [21]

Exercise *Decomposing the reverse shuffle*

Consider the permutation which takes $1, 2, \ldots, n$ to $n, n-1, \ldots, 1$.

a.) Write the cycle decomposition.

[19] *Answer*: $\frac{1}{2}n!$ for $n > 1$. To prove this note that the transformation $\phi \to \phi \circ (12)$ is an invertible transformation $S_n \to S_n$ that squares to the identity. On the other hand, it exchanges even and odd permutations.

[20] *Answer*: Conjugate (12) by the n-cycle to get (23). Then conjugate again to get (34) and so forth. Now we have the set of generators of the previous exercise.

[21] *Answer*: If $n = 2$ then S_n is Abelian and the center is all of S_2. If $n > 2$ then the center is the trivial group. To prove this suppose $z \in Z(S_n)$. If z is not the trivial element then it moves some i to some j. WLOG we can say it moves 1 to $i \neq 1$. Then $z(i) \neq i$. If $z(i) = 1$ then z is the transposition $(1, i)$. If $n > 2$ there will be some other $j \neq 1, i$ and z will not commute with $(1, j)$. If $z(i) = j$ with $j \neq 1, i$ then $\phi = (1, i)$ does not commute with z because $z\phi$ takes $1 \to j$ and ϕz takes $1 \to 1$.

b.) Write a decomposition of this permutation in terms of the *elementary generators* σ_i. [22]

Example 3.2 *The sign homomorphism.*

This is a very important example of a homomorphism:

$$\epsilon : S_n \to \mathbb{Z}_2 \tag{5.28}$$

where we identify $\mathbb{Z}_2$ as the multiplicative group $\{\pm 1\}$ of square roots of 1. The rule is:

$\epsilon : \sigma \to +1$ if σ is a product of an *even* number of transpositions.

$\epsilon : \sigma \to -1$ if σ is a product of an *odd* number of transpositions.

Put differently, we could define $\epsilon(ij) = -1$ for any transposition. This is compatible with the words defining the relations on transpositions. Since the transpositions generate the group the homomorphism is well-defined and completely determined.

In physics one often encounters the sign homomorphism in the guise of the "epsilon tensor" denoted:

$$\epsilon_{i_1 \cdots i_n} \tag{5.29}$$

Its value is:

1. $\epsilon_{i_1 \cdots i_n} = +1$ if
$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{5.30}$$
is an even permutation.

2. $\epsilon_{i_1 \cdots i_n} = -1$ if
$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{5.31}$$
is an odd permutation.

3. $\epsilon_{i_1 \cdots i_n} = 0$ if two indices are repeated. (This goes a bit beyond what we said above since in that case we are not discussing a permutation.)

So, e.g. among the 27 entries of ϵ_{ijk}, $1 \le i,j,k \le 3$ we have

$$\begin{aligned} \epsilon_{123} &= 1 \\ \epsilon_{132} &= -1 \\ \epsilon_{231} &= +1 \\ \epsilon_{221} &= 0 \end{aligned} \tag{5.32}$$

and so forth.

[22] *Hint*: Use the pictorial interpretation mentioned above.

Exercise
Show that

$$\epsilon_{i_1 i_2 \cdots i_n} \epsilon_{j_1 j_2 \cdots j_n} = \sum_{\sigma \in S_n} \epsilon(\sigma) \delta_{i_1 j_{\sigma(1)}} \delta_{i_2 j_{\sigma(2)}} \cdots \delta_{i_n j_{\sigma(n)}} \tag{5.33}$$

This formula is often useful when proving identities involving determinants. An important special case occurs for $n = 3$ where it is equivalent to the rule for the cross-product of 3 vectors in $\mathbb{R}^3$:

$$\vec{A} \times (\vec{B} \times \vec{C}) = \vec{B}(\vec{A} \cdot \vec{C}) - \vec{C}(\vec{A} \cdot \vec{B}) \tag{5.34}$$

The next two exercises assume some familiarity with concepts from linear algebra. See Chapter 2 below if they are not familiar.

Exercise *A Matrix Representation Of S_n*
Consider the standard Euclidean vector space $\mathbb{R}^n$ (or $\mathbb{C}^n$ or κ^n) with basis vectors $\vec{e}_1, \dots, \vec{e}_n$ where $\vec{e}_i$ has component 1 in the i^{th} position and zero else. Note that the symmetric group permutes these vectors in an obvious way:

$$T(\phi) : \vec{e}_i \to \vec{e}_{\phi(i)} \ , \tag{5.35}$$

and now extend by linearity so that

$$T(\phi) : \sum_{i=1}^{n} x_i e_i \mapsto \sum_{i=1}^{n} x_i e_{\phi(i)} = \sum_{i=1}^{n} x_{\phi^{-1}(i)} e_i \tag{5.36}$$

Thus to any permutation $\phi \in S_n$ we can associate a linear transformation $T(\phi)$. The matrix $A(\phi)$ of $T(\phi)$ defined by $T(\phi)$ and the ordered basis $\{e_1, \dots, e_n\}$ is defined by:

$$T(\phi)\vec{e}_i = \sum_{j=1}^{n} A(\phi)_{ji} \vec{e}_j \tag{5.37}$$

a.) Write out $A(\phi)$ for small values of n and some simple permutations ϕ.

b.) Write a general formula for the matrix elements of $A(\phi)$. [23]

c.) Show that $\phi \to A(\phi)$ is a matrix representation of S_n.

d.) The matrices $A(\phi)$ are called *permutation matrices.* In each row and column there is only one nonzero matrix element, and it is 1. If B is any other $n \times n$ matrix show that

$$\left(A(\phi) B A(\phi)^{-1}\right)_{i,j} = B_{\phi(i),\phi(j)} \tag{5.38}$$

[23] *Answer*: $A(\phi)_{i,j} = \delta_{i,\phi(j)} = \delta_{\phi^{-1}(i),j}$.

Exercise *Signed Permutation Matrices*

Define *signed permutation matrices* to be invertible matrices such that in each row and column there is only one nonzero matrix element, and the nonzero matrix element can be either $+1$ or -1. Finally, require the matrix to be invertible.

a.) Show that the set of $n \times n$ signed permutation matrices form a group. We will call it $W(B_n)$ for reasons that will not be obvious for a while.

b.) Define a group homomorphism $W(B_n) \to S_n$.

5.4 Diversion and Example: Card shuffling

One way we commonly encounter permutation groups is in shuffling a deck of cards.

A deck of cards is equivalent to an ordered set of 52 elements. Some aspects of card shuffling and card tricks can be understood nicely in terms of group theory.

Mathematicians often use the *perfect shuffle* or the *Faro shuffle*. Suppose we have a deck of $2n$ cards, so $n = 26$ is the usual case. There are actually two kinds of perfect shuffles: the In-shuffle and the Out-shuffle.

In either case we begin by splitting the deck into two equal parts, and then we interleave the two parts perfectly.

Let us call the top half of the deck the left half-deck and the bottom half of the deck the right half-deck. Then, to define the *Out-shuffle* we put the top card of the left deck on top, followed by the top card of the right deck underneath, and then proceed to interleave them perfectly. The bottom and top cards stay the same.

If we number the cards $0, 1, \dots, 2n-1$ from top to bottom then the top (i.e. left) half-deck consists of the cards numbered $0, 1, \dots, n-1$ while the bottom (i.e. right) half-deck consists of the cards $n, n+1, \dots, 2n-1$. Then the Out-shuffle gives the cards in the new order

$$0, n, 1, n+1, 2, n+2, \dots, n+2, 2n-2, n-1, 2n-1 \tag{5.39}$$

Another way to express this is that the Out-shuffle defines a permutation of $\{0, 1, \dots, 2n-1\}$. If we let C_x, $0 \le x \le 2n-1$ denote the cards in the original order then the new ordered set of cards C'_x are related to the old ones by:

$$C'_{\mathcal{O}(x)} = C_x \tag{5.40}$$

where

$$\mathcal{O}(x) = \begin{cases} 2x & x \le n-1 \\ 2x - (2n-1) & n \le x \le 2n-1 \end{cases} \tag{5.41}$$

Note that this already leads to a card trick: Modulo $(2n-1)$ the operation is just $x \to 2x$, so if k is the smallest number with $2^k = 1\text{mod}(2n-1)$ then k Out-shuffles will restore the deck perfectly.

For example: For a standard deck of 52 cards, $2^8 = 5 \times 51 + 1$ so 8 perfect Out-shuffles restores the deck!

We can also see this by working out the cycle presentation of the Out-shuffle:

$$\begin{aligned}\mathcal{O} = &(0)(1,2,4,8,16,32,13,26)(3,6,12,24,48,45,39,27)\\ &(5,10,20,40,29,7,14,28)(9,18,36,21,42,33,15,30)\\ &(11,22,44,37,23,46,41,31)(17,34)(19,38,25,50,49,47,43,35)(51)\end{aligned} \tag{5.42}$$

Clearly, the 8^{th} power gives the identity permutation.

Now, to define the *In-shuffle* we put the top card of the right half-deck on top, then the top card of the left half-deck underneath, and then proceed to interleave them.

Now observe that if we have a deck with $2n$ cards $\mathcal{D}(2n) := \{0, 1, \dots, 2n-1\}$ and we embed it in a Deck with $2n + 2$ cards

$$\mathcal{D}(2n) \to \mathcal{D}(2n+2) \tag{5.43}$$

by the map $x \to x + 1$ then *the Out-shuffle on the deck* $\mathcal{D}(2n + 2)$ *permutes the cards* $1, \dots, 2n$ *amongst themselves and acts as an In-shuffle on these cards!*

♣Explain this some more, e.g. by illustrating with a pack of 6 cards. ♣

Therefore, applying our formula for the Out-shuffle we find that the In-shuffle is given by the formula

$$\mathcal{I}(x) = \begin{cases} 2(x+1) - 1 & x + 1 \leq n \\ 2(x+1) - (2n+1) - 1 & n \leq x \leq 2n-1 \end{cases} \tag{5.44}$$

One can check that this is given by the uniform formula

$$\mathcal{I}(x) = (2x+1) \bmod (2n+1) \tag{5.45}$$

for $x \in \mathcal{D}(2n)$.

For $2n = 52$ this turns out to be one big cycle!

$$\begin{gathered}(0,1,3,7,15,31,10,21,43,34,16,33,14,29,6,13,27,2,5,\\ 11,23,47,42,32,12,25,51,50,48,44,36,20,41,30,8,17,\\ 35,18,37,22,45,38,24,49,46,40,28,4,9,19,26)\end{gathered} \tag{5.46}$$

so it takes 52 consecutive perfect In-shuffles to restore the deck.

One can do further magic tricks with In- and Out-shuffles. As one example there is a simple prescription for bringing the top card to any desired position, say, position ℓ by doing In- and Out-shuffles.

To do this we write ℓ in its binary expansion:

$$\ell = 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2^1 + a_0 \tag{5.47}$$

where $a_j \in \{0, 1\}$. Interpret the coefficients 1 as In-shuffles and the coefficients 0 as Out-shuffles. Then, reading from left to right, perform the sequence of shuffles given by the binary expression: $1a_{k-1}a_{k-2} \cdots a_1 a_0$.

To see why this is true consider iterating the functions $o(x) = 2x$ and $i(x) = 2x + 1$. Notice that the sequence of operations given by the binary expansion of ℓ are

$$\begin{aligned}
0 &\to 1 \\
&\to 2 \cdot 1 + a_{k-1} \\
&\to 2 \cdot (2 \cdot 1 + a_{k-1}) + a_{k-2} = 2^2 + 2a_{k-1} + a_{k-2} \\
&\to 2 \cdot (2^2 + 2a_{k-1} + a_{k-2}) + a_{k-3} = 2^3 + 2^2 a_{k-1} + 2a_{k-2} + a_{k-3} \\
\vdots \quad &\vdots \\
&\to 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2^1 + a_0 = \ell
\end{aligned} \tag{5.48}$$

For an even ordered set we can define a notion of permutations preserving *central symmetry*. For $x \in D_{2n}$ let $\bar{x} = 2n - 1 - x$. Then we define the group $W(B_n) \subset S_{2n}$ to be the subgroup of permutations which permutes the pairs $\{x, \bar{x}\}$ amongst themselves.

Note that there is clearly a homomorphism

$$\phi : W(B_n) \to S_n \tag{5.49}$$

Moreover, both $\mathcal{O}$ and $\mathcal{I}$ are elements of $W(B_n)$. Therefore the *shuffle group*, the group generated by these is a subgroup of $W(B_n)$. Using this one can say some nice things about the structure of the group generated by the in-shuffle and the out-shuffle. It was completely determined in a beautiful paper (the source of the above material):

"The mathematics of perfect shuffles," P. Diaconis, R.L. Graham, W.M. Kantor, Adv. Appl. Math. **4** pp. 175-193 (1983)

It turns out that shuffles of decks of 12 and 24 cards have some special properties. In particular, special shuffles of a deck of 12 cards can be used to generate a very interesting group known as the Mathieu group M_{12}. It was, historically, the first "sporadic" finite simple group. See section §15.4 below.

To describe M_{12} we need to introduce a *Mongean shuffle*. Here we take the deck of cards put the top card on the right. Then from the deck on the left alternatively put cards on the top or the bottom. So the second card from of the deck on the left goes on top of the first card, the third card from the deck on the left goes under the first card, and so on. If we label our deck as cards $1, 2, \dots, 2n$ then the Mongean shuffle is:

$$m : \{1, 2, \dots, 2n\} \to \{2n, 2n-2, \dots, 4, 2, 1, 3, 5, \dots, 2n-3, 2n-1\} \tag{5.50}$$

In formulae, acting on $\mathcal{D}(2n)$

$$m(x) = \text{Min}[2x, 2n + 1 - 2x] \tag{5.51}$$

In particular for $2n = 12$ we have

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \to \{12, 10, 8, 6, 4, 2, 1, 3, 5, 7, 9, 11\} \tag{5.52}$$

which has cycle decomposition (check!)

$$(3\ 8) \cdot (1\ 12\ 11\ 9\ 5\ 4\ 6\ 2\ 10\ 7) \tag{5.53}$$

Now consider the *reverse shuffle* that simply orders the cards backwards. In general for a deck $\mathcal{D}(2n)$ with $n = 2\text{mod}4$ Diaconis et. al. show that r and m generate the entire symmetric group. However, for a pack of 12 cards r and m generate the Mathieu group M_{12}. It turns out to have order

$$|M_{12}| = 2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95040 \tag{5.54}$$

Compare this with the order of S_{12}:

$$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 = 479001600 \tag{5.55}$$

So with the uniform probability distribution on S_{12}, the probability of finding a Mathieu permutation is $\frac{1}{5040} \sim 2 \times 10^{-4}$.

We mention some final loosely related facts:

1. There are indications that the Mathieu groups have some intriguing relations to string theory, conformal field theory, and K3 surfaces.

2. In the theory of L_∞ algebras and associated topics, which are closely related to string field theory one encounters the concept of the k-shuffle...

   FILL IN.

Exercise *Cycle structure for the Mongean shuffle*

Write the cycle structure for the Mongean shuffle of a deck with 52 cards. How many Mongean shuffles of such a deck will restore the original order?

---

6. Generators and relations

The presentation (5.24) of the symmetric group is an example of presenting a group by *generators and relations.*

Definition 6.1 A subset $\mathcal{S} \subset G$ is a *generating set* for a group if every element $g \in G$ can be written as a "word" or product of elements of $\mathcal{S}$. That is any element $g \in G$ can be written in the form

$$g = s_{i_1} \cdots s_{i_r} \tag{6.1}$$

where, for each $1 \leq k \leq r$ we have $s_{i_k} \in \mathcal{S}$.

Finitely generated means that the generating set $\mathcal{S}$ is finite, that is, there is a finite list of elements $\{s_1, \dots s_n\}$ so that all elements of the group can be obtained by taking products – "words" – in the "letters" drawn from $\mathcal{S}$. For example, the symmetric group is finitely generated by the transpositions. Typical Lie groups are not finitely generated.

The *relations* are then equalities between different words such that any two equivalent words in G can be obtained by successively applying the relations. [24]

In general if we have a finitely generated group we write

$$G = \langle g_1, \dots, g_n | R_1, \cdots R_r \rangle \tag{6.2}$$

where R_i are words in the letters of $\mathcal{S}$ which will be set to 1. **ALL** other relations, that is, all other identities of the form $W = 1$ are supposed to be consequences of these relations.

Remark: It is convenient to exclude the unit 1 from $\mathcal{S}$. When we write our words it is understood that we can raise a generator s to any integer power s^n where, $s^0 = 1$ and, if $n < 0$, this means $(s^{-1})^{|n|}$. Alternatively, we can, for each generator s introduce another generator t, which will play the role of s^{-1} and then impose another relation $st = ts = 1_G$. A generating set that contains s^{-1} for every generator s is said to be *symmetric*.

Example 2.1: If $\mathcal{S}$ consists of one element a then $F(\mathcal{S}) \cong \mathbb{Z}$. The isomorphism is given by mapping $n \in \mathbb{Z}$ to the word a^n.

Example 2.2: The group defined by

$$\langle a | a^N = 1 \rangle \tag{6.3}$$

is an abelian group of N elements. In fact it is isomorphic to the cyclic group $\mathbb{Z}_N$.

Example 2.3: *Free groups.* If there are no relations then we have the free group on $\mathcal{S}$, denoted $F(\mathcal{S})$. If $\mathcal{S}$ consists of one element then we just get $\mathbb{Z}$, as above. However, things are completely different if $\mathcal{S}$ consists of two elements a, b. Then $F(\mathcal{S})$ is very complicated. A typical element looks like one of

$$\begin{aligned} &a^{n_1} b^{m_1} \cdots a^{n_k} \\ &a^{n_1} b^{m_1} \cdots b^{m_k} \\ &b^{n_1} a^{m_1} \cdots a^{n_k} \\ &b^{n_1} a^{m_1} \cdots b^{m_k} \end{aligned} \tag{6.4}$$

where n_i, m_i are nonzero integers (positive or negative).

♣Say what the cardinality of the free group is ♣

Combinatorial group theorists use the notion of a *Cayley graph* to illustrate groups presented by generators and relations. Assuming that $1 \notin \mathcal{S}$ the Cayley graph is a graph whose vertices correspond to all group elements in G and the oriented edges are drawn between g_1 and g_2 if there is an $s \in \mathcal{S}$ with $g_2 = g_1 s$. We label the edge by s. (If $\mathcal{S}$ is symmetric we can identify this edge with the edge from g_2 to g_1 labeled by s^{-1}.) For the free group on two elements this generates the graph shown in Figure 3.

Example 2.4: *Coxeter groups*: Let m_{ij} by an $n \times n$ symmetric matrix whose entries are positive integers or ∞, such that $m_{ii} = 1$, $1 \leq i \leq n$, and $m_{ij} \geq 2$ or $m_{ij} = \infty$ for $i \neq j$.

[24] See Jacobsen, *Basic Algebra I*, sec. 1.11 for a more precise definition.

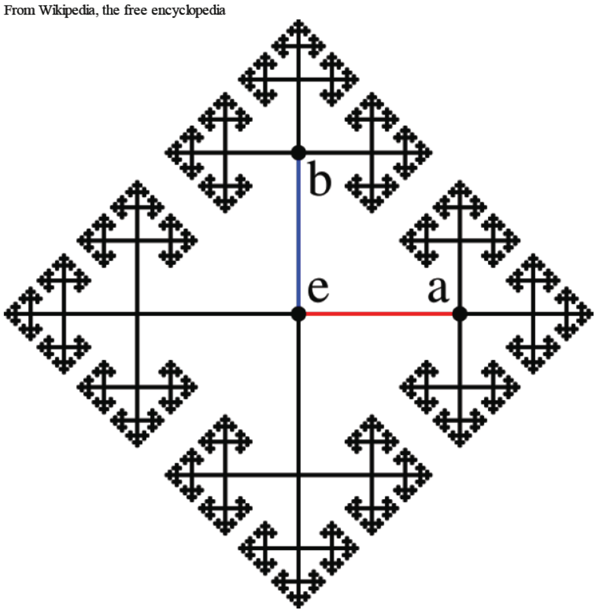

Figure 3: The Cayley graph for the free group on 2 generators a and b.

Then a *Coxeter group* is the group with generators and relations:

$$\langle s_1, \dots, s_n | \forall i, j : (s_i s_j)^{m_{ij}} = 1 \rangle \tag{6.5}$$

where, if $m_{ij} = \infty$ we interpret this to mean there is no relation.

Note that since $m_{ii} = 1$ we have

$$s_i^2 = 1 \tag{6.6}$$

That is, all the generators are *involutions*. It then follows that if $m_{ij} = 2$ then s_i and s_j commute. If $m_{ij} = 3$ then the relation can also be written:

$$s_i s_j s_i = s_j s_i s_j \tag{6.7}$$

A theorem of Coxeter's from the 1930's gives a classification of the finite Coxeter groups. [25] Coxeter found it useful to describe these groups by a diagrammatic notation: We draw a graph whose vertices correspond to the generators s_i. We draw an edge between vertices i and j if $m_{ij} \geq 3$. By convention the edges are labeled by m_{ij} and if $m_{ij} = 3$ then the standard convention is to omit the label.

It turns out that the *finite* Coxeter groups can be classified and their Coxeter diagrams are

The finite Coxeter groups turn out to be isomorphic to concrete groups of *reflections* in some Euclidean space. That is, finite subgroups of $O(N)$ for some N. That is, there is some vector space $\mathbb{R}^N$ and collection of vectors $v_i \in \mathbb{R}^N$ with inner products

$$v_i \cdot v_j = -2\cos(\frac{\pi}{m_{i,j}}) \tag{6.8}$$

[25] For a quick summary see the expository note by D. Allcock at https://web.ma.utexas.edu/users/allcock/expos/reflec-classification.pdf.

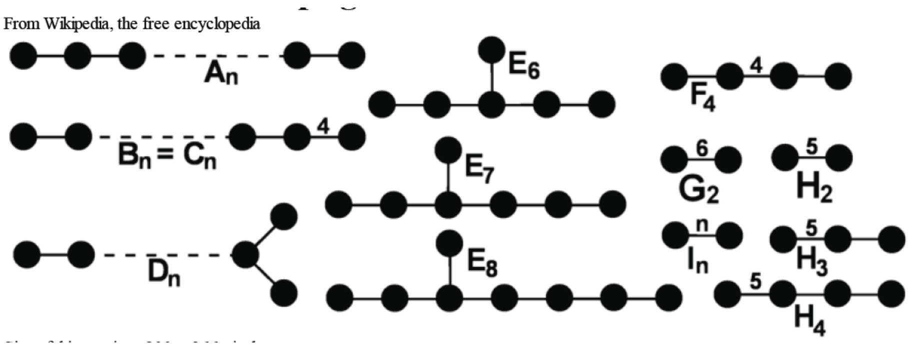

Figure 4: Coxeter's list of finite Coxeter groups. They are finite groups of reflections in some Euclidean space.

so that the group generated by reflections in the plane orthogonal to the vectors v_i:

$$P_{v_i} : v \mapsto v - \frac{2v \cdot v_i}{v_i \cdot v_i} v_i \tag{6.9}$$

is a finite group isomorphic to the Coxeter group with matrix $m_{i,j}$. (Note that since $m_{i,i} = 1$ we have $v_i^2 = 2$ and $P_{v_i}(v) = v - (v \cdot v_i)v_i$.)

Note that, if P_v is the Euclidean reflection in the plane orthogonal to v then $P_{v_1} \circ P_{v_2}$ is just rotation in the plane spanned by v_1, v_2 by an angle 2θ where the angle between v_1 and v_2 is θ. To prove this, note that $P_{v_1} \circ P_{v_2}$ clearly leaves all vectors in the plane orthogonal to v_1, v_2 fixed. Now represent vectors in a 2-dimensional Euclidean plane by complex numbers. WLOG take $v = e^{\mathrm{i}\theta}$. Then P_v is the transformation:

$$P_v : z \mapsto -e^{2\mathrm{i}\theta} \bar{z} \tag{6.10}$$

To check this formula note that if $z = e^{\mathrm{i}\theta}$ then $P_v(z) = -z$ and if $z = \mathrm{i}e^{\mathrm{i}\theta}$ is in the orthogonal hyperplane to v then $P_v(z) = z$.

Now if $v_a = e^{\mathrm{i}\theta_a}$, $a = 1, 2$, it is an easy matter to compute:

$$\begin{aligned} P_{v_1} \circ P_{v_2} : z &\mapsto -e^{2\mathrm{i}\theta_2} \bar{z} \\ &\mapsto -e^{2\mathrm{i}\theta_1} \overline{-e^{2\mathrm{i}\theta_2} \bar{z}} \\ &= e^{2\mathrm{i}(\theta_1 - \theta_2)} z \end{aligned} \tag{6.11}$$

So: The product of reflections in the hyper-planes orthogonal to two vectors at an angle θ is a rotation by an angle 2θ in the plane spanned by the two vectors.

We will meet some of these groups again later as Weyl groups of simple Lie groups. We have, in fact, already met two of these groups! The case A_n turns out to be isomorphic to the symmetric group S_{n+1}. [26] In this case we have seen that the elementary generators

[26] The notation here is standard but exceedingly unfortunate and confusing!!! Here A_n does <u>NOT</u> refer to the alternating group! It refers to Cartan's classification of simple Lie groups and the Coxeter group with this label is in fact isomorphic to S_{n+1}.

$\sigma_i = (i, i+1)$, $1 \le i \le n$ indeed satisfy the Coxeter relations:

$$\begin{aligned} \sigma_i^2 &= 1 \\ (\sigma_i \sigma_{i+1})^3 &= 1 \qquad 1 \le i \le n-1 \\ (\sigma_i \sigma_j)^2 &= 1 \qquad |i-j| > 1 \end{aligned} \tag{6.12}$$

Now consider the standard basis e_i for $\mathbb{R}^{n+1}$, $1 \le i \le n+1$ and consider the vectors:

$$\alpha_i = e_i - e_{i+1} \tag{6.13}$$

which have the inner products:

$$\alpha_i \cdot \alpha_j = C_{ij} = 2\delta_{i,j} - \delta_{i,j+1} - \delta_{i,j-1} \tag{6.14}$$

Then the map $s_i \to P_{\alpha_i}$ is an isomorphism of the Coxeter group A_n with a subgroup of $O(n+1)$. Moreover, one computes that

$$P_{\alpha_i}(e_j) = \begin{cases} e_j & j \ne i, i+1 \\ e_{i+1} & j = i \\ e_i & j = i+1 \end{cases} \tag{6.15}$$

So, referring to equation (5.35) we see that this is just the permutation action of σ_i on the standard basis of $\mathbb{R}^{n+1}$. This makes clear that the Coxeter group is isomorphic to the symmetric group S_{n+1}.

♣A presentation of the Monster in terms of generators and relations is known.(Atlas) Give it here? ♣

Remarks

1. One very practical use of having a group presented in terms of generators and relations is in the construction of homomorphisms. If one is constructing a homomorphism $\phi : G_1 \to G_2$, then it suffices to say what elements the generators map to. That is, if g_i are generators of G_1 we can fully specify a homomorphism by choosing elements $g_i' \in G_2$ (not necessarily generators) and declaring

$$\phi(g_i) = g_i' \quad . \tag{6.16}$$

   However, we cannot choose the g_i' arbitrarily. Rather, the g_i' must satisfy the same relations as the g_i. This puts useful constraints on what homomorphisms you can write down. For example, using this idea you can prove that there is no nontrivial homomorphism $\phi : \mathbb{Z}_N \to \mathbb{Z}$.

2. In general it is hard to say much about a group given a presentation in terms of generators and relations. For example, it is not even obvious, in general, if the group is the trivial group! This is part of the famous "word problem for groups." There are finitely presented groups where the problem of saying whether two words represent the same element is undecidable! [27] However, for many important finitely presented groups the word problem can be solved. Indeed, the word problem was first formulated by Max Dehn in 1911 and solved by him for the surface groups discussed below.

♣It would be more effective here to give an example of a set of generators and relations that is actually isomorphic to the trivial group - but not obviously so. ♣

[27] The Wikipedia article on "Word problem for groups," is useful.

3. Nevertheless, there are four Tietze transformations (adding/removing a relation, adding/removing a generator) which can transform one presentation of a group to a different presentation of an isomorphic group. It is a theorem [REF!] that any two presentations can be related by a finite sequence of Tietze transformations. How is this compatible with the previous remark? The point is that the number $f(n)$ of such transformations needed to transform a presentation of the trivial group with n relations into the trivial presentation grows faster than any recursive function of n.

4. It turns out that the case of Coxeter groups $B_n = C_n$ are isomorphic to the group of symmetric permutations $\mathcal{W}B_n \subset S_{2n}$ discussed in card-shuffling. The Coxeter diagrams are very similar to the *Dynkin diagrams* that are used to label finite dimensional simple Lie algebras over the complex numbers except that H_n and I_n do not correspond to Lie algebras.

Exercise *Homomorphisms involving $\mathbb{Z}_N$ and $\mathbb{Z}$*
a.) Write a nontrivial homomorphism $\mu : \mathbb{Z} \to \mathbb{Z}_N$.
b.) Show that there is no nontrivial homomorphism $\mu : \mathbb{Z}_N \to \mathbb{Z}$. [28]
c.) Find the most general homomorphism $\mu : \mathbb{Z} \to \mathbb{Z}$.
d.) Find the most general homomorphism $\mu : \mathbb{Z}_N \to \mathbb{Z}_N$.

Exercise *Simple Roots Of $SU(n+1)$*
a.) Verify equation (6.14). The matrix C_{ij} is known as a *Cartan matrix* of $SU(n+1)$.

b.) Show that the vectors α_i are all orthogonal to the all-one vector: $v = (1, \dots, 1)$ and that they span the orthogonal complement of v.

c.) Show that the permutation representation of S_{n+1} separately preserves v and the orthogonal complement of v. Thus, $\mathbb{R}^{n+1}$ gives what is known as a *reducible representation* of S_{n+1}.

d.) Compute the action of P_{α_i} on α_j.

Exercise Show that

$$\langle a, b | a^3 = 1, b^2 = 1, abab = 1 \rangle \tag{6.17}$$

[28] *Answer*: Since $\mathbb{Z}_N$ can be generated by one element, say $\bar{1}$, it suffices to say what the value of $\phi(\bar{1})$ is. The trivial homomorphism takes the generator to zero: $\phi(\bar{1}) = 0 \in \mathbb{Z}$ and hence takes every element to zero. On the other hand, if $\phi(\bar{1}) = k$ is a nonzero integer, then $Nk = N\phi(\bar{1}) = \phi(N\bar{1}) = \phi(\bar{0}) = 0$, a contradiction. So there is no nontrivial homomorphism.

is a presentation of S_3

Exercise

Consider the group with presentation:

$$\langle T, S | (ST)^3 = 1, S^2 = 1 \rangle \tag{6.18}$$

Is this group finite or infinite?

This group plays a very important role in string theory.

Exercise *Bounds on the minimal number of generators of a finite group*

Suppose we have a set of finite groups $G_1, G_2, G_3, \dots$ with a minimal set of generators $\mathcal{S}_1 \subset \mathcal{S}_2 \subset \cdots$ of cardinality $|\mathcal{S}_k| = k$. Show that $2|G_k| \leq |G_{k+1}|$ and hence as $k \to \infty$ the order $|G_k|$ must grow at least as fast as 2^k.

Remark: Denote the smallest cardinality of a set of generators of G by $d(G)$. If G is a finite and transitive permutation subgroup of S_n (meaning it acts transitively on some set X) then there is a constant C such that

$$d(G) \leq C \frac{n}{\sqrt{\log n}} \tag{6.19}$$

and if G is a primitive permutation group, meaning that it acts on a set X such that it does not preserve any nontrivial disjoint decomposition of X, then there is a constant C so that if $n \geq 3$:

$$d(G) \leq C \frac{\log n}{\sqrt{\log\log n}} \tag{6.20}$$

Moreover, these results are asymptotically the best possible. For a review of such results see. [29]

Exercise *Generators And Relations For Products Of Groups*

Suppose you are given groups G_1 and G_2 in terms of generators and relations. Write a set of generators and relations for the product group $G_1 \times G_2$. [30]

---

[29] F. Menegazzo, "The Number of Generators of a Finite Group," Irish Math. Soc. Bulletin 50 (2003), 117128.

[30] *Answer*: If $G_1 = \langle g_i | R_i \rangle$ and $G_2 = \langle h_a | S_a \rangle$ then $G_1 \times G_2 = \langle g_i, h_a | R_i, S_a, g_i h_a g_i^{-1} h_a^{-1} = 1 \rangle$.

6.1 Example Of Generators And Relations: Fundamental Groups In Topology

Presentations in terms of generators and relations is very common when discussing the *fundamental group* of a topological space X.

This subsection assumes some knowledge of topological spaces and the idea of a homotopy. Without trying to be too precise we choose a basepoint $x_0 \in X$ and let $\pi_1(X, x_0)$ be the set of closed paths in X, beginning and ending at x_0 where we identify two paths if they can be continuously deformed into each other. We can define a group multiplication by concatenation of paths. Inverses exist since we can run paths backwards. The following subsubsection contains more precise definitions.

♣Need to fix pictures and change p_0 to x_0. ♣

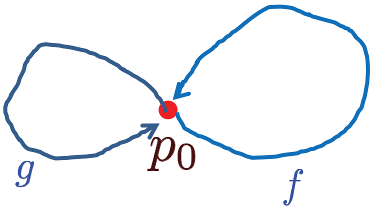

Figure 5: Two loops f, g with basepoint at x_0.

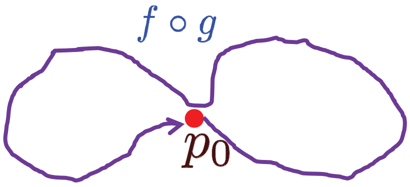

Figure 6: The concatenation of the looops $f \star g$. Note that the "later" loop is written on the right. This is generally a more convenient convention when working with homotopy and monodromy. In order for $f \star g$ to be a map from $[0, 1]$ into X we should run each of the individual loops at "twice the speed" so that at time $t = 1/2$ the loop returns to x_0. However, in homotoping $f \star g$ there is no reason why the point at $t = 1/2$ has to stay at x_0.

6.1.1 The Fundamental Group Of A Topological Space

Choose a point $x_0 \in X$. The fundamental group $\pi_1(X, x_0)$ based at x_0 is, as a set, the set

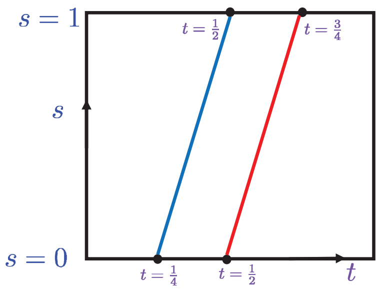

Figure 7: The homotopy demonstrating that loop concatenation is an associative multiplication on homotopy equivalence classes of closed loops. The blue line is $s = 4t - 1$ and the red line is $s = 4t - 2$.

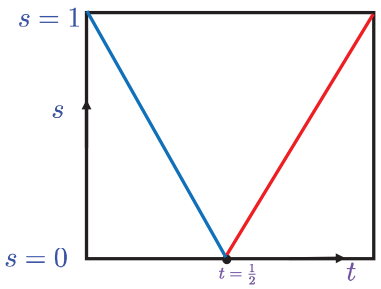

Figure 8: The homotopy demonstrating that the loop $g(t) = f(1-t)$ provides a representative for the inverse of $[f(t)]$.

of homotopy classes of closed curves.

That is we consider continuous maps:

$$f : ([0, 1], \{0, 1\}) \to (X, \{x_0\}) \tag{6.21}$$

These define paths in X with beginning and ending point fixed at x_0. The path must be traveled in time 1.

We say that two such paths f_0, f_1 are *homotopic* if there is a continuous map

$$F : [0, 1] \times [0, 1] \to X \tag{6.22}$$

such that

1. $F(0, t) = f_0(t)$ and $F(1, t) = f_1(t)$

2. $F(s, 0) = F(s, 1) = x_0$

If we define $f_s(t) := F(s,t)$ and consider $f_s(t)$ as a path in t at fixed s then, as we vary s we are describing a path of paths.

Now, homotopy of paths in X is an equivalence relation. [31] We denote by $[f]$ the equivalence class of a path f and we denote the set of such equivalence class by $\pi_1(X,x_0)$. We will see that this set has a natural and beautiful group structure.

We can define a group structure on $\pi_1(X,x_0)$ by concatenating curves as in Figure 6 and rescaling the time variable so that it runs from 0 to 1. In equations we have

$$f_1 \star f_2(t) := \begin{cases} f_1(2t) & 0 \le t \le \frac{1}{2} \\ f_2(2t-1) & \frac{1}{2} \le t \le 1 \end{cases} \tag{6.23}$$

The first and most basic example of a nontrivial fundamental group is the fundamental group of the circle. It should be intuitively clear that

$$\pi_1(S^1, x_0) \cong \mathbb{Z} \tag{6.24}$$

which just measures the number of times the path winds around the circle. The sign of the integer takes into account winding clockwise vs. counterclockwise.

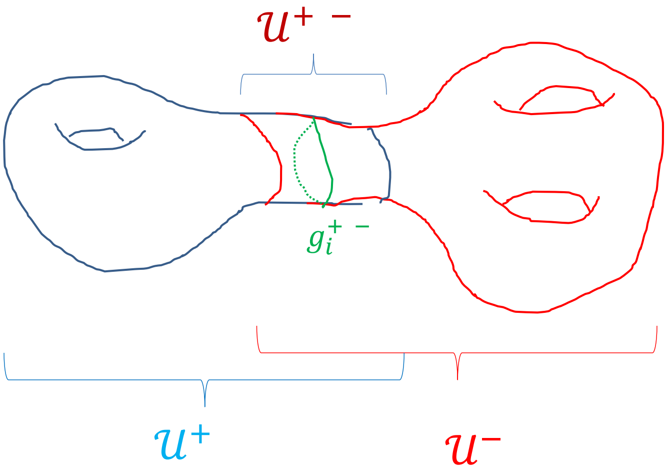

Figure 9: Illustrating the Seifert-VanKampen theorem. The green curve has a homotopy class in $\mathcal{U}^{+-}$ that is one of the generators of $\pi_1(\mathcal{U}^{+-})$. Now it must separately be a word W_i^+ in the generators of $\pi_1(\mathcal{U}^+)$ and W_i^- in the generators of $\pi_1(\mathcal{U}^-)$ so in $\pi_1(X)$ there must be a relation of the form $W_i^+ = W_i^-$.

Remarks

1. Note that we are composing successive paths *on the right*. This is slightly nonstandard but a nice convention when working with monodromy and path ordered expontentials of gauge fields - one of the main physical applications.

[31] See section 4.1 above for this notion.

2. Note well that $(f_1 \star f_2) \star f_3$ is *NOT* the same path as $f_1 \star (f_2 \star f_3)$. This observation ultimately leads to the notion of A_∞ spaces.

3. For the moment we simply notice that if we mod out by homotopy then we have a well-defined product on homotopy classes in $\pi_1(X, x_0)$

$$[f_1] \cdot [f_2] := [f_1 \star f_2] \tag{6.25}$$

and the virtue of passing to homotopy classes is that now the product (6.25) is in fact associative. The proof is in Figure 7. Written out in excruciating detail the homotopy is

$$F(s,t) = \begin{cases} f_1(\frac{4}{s+1}t) & 0 \le t \le \frac{s+1}{4} \\ f_2(4t-(s+1)) & \frac{s+1}{4} \le t \le \frac{s+2}{4} \\ f_3(\frac{4}{2-s}(t-\frac{s+2}{4})) & \frac{s+2}{4} \le t \le 1 \end{cases} \tag{6.26}$$

4. Since we have an associative product on $\pi_1(X, x_0)$ we are now ready to define a group structure. The identity element is clearly given by the (homotopy class of the) constant loop: $f(t) = x_0$. If a homotopy class is represented by a loop $f(t)$ then the inverse is represented by running the loop backwards: $g(t) := f(1-t)$. The two are joined at $t = 1/2$, and since this is in the open interval $(0,1)$ the image can be deformed away from x_0. See Figure 8. In equations, there is a homotopy of $f \star g$ with the constant loop given by

$$F(s,t) = \begin{cases} f(2t) & t \le \frac{1-s}{2} \\ f(1-s) & \frac{1-s}{2} \le t \le \frac{1+s}{2} \\ f(2-2t) & \frac{1+s}{2} \le t \le 1 \end{cases} \tag{6.27}$$

Thus, with the group operation defined by concatenation in the sense of (6.25) the set of homotopy classes $\pi_1(X, x_0)$ is a group. It is known as the fundamental group based at x_0.

5. A connected space such that $\pi_1(X, x_0)$ is the trivial group is called *simply connected.*

6. If $F : X \to Z$ is a continuous map of topological spaces and takes $x_0 \in X$ to $z_0 \in Z$ then we can define $F_* : \pi_1(X, x_0) \to \pi_1(Z, z_0)$ simply by $F_*[f] := [F \circ f]$. This can be shown to be a group homomorphism. In particular, if F is a homotopy equivalence, then it is a group isomorphism.

7. In algebraic topology books a major result which is proved is the *Seifert-van Kampen theorem.* This is an excellent illustration of defining groups by generators and relations. The theorem can be useful because it allows one to compute $\pi_1(X, x_0)$ by breaking up X into simpler pieces. Specifically, suppose that $X = U^+ \cup U^-$ is a

union of two open path-connected subsets and that $U^{+-} := U^{+} \cap U^{-}$ is also path-connected and contains x_0. See Figure 9. Now suppose we know presentations of the fundamental groups of the pieces U^{+}, U^{-}, U^{+-} in terms of generators and relations:

$$\begin{aligned} \pi_1(U^{+}, x_0) &\cong \langle g_1^{+}, \dots, g_{n^{+}}^{+} | R_1^{+}, \dots, R_{m^{+}}^{+} \rangle \\ \pi_1(U^{-}, x_0) &\cong \langle g_1^{-}, \dots, g_{n^{-}}^{-} | R_1^{-}, \dots, R_{m^{-}}^{-} \rangle \\ \pi_1(U^{+-}, x_0) &\cong \langle g_1^{+-}, \dots, g_{n^{+-}}^{+-} | R_1^{+-}, \dots, R_{m^{+-}}^{+-} \rangle \end{aligned} \tag{6.28}$$

Then the recipe for computing $\pi_1(X, x_0)$ is this: Denote the injection $\iota^{+} : U^{+-} \to U^{+}$ and $\iota^{-} : U^{+-} \to U^{-}$. Then the generators of $\pi_1(U^{+-}, x_0)$ push forward to words in g_i^{+} or g_i^{-}, respectively:

$$\begin{aligned} \iota_*^{+}(g_i^{+-}) &:= W_i^{+} \qquad i = 1, \dots, n^{+-} \\ \iota_*^{-}(g_i^{+-}) &:= W_i^{-} \qquad i = 1, \dots, n^{+-} \end{aligned} \tag{6.29}$$

Finally, we have the presentation:

$$\pi_1(X, x_0) \cong \langle g_1^{+}, \dots, g_{n^{+}}^{+}, g_1^{-}, \dots, g_{n^{-}}^{-} | R_\alpha \rangle \tag{6.30}$$

where the relations R_α include the *old relations*

$$R_1^{+}, \dots, R_{m^{+}}^{+}, R_1^{-}, \dots, R_{m^{-}}^{-} \tag{6.31}$$

and a set of *new relations*:

$$W_1^{+}(W_1^{-})^{-1}, \dots, W_{n^{+-}}^{+}(W_{n^{+-}}^{-})^{-1} \tag{6.32}$$

It is obvious that these are relations on the generators. What is not obvious is that these are the only ones. Note that in the final presentation the generators g_i^{+-} and the relations R_i^{+-} have dropped out of the description.

Exercise

Show that if $X = S^n$ with $n > 1$ then $\pi_1(X, x_0)$ is the trivial group.

Exercise

Does the fundamental group depend on a choice of basepoint x_0 ?

Exercise

Using the Seifert-van Kampen theorem show that if $X = S^1$ then $\pi_1(X, x_0) \cong \mathbb{Z}$.

Exercise
What is the fundamental group of Serin Physics Laboratory?

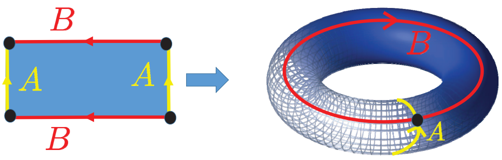

Figure 10: Right: Cutting a torus along the A and B cycles the surface falls apart into a rectangle, shown on the left. Conversely, gluing the sides of the rectangle together produces a torus with distinguished closed curves A, B.

6.1.2 Surface Groups And Braid Groups

The fundamental groups of two-dimensional surfaces, known as *surface groups* and braid groups turn out to provide a very rich set of examples of groups defined by generators and relations.

The simplest example of a nontrivial surface group is the torus. Let a, b denote the homotopy classes of the cycles A, B shown in Figure 10. One can convince oneself that these generate the fundamental group: Every closed curve based at x_0 can be homotoped to a word in $a^{\pm 1}$ and $b^{\pm 1}$. Now, if we cut the torus along the cycles the surface falls apart into a rectangle as shown in Figure 10. The edge of the rectangle represents the class $aba^{-1}b^{-1}$.

Definition: In general, in group theory an expression of the form $g_1 g_2 g_1^{-1} g_2^{-1}$ is known as a *group commutator* and is sometimes denoted $[g_1, g_2]$. It should not be confused with the commutator of matrices $[A_1, A_2] = A_1 A_2 - A_2 A_1$.

Returning to the fundamental group of the torus, the group commutator $[a, b]$ it can be contracted inside the rectangle to a point. Therefore, the generators a, b satisfy the relation:

$$aba^{-1}b^{-1} = 1 \tag{6.33}$$

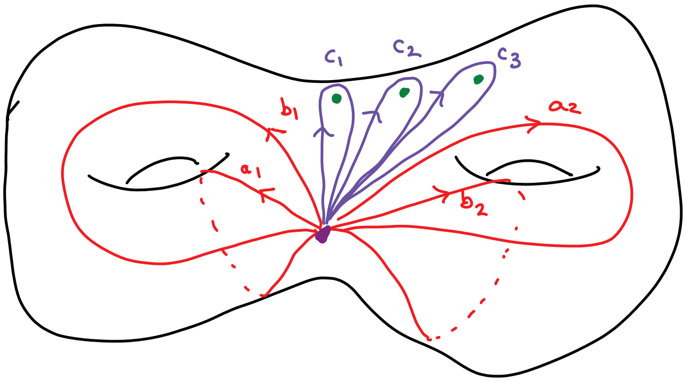

Figure 11: A collection of closed paths at x_0 which generate the fundamental group of a two-dimensional surface with two handles and three (green) holes.

so this means

$$ab = ba \tag{6.34}$$

In fact, this is the only relation and therefore:

$$\pi_1(T^2, x_0) \cong \mathbb{Z} \oplus \mathbb{Z}. \tag{6.35}$$

Now let us consider a more complicated surface, perhaps with punctures as shown in Figure 11. By cutting along the paths shown there the surface unfolds to a presentation by gluing as in Figure 12:

From these kinds of constructions one can prove [32] that the fundamental group of an orientable surface with g handles and p punctures will be

$$\pi_1(S, x_0) = \langle a_i, b_i, c_s | \prod_{i=1}^{g} [a_i, b_i] \prod_{s=1}^{p} c_s = 1 \rangle \tag{6.36}$$

There is only one relation so this is very close to a free group! In fact, for $p \geq 1$ we can solve for one generator c_s in terms of the rest so the group is just a free group on $2g+p-1$ generators. When there are no punctures the group is not a free group. Groups of the form (6.36) are sometimes called *surface groups*.

[32] See, for example, W. Massey, *Introduction to Algebraic Topology*, Springer GTM

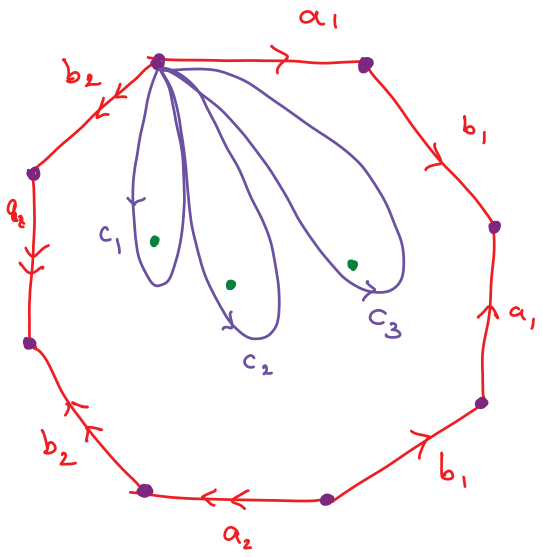

Figure 12: When the directed edges are identified according to their labels the above surface reproduces the genus two surface with three punctures. Since the disk is simply connected we derive one relation on the curves shown here.

Exercise *Fundamental group of the Klein bottle*

A very interesting unorientable surface is the Klein bottle. Its fundamental group has two natural presentations in terms of generators and relations. One is

$$\langle a, b | a^2 = b^2 \rangle \tag{6.37}$$

and the other is

$$\langle g_1, g_2 | g_1 g_2 g_1 g_2^{-1} = 1 \rangle \tag{6.38}$$

Show that these two presentations are equivalent.

Exercise

Use the Seifert-van Kampen theorem to relate the fundamental group of a torus to that of a torus with a disk cut out.

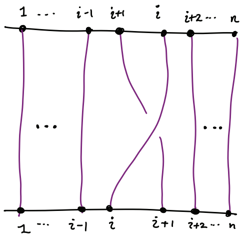

Figure 13: Pictorial illustration of the generator σ_i of the braid group B_n.

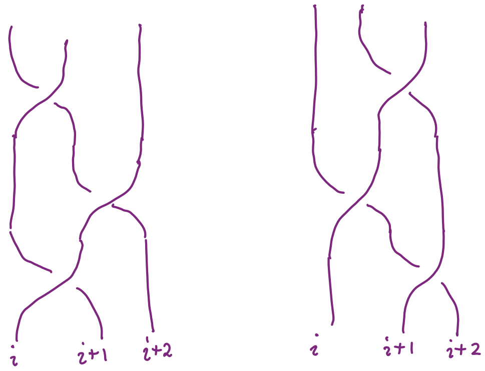

Figure 14: Pictorial illustration of the Yang-Baxter relation.

Example : *Braid groups.* Let us modify Figure 2 and Figure 1 to include an under-crossing and overcrossing of the strands. So now we are including more information - the topological configuration of the strands in three dimensions. In an intuitive sense, which we will not make precise here we obtain a group called the n^{th} *braid group.* It is generated by the overcrossing $\tilde{\sigma}_i$ of strings $(i, i+1)$, for $1 \leq i \leq n-1$ and may be pictured as in Figure 13. Note that $\tilde{\sigma}_i^{-1}$ is the undercrossing.

Now one verifies the relations

$$\tilde{\sigma}_i\tilde{\sigma}_j = \tilde{\sigma}_j\tilde{\sigma}_i \qquad\qquad |i-j| \geq 2 \tag{6.39}$$

and

$$\tilde{\sigma}_i\tilde{\sigma}_{i+1}\tilde{\sigma}_i = \tilde{\sigma}_{i+1}\tilde{\sigma}_i\tilde{\sigma}_{i+1} \tag{6.40}$$

where the relation (6.40) is illustrated in Figure 14.

The braid group $\mathcal{B}_n$ may be defined as the group generated by $\tilde{\sigma}_i$ subject to the relations (6.39)(6.40):

$$\mathcal{B}_n := \langle \tilde{\sigma}_1, \dots, \tilde{\sigma}_{n-1} | \tilde{\sigma}_i\tilde{\sigma}_j\tilde{\sigma}_i^{-1}\tilde{\sigma}_j^{-1} = 1, |i-j| \geq 2; \tilde{\sigma}_i\tilde{\sigma}_{i+1}\tilde{\sigma}_i = \tilde{\sigma}_{i+1}\tilde{\sigma}_i\tilde{\sigma}_{i+1} \rangle \tag{6.41}$$

The braid group $\mathcal{B}_n$ may also be defined as the fundamental group of the space of configurations of n unordered points on the disk D. We first consider the set:

$$\{(x_1, \dots, x_n) | x_i \in D \qquad x_i \neq x_j \quad i \neq j\} \tag{6.42}$$

Then we observe that there is a group action of S_n on this set. Note that this set is not simply connected: For example if we let x_1 loop around x_2 holding all other x_i fixed it should be intuitively clear that the loop cannot be deformed to the trivial loop. That is even more clear if you view the looping process as taking place in time on particles in a plane.

Now (see the discussion on orbits below) we consider the space of orbits under this group action:

$$\mathcal{C}_n := \{(x_1, \dots, x_n) | x_i \in D \qquad x_i \neq x_j \quad i \neq j\}/S_n \tag{6.43}$$

There are new nontrivial loops here where, for example, x_i and x_j exchange places, all other x_k staying fixed.

♣Since we must quotient by S_n this needs to be moved to the section on group actions on spaces. ♣

Note that the "only" difference from the presentation of the symmetric group is that we do *not* put any relation like $(\tilde{\sigma}_i)^2 = 1$. Indeed, $\mathcal{B}_n$ is of infinite order because $\tilde{\sigma}_i^n$ keeps getting more and more twisted as $n \to \infty$.

Exercise *Homomorphisms Between Braid And Symmetric Groups*

a.) Define a homomorphism $\mu : \mathcal{B}_n \to S_n$.

b.) Can you define a homomorphism $s : S_n \to \mathcal{B}_n$ so that $\mu \circ s$ is the identity transformation?

Remarks

1. In the theory of integrable systems the relation (6.40) is known as the "Yang-Baxter relation." It plays a fundamental role in integrable models of 2D statistical mechanics and field theory.

2. One interesting application of permutation groups to physics is in the quantum theory of identical particles. It was a major step in the development of quantum theory when Einstein and Bose realized that a system of n identical kinds of particles (photons, for example, or atomic Nuclei of the same isotope) are in fact *indistinguishable.* [33] In mathematical terms, there is a group action of S_n on a set of n indistinguishable particles leaving the physical system "the same." In quantum mechanics this translates into the statement that the Hilbert space of a system of n indistinguishable particles should be a representation of (a central extension of) S_n. There are many different representations of S_n (we have already encountered three different ones) but, remarkably, in relativistically invariant theories in spacetimes of dimension larger than 2 particles are either bosons or fermions. This is related to the classification of the *projective representations* of $SO(d,1)$, where d is the number of spatial dimensions, for relativistic systems and to representations of $SO(d)$ for nonrelativistic systems. (We will discuss projective representations in section **** below.) Now, when discussing projective representations the fundamental group of $SO(d,1)$ and $SO(d)$ becomes important. In fact $\pi_1(SO(d,1) \cong \pi_1(SO(d)$ for $d \geq 2$. However, there is a fundamental difference between $d \leq 2$ and $d > 2$. The essential point is that the fundamental group $\pi_1(SO(2)) \cong \mathbb{Z}$ is infinite while $\pi_1(SO(d)) \cong \mathbb{Z}_2$ for $d \geq 3$. A consequence of this, and other principles of physics is that in $2+1$ and $1+1$ dimensions particles with "anyonic" statistics can exist. [34] Anyons are defined by the property that, if we just consider the wavefunction of two identical such particles, $\Psi(z_1, z_2)$ where z_1, z_2 are points in the plane and then we adiabatically switch their positions using the kind of braiding that defines $\tilde{\sigma}$ then

$$\tilde{\sigma} \cdot \Psi(z_2, z_1) = e^{\mathrm{i}\theta} \Psi(z_1, z_2) \tag{6.44}$$

Unlike bosons and fermions where $\theta = 0, \pi \mathrm{mod} 2\pi$, respectively, for "anyons" the phase can be anything - hence the name. There are even physical realizations of this theoretical prediction in the fractional quantum Hall effect. Moreover, quantum wavefunctions should transform in representations of the braid group. The law (6.44) leads to the 1-dimensional representation $\tilde{\sigma} \to e^{\mathrm{i}\theta}$ but there can also be more interesting "nonabelian representations." That is, there can be interesting irreducible representations of dimension greater than one, and if wavefunctions transform in such representations there can be *nonabelian statistics.* There are some theoretical models of fractional quantum Hall states in which this takes place.

Here are some sources for more material about anyons:

♣NEED TO UPDATE THIS REFERENCE LIST!!! ♣

1. There are some nice lecture notes by John Preskill, which discuss the potential relation to quantum computation and quantum information theory: http://www.theory.caltech.edu/~preski

[33] See Chapters 24 and 25 in the book *Einstein and the Quantum* by A.D. Stone for a nice historical

2. For a reasonably up-to-date review see A. Stern, "Anyons and the quantum Hall effectA pedagogical review". Annals of Physics 323: 204; arXiv:0711.4697v1.
3. A. Lerda, *Anyons: Quantum mechanics of particles with fractional statistics* Lect.Notes Phys. M14 (1992) 1-138
4. A. Khare, *Fractional Statistics and Quantum Theory,*
5. G. Dunne, *Self-Dual Chern-Simons Theories.*
6. David Tong, "Lectures on the Quantum Hall Effect," e-Print: arXiv:1606.06687

7. Cosets and conjugacy

7.1 Lagrange Theorem

The reader should refresh her/his memory about equivalence relations - see section 4.1.

Definition 7.1.1: Let $H \subseteq G$ be a subgroup. The set

$$gH \equiv \{gh|h \in H\} \subset G \tag{7.1}$$

is called a *left-coset* of H.

Example 1: $G = \mathbb{Z}, H = 2\mathbb{Z}$. There are two cosets: H and $H + 1$. This is closely related to the example above.

Example 2: $G = S_3$, $H = \{1, (12)\} \cong S_2$. Cosets:

$$\begin{aligned}
1 \cdot H &= \{1, (12)\} \\
(12) \cdot H &= \{(12), 1\} = \{1, (12)\} \\
(13) \cdot H &= \{(13), (123)\} \\
(23) \cdot H &= \{(23), (132)\} \\
(123) \cdot H &= \{(123), (13)\} = \{(13), (123)\} \\
(132) \cdot H &= \{(132), (23)\} = \{(23), (132)\}
\end{aligned} \tag{7.2}$$

Claim: Two left cosets are either *identical* or *disjoint.* Moreover, every element $g \in G$ lies in some coset. That is, the cosets define an equivalence relation by saying $g_1 \sim g_2$ if there is an $h \in H$ such that $g_1 = g_2 h$. Here's a proof written out in excruciating detail. [35]

account of the importance of this discovery in the development of quantum mechanics.

[34] The possible existence of anyons was pointed out by Leinaas and Myrheim in 1977. The term "anyon" was invented in F. Wilczek, "Quantum Mechanics of Fractional-Spin Particles". Physical Review Letters 49 (14): 957959.

[35] In general, the reader should provide these kinds steps for herself or himself and we will not spell out proofs in such detail.

First, g is in gH, so every element is in *some* coset. Second, suppose $g \in g_1 H \cap g_2 H$. Then $g = g_1 h_1$ and $g = g_2 h_2$ for some $h_1, h_2 \in H$. This implies $g_1 = g_2(h_2 h_1^{-1})$ so $g_1 = g_2 h$ for an element $h \in H$. (Indeed $h = h_2 h_1^{-1}$, but the detailed form is not important.) By the rearrangement lemma $hH = H$, and hence $g_1 H = g_2 H$.

The basic principle above leads to a fundamental theorem:

Theorem 7.1.1 (Lagrange) If H is a subgroup of a finite group G then the order of H divides the order of G:

$$|G|/|H| \in \mathbb{Z}_+ \tag{7.3}$$

Proof : If G is finite $G = \amalg_1^m g_i H$ for some set of g_i, leading to *distinct* cosets. Now note that the order of any coset is the order of H:

$$|g_i H| = |H| \tag{7.4}$$

So $|G|/|H| = m$, where m is the number of distinct cosets. ♠

This theorem is simple, but powerful: For example we have the following

Corollary: Any finite group of prime order p is isomorphic to $Res(p) \cong \mathbb{Z}_p$. Moreover, such groups have exactly two subgroups: The trivial group and itself.

Proof: Choose a nonidentity element $g \in G$ and consider the subgroup generated by g i.e,

$$\{1, g, g^2, g^3, \dots\} \tag{7.5}$$

The order of this group must divide $|G|$ so if $|G| = p$ is prime it must be the entire group. ♠

Definition 7.1.2: If G is any group and H any subgroup then the *set of left cosets of H in G* is denoted G/H. It is the set of orbits under the left H action on G. A set of the form G/H is also referred to as a *homogeneous space*. The order of this set is the *index of H in G*, and denoted $[G : H]$.

Example 1: If $G = S_3, H = \{1, (12)\} \cong S_2$, then $G/H = \{H, (13) \cdot H, (23) \cdot H\}$, and $[G : H] = 3$.

Example 2: Let $G = \{1, \omega, \omega^2, \dots, \omega^{2N-1}\} \cong \mathbb{Z}_{2N}$ where ω is a primitive $(2N)^{th}$ root of 1. Let $H = \{1, \omega^2, \omega^4, \dots, \omega^{2N-2}\} \cong \mathbb{Z}_N$. Then $[G : H] = 2$ and $G/H = \{H, \omega H\}$.

Example 3: Let $G = A_4$ and $H = \{1, (12)(34)\} \cong \mathbb{Z}_2$. Then $[G : H] = 6$ and

$$G/H = \{H, (13)(24) \cdot H, (123) \cdot H, (132) \cdot H, (124) \cdot H, (142) \cdot H\} \tag{7.6}$$

Remark Note well! If $H \subset G$ is a subgroup and $g_1 H = g_2 H$ it does <u>not</u> follow that $g_1 = g_2$. All you can conclude is that there is some $h \in H$ with $g_1 = g_2 h$.

Exercise *Is there a converse to Lagrange's theorem?*

Suppose $n||G|$, does there then exist a subgroup of G of order n? Not necessarily! Find a counterexample. That is, find a group G and an n such that n divides $|G|$, but G has no subgroup of order n. [36]

Nevertheless, there is a very powerful theorem in group theory known as

Theorem 7.1.2: (Sylow's (first) theorem). Suppose p is prime and p^k divides $|G|$ for a nonnegative integer k. Then there is a subgroup $H \subset G$ of order p^k.

Herstein's book, sec. 2.12, waxes poetic on the Sylow theorems and gives three proofs. We'll give a proof as an application of the class equation in section 9 below. Actually, Sylow has a bit more to say. We will explain some more about this in the next section.

Definition: Thus far we have repeatedly spoken of the "order of a group G" and of various subsets of G, meaning simply the cardinality of the various sets. In addition a common terminology is to say that an element $g \in G$ *has order* n if n is the smallest natural number such that $g^n = 1$.

Note carefully that if g has order n and k is a natural number then $(g^n)^k = g^{nk} = 1$ and hence if $g^m = 1$ for some natural number m it does not necessarily follow that g has order m. However, as an application of Lagrange's theorem we can say the following: *If G is a finite group then the order of g must divide $|G|$, and in particular $g^{|G|} = 1$.* The proof is simple: Consider the subgroup generated by g, i.e. $\{1, g, g^2, \dots\}$. The order of this subgroup is the same as the order of g.

Exercise *Subgroups of A_4*

Write down all the subgroups of A_4. Draw a diagram indicating how these are subgroups of each other.

Exercise *Orders of group elements in infinite groups*

[36] *Answer:* One possible example is A_4, which has order 12, but no subgroup of order 6. By examining the table of groups below we can see that this is the example with the smallest value of $|G|$. Sylow's theorem (discussed below) states that if a prime power p^k divides $|G|$ then there is in fact a subgroup of order p^k. This fails for composite numbers - products of more than one prime. Indeed, the smallest composite number is $6 = 2 \cdot 3$. Thus, in regard to a hypothetical converse to Lagrange's theorem, as soon as things can go wrong, they do go wrong.

a.) Give an example of an infinite group in which all elements, other than the identity, have infinite order. (This should be quite easy for you.) [37]

b.) Give an example of an infinite group where some group elements have finite order and some have infinite order. [38]

c.) Give an example of an infinite group where all elements have finite order. [39]

Exercise

Suppose a finite group G has subgroups H_i, $i = 1, \dots, s$ of order h_i where the h_i are all mutually relatively prime integers. Show that $\prod_i h_i$ divides $|G|$.

7.2 Conjugacy

Now introduce a notion generalizing the idea of similarity of matrices:

Definition 7.2.1 :

a.) A group element h is *conjugate* to h' if $\exists g \in G \qquad h' = ghg^{-1}$.

b.) Conjugacy defines an equivalence relation and the *conjugacy class of h* is the equivalence class under this relation:

$$C(h) := \{ghg^{-1} : g \in G\} \tag{7.7}$$

c.) Let $H \subseteq G, K \subseteq G$ be two subgroups. We say "H is conjugate to K" if $\exists g \in G$ such that

$$K = gHg^{-1} := \{ghg^{-1} : h \in H\} \tag{7.8}$$

Example 7.2.1 : Let $G = GL(n, \kappa)$ be a matrix group. Then conjugacy is the same notion as similarity of matrices. The conjugacy class of a diagonalizable matrix A is the set of diagonalizable matrices with the same unordered set of eigenvalues as A. However, we stress that not all matrices are diagonalizable, so that the full description of conjugacy classes is more complicated. See the discussion of Jordan canonical form in Chapter two below. If we consider the conjugacy classes in $U(N)$ the story simplifies, thanks to the spectral theorem (See Chapter 2). The spectral theorem says that if $u \in U(N)$ there is a $g \in U(N)$ with $gug^{-1} = Diag\{z_1, \dots, z_N\}$ where $|z_i| = 1$. This does not mean that the set

[37] *One possible answer*: Take $\mathbb{Z}$ or $\mathbb{Z}^n$ or ....

[38] *One possible answer*: $\mathbb{Z} \times \mathbb{Z}_N$. Another possible answer is $G = U(1)$.

[39] *One possible answer*: Regard $U(1)$ as the group of complex numbers of modulus one. Let G be the subgroup of complex numbers so that $z^N = 1$ for some integer N. This is the group of all roots of unity of any order. It is clearly an infinite group, and by its very definition every element has finite order. Using the notation of the next section, this group is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

of conjugacy classes can be identified with $U(1)^N$. Consider, for example, the permutation matrix $A(\phi)$ for $\phi \in S_N$. This is unitary and

$$A(\phi)Diag\{z_1,\dots,z_N\}A(\phi)^{-1} = Diag\{z_{\phi(1)},\dots,z_{\phi(N)}\} \tag{7.9}$$

Once we have taken this into account we are done: *The set of conjugacy classes in $U(N)$ is the set of unordered N-tuples of phases.*

Groups which are self-conjugate are very special:

Definition 7.2.2: A subgroup $N \subseteq G$ is called a *normal* subgroup, or an *invariant* subgroup if

$$gNg^{-1} = N \qquad \forall g \in G \tag{7.10}$$

Sometimes this is denoted as $N \triangleleft G$.

In this case we have a nice theorem. In general the set of cosets of H in G, denoted G/H does not have any natural group structure. [40] However, if H is normal something special happens:

Theorem 7.2.1. If $N \subset G$ is a normal subgroup then the set of left cosets $G/N = \{gN|g \in G\}$ has a natural group structure with group multiplication defined by:

$$(g_1N)\cdot(g_2N) := (g_1 \cdot g_2)N \tag{7.11}$$

Proof- left as an exercise - see below.

Remark: All subgroups N of Abelian groups A are normal, and moreover the quotient group A/N is Abelian.

Example 7.2.1 Cyclic Groups For example $n\mathbb{Z} \subset \mathbb{Z}$ is normal, and the quotient group is $\mathbb{Z}/n\mathbb{Z}$. This is isomorphic to the cyclic group we have previously denoted as $Res(n)$ or $\mathbb{Z}_n$. So $\bar{r}$ is the equivalence class of an integer $r \in \mathbb{Z}$:

$$\bar{r} = r + n\mathbb{Z} \tag{7.12}$$

$$\bar{r} + \bar{s} = (r+s) + n\mathbb{Z} \tag{7.13}$$

Example 7.2.2 Elliptic Curves . Consider the Abelian group $\mathbb{C}$ of complex numbers with normal addition as the group operation. If τ is a complex number with nonzero

[40] Note that it might have many unnatural group structures. For example, if G/H is a finite set with n elements that we could choosely - arbitrarily!! - some one-one correspondence between the elements of G/H and the elements in any finite group with n elements and use this to define a group multiplication law on the set G/H. We hope the reader can appreciate how incredibly tasteless such a procedure would be. Technically, it is *unnatural* because it makes use of an arbitrary extra choice of one-one correspondence between the elements of G/H and the elements of some group.

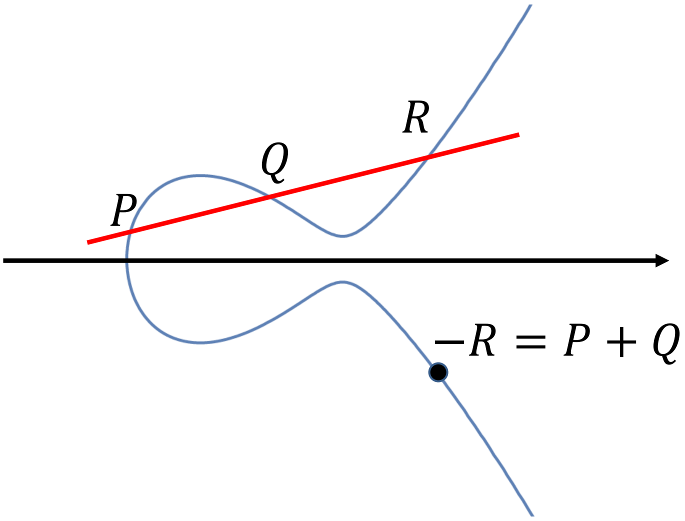

Figure 15: In a suitable range of real values of f, g the real points on the elliptic curve have the above form. Then the elliptic curve group law is easily pictured as shown.

imaginary part then $\mathbb{Z} + \tau\mathbb{Z}$ is the subgroup of complex numbers of the form $n_1 + \tau n_2$ where n_1 and n_2 are integers. Since $\mathbb{C}$ is abelian we can form the Abelian group $\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$. Note that $\mathbb{Z} + \tau\mathbb{Z}$ is a rank two lattice in the plane so that this quotient space can be thought of as a torus. As an Abelian group this group is isomorphic to $U(1) \times U(1)$. The explicit isomorphism is

$$(\sigma_1 + \tau\sigma_2) + (\mathbb{Z} + \tau\mathbb{Z}) \mapsto (e^{2\pi i\sigma_1}, e^{2\pi i\sigma_2}) \tag{7.14}$$

A remarkable fact is that this torus (minus one point) can be thought of as the space of solutions of the algebraic equation

$$y^2 = x^3 + fx + g \tag{7.15}$$

where $(x, y) \in \mathbb{C}^2$ and $f, g \in \mathbb{C}$. [41] The mapping between $[z] \in \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ and (x, y) and between f, g and the complex number τ involves very interesting functions known as elliptic functions. The solution set is known as an "elliptic curve." The Abelian group law expressed in terms of (x, y) is rather nontrivial and closely related to some deep topics in number theory. If one considers f, g to be real and studies the real solutions then the group law can be visualized as in Figure 15. (We are following the Wikipedia article here, which is quite clear.) One first defines the inverse $-P$ of a point P on the curve with coordinates $P = (x, y)$ to be $-P := (x, -y)$. Then, for generic points we can define $P + Q$ by saying that $P + Q = -R$ where R is on the intersection of the straight line through P, Q and the

[41] We can restore the point at infinity using projective geometry. The equation $zy^2 = x^3 + fxz^2 + gz^3$ makes sense for a point $[x : y : z] \in \mathbb{CP}^2$. The equation (7.15) is the equation we get in the patch $z \neq 0$ where we fix the scaling by setting $z = 1$. The point at infinity has $z = 0$. Therefore, by the equation $x = 0$, and since we have a point in $\mathbb{CP}^2$ we must have $y \neq 0$, which can therefore be scaled to $y = 1$. So, the point at infinity is $[0 : 1 : 0] \in \mathbb{CP}^2$.

elliptic curve. In formulae we can write the line between P, Q as

$$y = sx + d \tag{7.16}$$

with

$$s = \frac{y_P - y_Q}{x_P - x_Q} \qquad d = y_P - x_P \left(\frac{y_P - y_Q}{x_P - x_Q} \right) = y_Q - x_Q \left(\frac{y_P - y_Q}{x_P - x_Q} \right) \tag{7.17}$$

Now the intersection of this line with the cubic equation has x coordinates given by

$$(sx + d)^2 = x^3 + fx + g \tag{7.18}$$

and by simple rearrangement we can rewrite (7.18) as

$$x^3 - s^2 x^2 + (f - 2sd)x + (g - d^2) = 0 \tag{7.19}$$

On the other hand, this equation must be of the form

$$(x - x_P)(x - x_Q)(x - x_R) = 0 \tag{7.20}$$

Expanding out (7.19) and equating the coefficient of x^2 we obtain

$$x_R = s^2 - x_P - x_Q \tag{7.21}$$

so we have x_R explicitly as a function of x_P, x_Q, y_P, y_Q. Now the point (x_R, y_R) must lie on the line $y = sx + d$ so we can also say that

$$y_R = y_P + s(x_R - x_P) \tag{7.22}$$

expressing y_R and hence the coordinates of $R = (x_R, -y_R)$ as rational functions of x_P, x_Q, y_P, y_Q. It is not at all obvious that the above group law really satisfies the associativity constraint. When points coincide or the line is tangent to the elliptic curve one must carefully degenerate the above expressions. Indeed, requiring that $P + (-P) = 0$ shows that 0 must correspond to the point at infinity. When f, g are not in the range to give a figure like Figure 15 the algebraic equations above still define a group law. Indeed, these equations make sense over any field, thus allowing one to define an Abelian group law for elliptic curves defined over any field.

Example 7.2.3.

$$A_3 \equiv \{1, (123), (132)\} \subset S_3 \tag{7.23}$$

is normal. What group is S_3/A_3?

Example 7.2.4. Of course, in any group G the subgroup $\{1\}$ and G itself are normal subgroups. These are the trivial normal subgroups. It can happen that these are the only normal subgroups of G:

Definition . A group with no nontrivial normal subgroups is called a *simple group*.

The term is a bit of a misnomer: Some simple groups are pretty darn complicated. What it means is that there is no means of simplifying it using something called the Jordan-Holder decomposition - discussed below. Simple groups are extremely important in the structure theory of finite groups. One example of simple groups are the cyclic groups $\mathbb{Z}/p\mathbb{Z}$ for p prime. Can you think of others?

Remark *Sylow's theorems again.* Recall that Sylow's first theorem says that if p^k divides $|G|$ then G has a subgroup of order p^k. If we take the largest prime power dividing $|G|$, that is, if $|G| = p^k m$ with m relatively prime to p then a subgroup of order p^k is called a *p-Sylow subgroup.* Sylow's second theorem states that all the p-Sylow subgroups are conjugate. The third Sylow theorem says something about how many p-Sylow subgroups there are.

Exercise *Conjugacy Is An Equivalence Relation*

a.) Show that conjugacy is an equivalence relation

b.) Prove that if H is a subgroup of G then gHg^{-1} is also a subgroup of G using the multiplication structure on G.

Exercise *Due Diligence*

a.) Check the details of the proof of Theorem 7.2.1 ! [42]

b.) Consider the *right cosets.* Show that $N\backslash G$ is a group.

c.) Warning! Equation (7.10) does *not* mean that $gng^{-1} = n$ for all $n \in N$! Construct a counterexample using a normal subgroup of S_3.

Exercise *Even Permutations*

Example 7.2.2 has a nice generalization. Recall that a permutation is called *even* if it can be written as a product of an even number of transpositions.

a.) Show that the even permutations, A_n, form a normal subgoup of S_n.

b.) What is S_n/A_n?

---

[42] *Answer*: The main thing to check is that the product law defined by (7.11) is actually well defined. Namely, you must check that if $g_1N = g_1'N$ and $g_2N = g_2'N$ then $g_1g_2N = g_1'g_2'N$. To show this note that $g_1' = g_1n_1$ and $g_2' = g_2n_2$ for some $n_1, n_2 \in N$. Now note that $g_1'g_2' = g_1n_1g_2n_2 = g_1g_2(g_2^{-1}n_1g_2)n_2$. But, since N is normal $(g_2^{-1}n_1g_2) \in N$ and hence $(g_2^{-1}n_1g_2)n_2 \in N$ and hence indeed $g_1g_2N = g_1'g_2'N$. Once we see that (7.11) is well-defined the remaining checks are straightforward. Essentially all the basic axioms are inherited from the group law for multiplying g_1 and g_2. Associativity should be obvious. The identity is $1_GN = N$ and the inverse of gN is $g^{-1}N$. etc. ♠

Exercise *Subgroups Of Index Two*

a.) Suppose that $H \subset G$ is of index two: $[G : H] = 2$. Show that H is normal in G. What is the group G/H in this case? [43]

b.) Using (a) give another proof that $A_n \triangleleft S_n$ is a normal subgroup.

c.) As we will discuss later, the groups A_n for $n \geq 5$ are simple groups. Accepting this for the moment give an infinite set of counterexamples to the converse of Lagrange's theorem. [44]

Exercise

Look at the 3 examples of homogeneous spaces G/H in section 7.1. Decide which of the subgroups H is normal and what the group G/H would be.

Exercise *Sylow subgroups of A_4*

Write down the 2-Sylow and 3-Sylow subgroups of A_4.

Exercise *Commutator Subgroups And Abelianization*

If g_1, g_2 are elements of a group G then the *group commutator* is the element $[g_1, g_2] := g_1 g_2 g_1^{-1} g_2^{-1}$. If G is any group the *commutator subgroup* usually denoted $[G, G]$ (sometimes denoted G') is the subgroup generated by words in all group commutators $g_1 g_2 g_1^{-1} g_2^{-1}$.

a.) Show that $[G, G]$ is a normal subgroup of G.

b.) Show that $G/[G, G]$ is abelian. This is called the *abelianization* of G.

c.) Consider the free group on 2 generators. What is the abelianization?

d.) Consider a surface group of the type given in (6.36). The abelianization of this group is called the *homology group* $H_1(S)$ where S is the punctured surface. Compute this group.

[43] *Answer*: Suppose $G = H \amalg g_0 H$. Then take any $h \in H$. The element $g_0 h g_0^{-1}$ must be in H or $g_0 H$. But if it were in $g_0 H$ then there would be an $h' \in H$ such that $g_0 h g_0^{-1} = g_0 h'$ but this would imply g_0 is in H, which is false. Therefore, for all $h \in H$, $g_0 h g_0^{-1} \in H$, and hence H is a normal subgroup. Therefore $G/H \cong \mathbb{Z}_2$.

[44] *Answer*: Note that the order of $|A_n|$ is even and hence $\frac{1}{2}|A_n|$ is a divisor of $|A_n|$. However, a subgroup of order $|A_n|/2$ would have to be a normal subgroup, and hence does not exist, since A_n is simple. More generally, a high-powered theorem, known as the Feit-Thompson theorem states that a finite simple non-abelian group has even order. Therefore if G is a finite simple nonabelian group there is no subgroup of order $\frac{1}{2}|G|$, even though this is a divisor.

e.) Recall that a *simple* group is a group with no nontrivial normal subgroups. A *perfect* group is a group which is equal to its commutator subgroup. Show that a nonabelian simple group must be perfect.

Exercise *Signed Permutations Again*

Recall our discussion of a natural matrix representation of S_n and the group $W(B_n)$ of signed permutations from *** above.

a.) Show that the subgroup of $W(B_n)$ of diagonal matrices is a normal subgroup isomorphic to $\mathbb{Z}_2^n$.

b.) Show that every signed permutation matrix can be written in the form $D \cdot \Pi$ where D is a diagonal matrix of ±1's and Π is a permutation matrix.

c.) Conclude that the quotient of $W(B_n)$ by the normal subgroup of diagonal matrices is isomorphic to S_n.

d.) Show that every signed permutation can also be written as $\Pi' \cdot D'$. How is this decomposition related to writing it as $D \cdot \Pi$.

Exercise

Consider $O(n, \mathbb{R}) \subset GL(n, \mathbb{R})$. Is this a normal subgroup?

Exercise *The Normalizer Subgroup*

If $H \subset G$ is a subgroup then we define the *normalizer of H within G* to be the largest subgroup of G such that H is normal in that subgroup. Thus

$$N_G(H) := \{g \in G | gHg^{-1} = H\} \tag{7.24}$$

Of course, $H \subset N_G(H)$ is a subgroup - but the point is that it is a normal subgroup and $N_G(H)$ is the largest subgroup of G for which that is the case.

a.) Let $D \subset SU(2)$ be the subgroup of diagonal matrices. Note that $D \cong U(1)$. Compute

$$N_{SU(2)}(D) \tag{7.25}$$

explicitly. [45]

[45] *Answer*: The normalizer is the subgroup of $SU(2)$ that is the union of matrices of the form

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$$

b.) Compute the quotient group $N_{SU(2)}(D)/D$. [46]

Exercise *Homomorphic Images And Normal Subgroups*

Suppose $N \triangleleft G$, and suppose that $\varphi : G \to \tilde{G}$ is a homomorphism to some other group $\tilde{G}$. Then $\varphi(N) \subset \tilde{G}$ is a subgroup. Is it a normal subgroup? [47]

♣Your answer here should have a more explicit counterexample. ♣

Exercise *Products Of Simple Groups*

Let G_1 and G_2 be simple groups.

a.) What are the subgroups of the Cartesian product $G_1 \times G_2$? [48]

b.) Suppose G_i, $i \in I$ is a set of simple groups. What are the subgroups of $\prod_{i \in I} G_i$?

7.3 Conjugacy Classes In S_n

Above we discussed the cycle decomposition of elements of S_n. Now let us study how the cycles change under conjugation.

When showing that transpositions generate S_n we noted the following fact:

If $(i_1 i_2 \cdots i_k)$ is a cycle of length k then $g(i_1 i_2 \cdots i_k)g^{-1}$ is a cycle of length k. It is the cycle where we replace $i_1, i_2, \dots$ by their images under g. That is, if $g(i_a) = j_a$, $a = 1, \dots, k$, then $g(i_1 i_2 \cdots i_k)g^{-1} = (j_1 j_2 \cdots j_k)$.

It therefore follows that:

Any two cycles of length k are conjugate.

Example In S_3 there are two cycles of length 3 and they are indeed conjugate:

$$(12)(123)(12)^{-1} = (213) = (132) \tag{7.26}$$

or of the form

$$\begin{pmatrix} 0 & -z^{-1} \\ z & 0 \end{pmatrix}$$

where z is a phase.

[46] *Answer* The quotient is isomorphic to $\mathbb{Z}_2$. In general, if $D \subset SU(n)$ is the subgroup of diagonal matrices then $N_{SU(n)}(D)/D$ is known as the *Weyl group of* $SU(n)$ and is isomorphic to S_n.

[47] *Answer*: In general it is not a normal subgroup. However, if φ is surjective then it is easy to see that it is a normal subgroup

[48] *Answer*: Only $\{1\}$, $G_1 \times \{1_{G_2}\}$, $\{1_{G_1}\} \times G_2$ and $G_1 \times G_2$.

Now recall that any element in S_n can be written as a product of disjoint cycles.

Therefore, the conjugacy classes in S_n are labeled by specifying a nonnegative integer, denoted ℓ_j, where $j = 1, \dots, n$, and ℓ_j is the number of distinct cycles of length j in the cycle decomposition of any typical element σ of $C(\sigma)$.

Example In S_4 there are 3 elements with cycle decomposition of type $(ab)(cd)$:

$$(12)(34), \qquad (13)(24), \qquad (14)(23) \tag{7.27}$$

Note that these can be conjugated into each other by suitable transpositions. So this conjugacy class is determined by

$$\ell_1 = 0 \qquad \ell_2 = 2 \qquad \ell_3 = 0 \qquad \ell_4 = 0 \tag{7.28}$$

In general we can denote a conjugacy class in S_n by:

$$(1)^{\ell_1}(2)^{\ell_2}\cdots(n)^{\ell_n} \tag{7.29}$$

Then, since we must account for all n letters being permuted we must have:

$$n = 1\cdot\ell_1 + 2\cdot\ell_2 + \cdots n\cdot\ell_n = \sum_{j=1}^{n} j\cdot\ell_j \tag{7.30}$$

Definition A decomposition of n into a sum of nonnegative integers is called a *partition of n*.

Therefore:

$$\boxed{\text{The conjugacy classes of } S_n \text{ are in 1-1 correspondence with the partitions of } n.}$$

Definition The number of distinct partitions of n is called the partition function of n, and denoted $p(n)$. [49]

Example For $n = 4, 5$ $p(4) = 5$ and $p(5) = 7$ and the conjugacy classes of S_4 and S_5 are:

Partition	Cycle decomposition	Typical g	$\vert C(g)\vert$	Order of g
$4 = 1+1+1+1$	$(1)^4$	1	1	1
$4 = 1+1+2$	$(1)^2(2)$	(ab)	$\binom{4}{2} = 6$	2
$4 = 1+3$	$(1)(3)$	(abc)	$2\cdot 4 = 8$	3
$4 = 2+2$	$(2)^2$	$(ab)(cd)$	$\frac{1}{2}\binom{4}{2} = 3$	2
$4 = 4$	(4)	$(abcd)$	6	4

[49] This is a term in number theory. It is not to be confused with the "partition function" of a field theory!

Cycle decomposition	$\lvert C(g)\rvert$	Typical g	Order of g
$(1)^5$	1	1	1
$(1)^3(2)$	$\binom{5}{2}=10$	(ab)	2
$(1)^2(3)$	$2\cdot\binom{5}{3}=20$	(abc)	3
$(1)(4)$	$6\cdot\binom{5}{4}=30$	$(abcd)$	4
$(1)(2)^2$	$5\cdot\frac{1}{2}\binom{4}{2}=15$	$(ab)(cd)$	2
$(2)(3)$	$2\cdot\binom{5}{2}=20$	$(ab)(cde)$	6
(5)	$4!=24$	$(abcde)$	5

♣Put the tables in uniform format and add one for S_6. ♣

Exercise *Sign of the conjugacy class*

Let $\epsilon : S_n \to \{\pm 1\}$ be the sign homomorphism. Show that $\epsilon(g) = (-1)^{n+\sum_j \ell_j}$ if g is in the conjugacy class (7.29).

Exercise *Order of the conjugacy class*

Given a conjugacy class of type (7.29) compute the order $|C(g)|$. [50]

7.3.1 Conjugacy Classes In S_n And Harmonic Oscillators

♣The following remarks assume some knowledge of the quantum mechanics of a simple harmonic oscillator. This is covered later. ♣

There is a beautiful relation of conjugacy classes of the symmetric group with special collections of harmonic oscillators. We'll give a taste of how that happens here. Suppose we have a system which is described by an infinite collection of harmonic oscillators:

$$[a_j, a_k] = 0 \qquad [a_j^\dagger, a_k^\dagger] = 0 \qquad [a_j, a_k^\dagger] = \delta_{j,k} \qquad j,k = 1,\dots \tag{7.31}$$

Suppose they have frequencies which are all a multiple of a basic harmonic which we'll denote ω, so the frequencies are associated with the oscillators $a_1, a_2, a_3, \dots$ are $\omega, 2\omega, 3\omega, \dots$.

Remark: A natural way in which such a collection of oscillators arises is in the quantum mechanics of a string, where the frequencies are those of the harmonics of a vibrating string. If one considers a single massless real scalar field $X(t,\sigma)$ in $1+1$ dimensions on a spacetime of the form $S^1 \times \mathbb{R}$ with action:

$$S = \frac{1}{4\pi\ell_s^2}\int dt \int_0^{2\pi} d\sigma \sqrt{h} h^{ab}\partial_a X \partial_b X \tag{7.32}$$

[50] *Answer*: $|C(g)| = n!/(\prod_{i=1}^n i^{\ell_i}\ell_i!)$.

where ℓ_s has units of length, or inverse mass, and we have temporarily set $\hbar = c = 1$ by choice of units. Then the general solution of the classical equation of motion (the wave equation) is

$$X(t,\sigma) = X_0 + \ell_s^2 pt + \mathrm{i}\frac{\ell_s}{\sqrt{2}} \sum_{n\neq 0} \left(\frac{\alpha_n}{n} e^{\mathrm{i}n(t+\sigma)} + \frac{\tilde{\alpha}_n}{n} e^{\mathrm{i}n(t-\sigma)} \right) \tag{7.33}$$

with complex numbers $\alpha_n = (\alpha_{-n})^*$ and $\tilde{\alpha}_n = (\tilde{\alpha}_{-n})^*$ and X_0, p are real. When quantizing this system we find that $[X_0, p] = \mathrm{i}\hbar$ and

$$[\alpha_n, \alpha_m] = n\delta_{n+m,0} \qquad [\tilde{\alpha}_n, \tilde{\alpha}_m] = n\delta_{n+m,0} \qquad [\alpha_n, \tilde{\alpha}_m] = 0 \tag{7.34}$$

The Hamiltonian computed from the action is

$$H = \frac{1}{2}\ell_s p^2 + \frac{1}{2}\ell_s^{-1} \sum_{n\neq 0} (\alpha_{-n}\alpha_n + \tilde{\alpha}_{-n}\tilde{\alpha}_n) \tag{7.35}$$

and thus corresponds to two towers of oscillators (for left- and right-moving waves). If we represent the Heisenberg algebras with vacua so that $\alpha_n|0\rangle = \tilde{\alpha}_n|0\rangle = 0$ for $n > 0$ then we get standard Harmonic oscillators by defining $a_n = \alpha_n/\sqrt{n}$ and $a_n^\dagger = \alpha_{-n}/\sqrt{n}$ for $n > 0$, and similarly for the right-moving modes $\tilde{\alpha}_n$. We thus recognize $\omega = \ell_s^{-1}$ as our basic frequency.

Returning to our system of a single tower of harmonic oscillators with frequencies $\omega, 2\omega, \dots,$ if we write the standard sum of harmonic oscillator Hamiltonians we get, formally,

$$H^{\text{formal}} = \sum_{j=1}^{\infty} j\omega(a_j^\dagger a_j + \frac{1}{2}) \tag{7.36}$$

This is formal, because on the usual lowest weight module of the system defined by saying the vacuum line satisfies:

$$a_j|vac\rangle = 0 \qquad\qquad \forall j \tag{7.37}$$

the groundstate energy is infinite. This is typical of the divergences of quantum field theory [51] An infinite number of degrees of freedom typically leads to divergences in physical quantities. However, there is a very natural way to regularize and renormalize this divergence by using the Riemann zeta function:

$$\sum_{j=1}^{\infty} \frac{j}{2}\omega = \frac{\omega}{2} \sum_{j=1}^{\infty} \frac{1}{j^{-1}} \to \frac{\omega}{2}\zeta(-1) = -\frac{\omega}{24} \tag{7.38}$$

[52] This can be justified much more rigorously and indeed it gives the correct Casimir energy for a chiral massless scalar field on a circle. In our units above the spatial circle has length

[51] The quantum field theory in question is that of a massless scalar field in a spacetime of $1+1$ dimensions.

[52] One way to see that $\zeta(-1) = -1/12$ is to use the functional equation for the Riemann zeta function. $\zeta(s)$ is a convergent series for $Re(s) > 1$. Define $\xi(s) = \frac{1}{2}\pi^{-s/2}s(s-1)\Gamma(\frac{s}{2})\zeta(s)$. Then one proves the stunning result: $\xi(s) = \xi(1-s)$ for the analytically continued ζ-function. Now, one can analytically continue the Γ function using $\Gamma(x+1) = x\Gamma(x)$, and then evaluate both sides of the functional equation at $s = 2$ using $\Gamma(1/2) = \sqrt{\pi}$ and $\zeta(2) = \pi^2/6$. The analytic continuation of the ζ-function can be derived from the integral representation $2\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty x^{s/2}(\vartheta(\mathrm{i}x) - 1)dx$ and from this representation one easily derives the functional equation once one knows the modular transformation law of the theta function $\vartheta(\tau)$. See section *** below for a physical derivation of the modular transformation law of the theta function.

2π. Restoring the radius of the circle so that the length is $2\pi L$ the ground state energy is:

$$E_{\rm ground} = -\frac{1}{24L} = -\frac{\hbar c}{24L} \tag{7.39}$$

where in the second equation we restored $\hbar$ and c which had been set to 1. Of course, unless you couple the system to gravity, the zero of energy is arbitrary. Here the zero of energy is defined by saying the massless scalar field on the real line has zero groundstate energy. Then the above formula for the Casimir energy is meaningful. What is meaningful independent of the choice of zero of energy is the Casimir force $-\frac{\partial E_{\rm ground}}{\partial L}$.

In any case, things work out very nicely if we take the Hamiltonian to be:

$$H = \sum_{j=1}^{\infty} j\omega a_j^\dagger a_j - \frac{\omega}{24} \tag{7.40}$$

The dimension of the space of states of energy $n\omega$ above the groundstate is $p(n)$. A natural basis of this space is labeled by partitions of n:

$$(a_1^\dagger)^{\ell_1}(a_2^\dagger)^{\ell_2}\cdots(a_n^\dagger)^{\ell_n}|0\rangle \tag{7.41}$$

and hence the vectors in this basis are in 1-1 correspondence with the conjugacy classes of S_n. This turns out to be significant in the boson-fermion correspondence in 1+1 dimensional quantum field theory.

Let q be a complex number with $|q| < 1$. Notice that:

$$\frac{1}{\prod_{j=1}^{\infty}(1-q^j)} = 1 + \sum_{n=1}^{\infty} p(n) q^n \tag{7.42}$$

Indeed, note that this is almost exactly the same as the physical partition function of our system of oscillators!

$$Z^{osc}(\beta) = {\rm Tr} e^{-\beta H} = \frac{1}{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)}, \tag{7.43}$$

where we trace over the Hilbert space of states of our collection of oscillators. Here we identify $q = e^{-\beta\omega}$. Expanding out (7.42) gives the first few values of $p(n)$:

$$\begin{aligned} &1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + 11q^6 + 15q^7 + 22q^8 + 30q^9 + \\ &+ 42q^{10} + 56q^{11} + 77q^{12} + 101q^{13} + 135q^{14} + \cdots \end{aligned} \tag{7.44}$$

and one can easily generate the first few 100 values using Maple or Mathematica or Sage or ...

It turns out the generating series has a remarkable "modular transformation property" relating $Z(\beta)$ to $Z(1/\beta)$:

$$\beta^{-1/4} Z^{osc}(\beta) = \tilde{\beta}^{-1/4} Z^{osc}(\tilde{\beta}) \tag{7.45}$$

$$\beta\tilde{\beta} = \left(\frac{2\pi}{\omega}\right)^2 \tag{7.46}$$

The property (7.45) and (7.46) is proven in textbooks on analytic number theory. From the physics viewpoint it is quite natural for the following reason. Consider the massless scalar field on the circle. It has two copies of our infinite towers of oscillators: One for the clockwise moving waves and one for the counterclockwise moving waves. So

$$Z(\beta) := Tre^{-\beta H} = (2\pi\beta\omega)^{-1/2} \left|Z^{osc}((\beta)\right|^2 \tag{7.47}$$

where the prefactor comes from the zeromode degrees of freedom (X_0, p) of the scalar field and is obtained from the Gaussian integral

$$\ell_s \int_{-\infty}^{+\infty} \frac{dp}{2\pi} e^{-\beta\frac{1}{2}\ell_s p^2} = \frac{\ell_s}{\sqrt{2\pi\beta\ell_s}} = \frac{1}{\sqrt{2\pi\beta\omega}} \tag{7.48}$$

We have written this for β real.

Moreover, it is a standard and fundamental result that for real β the partition function $Tre^{-\beta H}$ can be written as a path integral with periodic Euclidean time of period β. However, the quantum field X is already a map from the circle to the real line so altogether we have a path integral on a torus $S^1 \times S^1$ with metric $ds^2 = (2\pi)^2((d\sigma)^2 + \beta^2(d\tau)^2)$.

Now, in statistical physics it is natural to consider the analytic continuation of $Z(\beta)$ to the subset of the complex β-plane with positive real part. In this case, to interpret the analytic continuation as a trace we should split the Hamiltonian into contributions of left- and right-moving oscillators and consider the expression [53]

$$Z(\beta) = \mathrm{Tr} q^{H_L} \bar{q}^{H_R} \tag{7.49}$$

where we set $q = e^{2\pi \mathrm{i}\tau} = e^{-\beta\omega}$ so $\tau = \mathrm{i}\frac{\beta\omega}{2\pi}$. The path integral interpretation is now that of a massless scalar field on a torus $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ with a flat metric $ds^2 = |dz|^2$ where τ is a complex number in the upper half-plane. One can easily (and rigorously) compute that path integral and show that it is

$$Z(\beta) = (\mathrm{Im}\tau)^{-1/2} |\eta(\tau)|^{-2} \tag{7.50}$$

where

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \tag{7.51}$$

confirming the general principle we just enunciated. On the other hand, the path integral is invariant under large diffeomorphisms of the torus. If we take $z = x + \tau y$ with x, y real and x, y identified modulo one, then we can make the diffeomorphism that rotates by 90 degrees in the x, y plane. This takes the torus to a torus with $\tau \to -1/\tau$ and the flat metric rescaled by a constant factor: If $ds^2 = |dz|^2$ with $z = x + \mathrm{i}y$ then the pull-back is $ds^2 = |\tau|^2 |dx' + \tau' dy'|^2$ with $x' = y$ and $y' = -x'$ and $\tau' = -1/\tau$. But the massless scalar

[53] To amplify on this some more, $H = \frac{1}{2}(H_L + H_R)$ but when splitting into left and rightmovers we define $H_L = H + P$ and $H_R = H - P$ where P is the total momentum of the field. Then the trace can be written as $\mathrm{Tr} e^{-Re(\beta\omega)H} e^{-\mathrm{i}Im(\beta\omega)P}$. The extra insertion of P accounts for the shift made before identifying the edges at Euclidean times 0 and $Re(\beta)$.

field is a conformal field theory, and for a flat metric the path integral will be invariant. Therefore $(\mathrm{Im}\tau)^{-1/2}|\eta(\tau)|^{-2}$ is invariant under $\tau \to -1/\tau$ and since $\eta(\tau)$ is holomorphic one can deduce the very important result:

$$\eta(-1/\tau) = (-\mathrm{i}\tau)^{1/2}\eta(\tau). \tag{7.52}$$

This equation is equivalent to the identity in equations (7.45) and (7.46).

As an interesting application, when combined with the method of stationary phase, one can derive the Hardy-Ramanujan formula giving an asymptotic formula for large values of n:

$$p(n) \sim \frac{1}{\sqrt{2}}\Big(\frac{1}{24}\Big)^{3/4} n^{-1} \exp\left(2\pi\sqrt{\frac{n}{6}}\right) \tag{7.53}$$

Note that this grows much more slowly than the order of the group, $n!$. So we conclude that some conjugacy classes must be very large! (See discussion in the next section on the class equation if this is not obvious.)

Analogs of equation (7.53) for a class of functions known as *modular forms* plays an important role in modern discussions of the entropy of supersymmetric (and extreme) black hole solutions of supergravity.

Exercise *Deriving the Hardy-Ramanujan formula*

The function $Z(\beta)$ has a nice analytic continuation into the right half complex plane where $\mathrm{Re}(\beta) > 0$. Note that $q^{1/24}Z(\beta)$ is periodic under imaginary shifts $\beta \to \beta + \frac{2\pi \mathrm{i}}{\omega}$.

Write

$$p(n) = \int_{\beta_0}^{\beta_0 + \frac{2\pi\mathrm{i}}{\omega}} d\beta e^{-n\beta\omega} q^{1/24} Z(\beta) \tag{7.54}$$

and use the above transformation formula, together with the stationary phase method to derive (7.53). [54]

7.3.2 Conjugacy Classes In S_n And Partitions

Another way of thinking about partitions of n uses the general idea of partitions: In general, a *partition* is a sequence of nonnegative integers $\{\lambda_1, \lambda_2, \lambda_3, \dots\}$ so that

a.) λ_i are nonincreasing: $\lambda_i \geq \lambda_{i+1}$.

b.) The λ_i eventually become zero.

[54] *Answer*: Write $p(n) = \int_{-1/2+\mathrm{i}\beta}^{1/2+\mathrm{i}\beta} e^{-2\pi \mathrm{i} n\tau} q^{1/24}\eta(\tau)^{-1} d\tau$ where $\tau = x + \mathrm{i}\beta$ and the contour is along a horizontal line. One argues that, as $\beta \to 0^+$ the dominant terms in the integral come from the region near $x \cong 0$. (This is a rather subtle step to do correctly.) Then, using the modular transformation law one writes $\eta(\tau)^{-1} = (-\mathrm{i}\tau)^{1/2}\eta(-1/\tau)^{-1}$ and for $\mathrm{Im}(-1/\tau) \to \infty$ one approximates $\eta(-1/\tau)^{-1} \cong \exp[2\pi\mathrm{i}/(24\tau)]$. Now one applies the standard stationary phase technique. When this procedure is carried out more systematically one is led to the famous Rademacher expansion for coefficients of certain modular functions.

Given a partition, we define $|\lambda| = \sum_i \lambda_i$ so that a partition of n can be written:

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_k \tag{7.55}$$

as a sum of positive integers with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$. The nonzero λ_i are called the *parts of the partition.* The above is a partition of n with k parts.

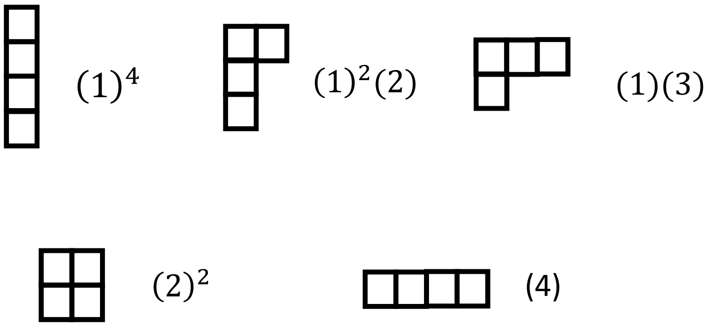

Figure 16: Young diagrams corresponding to the 5 different partitions of 4.

In general, to a partition λ we can associate a *Young diagram.* This is a diagram with λ_1 boxes in the first row, λ_2 boxes in the second row and so forth. The boxes are arranged to make, roughly speaking, an upside-down L-shape. See Figure 16 for some examples. We will talk much more about these when discussing representations of the symmetric group and representations of $SU(n)$.

We can associate a conjugacy class in S_n with a partition as follows. We let

$$m_i(\lambda) := |\{j|\lambda_j = i\}| \tag{7.56}$$

denote the *multiplicity of i in λ* and then we have

$$(1)^{m_1}(2)^{m_2}\cdots \tag{7.57}$$

as the associated conjugacy class.

It is worth noting that there is another associated partition and conjugacy class known as the conjugate partition λ. It corresponds to the partition obtained by flipping on the main diagonal. Here λ'_i is the number of boxes in the i^{th} column. Note that

$$\lambda_i = |\{j|\lambda'_j \geq i\}| \tag{7.58}$$

and since $\lambda'' = \lambda$ this means

$$\lambda'_i = |\{j|\lambda_j \geq i\}| \tag{7.59}$$

and hence

$$m_i(\lambda) = \lambda'_i - \lambda'_{i+1} \tag{7.60}$$

This corresponds to the identity

$$\lambda'_1+\lambda'_2+\cdots+\lambda'_n = (\lambda'_1-\lambda'_2)+2(\lambda'_2-\lambda'_3)+3(\lambda'_3-\lambda'_4)+\cdots+(n-1)(\lambda'_{n-1}-\lambda'_n)+n\lambda'_n \tag{7.61}$$

Thus, we can associate this to the conjugacy class

$$(1)^{\lambda'_1-\lambda'_2}(2)^{\lambda'_2-\lambda'_3}\cdots(n)^{\lambda'_n} \tag{7.62}$$

Now, when n is large we can ask what the "typical" partition is. That is, what are the "typical" conjugacy classes in S_n when n is large? This is an imprecise, and rather subtle question. To get some sense of an answer it is useful to consider the number $p_k(n)$ of partitions of n into precisely k parts (as in (7.55)). The generating function is

$$\sum_{n=1}^{\infty} p_k(n)x^n = \prod_{j=1}^{k} \frac{x}{1-x^j} \tag{7.63}$$

One natural guess, then, is that the "typical" partition has $k \cong \sqrt{n}$ with "most of the parts" on the order of $\sqrt{n}$. This naive picture can be considerably improved using the statistical theory of partitions. [55] Without going into a lot of complicated asymptotic formulae, the main upshot is that, for large n, as a function of k, $p_k(n)$ indeed is sharply peaked with a maximum around

$$\bar{k}(n) := \frac{\sqrt{6}}{2\pi}\sqrt{n}\mathrm{log}n \tag{7.64}$$

See Figure 17 for a numerical illustration. Moreover, and again speaking very roughly, the number of terms in the partition λ_j with $\lambda_j \cong \frac{\sqrt{6}}{2\pi}\sqrt{n}$ is order $\sqrt{6n}/\pi$.

Remark: Recall that in our discussion of a string, or equivalently of a massless scalar field on the circle, there are $p(n)$ states in the energy eigenspace with energy $E = (n - \frac{1}{24})\omega$. Thus we can interpret the above result as a kind of equipartition theorem: The most likely state is the one where the energy is shared equally by the different oscillators.

Exercise *Generating Function For $p_k(n)$*

Prove equation (7.63). [56]

[55] It is a large subject. See P Erdös and J. Lehner, "The distribution of the number of summands in the partition of a positive integer," Duke Math. Journal **8**(1941)335-345 or M. Szalay and P. Turán, "On some problems of the statistical theory of partitions with application to characters of the symmetric group. I," Acta Math. Acad. Scient. Hungaricae, Vol. 29 (1977), pp. 361-379.

[56] *Answer*: A partition of n into exactly k-parts means that $\lambda_k \geq 1$. So now write

$$n-k = (\lambda_1-\lambda_2)+2(\lambda_2-\lambda_3)+\cdots+(k-1)(\lambda_{k-1}-\lambda_k)+k(\lambda_k-1)$$

This is a partition of $n-k$ as a sum of integers drawn from $\{1,\ldots,k\}$. Enumerating those is clearly given by $\prod_{j=1}^{k}(1-x^j)^{-1}$.

Exercise *Transpose Partition*

Show that the reflection of a partition around the diagonal is another partition λ'. Write a formula for λ'_i in terms of λ

8. More About Group Actions And Orbits

NOTE BENE! THE MATERIAL IN THIS SECTION IS IDENTICAL TO SECTION 2 OF CHAPTER 3

In Section 4.2 above we introduced the notion of a group action on a set. In this section we develop this important idea a bit further.

8.1 Some Definitions And Terminology Associated With Group Actions

Let X be any set (possibly infinite). Recall the definition we gave in Section 4.2.

A *permutation* of X is a 1-1 and onto mapping $X \to X$. The set S_X of all permutations forms a group under composition. A *transformation group* on X is a subgroup of S_X.

Equivalently, a *G-action on a set X* is a map $\phi : G \times X \to X$ compatible with the group multiplication law as follows:

A *left-action* satisfies:

$$\phi(g_1, \phi(g_2, x)) = \phi(g_1 g_2, x) \tag{8.1}$$

A *right-action* satisfies

$$\phi(g_1, \phi(g_2, x)) = \phi(g_2 g_1, x) \tag{8.2}$$

In addition in both cases we require that

$$\phi(1_G, x) = x \tag{8.3}$$

for all $x \in X$.

Remarks:

1. If ϕ is a left-action then it is natural to write $g \cdot x$ for $\phi(g, x)$. In that case we have

$$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x. \tag{8.4}$$

Similarly, if ϕ is a right-action then it is better to use the notation $\phi(g, x) = x \cdot g$ so that

$$(x \cdot g_2) \cdot g_1 = x \cdot (g_2 g_1). \tag{8.5}$$

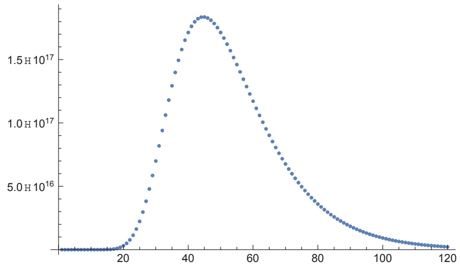

Figure 17: Showing the distribution of $p_k(n)$ as a function of k for $n = 400$ and $1 \leq k \leq 120$. Note that the Erdös-Lehner mean value of k is $\bar{k} = \frac{\sqrt{6}}{2\pi} 20 \log(20) \cong 46.7153$ is a very good approximation to where the distribution has its sharp peak. The actual maximum is at $k = 45$.

2. If ϕ is a left-action then $\tilde{\phi}(g, x) := \phi(g^{-1}, x)$ is a right-action, and vice versa. Thus there is no essential difference between a left- and right-action. However, in computations with nonabelian groups it is extremely important to be consistent and careful

about which choice one makes.

3. A given set X can admit more than one action by the same group G. If one is working simultaneously with several different G actions on the same set then the notation $g \cdot x$ is ambiguous and one should write, for example, $\phi_g(x) = \phi(g, x)$ or speak of ϕ_g, etc. A good example of a set X with several natural G actions is the case of $X = G$ itself. Then there are the actions of left-multiplication, right-multiplication, and conjugation:

$$\begin{aligned} L(g, g') &= gg' \\ R(g, g') &= g'g \\ C(g, g') &= g^{-1}g'g \end{aligned} \tag{8.6}$$

where on the RHS of these equations we use group multiplication. Note that our choice of C makes it a right-action of G on G. (Had we defined conjugation by $g' \mapsto gg'g^{-1}$ we would have defined a left-action.)

There is some important terminology one should master when working with G-actions. First here are some terms used when describing a G-action on a set X:

Definitions:

1. A group action is *effective* or *faithful* if for any $g \neq 1$ there is some x such that $g \cdot x \neq x$. Equivalently, the only $g \in G$ such that ϕ_g is the identity transformation is $g = 1_G$. A group action is *ineffective* if there is some $g \in G$ with $g \neq 1$ so that $g \cdot x = x$ for all $x \in X$. The set of $g \in G$ that act ineffectively is a normal subgroup of G.
2. A group action is *transitive* if for any pair $x, y \in X$ there is some g with $y = g \cdot x$.
3. A group action is *free* if for any $g \neq 1$ then for *every* x, we have $g \cdot x \neq x$.

In summary:

1. *Effective*: $\forall g \neq 1, \exists x$ s.t. $g \cdot x \neq x$.
2. *Ineffective*: $\exists g \neq 1$,s.t. $\forall x \; g \cdot x = x$.
3. *Transitive*: $\forall x, y \in X, \exists g$ s.t. $y = g \cdot x$.
4. *Free*: $\forall g \neq 1, \forall x, \; g \cdot x \neq x$

In addition there are some further important definitions:

1. Given a point $x \in X$ the set of group elements:

$$\mathrm{Stab}_G(x) := \{g \in G : g \cdot x = x\} \tag{8.7}$$

is called the *isotropy group at x*. It is also called the *stabilizer group* of x. It is often denoted G^x. The reader should show that $G^x \subset G$ is in fact a subgroup. Note that a group action is free iff for every $x \in X$ the stabilizer group G^x is the trivial subgroup $\{1_G\}$.

2. A point $x \in X$ is a *fixed point* of the G-action if there exists some element $g \in G$ with $g \neq 1$ such that $g \cdot x = x$. So, a point $x \in X$ is a fixed point of G iff $\mathrm{Stab}_G(x)$ is not the trivial group. Some caution is needed here because if an author says "x is a fixed point of G" the author might mean that $\mathrm{Stab}_G(x) = G$. That would not be implied by our terminology.

3. Given a group element $g \in G$ the *fixed point set* of g is the set

$$\mathrm{Fix}_X(g) := \{x \in X : g \cdot x = x\} \tag{8.8}$$

   The fixed point set of g is often denoted by X^g. Note that if the group action is free then for every $g \neq 1$ the set $\mathrm{Fix}_X(g)$ is the empty set.

4. We repeat the definition from section **** above. The *orbit of G through a point x* is the set of points $y \in X$ which can be reached by the action of G:

$$O_G(x) = \{y : \exists g \quad \text{such that} \quad y = g \cdot x\} \tag{8.9}$$

Remarks:

1. If we have a G-action on X then we can define an equivalence relation on X by defining $x \sim y$ if there is a $g \in G$ such that $y = g \cdot x$. (Check this is an equivalence relation!) The orbits of G are then exactly the equivalence classes of under this equivalence relation. Therefore, X is partitioned into a disjoint union of all the G-orbits.

2. The group action restricts to a transitive group action on any orbit.

3. If x, y are in the same orbit then the isotropy groups G^x and G^y are conjugate subgroups in G. Therefore, to a given orbit, we can assign a definite *conjugacy class* of subgroups.

Point 3 above motivates the

Definition If G acts on X a *stratum* is a set of G-orbits such that the conjugacy class of the stabilizer groups is the same. The set of strata is sometimes denoted $X \parallel G$.

♣HAVE ALL THE CONCEPTS HERE TO DEFINE THE IDEA OF A TORSOR AND THIS IS THE RIGHT PLACE TO INTRODUCE THE CONCEPT. MOVE SOME MATERIAL FROM AFFINE EUCLIDEAN SPACE DISCUSSION SECTION 13.4 BELOW TO HERE. ♣

Exercise

Recall that a group action of G on X can be viewed as a homomorphism $\phi : G \to S_X$. Show that the action is effective iff the homomorphism is injective.

Exercise

Suppose X is a G-set.

a.) Show that the subset H of elements which act ineffectively, i.e. the set of $h \in G$ such that $\phi(h,x) = x$ for all $x \in X$ is a normal subgroup of G.

b.) Show that the group G/H acts effectively on X.

Exercise

Let G act on a set X.

a.) Show that the stabilizer group at x, denoted G^x above, is in fact, a subgroup of G.

b.) Show that the G action is free iff the stabilizer group at every $x \in X$ is the trivial subgroup $\{1_G\}$.

c.) Suppose that $y = g \cdot x$. Show that G^y and G^x are conjugate subgroups in G. [57]

Exercise *Derangements*

A permutation in S_n which acts on $\{1, \dots, n\}$ without fixed points is called a *derangement.* Show that the number of derangements in S_n is given by

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \tag{8.10}$$

8.2 The Stabilizer-Orbit Theorem

There is a beautiful relation between orbits and isotropy groups:

Theorem [Stabilizer-Orbit Theorem]: Each left-coset of G^x in G is in 1-1 correspondence with the points in the G-orbit of x:

$$\psi : Orb_G(x) \to G/G^x \tag{8.11}$$

for a $1-1$ map ψ.

Proof: Suppose y is in a G-orbit of x. Then $\exists g$ such that $y = g \cdot x$. Define $\psi(y) \equiv g \cdot G^x$. You need to check that ψ is actually well-defined.

[57] *Answer*: If $y = g_0 \cdot x$ and $g \cdot x = x$ then $(g_0 g g_0^{-1}) \cdot y = y$ so $G^y = g_0 G^x g_0^{-1}$.

$$y = g' \cdot x \qquad \rightarrow \qquad \exists h \in G^x \qquad g' = g \cdot h \qquad \rightarrow \qquad g'G^x = ghG^x = gG^x \tag{8.12}$$

Conversely, given a coset $g \cdot G^x$ we may define

$$\psi^{-1}(gG^x) \equiv g \cdot x \tag{8.13}$$

Again, we must check that this is well-defined. Since it inverts ψ, ψ is 1-1. ♠

Corollary: If G acts transitively on a set X then the isotropy groups G^x for all the points $x \in X$ are conjugate subgroups of G, and for any $x \in X$, there is a $1-1$ correspondence between X and the set of cosets G/G^x. If H is any one of these isotropy groups we can therefore identify X with the set of left-cosets G/H.

Remark: Sets of the type G/H are called *homogeneous spaces*. This theorem is the beginning of an important connection between the *algebraic* notions of subgroups and cosets to the *geometric* notions of orbits and fixed points. Below we will show that if G, H are topological groups then, in some cases, G/H are beautifully symmetric topological spaces, and if G, H are Lie groups then, in some cases, G/H are beautifully symmetric manifolds.

Exercise *The Lemma that is not Burnside's*

Suppose a finite group G acts on a finite set X as a transformation group. A common notation for the set of points fixed by g is X^g. Show that the number of distinct orbits is the averaged number of fixed points:

$$|\{orbits\}| = \frac{1}{|G|}\sum_g |X^g| \tag{8.14}$$

For the answer see. [58]

Exercise *Jordan's theorem*

[58] *Answer*: Write

$$\sum_{g \in G} |X^g| = |\{(x,g)|g \cdot x = x\}| = \sum_{x \in X} |G^x| \tag{8.15}$$

Now use the stabilizer-orbit theorem to write $|G^x| = |G|/|\mathcal{O}_G(x)|$. Now in the sum

$$\sum_{x \in X} \frac{1}{|\mathcal{O}_G(x)|} \tag{8.16}$$

the contribution of each distinct orbit is exactly 1.

Suppose G is finite and acts transitively on a finite set X with more than one point. Show that there is an element $g \in G$ with no fixed points on X. [59]

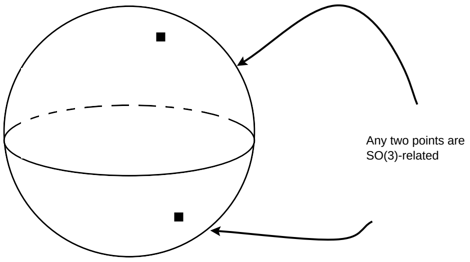

Figure 18: Transitive action of $SO(3,\mathbb{R})$ on the sphere.

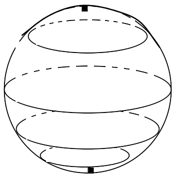

Figure 19: Orbits of $SO(2,\mathbb{R})$ on the two sphere.

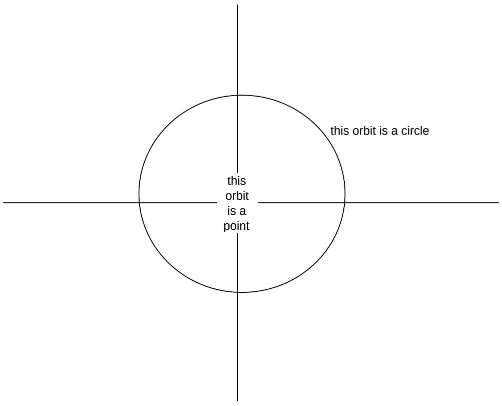

Figure 20: Notice not all orbits have the same dimensionality. There are two qualitatively different kinds of orbits of $SO(2,\mathbb{R})$.

8.3 Examples Of Orbits

The concept of a G-action on a set is an extremely important concept, so let us consider a number of examples:

Examples

[59] Hint: Note that $X = G/H$ for some H and apply the Burnside lemma.

1. Let $X = \{1, \cdots n\}$, so $S_X = S_n$ as before. The action is effective and transitive, but not free. Indeed, the fixed point of any $j \in X$ is just the permutations that permute everything else, and hence $S_X^j \cong S_{n-1}$. Note that different j have different stabilizer subgroups isomorphic to S_{n-1}, but they are all conjugate.

2. *Group actions on the plane.* The group $G = GL(2, \mathbb{R})$ acts on the plane $X = \mathbb{R}^2$ by linear transformation. The action is effective: If $g \neq 1$ then it moves some vector a nonzero amount! There are only two orbits: Note that if $\vec{x} = 0$ then it remains zero under linear transformation, so $\{\vec{0}\}$ is an orbit. On the other hand, if $\vec{x}, \vec{y}$ are both nonzero then some linear transformation certainly will map $\vec{x}$ to $\vec{y}$. The action is therefore not transitive, and not free.

3. Similarly, $GL(n, \mathbb{R})$ acts on $\mathbb{R}^n$. If we act with a matrix on a column vector we get a left action. If we act on a row vector we get a right action. Either way, there are two orbits.

4. We can restrict the $GL(2, \mathbb{R})$ action on $\mathbb{R}^2$ to the action of the subgroup $G = SO(2, \mathbb{R})$. This completely changes the picture. The action is:
$$R(\phi) : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \rightarrow \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \tag{8.17}$$
The group action is effective. It is not free, and it is not transitive. There are now infinitely many orbits of $SO(2)$, and they are all distinguished by the invariant value of $x^2 + y^2$ on the orbit. From the viewpoint of topology, there are two distinct "kinds" of orbits acting on $\mathbb{R}^2$. One has trivial isotropy group and one has isotropy group $SO(2)$. See Figure 20. These give two strata.

5. Orbits of $O(2)$. We have seen that $O(2)$ can be written as a disjoint union:
$$O(2) = SO(2) \amalg P \cdot SO(2) \tag{8.18}$$
where P is not canonical and can be taken to be reflection in any line through the origin. The orbits of $SO(2)$ and $O(2)$ are the same.

6. Similarly, $SO(3, \mathbb{R})$ acts on $X = \mathbb{R}^3$. It is effective, not transitive, and not fixed-point-free. There are two strata: We can have G^x isomorphic to $SO(2, \mathbb{R})$ and we can have $G^x = SO(3, \mathbb{R})$ (when $x = 0$).

7. Now restrict the $SO(3, \mathbb{R})$ action on $\mathbb{R}^3$ to a nontrivial orbit, namely a sphere of positive radius S_R^2. The action is then transitive on the sphere, The isotropy group of any point $x \in S_R^2$ is the subgroup of rotations about the axis through that point. That subgroup is isomorphic to $SO(2, \mathbb{R})$, but as x varies the particular subgroup varies. For example, with usual conventions, if x is on the x^3-axis then the subgroup is the subgroup of matrices of the form
$$\begin{pmatrix} \cos\phi & \sin\phi & 0 \\ -\sin\phi & \cos\phi & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{8.19}$$

♣Improve this example and use this transitive action to derive the range of the three Euler angles ϕ, ψ identified modulo 2π and $0 \leq \theta \leq \pi$. That will be useful when we discuss the double cover $SU(2)$ below. ♣

but if x is on the x^1-axis the subgroup is the subgroup of matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\phi & \sin\phi \\ 0 & -\sin\phi & \cos\phi \end{pmatrix} \tag{8.20}$$

and so on. For a nonzero vector x on the sphere let $SO(2)_x \subset SO(3)$ denote the subgroup, isomorphic to $SO(2,\mathbb{R})$, which stabilizes x. According to the stabilizer-orbit theorem there is a natural one-one correspondence

$$S^2 \cong SO(3)/SO(2)_x \tag{8.21}$$

Therefore, fixing any $x \in S^2$ there is a map

$$\pi : SO(3,\mathbb{R}) \to S^2 \tag{8.22}$$

Put simply, $\pi(R)$ rotates $x \in S^2$ to $R \cdot x \in S^2$. This turns out to be a very interesting map and we will come back to it.

8. By contrast consider a fixed $SO(2,\mathbb{R})$ subgroup of $SO(3,\mathbb{R})$, say, the subgroup defined by rotations around the z-axis. This subgroup also acts on the sphere - but *not* transitively. The G-orbits are shown in Figure 19.

9. If $G = \mathbb{Z}_2$ acts linearly on $\mathbb{R}^{n+1}$ (i.e. $V = \mathbb{R}^{n+1}$ is a representation of $\mathbb{Z}_2$) then we can choose coordinates so that the nontrivial element $\sigma \in G$ acts by

$$\sigma \cdot (x^1, \dots, x^{n+1}) = (x^1, \dots, x^p, -x^{p+1}, \cdots, -x^{p+q}) \tag{8.23}$$

where $p + q = n + 1$. Note that this action preserves the equation of the sphere $\sum_i (x^i)^2 - 1 = 0$ and hence descends to a $\mathbb{Z}_2$-action on the sphere S^n. The case $p = 0, q = n + 1$ is the antipodal map. The set of orbits is known as $\mathbb{RP}^n \cong S^n/\langle -1 \rangle$. There are many other natural actions of $\mathbb{Z}_2$ on S^n.

10. Let the group be $G = \mathbb{C}^*$. This acts on $X = \mathbb{C}^n$ by scaling all the coordinates. The set of orbits is not a nice manifold, but the set of orbits of the action on $\tilde{X} = \mathbb{C}^n - \{0\}$ is a good manifold (see below). It is called $\mathbb{CP}^{n-1}$.

11. Now consider a set of integers $(q_1, \dots, q_n) \in \mathbb{Z}^n$. Then for each such set of integers there is a $\mathbb{C}^*$-action on $\mathbb{CP}^{n-1}$ defined by

$$\mu \cdot [X^1 : \cdots : X^n] := [\mu^{q_1} X^1 : \cdots : \mu^{q_n} X^n] \tag{8.24}$$

for $\mu \in \mathbb{C}^*$. (Check it is well-defined!)

12. The group $G = SL(2,\mathbb{R})$ acts on the complex upper half plane:

$$\mathcal{H} = \{\tau | \mathrm{Im}\tau > 0\} \tag{8.25}$$

via

$$g \cdot \tau := \frac{a\tau + b}{c\tau + d} \tag{8.26}$$

where

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{8.27}$$

13. *Actions of $\mathbb{Z}$ on* <u>*any*</u> *set X.* Let us consider $\mathbb{Z}$ to be the free group with one generator g_0. Then, given <u>any</u> invertible map $f : X \to X$ we can define a group action of $\mathbb{Z}$ on X by

$$g_0^n \cdot x = \begin{cases} \underbrace{f \circ \cdots \circ f}_{n \quad \text{times}}(x) & n > 0 \\ x & n = 0 \\ \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{|n| \quad \text{times}}(x) & n < 0 \end{cases} \tag{8.28}$$

Conversely, any $\mathbb{Z}$-action must be of this form since we can define $f(x) := g_0 \cdot x$.

14. Let G be any group and consider the group action defined by $\phi(g, x) = x$ for all $g \in G$. This is as ineffective as a group action can be: For every x, the istropy group is all of G, and for all $g \in G$, $\mathrm{Fix}(g) = X$. In particular, this situation will arise if X consists of a single point. This example is not quite as stupid as might at first appear, once one takes the categorical viewpoint, for $pt//G$ is a very rich category indeed.

Exercise $\mathbb{Z}_2$ *Actions On The Sphere*

Consider the action of $\mathbb{Z}_2$ on the sphere defined by (8.23).

a.) For which values of p, q is the action effective?

b.) For which values of p, q is the action transitive?

c.) Compute the fixed point set of the nontrivial element $\sigma \in \mathbb{Z}_2$.

d.) For which values of p, q is the action free?

Exercise $\mathbb{C}^*$ *Actions On* $\mathbb{CP}^{n-1}$

Consider the action of $G = \mathbb{C}^*$ on $\mathbb{CP}^{n-1}$ defined by (8.24).

a.) For which values of $(q_1, \dots, q_n)$ is the action effective?

b.) For which values of $(q_1, \dots, q_n)$ is the action transitive?

c.) What are the fixed points of the $\mathbb{C}^*$ action?

d.) What are the stabilizers at the fixed points of the $\mathbb{C}^*$ action?

Exercise *Group Actions On* $\mathbb{CP}^1$

As explained above, $\mathbb{CP}^1$ can be identified with equivalence classes of points $(z_1, z_2) \in \mathbb{C}^2 - \{0\}$ with equivalence relation $(z_1', z_2') \sim (\lambda z_1, \lambda z_2)$. We denote equivalence classes by $[z_1 : z_2]$.

a.) Show that there is an action of $GL(2;\mathbb{C})$ on $\mathbb{CP}^1$. Identify the subgroup $B \subset GL(2,\mathbb{C})$ stabilizing $[1:0]$. Conclude that there is a 1-1 correspondence

$$GL(2;\mathbb{C})/B \cong \mathbb{CP}^1 \tag{8.29}$$

(This is in fact and isomorphism of complex manifolds, but we have not developed the tools to prove that.)

b.) Show that there is an action of $SU(2)$ on $\mathbb{CP}^1$. Show that the stabilizer of $[1:0]$ is isomorphic to $U(1)$. Conclude that there is an identification

$$\mathbb{CP}^1 \cong SU(2)/U(1) \tag{8.30}$$

and hence there is a natural map

$$\pi : SU(2) \to \mathbb{CP}^1 \tag{8.31}$$

defined by this identification. This is a famous map in mathematics and physics known as the *Hopf map* and has many beautiful properties. It appears in the physics of magnetic monopoles and in several other related contexts.

Exercise $SL(2,\mathbb{R})$ *Action On The Upper Half-Plane*

a.) Show that (8.26) above defines a left-action of $SL(2,\mathbb{R})$ on the complex upper half-plane. [60]

b.) Is the action effective?

c.) Is the action transitive?

d.) Which group elements have fixed points?

e.) What is the isotropy group of $\tau = \mathrm{i}$? [61]

[60] *Hint*: Show that $\mathrm{Im}(g \cdot \tau) = \frac{\mathrm{Im}\tau}{|c\tau+d|^2}$.

[61] The isotropy group is the subgroup $SO(2,\mathbb{R}) \subset SL(2,\mathbb{R})$. To see this set $\frac{a\mathrm{i}+b}{c\mathrm{i}+d} = \mathrm{i}$ and conclude that $a = d$ and $b = -c$. Then since $ad - bc = 1$ we have $a^2 + b^2 = 1$ but this implies that the group element is in $SO(2,\mathbb{R})$.

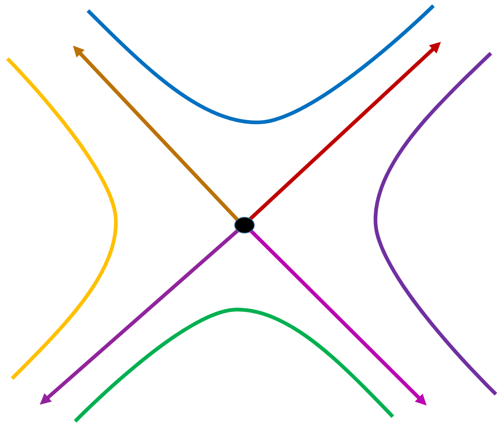

Figure 21: The distinct kinds of orbits of $SO(1,1,\mathbb{R})$ are shown in different colors. If we enlarge the group to include transformations that reverse the orientation of time and/or space then orbits of the larger group will be made out of these orbits by reflection in the space or time axis.

8.3.1 Extended Example: The Case Of $1+1$ Dimensions

Consider 1+1-dimensional Minkowski space with coordinates $x = (x^0, x^1)$ and metric given by

$$\eta := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \tag{8.32}$$

i.e. the quadratic form is $(x, x) = -(x^0)^2 + (x^1)^2$. The two-dimensional Lorentz group is defined by

$$O(1,1) = \{A | A^{tr} \eta A = \eta\} \tag{8.33}$$

This group acts on $\mathbb{M}^{1,1}$ preserving the Minkowski metric.

The connected component of the identity is the group of Lorentz boosts of rapidity θ:

$$x^0 \to \cosh\theta \; x^0 + \sinh\theta \; x^1 \tag{8.34}$$

$$x^1 \to \sinh\theta \; x^0 + \cosh\theta \; x^1 \tag{8.35}$$

that is:

$$SO_0(1,1;\mathbb{R}) \equiv \{B(\theta) = \begin{pmatrix} \cosh\theta & \sinh\theta \\ \sinh\theta & \cosh\theta \end{pmatrix} | -\infty < \theta < \infty\} \tag{8.36}$$

In the notation the S indicates we look at the determinant one subgroup and the subscript 0 means we look at the connected component of 1. This is a group since

$$B(\theta_1)B(\theta_2) = B(\theta_1 + \theta_2) \tag{8.37}$$

so $SO_0(1,1) \cong \mathbb{R}$ as groups. Indeed, note that

$$B(\theta) = \exp\left[\theta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] \tag{8.38}$$

It is often useful to define *light cone coordinates*: [62]

$$x^{\pm} := x^0 \pm x^1 \tag{8.39}$$

and the group action in these coordinates is simply:

$$x^{\pm} \to e^{\pm\theta} x^{\pm} \tag{8.40}$$

so it is obvious that $x^+x^- = -(x,x)$ is invariant.

It follows that the orbits of the Lorentz group are, in general, hyperbolas. They are separated by different values of the Lorentz invariant $x^+x^- = \lambda$, but this is not a complete invariant, since the sign (or vanishing) of x^+ and of x^- is also Lorentz invariant. For a real number r define

$$\mathrm{sign}(r) := \begin{cases} +1 & r > 0 \\ 0 & r = 0 \\ -1 & r < 0 \end{cases} \tag{8.41}$$

Then $(\lambda, \mathrm{sign}(x^+), \mathrm{sign}(x^-))$ is a complete invariant of the orbits. That is, given this triple of data there is a unique orbit with these properties.

It is now easy to see what the different types of orbits there are. They are shown in Figure 21: They are:

♣Actually, the lightrays and hyperbolas have trivial stabilizer and hence are in the same strata. This is a problem with using strata. ♣

1. hyperbolas in the forward/backward lightcone and the left/right of the lightcone
2. 4 disjoint lightrays.
3. the origin: $x^+ = x^- = 0$.

It is now interesting to consider the orbits of the full Lorentz group $O(1,1)$ and its relation to the massless wave equations. We can write (noncanonically),

♣Should give a full proof of this claim. ♣

$$O(1,1) = SO_0(1,1) \amalg P \cdot SO_0(1,1) \amalg T \cdot SO_0(1,1) \amalg PT \cdot SO_0(1,1) \tag{8.42}$$

with

$$P = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \tag{8.43}$$

The P and T operations map various orbits of $SO_0(1,1)$ into each other: P is a reflection in the time axis, i.e., a reflection of the spatial coordinate, while T is a reflection in the space axis, i.e. a reflection of the time coordinate. Thus the orbits of the groups $SO(1,1)$, $SO_0(1,1) \amalg PT \cdot SO_0(1,1)$, and $O(1,1)$ all differ slightly from each other.

♣Should give more details here, or form an exercise. ♣

As an example of a physical manifestation of orbits let us consider the energy-momentum dispersion relation of a particle of mass m with energy-momentum $(E,p) \in \mathbb{R}^{1,1}$.

[62] Some authors will define these with a $1/2$ or $1/\sqrt{2}$. One should exercise care with this choice of convention.

1. Massive particles: $m^2 > 0$ have (E, p) along an orbit in the upper quadrant:

$$\mathcal{O}^+(m) = \{(m\cosh\theta, m\sinh\theta)|\theta \in \mathbb{R}\} \tag{8.44}$$

2. Massless particles move at the speed of light. In 1+1 dimensions there is an interesting refinement of the massless orbits: Left-moving particles with positive energy have support on [63] $p_+ = \frac{1}{2}(E + p) = 0$ and $p_- = \frac{1}{2}(E - p) \neq 0$. Right-moving particles with positive energy have support on $p^- = 0$ and $p^+ \neq 0$. In $d + 1$ dimensions with $d > 1$ the orbits of $SO_0(1, d)$ consisting of the forward and backward lightcones (minus the origin) are connected.

3. Tachyons have $E^2 - p^2 = m^2 < 0$ and have their support on the left or right quadrant. If we try to expand a solution to the wave-equation with $e^{\mathrm{i}(k_0x^0+k_1x^1)}$ then $k_0^2 = \sqrt{k_1^2 + m^2}$ and so if the spatial momentum k_1 is sufficiently small then k_0 is pure imaginary and the wave grows exponentially, signaling and instability. This tells us our theory is out of control and some important new physical input is needed.

4. A massless "particle" of zero energy and momentum.

9. Centralizer Subgroups And Counting Conjugacy Classes

Definition 9.1: Let $g \in G$, the *centralizer subgroup* of g, (also known as the *normalizer subgroup*), denoted, $Z(g)$, is defined to be:

$$Z(g) := \{h \in G|hg = gh\} \tag{9.1}$$

Exercise *Due Diligence*
a.) Check that $Z(g) \subset G$ is a subgroup.
b.) Show that $g^n \in Z(g)$ for any integer n.
c.) If $g_1 = g_0g_2g_0^{-1}$ show that $Z(g_1) = g_0Z(g_2)g_0^{-1}$.
d.) Show that

$$Z(G) = \cap_{g\in G}Z(g) \tag{9.2}$$

Exercise *Is $Z(g)$ always an Abelian group?*
a.) Show that $Z(1) = G$. Answer the above question.
b.) Show that the centralizer of the transposition (12) in S_n for $n \leq 3$ is isomorphic to S_2.

[63] Note the factors of two, so that $x^0p_0 + x^1p_1 = x^+p_+x^-p_-$. This is an example of the tricky factors of two one encounters when working with light-cone coordinates.

c.) Show that the centralizer of the transposition (12) in S_n for $n \geq 4$ is isomorphic to $S_2 \times S_{n-2}$.

Recall that $C(g)$ denotes the conjugacy class of g. Using the Stabilizer-Orbit theorem we can establish a 1-1 correspondence between $C(g)$ and the cosets of $G/Z(g)$. As in the proof of that theorem we have a map $\psi : G/Z(g) \to C(g)$ by

$$\psi : g_i Z(g) \to g_i g g_i^{-1} \in C(g) \tag{9.3}$$

It is 1-1 and onto.

Since conjugacy is an equivalence relation G decomposes as a disjoint union of the orbits, which in this case are the conjugacy classes. When G is a finite group this decomposition leads to some useful theorems based on simple counting ideas. When $|G|$ is finite we can usefully write:

$$|G| = \sum_{conj.\ classes} |C(g)| \tag{9.4}$$

The sum is over distinct conjugacy classes. What is g in this formula? For each class we may choose any representative element from that class.

Now, if G is finite, then by the above 1-1 correspondence we may write:

$$|C(g)| = \frac{|G|}{|Z(g)|} \tag{9.5}$$

which allows us to write the above decomposition of $|G|$ in a useful form sometimes called the *class equation*:

$$|G| = \sum_{conj.\ classes} \frac{|G|}{|Z(g)|} \tag{9.6}$$

Again, we sum over a complete set of distinct non-conjugate elements g. Which g we choose from each conjugacy class does not matter since if $g_1 = hg_2h^{-1}$ then $Z(g_1) = hZ(g_2)h^{-1}$ are conjugate groups, and hence have the same order. So, for each distinct conjugacy class we just choose any element we like.

Remarks:

1. Gauge theories can be formulated for discrete groups just as well as for compact Lie groups. [64] In the finite group case physical answers typically come out in terms of sums over conjugacy classes. The simplest example is "Yang-Mills theory" in $0 + 1$ dimensions where the gauge group is a finite group G. The partition function on the circle is

$$Z(S^1) = \frac{1}{|G|} \sum_{g \in G} 1 \tag{9.7}$$

♣If you don't understand this remark. Don't panic! We will not use it later. ♣

[64] See section 17 below for a discussion of gauge theory that uses minimal prerequisites and is suffcient to understand this remark.

Here we are summing over bundles with connection and dividing by the volume of the group of gauge transformations. The Yang-Mills action in this case is rather trivially zero. Of course, the answer is $Z(S^1) = 1$. As in any field theory, the partition function on $X \times S^1$ is a trace over the Hilbert space on X. In this case, X is a point, and $Z(S^1) = 1$ tells us the Hilbert space is one dimensional. Indeed we expect to find only one state in this rather trivial theory! The relation to the present section is the following: We can organize the sum into conjugacy classes:

$$Z(S^1) = \frac{1}{|G|}\sum_{cc} |C(g)| = \sum_{cc} \frac{1}{|Z(g)|} \tag{9.8}$$

In the last sum can be viewed as a sum over isomorphism classes of bundles weighted by the one over the order of the automorphism group of the bundle.

Three applications of the Counting Principle:

Application 1:

Theorem: If $|G| = p^n$ then the center has nontrivial elements, i.e., $Z(G) \neq \{1\}$.

Proof: Observe that an element g is central *if and only if* $C(g) = \{g\}$ has order 1. Now let us use the class equation. We can usefully split up the sum over conjugacy classes as a sum over the center and the rest:

$$|G| = |Z(G)| + \sum_{classes}{}' \frac{|G|}{|Z(a)|} \tag{9.9}$$

where the sum with a prime is over over conjugacy classes with more than one element. For these classes $|Z(a)| < |G|$. But by Lagrange's theorem $|Z(a)| = p^{n-n_a}$ for some $n_a < n$. Therefore, the second term on the RHS of (9.9) is divisible by p and hence $p||Z(G)|$. ♠

Application 2: *Cauchy's theorem*:

In a similar style, we can prove the very useful:

Theorem: If p divides $|G|$ then there is an element $g \in G$, $g \neq 1$ with order p.

Proof 1: This is a nice application of the stabilizer-orbit theorem. Consider the set

$$X = \{(g_1, \dots, g_p) | \prod_i g_i = 1\} \subset G^p \tag{9.10}$$

Note that the cyclic group $\mathbb{Z}_p$ acts on this set with the standard generator acting by

$$\omega \cdot (g_1, \dots, g_p) = (g_p, g_1, g_2, \dots, g_{p-1}) \tag{9.11}$$

A fixed point of the $\mathbb{Z}_p$-action corresponds to an element of the form $(g, \dots, g)$ such that $g^p = 1$. If $g \neq 1$ then this corresponds to an element of order p. Now, by the stabilizer-orbit theorem, the orbits of any $\mathbb{Z}_p$ action (on any set) have cardinality either 1 or p. Let N_1 be the number of orbits of length one other than the element $(1, \dots, 1)$. (As just explained, these are in 1-1 correspondence with the elements of order p.) Let N_p be the number of orbits of length p. Then, by the counting principle we have:

$$|G| = (1 + N_1) + pN_p \tag{9.12}$$

So, if p divides $|G|$ then $N_1 = (p-1)\text{mod}p$ and in particular must be positive. ♠

Proof 2: We can also prove Cauchy's theorem using induction on the order of G, dividing the proof into two cases: First we consider the case where G is Abelian and then the case where it is nonabelian.

Case 1: G is Abelian:

If $|G| = p$ then G is cyclic and the statement is obvious: Any generator has order p. More generally, note that if G is a cyclic group $\mathbb{Z}/N\mathbb{Z}$ with $N > p$ and p divides N then $\overline{N/p} \in \mathbb{Z}/N\mathbb{Z}$ has order p. This establishes the result for cyclic groups.

Now suppose our Abelian group has order $|G| > p$. Choose an element $g_0 \neq 1$ and suppose that g_0 does not have order p. Let $H = \langle g_0 \rangle$. If $H = G$ then G would be cyclic but then as we just saw, it would have an element of order p. So now assume H is a proper subgroup of G. If p divides $|H|$ then H (and hence G) has an element of order p by the inductive hypothesis. If p does not divide $|H|$ then we consider the group G/H. But this has order strictly less than $|G|$ and p divides the order of G/H. So there is an element aH of order p meaning $a^p = g_0^x$ for some x. If $g_0^x = 1$ we are done. If not then there is some smallest positive integer y so that $g_0^{xy} = 1$ but then a^y has order p. We have now proved Cauchy's theorem for abelian groups.

Case 2: G is non-Abelian: By the class equation we can write

$$|G| = |Z(G)| + {\sum}' \frac{|G|}{|Z(g_i)|} \tag{9.13}$$

If p divides the order of the centralizer $Z(G)$ then we can apply our previous result about Cauchy's theorem for Abelian groups. If p does not divide $Z(G)$ then there must be some g_i so that p does not divide $\frac{|G|}{|Z(g_i)|}$ but this means p divides $|Z(g_i)|$, but now by the inductive hypothesis $Z(g_i)$, and hence G has an element of order p. This completes the proof. ♠

Application 3: *Sylow's theorem*:

Finally, as a third application we give a simple proof of Sylow's first theorem: If p is prime and $|G| = p^k m$ where p does not divide m then G has a subgroup of order p^k.

Proof 1: The first proof is again an application of the stabilizer-orbit theorem. [65] Suppose $|G| = p^{k+r}u$ with $gcd(u,p) = 1$ and $r \geq 0$ and $k > 0$. We will show that G has a subgroup

[65] We are following the nice article on Wikipedia here.

of order p^k. Let Ω be the set of all subsets (not subgroups!) of G of cardinality p^k. The cardinality of Ω is clearly:

$$|\Omega| = \binom{p^{k+r}u}{p^k} = p^r u \prod_{j=1}^{p^k-1} \frac{p^{k+r}u/j - 1}{p^k/j - 1} \tag{9.14}$$

In the product we have a ratio of rational numbers which do not have p as a factor so p^r divides Ω and that is the maximal power which does so.

Now note that G acts on Ω via:

$$\phi_g : \omega \mapsto g \cdot \omega := \{gh | h \in \omega\} \tag{9.15}$$

where we are denoting an element of Ω by ω. Consider the stabilizer subgroup G^ω of any $\omega \in \Omega$. Note that if $\alpha \in \omega$ then every element $g \cdot \alpha \in \omega$ for $g \in G^\omega$. (Why? Because $g \cdot \omega = \omega$ if $g \in G^\omega$.) But this means that $G^\omega \cdot \alpha$ is a subset of ω and hence

$$|G^\omega| = |G^\omega \cdot \alpha| \leq |\omega| = p^k \tag{9.16}$$

We now aim to show that some stabilizer group G^ω has order exactly p^k. This will be our subgroup predicted by Sylow's theorem. Suppose, on the contrary that no stabilizer group has order p^k. Then every stabilizer group satisfies $|G^\omega| < p^k$, and therefore it is divisible at most by p^{k-1}. Now, by the stabilizer-orbit theorem

$$|G| = |G^\omega| \cdot |\mathcal{O}_\omega| \tag{9.17}$$

where Ω_ω is the G-orbit through ω. Now p^{k+r} divides $|G$ and if G^ω is divisible by at most p^{k-1} then p^s divides $|\Omega_\omega$ for $s > r$. But now

$$|\Omega| = \sum_{\text{distinct orbits}} |\Omega_\omega| \tag{9.18}$$

If all the orbits on the RHS were divisible by p^s with $s > r$ then $|\Omega|$ would be divisible by p^s with $s > r$. But this is not true. Therefore, some orbit is divisible by p^r and no higher power. Therefore some $|G^\omega|$ is divisible by p^k, therefore $|G^\omega| = p^k$. ♠

Proof 2: The more conventional proof is similar to that of Cauchy's theorem. We work by induction on $|G|$, and divide the proof into two cases:

Case 1: p divides the order of $Z(G)$.: By Cauchy's theorem $Z(G)$ has an element of order p and hence a subgroup $N \subset Z(G)$ of order p. N is clearly a normal subgroup of G (being a subgroup of the center of G) so G/N is a group. It is clearly of order $p^{k-1}m$. So, by the inductive hypothesis there is a subgroup $\bar{H} \subset G/N$ of order p^{k-1}. Now let $H = \{g \in G | gN \in \bar{H}\}$. It is not hard to show that H is a a subgroup of G containing N and in fact $H/N = \bar{H}$. Therefore $|H| = p^k$, so H is a p-Sylow subgroup of G.

Case 2: p does not divide the order of $Z(G)$.: In this case, by the class equation p must not divide $|C(g)| = |G|/|Z(g)|$ for some nontrivial conjugacy class $C(g)$. But that means that for such an element g we must have that p^k divides $|Z(g)| < |G|$. So $Z(g)$ has a p-Sylow subgroup which can serve as a p-Sylow subgroup of G. ♠

♣Again, there is a nice proof using the orbit-stabilizer theorem. See Wikipedia article. Give this in the section on Orbit-Stabilizer below? ♣

Exercise
Show that if the centralizer $Z(G)$ is such that $G/Z(G)$ is cyclic then G is Abelian.

Exercise
If p^k divides $|G|$ with $k > 1$ does it follow that there is an element of order p^k? [66]

Exercise *Groups Whose Order Is A Square Of A Prime Number*
If $|G| = p^2$ where p is a prime then show that
1. G is abelian
2. $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.

Exercise
Write out the class equation for the groups S_4 and S_5.

Exercise
Find the centralizer $Z(g) \subset S_n$ of $g = (12 \dots n)$ in S_n.

Exercise
Prove that if $|G| = 15$ then $G = \mathbb{Z}/15\mathbb{Z}$.

[66] *Answer*: NO! $\mathbb{Z}_p^k$ is a counterexample: It has order p^k and every element has order p.

Exercise *Groups whose order is a product of two primes*

Suppose that G has order pq where p and q are distinct primes. We assume WLOG that $p < q$. We now also assume that and p does not divide $q - 1$.

a.) Show that G is isomorphic to $\mathbb{Z}_{pq}$.

Warning!! This is hard. [67]

b.) Why is it important to say that p does not divide $q - 1$? [68]

c.) Show that this result implies that if a nonabelian group has odd order then the order must be ≥ 21. (And in fact, there does exist a nonabelian group of order 21.)

10. Kernel, Image, And Exact Sequence

Given an arbitrary homomorphism

$$\mu : G \to G' \tag{10.1}$$

there is automatically a "God-given" subgroup of both G and G':

Definition 10.1:

a.) The *kernel* of μ is

$$K = \mathrm{ker}\mu := \{g \in G | \mu(g) = 1_{G'}\} \tag{10.2}$$

[67] *Answer*. By Cauchy's theorem we know there is an element a of order p and an element b of order q. We can easily reduce to the case the center of G is trivial. In general the subgroup $Z(G)$ must have order pq, p, q, or 1. If $Z(G)$ has order pq then a and b commute and $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. If $|Z(G)|$ has order p or q then $G/Z(G)$ must be cyclic of order q or p, respectively. Hence by an easy exercise above G is cyclic. This leaves us with the hard case where $Z(G) = \{1\}$ is the trivial subgroup. Let us consider the conjugacy classes of the powers of a, $C(a)$, $C(a^2)$,.... Since $Z(a)$ has order at least p and its order must divide pq and it can't be the whole group (since $Z(G) = \{1\}$) it must be that $Z(a) = \{1, a, \dots, a^{p-1}\}$ and hence $C(a)$ has order q. Indeed, for <u>any</u> element $g \in G$ that is not the identity it must be that $Z(g)$ has order p or q and $C(g)$ has order q or p. Now note that $Z(a) \supset Z(a^2) \supset \cdots$. So, as long as a^x is not one, it must be that $Z(a^x) = Z(a)$ and $C(a^x)$ has order q. Now we claim that the different conjugacy classes $C(a)$, $C(a^2)$,..., $C(a^{p-1})$ are all <u>distinct</u>. The statement that these are distinct can be reduced to the statement that it is not possible to have $bab^{-1} = a^x$ for any x, so now we verify this latter statement. If it were the case that $bab^{-1} = x$ then since the general element of the conjugacy class is $b^j ab^{-j}$ the conjugacy class would have to be $\{a, a^x, a^{2x}, \dots, a^{(q-1)x}\}$. But that set must be the set $C(a) = \{a, a^2, \cdots, a^{p-1}\}$ of p elements. Since $q > p$ it must be that $b^{j_1} ab^{-j_1} = b^{j_2} ab^{-j_2}$ where $1 \leq j_1, j_2 \leq (q-1)$ and $j_1 \neq j_2$. So we have to have $b^j ab^{-j} = a$ for some $1 \leq j \leq (q-1)$. But then $b^j \neq 1$. But then such an element b^j would be in $Z(a)$. This is impossible. So we can never have $bab^{-1} = a^x$ and hence $C(a)$, $C(a^2)$,..., $C(a^{p-1})$ are all <u>distinct</u>. Now the class equation says that

$$pq = 1 + (p-1)q + X$$

where X accounts for all the other conjugacy classes. As we have remarked these must have order p or q and hence $X = rp + sq$ for nonnegative integers r, s. But now

$$q - 1 = rp + sq$$

But this is impossible: If $s \geq 1$ the RHS is too large. So $s = 0$ but then p would have to divide $q - 1$.

[68] *Answer*: Consider $p = 2$ and $q = 3$ and note that S_3 is not isomorphic to $\mathbb{Z}_6$.

b.) The *image* of μ is

$$\mathrm{im}\mu := \mu(G) \subset G' \tag{10.3}$$

Exercise *Due Diligence*
b.) Check that $\mu(G) \subseteq G'$ is indeed a subgroup.
a.) Check that $\ker(\mu) \subset G$ is indeed a subgroup. [69]

In mathematics one often encounters the notation of an *exact sequence*: Suppose we have three groups and two homomorphisms f_1, f_2

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \tag{10.4}$$

$$\boxed{\text{We say the sequence is } \textit{exact at } G_2 \text{ if } \mathrm{im} f_1 = \ker f_2.}$$

This generalizes to sequences of several groups and homomorphisms

$$\cdots G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots \tag{10.5}$$

The sequence can be as long as you like. It is said to be *exact at* G_i if $\mathrm{im}(f_{i-1}) = \ker(f_i)$.

A *short exact sequence* is a sequence of the form

$$1 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow 1 \tag{10.6}$$

which is exact at G_1, G_2, and G_3. Here 1 refers to the trivial group with one element. There is then a unique homomorphism $1 \to G_1$ and $G_3 \to 1$ so we don't need to specify it. Thus, the meaning of saying that (10.6) is a short exact sequence is that

1. Exactness at G_1: The kernel of f_1 is the image of the inclusion $\{1\} \hookrightarrow G_1$, and hence is the trivial group. Therefore f_1 an injection of G_1 into G_2.

2. Exactness at G_2: $\mathrm{im} f_1 = \ker f_2$.

3. Exactness at G_3: $G_3 \to 1$ is the homomorphism which takes every element of G_3 to the identity element in the trivial group. The kernel of this homomorphism is therefore all of G_3. Exactness at G_3 means that this kernel is the image of the homomorphism f_2, and hence f_2 is a surjective homomorphism.

In particular, note that if $\mu : G \to G'$ is any group homomorphism then we automatically have a short exact sequence:

$$1 \to K \to G \overset{\mu}{\to} \mathrm{im}(\mu) \to 1 \tag{10.7}$$

[69] *Answer*: If $k_1, k_2 \in K$ then $\mu(k_1 k_2) = \mu(k_1)\mu(k_2) = 1_{G'}$. So K is closed under multiplication. The group properties of K now follow.

where K is the kernel of μ.

When we have a short exact sequence of groups there is an important relation between them, as we now explain.

Theorem 10.1: Let $K \subseteq G$ be the kernel of a homomorphism (10.1). Then K is a normal subgroup of G.

Proof: $\mu(gkg^{-1}) = \mu(g)\mu(k)\mu(g^{-1}) = \mu(g)1_{G'}\mu(g)^{-1} = 1_{G'} \Rightarrow K$ is normal. ♠

Exercise *Is the image of a homomorphism a normal subgroup?*
If $\mu : G \to G'$ is a group homomorphism is $\mu(G)$ a normal subgroup of G'?
Answer the question with a proof or a counterexample. [70]

It follows by Theorem 7.2.1, that G/K has a group structure. Note that $\mu(G)$ is also naturally a group.

These two groups are closely related because

$$\mu(g) = \mu(g') \qquad \leftrightarrow \qquad gK = g'K \tag{10.8}$$

Thus we have

Theorem 10.2:

$$\boxed{\mu(G) \cong G/K} \tag{10.9}$$

Proof: We associate the coset gK to the element $\mu(g)$ in G'.

$$\psi : gK \mapsto \mu(g) \tag{10.10}$$

Claim: ψ is an isomorphism. You have to show three things:

1. ψ is a well defined map:

$$gK = g'K \Rightarrow \exists k \in K, g' = gk \Rightarrow \mu(g') = \mu(gk) = \mu(g)\mu(k) = \mu(g) \tag{10.11}$$

2. ψ is in fact a homomorphism of groups

$$\psi(g_1K \cdot g_2K) = \psi(g_1K) \cdot \psi(g_2K) \tag{10.12}$$

where on the LHS we have the product in the group G/K and on the RHS we have the product in G'. We leave this as an exercise for the reader.

[70] *Answer*: Definitely not! Any subgroup $H \subset G$ is the image of the inclusion homomorphism. In general, subgroups are not normal subgroups.

3. ψ is one-one, i.e. ψ is onto and invertible. The surjectivity should be clear. To prove injectivity note that:

$$\mu(g') = \mu(g) \Rightarrow \exists k \in K, g' = gk \Rightarrow g'K = gK \qquad \spadesuit \tag{10.13}$$

Remarks:

1. If we have a short exact sequence

$$1 \to N \to G \to Q \to 1 \tag{10.14}$$

then it automatically follows that N is isomorphic to a normal subgroup of G (it is the kernel of a homomorphism $G \to Q$) and moreover Q is isomorphic to G/N. For this reason we call Q the *quotient group*. A frequently used terminology is that *"G is an extension of Q by N."* Some authors [71] will use the terminology that "G is an extension of N by Q." So it is best simply to speak of a group extension with kernel N and quotient Q.

2. **VERY IMPORTANT**: In quantum mechanics physical states are actually represented by "rays" in Hilbert space, or better, by one-dimensional subspaces of Hilbert space, or, even better, by orthogonal projection operators of rank one. (This is for "pure states." More generally, "states" are described mathematically by density matrices.) When comparing symmetries of quantum systems with their classical counterparts, group extensions play an important role so we will discuss them rather thoroughly in §14 below. For the moment we quote three important examples:

Example 1: Consider the group of fourth roots of unity, $Res(4)$ and the homomorphism $\pi : Res(4) \to Res(2)$ given by $\pi(g) = g^2$. The kernel is $\{\pm 1\} = Res(2)$ and so we have:

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{10.15}$$

As an exercise the reader should also describe this extension thinking of $\mathbb{Z}_4$ additively as $\mathbb{Z}/4\mathbb{Z}$, and generalize it to

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 1 \tag{10.16}$$

where p is prime.

Example 2: Consider the homomorphism

$$r_N : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \tag{10.17}$$

given by reduction modulo N. (Or, if you prefer to think multiplicatively, $r_N(n) = \omega^n$ where ω is a primitive N^{th} root of 1.) The kernel is $K = N\mathbb{Z} \subset \mathbb{Z}$. As a group this kernel is isomorphic to $\mathbb{Z}$ and so we have

$$0 \to \mathbb{Z} \overset{\iota_N}{\to} \mathbb{Z} \overset{r_N}{\to} \mathbb{Z}/N\mathbb{Z} \to 0 \tag{10.18}$$

[71] notably, S. MacLane, one of the inventors of group cohomology,

where $\iota_N(x) = Nx$.

Example 3: *Finite Heisenberg Groups*: Let P, Q be $N \times N$ "clock" and "shift" matrices. To define these introduce an N^{th} root of unity, say $\omega = \exp[2\pi i/N]$. Then

$$P_{i,j} = \delta_{i=j+1 \mathrm{mod} N} \tag{10.19}$$

$$Q_{i,j} = \delta_{i,j}\omega^j \tag{10.20}$$

Note that $P^N = Q^N = 1$ and no smaller power is equal to 1. Further note that [72]

$$QP = \omega PQ \tag{10.21}$$

For $N = 4$ the matrices look like

$$P = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad Q = \begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 \\ 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{10.22}$$

with $\omega = e^{2\pi i/4}$. The group of matrices generated by P, Q and $\omega \mathbf{1}_{N\times N}$ is a finite subgroup of $GL(N, \mathbb{C})$ isomorphic to a *finite Heisenberg group*, denoted Heis_N. It is an extension

$$1 \to \mathbb{Z}_N \to \mathrm{Heis}_N \xrightarrow{\pi} \mathbb{Z}_N \times \mathbb{Z}_N \to 1 \tag{10.23}$$

and has many pretty applications to physics and we will return to this group several times below. See, for example section 10.2 below for a physical interpretation.

Exercise
Give a formula for π in the exact sequence (10.23).

Exercise A_n
Use Theorem 7.1 to show that A_n is a normal subgroup of S_n.

Exercise *Induced maps on quotient groups*
We will use the following result in §11.3: Suppose $\mu : G_1 \to G_2$ is a homomorphism and $H_2 \subset G_2$ is a subgroup.

[72] The fastest way to check that - and thereby to check that you have your conventions under control - is to compute QPQ^{-1} because $(Q^{-1}PQ)_{ij} = Q_{ii}P_{ij}(Q_{jj})^{-1} = \omega P_{ij}$.

a.) Show that $\mu^{-1}(H_2) \subset G_1$ is a subgroup.

b.) If $H_1 \subset \mu^{-1}(H_2)$ is a subgroup show that there is an induced map $\bar{\mu} : G_1/H_1 \to G_2/H_2$.

c.) Show that if H_1 and H_2 are normal subgroups then $\bar{\mu}$ is a homomorphism.

d.) In this case there is an exact sequence

$$1 \to \mu^{-1}(H_2)/H_1 \to G_1/H_1 \to G_2/H_2 \tag{10.24}$$

Exercise

Let A, B be abelian groups and $A_1 \subset A$ and $B_1 \subset B$ subgroups, and suppose $\phi : A \to B$ is a homomorphism such that ϕ takes A_1 into B_1.

a.) Show that ϕ induces a homomorphism

$$\bar{\phi} : A/A_1 \to B/B_1 \tag{10.25}$$

b.) Show that if $\phi : A_1 \to B_1$ is *surjective* then

$$\ker\{\bar{\phi} : A/A_1 \to B/B_1\} \cong \frac{\ker\{\phi : A \to B\}}{\ker\{\phi : A_1 \to B_1\}} \tag{10.26}$$

Exercise

Let n be a natural number and let

$$\psi : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^d \tag{10.27}$$

be given by the diagonal map $\psi(\omega) = (\omega, \cdots, \omega)$.

Find a set of generators and relations for $G/\psi(H)$.

Exercise

Let $G = \mathbb{Z} \times \mathbb{Z}_4$. Let K be the subgroup generated by $(2, \omega^2)$ where we are writing $\mathbb{Z}_4$ as the multiplicative group of 4^{th} roots of 1. Note $(2, \omega^2)$ is of infinite order so that $K \cong \mathbb{Z}$. Show that $G/K \cong \mathbb{Z}_8$.

Exercise *The Finite Heisenberg Groups*

a.) Using the matrices of (10.19) and (10.20) show that the word

$$P^{n_1}Q^{m_1}P^{n_2}Q^{m_2}\cdots P^{n_k}Q^{m_k} \tag{10.28}$$

where $n_i, m_i \in \mathbb{Z}$ can be written as $\xi P^x Q^y$ where $x, y \in \mathbb{Z}$ and ξ is an N^{th} root of unity. Express x, y, ξ in terms of n_i, m_i.

b.) Show that $P^N = Q^N = 1$.

c.) Find a presentation of Heis_N in terms of generators and relations.

d.) What is the order of Heis_N ?

Exercise

Let $\mathcal{B}_n$ be a braid group. Compute the kernel of the natural homomorphism $\phi : \mathcal{B}_n \to S_n$ and show that there is an exact sequence

$$1 \to \mathbb{Z}^{n-1} \to \mathcal{B}_n \to S_n \to 1 \tag{10.29}$$

Exercise *Centrally symmetric shuffles*

Let us consider again the permutation group of the set $\{0, 1, \dots, 2n-1\}$. Recall we let $W(B_n)$ denote the subgroup of S_{2n} of centrally symmetric permutations which permutes the pairs $x + \bar{x} = 2n - 1$ amongst themselves.

Show that there is an exact sequence

$$1 \to \mathbb{Z}_2^n \to W(B_n) \to S_n \to 1 \tag{10.30}$$

and therefore $|W(B_n)| = 2^n n!$.

Exercise *Weyl Group Of $SU(N)$*

Every element of $SU(N)$ can be conjugated into the set T Of diagonal matrices.

a.) Show that the normalizer $N(T)$ of T within $SU(N)$ is larger than T by considering permutation matrices $\mathrm{i}(e_{ij} + e_{ji})$.

b.) Show that these act by permuting the ii and jj diagonal elements .

c.) Show that there is a homomorphism $N(T) \to S_N$.

d.) In fact, there is an exact sequence

$$1 \to T \to N(T) \to S_N \to 1 \tag{10.31}$$

10.1 The Relation Of $SU(2)$ And $SO(3)$

There is a standard homomorphism

$$\pi : SU(2) \to SO(3) \quad . \tag{10.32}$$

To define it we note that for any $u \in SU(2)$ there is a unique $R \in SO(3)$ such that, for all $\vec{x} \in \mathbb{R}^3$ we have:

$$u\vec{x} \cdot \vec{\sigma} u^{-1} = (R\vec{x}) \cdot \vec{\sigma} \tag{10.33}$$

where $R \in SO(3)$.

To prove (10.33) we begin by noting that, since $u^{-1} = u^{\dagger}$ and $\vec{x}$ is real, the 2×2 matrix $u\vec{x} \cdot \vec{\sigma} u^{-1}$ is hermitian, and traceless, and hence has to be of the form $\vec{y} \cdot \vec{\sigma}$, where $\vec{y} \in \mathbb{R}^3$. Moreover, $\vec{y}$ depends linearly on $\vec{x}$. So the transformation $\vec{x} \mapsto \vec{y}$ defined by $u\vec{x} \cdot \vec{\sigma} u^{-1} = \vec{y} \cdot \vec{\sigma}$ is a linear transformation of $\mathbb{R}^3$. In fact it is a norm-preserving transformation. One way to prove this is to note that (see exercise below)

$$(\vec{x} \cdot \vec{\sigma})^2 = \vec{x}^2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{10.34}$$

or, alternatively (see exercise below)

$$\mathrm{det}\vec{x} \cdot \vec{\sigma} = -\vec{x}^2 \tag{10.35}$$

From either formula we conclude that (see exercise below) $\vec{x}^2 = \vec{y}^2$. We therefore conclude that $\vec{y} = R\vec{x}$ with $R \in O(3)$.

We define $\pi(u) = R$ by using this equation. To be totally explicit

$$u\sigma^i u^{-1} = R_{ji}\sigma^j \quad . \tag{10.36}$$

It should be clear from the definition that $\pi(u_1 u_2) = \pi(u_1)\pi(u_2)$, that is that π is a homomorphism of groups. Now to show that actually $R \in SO(3) \subset O(3)$ note that

$$\begin{aligned} 2\mathrm{i} &= \mathrm{tr}\, \left(\sigma^1 \sigma^2 \sigma^3\right) \\ &= \mathrm{tr}\, \left(u\sigma^1 u^{-1} u\sigma^2 u^{-1} u\sigma^3 u^{-1}\right) \\ &= R_{j_1,1} R_{j_2,2} R_{j_3,3} \mathrm{tr}\, \left(\sigma^{j_1}\sigma^{j_2}\sigma^{j_3}\right) \\ &= 2\mathrm{i}\epsilon^{j_1 j_2 j_3} R_{j_1,1} R_{j_2,2} R_{j_3,3} \\ &= 2\mathrm{i}\mathrm{det}R \end{aligned} \tag{10.37}$$

and hence $\mathrm{det}R = 1$. Alternatively, if you know about Lie groups, you can use the fact that π is continuous, and $SU(2)$ is a connected manifold.

We will now prove that:

1. $\ker(\pi) = \{\pm \mathbf{1}_{2\times 2}\} = Z(SU(2))$.

2. Every proper rotation R comes from some $u \in SU(2)$:

Thus we have the extremely important extension:

$$1 \to \mathbb{Z}_2 \overset{\iota}{\to} SU(2) \overset{\pi}{\to} SO(3) \to 1 \tag{10.38}$$

Thus, $SU(2)$ is a two-fold cover of $SO(3)$ and in fact

$$SO(3,\mathbb{R}) \cong SU(2)/\mathbb{Z}_2 \tag{10.39}$$

where the $\mathbb{Z}_2$ we quotient by is the center $\{\pm \mathbf{1}_{2\times 2}\}$. This is arguably the most important exact sequence in physics.

To prove the above two claims we will need to get to know $SU(2)$ a bit better.

First we claim that, as a manifold, $SU(2)$ can be identified with the unit three-dimensional sphere. One way to see this is to consider the unit sphere in $\mathbb{R}^4$ as the space of unit vectors in a two-dimensional complex Hilbert space (the space of states of "one Qbit"):

$$S^3 \cong \{\vec{z} | \vec{z}^\dagger \vec{z} = 1\} \subset \mathbb{C}^2 \tag{10.40}$$

This is easily seen by writing

$$\vec{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \tag{10.41}$$

and decomposing z_1, z_2 into their real and imaginary parts. Next, we note that $SU(2)$ has a transitive action on the unit sphere:

$$\phi_u : \vec{z} \mapsto u\vec{z} \tag{10.42}$$

The action is transitive because, given any unit vector we can find another orthogonal unit vector. But any two ON bases are related by some unitary transformation. By changing the phase of the second vector we can arrange that they are related by a special unitary transformation.

Therefore, we should invoke the stabilizer-orbit theorem and compute the stabilizer of, say

$$\vec{z}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad . \tag{10.43}$$

These are the upper triangular $SU(2)$ matrices with one on the diagonal: The stabilizer is trivial. So

$$SU(2) \cong S^3 \tag{10.44}$$

In particular, a general $SU(2)$ element must have the form

$$u = \begin{pmatrix} z_1 & * \\ z_2 & * \end{pmatrix} \tag{10.45}$$

with $|z_1|^2 + |z_2|^2 = 1$. Now imposing the condition

$$u^{-1} = u^\dagger \tag{10.46}$$

we solve for the other two matrix elements and conclude that every $SU(2)$ element is of the form

$$u = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \tag{10.47}$$

where

$$|\alpha|^2 + |\beta|^2 = 1 \tag{10.48}$$

This makes the identification of the group as a manifold quite clear.

There are many ways to parametrize S^3. One is to introduce a polar angle and stratify S^3 by two-dimensional spheres. Viewed this way, we can write the general $SU(2)$ element as

$$u = \cos\chi + \mathrm{i}\sin\chi \vec{n} \cdot \vec{\sigma} \tag{10.49}$$

where $0 \le \chi \le \pi$ and $\vec{n} \in S^2$. From this form it is easy to check that u only with all the σ^i if $\sin\chi = 0$ so $\cos\chi = \pm 1$. From this we conclude

$$\ker(\pi) = \{\pm \mathbf{1}_{2\times 2}\} = Z(SU(2)) \tag{10.50}$$

Now let us study the restriction of the homomorphism π to some special $U(1)$ subgroups of $SU(2)$. First consider the subgroup of diagonal matrices D of the form:

$$\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \tag{10.51}$$

with $|\xi| = 1$. These act by

$$\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \begin{pmatrix} x_3 & x_1 - \mathrm{i}x_2 \\ x_1 + \mathrm{i}x_2 & -x_3 \end{pmatrix} \begin{pmatrix} \xi^{-1} & 0 \\ 0 & \xi \end{pmatrix} = \begin{pmatrix} x_3 & \xi^2(x_1 - \mathrm{i}x_2) \\ \xi^{-2}(x_1 + \mathrm{i}x_2) & -x_3 \end{pmatrix} \tag{10.52}$$

If we write

$$\xi = e^{-\mathrm{i}\phi/2} \tag{10.53}$$

for some angle ϕ then π maps the diagonal matrix to $R \in SO(3)$ that is a rotation around the x^3 axis. It is a counterclockwise rotation by ϕ in the $x^1 - x^2$ plane with the orientation $dx^1 \wedge dx^2$.

Another obvious subgroup of $SU(2)$ is $SO(2)$, the real unitary matrices. We parametrize the group by

$$R(\theta/2) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix} e^{-\mathrm{i}\frac{\theta}{2}\sigma^2} \tag{10.54}$$

Of course, the eigenvalues are $e^{\pm \mathrm{i}\theta/2}$ and indeed

$$SR(\theta/2)S^{-1} = e^{-\mathrm{i}\frac{\theta}{2}\sigma^3} \tag{10.55}$$

where

$$S = \frac{1}{\sqrt{2}}(1 - \mathrm{i}\sigma^1) \in SU(2) \tag{10.56}$$

(all you have to check is $S\sigma^2 S^{-1} = \sigma^3$.) We find that

$$\pi(R(\theta/2)) = \begin{pmatrix} \cos(\theta/2) & 0 & \sin(\theta/2) \\ 0 & 1 & 0 \\ -\sin(\theta/2) & 0 & \cos(\theta/2) \end{pmatrix} \tag{10.57}$$

is rotation by θ around the x^2 axis. By the Euler angle parametrization we therefore learn that π is onto. In fact, we can parametrize all $SU(2)$ elements by

$$u = e^{\phi T^3} e^{\theta T^2} e^{\psi T^3} \tag{10.58}$$

where

$$T^i = -\frac{\mathrm{i}}{2}\sigma^i \qquad 1 \le i \le 3 \tag{10.59}$$

The range of Euler angles that covers $SO(3)$ once is $0 \le \theta \le \pi$ with ϕ and ψ identified modulo 2π. Because $SU(2)$ is a double cover we should extend the range of ϕ or ψ by a factor of 2 if we want to cover the group $SU(2)$ once. For example, taking:

$$\begin{aligned} &0 \le \theta \le \pi \\ &\phi \sim \phi + 2\pi \\ &\psi \sim \psi + 4\pi \end{aligned} \tag{10.60}$$

Then for <u>generic</u> $SU(2)$ elements we will have a unique representation

$$u = e^{\phi T^3} e^{\theta T^2} e^{\psi T^3} = \exp[-\frac{\mathrm{i}}{2}\phi\sigma^3]\exp[-\frac{\mathrm{i}}{2}\theta\sigma^2]\exp[-\frac{\mathrm{i}}{2}\psi\sigma^3] = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \alpha \end{pmatrix} \tag{10.61}$$

with

$$\alpha = e^{\mathrm{i}\frac{1}{2}(\phi+\psi)}\cos(\theta/2) \qquad \beta = -e^{\mathrm{i}\frac{1}{2}(\phi-\psi)}\sin(\theta/2) \tag{10.62}$$

The Euler angle coordinates on $SU(2)$ break down at $\theta = 0, \pi$. At $\theta = 0$ the product only depends on $(\phi + \psi)$ even though we have a three-dimensional manifold Similarly at $\theta = \pi$ the product only depends on $(\phi - \psi)$.

Remark: As we will discuss later, a good parametrization near the identity would be

$$u = \exp[\theta^k T^k] \tag{10.63}$$

where we are exponentiating the general element of the Lie algebra $\mathfrak{su}(2)$

Exercise *Simple Identities For $\vec{x} \cdot \vec{\sigma}$*
a.) Prove (10.34)
b.) Prove (10.35)
c.) Show that both these formulae imply that $\vec{x}^2 = \vec{y}^2$.

Exercise *Polar Angle Decomposition Of $SU(2)$*

a.) Prove that every element of $SU(2)$ can be written in the form of (10.49).

b.) Express α, β in terms of χ and $\hat{n}$.

c.) The coordinates $\chi, \hat{n}$ cover a product of an interval and a two-dimensional sphere. Prove that $[0,\pi] \times S^2$ is not topologically the same as $SU(2)$. Where does the $\chi, \hat{n}$ coordinate system go bad?

Exercise *A Basis For The Lie Algebra $\mathfrak{su}(2)$*

a.) Show that every traceless anti-Hermitian 2×2 matrix is a real linear combination of the three matrices T^i defined in (10.59).

b.) Show that the matrix commutators satisfy

$$[T^i, T^j] = \epsilon^{ijk} T^k \tag{10.64}$$

with the convention $\epsilon^{123} = +1$.

Exercise

Show that in the Euler angle parametrization the shift

$$\psi \to \psi + 2\pi \tag{10.65}$$

takes $u \to -u$.

10.2 The Finite Heisenberg Group And The Quantum Mechanics Of A Particle On A Discrete Approximation To A Circle

It is very illuminating to interpret the group Heis_N in terms of the quantum mechanics of a particle on a discrete approximation to a circle.

♣This sub-section assumes some knowledge of linear algebra and quantum mechanics explained in chapter 2. ♣

Recall that if G acts on a set X then it acts on the functions $\mathcal{F}[X \to Y]$ for any Y. Moreover, G always acts on itself by left-translation. Let us apply this general idea to $G = \mathbb{Z}_N$, thought of as the N^{th} roots of unity and $Y = \mathbb{C}$, the complex numbers. So we are studying complex-valued functions on the group G. We can picture the group as a discrete set of points on the unit circle so we can think, physically, of $\mathcal{F}[X \to Y]$ as the space of wavefunctions of a particle moving on a discrete approximation to a circle.

Now, as a vector space it is clear that $\mathcal{F}[\mathbb{Z}_N \to \mathbb{C}]$ is isomorphic to $\mathbb{C}^N$. To specify a function is to specify the N different complex values $\Psi(\omega^k)$ where ω is a primitive N^{th} root of one, say, $\omega = \exp[2\pi \mathrm{i}/N]$ for definiteness, and $k = 0, \dots, N-1$. (We will not try to

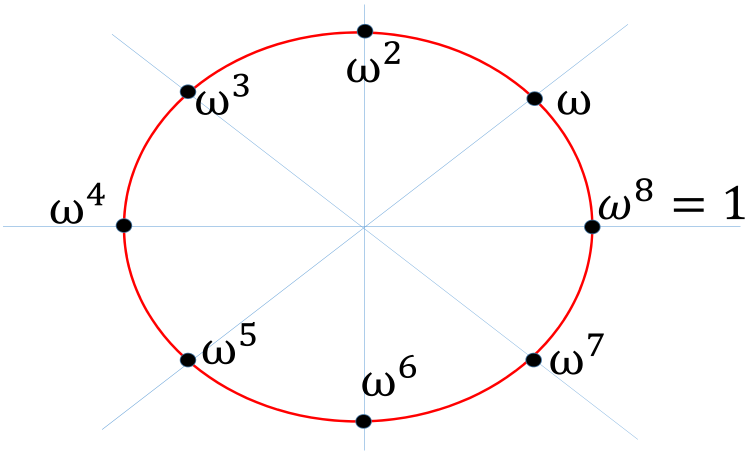

Figure 22: Roots of unity on the unit circle in the complex plane. Here $\omega = e^{2\pi \mathrm{i}/8}$ is a primitive eighth root of 1.

normalize our wavefunctions Ψ, but we could. It would make no difference to the present considerations.)

Another way to see we have an isomorphism is to choose a natural basis, the delta-function basis:

$$\delta_j(\omega^k) = \delta_{\bar{j},\bar{k}} \tag{10.66}$$

where $\bar{j}, \bar{k} \in \mathbb{Z}/N\mathbb{Z}$, viewed additively. So our isomorphism is $\delta_j \mapsto \vec{e}_j$. Put differently, every wavefunction can be uniquely expressed as

$$\Psi = \sum_{j=0}^{N-1} z_j \delta_j \tag{10.67}$$

where $z_j \in \mathbb{C}$. Indeed $z_j = \Psi(\omega^j)$.

In fact, we can make $\mathcal{H} = \mathcal{F}[\mathbb{Z}_N \to \mathbb{C}]$ into a Hilbert space in a natural way by declaring that the inner product is:

$$\langle \Psi_1, \Psi_2 \rangle := \frac{1}{|G|} \sum_{g \in G} \Psi_1^*(g) \Psi_2(g) \tag{10.68}$$

Note that with this inner product the basis δ_j, $j = 0, \dots, N-1$, to be an orthonormal basis of $\mathcal{H}$. Note that

Note that the sum on the RHS of (10.68) defines a measure on the group: If $F : G \to \mathbb{C}$ we define its integral

$$\int_G F d\mu := \frac{1}{|G|} \sum_{g \in G} F(g) \tag{10.69}$$

and we have normalized the measure so that the group has "volume 1." This is an example of an important idea called a *Haar measure* that we will discuss more later.

Now, recall the general definition from section 4.2. G acts naturally on X (which happens to be G itself) by left-multiplication. The induced action of G on the complex-valued functions on G in this case is such that the generator ω of $\mathbb{Z}_N$ acts on the space of functions via:

$$\begin{aligned}\tilde{\phi}(\omega,\Psi)(\omega^k) &:= \Psi(\phi(\omega^{-1},\omega^k))\\ &= \Psi(\omega^{k-1})\end{aligned} \tag{10.70}$$

So the generator ω of the group $\mathbb{Z}_N$ acts linearly on the functions $\mathcal{F}[\mathbb{Z}_N \to \mathbb{C}]$. We call this linear operator P. We can therefore rewrite (10.70) as

$$(P \cdot \Psi)(\omega^k) := \Psi(\omega^{k-1}) \tag{10.71}$$

Note that with respect to the inner product (10.68) P is clearly a unitary operator.

The operator P can be viewed as translation operator around the discrete circle by one step in the clockwise direction. Recall that in the quantum mechanics of a particle on the line translation by a distance a is

$$(T(a) \cdot \Psi)(x) = \Psi(x-a) \tag{10.72}$$

This equation makes sense also for a particle on the circle, that is, with x, a considered periodically. So our P is $T(a)$ for translation by $2\pi/N$ times around the circle clockwise.

Remark: In the quantum mechanics of a particle on a line or circle we could also write

$$(T(a) \cdot \Psi)(x) = \Psi(x-a) = (\exp[\mathrm{i}a\hat{p}])\Psi(x) = (\exp[-a\frac{d}{dx}] \cdot \Psi)(x) \tag{10.73}$$

so the momentum operator $\hat{p}$ generates translations. In the finite Heisenberg group there is no analog of the infinitesimal translations generated by $\hat{p}$, but only of a finite set of discrete translations.

Now let Q be the position operator:

$$(Q \cdot \Psi)(\omega^k) := \omega^k \Psi(\omega^k) \tag{10.74}$$

Q is likewise a unitary operator.

Now note that

$$\begin{aligned}(P \circ Q \cdot \Psi)(\omega^k) &= (Q \cdot \Psi)(\omega^{k-1})\\ &= \omega^{k-1}\Psi(\omega^{k-1})\end{aligned} \tag{10.75}$$

while

$$\begin{aligned}(Q \circ P \cdot \Psi)(\omega^k) &= \omega^k (P \cdot \Psi)(\omega^k)\\ &= \omega^k \Psi(\omega^{k-1})\end{aligned} \tag{10.76}$$

and therefore we conclude that we have the operator equation:

$$Q \circ P = \omega P \circ Q \tag{10.77}$$

Given a linear transformation and ordered bases for domain and range we can associate a matrix. (See Chapter two for details if you do not know this.) Now, let us choose the ordered basis $\delta_1, \dots, \delta_N$. Then we easily compute

$$P \cdot \delta_j = \delta_{j+1} \tag{10.78}$$

and therefore the matrix for P relative to the basis $\{\delta_j\}$, is the matrix with matrix elements

$$P_{i,j} = \delta_{i,j+1} \tag{10.79}$$

so, for $N = 3$ it is

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \tag{10.80}$$

Similarly, in the basis δ_j we have

$$Q_{i,j} = \omega^j \delta_{i,j} \tag{10.81}$$

and since $j = 0, 1, \dots, N-1$ we have for $N = 3$:

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \tag{10.82}$$

Thus, we have recovered the $N \times N$ clock and shift matrices we discussed above. The group of unitary operators generated by discrete position and translation operators is the finite Heisenberg group.

It is interesting to study the operators P and Q in a different basis. We can introduce a "plane wave basis" of functions $\Psi_j \in \mathcal{H}$, with $j = 0, \dots, N-1$ defined by

$$\Psi_j(\omega^k) = \omega^{jk} \tag{10.83}$$

It is now easy to compute the action of P and Q on this basis:

$$\begin{aligned} P \cdot \Psi_j &= \omega^{-j} \Psi_j \\ Q \cdot \Psi_j &= \Psi_{j+1} \end{aligned} \tag{10.84}$$

The roles of P and Q have been exchanged! P (as is P^{-1}) is now representated by "clock matrix" and Q is represented by a "shift matrix". Indeed, what we have done is perform a transformation from a position representation to a momentum representation in the language of quantum mechanics.

The basis Ψ_j represents a very general and beautiful fact: The Ψ_j are actually group homomorphisms $\Psi_j : \mathbb{Z}_N \to U(1) \subset GL(1, \mathbb{C})$ because

$$\Psi_j(\omega^{k_1} \omega^{k_2}) = \Psi_j(\omega^{k_1}) \cdot \Psi_j(\omega^{k_2}) \tag{10.85}$$

as is easily checked. The one-dimensional vector spaces spanned by the individual Ψ_j decompose the Hilbert space $L^2(\mathbb{Z}_N)$, which is an N-dimensional representation of $\mathbb{Z}_N$ into a direct sum of 1-dimensional (irreducible) representations. [73]

♣The next several paragraphs are now redundant with material in section 14.5.5 et. seq. You might want to leave this ought and bring back the example in those later sections. ♣

In general, for compact Lie groups there is a left action of G on $L^2(G)$ and, as a representation of G

$$L^2(G) \cong \oplus_j (\mathrm{dim} V_j) V_j \tag{10.86}$$

where V_j runs over the distinct irreducible representations. This is part of an important general theorem about compact Lie groups known as the *Peter-Weyl theorem*.

Moreover, the exchange of clock and shift matrices by passing from the δ_j basis to the basis of characters is again an instance of a general fact:

Let $\widehat{G}$ be the set of homomorphisms $\chi : G \to U(1)$. For an Abelian group G the set $\widehat{G}$ is also a group, using the product law:

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g)\chi_2(g) \tag{10.87}$$

The reader should be able to check that this defines a group law on $\widehat{G}$. The group $\widehat{G}$ is known as the *Pontryagin dual group*

For reasonable [74] Abelian groups we have

$$\widehat{\widehat{G}} \cong G \tag{10.88}$$

If χ is a homomorphism we can define the Fourier transform

$$\widehat{\Psi}(\chi) := \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi(g)\Psi(g) \tag{10.89}$$

giving an <u>isometry</u> of $L^2(\widehat{G})$ with $L^2(G)$. Being an isometry means that

$$\langle \widehat{\Psi}_1, \widehat{\Psi}_2 \rangle_{L^2(\widehat{G})} = \langle \Psi_1, \Psi_2 \rangle_{L^2(G)} \tag{10.90}$$

and this in turn implies that

$$\begin{aligned} \frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} \chi^*(g_1)\chi(g_2) &= \delta_{g_1,g_2} \\ \frac{1}{|G|} \sum_{g \in G} \chi_1^*(g)\chi_2(g) &= \delta_{\chi_1,\chi_2} \end{aligned} \tag{10.91}$$

These equations are special cases of the famous orthogonality relations for the matrix elements of irreducible representations of compact groups.

Now, for $G = \mathbb{Z}_N$ we have $\widehat{G} \cong \mathbb{Z}_N$. The passage from the δ_j basis to the Ψ_j basis, which diagonalizes P is just the *finite Fourier transform*.

[73] See Chapter four for a detailed discussion of the idea of reducible and irreducible representations. In brief, a representation $\rho : G \to GL(V)$ is *reducible* if there is a nonzero linear subspace $W \subset V$ which is preserved by all the operators $\rho(g)$. Note that one-dimensional representations are trivially irreducible.

[74] e.g. locally compact Abelian groups. See the book by Kirillov on representation theory.

In more concrete terms: The trace of all the powers of P less than N is also obviously zero and $P^N = 1$ and no smaller power of P is the identity. So P must be unitarily equivalent to Q. Now we can easily check that

$$SPS^{-1} = Q \tag{10.92}$$

where S is the finite Fourier transform matrix

$$S_{j,k} = \frac{1}{\sqrt{N}} e^{2\pi \mathrm{i} \frac{jk}{N}} \tag{10.93}$$

One easy way to check this is to multiply the matrices SP and QS in the δ_j basis. The reader should check that S is in fact a unitary matrix and that the matrix elements only depend on the projections $\bar{j}, \bar{k} \in \mathbb{Z}/N\mathbb{Z}$.

In any case, $S_{j,k}$ takes us from a position basis δ_j to a "momentum basis" where P is diagonal, in beautiful analogy to how the Fourier transform converts a position basis to a momentum basis for a particle on the line.

We will return to these ideas and discuss Pontryagin duality and Fourier transforms in Chapter 4 below.

Exercise *The Pontryagin Dual Of $\mathbb{Z}_N$ Is Isomorphic To $\mathbb{Z}_N$*

Let $\chi : \mathbb{Z}_N \to U(1)$ be a homomorphism. Let g be a generator of $\mathbb{Z}_N$. Show that $\chi(g)$ must be an N^{th} root of unity, and choosing any N^{th} root of unity defines the homomorphism. Conclude that $\widehat{\mathbb{Z}_N} \cong \mathbb{Z}_N$.

Exercise *Orthogonality For $\mathbb{Z}_N$*

Write out the equations (10.91) for the case $G = \mathbb{Z}_N$

---

11. Group Theory And Elementary Number Theory

In this chapter we review some very elementary number theory that has a strong connection to group theory. The facts here can be very useful in thinking about many physics problems.

Two general references are

Hardy and Wright, *An Introduction To The Theory Of Numbers*

Ireland and Rosen, *A Classical Introduction to Modern Number Theory*

11.1 Reminder On gcd And The Euclidean Algorithm

Let us recall some basic facts from grade school arithmetic:

First, if $A > B$ are two positive integers then we can write

$$A = qB + r \qquad 0 \le r < B \tag{11.1}$$

for unique nonnegative integers q and r known as the *quotient* and the *residue*, respectively.

Next, let $(A,B) = (\pm A, \pm B) = (\pm B, \pm A)$ denote the greatest common divisor of A, B. Then we can find it using the *Euclidean algorithm* by looking at successive quotients. If $A = qB$ with $r = 0$ we are done! Then $(A,B) = B$. If $r > 0$ then we proceed as follows:

$$\begin{aligned}
A &= q_1 B + r_1 \qquad & 0 < r_1 < B \\
B &= q_2 r_1 + r_2 \qquad & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 \qquad & 0 < r_3 < r_2 \\
r_2 &= q_4 r_3 + r_4 \qquad & 0 < r_4 < r_3 \\
&\vdots \quad \vdots & \\
r_{j-2} &= q_j r_{j-1} + r_j \qquad & 0 < r_j < r_{j-1} \\
r_{j-1} &= q_{j+1} r_j &
\end{aligned} \tag{11.2}$$

Note that $B > r_1 > r_2 > \cdots \geq 0$ is a strictly decreasing sequence of nonnegative integers and hence must terminate at $r_* = 0$ after a finite number of steps.

Examples

$A = 96$ and $B = 17$:

$$\begin{aligned}
96 &= 5 \cdot 17 + 11 \\
17 &= 1 \cdot 11 + 6 \\
11 &= 1 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + 1 \\
5 &= 5 \cdot 1
\end{aligned} \tag{11.3}$$

$A = 96$ and $B = 27$:

$$\begin{aligned}
96 &= 3 \cdot 27 + 15 \\
27 &= 1 \cdot 15 + 12 \\
15 &= 1 \cdot 12 + 3 \\
12 &= 4 \cdot 3
\end{aligned} \tag{11.4}$$

Note well: In (11.1) the remainder might be zero but in the first j lines of the Euclidean algorithm the remainder is positive, unless B divides A, in which case rather trivially $(A,B) = B$. The last positive remainder r_j is the gcd (A,B). Indeed if m_1, m_2 are integers then the gcd satisfies:

$$(m_1, m_2) = (m_2, m_1) = (m_2, m_1 - x m_2) \tag{11.5}$$

for any integer x. Applying this to the Euclidean algorithm above we get:

$$(A,B) = (B, r_1) = (r_1, r_2) = \cdots = (r_{j-1}, r_j) = (r_j, 0) = r_j. \tag{11.6}$$

A corollary of this algorithm is that if $g = (A, B)$ is the greatest common divisor then there exist integers (x, y) so that

$$Ax + By = g \tag{11.7}$$

In particular, two integers m_1, m_2 are *relatively prime*, that is, have no common integral divisors other than ±1, if and only if there exist integers x, y such that

$$m_1 x + m_2 y = 1. \tag{11.8}$$

Of course x, y are not unique. Equation (11.8) is sometimes known as "Bezout's theorem." We can prove these statements from the Euclidean algorithm as follows.

♣Putting this discussion here makes part of the section on $SL(2,\mathbb{Z})$ and continued fractions a little redundant. ♣

For an integer n define

$$T(n) := \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = T^n \tag{11.9}$$

where

$$T := T(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad . \tag{11.10}$$

Now let us write the first line of the Euclidean algorithm as a matrix identity as

$$T(-q_1)\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} r_1 \\ B \end{pmatrix} \tag{11.11}$$

and better, we write this as:

$$\sigma^1 T(-q_1)\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} B \\ r_1 \end{pmatrix} \tag{11.12}$$

Then the second line of the Euclidean algorithm becomes:

$$\sigma^1 T(-q_2)\sigma^1 T(-q_1)\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \tag{11.13}$$

Thus we have

$$\sigma^1 T(-q_j)\cdots\sigma^1 T(-q_2)\sigma^1 T(-q_1)\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix} \tag{11.14}$$

and in the final step:

$$\sigma^1 T(-q_{j+1})\sigma^1 T(-q_j)\cdots\sigma^1 T(-q_2)\sigma^1 T(-q_1)\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} r_j \\ 0 \end{pmatrix} \tag{11.15}$$

Multiplying out the matrices on the LHS gives an expression:

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} r_j \\ 0 \end{pmatrix} \tag{11.16}$$

(Note that x, y, u, v are polynomials in the q_i. See comments on continued fractions below.)

Remarks:

1. *The Euclidean algorithm is fast*: A theorem of Lamé asserts that the Euclidean algorithm is very efficient. It should be completely obvious to you that the number of steps cannot exceed B. (Recall that $A > B$.) However, Lamé asserts that in fact the number of steps never exceeds $5\log_{10} B$. This is important for RSA (see below).

2. *Relation to continued fractions*: Note that from equation (11.15) we can also write

$$\begin{pmatrix} A \\ B \end{pmatrix} = T(q_1)\sigma^1 T(q_2)\sigma^1 \cdots T(q_j)\sigma^1 T(q_{j+1})\sigma^1 \begin{pmatrix} r_j \\ 0 \end{pmatrix} \tag{11.17}$$

Let us write:

$$M(q) := T(q)\sigma^1 = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \tag{11.18}$$

We now define two sequences of polynomials in n variables that we call $N_n(q_1, \dots, q_n)$ and $D_n(q_1, \dots, q_n)$ for all $n \geq 1$. It is convenient to define $N_0 = 1$ and $D_0 = 1$ and then we can write:

$$M(q_1) \cdots M(q_n) := \begin{pmatrix} N_n(q_1, \dots, q_n) & N_{n-1}(q_1, \dots, q_{n-1}) \\ D_n(q_1, \dots, q_n) & D_{n-1}(q_1, \dots, q_{n-1}) \end{pmatrix} \tag{11.19}$$

(The reader should check that this is a consistent definition for all n.) One easily generates:

$$\begin{aligned} N_1(q_1) &= q_1 \\ N_2(q_1, q_2) &= 1 + q_1 q_2 \\ N_3(q_1, q_2, q_3) &= q_1 + q_3 + q_1 q_2 q_3 \end{aligned} \tag{11.20}$$

$$\begin{aligned} D_1(q_1) &= 1 \\ D_2(q_1, q_2) &= q_2 \\ D_3(q_1, q_2, q_3) &= 1 + q_2 q_3 \end{aligned} \tag{11.21}$$

These polynomials are closely related to continued fractions, defined as:

$$[q_1, q_2, q_3, \cdots, q_j] := q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_j}}} \tag{11.22}$$

Indeed, now that

$$M(q_1) \cdot (M(q_2) \cdots M(q_{n+1})) = M(q_1) \begin{pmatrix} N_n(q_2, \dots, q_{n+1}) & N_{n-1}(q_2, \dots, q_n) \\ D_n(q_2, \dots, q_{n+1}) & D_{n-1}(q_2, \dots, q_n) \end{pmatrix} \tag{11.23}$$

from which one deduces the recursion relations:

$$\begin{aligned} N_{n+1}(q_1, \dots, q_{n+1}) &= q_1 N_n(q_2, \dots, q_{n+1}) + D_n(q_2, \dots, q_{n+1}) \\ D_{n+1}(q_1, \dots, q_{n+1}) &= N_n(q_2, \dots, q_{n+1}) \end{aligned} \tag{11.24}$$

On the other hand, writing

$$[q_1, q_2, q_3, \cdots, q_n] := \frac{P_n(q_1, \dots, q_n)}{Q_n(q_1, \dots, q_n)} \tag{11.25}$$

we see that

$$\begin{aligned} [q_1, q_2, q_3, \cdots, q_{n+1}] &= q_1 + \frac{1}{[q_2, \dots, q_{n+1}]} \\ &= \frac{q_1 P_n(q_2, \dots, q_{n+1}) + Q_n(q_2, \dots, q_{n+1})}{P_n(q_2, \dots, q_{n+1})} \end{aligned} \tag{11.26}$$

So, P_n, Q_n satisfy the same recursion relations as N_n, D_n, respectively, and since the initial values are also the same we conclude that $P_n = N_n$ and $Q_n = D_n$.

Exercise
Check the Lamé bound for the two examples above.

Exercise
Given one solution for (11.7), find all the others.

Exercise *Continued fractions and the Euclidean algorithm*
a.) Show that the quotients q_i in the Euclidean algorithm define a continued fraction expansion for A/B:

$$\frac{A}{B} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_j}}} := [q_1, q_2, q_3, \cdots, q_j] \tag{11.27}$$

The fractions $[q_1], [q_1, q_2], [q_1, q_2, q_3], \dots$ are known as the *convergents* of the continued fraction.

b.) Show that [75]

$$\begin{aligned} N_{n+1}(q_1, \dots, q_{n+1}) &= q_{n+1} N_n(q_1, \dots, q_n) + N_{n-1}(q_1, \dots, q_{n-1}) \\ D_{n+1}(q_1, \dots, q_{n+1}) &= q_{n+1} D_n(q_1, \dots, q_n) + D_{n-1}(q_1, \dots, q_{n-1}) \end{aligned} \tag{11.28}$$

c.) Show that

$$N_n D_{n-1} - D_n N_{n-1} = (-1)^n \tag{11.29}$$

---

[75] *Answer*: Write $M(q_1) \cdots M(q_{n+1}) = (M(q_1) \cdots M(q_n)) \cdot M(q_{n+1})$.

11.2 Application: Expressing elements of $SL(2,\mathbb{Z})$ as words in S and T

The group $SL(2,\mathbb{Z})$ is generated by

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \& \qquad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{11.30}$$

Here is an algorithm for decomposing an arbitrary element

$$h = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL(2,\mathbb{Z}) \tag{11.31}$$

as a word in S and T.

First, note the following simple

Lemma Suppose $h \in SL(2,\mathbb{Z})$ as in (11.31). Suppose moreover that $g \in SL(2,\mathbb{Z})$ satisfies:

$$g \cdot \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{11.32}$$

Then

$$gh = T^n \tag{11.33}$$

for some integer $n \in \mathbb{Z}$.

The proof is almost immediate by combining the criterion that $gh \in SL(2,\mathbb{Z})$ has determinant one and yet must have the first column $(1,0)$.

Now, suppose h is such that $A > C > 0$. Then $(A,C) = 1$ and hence we have the Euclidean algorithm to define integers q_ℓ, $\ell = 1, \dots N+1$, where $N \geq 1$, such that

$$\begin{aligned} A &= q_1 C + r_1 \qquad 0 < r_1 < C \\ C &= q_2 r_1 + r_2 \qquad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \qquad 0 < r_3 < r_2 \\ \vdots & \quad \vdots \\ r_{N-2} &= q_N r_{N-1} + r_N \qquad 0 < r_N < r_{N-1} \\ r_{N-1} &= q_{N+1} r_N \end{aligned} \tag{11.34}$$

with $r_N = (A,C) = 1$. (Note you can interpret $r_0 = C$, as is necessary if $N = 1$.) Now, write the first line in the Euclidean algorithm in matrix form as: ♣$N = 0$ here?♣

$$\begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} r_1 \\ C \end{pmatrix} \tag{11.35}$$

We would like to have the equation in a form that we can iterate the algorithm, so we need the larger integer on top. Therefore, rewrite the identity as:

$$\sigma^1 \begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} C \\ r_1 \end{pmatrix} \tag{11.36}$$

We can now iterate the procedure. So the Euclidean algorithm implies the matrix identity:

$$\tilde{g}\begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{11.37}$$

$$\tilde{g} = (\sigma^1 T^{-q_{N+1}}) \cdots (\sigma^1 T^{-q_1}) \tag{11.38}$$

Now, to apply the Lemma we need g to be in $SL(2,\mathbb{Z})$, but

$$\det\tilde{g} = (-1)^{N+1} \tag{11.39}$$

We can easily modify the equation to obtained a desired element g. We divide the argument into two cases:

1. Suppose first that $N+1 = 2s$ is even. Then we group the factors of $\tilde{g}$ in pairs and write

$$\begin{aligned}(\sigma^1 T^{-q_{2\ell}})(\sigma^1 T^{-q_{2\ell-1}}) &= (\sigma^1\sigma^3)(\sigma^3 T^{-q_{2\ell}}\sigma^3)(\sigma^3\sigma^1)T^{-q_{2\ell-1}} \\ &= -ST^{q_{2\ell}}ST^{-q_{2\ell-1}}\end{aligned} \tag{11.40}$$

where we used that $\sigma^1\sigma^3 = -\mathrm{i}\sigma^2 = S$. Therefore, we can write

$$\tilde{g} = g = (-1)^s \prod_{\ell=1}^{s}(ST^{q_{2\ell}}ST^{-q_{2\ell-1}}) \tag{11.41}$$

2. Now suppose that $N+1 = 2s+1$ is odd. Then we rewrite the identity (11.37) as:

$$\sigma^1\tilde{g}\begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{11.42}$$

so now we simply take

$$g = \sigma^1\tilde{g} = (-1)^{s+1}(ST^{-q_{2s+1}})\prod_{\ell=1}^{s}(ST^{q_{2\ell}}ST^{-q_{2\ell-1}}) \tag{11.43}$$

Thus we can summarize both cases by saying that

$$g = (-1)^{\lfloor\frac{N+1}{2}\rfloor}\prod_{\ell=1}^{N+1}(ST^{(-1)^\ell q_\ell}) \tag{11.44}$$

Then we can finally write

$$h = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = g^{-1}T^n \tag{11.45}$$

as a word in S and T for a suitable integer n. (Note that $S^2 = -1$.)

♣It would be good to give an algorithm for determining n. ♣

Now we need to show how to bring the general element $h \in SL(2,\mathbb{Z})$ to the form with $A > C > 0$ so we can apply the above formula. Note that

$$\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ C+mA & D+mB \end{pmatrix} \tag{11.46}$$

while

$$\begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix} = ST^m S^{-1} \tag{11.47}$$

Thus, if $A > 0$ we can use this operation to shift C so that $0 \le C < A$. In case $A < 0$ we can multiply by $S^2 = -1$ to reduce to the case $A > 0$. Finally, if $A = 0$ then

$$h = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & n \end{pmatrix} \tag{11.48}$$

and we write

$$ST^n = \begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix} \tag{11.49}$$

♣Need to summarize the result in a useful way ♣

11.3 Products Of Cyclic Groups And The Chinese Remainder Theorem

Recall the elementary definition we met in the last exercise of section 2.

Definition Let H, G be two groups. The *direct product* of H and G, denoted $H \times G$, is the set $H \times G$ with product:

$$(h_1, g_1) \cdot (h_2, h_2) = (h_1 \cdot h_2, g_1 \cdot g_2) \tag{11.50}$$

We will consider the direct product of cyclic groups. According to our general notation we would write this as $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. However, since $\mathbb{Z}_m$ is also a ring the notation $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ also often used, and we will use it below, especially when we write our Abelian groups additively.

Let us begin with the question: Is it true that

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \overset{?}{\cong} \mathbb{Z}_{m_1 m_2}. \tag{11.51}$$

In general (11.51) is *false*!

Exercise

a.) Show that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. (There is a one-line proof.) [76]

b.) Is p is prime is $\mathbb{Z}_p \oplus \mathbb{Z}_p$ isomorphic to $\mathbb{Z}_{p^2}$?

c.) Is $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ isomorphic to $\mathbb{Z}_{15}$?

Write $g = \gcd(m_1, m_2)$ and $\ell = \mathrm{lcm}(m_1, m_2)$. Then there are two natural exact sequences:

$$1 \to \mathbb{Z}_g \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \to \mathbb{Z}_\ell \to 1 \tag{11.52}$$

$$0 \to \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \to \mathbb{Z}/g\mathbb{Z} \to 0 \tag{11.53}$$

[76] *Answer*: Every element in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is of order two. But some elements of $\mathbb{Z}_4$ have order four. The but the order of a group element is preserved under isomorphism.

In fact, we will show below that

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cong \mathbb{Z}_g \times \mathbb{Z}_\ell \tag{11.54}$$

Remarks:

1. The sequence (11.52) is easier to write down multiplicatively, while (11.53) is easier to write down additively. See the discussion below. (Of course, both are true in either formulation!)
2. If $g = 1$ since $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z}$ is the trivial group we can indeed conclude that $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cong \mathbb{Z}_{m_1 m_2}$ but otherwise this is false. We will return to this point.

Now, let us prove (11.52) and (11.53).

Recall that

$$m_1 m_2 = g\ell \tag{11.55}$$

a fact that will be useful momentarily. (If you do not know this we will prove it below.) It will also be useful to write $m_1 = \mu_1 g$ and $m_2 = \mu_2 g$ where μ_1, μ_2 are relatively prime. Thus there are integers ν_1, ν_2 with

$$\mu_1 \nu_1 + \mu_2 \nu_2 = 1 \tag{11.56}$$

and hence

$$m_1 \nu_1 + m_2 \nu_2 = g. \tag{11.57}$$

To prove (11.52) think of $\mathbb{Z}_m$ as the multiplicative group of m^{th} roots of 1, so they are all subgroups of $U(1)$. Now define a group homomorphism:

$$\pi : \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \to \mathbb{Z}_\ell \tag{11.58}$$

by:

$$\pi : (\xi_1, \xi_2) \to \xi_1 \xi_2 \tag{11.59}$$

That is, we merely multiply the two entries. (This makes it clear that it is a group homomorphism since the group law is multiplication of complex numbers and that multiplication is commutative.) Here ξ_1 is an m_1^{th} root of unity and ξ_2 is an m_2^{th} root of unity. The only thing you need to check is that indeed then $\xi_1 \xi_2$ is an ℓ^{th} root of unity, so π indeed maps into $\mathbb{Z}_\ell$.

Now we prove that π is surjective: Let $\omega_1 = e^{\frac{2\pi i}{m_1}}$ and $\omega_2 = e^{\frac{2\pi i}{m_2}}$. These are generators of $\mathbb{Z}_{m_1}$ and $\mathbb{Z}_{m_2}$. Choose integers ν_1, ν_2 so that $\nu_1 m_1 + \nu_2 m_2 = g$ then π maps

$$\begin{aligned} \pi : (\omega_1^{\nu_2}, \omega_2^{\nu_1}) \mapsto & \ \omega_1^{\nu_2} \omega_2^{\nu_1} \\ & = \exp\left[2\pi \mathrm{i}\left(\frac{\nu_2}{m_1} + \frac{\nu_1}{m_2}\right)\right] \\ & = \exp\left[2\pi \mathrm{i}\left(\frac{m_2\nu_2 + m_1\nu_1}{m_1 m_2}\right)\right] \\ & = \exp\left[2\pi \mathrm{i}\frac{g}{m_1 m_2}\right] \\ & = \exp\left[2\pi \mathrm{i}\frac{1}{\ell}\right] \end{aligned} \tag{11.60}$$

But $\exp\left[2\pi i\frac{1}{\ell}\right]$ is a generator of the multiplicative group of ℓ^{th} roots of unity, isomorphic to $\mathbb{Z}_\ell$, and hence the homomorphism π is onto. Thus, we have checked exactness of the sequence at $\mathbb{Z}_\ell$.

On the other hand the injection map

$$\iota : \mathbb{Z}_g \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \tag{11.61}$$

is defined by identifying $\mathbb{Z}_g$ with the multiplicative group of g^{th} roots of unity and just sending:

$$\iota(\xi) = (\xi, \xi^{-1}) \tag{11.62}$$

Note that a g^{th} root of unity ξ has the property that $\xi^{\pm 1}$ is also both an m_1^{th} and an m_2^{th} root of unity. So this makes sense. It is now easy to check that indeed the kernel of π is the image of ι. Since π takes the product of the two entries it is immediate from the definition (11.62) that $im(\iota) \subset \ker(\pi)$. On the other hand, if $\pi(\xi_1, \xi_2) = \xi_1\xi_2 = 1$ then clearly $\xi_2 = \xi_1^{-1}$, so this must be in the image of ι. Now we have checked exactness at the middle of the sequence. Exactness at $\mathbb{Z}_g$ is trivial. This concludes the proof of (11.52) ♠

It is worth noting that we can write "additive" version of the maps ι and π as:

$$\begin{aligned} \iota(x) &= \mu_1 x \oplus (-\mu_2 x) \\ \pi(x_1 \oplus x_2) &= \mu_2 x_1 + \mu_1 x_2 \end{aligned} \tag{11.63}$$

You should check that written this way it is well defined, and the sequence is exact.

Exercise

a.) Show that there is an exact sequence

$$0 \to \mathbb{Z}/\ell\mathbb{Z} \overset{\iota}{\to} \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \overset{\pi}{\to} \mathbb{Z}/g\mathbb{Z} \to 0 \tag{11.64}$$

where

$$\pi : x_1 \oplus x_2 \mapsto (x_1 - x_2)\mathrm{mod} g\ . \tag{11.65}$$

$$\iota : x \mapsto (x\mathrm{mod} m_1 \oplus x\mathrm{mod} m_2) \tag{11.66}$$

b.) Show that if we think of these groups as groups of roots of unity then we have $\pi(\xi_1, \xi_2) = \xi_1^{\mu_1}\xi_2^{-\mu_2}$ and $\iota(\omega) = (\omega^{\mu_2}, \omega^{\mu_1})$ with $m_1 = \mu_1 g$ and $m_2 = \mu_2 g$.

Now we prove that in general

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cong \mathbb{Z}_g \times \mathbb{Z}_\ell \tag{11.67}$$

First, it follows from either of the two exact sequences we proved above that if $(m_1, m_2) = 1$ then indeed

$$\mathbb{Z}_{m_1 m_2} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \tag{11.68}$$

Next, recall that any integer can be decomposed into its prime factors:

$$m = \prod_p p^{v_p(m)} \tag{11.69}$$

where $v_p(m) \in \mathbb{Z}_+$, known as the *valuation of m at p* is zero for all but finitely many primes. (So we have an infinite product of 1's on the RHS of the above equation.)

Now in terms of the prime factorizations of m_1, m_2 we can write:

$$\begin{aligned} g = \mathrm{gcd}(m_1, m_2) &= \prod_p p^{\min[v_p(m_1), v_p(m_2)]} \\ \ell = \mathrm{lcm}(m_1, m_2) &= \prod_p p^{\max[v_p(m_1), v_p(m_2)]} \end{aligned} \tag{11.70}$$

Now, from the above we know that $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cong \mathbb{Z}_{m_1 m_2}$ if m_1 and m_2 are relatively prime. Therefore we can write

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_p (\mathbb{Z}/p^{v_p(m)}\mathbb{Z}) \tag{11.71}$$

Applying this to each of the two factors in $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ and using $G_1 \times G_2 \cong G_2 \times G_1$ to arrange the factors so the minimum power is on the left and maximum on the right and regrouping gives (11.67). In equations:

$$\begin{aligned} \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} &\cong \prod_p \mathbb{Z}_{p^{\nu_p(m_1)}} \times \prod_p \mathbb{Z}_{p^{\nu_p(m_2)}} \\ &\cong \prod_p \mathbb{Z}_{p^{\min[\nu_p(m_1), \nu_p(m_2)]}} \times \prod_p \mathbb{Z}_{p^{\max[\nu_p(m_1), \nu_p(m_2)]}} \\ &\cong \mathbb{Z}_g \times \mathbb{Z}_\ell \end{aligned} \tag{11.72}$$

A second proof gives some additional insight by providing an interesting visual picture of what is going on, as well as relating this fact to lattices. It is related to the first by "taking a logarithm" and involves exact sequences of infinite groups which induce sequences on finite quotients.

Consider the sublattice of $\mathbb{Z} \oplus \mathbb{Z}$ given by

$$\Lambda = m_1\mathbb{Z} \oplus m_2\mathbb{Z} = \{ \begin{pmatrix} m_1\alpha \\ m_2\beta \end{pmatrix} | \alpha, \beta \in \mathbb{Z} \} \tag{11.73}$$

Then $\Lambda \subset \mathbb{Z} \oplus \mathbb{Z}$ is a sublattice and it should be pretty clear that

$$\mathbb{Z}^2/\Lambda = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \tag{11.74}$$

Now, write $m_1 = \mu_1 g, m_2 = \mu_2 g$ as above. Choose integers ν_1, ν_2 so that $\mu_1\nu_1 + \mu_2\nu_2 = 1$ and consider the matrix

$$\begin{pmatrix} \mu_2 & \mu_1 \\ -\nu_1 & \nu_2 \end{pmatrix} \in SL(2, \mathbb{Z}) \tag{11.75}$$

This is an invertible matrix over the integers, so we can change coordinates on the lattice from $x = m_1\alpha, y = m_2\beta$ to

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \mu_2 & \mu_1 \\ -\nu_1 & \nu_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{11.76}$$

that is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \nu_2 & -\mu_1 \\ \nu_1 & \mu_2 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \tag{11.77}$$

which we prefer to write as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = x' \begin{pmatrix} \nu_2 \\ \nu_1 \end{pmatrix} + y' \begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \tag{11.78}$$

We interpret this as saying that x', y' are the coordinates of the vector $(x, y) \in \mathbb{Z}^2$ relative to the new basis vectors for $\mathbb{Z}^2$.

$$v_1 = \begin{pmatrix} \nu_2 \\ \nu_1 \end{pmatrix} \qquad v_2 = \begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \tag{11.79}$$

The good property of this basis is that the smallest multiple of v_1 that sits in Λ is ℓv_1 (prove this) [77] Similarly, the smallest multiple of v_2 in Λ is $g v_2$. Thus, we have a way of writing $\mathbb{Z}^2$ as $\mathbb{Z}v_1 \oplus \mathbb{Z}v_2$ such that the projection of Λ to the v_1 axis is the group $\ell\mathbb{Z}$ while the kernel is the subgroup of $\mathbb{Z}v_2$ that maps into Λ, and that is just $\cong g\mathbb{Z}$.

Put differently, there is a homomorphism $\psi : \mathbb{Z}^2 \to \mathbb{Z}$ that takes

$$\psi : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto x' \ . \tag{11.80}$$

This is the projection on the v_1 axis. This defines a surjective homomorphism onto $\mathbb{Z}$. (Explain why.) On the other hand, using (11.76) and $\mu_1\mu_2 g = \ell$ we see that the image of Λ under ψ is $\ell\mathbb{Z}$. Therefore, using the exercise result (10.24) ψ descends to a map

$$\bar{\psi} : \mathbb{Z}^2/\Lambda \to \mathbb{Z}/\ell\mathbb{Z} \tag{11.81}$$

Now note from (11.78) that

$$\begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \mathrm{mod}\Lambda \tag{11.82}$$

is in the kernel of $\bar{\psi}$, and moreover it generates a cyclic subgroup of order g in $\mathbb{Z}^2/\Lambda$. By counting, this cyclic subgroup must be the entire kernel of $\bar{\psi}$. Therefore we have an exact sequence

$$0 \to \mathbb{Z}_g \to \mathbb{Z}^2/\Lambda \to \mathbb{Z}_\ell \to 0 \tag{11.83}$$

$*************************$

AND THERE IS A MAP TO y' AND TOGETHER THESE GIVE ISOMORPHISM TO $\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/g\mathbb{Z}$.

$*************************$

This concludes our second proof. ♠

♣Should really add a figure to illustrate this. Unfortunately the first really nontrivial case is $m_1 = 2 \cdot 3$ and $m_2 = 2 \cdot 5$ so $\ell = 30$. ♣

Exercise

Using the Kronecker theorem show that if a finite Abelian group G is not a cyclic group then there is a nontrivial divisor n of $|G|$ so that $g^n = 1$ for all $g \in G$.

11.3.1 The Chinese Remainder Theorem

In fact, there is an important generalization of this statement known as the *Chinese remainder theorem*:

Theorem Suppose $m_1, \dots, m_r$ are pairwise relatively prime positive integers, (i.e. $(m_i, m_j) = 1$ for all $i \neq j$) then

$$(\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \cong \mathbb{Z}/M\mathbb{Z} \tag{11.84}$$

where $M = m_1 m_2 \cdots m_r$.

Proof:

The fastest proof makes use of the previous result and induction on r.

A second proof offers some additional insight into solving simultaneous congruences: We construct a homomorphism

$$\psi : \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \tag{11.85}$$

by

$$\psi(x) = (x \text{mod} m_1, x \text{mod} m_2, \dots, x \text{mod} m_r) \tag{11.86}$$

We first claim that $\psi(x)$ is *onto.* That is, for any values $a_1, \dots, a_r$ we can solve the simultaneous congruences:

$$\begin{aligned} x &= a_1 \text{mod} m_1 \\ x &= a_2 \text{mod} m_2 \\ \vdots &\quad \vdots \\ x &= a_r \text{mod} m_r \end{aligned} \tag{11.87}$$

for some common value $x \in \mathbb{Z}$.

[77] *Answer*: We have $x v_1 \in \Lambda$ iff $x\nu_2 = 0 \text{mod}(g\mu_1)$ and $x\nu_1 = 0\text{mod}(g\mu_2)$. Multiply these equations by μ_2 and μ_1, respectively, and add them. Find that $x = 0\text{mod}\ell$.

To prove this note that $\hat{m}_i := M/m_i = \prod_{j\neq i} m_j$ is relatively prime to m_i (by the hypothesis of the theorem). Therefore there are integers x_i, y_i such that

$$x_i m_i + y_i \hat{m}_i = 1 \tag{11.88}$$

Let $g_i = y_i \hat{m}_i$. Note that

$$g_i = \delta_{i,j} \text{mod} m_j \qquad \forall 1 \leq i,j \leq r \tag{11.89}$$

Therefore if we set

$$x = \sum_{i=1}^{r} a_i g_i \tag{11.90}$$

then x is a desired solution to (11.87) and hence is a preimage under ψ.

On the other hand, the kernel of ψ is clearly $M\mathbb{Z}$. Therefore:

$$0 \to M\mathbb{Z} \to \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \to 0 \tag{11.91}$$

and hence the desired isomorphism follows. ♠

Remarks

1. Equation (11.67) is used implicitly all the time in physics, whenever we have two degrees of freedom with different but commensurable frequencies. Indeed, it is used all the time in everyday life. As a simple example, suppose you do X every other day. You will then do X on Mondays every other week, i.e., every 14 days, because 2 and 7 are relatively prime. More generally, consider a system with a discrete configuration space $\mathbb{Z}/p\mathbb{Z}$ thought of as the multiplicative group of p^{th} roots of 1. Suppose the time evolution for $\Delta t = 1$ is $\omega_p^r \to \omega_p^{r+1}$ where ω_p is a primitive p^{th} root of 1. The basic period is $T = p$. Now, if we have *two* oscillators of periods p, q, the configuration space is $\mathbb{Z}_p \times \mathbb{Z}_q$. The basic period of this system is - obviously - the least common multiple of p and q. That is the essential content of (**??**).

2. Our second proof shows that in fact equation (11.84) is a statement of an isomorphism of rings.

3. One might wonder how the theorem got this strange name. (Why don't we refer to the "Swiss-German theory of relativity?") The theorem is attributed (see, e.g. Wikipedia) to Sun-tzu Suan-ching in the 3rd century A.D. (He should not be confused with Sun Tzu who lived in the earlier Spring and Autumn period and wrote *The Art of War.*) For an interesting historical commentary see [78] which documents the historical development in India and China up to the definitive treatments by Euler, Lagrange, and Gauss who were probably unaware of previous developments hundreds of years earlier. The original motivation was apparently related to construction of calendars, and this is certainly mentioned by Gauss in his renowned book *Disquisitiones Arithmeticae.* The Chinese calendar is based on *both* the lunar and solar cycles. Roughly speaking, one starts the new year based on both the winter solstice

and the new moon. Thus, to find periods of time in this calendar one needs to solve simultaneous congruences. I suspect the name "Chinese Remainder Theorem" is an invention of 19th century mathematicians. Hardy & Wright (1938) do not call it that, but do recognize Sun Tzu.

♣Some students with Chinese background say this is wrong. Check it out. ♣

Exercise *Counting your troops*

Suppose that you are a general and you need to know how many troops you have from a cohort of several hundred. Time is too short to take attendance.

So, you have your troops line up in rows of 5. You observe that there are 3 left over. Then you have your troops line up in rows of 11. Now there are 2 left over. Finally, you have your troops line up in rows of 13, and there is only one left over.

How many troops are there? [79]

Exercise

a.) Show that the Chinese Remainder theorem is false if the m_i are not pairwise relatively prime.

b.) Show that the obstruction to finding a solution x to $x = a_i \text{mod} m_i$ is given by the reductions $(a_i - a_j)\text{mod}(m_i, m_j)$ over all pairs $i \neq j$. That is, a solution exists iff all of these vanish.

12. The Group Of Automorphisms

Recall that an *automorphism* of a group G is an isomorphism $\mu : G \to G$, i.e. an isomorphism of G onto itself.

One easily checks that the composition of two automorphisms μ_1, μ_2 is an automorphism. The identity map is an automorphism, and every automorphism is invertible. In this way, the set of automorphisms, $\text{Aut}(G)$, is *itself a group* with group law given by composition.

Given a group G there are God-given automorphisms given by conjugation. That is, if $a \in G$ then

$$I(a) : g \to aga^{-1} \tag{12.1}$$

[78] Kang Sheng Shen, "Historical development of the Chinese remainder theorem," Arch. Hist. Exact Sci. 38 (1988), no. 4, 285305.

[79] Apply the Chinese remainder theorem with $m_1 = 5, m_2 = 11, m_3 = 13$. Then $M = 715$, $\hat{m}_1 = 143$, $\hat{m}_2 = 65$ and $\hat{m}_3 = 55$. Using the Euclidean algorithm you find convenient lifts to the integers $g_1 = 286$, $g_2 = -65$ and $g_3 = -220$. Then the number of troops is $3 \times 286 - 2 \times 65 - 1 \times 220 = 508 \text{mod} 715$. Therefore there are 508 soldiers.

defines an automorphism of G. Indeed $I(a) \circ I(b) = I(ab)$ and hence $I : G \to \mathrm{Aut}(G)$ is a homomorphism. The subgroup $\mathrm{Inn}(G)$ of such automorphisms is called the group of *inner automorphisms*. Note that if $a \in Z(G)$ then $I(a)$ is trivial, and conversely. Thus we have:

$$\mathrm{Inn}(G) \cong G/Z(G). \tag{12.2}$$

Moreover, $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$, since for any automorphism $\phi \in \mathrm{Aut}(G)$:

$$\phi \circ I(a) \circ \phi^{-1} = I(\phi(a)). \tag{12.3}$$

Therefore we have another group

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G) \tag{12.4}$$

known as the group of "outer automorphisms." Thus

$$1 \to \mathrm{Inn}(G) \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1 \tag{12.5}$$

Note we can also write and exact sequence of length four:

$$1 \to Z(G) \to G \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1 \tag{12.6}$$

Remarks

1. In practice one often reads or hears the statement that an element $\varphi \in \mathrm{Aut}(G)$ is an "outer automorphism." What this means is that it projects to a nontrivial element of $\mathrm{Out}(G)$. However, strictly speaking this is an abuse of terminology and an outer automorphism is in the quotient group (12.4). These notes might sometimes perpetrate this abuse of terminology.

2. Note that for any abelian group G all nontrivial automorphisms are outer automorphisms.

Example 12.1: Consider $\mathrm{Aut}(\mathbb{Z}_3)$. This group is Abelian so all automorphisms are outer. Thinking of it multiplicatively, the only nontrivial choice is $\omega \to \omega^{-1}$. If we think of $A_3 \cong \mathrm{Aut}(\mathbb{Z}_3)$ then we are taking

$$(123) \to (132) \tag{12.7}$$

So: $Aut(\mathbb{Z}_3) \cong \mathbb{Z}_2$.

Example 12.2: Consider $Aut(\mathbb{Z}_4)$. Think of $\mathbb{Z}_4$ as the group of fourth roots of unity, generated by $\omega = \exp[i\pi/2] = i$. A generator must go to a generator, so there is only one possible nontrivial automorphism: $\phi : \omega \to \omega^3$. Note that $\omega \to \omega^2$ is a nontrivial homomorphism of $\mathbb{Z}_4 \to \mathbb{Z}_4$, but it is not an automorphism. Thus $Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$.

Example 12.3: Consider $Aut(\mathbb{Z}_5)$. Think of $\mathbb{Z}_5$ as the group of fifth roots of unity, generated by $\omega = \exp[2\pi i/5]$. Now there are several automorphisms: ϕ_2 defined by its action on the generator $\omega \to \omega^2$. Similarly, we can define ϕ_3, by $\omega \to \omega^3$ and ϕ_4, by $\omega \to \omega^4$. Letting ϕ_1 denote the identity we have

$$\phi_2^2 = \phi_4 \qquad \phi_2^3 = \phi_3 \qquad \phi_2^4 = \phi_4^2 = \phi_1 = 1 \tag{12.8}$$

So $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$. The explicit isomorphism is

$$\begin{aligned} \phi_2 &\to \bar{1} \\ \phi_4 &\to \bar{2} \\ \phi_3 &\to \bar{3} \end{aligned} \tag{12.9}$$

Example 12.4: Consider Aut($\mathbb{Z}_N$), and let us think of $\mathbb{Z}_N$ multiplicatively as the group of N^{th} roots of 1. An automorphism ϕ of $\mathbb{Z}_N$ must send $\omega \mapsto \omega^r$ for some r. On the other hand, ω^r must also be a generator of $\mathbb{Z}_N$. Automorphisms must take generators to generators. Hence r is relatively prime to N. This is true iff there is an s with

$$rs = 1 \mathrm{mod} N \tag{12.10}$$

Thus, $Aut(\mathbb{Z}_N)$ is the group of transformations $\omega \to \omega^r$ where r admits a solution to $rs = 1\mathrm{mod}N$. We will examine this interesting group in a little more detail in §12.1 below.

Example 12.5: *Automorphisms Of The Symmetric Group S_n*: There are no outer automorphisms of S_n so

$$Aut(S_n) \cong Inn(S_n) \cong S_n, \qquad n \neq 2, 6 \tag{12.11}$$

Note the exception: $n = 2, 6$. Note the striking contrast from an abelian group, all of whose automorphisms are outer.

This is not difficult to prove: Note that an automorphism ϕ of S_n must take conjugacy classes to conjugacy classes. Therefore we focus on how it acts on transpositions. These are involutions, and involutions must map to involutions so the conjugacy class of transpositions must map to a conjugacy class of the form $(1)^k(2)^\ell$ with $k + 2\ell = n$. We will show below that, just based on the order of the conjugacy class, ϕ must map transpositions to transpositions. We claim that any automorphism that maps transpositions to transpositions must be inner. Let us say that

$$\phi((ab)) = (xy) \qquad \phi((ac)) = (zw) \tag{12.12}$$

where a, b, c are all distinct. We claim that x, y, z, w must comprise precisely three distinct letters. We surely can't have $(xy) = (zw)$ because ϕ is 1-1, and we also can't have (xy) and (zw) commuting because the group commutator of (ab) and (ac) is (abc). Therefore we can write

$$\phi((ab)) = (xy) \qquad \phi((ac)) = (xz) \tag{12.13}$$

Therefore, we have defined a permutation $a \to x$ and ϕ is the inner automorphism associated with this permutation.

Now let us consider the size of the conjugacy classes. This was computed in exercise *** above. The size of the conjugacy class of transpositions is of course

$$\binom{n}{2} = \frac{n!}{(n-2)!2!} \tag{12.14}$$

The size of a conjugacy class of the form $(1)^k(2)^\ell$ with $k + 2\ell = n$ is

$$\frac{n!}{(n-2\ell)!\ell!2^\ell} \tag{12.15}$$

Setting these equal results in the identity

$$\frac{(n-2)!}{(n-2\ell)!} = \ell!2^{\ell-1} \qquad n \geq 2\ell \tag{12.16}$$

For a fixed ℓ the LHS is a polynomial in n which is growing for $n \geq 2\ell$ and therefore bounded below by $(2\ell-2)!$. Therefore we consider whether there can be a solution with $n = 2\ell$:

$$(2\ell-2)! = \ell!2^{\ell-1} \tag{12.17}$$

For $\ell = 3$, corresponding to $n = 6$, there is a solution, but for $\ell > 3$ we have $(2\ell - 2)! > \ell!2^{\ell-1}$. The peculiar exception $n = 6$ is related to the symmetries of the icosahedron. For more information see

1.http://en.wikipedia.org/wiki/Automorphisms of the symmetric and alternating groups

2. http://www.jstor.org/pss/2321657

3. I.E. Segal, "The automorphisms of the symmetric group," *Bulletin of the American Mathematical Society* **46**(1940) 565.

Example 12.6: *Automorphisms Of Alternating Groups.* For the group $A_n \subset S_n$ there is an automorphism which is not obviously inner: Conjugation by any odd permutation. Recall that $Out(G) = Aut(G)/Inn(G)$ is a quotient group so conjugation by any odd permutation represents the same element in $Out(G)$. If we consider $A_3 \subset S_3$ then

$$(12)(123)(12)^{-1} = (132) \tag{12.18}$$

is indeed a nontrivial automorphism of A_3 and since A_3 is abelian this automorphism must be an outer automorphism. In general conjugation by an odd permutation defines an outer automorphism of A_n. For example suppose conjugation by (12) were inner. Then there would be an even permutation a so that conjugation by $a \cdot (12)$ centralizes every $h \in A_n$. But $a \cdot (12)$ together with A_n generates all of S_n and then $a \cdot (12)$ would have to be in the center of S_n, a contradiction. Thus, the outer automorphism group of A_n contains a nontrivial involution. Again for $n = 6$ there is an exceptional outer automorphism.

The above example nicely illustrates a general idea: If $N \triangleleft G$ is a normal subgroup of G and $g \notin H$ then conjugation by g defines an automorphism $H \to H$ which is, in general, not an inner automorphism.

Example 12.7: Consider $G = GL(n, \mathbb{C})$. Then $A \to A^*$ is an outer automorphism: That is, there is no invertible complex matrix $S \in GL(n, \mathbb{C})$ such that, for every invertible matrix $A \in GL(n, \mathbb{C})$ we have

$$A^* = SAS^{-1} \tag{12.19}$$

Exercise *Outer Automorphisms Of Some Matrix Groups*

a.) Prove (12.19). [80]

b.) Consider maps of $GL(n,\mathbb{C})$ given by $A \to A^{tr}$, $A \to A^{-1}$ and $A \to A^{tr,-1}$. Which of these are automorphisms? Which of these are outer automorphisms?

c.) Consider $G = SU(2)$. Is $A \to A^*$ an outer automorphism? [81]

d.) Consider the automorphism of $G = SO(2)$

$$R(\phi) \to R(-\phi) \tag{12.20}$$

Is this inner or outer?

Exercise *Automorphisms of* $\mathbb{Z}$

Show that $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$. [82]

Exercise

Although $\mathbb{Z}_2$ does not have any automorphisms the product group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ certainly does.

a.) Show that an automorphism of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ must be of the form

$$\phi(x_1, x_2) = (a_1 x_1 + a_2 x_2, a_3 x_3 + a_4 x_4) \tag{12.21}$$

where we are writing the group additively, and

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in GL(2, \mathbb{Z}_2) \tag{12.22}$$

b.) Show that $GL(2,\mathbb{Z}_2) \cong S_3$. [83]

[80] *Hint*: Consider the invertible matrix $A = \mathrm{i}1_{n\times n}$.

[81] *Answer*: No! Note that $(\mathrm{i}\sigma^k)^* = -\mathrm{i}(\sigma^k)^* = (\mathrm{i}\sigma^2)(\mathrm{i}\sigma^k)(\mathrm{i}\sigma^2)^{-1}$. But $\mathrm{i}\sigma^2 \in SU(2)$ and every $SU(2)$ matrix is a real linear combination of 1 and $\mathrm{i}\sigma^k$. This has an important implication for the representation theory of $SU(2)$: Every irreducible representation is either real or "pseudoreal" (quaternionic).

[82] *Answer*: The most general homomorphism $\mathbb{Z} \to \mathbb{Z}$ is the map $n \mapsto an$ for some integer a. But for an automorphism a must be mutliplicatively invertible in the integers. Therefore a is $+1$ or -1.

[83] *Hint*: Consider what the group does to the three nontrivial elements $(1,0)$, $(0,1)$, and $(1,1)$. The three transpositions correspond to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and the two elements of order 3 are $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

c.) Now describe $\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_4)$. [84]

Exercise *Automorphisms of $\mathbb{Z}_p^N$*

(Warning: This is hard and uses some other ideas from algebra.)

Let p be prime. Describe the automorphisms of $\mathbb{Z}_p^N$, and show that the group has order [85]

$$|\mathrm{Aut}(\mathbb{Z}_p^N)| = (p^N - 1)(p^N - p)(p^N - p^2) \cdots (p^N - p^{N-1}) \tag{12.23}$$

Exercise *Automorphisms Of The Quaternion Group*

♣This exercise should go later, perhaps in the section on extensions. Perhaps in the chapter on symmetries of regular objects. ♣

Show that the group of automorphisms of the quaternion group $Q = \{\pm 1, \pm \mathfrak{i}, \pm \mathfrak{j}, \pm \mathfrak{k}\}$ is isomorphic to S_4. [86]

(This assumes you know what the quaternions are. See below for various descriptions of the quaternion group Q.)

Exercise *Isomorphisms between two different groups*

Let G_1, G_2 be two groups which are isomorphic, but not presented as the same set with the same multiplication table. Let $\mathrm{Isom}(G_1, G_2)$ be the set of all isomorphisms from $G_1 \to G_2$.

Show that

a.) Any two isomorphisms $\Psi, \Psi' \in \mathrm{Isom}(G_1, G_2)$ are related by $\Psi' = \Psi \circ \phi$ where $\phi \in \mathrm{Aut}(G_1)$.

[84] *Answer*: This group has a homomorphism onto $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ with a kernel isomorphic to $\mathbb{Z}_2^4$.

[85] *Answer*: The group is the group of $N \times N$ invertible matrices over the ring $\mathbb{Z}_p$. These are in one-one correspondence with the possible bases for the vector space $\mathbb{Z}_p^N$. How many ordered bases are there? Note that any nonzero vector can serve as the first basis vector, and there are $p^N - 1$ nonzero vectors. Choose one and call it e_1. Now, e_2 can be any vector not in the linear span of e_1. But the linear span of e_1 is a one-dimensional subspace of p elements. These are all excluded so e_2 must be chosen from a set of $p^N - p$ vectors. Make a choice of e_2. Then e_3 must be chosen from a vector not in the span of e_1, e_2. The span of e_1, e_2 consists of p^2 vectors so there are $p^N - p^2$ choices for e_3, and so on.

[86] *Answer*: First, the group of inner automorphisms is $Q/Z(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. The three nontrivial elements are given by conjugation by $\mathfrak{i}, \mathfrak{j}, \mathfrak{k}$. Now, any automorphism must permute the three normal subgroups generated by $\mathfrak{i}, \mathfrak{j}, \mathfrak{k}$, and automorphisms leading to nontrivial permutations of normal subgroups must be outer. So the outer automorphism group must be a subgroup of S_3. Now, in fact, one can construct such outer automorphisms. In fact, it suffices to say what the image of $\mathfrak{i}$ and $\mathfrak{j}$ are since these generate the whole group. Thus, the automorphism group is an extension of S_3 by $\mathbb{Z}_2 \times \mathbb{Z}_2$ and one can then map this isomorphically to S_4.

b.) Any two isomorphisms $\Psi, \Psi' \in \mathrm{Isom}(G_1, G_2)$ are related by $\Psi' = \phi \circ \Psi$ where $\phi \in \mathrm{Aut}(G_2)$.

The set $Isom(G_1, G_2)$ with G_1, G_2 not equal but isomorphic is a good example of what is called a *torsor*. A *torsor* for a group G is a set X with a free transitive action.

12.1 The group of units in $\mathbb{Z}_N$

We have seen that $\mathbb{Z}/N\mathbb{Z}$ is a group inherited from the *additive* law on $\mathbb{Z}$. For an integer $n \in \mathbb{Z}$ denote its image in $\mathbb{Z}/N\mathbb{Z}$ by $\bar{n}$. With this notation the group law on $\mathbb{Z}/N\mathbb{Z}$ is

$$\bar{n}_1 + \bar{n}_2 = \overline{n_1 + n_2}, \tag{12.24}$$

and $\bar{0}$ is the unit element.

However, note that since

$$(n_1 + N\ell_1)(n_2 + N\ell_2) = n_1 n_2 + N\ell'' \tag{12.25}$$

we do have a well-defined operation on $\mathbb{Z}/N\mathbb{Z}$ inherited from *multiplcation* in $\mathbb{Z}$:

$$\bar{n}_1 \cdot \bar{n}_2 := \overline{n_1 \cdot n_2}. \tag{12.26}$$

In general, even if we omit $\bar{0}$, $\mathbb{Z}/N\mathbb{Z}$ is *not* a group with respect to the multiplication law (find a counterexample). Nevertheless, $\mathbb{Z}/N\mathbb{Z}$ with $+, \times$ is an interesting object which is an example of something called a *ring*. See the next chapter for a general definition of a ring.

Let us define *the group of units in the ring* $\mathbb{Z}/N\mathbb{Z}$:

$$(\mathbb{Z}/N\mathbb{Z})^* := \{\bar{m} : 1 \le m \le N-1, \gcd(m, N) = 1\} \tag{12.27}$$

where (m, N) is the *greatest common divisor* of m and N. We will also denote this group as $\mathbb{Z}_N^*$.

Then, $(\mathbb{Z}/N\mathbb{Z})^*$ *is* a group with the law (12.26) ! Clearly the multiplication is closed and $\bar{1}$ is the unit. The existence of multiplicative inverses follows from (11.8).

Moreover, as we have seen above, we can identify

$$\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^* \tag{12.28}$$

The isomorphism is that $a \in (\mathbb{Z}/N\mathbb{Z})^*$ is mapped to the transformation

$$\psi_a : n \ \mathrm{mod} N \to an \ \mathrm{mod} N \tag{12.29}$$

if we think of $\mathbb{Z}/N\mathbb{Z}$ additively or

$$\psi_a : \omega \to \omega^a \tag{12.30}$$

if we think of it multiplicatively. Note that $\psi_{a_1} \circ \psi_{a_2} = \psi_{a_1 a_2}$.

The order of the group $(\mathbb{Z}/N\mathbb{Z})^*$ is denoted $\phi(N)$ and is called the Euler ϕ-function or *Euler's totient function.* [87] One can check that

$$\begin{aligned}\phi(2) &= 1\\ \phi(3) &= 2\\ \phi(4) &= 2\end{aligned} \tag{12.31}$$

What can we say about the structure of $\mathbb{Z}_N^*$? Now, in general it is <u>not</u> true that $\mathrm{Aut}(G_1 \times G_2)$ and $\mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$ are isomorphic. Counterexamples abound. For example $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ but $\mathrm{Aut}(\mathbb{Z} \oplus \mathbb{Z}) \cong GL(2,\mathbb{Z})$. Nevertheless, it actually is true that $\mathrm{Aut}(\mathbb{Z}_n \times \mathbb{Z}_m) \cong \mathrm{Aut}(\mathbb{Z}_n) \times \mathrm{Aut}(\mathbb{Z}_m)$ when n and m are relatively prime. To prove this, let v_1 be a generator of $\mathbb{Z}_n$ and v_2 a generator of $\mathbb{Z}_m$ and let us write our Abelian group additively. The general endomorphism of $\mathbb{Z}_n \oplus \mathbb{Z}_m$ is of the form

$$\begin{aligned}v_1 &\to \alpha v_1 + \beta v_2\\ v_2 &\to \gamma v_1 + \delta v_2\end{aligned} \tag{12.32}$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Now impose the conditions $nv_1 = 0$ and $mv_2 = 0$ and the fact that $\bar{n}$ is multiplicatively invertible in $\mathbb{Z}_m$ and $\bar{m}$ is multiplicatively invertible in $\mathbb{Z}_n$ to learn that in fact an endomorphism must have $\beta = 0 \mathrm{mod}\ m$ and $\gamma = 0 \mathrm{mod}\ n$. Therefore $\beta v_2 = 0$ and $\gamma v_1 = 0$. Therefore, an automorphism of $\mathbb{Z}_n \oplus \mathbb{Z}_m$ is determined by $v_1 \to \alpha v_1$ with $\bar{\alpha} \in \mathbb{Z}_n^*$ and $v_2 \to \delta v_2$ with $\bar{\delta} \in \mathbb{Z}_m^*$ and hence $\mathrm{Aut}(\mathbb{Z}_n \oplus \mathbb{Z}_m) \cong \mathrm{Aut}(\mathbb{Z}_n) \times \mathrm{Aut}(\mathbb{Z}_m)$ when n and m are relatively prime. (The corresponding statement is absolutely false when they are not relatively prime.) So we have:

$$\mathbb{Z}_{nm}^* \cong \mathbb{Z}_n^* \times \mathbb{Z}_m^* \tag{12.33}$$

In particular, ϕ is a multiplicative function: $\phi(nm) = \phi(n)\phi(m)$ if $(n,m) = 1$. Therefore, if $N = p_1^{e_1} \cdots p_r^{e_r}$ is the decomposition of N into distinct prime powers then

$$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \cdots (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^* \tag{12.34}$$

Moreover, $(\mathbb{Z}/p^e\mathbb{Z})^*$ is of order $\phi(p^e) = p^e - p^{e-1}$, as is easily shown [88] and hence

$$\phi(N) = \prod_i (p_i^{e_i} - p_i^{e_i - 1}) = N \prod_{p|N} (1 - \frac{1}{p}) \tag{12.35}$$

Remark: For later reference in our discussion of cryptography note one consequence of this: If we choose, randomly - i.e. with uniform probability density - a number between 1 and N the probability that it will be relatively prime to N is

$$\frac{\phi(N)}{N} = \prod_{p|N} (1 - \frac{1}{p}) \tag{12.36}$$

[87] Do not confuse $\phi(N)$ with the ϕ_a above!

[88] Proof: The numbers between 1 and p^e which have gcd larger than one must be of the form px where $1 \le x \le p^{e-1}$. So the rest are relatively prime.

This means that, if N is huge and a product of just a few primes, then a randomly chosen number will almost certainly be relatively prime to N.

In elementary number theory textbooks it is shown that if p is an odd prime then $(\mathbb{Z}/p^e\mathbb{Z})^*$ is a cyclic group.

♣Finish proof for $e > 1$. ♣

To prove this let us begin with $(\mathbb{Z}/p\mathbb{Z})^*$. (This proof uses some ideas from the algebra of fields.) Suppose this group were <u>not</u> cyclic. Then there would be some n which is a nontrivial divisor of the order, $\phi(p) = p - 1$ such that $x^n = 1$ for all $x \in (\mathbb{Z}/p\mathbb{Z})^*$. That would imply that in the field $\mathbb{F}_p$ the equation $x^n - 1$ would have $p - 1$ distinct roots. On the other hand, the equation $x^n - 1$ can have at most n roots, and that is a contradiction. We conclude that, in fact,$(\mathbb{Z}/p\mathbb{Z})^*$ must be cyclic.

Of course, all primes are odd, and two is the oddest prime of all. If $p = 2$ the result is a little different and we have:

$$(\mathbb{Z}/4\mathbb{Z})^* \cong \{\pm 1\} \tag{12.37}$$

is cyclic but

$$(\mathbb{Z}/2^e\mathbb{Z})^* = \{(-1)^a 5^b | a = 0, 1, 0 \leq b < 2^{e-2}\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{e-2}\mathbb{Z}) \tag{12.38}$$

when $e \geq 3$.

In fact, more generally, it turns out that $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic iff $n \in \{1, 2, 4, p^k, 2p^k\}$ where p runs over odd primes and $k > 0$.

Note that if we take a product of two distinct odd prime powers then

$$(\mathbb{Z}/(p_1^{k_1} p_2^{k_2}\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^* \tag{12.39}$$

But $\phi(p_1^{k_1})$ and $\phi(p_2^{k_2})$ are both even, being divisible by $p_1 - 1$ and $p_2 - 1$, respectively, and hence are not relatively prime, and hence $(\mathbb{Z}/(p_1^{k_1} p_2^{k_2}\mathbb{Z})^*$ is not cyclic.

Examples

1. $(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}\mathrm{mod}7 \cong \mathbb{Z}_6$. Note that 3 and 5 are generators:

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1 \qquad \mathrm{mod}7 \tag{12.40}$$

$$5^1 = 5, \quad 5^2 = 4, \quad 5^3 = 6, \quad 5^4 = 2, \quad 5^5 = 3, \quad 5^6 = 1 \qquad \mathrm{mod}7 \tag{12.41}$$

   However, $2 = 3^2\mathrm{mod}7$ is *not* a generator, even though it is prime. Rather, it generates an index 2 subgroup $\cong \mathbb{Z}_3$, as does 4, while 6 generates an index 3 subgroup $\cong \mathbb{Z}_2$. Do not confuse this isomorphic copy of $\mathbb{Z}_6$ with the additive presentation $\mathbb{Z}_6 \cong \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$ with the *additive* law. Then 1 and 5 are generators, but not $2, 3, 4$.

2. $(\mathbb{Z}/9\mathbb{Z})^* = \{1, 2, 4, 5, 7, 8\}\mathrm{mod}9 \cong \mathbb{Z}_6$. It is a cyclic group generated by 2 and $2^5 = 5\mathrm{mod}9$, but it is not generated by $2^2 = 4$, $2^3 = 8$ or $2^4 = 7\mathrm{mod}9$, because $2, 3, 4$ are not relatively prime to 6.

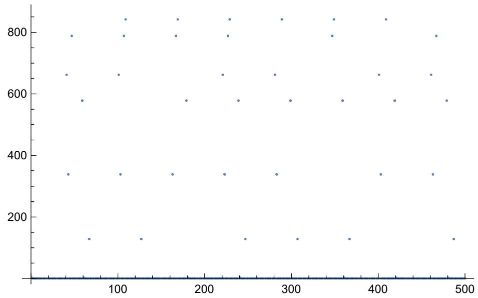

Figure 23: A plot of the residues of $2^x \delta_x$ modulo $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$, for $1 \leq x \leq 500$. Here $\delta_x = 0$ if $gcd(x, N) > 1$ so that we only see the values in $(\mathbb{Z}/N\mathbb{Z})^*$. Notice the apparently random way in which the value jumps as we increase x.

3. $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Note that $3^2 = 5^2 = 7^2 = 1 \text{mod} 8$ and $3 \cdot 5 = 7 \text{mod} 8$, so we can take 3 and 5 to be the generators of the two $\mathbb{Z}_2$ subgroups.

4. $(\mathbb{Z}/15\mathbb{Z})^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

Remarks

1. When $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic a generator is called a *primitive root modulo n*, and is not to be confused with a primitive n^{th} root of one. It is trivial to find examples of the latter and highly nontrivial to find examples of the former.

2. The values of $f(x) = a^x \text{mod} N$ for $(a, N) = 1$ appear to jump about randomly as a function of x, as shown in Figure 23. Therefore, finding the period of this function, that is, the smallest positive integer r so that $f(x + r) = f(x)$ is not easy. This is significant because of the next remark.

3. *Factoring Integers*. Suppose N is a positive integer and a is a positive integer so that $(a, N) = 1$, and the order, denoted r, of $\bar{a} \in (\mathbb{Z}/N\mathbb{Z})^*$ is <u>even</u> and finally suppose that $b := a^{r/2} \neq \pm 1 \text{mod} N$. Note that $b^2 = 1 \text{mod} N$ so $\bar{b}$ is a nontrivial squareroot of $\bar{1} \in (\mathbb{Z}/N\mathbb{Z})^*$. Then we claim that $d_\pm := gcd(b \pm 1, N)$ are in fact <u>nontrivial</u> factors of N. To see this we need to rule out $d_\pm = 1$ and $d_\pm = N$, the trivial factors of N. If we had $d_\pm = N$ then N would divide $b \pm 1$ but that would imply $b = \mp 1 \text{mod} N$, contrary to assumption. Now, suppose $d_\pm = 1$, then by Bezout's theorem there would be integers $\alpha_\pm, \beta_\pm$ so that

$$(b \pm 1)\alpha_\pm + N\beta_\pm = 1 \tag{12.42}$$

But then multiply the equation by $b \mp 1$ to get

$$(b^2 - 1)\alpha_\pm + N\beta_\pm(b \mp 1) = b \mp 1 \tag{12.43}$$

But now, N divides the LHS so $b \mp 1 = 0 \text{mod} N$ which implies $b = \pm 1 \text{mod} N$, again contrary to assumption. Thus, $d_\pm$ are <u>nontrivial</u> divisors of N.

To give a concrete example, take $N = 3 \cdot 5 \cdot 7 = 105$, so $\phi(N) = 48$. Then the period of $f(x) = 2^x$ is $r = 12$, and $b = 2^{12/2} = 64$. Well $gcd(64 + 1, 105) = 5$ and $gcd(64 - 1, 105) = 21$ are both divisors of 105. In fact $105 = 5 \cdot 21$.

4. *Artin's Conjecture*: Finding a generator is not always easy, and it is related to some deep conjectures in number theory. For example, the Artin conjecture on primitive roots states that for any positive integer a which is not a perfect square there are an infinite number of primes so that $\bar{a}$ is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. In fact, if a is not a power of another integer, and the square-free part of a is not 1mod4 then Artin predicts the density of primes for which a is a generator to be

$$\prod_{Artin\ primes} \left(1 - \frac{1}{p(p-1)}\right) = 0.37.... \tag{12.44}$$

According to the Wikipedia page, there is not a single number a for which the conjecture is known to be true. For example, the primes $p < 500$ for which $a = 2$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ is

$$\{3,5,11,13,19,29,37,53,59,61,67,83,101,107,131,139,149,163,173,179,181, 197,211,227,269,293,317,347,349,373,379,389,419,421,443,461,467,491\} \tag{12.45}$$

5. A good reference for this material is Ireland and Rosen, *A Classical Introduction to Modern Number Theory* Springer GTM

Exercise *Euler's theorem and Fermat's little theorem*

a.) Let G be a finite group of order n. Show that if $g \in G$ then $g^n = e$ where e is the identity element.

b.) Prove *Euler's theorem*: For all integers a relatively prime to N, $g.c.d(a, N) = 1$,

$$a^{\phi(N)} = 1 \text{mod} N \tag{12.46}$$

Note that a special case of this is Fermat's little theorem: If a is an integer and p is prime then

$$a^p = a \text{mod} p \tag{12.47}$$

Remark: This theorem has important practical applications in *prime testing.* If we want to test whether an odd integer n is prime we can compute $2^n \text{mod} n$. If the result is $\neq 2 \text{mod} n$ then we can be sure that n is not prime. Now $2^n \text{mod} n$ can be computed *much* more quickly with a computer than the traditional test of seeing whether the primes up to $\sqrt{n}$ divide n. If $2^n \text{mod} n$ is indeed $= 2 \text{mod} n$ then we can suspect that n is prime. Unfortunately, there are composite numbers which will masquerade as primes in this test. They are called "base 2 pseudoprimes." In fact, there are numbers n, known as *Carmichael numbers* which satisfy $a^n = a \text{mod} n$ for all integers a. The good news is that they are rare. The bad news is that there are infinitely many of them. According to Wikipedia the first few Carmichael numbers are

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, \dots, \tag{12.48}$$

The first Carmichael number is $561 = 3 \cdot 11 \cdot 17$ and Erdös proved that the number $C(X)$ of Carmichael numbers smaller than X is bounded by

$$C(X) < X \text{exp} \left(- \frac{\kappa \text{log} X \text{logloglog} X}{\text{loglog} X} \right) \tag{12.49}$$

where κ is a positive real number.

Exercise *Periodic Functions*

a.) Consider the function

$$f(x) = 2^x \text{mod } N \tag{12.50}$$

for an odd integer N. Show that this function is periodic $f(x+r) = f(x)$ for a minimal period r which divides $\phi(N)$.

b.) Compute the period for $N = 15, 21, 105$. [89]

c.) More generally, if $(a, N) = 1$ show that $f(x) = a^x$ mod N is a periodic function.

Exercise *How Many Primitive Roots Of n Are There?*

Show that n has either zero or $\phi(\phi(n))$ different primitive roots.

12.2 Group theory and cryptography

Any invertible map $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ can be used to define a code. For example, if $N = 26$ we may identify the elements in $\mathbb{Z}/26\mathbb{Z}$ with the letters in the Latin alphabet:

$$a \leftrightarrow \bar{0}, b \leftrightarrow \bar{1}, c \leftrightarrow \bar{2}, \dots \tag{12.51}$$

Exercise *Caesar Shift*

a.) Show that $f(m) = (m-3)\text{mod}26$ defines a code. In fact, the above remark, and this example in particular, is attributed to Julius Caesar. Using this decode the message:

$$ZOLPPQEBORYFZLK! \tag{12.52}$$

b.) Is $f(m) = (3m)\text{mod}26$ a valid code? By adding symbols or changing the alphabet we can change the value of N above. Is $f(m) = (3m)\text{mod}27$ a valid code?

The RSA public key encryption system is a beautiful application of Euler's theorem and works as follows. The basic idea is that with numbers with thousands of digits it is relatively easy to compute powers $a^n\text{mod}m$ and greatest common divisors, but it is very difficult to factorize such numbers into their prime parts. For example, for a 1000 digit number the brute force method of factorization requires that we sample up to

$$\sqrt{10^{1000}} = 10^{500} \tag{12.53}$$

[89] *Answer*: $r = 4, 6, 12$ divides $\phi(N) = 8, 12, 48$.

divisors. Bear in mind that our universe is about $\pi \times 10^7 \times 13.79 \times 10^9 \cong 4 \times 10^{17}$ seconds old. [90] There are of course more efficient algorithms, but all the publicly known ones are still far too slow.

Now, Alice wishes to receive and decode secret messages sent by any member of the public. She chooses two large primes (thousands of digits long) p_A, q_A and computes $n_A := p_A q_A$. These primes are to be kept secret. How does she find her secret thousand-digit primes? She chooses a random thousand digit number and applies the Fermat primality test. By the prime number theorem she need only make a few thousand attempts, and she will find a prime. [91]

Next, Alice computes $\phi(n_A) = (p_A - 1)(q_A - 1)$, and then she chooses a random thousand-digit number d_A such that $gcd(d_A, \phi(n_A)) = 1$ and computes an inverse $d_A e_A = 1 \mathrm{mod} \phi(n_A)$. All these steps are relatively fast and easy, because Euclid's algorithm is very fast. Thus there is some integer f so that

$$d_A e_A - f\phi(n_A) = 1 \tag{12.54}$$

That is, she solves the congruence $x = 1\mathrm{mod}\phi(n_A)$ and $x = 0\mathrm{mod} d_A$, for the smallest positive x and then computes $e_A = x/d_A$.

Finally, she publishes for the world to see the encoding key: $\{n_A, e_A\}$, but she keeps the numbers $p_A, q_A, \phi(n_A), d_A$ secret. This means that if anybody, say Bob, wants to send Alice a secret message then he can do the following:

Bob converts his plaintext message into a number less than n_A by writing $a \leftrightarrow 01$, $b \leftrightarrow 02$, ..., $z \leftrightarrow 26$. (Thus, when reading a message with an odd number of digits we should add a 0 in front. If the message is long then it should be broken into pieces of length smaller than n_A.) Let Bob's plaintext message thus converted be denoted m. It is a positive integer smaller than n_A.

Now to compute the ciphertext Bob looks up Alice's numbers $\{n_A, e_A\}$ on the public site and uses these to compute the ciphertext:

$$c := m^{e_A} \mathrm{mod} n_A \tag{12.55}$$

Bob sends the ciphertext c to Alice over the internet. Anyone can read it.

Then Alice can decode the message by computing

$$\begin{aligned} c^{d_A} \mathrm{mod} n_A &= m^{e_A d_A} \mathrm{mod} n_A \\ &= m^{1+f\phi(n_A)} \mathrm{mod} n_A \\ &= m \mathrm{mod} n_A \end{aligned} \tag{12.56}$$

Thus, to decode the message Alice just needs one piece of private information, namely the integer d_A.

[90] There are $\pi \times 10^7$ seconds in a year, to 0.3% accuracy.

[91] The prime number theorem says that if $\pi(x)$ is the number of primes between 1 and x then as $x \to \infty$ we have $\pi(x) \sim \frac{x}{\mathrm{log} x}$. Equivalently, the n^{th} prime is asymptotically like $p_n \sim n \mathrm{log} n$. This means that the density of primes for large x is $\sim 1/\mathrm{log} x$, so if $x \sim 10^n$ then the density is $1/n$ so if we work with thousand-digit primes then after about one thousand random choices we will find a prime.

Now Eve, who has a reputation for making trouble, cannot decode the message without knowing d_A. Just knowing n_A and e_A but not the prime factorization $n_A = p_A q_A$ there is no obvious way to find d_A. The reason is that even though the number n_A is public it is hard to compute $\phi(n_A)$ without knowing the prime factorization of n_A. Of course, if Eve finds out about the prime factorization of n_A then she can compute $\phi(n_A)$ immediately and then quickly (using the Euclidean algorithm) invert e_A to get d_A. Thus, the security of the method hinges on the inability of Eve to factor n_A into primes.

In summary,

1. The <u>intended receiver</u> of the message, namely Alice in our discussion, knows

$$(p_A, q_A, n_A = p_A q_A, \phi(n_A) = (p_A - 1)(q_A - 1), e_A, d_A). \tag{12.57}$$

2. Alice publishes (n_A, e_A). Anybody can look these up.

3. The <u>sender</u> of the message, namely Bob in our discussion, takes a secret message m_B and computes the ciphertext $c = m_B^{e_A} \mathrm{mod} n_A$.

4. Alice can decode Bob's message by computing $m_B = c^{d_A} \mathrm{mod} n_A$ using her secret knowledge of d_A.

5. The <u>attacker</u>, namely Eve in our discussion, knows (n_A, e_A, c) but will have to work to find d_A or some other way of decoding the ciphertext.

Remarks

1. Note that the decoding will *fail* if m and n_A have a common factor. However, $n_A = p_A q_A$ and p_A, q_A are primes with thousands of digits. The probability that Bob's message is one of these is around 1 in 10^{1000}.

Exercise *Your turn to play Eve*
Alice has published the key

$$(n = 661643, e = 325993) \tag{12.58}$$

Bob sends her the ciphertext in four batches:

$$c_1 = 541907 \quad c_2 = 153890 \quad c_3 = 59747 \quad c_4 = 640956 \tag{12.59}$$

What is Bob's message? [92]

---

[92] Factor the integer $n = 541 * 1223$. Then you know p, q and hence $\phi(n) = 659880$. Now take e and compute d by using the Chinese Remainder theorem to compute $x = 1 \mathrm{mod} \phi$ and $x = 0 \mathrm{mod} e$. This gives $x = 735766201 = de$ and hence $d = 2257$. Now you can compute the message from the ciphertext $m = c^d \mathrm{mod} n$.

12.2.1 How To Break RSA: Period Finding

The attacker, Eve, can read the ciphertext $c\text{mod}n_A$. That means the attacker can try to compute the period of the function

$$f(x) := c^x \text{mod} n_A \tag{12.60}$$

Suppose (as is extremely likely when n_A is a product of two large primes) that c is relatively prime to n_A. Then the cyclic group $\langle c \rangle \in (\mathbb{Z}/n_A\mathbb{Z})^*$ generated by c must coincide with the cyclic group generated by the message m_B and in particular they both have the same period r, which divides $\phi(n_A)$. Suppose Eve figures out the period r. Since the published value e_A is relatively prime to $\phi(n_A)$ it will be relatively prime to r and therefore there exists a new decoding method: Compute d_E such that

$$e_A d_E = 1 \text{ mod } r \tag{12.61}$$

Then

$$c^{d_E} = m^{e_A d_E} \text{mod} n_A = m_B^{1+\ell r} \text{mod} n_A = m_B \text{mod} n_A \tag{12.62}$$

decodes the message.

Thus, if the attacker can find the period of $f(x)$ the message can be decoded.

Another way in which finding the period leads to rapid decoding is through explicit factoring:

We saw in our discussion of $\mathbb{Z}_N^*$ that, if one has an element $\bar{a} \in \mathbb{Z}_N^*$ with even period r and $\bar{b} = \bar{a}^{r/2} \neq \overline{\pm 1}$ then $d_\pm = gcd(b \pm 1, N)$ are nontrivial factors of N. Suppose there were a quick method to find the period r. Then we could quickly factor N as follows:

1. Choose a random integer a and using Euclid check that $(a, N) = 1$. If N is a product of two large primes you will only need to make a few choices of a before succeeding.

2. Compute the period r of the function $f(x) = a^x \text{mod} N$.

3. If r is odd go back and choose another a until you get one with r even.

4. Then check that $b = a^{r/2} \neq -1\text{mod}N$. Again this can be done quickly, thanks to Euclid. If you get $b = -1\text{mod}N$ go back and choose another a, until you find one that works. The point is that, with high probability, if you pick a at random you will succeed. So you might have a try a few times, but not many.

So, the only real bottleneck in factoring N is computing the order r of $\bar{a}$ in $\mathbb{Z}_N^*$. Equivalently, this is computing the period of the function $f(x) = a^x \text{ mod } N$ where $(a, N) = 1$. This is where the "quantum Fourier transform" and "phase estimation" come in. Quantum computers give a way to compute this period in polynomial time in N, as opposed to classical computers which take exponential time in N. We will come back to this.

12.2.2 Period Finding With Quantum Mechanics

♣This section is out of place. Goes later in the course ♣

Here we sketch how quantum computation allows one to find the period of the function $f(x) = a^x \text{mod} N$ where $(a, N) = 1$. This is just a sketch. A nice and clear and elementary account (which we used heavily) can be found in D. Mermin's book *Quantum Computer Science* and more details and a more leisurely discussion can be found there.

Quantum computation is based on the action of certain unitary operators on a system of n Qbits, that is, on a Hilbert space

$$\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n} \tag{12.63}$$

equipped with the standard inner product. For each factor $\mathbb{C}^2$ one chooses a basis $\{|0\rangle, |1\rangle\}$, which one should think of as, for example spin up/down eigenstates of an electron or photon helicity polarization states. Then there is a natural basis for $\mathcal{H}_n$:

$$|\vec{x}\rangle := |x_{n-1}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle \tag{12.64}$$

Here, for each i, $x_i \in \{0,1\}$. One can identify the vector $\vec{x} \in \mathbb{F}_2^n$, the n-dimensional vector space over the field $\mathbb{F}_2$. In our discussion we will only use its Abelian group structure, so one can also think of it as $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$ with n summands. The basis of states (12.64) is known as the *computational basis* or, the *Classical basis*. Now to each computational basis vector we can assign an integer by its binary expansion:

$$N(\vec{x}) := 2^{n-1}x_{n-1} + \cdots + 2^2 x_2 + 2^1 x_1 + x_0 \tag{12.65}$$

Now, let $N := 2^n$. We can also define the Hilbert space $L^2(\mathbb{Z}_N)$ of functions on the group $\mathbb{Z}_N$ with the natural Haar measure. Of course $\mathcal{H}_n$ is isomorphic to $L^2(\mathbb{Z}_N)$ and the isomorphism we choose to use is the one which identifies the computational basis vector $|\vec{x}\rangle$ with the delta function supported at $N(\vec{x})\mathrm{mod}\ N$. We will denote the latter states as $|N(\vec{x})\rangle\rangle_N$, where the subscript indicates which Abelian group $\mathbb{Z}_N$ we are working with.

In quantum computation one works with a Hilbert space decomposed as

$$\mathcal{H} = \mathcal{H}_{input} \otimes \mathcal{H}_{output} \tag{12.66}$$

The two factors have dimension $N_{in} = 2^{n_{in}}$ and $N_{out} = 2^{n_{out}}$, respectively. The quantum gates are unitary operators and, moreover, under identification of $\mathcal{H}$ as a tensor product of Qbits there should be a notion of “locality” in the sense that they only act nontrivially on “a few” adjacent factors. The locality reflects the spatial locality in some realization in the lab in terms of, say, spin systems. Moreover, we should only have to apply “ a few” quantum gates in a useful circuit. With an arbitrary number of gates we can construct any unitary out of products of local ones to arbitrary accuracy. The above notions can be made precise, but that is beyond the scope of this section.

♣Still, it is essential to explain more about the notion of “local quantum gate” and quantum circuit and illustrate a few examples of simple gates. ♣

Now suppose we have a function

$$f : (\mathbb{Z}_N)^* \to (\mathbb{Z}_N)^* \tag{12.67}$$

(such as $f(x) = a^x \mathrm{mod} N$ for $(a,N) = 1$). We would like to convert this to a map

$$\check{f} : \mathbb{F}_2^{n_{in}} \to \mathbb{F}_2^{n_{out}} \tag{12.68}$$

We now choose a fundamental domain which is a subset of $\{1, 2, \ldots, N-1\}$ for $(\mathbb{Z}_N)^*$ with $N < N_{out}$ and $N < N_{in}$ (in fact we will eventually assume $N \ll N_{out}$ and $N \ll N_{in}$) so that we can view elements of $(\mathbb{Z}/N\mathbb{Z})^*$ as elements of the set $\{1, 2, \ldots, N-1\}$ which is, in turn, a subset of $\mathbb{Z}/N_{in}\mathbb{Z}$ and $\mathbb{Z}/N_{out}\mathbb{Z}$. We use the function $N(\vec{x})$ above to define $\check{f}$ such that

$$f(N(\vec{x})) = N(\check{f}(\vec{x}))\text{mod}2^{n_{out}} \tag{12.69}$$

This does not uniquely specify $\check{f}$ but the ambiguity will not affect the discussion. To read this equation, suppose you want to compute $\check{f}(\vec{x})$ for some $\vec{x} \in \mathbb{F}_2^{n_{in}}$. Then you compute $N(\vec{x})$ which is a nonnegative integer between 0 and N_{in}. Then you reduce it modulo N. If it is relatively prime to N you can compute $f(N(\vec{x}))$ and considerate the result as a number between 1 and $2^{n_{out}} - 1$. The above equation then pins down $\check{f}(\vec{x})$. Using $\check{f}$ we can define a unitary operator U_f by its action on the computational basis:

♣And what if $N(\vec{x})$ is not relatively prime to N? Of course, we are thinking this is rare, but it can happen. What is the best way to extend the function? ♣

$$U_f : |\vec{x}\rangle \otimes |\vec{y}\rangle \to |\vec{x}\rangle \otimes |\vec{y} + \check{f}(\vec{x})\rangle \tag{12.70}$$

where on the right-hand side addition is in the Abelian group $(\mathbb{Z}_2)^{n_{out}}$. We will say that the function f *is nice* if U_f can be implemented with a "reasonable" number of local unitary gates. (Of course, one could make this notion much more precise.)

A good example of a local unitary operator on a Qbit is the *Hadamard gate* that acts by

$$\begin{aligned} H : |0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H : |1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{12.71}$$

This can be summarized by the formula

$$H|y\rangle = \frac{1}{\sqrt{2}}\sum_x (-1)^{xy}|x\rangle \tag{12.72}$$

So,

$$H^{\otimes n}|\vec{y}\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{\vec{x}\in\mathbb{F}_2^n} (-1)^{\vec{x}\cdot\vec{y}}|\vec{x}\rangle \tag{12.73}$$

and in particular

$$H^{\otimes n}|\vec{0}\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{\vec{x}\in\mathbb{F}_2^n} |\vec{x}\rangle \tag{12.74}$$

Therefore, (recall that double brackets $|j\rangle\rangle$ refer to the position basis in $L^2(\mathbb{Z}_N)$) we have

$$U_f\left(H^{\otimes n_{in}} \otimes 1\right) : |0\rangle_{in} \times |0\rangle_{out} \to \left(\frac{1}{\sqrt{2}}\right)^{n_{in}} \sum_{j\in\mathbb{Z}_{N_{in}}} |j\rangle\rangle_{N_{in}} \otimes |f(j)\rangle\rangle_{N_{out}} \tag{12.75}$$

Now we wish to apply this to the function $f(x) = a^x$ mod N with $(a, N) = 1$ and N is the number we would like to factorize. So, in particular we don't want $N = 2^n$ for some n. Nobody will be impressed if you can factor a power of two! Rather, we identify the group $\mathbb{Z}_N^*$, as a set, with the integers $\{1, \ldots, N-1\}$ so that it can be considered to be a subset of the natural fundamental domain $\{0, \ldots, N_{in} - 1\}$ for $\mathbb{Z}_{N_{in}}$, and similarly for

$\mathbb{Z}_{N_{out}}$. Then to compute f we compute a^x, take the residue modulo N to get an integer in the fundamental domain, and then consider that number modulo N_{out}. Hence, we should choose $N_{out} = 2^{n_{out}}$ to be some integer larger than N. A key claim, explained in textbooks on quantum information theory is that such a function f is nice. That is, it makes sense to compute it with a quantum circuit.

So, we conclude that a suitable quantum circuit can implement:

$$\begin{aligned} U_f\left(H^{\otimes n} \otimes 1\right) : |0\rangle_{N_{in}} \times |0\rangle_{N_{out}} \to \left(\frac{1}{\sqrt{2}}\right)^{n_{in}} \sum_{k \in \mathbb{Z}_{N_{in}}} |k\rangle\rangle_{N_{in}} \otimes |a^k\rangle\rangle_{N_{out}} \\ = \left(\frac{1}{\sqrt{2}}\right)^{n_{in}} \sum_{f_0 \in \mathbb{Z}_N^*}{}' \left(|j_0\rangle\rangle_{N_{in}} + |j_0 + r\rangle\rangle_{N_{in}} + |j_0 + 2r\rangle\rangle_{N_{in}} + \cdots\right) \otimes |f_0\rangle\rangle_{N_{out}} \end{aligned} \tag{12.76}$$

In the second line we are considering $\mathbb{Z}_N^*$ as a subset of $\mathbb{Z}_{N_{out}}$ as explained above and the prime on the sum means that we are just summing over the values that are in the image of $f(x) = a^x \text{mod } N$. This will be all the values in $\mathbb{Z}_N^*$ if a is a generator of $\mathbb{Z}_N^*$ but in general might be smaller. Also, j_0 is some solution of $f_0 = a^{j_0} \bmod N$, and r is the period of $f(x)$, that is, the smallest positive integer so that $f(x+r) = f(x)$ for all x. We can choose j_0 so that $0 \le j_0 < r$ and write the RHS of (12.76) as

$$\Psi = \left(\frac{1}{\sqrt{2}}\right)^{n_{in}} \sum_{0 \le j_0 < r} \left(\sum_{s=0}^{\mathcal{O}-1} |j_0 + sr\rangle\rangle_{N_{in}}\right) \otimes |a^{j_0}\rangle\rangle_{N_{out}} \tag{12.77}$$

Here $\mathcal{O}$ is the smallest integer such that $j_0 + \mathcal{O}r \ge N_{in}$. So

$$\mathcal{O} = \lfloor \frac{N_{in} - j_0}{r} \rfloor \tag{12.78}$$

In the applications we have in mind N_{in} and r are typically very large numbers so that this is a (very weak) function of j_0. At the end of this section we will use the observation that in this case, $r\mathcal{O}/N_{in}$ is, to very good accuracy, just equal to 1.

Now we measure the output system and get some result, say, $f_0 = a^{k_0} \text{mod} N$. Applying the usual Born rule we get the state for the input system

$$P_{f_0}(\Psi) = \frac{1}{\sqrt{\mathcal{O}}} \sum_{s=0}^{\mathcal{O}-1} |k_0 + sr\rangle\rangle_{N_{in}} \tag{12.79}$$

It is some kind of plane wave state in $L^2(\mathbb{Z}_N)$, so measuring position will give no useful information on r. Of course, we should therefore go to the Fourier dual basis to learn about the period. In terms of the position basis of $L^2(\mathbb{Z}_N)$ we can apply V_{FT} to get:

$$V_{FT} P_{f_0} \Psi = \frac{1}{\sqrt{N_{in}\mathcal{O}}} \sum_{p \in \mathbb{Z}_{N_{in}}} \sum_{s=0}^{\mathcal{O}-1} e^{2\pi \mathrm{i} \frac{(k_0 + sr)p}{N_{in}}} |p\rangle\rangle_{N_{in}} \tag{12.80}$$

Note that this Fourier transform is quite nontrivial and nontransparent in the computational basis because of the nontrivial isomorphism between $\mathcal{H}_n$ and $L^2(\mathbb{Z}_N)$ with $N = 2^n$.

Nevertheless, and this is nontrivial and part of the magic of Shor's algorithm, the Fourier transform operator V_{FT} can be implemented nicely with quantum gates in the computational basis. Again, the textbooks on quantum information theory give explicit construction of V_{FT} as a quantum circuit in the computational basis. It is exactly at this point that the exponential speed-up of the period finding takes place:

1. Classical Fourier Transform: $N^2 = 2^{2n}$ operations. We learn every Fourier coefficient.

2. Fast Fourier Transform: $nN = n2^n$ operations. We learn every Fourier coefficient.

3. Quantum Fourier Transform: n^2 quantum gates. We only learn about correlations of the output state.

Now to find the period we make a measurement of the amplitudes for the various Fourier components $|p\rangle\rangle_{N_{in}}$. (Here we are using the isomorphism between $\mathbb{Z}_{N_{in}}$ and its unitary dual.) The probability to measure p is

$$\begin{aligned} Prob(p) &= \frac{1}{N_{in}\mathcal{O}} |\sum_{s=0}^{\mathcal{O}-1} (e^{2\pi \mathrm{i} \frac{p}{N_{in}/r}})^s|^2 \\ &= \frac{1}{N_{in}\mathcal{O}} \frac{\sin^2\left(\pi \cdot p \cdot \frac{\mathcal{O}r}{N_{in}}\right)}{\sin^2\left(\pi \cdot p \cdot \frac{r}{N_{in}}\right)} \end{aligned} \tag{12.81}$$

The basic idea is that the probability, as a function of p, will be peaked near values of p from which we can deduce the crucial number r, but we need to be a bit careful at this point.

Let us ask what is the probability that we will measure a value p of the form

$$p_j = j\frac{N_{in}}{r} + \delta_j \qquad\qquad |\delta_j| \leq 1/2 \tag{12.82}$$

If p_j is of this form with any value $j = 1, \dots, r-1$ then we can extract r. Thus, substituting such a value for p_j into the formula for the probability we have

$$\frac{1}{N_{in}\mathcal{O}} \frac{\sin^2\left(\pi \cdot \delta_j \cdot \frac{\mathcal{O}r}{N_{in}}\right)}{\sin^2\left(\pi \cdot \delta_j \cdot \frac{r}{N_{in}}\right)} \tag{12.83}$$

Now recall that $\mathcal{O}r/N_{in}$ is equal to 1 to excellent accuracy. Suppose we also choose a number of Qbits so that

$$N_{in} \gg N > r \tag{12.84}$$

Then the argument of the sign in the denominator is extremely small and we can replace $\sin(x)$ by x. So we get:

$$\begin{aligned} Prob(p_j) &\cong \frac{1}{N_{in}\mathcal{O}} \frac{\sin^2(\pi\delta_j)}{\left(\pi \cdot \delta_j \cdot \frac{r}{N_{in}}\right)^2} \\ &= \frac{N_{in}}{r\mathcal{O}} \cdot \frac{1}{r} \left(\frac{\sin \pi\delta_j}{\pi\delta_j}\right)^2 \\ &\cong \frac{1}{r} \left(\frac{\sin \pi\delta_j}{\pi\delta_j}\right)^2 \end{aligned} \tag{12.85}$$

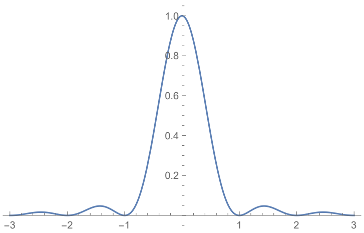

Figure 24: A plot of the function $\sin^2(\pi x)/(\pi x)^2$ as a function of x. This function, very familiar from the theory of diffraction, is symmetric in $x \to -x$ and monotonically decreasing in the interval $0 \le x \le 1/2$. It therefore takes its minimal value in this interval at $x = 1/2$ where it is about $\cong 0.405$.

Now for $0 \le \delta \le \pi/2$ we have $\frac{\sin x}{x} \ge \frac{2}{\pi}$ so

$$\sum_j Prob(p_j) \ge \frac{r-1}{r}\frac{4}{\pi^2} \cong 0.4 \tag{12.86}$$

Now, using various tricks one can raise this 40% value to near 100%. For these tricks consult Mermin's book. Two other useful textbooks on quantum information theory and quantum computing where one can look these things up include:

1. Nielsen and Chuang, Quantum Information Theory
2. A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Grad Studies in Math 47, AMS
3. J. Preskill, lecture notes at http://www.theory.caltech.edu/∼preskill/ph219/ph219-2019-20

13. Semidirect Products

We have seen a few examples of direct products of groups above. We now study a more subtle notion, the semidirect product. The semidirect product is a twisted version of the direct product of groups H and G which can be defined once we are given one new piece of extra data. The new piece of data we need is a homomorphism

$$\alpha : G \to \mathrm{Aut}(H). \tag{13.1}$$

For an element $g \in G$ we will denote the corresponding automorphism by α_g. The value of α_g on an element $h \in H$ is denoted $\alpha_g(h)$. Thus $\alpha_g(h_1 h_2) = \alpha_g(h_1)\alpha_g(h_2)$ because α_g is a homomorphism of H to itself while we also have $\alpha_{g_1 g_2}(h) = \alpha_{g_1}(\alpha_{g_2}(h))$ because α is a homomorphism of G into the group of automorphisms $\mathrm{Aut}(H)$. We also have that α_1 is the identity automorphism. (Prove this!)

Using the extra data given by α we can form a more subtle kind of product called the **semidirect product** $H \rtimes G$, or $H \rtimes_\alpha G$ when we wish to stress the role of α. In the math literature on group theory the notation $H : G$ is also used. This group is the Cartesian product $H \times G$ as a *set* but has the "twisted" multiplication law:

$$(h_1, g_1) \cdot (h_2, g_2) := (h_1 \alpha_{g_1}(h_2), g_1 g_2) \tag{13.2}$$

A good intuition to have is that "as g_1 moves from left to right across the h_2 they interact via the action of g_1 on h_2."

Exercise *Due diligence*

a.) Show that (13.2) defines an associative group law.

b.) Show that $(1_H, 1_G)$ defines the unit and

$$(h, g)^{-1} = \left(\alpha_{g^{-1}}(h^{-1}), g^{-1}\right) \tag{13.3}$$

c.) Compute the group commutator $[(h_1, g_1), (h_2, g_2)]$ for a semidirect product. [93]

d.) Let $\mathrm{End}(H)$ be the set of all homomorphisms $H \to H$. Note that this set is closed under the operation of composition, and this operation is associative, but $\mathrm{End}(H)$ is not a group because some homomorphisms will not be invertible. Nevertheless, it is a monoid. Show that if $\alpha_g : G \to \mathrm{End}(H)$ is a homomorphism of monoids then (13.2) still defines a monoid. When is it a group?

Example 13.1: *Infinite dihedral group.* Let $G = \{e, \sigma\} \cong \mathbb{Z}_2$ with generator σ, and let $H = \mathbb{Z}$, written additively. Then define a nontrivial $\alpha : G \to Aut(H)$ by letting α_σ act on $x \in H$ as $\alpha_\sigma(x) = -x$. Then $\mathbb{Z} \rtimes \mathbb{Z}_2$ is a group with elements (x, e) and (x, σ), for $x \in \mathbb{Z}$. Note the multiplication laws:

$$\begin{aligned} (x_1, e)(x_2, e) &= (x_1 + x_2, e) \\ (x_1, e)(x_2, \sigma) &= (x_1 + x_2, \sigma) \\ (x_2, \sigma)(x_1, e) &= (x_2 - x_1, \sigma) \\ (x_1, \sigma)(x_2, \sigma) &= (x_1 - x_2, e) \end{aligned} \tag{13.4}$$

and hence the resulting group is nonabelian with this twisted multiplication law. Since $Aut(\mathbb{Z}) \cong \mathbb{Z}_2$ this is the only nontrivial semidirect product we can form. This group is known as the *infinite dihedral group* sometimes denoted D_∞. It has a presentation:

$$\mathbb{Z} \rtimes \mathbb{Z}_2 \cong \langle r, s | s^2 = 1 \qquad srs = r^{-1} \rangle \tag{13.5}$$

[93] *Answer*: $[(h_1, g_1), (h_2, g_2)] = \left(h_1 \alpha_{g_1}(h_2) \alpha_{g_1 g_2 g_1^{-1}}(h_1^{-1}) \alpha_{g_1 g_2 g_1^{-1} g_2^{-1}}(h_2^{-1}), g_1 g_2 g_1^{-1} g_2^{-1}\right)$.

(e.g. take $s = (0, \sigma)$ and $r = (1, e)$)

Remark: Taking $x = s$ and $y = rs$ we see that D_∞ also has a presentation as a Coxeter group:

$$\mathbb{Z} \rtimes \mathbb{Z}_2 \cong \langle x, y | x^2 = 1 \qquad y^2 = 1 \rangle \tag{13.6}$$

Indeed it is the Weyl group for the affine Lie group $LSU(2)$.

Example 13.2: *Finite dihedral group.* We can use the same formulae as in Example 1, retaining $G = \{e, \sigma\} \cong \mathbb{Z}_2$ but now we take $H = \mathbb{Z}/N\mathbb{Z}$. We still have

$$\alpha_\sigma : \bar{n} \to -\bar{n} \tag{13.7}$$

where we are writing $\mathbb{Z}/N\mathbb{Z}$ additively. The semi-direct product of $\mathbb{Z}/N\mathbb{Z}$ with $\mathbb{Z}_2$ using this automorphism gives one definition of an important group, the *finite dihedral group* D_N. Observe that, when we write $\mathbb{Z}_N = Res(N)$ multiplicatively, the automorphism is $\alpha_\sigma(\omega^j) = \omega^{-j}$. In this way we can obtain a presentation of D_N of the form:

$$\mathbb{Z}_N \rtimes_\alpha \mathbb{Z}_2 \cong \langle r, s | s^2 = 1, \qquad srs = r^{-1}, \qquad r^N = 1 \rangle \tag{13.8}$$

Note that here we have switched to a multiplicative model for the group $\mathbb{Z}_N$. The group has the order given by the cardinality of the Cartesian product $\mathbb{Z}_N \times \mathbb{Z}_2$ so it has order $2N$. Note that using the relations, every word in the r, s can be converted to the form r^x or $r^x s$ with $0 \le x \le N-1$, thus accounting for all $2N$ elements.

$$|D_N| = 2N. \tag{13.9}$$

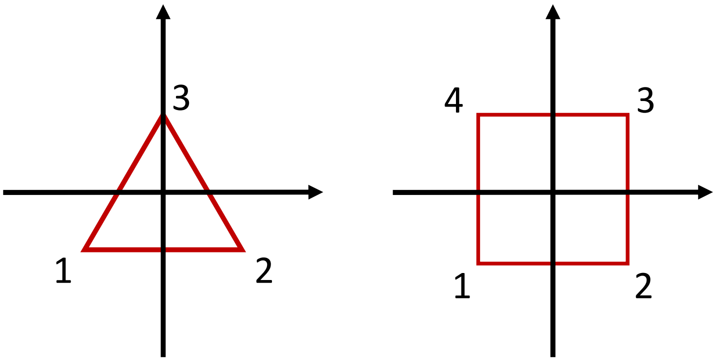

Figure 25: A regular 3-gon and 4-gon in the plane, centered at the origin. The subgroup of $O(2)$ that preserves these is D_3 and D_4, respectively.

Important Remark: *The Dihedral Groups And Symmetries Of Regular Polygons.* The group D_N has a natural action on the vector space $\mathbb{R}^2$. The generator r acts by a rotation around the origin: $\phi_r = R(2\pi/N)$. This generates a group isomorphic to $\mathbb{Z}_N$ and in this context it is usually denoted C_N. If P is <u>any</u> reflection through a line through the origin then $\phi_s = P$ will satisfy all the relations. The resulting group of transformations of the plane generated by ϕ_r and ϕ_s is isomorphic to D_N. Moreover, if we consider the regular N-gon centered at the origin of the plane $\mathbb{R}^2$ then the subgroup of $O(2)$ that maps it to itself is isomorphic to D_N, although to preserve the polygon we must choose P carefully so that it is a reflection through an axis of symmetry. For example, if we consider the regular triangle illustrated in 25 then reflection in the y-axis is a symmetry, as is rotation by integral amounts of $2\pi/3$. So we have a two-dimensional matrix representation of D_3:

$$\begin{aligned} s \to P &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ r \to R(2\pi/3) &= \begin{pmatrix} \cos(2\pi/3) & \sin(2\pi/3) \\ -\sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} \end{aligned} \tag{13.10}$$

Note that, if we label the vertices of the triangle $1,2,3$ as shown in the figure then the various symmetries are in 1-1 correspondence with permutations of $\{1,2,3\}$. So in fact, we have an isomorphism

$$D_3 \cong S_3 \tag{13.11}$$

with $P \to (12)$ and $R(2\pi/3) \to (123)$. Similarly, D_4 is the group of symmetries of the square. We can take $s \to P$ as before and now $r \to R(2\pi/4)$. Again we can label the vertices of the square $1,2,3,4$. Again transformations are uniquely determined by permutations of $\{1,2,3,4\}$. However, the group of permutations we get this way is only a subgroup of the permutation group S_4.

Clearly there is something quite different about the groups D_N when N is even and odd. This is nicely seen in the set of conjugacy classes. As you show in the exercise below the conjugacy classes in D_N are of the form

$$C(r^x) = \{r^x, r^{-x}\} \tag{13.12}$$

and

$$C(r^x s) = \{r^{x+2y}s | y \in \mathbb{Z}\} \tag{13.13}$$

Now, thinking in terms of symmetry actions on the plane, r^x correspond to rotations by $2\pi x/N$, whereas $r^x s$ correspond to reflections. Now note that for N odd, since $(2,N)=1$ the conjugacy class $C(r^x s)$ will contain all the elements of the form $r^z s$, in other words all the reflections. However, if N is even then there are two distinct conjugacy classes: $C(r^x s)$ for x even and odd are distinct. This is nicely in accord with symmetries of the N-gon: For N odd it is clear that all the symmetry axes can be mapped to each other by using the symmetries of the N-gon. Whereas for N even there are two distinct kinds of reflection axes: Those that go through vertices and those that go through edges.

Exercise *D_4 and permutations*

Show that under the map to S_4 described above the dihedral group D_4 maps to the subgroup containing just the identity, the cyclic permtuations (the rotations)

$$(1234), (1234)^2 = (13)(24), (1234)^3 = (1432) \tag{13.14}$$

and four reflections:

$$(12)(34), \quad (23)(14), \quad (13), \quad , (24) \tag{13.15}$$

Exercise
Show that D_N is a quotient of the infinite dihedral group. [94]

Exercise *Conjugacy Classes In D_N*
a.) Using the presentation of D_N in terms of generators r, s and relations $s^2 = 1$ and $srs = r^{-1}$, and $r^N = 1$ show that we have conjugacy classes given by (13.12) and (13.13).
b.) List the distinct conjugacy classes in D_N for N even and N odd.

♣Should provide answer in a footnote here. ♣

Example 13.3: In equations (2.22) and (2.33) we found the most general form of a matrix in $O(2)$. It is a disjoint union of two circles, each circle being the elements of determinant $\det(A) = \pm 1$. As a group we have an isomorphism

$$O(2) \cong SO(2) \rtimes \mathbb{Z}_2 \tag{13.17}$$

In fact, there are many such isomorphisms.

We can write an explicit isomorphism as follows: Let $\mathbb{Z}_2 = \{1, \sigma\}$. Then

$$\alpha : \mathbb{Z}_2 \to \mathrm{Aut}(SO(2)) \tag{13.18}$$

is given by

$$\alpha(\sigma) : R(\phi) \to R(-\phi) \tag{13.19}$$

Now choose any nonzero vector $v \in \mathbb{R}^2$ and define an isomorphism

$$\Psi_v : SO(2) \rtimes \mathbb{Z}_2 \to O(2) \tag{13.20}$$

by

$$\begin{aligned} \Psi_v &: (1, \sigma) \to P_v \\ \Psi_v &: (R(\phi), 1) \to R(\phi) \end{aligned} \tag{13.21}$$

[94] *Answer*: Note that $\mathcal{N} = \{(x, e) | x = 0 \mathrm{mod} N\} \subset \mathbb{Z} \rtimes \mathbb{Z}_2$ is a normal subgroup and

$$(\mathbb{Z}/N\mathbb{Z}) \rtimes \mathbb{Z}_2 \cong (\mathbb{Z} \rtimes \mathbb{Z}_2)/\mathcal{N}. \tag{13.16}$$

Here P_v is the reflection in the line orthogonal to v. We need to check that this is a well-defined homomorphism by checking that the images we have specified are indeed compatible with the relations in the semidirect product. This amounts to checking that $P_v^2 = 1$, which is obvious, and

$$P_v R(\phi) P_v^{-1} = R(-\phi) \tag{13.22}$$

Thanks to (13.22) the relations are indeed satisfied and now it is an easy matter to check that Ψ_v is injective and surjective, so it is an isomorphism.

Note that there are many different such isomorphisms, Ψ_v, depending on the choice of v. If v' is another nonzero vector in the plane then recall from (6.11) that $P_v P_{v'} = R(2\theta)$ where θ is the angle between v and v'. Then

$$\begin{aligned} \Psi_{v'} : (1,\sigma) &\mapsto P_{v'} \\ &= (P_v' P_v) P_v \\ &= R(2\theta) P_v \\ &= R(\theta) P_v R(-\theta) \end{aligned} \tag{13.23}$$

So

$$\Psi_{v'} = I(R(\theta)) \circ \Psi_{v'} \tag{13.24}$$

and changing $v \to v'$ changes Ψ_v by composition with an inner automorphism of $O(2)$.

More generally, it is true that:

1. When d is odd
$$O(d) \cong SO(d) \times \mathbb{Z}_2 \tag{13.25}$$

2. When d is even
$$O(d) \cong SO(d) \rtimes \mathbb{Z}_2 \tag{13.26}$$

In the case when d is odd the element $-\mathbf{1}_{d\times d}$ has determinant -1, so it is in the nontrivial component of $O(d)$, and yet it is also central: so conjugating elements $R \in SO(d)$ acts trivially. The semi-direct product is isomorphic to a direct product in this case. On the other hand, when d is even $-\mathbf{1}_{d\times d}$ has determinant $+1$ and is an element of $SO(d)$. However, it is still true that if Ψ_v is reflection in the hyperplane orthogonal to a nonzero vector v then

$$\alpha_v(R) := P_v R P_v \tag{13.27}$$

is a nontrivial automorphism of $SO(d)$ and we have a family of isomorphisms:

$$\Psi_v : SO(d) \rtimes_{\alpha_v} \mathbb{Z}_2 \to O(d) \tag{13.28}$$

The same discussion as above shows that the dependence on v is through composition with an inner automorphism of $SO(d)$.

Example 13.4: *Affine Euclidean Space.* Imagine that the surface of the earth is flat and of infinite extent. Is this a copy of $\mathbb{R}^2$? Yes and no. We can identify it with $\mathbb{R}^2$, but not in any natural way: $\mathbb{R}^2$ is a vector space with a distinguished vector $\vec{0}$. Where should we put the origin? Rome? Beijing? Moscow? London? New York? Piscataway? If the UN tried to assign an origin there would be endless disputes. However, there would never be any dispute about the vector in $\mathbb{R}^2$ needed to translate from New York to London. The infinite flat earth is an example of two-dimensional affine Euclidean space $\mathbb{E}^2$. More formally: An *affine space* $\mathbb{E}^d$ *modeled on* $\mathbb{R}^d$ is a space of points with an action of $\mathbb{R}^d$ that translates the points so that nonzero vectors always move points and one can get from one point to any other by the action of a vector. But there is no natural choice of origin. In equations:

1. If $v \in \mathbb{R}^d$ and $p \in \mathbb{E}^d$ then there is a point $p+v \in \mathbb{E}^d$ so that $(p+v)+v' = p+(v+v')$.

2. If $p+v = p$ then $v = 0$.

3. If $p, p' \in \mathbb{E}^d$ there is a (unique) vector $v \in \mathbb{R}^d$ so that $p' = p+v$. We can therefore say $p' - p = v$.

If we do choose an origin (this choice is arbitrary) then we can identify $\mathbb{E}^d \cong \mathbb{R}^d$. Indeed, given the above statements, given $p \in \mathbb{E}^d$, every $p' \in \mathbb{E}^d$ is of the form $p' = p+v$ for a unique $v \in \mathbb{R}^d$. So we map $\Psi_p : \mathbb{E}^d \to \mathbb{R}^d$ by taking $\Psi_p : p' \mapsto v$.

Definition A *torsor* or *principal homogeneous space* for a group G is a G-set X on which the action is transitive and free.

In this language we can say that $\mathbb{E}^d$ is a principal homogeneous space for the Abelian group $\mathbb{R}^d$.

♣This should really have been introduced in the introductory section on group actions on sets, with the example of $\mathbb{Z}+\theta$. ♣

There is a distance between points which we take to be the Euclidean norm of the vector:

$$dist(p,p') := \parallel v \parallel \tag{13.29}$$

Now we can study the group of *isometries of* $\mathbb{E}^d$. This is the group of transformations $T : \mathbb{E}^d \to \mathbb{E}^d$ that preserves these distances:

$$dist(T(p), T(p')) = dist(p,p') \tag{13.30}$$

We denote it as Euc(d) and refer to it as the *Euclidean group.*

Some natural examples of isometries are the following: Given any vector $v \in \mathbb{R}^d$ we have the translation operator

$$T_v : p \to p' \tag{13.31}$$

Moreover, if $R \in O(d)$ then, if we choose a point p, we can define an operation:

$$R_p : p+v \to p+Rv \tag{13.32}$$

It turns out (this is a nontrivial theorem) that all isometries are obtained by composing such transforamtions. A simple way to express the general transformation, then, is to choose a point p as the "origin" of the affine space thus giving an identification $\mathbb{E}^d \cong \mathbb{R}^d$. Then, to a pair $R \in O(d)$ and $v \in \mathbb{R}^d$ we can associate the isometry: [95]

$$\{v|R\} : x \mapsto v + Rx \qquad\qquad \forall x \in \mathbb{R}^d \tag{13.33}$$

[95] Our notation is logically superior to the standard notation in the condensed matter physics literature where it is known as the Seitz notation. In the cond-matt literature we have $\{R|v\} : x \mapsto Rx + v$.

In this notation the group multiplication law is

$$\{v_1|R_1\}\{v_2|R_2\} = \{v_1 + R_1 v_2|R_1 R_2\} \tag{13.34}$$

which makes clear that there is a nontrivial automorphism used to construct the semidirect product of the group of translations, isomorphic to $\mathbb{R}^d$ with the rotation-inversion group $O(d)$.

Put differently: $O(d)$ acts as an automorphism group of $\mathbb{R}^d$:

$$\alpha_R : v \mapsto Rv \tag{13.35}$$

so we can form the abstract group $\mathbb{R}^d \rtimes_\alpha O(d)$. Then, once we choose an origin $p \in \mathbb{E}^d$ we can write an isomorphism

$$\Psi_p : \mathbb{R}^d \rtimes_\alpha O(d) \to \mathrm{Euc}(d) \tag{13.36}$$

To be concrete:

$$\Psi_p(v, R) : p + x \mapsto p + (v + Rx) \tag{13.37}$$

As in our example of $O(d)$ we now have a family of isomorphisms. If $\Psi_{p'}$ is another such based on a different origin $p' = p + v_0$ then the two isomorphisms are related by a translation. See the exercise below.

Exercise *Internal Definition Of Semidirect Products*

Suppose there is a homomorphism $\alpha : G \to \mathrm{Aut}(H)$ so that we can form the semidirect product $H \rtimes_\alpha G$.

a.) Show that elements of the form $(1, g)$, $g \in G$ form a subgroup $Q \subset H \rtimes G$ isomorphic to G, while elements of the form $(h, 1)$, $h \in H$ constitute another subgroup, call it N, which is isomorphic to H.

b.) Show that $N = \{(h, 1)|h \in H\}$ is a *normal* subgroup of $H \rtimes G$, while $Q = \{(1, g)|g \in G\}$ in general is not a normal subgroup. [96] This explains the funny product symbol $\rtimes$ that looks like a fish: it is a combination of × with the normal subgroup symbol $\triangleleft$.

c.) Show that we have a short exact sequence:

$$1 \to N \to H \rtimes_\alpha G \to Q \to 1 \tag{13.39}$$

d.) Show that $H \rtimes G = NQ = QN$ and show that $Q \cap N = \{1\}$. Here NQ means the sent of elements nq where $n \in N$ and $q \in Q$. [97]

[96] Answer to (b): Compute $(h_1, g_1)(h, 1)(h_1, g_1)^{-1} = (h_1 \alpha_{g_1}(h) h_1^{-1}, 1)$ and

$$(h_1, g_1)(1, g)(h_1, g_1)^{-1} = (h_1 \alpha_{g_1 g g_1^{-1}}(h_1^{-1}), g_1 g g_1^{-1}). \tag{13.38}$$

[97] The notation is slightly dangerous here: We are considering the group Q both as a subgroup of G <u>and</u>, in equation (13.39), as a quotient. In general, as we will see below in the chapter on exact sequences, there is no way to view a quotient of a group G as a subgroup of G. Failure to appreciate this point has led to many, many, many errors in the physics literature.

e.) Conversely, show that if $\tilde{G} = NQ$ where N is a normal subgroup of $\tilde{G}$ and Q is a subgroup of $\tilde{G}$, (that is, every element of $\tilde{G}$ can be written in the form $g = nq$ with $n \in N$ and $q \in Q$ and $N \cap Q = \{1\}$) then $\tilde{G}$ is a semidirect product of N and Q. Show how to recover the action of Q as a group of automorphisms of N by defining $\alpha_q(n) := qnq^{-1}$. Note that α_q in general is *NOT* an inner automorphism of N.

Exercise *When is a semidirect product actually a direct product?*

Show that if $G = NQ$ is a semidirect product and Q is *also* a normal subgroup of G, then G is the direct product of N and Q. [98]

It is useful to think about the Euclidean group in terms of the “internal” characterization of semi-direct products explained in the exercise above. Here we have a normal subgroup $N := \{\{v|1\}|v \in \mathbb{R}^d\}$ and a subgroup Q given by the set of elements of the form $\{0|R\}$. To check that N is normal a short computation using the group law reveals

$$\{v|R\}\{w|1\} = \{Rw|1\}\{v|R\} \tag{13.40}$$

and hence:

$$\{v|R\}\{w|1\}\{v|R\}^{-1} = \{Rw|1\} \tag{13.41}$$

Note that, again, thanks to the group law, $\pi : \{v|R\} \to R$ is a surjective homomorphism $\mathrm{Euc}(d) \to O(d)$. Thus there is an exact sequence:

$$0 \to \mathbb{R}^d \to Euc(d) \to O(d) \to 1 \tag{13.42}$$

Almost identical considerations show that the Poincaré group is isomorphic to the semidirect product of the translation and Lorentz groups:

$$\mathrm{Poincare}(\mathbb{M}^{1,d-1})) \cong \mathbb{M}^{1,d-1} \rtimes O(1, d-1) \tag{13.43}$$

where, once again, the choice of isomorphism depends on a choice of origin.

Example 13.5: *Wreath Products.* If X and Y are sets then let $\mathcal{F}[X \to Y]$ be the set of functions from X to Y. Recall that

1. If $Y = G_1$ is a group then $\mathcal{F}[X \to G_1]$ is itself a group.

2. If a group G_2 acts on X and Y is any set then G_2 actions on the function space $\mathcal{F}[X \to Y]$ in a natural way.

[98] *Answer:* Note that $n_1q_1n_2q_2 = n_1n_2(n_2^{-1}q_1n_2q_1^{-1})q_1q_2$. However, if both N and Q are normal subgroups then $(n_2^{-1}q_1n_2q_1^{-1}) \in N \cap Q = \{1\}$. Therefore $n_1q_1n_2q_2 = n_1n_2q_1q_2$ is the direct product structure.

We can combine these two ideas as follows: Suppose that G_2 acts on a set X and $Y = G_1$ is itself a group. Then let

$$\alpha : G_2 \to \mathrm{Aut}(\mathcal{F}[X \to G_1]) \tag{13.44}$$

be the canonical G_2 action on the function space: so if $\phi : G_2 \times X \to X$ is the action on X (part of our given data) then the induced action on the function space is

$$\alpha_g : F \mapsto \alpha_g(F) \in \mathcal{F}[X \to G_1] \tag{13.45}$$

where we define

$$\alpha_g(F)(x) = F(\phi(g^{-1}, x)) \qquad \forall g \in G_2, x \in X \tag{13.46}$$

Then we can form the semidirect product

$$\mathcal{F}[X \to G_1] \rtimes G_2 \tag{13.47}$$

This is a *generalized wreath product*. The traditional wreath product is a special case where $G_2 = S_n$ for some n and S_n acts on $X = \{1, \dots, n\}$ by permutations in the standard way. Note that the group $\mathcal{F}[X \to G_1] \cong G_1^n$. The traditional wreath product $G_1 \mathrm{wr} S_n$, also denoted $G_1 \wr S_n$, is then $\mathcal{F}[X \to G_1] \rtimes S_n$. To be quite explicit, the group elements in $G_1 \wr S_n$ are

$$(h_1, \dots, h_n; \phi) \tag{13.48}$$

with $h_i \in G_1$ and $\phi \in S_n$ and the product is

$$(h_1, \dots, h_n; \phi)(h_1', \dots, h_n'; \phi') = (h_1 h'_{\phi^{-1}(1)}, h_2 h'_{\phi^{-1}(2)}, \dots, h_n h'_{\phi^{-1}(n)}, \phi \circ \phi') \tag{13.49}$$

Example 13.6: *Kaluza-Klein theory.* The basic idea of Kaluza-Klein theory is that we study physics on a product manifold $\mathcal{X} \times \mathcal{Y}$ and partially rigidify the situation by putting some structure on $\mathcal{Y}$. We then regard $\mathcal{Y}$ as "small" and study the physics as "effectively" taking place on $\mathcal{X}$.

The idea is intuitively understood by imagining a $2+1$ dimensional world where space is a cylinder of radius R. If we imagine beings in this flatland of a fixed lengthscale, and shrink $R \to 0$ then the beings will end up perceiving themselves as living in a $1+1$ dimensional world.

♣SUITABLE FIGURE NEEDED HERE ♣

Historically, Kaluza-Klein theory arose from attempts to unify the field theories of general relativity with Maxwell's theory of electromagnetism. The basic idea is that pure general relativity on $\mathcal{X} \times \mathcal{Y}$ appears, when $\mathcal{Y}$ is "small" to be a theory of several fields, including electro-magnetism, in $\mathcal{X}$. As originally conceived the idea is very beautiful, but now regarded as too naive and simplistic. Nevertheless, the idea that there might be extra dimensions of spacetime in a compact manifold survives to this day and models that make use of it come astonishingly close to describing the standard model of particle physics and gravity, in the context of "string compactification."

The canonical example of Kaluza-Klein theory is the case where $\mathcal{X} = \mathbb{M}^{1,d-1}$ is d-dimensional Minkowski space and $\mathcal{Y} = S^1$ is the circle. We rigidify the situation by putting a metric on the circle S^1 so that the metric on space-time is

$$ds^2 = \eta_{\mu\nu} dx^\mu dx^\nu + R^2 (d\theta)^2 \tag{13.50}$$

where R is the radius of the circle, $\theta \sim \theta + 2\pi$ and $0 \leq \mu \leq d-1$. Our signature is mostly plus. Now we consider a <u>massless</u> scalar field in $(d+1)$ dimensions on this spacetime. A massless scalar field would satisfy the wave equation:

$$\left[\eta^{\mu\nu}\frac{\partial}{\partial x^\mu}\frac{\partial}{\partial x^\nu} + \frac{1}{R^2}\left(\frac{\partial}{\partial\theta}\right)^2\right]\phi = 0 \tag{13.51}$$

In Quantum Field Theory one makes a huge leap: The quantization of the field leads to quantum states which are interpreted as the states of a system of <u>particles</u>. An essential step in this feat of magic is that one makes a Fourier-decomposition of the field. The Fourier modes of the field are interpreted as creation/annihilation operators of particle states. For the massless scalar field the Fourier modes are

$$e^{\mathrm{i}p_M x^M} = e^{\mathrm{i}p_\mu x^\mu} e^{\mathrm{i}p_\theta \theta} \tag{13.52}$$

corresponding to single-particle creating and annihilation operators of definite energy-momentum. But since $\theta \sim \theta + 2\pi$ single-valuedness of the field implies that $p_\theta = n \in \mathbb{Z}$ is an integer. But now the wave-equation implies that we have a dispersion relation:

$$E^2 - \vec{p}^2 = \frac{n^2}{R^2} \tag{13.53}$$

where $p_\mu = (E, \vec{p})$. From the viewpoint of a d-dimensional field theory, Fourier modes with $n \neq 0$ describe <u>massive</u> particles with $m^2 = n^2/R^2$.

Now consider the case that R is very small compared to the scale of any observer. Then that observer will perceive only a d-dimensional spacetime. If R is very small the single massless particle in $d+1$-dimensions is percieved as an infinite set of different massive particles with mass $|n|/R$ in d dimensions. As $R \to 0$ the masses of the particles $\sim |n|/R$ goes to infinity. So, except for the $n = 0$ modes, the particles are very massive and therefore will not be created by low energy processes, and are hence in general unobservable. For example, if R is on the order of the Planck scale then the nonzero Fourier modes are fields that represent particles of Planck-scale mass.

In a similar spirit, one finds that the Einstein-Hilbert action in $(d+1)$ dimensions describing gravity in $(d+1)$ dimensions is equivalent, upon keeping only the $n = 0$ Fourier modes, to the action of d-dimensional general relativity together with the Maxwell action and the action for a scalar field. In a little more detail, suppose that $\mathcal{Y} = S^1$ and we use coordinates X^M, $M = 0, \ldots, d+1$ on $\mathcal{X} \times S^1$ and coordinates x^μ with $\mu = 0, \ldots, d$ on $\mathcal{X}$. So that $X^M = (x^\mu, \theta)$ where θ is an angular coordinate around S^1. Then we consider the metric:

$$ds^2 = g_{MN}dX^M dX^N = g_{\mu\nu}(x)dx^\mu dx^\nu + \Omega^2(x)(d\theta + A_\mu(x)dx^\mu)^2 \tag{13.54}$$

where the metric $g_{\mu\nu}$, the "warp factor" Ω^2 and the "gauge connection" A_μ are only functions of x^μ (that is, we make the restriction to zero Fourier modes).

Note that this means the metric tensor looks like

$$g_{MN}(x^\mu, \theta) = \begin{pmatrix} g_{\mu\nu}(x) + \Omega^2(x)A_\mu(x)A_\nu(x) & \Omega^2(x)A_\mu(x) \\ \Omega^2(x)A_\nu(x) & \Omega^2(x) \end{pmatrix} \tag{13.55}$$

The general symmetric $(d+1)\times(d+1)$ matrix has

$$\frac{1}{2}(d+1)(d+2)=\frac{1}{2}d(d+1)+d+1 \tag{13.56}$$

independent components, so we have not lost any generality in the form of the matrix, but writing it this way makes the connection to physical quantities (and to connections on a principal $U(1)$ bundle) clearer. By writing the fields on the RHS as functions of x^{μ} and not (x^{μ},θ) we have made a severe restriction - limiting attention to the massless modes in d dimensions, as explained above.

Under these conditions one computes that the Riemann scalar for the $(d{+}1)$-dimensional metric is:

$$\mathcal{R}[g_{MN}]=\mathcal{R}[g_{\mu\nu}]-\frac{\Omega^2}{4}F_{\mu\nu}F^{\mu\nu}-2(\nabla\log\Omega)^2-2\nabla^2\log\Omega \tag{13.57}$$

so the Einstein-Hilbert action for GR in $(d+1)$ dimensions reduces to that of Einstein-Hilbert-Maxwell-Scalar in d dimensions. This is a truly remarkable equation: Pure gravity in $(d+1)$ dimensions leads to both gravity and electricity and magnetism in d dimensions!

Remarks:

1. The KK ansatz also leads to a scalar field $\log\Omega^2(x)$, known as the "dilaton" because it can dilate, in a space-time dependent way, the size of the "internal dimensions" $\mathcal{Y}$. Note that in electricity and magnetism the coupling constant enters via

$$S_{\text{Maxwell}}=\int\sqrt{g}\frac{1}{4e^2}F_{\mu\nu}F^{\mu\nu} \tag{13.58}$$

so the presence of the dilaton can lead to space-time variation of the fine structure constant. In physically viable models one must explain why the dilaton does not fluctuate wildly. The discovery of the naturally occurring nuclear reactor in Oklo, Africa, has led to the bound

$$|\frac{\dot{\alpha}}{\alpha}|<few\times 10^{-17}yr^{-1} \tag{13.59}$$

2. By considering internal spaces $\mathcal{Y}$ equipped with metric with isometry group H similar considerations lead gauge theory with gauge group H in $\mathcal{X}$.

It is interesting to understand how gauge symmetries in theories on $\mathcal{X}$ arise in this point of view. Suppose $\mathcal{D}\cong Diff(\mathcal{X})$ is a subgroup of diffeomorphisms of $\mathcal{X}\times\mathcal{Y}$ of the form

$$\psi_f:(x,y)\to(f(x),y)\qquad\qquad f\in Diff(\mathcal{X}). \tag{13.60}$$

We also consider a subgroup $\mathcal{G}$ of $Diff(\mathcal{X}\times\mathcal{Y})$ where $\mathcal{G}$ is isomorphic to a subgroup of $Map(\mathcal{X},Diff(\mathcal{Y}))$. For the moment just take $\mathcal{G}=Map(\mathcal{X},Diff(\mathcal{Y}))$, so an element $g\in\mathcal{G}$ is a family of diffeomorphisms of $\mathcal{Y}$ parametrized by $\mathcal{X}$: For each x we have a diffeomorphism of $\mathcal{Y}$: $g_x:y\to g(y;x)$. Then we take $\mathcal{G}$ to be the subgroup of diffeomorphisms of $Diff(\mathcal{X}\times\mathcal{Y})$ of the form

$$\psi_g:(x,y)\to(x,g(y;x))\qquad\qquad g\in\mathcal{G} \tag{13.61}$$

Note that within $Diff(\mathcal{X} \times \mathcal{Y})$ we can write the subgroup

$$\mathcal{G}\mathcal{D} \tag{13.62}$$

and $\mathcal{D}$ acts as a group of automorphisms of $\mathcal{G}$ via

$$\begin{aligned} \psi_f \psi_g \psi_f^{-1} : (x, y) &\to (f^{-1}(x), y) \\ &\to (f^{-1}(x), g(y; f^{-1}(x))) \\ &\to (x, g(y; f^{-1}(x))) \end{aligned} \tag{13.63}$$

so if $g \in \mathcal{G}$ and $f \in \mathcal{D}$ then $\psi_f \psi_g \psi_f^{-1} = \psi_{g'}$ with $g' \in \mathcal{G}$ and hence $\mathcal{G}\mathcal{D}$ is a semidirect product. In fact, it is an example of the generalized wreath product of the previous example.

This is a model for the group of gauge transformations in Kaluza-Klein theory. So $\mathcal{X}$ is the "large", possibly noncompact, spacetime where we have general relativity, while $\mathcal{Y}$ is the "small," possibly compact space giving rise to gauge symmetry. $\mathcal{D}$ is the diffeomorphism group of the large spacetime and is the gauge symmetry of general relativity on $\mathcal{X}$. Typically, $\mathcal{Y}$ is endowed with a fixed metric $ds^2_{\mathcal{Y}}$ and the diffeomorphism symmetry of $\mathcal{Y}$ is (spontaneously) broken down to the group of isometries of $\mathcal{Y}$, $Isom(\mathcal{Y}, ds^2_{\mathcal{Y}})$. So in the above construction we take $\mathcal{G}$ to be the unbroken subgroup $Map(\mathcal{X}, Isom(\mathcal{Y}, ds^2_{\mathcal{Y}})) \subset Map(\mathcal{X}, Diff(\mathcal{Y}))$. This subgroup $Map(\mathcal{X}, Isom(\mathcal{Y}, ds^2_{\mathcal{Y}}))$ is interpreted as a group of gauge transformations of a gauge theory on $\mathcal{X}$ coupled to general relativity on $\mathcal{X}$.

As a simple example of the remarks of the previous paragraph let us suppose that $\mathcal{Y} = S^1$ with coordinate θ and round metric $(d\theta)^2$. The isometries of the circle are just constant translations, $\theta \to \theta + \epsilon$. So if

$$g \in \mathrm{Map}(\mathcal{X}, Isom(S^1)) \tag{13.64}$$

then $g(x)$ will take $\theta \to \theta + \epsilon(x)$, so

$$\psi_g : (x^\mu, \theta) \to (x^\mu, \theta + \epsilon(x)) \tag{13.65}$$

so the metric in (13.54) transforms as

$$\psi_g^*(ds^2) = g_{\mu\nu}(x) dx^\mu dx^\nu + \Omega^2(x)(d\theta + dx^\mu \partial_\mu \epsilon + A_\mu(x) dx^\mu)^2 \tag{13.66}$$

meaning that the fields $g_{\mu\nu}$ and Ω are invariant, but

$$A_\mu \to A_\mu + \partial_\mu \epsilon \tag{13.67}$$

and thus, these special diffeomorphisms appear as gauge transformations of the Maxwell field!

Exercise

Show that $S_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ where the generator of $\mathbb{Z}_2$ acts as the nontrivial outer automorphism of $\mathbb{Z}_3$.

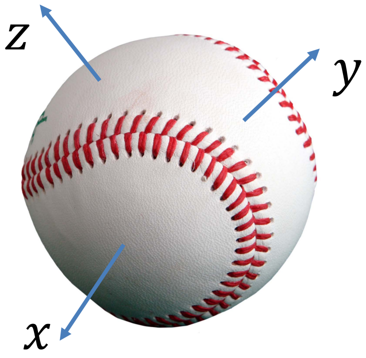

Figure 26: A baseball.

Exercise *Symmetries Of The Baseball*

Ignoring any writing, but taking into account the seams, find the symmetry group of a baseball. (See figure 26.) [99]

Exercise *Symmetries Of The Cube*

a.) Consider a perfect cube. By considering the action of proper rotations on the four diagonal axes through vertices show that the symmetry group is isomorphic to S_4.

b.) Centering the cube on the origin with vertices $(\pm 1, \pm 1, \pm 1)$ show that the symmetry group is $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3$. Deduce that

$$S_4 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3 \tag{13.68}$$

Exercise *Centralizers in the symmetric group*

a.) Suppose that $g \in S_n$ has a conjugacy class given by $\prod_{i=1}^{n}(i)^{\ell_i}$. Show that the centralizer $Z(g)$ is isomorphic to

$$Z(g) \cong \prod_{i=1}^{n} \left(\mathbb{Z}_i^{\ell_i} \rtimes S_{\ell_i} \right) \tag{13.69}$$

[99] *Answer* D_4.

where $\prod_i$ is a direct product.

b.) Use this to compute the order of a conjugacy class in the symmetric group.

Exercise *The Lorentz Group As A Semidirect Product*

Let $\eta = Diag\{-1, \mathbf{1}_d\}$. The Lorentz group in $d+1$ dimensions, denoted $O(1,d)$ is the matrix group

$$O(1,d) = \{A | A\eta A^{tr} = \eta\} \tag{13.70}$$

a.) Considering the case $d=1$ find the general solution and show that there are four connected components. [100]

b.) Show that, group-theoretically, we have

$$O(1,1) = SO_0(1,1) \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2) \tag{13.72}$$

where $SO_0(1,1)$ is the connected component of the identity.

Remark: In fact, more generally $O(1,d)$ has four connected components for $d \geq 1$ and

$$O(1,d) = SO_0(1,d) \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2) \tag{13.73}$$

You can easily see that there are at least four components since $\det A \in \{\pm 1\}$ and moreover $A_{00}^2 = 1 + \sum_{i=1}^d A_{0i}^2$ so that we can independently have $A_{00} \geq 1$ or $A_{00} \leq -1$.

Exercise *Holomorph*

Given a finite group G a canonical semidirect product group is $G \rtimes \mathrm{Aut}(G)$ known as the holomorph of G.

a.) Show that this is the normalizer of the copy of G in the symmetric group $S_{|G|}$ given by Cayley's theorem.

b.) Show that the affine Euclidean group $Euc(d)$ is the holomorph of the Abelian group $\mathbb{R}^d$.

Exercise *Equivalence of semidirect products*

[100] *Answer*: Writing out the four matrix elements of the defining equation easily arrives at the general solution:

$$A = \begin{pmatrix} \xi_1 \cosh\theta & \xi_2 \sinh\theta \\ \xi_4 \sinh\theta & \xi_3 \cosh\theta \end{pmatrix} \tag{13.71}$$

where $\theta \in \mathbb{R}$, $\xi_i \in \{\pm 1\}$ and $\xi_4 = \xi_1\xi_2\xi_3$. By changing the sign of θ we can set $\xi_=2$. The sign of ξ_1, ξ_2 is meaningful, giving us four components.

A nontrivial homomorphism $\alpha : G \to \mathrm{Aut}(H)$ can lead to a semidirect product which is in fact isomorphic to a direct product. Show this as follows: Suppose $\phi : G \to H$ is a homomorphism. Define $\alpha : G \to \mathrm{Aut}(H)$ by $\alpha_g = I(\phi(g))$. Construct an isomorphism [101]

$$\Psi : H \rtimes_\alpha G \to H \times G \tag{13.74}$$

Exercise *Manipulating the Seitz notation*

a.) Show that:

$$\begin{aligned} \{v|R\}^{-1} &= \{-R^{-1}v|R^{-1}\} \\ \{0|R\}\{v|1\} &= \{Rv|R\} \\ \{v|1\}\{0|R\} &= \{v|R\} \\ \{w|1\}\{v|R\} &= \{w+v|R\} \\ \{v_1|R_1\}\{v_2|R_2\}\{v_1|R_1\}^{-1} &= \{R_1v_2 + (1 - R_1R_2R_1^{-1})v_1|R_1R_2R_1^{-1}\} \\ [\{v_1|R_1\},\{v_2|R_2\}] &= \{(1 - R_1R_2R_1^{-1})v_1 - R_1R_2R_1^{-1}R_2^{-1}(1 - R_2R_1R_2^{-1})v_2|R_1R_2R_1^{-1}R_2^{-1}\} \end{aligned} \tag{13.75}$$

b.) Show that the subgroup of pure translations, that is, the subgroup of elements of the form $\{v|1\}$ with $v \in \mathbb{R}^d$ is a normal subgroup of $\mathrm{Euc}(d)$.

c.) Can you construct a homomorphism $O(d) \to \mathrm{Euc}(d)$?

d.) Consider the group $G = L \rtimes \mathbb{Z}_2$ where L is a lattice and the nontrivial element in $\mathbb{Z}_2$ acts on L by $v \to -v$. Compute the conjugacy classes in G. [102]

Exercise *Dependence on basepoint for isomorphism of Euclidean group*

Show that if $p' = p + v_0$ then

$$\Psi_{p'}(v', R) = \Psi_p(v, R) \in \mathrm{Euc}(d) \tag{13.76}$$

for

$$v' = v + (1 - R)v_0 \tag{13.77}$$

---

14. Group Extensions and Group Cohomology

14.1 Group Extensions

♣Add: Pushforward extensions ♣

Recall that an extension of Q by a group N is an exact sequence of the form:

[101] *Answer*: $\Psi(h, g) = (h\phi(g), g)$.

[102] *Answer*: $C(\{v|1\}) = \{\{\pm v|1\}\}$ has two elements while $C(\{v|-1\}) = \{\{\pm v + 2v_1| - 1\}|v_1 \in L\}$ has infinitely many elements.

$$1 \to N \overset{\iota}{\to} G \overset{\pi}{\to} Q \to 1 \tag{14.1}$$

There is a notion of *homomorphism of two group extensions*

$$1 \to N \overset{\iota_1}{\to} G_1 \overset{\pi_1}{\to} Q \to 1 \tag{14.2}$$

$$1 \to N \overset{\iota_2}{\to} G_2 \overset{\pi_2}{\to} Q \to 1 \tag{14.3}$$

This means that there is a group homomorphism $\varphi : G_1 \to G_2$ so that the following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota_1"] \arrow[d, leftrightarrow, "\mathrm{Id}"] & G_1 \arrow[r, "\pi_1"] \arrow[d, "\varphi"] & Q \arrow[r] \arrow[d, leftrightarrow, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\iota_2"] & G_2 \arrow[r, "\pi_2"] & Q \arrow[r] & 1
\end{tikzcd} \tag{14.4}$$

To say that a "diagram commutes" means that if one follows the maps around two paths with the same beginning and ending points then the compositions of the maps are the same. Thus (14.4) is completely equivalent to the pair of equations:

$$\begin{aligned} \pi_1 &= \pi_2 \circ \varphi \\ \iota_2 &= \varphi \circ \iota_1 \end{aligned} \tag{14.5}$$

However, drawing a diagram makes the relations between maps, domains and codomains much more transparent. Sometimes a picture is worth a thousand equations. This is why mathematicians like commutative diagrams.

When there is a homomorphism of group extensions based on $\psi : G_2 \to G_1$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity then the group extensions are said to be isomorphic.

It can certainly happen that there is more than one nonisomorphic extension of Q by N. Classifying all extensions of Q by N is a difficult problem. We will discuss it more in section 14.7 below.

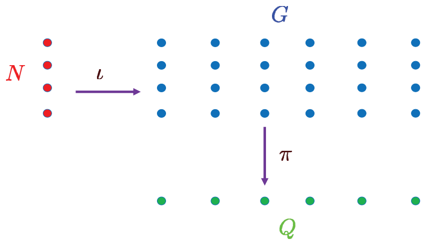

Figure 27: Illustration of a group extension $1 \to N \to G \to Q \to 1$ as an N-bundle over Q.

We would encourage the reader to think geometrically about this problem, even in the case when Q and N are finite groups, as in Figure 27. In particular we will use the important notion of a *section*, that is, a right-inverse to π: It is a map $s : Q \to G$ such that $\pi(s(q)) = q$ for all $q \in Q$. Such sections always exist.[103] Note that in general $s(\pi(g)) \neq g$. This is obvious from Figure 27. The set of pre-images, $\pi^{-1}(q)$, is called *the fiber of* π *over* q. The map π projects the entire fiber over q to the single element q. A choice of section s is a choice, for each and every $q \in Q$, of just one single point in the fiber above q.

In order to justify the picture of Figure 27 let us prove that, as a set, G is just the product $N \times Q$. Note that for any $g \in G$ and any section s:

$$g(s(\pi(g)))^{-1} \tag{14.6}$$

maps to 1 under π (check this). Therefore, since the sequence is exact

$$g(s(\pi(g)))^{-1} = \iota(n) \tag{14.7}$$

for some $n \in N$. That is, every $g \in G$ can be written as

$$g = \iota(n)s(q) \tag{14.8}$$

for some $n \in N$ and some $q \in Q$. In fact, this decomposition is *unique*: Suppose that:

$$\iota(n_1)s(q_1) = \iota(n_2)s(q_2) \tag{14.9}$$

Then we rewrite this as

$$\iota(n_2^{-1}n_1) = s(q_2)s(q_1)^{-1} \tag{14.10}$$

Now, applying π we learn that $1 = q_2\pi(s(q_1)^{-1}) = q_2\left(\pi(s(q_1))\right)^{-1} = q_2q_1^{-1}$, so $q_1 = q_2$. But that implies $n_1 = n_2$. Therefore, as a set, G can be identified with $N \times Q$.

Remark: As a nice corollary of the decomposition (14.8) note that if φ defines a morphism of group extensions then φ is in fact an isomorphism of G_1 to G_2. It is a homomorphism by definition. Now note that if $s_1 : Q \to G_1$ is a section of π_1 then $s_2 := \varphi \circ s_1 : Q \to G_2$ is a section of π_2 so

$$\begin{aligned}\varphi(g) &= \varphi(\iota_1(n)s_1(q))\\ &= \varphi(\iota_1(n))\varphi(s_1(q))\\ &= \iota_2(n)s_2(q)\end{aligned} \tag{14.11}$$

and since the decomposition is unique (given a choice of section) the map φ is $1-1$.

Now, given an extension and a choice of section s we define a map

$$\omega : Q \to \mathrm{Aut}(N) \tag{14.12}$$

denoted by

$$q \mapsto \omega_q \tag{14.13}$$

[103] By the axiom of choice. For continuous groups such as Lie groups there might or might not be continuous sections.

where the definition of ω_q is given by

$$\iota(\omega_q(n)) = s(q)\iota(n)s(q)^{-1} \tag{14.14}$$

Because $\iota(N)$ is normal the RHS is again in $\iota(N)$. Because ι is injective $\omega_q(n)$ is well-defined. Moreover, for each q the reader should check that indeed $\omega_q(n_1 n_2) = \omega_q(n_1)\omega_q(n_2)$, and ω_q is one-one on N. Therefore we really have a map of sets (14.12). Note carefully that we are not saying that $q \mapsto \omega_q$ is a group homomorphism. In general, it is not.

Remark: Clearly the ι is a bit of a nuisance and leads to clutter and it can be safely dropped if we consider N simply to be a subgroup of G, for then ι is simply the inclusion map. The confident reader is encouraged to do this. The formulae will be a little cleaner. However, we will be pedantic and retain the ι in most of our formulae.

Let us stress that the map $\omega : Q \to \mathrm{Aut(N)}$ *in general is not a homomorphism* and *in general depends on the choice of section s.* We will discuss the dependence on the choice of section s below when we have some more machinery and context. For now let us see how close ω comes to being a group homomorphism:

$$\begin{aligned} \iota\left(\omega_{q_1} \circ \omega_{q_2}(n)\right) &= s(q_1)\iota(\omega_{q_2}(n))s(q_1)^{-1} \\ &= s(q_1)s(q_2)\iota(n)(s(q_1)s(q_2))^{-1} \end{aligned} \tag{14.15}$$

We want to compare this to $\iota\left(\omega_{q_1 q_2}(n)\right)$. In general they will be different unless $s(q_1 q_2) = s(q_1)s(q_2)$, that is, unless $s : Q \to G$ is a homomorphism. In general the section is not a homomorphism, but clearly something nice happens when it is:

Definition: We say an extension *splits* if there exists a section $s : Q \to G$ which is *also* a *group homomorphism.* A choice of a section which is a group homomorphism is called a (choice of) *splitting.*

Theorem: An extension is isomorphic to a semidirect product iff it is a split extension.

Proof:

First suppose it splits. Choose a splitting s. Then from (14.15) we know that

$$\omega_{q_1} \circ \omega_{q_2} = \omega_{q_1 q_2} \tag{14.16}$$

and hence $q \mapsto \omega_q$ defines a homomorphism $\omega : Q \to \mathrm{Aut}(N)$. Therefore, we can aim to prove that there is an isomorphism of G with $N \rtimes_\omega Q$.

In general if s is just a section the image $s(Q) \subset G$ is not a subgroup. But if the sequence splits, then it is a subgroup. The equation (14.8) implies that $G = \iota(N)s(Q)$ where $s(Q)$ is a subgroup, and by the internal characterization of semidirect products that means we have a semidirect product.

To give a more concrete proof, let us write the group law in the parametrization (14.8). Write

$$\iota(n)s(q)\iota(n')s(q') = \iota(n)\left(s(q)\iota(n')s(q)^{-1}\right)s(qq') \tag{14.17}$$

Note that

$$s(q)\iota(n')s(q)^{-1} = \iota(\omega_q(n')) \tag{14.18}$$

so

$$\iota(n_1)s(q_1)\iota(n_2)s(q_2) = \iota\left(n_1\omega_{q_1}(n_2)\right)s(q_1q_2) \tag{14.19}$$

But this just means that

$$\Psi(n,q) = \iota(n)s(q) \tag{14.20}$$

is in fact an isomorphism $\Psi : N \rtimes_\omega Q \to G$. Indeed equation (14.19) just says that:

$$\Psi(n_1,q_1)\Psi(n_2,q_2) = \Psi((n_1,q_1)\cdot_\omega(n_2,q_2)) \tag{14.21}$$

where $\cdot_\omega$ stresses that we are multiplying with the semidirect product rule.

Thus, we have shown that a split extension is isomorphic to a semidirect product $G \cong N \rtimes Q$. The converse is straightforward. ♠

In §14.7 below we will continue the general line of reasoning begun here. However, in order to appreciate the formulae better it is a good idea first to step back and consider a simple but important special case of extensions, namely, the *central extensions*. These are extensions such that $\iota(N)$ is a subgroup of the center of G. Here is the official definition: (Note the change of notation from the general situation above):

♣Do the general case first and then specialize? ♣

Let A be an abelian group and G any group.

Definition A *central extension* of G by A, [104] is a group $\tilde{G}$ and an extension such that

$$1 \to A \xrightarrow{\iota} \tilde{G} \xrightarrow{\pi} G \to 1 \tag{14.22}$$

such that $\iota(A) \subset Z(\tilde{G})$.

We stress again that what we called G in the previous discussion is here called $\tilde{G}$, and what we called Q in the previous discussion is here called G.

Example And Remark:*Sections of group extensions vs. continuous sections of principal fiber bundles.* Let us return to the very important exact sequence (10.38):

$$1 \to \mathbb{Z}_2 \xrightarrow{\iota} SU(2) \xrightarrow{\pi} SO(3) \to 1 \tag{14.23}$$

The $\mathbb{Z}_2$ is embedded as the subgroup $\{\pm 1\} \subset SU(2)$, so this is a central extension. We said above that there is always a section, but when we said that we did not impose any properties of continuity in the case where G and Q are continuous groups. In this example while there is a section of π there is, in fact, no continuous section. Such a continuous section $\pi s = Id$ would imply that $\pi_* s_* = 1$ on the first homotopy group of $SO(3)$. But that is impossible since it would have factor through $\pi_1(SU(2)) = 1$.

We are using a few facts here:

[104] Some authors say an extension of A by G.

1. Every $SU(2)$ matrix can be written as
$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \tag{14.24}$$
where α, β are complex numbers with $|\alpha|^2 + |\beta|^2 = 1$. Writing this equation in terms of the real and imaginary parts of α, β we recognize the equation of the unit three dimensional sphere. Now recall that all the spheres of dimension ≥ 2 are simply connected. Therefore $\pi_1(SU(2)) = 1$ is simply connected.

2. But $SO(3)$ is not simply connected! In fact, using a coffee cup you can informally demonstrate that $\pi_1(SO(3)) \cong \mathbb{Z}_2$. [Demonstrate].

3. If there were a continuous section then $s_* : \pi_1(SO(3)) \to \pi_1(SU(2))$ would be a well-defined group homomorphism and $s \circ \pi = Id$ would imply that on the fundamental groups $Id_* = s_* \pi_*$ in
$$\pi_1(SO(3)) \to \pi_1(SU(2)) = 1 \to \pi_1(SO(3)) \tag{14.25}$$
But Id_* takes the nontrivial element of $\mathbb{Z}_2$ to the nontrivial element, not to the trivial element. This is impossible if you factor through the trivial group.

In algebraic topology one introduces another kind of topological invariant known as homology. The homology groups of a manifold are Abelian groups that encode many important properties of the manifold. The homology group $H_1(M; \mathbb{Z}_2)$ tells us what are the possible 2-fold covers of the manifold M. It turns out that $H_1(SO(3); \mathbb{Z}_2) \cong \mathbb{Z}_2$, (this is closely related to $\pi_1(SO(3)) \cong \mathbb{Z}_2$. so there are two double covers of $SO(3)$. One is $O(3) = \mathbb{Z}_2 \times SO(3)$ and the other is $SU(2)$, the nontrivial double cover.

The extension (14.1) generalizes to
$$1 \to \mathbb{Z}_2 \quad \overset{\iota}{\to} \quad \mathrm{Spin}(d) \quad \overset{\pi}{\to} \quad SO(d) \to 1 \tag{14.26}$$
as well as the two Pin groups which extend $O(d)$:
$$1 \to \mathbb{Z}_2 \quad \overset{\iota}{\to} \quad \mathrm{Pin}^{\pm}(d) \quad \overset{\pi}{\to} \quad O(d) \to 1 \tag{14.27}$$
we discuss these in Section *** below. Again, in these cases there is no continuous section. Thus, these examples are nontrivial as fiber bundles. Moreover, even if we allow ourselves to choose a discontinuous section, we cannot do so and make it a group homomorphism. In other words these examples are also nontrivial as group extensions.

Exercise

If $s : Q \to G$ is any section of π show that for all $q \in Q$,
$$s(q^{-1}) = s(q)^{-1} n = n' s(q)^{-1} \tag{14.28}$$

for some $n, n' \in N$.

Exercise *The pullback construction*

There is one general construction with extensions which is useful when discussing symmetries in quantum mechanics. This is the notion of *pullback extension.* Suppose we are given both an extension

$$\begin{tikzcd} 1 \arrow[r] & H' \arrow[r, "\iota"] & H \arrow[r, "\pi"] & H'' \arrow[r] & 1 \end{tikzcd} \tag{14.29}$$

and a homomorphism

$$\rho : G \to H'' \tag{14.30}$$

one can define another extension of G by H' known as a *pullback extension.* We are trying to fill in the diagram:

$$\begin{tikzcd} & & & G \arrow[d, "\rho"] & \\ 1 \arrow[r] & H' \arrow[r, "\iota"] & H \arrow[r, "\pi"] & H'' \arrow[r] & 1 \end{tikzcd} \tag{14.31}$$

with an extension on the first row of G by H'.

We do this by defining a subgroup of the Cartesian product $\tilde{G} \subset H \times G$:

$$\tilde{G} := \{(h,g) | \pi(h) = \rho(g)\} \subset H \times G \tag{14.32}$$

We have an extension of the form

$$\begin{tikzcd} 1 \arrow[r] & H' \arrow[r, "\iota"] & \tilde{G} \arrow[r, "\tilde{\pi}"] & G \arrow[r] & 1 \end{tikzcd} \tag{14.33}$$

where $\tilde{\pi}(h,g) := g$. Show that this extension fits in the commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & H' \arrow[r] \arrow[d, equal] & \tilde{G} \arrow[r, "\tilde{\pi}"] \arrow[d, "\tilde{\rho}"] & G'' \arrow[r] \arrow[d, "\rho"] & 1 \\ 1 \arrow[r] & H' \arrow[r] & H \arrow[r, "\pi"] & H'' \arrow[r] & 1 \end{tikzcd} \tag{14.34}$$

(N.B. This is <u>not</u> a morphism of extensions.)

Exercise *The pushforward extension*

Under some circumstances one can complete the diagram

$$\begin{tikzcd} 1 \arrow[r] & H' \arrow[r, "\iota"] \arrow[d, "\rho"] & H \arrow[r, "\pi"] & H'' \arrow[r] & 1 \\ & \tilde{H} & & & \end{tikzcd} \tag{14.35}$$

to get an extension of H'' by $\tilde{H}$. This is not as universal as the pullback. But one can construct it if $\rho : H' \to \tilde{H}$ is surjective and $\iota(\ker(\rho)) \triangleleft H$. Give the construction. [105]

Exercise *Choice of splitting and the Euclidean group* Euc(d)

As we noted, the Euclidean group Euc(d) is isomorphic to the semidirect product $\mathbb{R}^d \rtimes O(d)$, but to exhibit that we needed to choose an origin about which to define rotation-inversions. See equation (13.37) above.

a.) Show that a change of origin corresponds to a change of splitting.

b.) Using the Seitz notation show that another choice of origin leads to the splitting $R \mapsto \{(1-R)v|R\}$, and verify that this is also a splitting.

♣This is almost redundant with another exercise above. ♣

Exercise *Another form of splitting*

Show that an equivalent definition of a split exact sequence for a central extension is that there is a homomorphism $t : \tilde{G} \to A$ which is a left-inverse to ι, $t(\iota(a)) = a$.

(Hint: Define $s(\pi(\tilde{g})) = \iota t(\tilde{g}^{-1}))\tilde{g}$.)

Exercise *The exact sequence for a product of two cyclic groups*

Revisit the exact sequence discussed in equation (11.52). Show that this sequence splits. [106]

Exercise *Is A Restriction Of A Split Extension Split?*

[105] *Answer*: Define the group $\tilde{G} := H/\iota(\ker(\rho))$. Then note that we can define $\tilde{\iota} : \tilde{H} \to \tilde{G}$ via $\tilde{\iota}(\rho(h)) = \iota(h) + \iota(\ker(\rho))$. Note that if $\rho(h) = \rho(h')$ then the RHS is the same so this does give a well-defined map $\tilde{\iota}$ on the image of ρ, but if ρ is surjective that is enough. Now define $\tilde{\pi}(\tilde{e}) = \pi(e)$ where $\tilde{e} = e + \iota(\ker\rho)$. Then we have a commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & H' \arrow[r, "\iota"] \arrow[d, "\rho"] & H \arrow[r, "\pi"] \arrow[d, "\varphi"] & H'' \arrow[r] & 1 \\
1 \arrow[r] & \tilde{H} \arrow[r, "\tilde{\iota}"] & \tilde{G} \arrow[r, "\tilde{\pi}"] & H'' \arrow[r] \arrow[u, "Id"] & 1
\end{tikzcd} \tag{14.36}$$

where $\varphi(h) = h + \iota(\ker(\rho))$.

[106] *Answer*: Let ω_ℓ generate $\mathbb{Z}_\ell$ then, using the notation above let $s : \omega_\ell \mapsto (\omega_\ell^{\mu_2\nu_2}, \omega_\ell^{\mu_1\nu_1})$.

Suppose

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & Q \arrow[r] & 1 \end{tikzcd} \quad (14.37)$$

is a split extension and $N_1 \subset N$ and $Q_1 \subset Q$, so that there is an extension

$$\begin{tikzcd} 1 \arrow[r] & N_1 \arrow[r, "\iota"] & G_1 \arrow[r, "\pi"] & Q_1 \arrow[r] & 1 \end{tikzcd} \quad (14.38)$$

given by restriction to $G_1 \subset G$. Does it follow that this extension is a split extension?

Exercise *A Split Central Extension Is A Direct Product*
Suppose

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & Q \arrow[r] & 1 \end{tikzcd} \quad (14.39)$$

is a split central extension. Show that $G \cong N \times Q$ and the extension is isomorphic to the trivial extension with ι inclusion into the first factor and π projection onto the second factor. [107]

14.2 Projective Representations

We have already encountered the notion of a matrix representation of a group G. This is a homomorphism from G into $GL(d, \kappa)$ for some field κ. In many contexts in mathematics and physics (especially in quantum physics) one encounters a generalization of the notion of matrix representation known as a *projective representation.* The theory of projective representations is closely related to the theory of central extensions.

Recall that a matrix representation of a group G is a group homomorphism

$$\rho : G \to GL(d, \kappa) \quad (14.41)$$

A *projective representation* is a map

$$\rho : G \to GL(d, \kappa) \quad (14.42)$$

which is "almost a homomorphism" in the sense that

$$\rho(g_1)\rho(g_2) = f(g_1, g_2)\rho(g_1, g_2) \quad (14.43)$$

[107] *Answer*: Choose a splitting s. Then use the parametrization $g = \iota(n)s(q)$. The group multiplication can be written

$$\begin{aligned} g_1 g_2 &= \iota(n_1)s(q_1)\iota(n_2)s(q_2) \\ &= \iota(n_1)\iota(n_2)s(q_1)s(q_2) \\ &= \iota(n_1 n_2)s(q_1 q_2) \end{aligned} \quad (14.40)$$

In the going from the first to second line we used that $\iota(n_2)$ is in the center. In going from the second to the third line we used that ι and s are group homomorphisms. (Recall s is a group homomorphism because it is a splitting.)

for some function $f : G \times G \to \kappa^*$. Of course $f(g_1, g_2)$ is "just a c-number" so you might think it is an unimportant nuisance. You might try to get rid of it by redefining

$$\tilde{\rho}(g) = b(g)\rho(g) \tag{14.44}$$

where $b(g) \in \kappa^*$ is a c-number. Then <u>if</u> there exists a function $b : G \to \kappa^*$ such that

$$f(g_1, g_2) \overset{?}{=} \frac{b(g_1 g_2)}{b(g_1)b(g_2)} \tag{14.45}$$

then $\tilde{\rho}$ would be an honest representation.

The trouble is, in many important contexts, there is no function b so that (14.45) holds. So we need to deal with it.

A simple example is the "spin representation of the rotation group $SO(3)$" where one attempts to define a map:

$$\rho : SO(3) \to SU(2) \subset GL(2, \mathbb{C}) \tag{14.46}$$

that attempts to describe the effects of a rotation on - say - a spin 1/2 particle. In fact, there is no such thing as the "spin representation of the rotation group $SO(3)$." There is a spin <u>projective</u> representation of $SO(3)$. [108]

We saw above that there is a very natural group homomorphism from $SU(2)$ to $SO(3)$, but there is no group homomorphism back from $SO(3)$ to $SU(2)$: There is no splitting. The so-called "spin representation of $SO(3)$" is usually presented by attempting to construct a splitting $\rho : SO(3) \to SU(2)$ using Euler angles. Indeed, under the standard homomorphism $\pi : SU(2) \to SO(3)$ one recognizes that $\exp[\mathrm{i}\theta\sigma^i]$ maps to a rotation by angle 2θ around the the i^{th} axis. For example,

$$u = \exp[\mathrm{i}\theta\sigma^3] = \begin{pmatrix} e^{\mathrm{i}\theta} & 0 \\ 0 & e^{-\mathrm{i}\theta} \end{pmatrix} = \cos\theta + \mathrm{i}\sin\theta\sigma^3 \tag{14.47}$$

acts by

$$\begin{aligned} u\vec{x}\cdot\vec{\sigma}u^{-1} &= u \begin{pmatrix} z & x - \mathrm{i}y \\ x + \mathrm{i}y & -z \end{pmatrix} u^{-1} \\ &= \begin{pmatrix} z & e^{2\mathrm{i}\theta}(x - \mathrm{i}y) \\ e^{-2\mathrm{i}\theta}(x + \mathrm{i}y) & -z \end{pmatrix} \end{aligned} \tag{14.48}$$

One can represent any rotation in $SO(3)$ by a rotation around the z-axis, then around the x-axis, then around the z axis. Call this $R(\phi, \theta, \psi)$. So one attempts to define ρ by assigning

$$\rho : R(\phi, \theta, \psi) \to e^{\mathrm{i}\frac{\phi}{2}\sigma^3} e^{\mathrm{i}\frac{\theta}{2}\sigma^1} e^{\mathrm{i}\frac{\psi}{2}\sigma^3}. \tag{14.49}$$

Clearly, we are going to have problems making this mapping well-defined. For example, $R(\phi, 0, 0)$ would map to $e^{\mathrm{i}\frac{\phi}{2}\sigma^3}$, but this is not well-defined for all ϕ because $R(2\pi, 0, 0) = 1$

[108] However, there is a perfectly well-defined spin representation of the <u>Lie algebra</u> $\mathfrak{so}(3)$.

and $e^{\mathrm{i}\frac{2\pi}{2}\sigma^3} = -1$. The problem is that the Euler angle coordinates on $SO(3)$ are sometimes singular. So, we need to restrict the domain of ϕ, θ, ψ so that (14.49) is well-defined for every $R \in SO(3)$. However, when we make such a restriction we will spoil the group homomorphism property, but only up to a phase. So, in this way, we get a two-dimensional projective representation of $SO(3)$.

As an exercise you can try the following: Every $SU(2)$ matrix can be written as $u = \cos(\chi) + \mathrm{i}\sin(\chi)\hat{n}\cdot\vec{\sigma}$ and this maps under π to a rotation by 2χ around the $\hat{n}$ axis. But again, you cannot smoothly identify every $SO(3)$ rotation by describing it as a rotation by 2χ around an axis.

Exercise *Projective representations of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and the Pauli group*

Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ multiplicatively:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{1, g_1, g_2, g_1 g_2\} \tag{14.50}$$

with relations $g_1^2 = g_2^2 = 1$ and $g_1 g_2 = g_2 g_1$. Consider the map

$$\rho : \mathbb{Z}_2 \times \mathbb{Z}_2 \to GL(2, \mathbb{C}) \tag{14.51}$$

defined by

$$\begin{aligned} \rho(1) &= 1 \\ \rho(g_1) &= \sigma^1 \\ \rho(g_2) &= \sigma^2 \\ \rho(g_1 g_2) &= \sigma^3 \end{aligned} \tag{14.52}$$

a.) Show that this defines a projective representation of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

b.) Try to remove the phase to get a true representation.

c.) Show that ρ defines a section of an exact sequence with G given by the Pauli group.

14.2.1 How projective representations arise in quantum mechanics

The following material, while very important, assumes knowledge of some of the linear algebra from Chapter 2 and some familiarity with quantum mechanics. For further details see Chapter **** below. The reader should also consult Section 2 of [109]

Let us review, very briefly the most essential points of quantum mechanics: The Dirac-von Neumann axioms of quantum mechanics posit that to a physical system we associate a complex Hilbert space $\mathcal{H}$ such that

[109] http://www.physics.rutgers.edu/~gmoore/695Fall2013/CHAPTER1-QUANTUMSYMMETRY-OCT5.pdf

1. Physical states are identified with traceclass positive operators ρ of trace one. They are usually called *density matrices.* We denote the space of physical states by $\mathcal{S}$. [110]

2. Physical observables are identified with self-adjoint operators. We denote the set of (bounded) self-adjoint operators by $\mathcal{O}$.

3. The *Born rule* states that when measuring the observable O in a state ρ the probability of measuring value $e \in E \subset \mathbb{R}$, where E is a Borel-measurable subset of $\mathbb{R}$, is
$$P_{\rho,O}(E) = \mathrm{Tr} P_O(E)\rho. \tag{14.53}$$
Here P_O is the projection-valued-measure associated to the self-adjoint operator O by the spectral theorem. For example, if $\mathcal{O}$ has a complete discrete spectrum $\{\lambda_i\}$ of eigenvalues so that
$$\mathcal{O} = \sum_i \lambda_i P(\lambda_i) \tag{14.54}$$
where $P(\lambda_i)$ is the projection operator onto the eigenspace with eigenvalue λ_i then
$$P_O(E) = \sum_{\lambda_i \in E} P(\lambda_i) \tag{14.55}$$
When the spectrum of O is more complicated, e.g. if there is a continuous spectrum, one can still define $P_O(E)$, but the story is more involved. See Chapter 2, the Linear Algebra User's Manual.

4. There are further axioms regarding time-development, and so on, but the above is all we need for the present discussion.

Given this setup up the natural notion of a general "symmetry" in quantum mechanics is the following:

Definition An *automorphism* of a quantum system is a pair of bijective maps $s_1 : \mathcal{S} \to \mathcal{S}$ and $s_2 : \mathcal{O} \to \mathcal{O}$ and where s_2 is real linear on $\mathcal{O}$ such that (s_1, s_2) preserves probability measures:
$$P_{s_1(\rho),s_2(O)} = P_{\rho,O} \tag{14.56}$$
This set of mappings forms a group which we will call the group of *quantum automorphisms.*

♣Need to state some appropriate continuity properties. ♣

While this is conceptually straightforward, it is an unwieldy notion of symmetry. We will now simplify it considerably, ending up with the crucial theorem known as *Wigner's theorem.*

[110] As explained in the Linear Algebra User's Manual, positive operators can be defined as operators A such that $(\psi, A\psi) \geq 0$ for every $\psi \in \mathcal{H}$. Such operators are always self-adjoint. Indeed, any operator A such that $(\psi, A\psi) \in \mathbb{R}$ for all $\psi \in \mathcal{H}$ is self-adjoint. To see this note that $(\psi, A\psi)^* = (\psi, A\psi)$ and hence $(\psi, A\psi) = (\psi, A^\dagger\psi)$. Now apply this equation to $\psi_1 + z\psi_2$ for $z = 1$ and $z = \sqrt{-1}$ and add the resulting equations to deduce that $(\psi_1, A\psi_2) = (\psi_1, A^\dagger\psi_2)$ for all pairs $\psi_1, \psi_2 \in \mathcal{H}$. Choose an ON basis for $\mathcal{H}$ to deduce that $A = A^\dagger$.

We begin by noting that the space of density matrices is a convex set. The convexity means that if ρ_1, ρ_2 are density matrices then for all $0 \le t \le 1$

$$t\rho_1 + (1-t)\rho_2 \tag{14.57}$$

is a density matrix. Given a convex set on defines an *extremal point* to be a point in the set which cannot be written in the above form with $0 < t < 1$. By definition, the *pure states* are the extremal points of $\mathcal{S}$. The pure states are just the dimension one projection operators.

Pure states are often referred to in the physics literature as "rays in Hilbert space" for the following reason:

If $\psi \in \mathcal{H}$ is a nonzero vector then it determines a line

$$\ell_\psi := \{z\psi | z \in \mathbb{C}\} := \psi\mathbb{C} \tag{14.58}$$

Note that the line does not depend on the normalization or phase of ψ, that is, $\ell_\psi = \ell_{z\psi}$ for any nonzero complex number z. Put differently, the space of such lines is projective Hilbert space

$$\mathbb{P}\mathcal{H} := (\mathcal{H} - \{0\})/\mathbb{C}^* \tag{14.59}$$

Equivalently, this can be identified with the space of rank one projection operators. Indeed, given any line $\ell \subset \mathcal{H}$ we can write, in Dirac's bra-ket notation: [111]

$$P_\ell = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle} \tag{14.60}$$

where ψ is any nonzero vector in the line ℓ.

It is possible to argue (see the above reference) that such a symmetry maps pure states to pure states, and is completely determined by this map. So we can view the group of quantum automorphisms as the group of transformations of one-dimensional projection operators (or rays) that preserves overlaps

$$\mathrm{Tr}(P_1 P_2) = \frac{|\langle\psi_1|\psi_2\rangle|^2}{\parallel \psi_1 \parallel^2 \parallel \psi_2 \parallel^2} \tag{14.61}$$

The group of such transformations is denoted $\mathrm{Aut}(QM)$. Any symmetry of a quantum mechanical system will define a subgroup of this group.

Example: Let us consider this case of a single Qbit, namely $\mathcal{H} = \mathbb{C}^2$. First we write the most general general density matrix. Any 2×2 Hermitian matrix is of the form $a + \vec{b} \cdot \vec{\sigma}$

[111] We generally denote inner products in Hilbert space by $(x_1, x_2) \in \mathbb{C}$ where $x_1, x_2 \in \mathcal{H}$. Our convention is that it is complex-linear in the second argument. However, we sometimes write equations in Dirac's bra-ket notation because it is very popular. In this case, identify x with $|x\rangle$. Using the Hermitian structure there is a unique anti-linear isomorphism of $\mathcal{H}$ with $\mathcal{H}^*$ which we denote $x \mapsto \langle x|$. Sometimes we denote vectors by Greek letters $\psi, \chi, \dots$, and scalars by Latin letters $z, w, \dots$. But sometimes we denote vectors by Latin letters, $x, w, \dots$ and scalars by Greek letters, $\alpha, \beta, \dots$.

where $\vec{\sigma}$ is the vector of "Pauli matrices":

$$\begin{aligned}\sigma^1 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma^2 &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma^3 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\end{aligned} \tag{14.62}$$

$a \in \mathbb{R}$ and $\vec{b} \in \mathbb{R}^3$. Now a density matrix ρ must have trace one, and therefore $a = \frac{1}{2}$. Then the eigenvalues are $\frac{1}{2} \pm |\vec{b}|$ so positivity means it must have the form

$$\rho = \frac{1}{2}(1 + \vec{x} \cdot \vec{\sigma}) \tag{14.63}$$

where $\vec{x} \in \mathbb{R}^3$ with $\vec{x}^2 \leq 1$.

The extremal states, corresponding to the rank one projection operators are therefore of the form

$$P_{\vec{n}} = \frac{1}{2}(1 + \vec{n} \cdot \vec{\sigma}) \tag{14.64}$$

where $\vec{n}$ is a unit vector. This gives the explicit identification of the pure states with elements of S^2. Moreover, we can easily compute:

$$\mathrm{Tr} P_{\vec{n}_1} P_{\vec{n}_2} = \frac{1}{2}(1 + \vec{n}_1 \cdot \vec{n}_2) \tag{14.65}$$

and $\vec{n}_1 \cdot \vec{n}_2 = \cos(\theta_1 - \theta_2)$ where $|\theta_1 - \theta_2|$ (with θ's chosen so this is between 0 and π) is the geodesic distance between the two points on the unit sphere.

There is another viewpoint which is useful. Nonzero vectors in $\mathbb{C}^2$ can be normalized to be in the unit sphere S^3. Then the association of projector to state given by

$$|\psi\rangle \rightarrow |\psi\rangle\langle\psi| = \frac{1}{2}(1 + \vec{n} \cdot \vec{\sigma}) \tag{14.66}$$

defines a map $\pi : S^3 \rightarrow S^2$ known as the *Hopf fibration.*

The unit sphere is a principal homogeneous space for $SU(2)$ and we may coordinatize $SU(2)$ by the Euler angles:

$$u = e^{-i\frac{\phi}{2}\sigma^3} e^{-i\frac{\theta}{2}\sigma^2} e^{-i\frac{\psi}{2}\sigma^3} \tag{14.67}$$

with range $0 \leq \theta \leq \pi$ and identifications:

$$(\phi, \psi) \sim (\phi + 4\pi, \psi) \sim (\phi, \psi + 4\pi) \sim (\phi + 2\pi, \psi + 2\pi) \tag{14.68}$$

We can make an identification with the unit sphere in $\mathbb{C}^2$ by viewing it as a homogeneous space:

$$\psi = \begin{pmatrix} e^{-i\frac{\psi+\phi}{2}} \cos\theta/2 \\ e^{-i\frac{\psi-\phi}{2}} \sin\theta/2 \end{pmatrix} = u \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{14.69}$$

The projector onto the line through this space is

$$P_{\ell_\psi} = |\psi\rangle\langle\psi| = \frac{1}{2}(1 + \vec{n}\cdot\vec{\sigma}) \tag{14.70}$$

with $\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ as usual. Alternatively, we could map $\pi : S^3 \to S^2$ by $\pi(\psi) = [\psi_1 : \psi_2] \cong \mathbb{C}P^1$, and this will correspond to the point in S^2 by the usual stereographic projection.

♣from which pole? ♣

In any case, for the case $N = 2$ we see that $\mathrm{Aut}_{\mathrm{qtm}}(\mathbb{P}\mathcal{H})$ is just the group of isometries of S^2 with its round metric. This group is well known to be the orthogonal group $O(3)$.

In general for $\mathcal{H} = \mathbb{C}^{N+1}$ the space of pure states is $\mathbb{CP}^N$. This space has a natural homogeneous metric known as the Fubini-Study metric. When it is suitably normalized the overlap function $\mathfrak{o}$ is nicely related to the Fubini-Study distance d by

$$\mathfrak{o}(\ell_1, \ell_2) = \left(\cos\frac{d(\ell_1, \ell_2)}{2}\right)^2 \tag{14.71}$$

Now, it is hard to work with the space of one-dimensional projection operators since it is not a linear space: The sum of two one-dimensional projection operators is typically not even proportional to a projection operator. It would be much nicer to work with operators acting on Hilbert space. A fundamental theorem of quantum mechanics known as *Wigner's theorem* states that $\mathrm{Aut}(QM)$ is indeed a quotient of a certain group of operators on a Hilbert space. This group, denoted $\mathrm{Aut}(\mathcal{H})$, is the group of the norm-preserving unitary and anti-unitary operators on Hilbert space. We now explain a bit more about $\mathrm{Aut}(\mathcal{H})$.

A unitary operator on $\mathcal{H}$ is a $\mathbb{C}$-linear operator $u : \mathcal{H} \to \mathcal{H}$ that preserves norms:

$$\parallel u\psi \parallel = \parallel \psi \parallel \tag{14.72}$$

An anti-unitary operator on $\mathcal{H}$ is an $\mathbb{C}$-anti-linear operator [112] $a : \mathcal{H} \to \mathcal{H}$ that preserves norms:

$$\parallel a\psi \parallel = \parallel \psi \parallel \tag{14.73}$$

The composition of unitary operators is clearly unitary. The composition of unitary and antiunitary is antiunitary, and the composition of antiunitaries is unitary so we have an exact sequence

$$1 \to U(\mathcal{H}) \to \mathrm{Aut}(\mathcal{H}) \xrightarrow{\phi} \mathbb{Z}_2 \to 1 \tag{14.74}$$

where

$$\phi(g) = \begin{cases} +1 & g \text{ unitary} \\ -1 & g \text{ anti} - \text{unitary} \end{cases} \tag{14.75}$$

There is a homomorphism $\pi : \mathrm{Aut}(\mathcal{H}) \to \mathrm{Aut}(QM)$ defined by

$$\pi(u) : P \mapsto uPu^\dagger \tag{14.76}$$

[112] See Chapter 2, the Linear Algebra User's Manual, for more on this. Briefly this means $a(\psi_1 + \psi_2) = a(\psi_1) + a(\psi_2)$ for any two vectors but $a(z\psi) = z^* a(\psi)$ for any scalar $z \in \mathbb{C}$. Note that we must then define the adjoint by $\langle a^\dagger\psi_1, \psi_2\rangle := \langle\psi_1, a\psi_2\rangle^*$ in a convention where the sesquilinear form is $\mathbb{C}$-antilinear in the first argument and linear in the second.

for $u \in U(\mathcal{H})$ and similarly

$$\pi(a) : P \mapsto aPa^\dagger \tag{14.77}$$

for anti-unitary operators a. See the footnote above for the definition of the adjoint of an anti-unitary operator. In both cases $u^{-1} = u^\dagger$ and $a^{-1} = a^\dagger$ and these operations preserve the overlap function.

The fiber of the map π can be thought of as possible c-number phases which can multiply the operator on Hilbert space representing a symmetry operation:

$$1 \ \to \ U(1) \ \to \ \mathrm{Aut}(\mathcal{H}) \xrightarrow{\pi} \mathrm{Aut}(QM) \ \to 1 \tag{14.78}$$

Here the $U(1)$ is the group of phases acting on quantum states: $\psi \to z\psi$ for $z \in U(1)$.

The upshot is that, given a classical symmetry group G of a physical system, for each $g \in G$ we can associate a unitary, or antiunitary, operator $U(g)$ acting on a Hilbert space. Quantum mechanics only guarantees that

$$U(g_1)U(g_2) = c(g_1, g_2)U(g_1 g_2) \tag{14.79}$$

for some phase factor $c(g_1, g_2)$, which, in general, cannot be removed by a redefinition of $U(g)$ by a phase $\tilde{U}(g) = b(g)U(g)$. So we have a projective representation of the classical symmetry G.

Put differently: In a given physical system we will not consider the full group $\mathrm{Aut}(QM)$ as a group of symmetries because. For example, the time-dynamics of a nonrelativistic quantum system is governed by the Schrödinger equation:

$$\mathrm{i}\hbar \frac{\partial \psi}{\partial t} = H\psi \tag{14.80}$$

where H is a self-adjoint operator, the Hamiltonian. For time-independent Hamiltonians the unitary time evolution is governed by

$$U(t) = \exp[-\mathrm{i}\frac{t}{\hbar}H] \tag{14.81}$$

Only a subgroup of $Aut(QM)$ will commute with the resultant flows on the space of states. If we think of G as embedded in $\mathrm{Aut}(QM)$ then we have

$$\begin{tikzcd} & & & G \arrow[d, "\rho"] & \\ 1 \arrow[r] & U(1) \arrow[r, "\iota"] & \mathrm{Aut}(\mathcal{H}) \arrow[r, "\pi"] & \mathrm{Aut}(QM) \arrow[r] & 1 \end{tikzcd} \tag{14.82}$$

The group which acts on the Hilbert space will be a central extension of G given by the pullback construction.

One thing we can note is that finite dimensional matrices are always associative! [113] So for all $g_1, g_2, g_3 \in G$

$$(U(g_1)U(g_2))U(g_3) = U(g_1)(U(g_2)U(g_3)) \tag{14.83}$$

[113] And the same holds for linear operators on infinite-dimensional Hilbert spaces provided the domains are such that the composition of the three operators is well-defined.

and hence

$$c(g_1, g_2)c(g_1g_2, g_3) = c(g_1, g_2g_3)c(g_2, g_3) \tag{14.84}$$

We note that projective representations are quite pervasive in modern physics:

1. Projective representations appear naturally in quantization of bosons and fermions. The Heisenberg group is an extension of a translation group (on phase space). In addition, the symplectic group of linear canonical transformations gets quantum mechanically modified by a central extension to define something called the metaplectic group.

2. Projective representations are important in the theory of anomalies in quantum field theory.

3. Projective representations are very important in conformal field theory. The Virasoro group, and the Kac-Moody groups are both nontrivial central extensions of simpler objects.

Now, as we will explain near the end of section 14.3 below projective representations are very closely connected to central extensions. So in the next section we turn to a deeper investigation into the structure of central extensions.

Remark: The fact that the symmetry operators $U(g)$ should commute with the Hamiltonian has an important implication. Suppose that H has a complete set of eigenvectors Ψ_λ where $\lambda \in \text{Spec}(H)$ is a discrete set of eigenvalues. Then we can restrict $U(g)$ to the different eigenspaces $\mathcal{H}_\lambda$ of H, for if

$$H\psi_\lambda = E_\lambda \psi_\lambda \tag{14.85}$$

and $U(g)$ commutes with H then $U(g)\psi_\lambda$ also is an eigenvector of eigenvalue E_λ. This means that the eigenspaces $\mathcal{H}_\lambda$ are each projective representations of G. This can be extremely useful in diagonalizing H and simplifying computations.

♣Need to work in some examples ♣

Exercise *Kernel Of π In The Wigner Sequence*

Show that the kernel of π in the exact sequence (14.78) is precisely the group of phases times the identity operator. [114]

---

[114] *Answer*: Suppose $uP = Pu$ for every rank one projection operator. Consider the projection operator for the line through $\psi_1 + z\psi_2$ for any two nonzero vectors $\psi_1, \psi_2 \in \mathcal{H}$. Applying the condition for the cases $z = 1$ and $z = \sqrt{-1}$ deduce that u commutes with $|\psi_1\rangle\langle\psi_2|$. Thus, choosing an ON basis e_i it commutes with $|e_i\rangle\langle e_j|$ and therefore must be proportional to the identity matrix. On the other hand, it also must preserve norms, so it is the group of multiplication by a phase.

14.3 How To Classify Central Extensions

There is an interesting way to classify central extensions of G by A.

As before let $s : G \to \tilde{G}$ be a "section" of π. That is, a map such that

$$\pi(s(g)) = g \qquad \forall g \in G \tag{14.86}$$

As we have stressed, in general s is not a homomorphism. In the case when the sequence splits, that is, when there exists a section which is a homomorphism, then we can say $\tilde{G}$ is isomorphic to a direct product $\tilde{G} \cong A \times G$ via

$$\iota(a)s(g) \to (a, g) \tag{14.87}$$

When the sequence splits the semidirect product of the previous section is a direct product because A is central, so $\omega_g(a) = a$.

Now, let us allow that (14.22) does not necessarily split. Let us choose any section s and measure by how much s differs from being a homomorphism by considering the combination:

$$s(g_1)s(g_2)\left(s(g_1g_2)\right)^{-1}. \tag{14.88}$$

Now the quantity (14.88) is in the kernel of π and hence in the image of ι. Since ι is injective we can *define* a function $f_s : G \times G \to A$ by the equation

$$\iota(f_s(g_1, g_2)) := s(g_1)s(g_2)\left(s(g_1g_2)\right)^{-1}. \tag{14.89}$$

That is, we can write:

$$s(g_1)s(g_2) = \iota(f_s(g_1, g_2))s(g_1g_2) \tag{14.90}$$

The function f_s satisfies the important *cocycle identity*

$$\boxed{\boxed{f(g_2, g_3)f(g_1, g_2g_3) = f(g_1, g_2)f(g_1g_2, g_3)}} \tag{14.91}$$

Exercise *Derivation Of The Cocycle Identity*

Verify (14.91) by using (14.89) to compute $s(g_1g_2g_3)$ in two different ways.

(Note that simply substituting (14.89) into (14.91) is not obviously going to work because $\tilde{G}$ need not be abelian.)

Exercise *Simple consequences of the cocycle identity*

a.) By putting $g_1 = 1$ and then $g_3 = 1$ show that any cocycle f must satisfy:

$$f(g, 1) = f(1, g) = f(1, 1) \qquad \forall g \in G \tag{14.92}$$

b.) Show that [115]

$$f(g, g^{-1}) = f(g^{-1}, g). \tag{14.93}$$

Now we introduce some fancy terminology:

Definition: In general

1. A *2-cochain on G with values in A* is a function

$$f : G \times G \to A \tag{14.94}$$

We denote the set of all such 2-cochains by $C^2(G, A)$.

2. A *2-cocycle* is a 2-cochain $f : G \times G \to A$ satisfying (14.91). We denote the set of all such 2-cocycles by $Z^2(G, A)$.

Remarks:

1. The fancy terminology is introduced for a good reason because there is a topological space and a cohomology theory underlying this discussion. See Section §14.8 and Section §16.2 for further discussion.

2. Note that $C^2(G, A)$ is naturally an abelian group because A is an abelian group. (Recall example 2.7 of Section §2.) $Z^2(G, A)$ inherits an abelian group structure from $C^2(G, A)$.

So, in this language, given a central extension of G by A and a section s we naturally obtain a two-cocycle $f_s \in Z^2(G, A)$ via (14.89).

Now, if we choose a different section $\hat{s}$ then [116]

$$\hat{s}(g) = \iota(t(g))s(g) \tag{14.95}$$

for some function $t : G \to A$. It is easy to check that

$$f_{\hat{s}}(g_1, g_2) = f_s(g_1, g_2)t(g_1)t(g_2)t(g_1g_2)^{-1} \tag{14.96}$$

where we have used that $\iota(A)$ is central in $\tilde{G}$.

Definition: In general two 2-cochains f and $\hat{f}$ are said to *differ by a coboundary* if there exists a function $t : G \to A$ such that

$$\hat{f}(g_1, g_2) = f(g_1, g_2)t(g_1)t(g_2)t(g_1g_2)^{-1} \tag{14.97}$$

[115] *Answer*: Consider the triple $g \cdot g^{-1} \cdot g$ and apply part (a).

[116] Since we are working with central extensions we could put the $\iota(t(g))$ on either side of the $s(g)$. However, when we discuss non-central extensions later the order will matter.

for all $g_1, g_2 \in G$.

One can readily check, using the condition that A is Abelian, that if f is a cocycle then any other $\hat{f}$ differing by a coboundary is also a cocycle. Moreover, being related by a cocycle defines an equivalence relation on the set of cocycles $f \sim \hat{f}$. Thus, we may define:

Definition: The *group cohomology* $H^2(G, A)$ is the set of equivalence classes of 2-cocycles modulo equivalence by coboundaries.

Now, the beautiful theorem states that group cohomology classifies central extensions: [117]

Theorem: Isomorphism classes of central extensions of G by an abelian group A are in 1-1 correspondence with the second cohomology set $H^2(G, A)$.

Proof: Let $\mathcal{E}(G, A)$ denote the set of all extensions of G by A, and let $\overline{\mathcal{E}}(G, A)$ denote the set of all isomorphism classes of extensions of G by A.

We first construct a map:

$$\Psi_{\mathcal{E}\to H} : \mathcal{E}(G, A) \to H^2(G, A) \tag{14.98}$$

To do this, we choose a section, then from (14.89)(14.91)(14.96) we learn that we get a cocycle whose cohomology class does not depend on the section. So

$$\Psi_{\mathcal{E}\to H}\Big(1 \to A \to \tilde{G} \to G \to 1\Big) = [f_s] \tag{14.99}$$

is well-defined, because the RHS does not depend on the choice of section s.

Now we claim that this map descends to a map $\overline{\Psi}_{\mathcal{E}\to H} : \overline{\mathcal{E}}(G, A) \to H^2(G, A)$. Indeed, if we have an isomorphism of central extensions:

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\mathrm{Id}"] & \widetilde{G} \arrow[r, "\pi"] \arrow[d, "\psi"] & G \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & A \arrow[r, "\iota'"] & \widetilde{G}' \arrow[r, "\pi'"] & G \arrow[r] & 1
\end{tikzcd} \tag{14.100}$$

where $\psi : \tilde{G} \to \tilde{G}'$ is an isomorphism such that the inverse also leads to a commutative diagram, then ψ can be used to map sections of $\pi : \tilde{G} \to G$ to sections of $\pi' : \tilde{G}' \to G$ by $s \mapsto s'$ where $s'(g) = \psi(s(g))$. Then

♣where do we use this condition in the proof? ♣

$$\begin{aligned}
s'(g_1)s'(g_2) &= \psi(s(g_1))\psi(s(g_2)) \\
&= \psi(s(g_1)s(g_2)) \\
&= \psi(\iota(f_s(g_1, g_2))s(g_1g_2)) \\
&= \psi(\iota(f_s(g_1, g_2)))\psi(s(g_1g_2)) \\
&= \iota'(f_s(g_1, g_2))s'(g_1g_2)
\end{aligned} \tag{14.101}$$

[117] In fact, both the set of isomorphism classes of extensions and $H^2(G, A)$ are Abelian groups and a stronger statement is that the 1-1 correspondence described here is an isomorphism of Abelian groups.

and hence we assign precisely the same 2-cocycle $f(g_1, g_2)$ to the section s'. Hence the map $\Psi_{\mathcal{E}\to H}$ only depends on the isomorphism class of the extension. This defines the map $\overline{\Psi}_{\mathcal{E}\to H}$.

Conversely, we can define a map $\Psi_{H\to\mathcal{E}} : Z^2(G, A) \to \mathcal{E}(G, A)$ as follows: Given a cocycle $f \in Z^2(G, A)$ we may define $\tilde{G} = A \times G$ as a set and we use f to *define* the multiplication law:

$$(a_1, g_1)(a_2, g_2) := (a_1 a_2 f(g_1, g_2), g_1 g_2) \tag{14.102}$$

You should check that this does define a valid group multiplication: The associativity follows from the cocycle relation. Note that if we use the *trivial cocycle*: $f(g_1, g_2) = 1$ for all $g_1, g_2 \in G$ then we just get the direct product of groups.

Now suppose that we use two 2-cocycles f and f' which are related by a coboundary as in (14.97) above. Then we claim that the map $\psi : \tilde{G} \to \tilde{G}'$ defined by

$$\psi : (a, g) \to (at(g)^{-1}, g) \tag{14.103}$$

is an isomorphism of central extensions as in (14.100). This means that the map $\Psi_{H\to\mathcal{E}} : Z^2(G, A) \to \mathcal{E}(G, A)$ actually descends to a well-defined map

$$\overline{\Psi}_{H\to\mathcal{E}} : H^2(G, A) \to \overline{\mathcal{E}}(G, A) \tag{14.104}$$

We leave it to the reader to check that $\overline{\Psi}_{H\to\mathcal{E}}$ and $\overline{\Psi}_{\mathcal{E}\to H}$ are inverse maps. ♠

Remarks:

1. *Central extensions and projective representations.* A very important consequence of the construction (14.102) is that, if we are given a projective representation of G then we can associate a centrally extended group $\widetilde{G}$:

$$1 \to U(1) \to \widetilde{G} \to G \to 1 \tag{14.105}$$

and a <u>true</u> representation $\widetilde{\rho}$ of $\widetilde{G}$:

$$\widetilde{\rho}(z, g) := z\rho(g) \tag{14.106}$$

The evil failure of $\rho(g)$ to be a true representation of G now becomes a virtuous fact that allows $\widetilde{\rho}$ to be a true representation of $\widetilde{G}$. This is the typical situation in quantum mechanics, where G is a group of classical symmetries and $\widetilde{G}$ is the group that is implemented quantum-mechanically. A good example is the spin-1/2 system where $G = SO(3)$ is the classical group of rotations but for a quantum rotor the proper symmetry group is $\widetilde{G} = SU(2)$. There are many many other examples.

2. *Group Structure on* $\overline{\mathcal{E}}(G, A)$. The set $H^2(G, A)$ carries a natural structure of an Abelian group. Indeed, as we remarked above $C^2(G, A)$, being a set of maps with target space a group, A, is naturally a group. Then, because A is Abelian, we can define a group structure on $Z^2(G, A)$ by the rule:

$$(f_1 \cdot f_2)(g, g') = f_1(g, g') \cdot f_2(g, g') \tag{14.107}$$

where we are writing the product in A multiplicatively. Again using the fact that A is abelian this descends to a well-defined multiplication on cohomology classes: $[f_1]\cdot[f_2] := [f_1 \cdot f_2]$. Therefore $H^2(G,A)$ itself is an abelian group. The identity element corresponds to the cohomology class of the trivializable cocycles, which in turn corresponds to the split extension $A \times G$.

♣It might be clearer to write A additively... ♣

It is natural to ask whether one can give a more canonical description of the abelian group structure on the set of equivalence classes of central extensions of G by A. Indeed we can: We pull back the Cartesian product to the diagonal of $G \times G$ and then push forward by the multiplication map $\mu : A \times A \to A$. That is, suppose we have two central extensions:

$$\mathcal{E}_1 : \qquad 1 \to A \overset{\iota_1}{\to} \tilde{G}_1 \overset{\pi_1}{\to} G \to 1 \tag{14.108}$$

$$\mathcal{E}_2 : \qquad 1 \to A \overset{\iota_2}{\to} \tilde{G}_2 \overset{\pi_2}{\to} G \to 1 \tag{14.109}$$

The Cartesian product $\mathcal{E}_1 \times \mathcal{E}_2$ is the extension of $G \times G$ by $A \times A$ using the group $\tilde{G}_1 \times \tilde{G}_2$ with the Cartesian product of the group homomorphisms. We want an extension of G by A, corresponding, under the 1-1 correspondence of the above theorem to the natural group structure on $H^2(G,A)$. To construct it, let

$$\Delta : G \to G \times G \tag{14.110}$$

be the diagonal homomorphism: $\Delta : g \mapsto (g,g)$. Then we claim that the product extension $\mathcal{E}_1 \cdot \mathcal{E}_2$ can be identified as

$$\mathcal{E}_1 \cdot \mathcal{E}_2 = \mu_* \Delta^*(\mathcal{E}_1 \times \mathcal{E}_2) \tag{14.111}$$

where $\Delta^*(\mathcal{E}_1 \times \mathcal{E}_2)$ is the pull-back extension under Δ (see equation (14.34)), an extension of G by $A \times A$, and μ_* is the pushforward extension. In concrete terms the pullback extension under Δ^* is:

$$1 \to A \times A \overset{(\iota_1,\iota_2)}{\to} \widehat{G_{12}} \overset{\pi_{12}}{\to} G \to 1 \tag{14.112}$$

where

$$\widehat{G_{12}} := \{(\tilde{g}_1, \tilde{g}_2) | \pi_1(\tilde{g}_1) = \pi_2(\tilde{g}_2)\} \subset \tilde{G}_1 \times \tilde{G}_2 \tag{14.113}$$

We can define $\pi_{12}(\tilde{g}_1,\tilde{g}_2) := \pi_1(\tilde{g}_1) = \pi_2(\tilde{g}_2)$. Now consider the "anti-diagonal"

$$A^{\rm anti} := \ker(\mu) = \{(a, a^{-1})\} \subset A \times A \tag{14.114}$$

and its image:

$$N := \{(\iota_1(a), \iota_2(a^{-1})) | a \in A\} \subset \widehat{G_{12}} \tag{14.115}$$

Because we are working with central extensions this will be a normal subgroup. Then we let

$$\tilde{G}_{12} := \widehat{G_{12}}/N \tag{14.116}$$

Since N is in the kernel of π_{12} and since it is central the homomorphism π_{12} descends to a surjective homomorphism which we will also call $\pi_{12} : \tilde{G}_{12} \to G$. Now we have an exact sequence

$$1 \to A \overset{\iota_{12}}{\to} \tilde{G}_{12} \overset{\pi_{12}}{\to} G \to 1 \tag{14.117}$$

where $\iota_{12}(a) := [(\iota_1(a), \iota_2(1))] = [(\iota_1(1), \iota_2(a))]$. Given sections s_1, s_2 of π_1, π_2 respectively we can define a section $s_{12}(g) := [(s_1(g), s_2(g))]$ and one can check that the resulting cocycle is indeed in the cohomology class of $f_{s_1} \cdot f_{s_2}$. The extension (14.117) represents the product of extensions (14.108) and (14.109). The point of this construction is that it is canonical: We did not make any choices of sections to define the product extension.

3. *Trivial vs. Trivializable.* Above we defined the trivial cocycle to be the one with $f(g_1, g_2) = 1_A$ for all g_1, g_2. We define a cocycle to be *trivializable* if it is cohomologous to the trivial cocycle. Note that a trivializable cocycle f could be trivialized in multiple ways. Suppose both b and $\tilde{b}$ trivialize f. Then you should show that $\tilde{b}$ and b "differ" by a group homomorphism $\phi : G \to A$ in the sense that

$$\tilde{b}(g) = \phi(g) b(g) \tag{14.118}$$

There are situations where a cohomological obstruction vanishes and the choice of trivialization has physical significance.

♣Should give some examples: H^3 is obstruction to orbifolding CFT and choice of trivialization is H^2 - hence discrete torsion. There are bundle examples. Find example where class in H^2 is zero but trivialization has physical meaning. ♣

4. *An analogy to gauge theory*: Changing a cocycle by a coboundary is strongly analogous to making a gauge transformation in a gauge theory. In Maxwell's theory we can make a change of gauge of the vector potential A_μ by

$$A'_\mu(x) = A_\mu(x) - \mathrm{i} g^{-1}(x) \partial_\mu g(x) \tag{14.119}$$

where $g(x) = e^{\mathrm{i}\epsilon(x)}$ is a function on spacetime valued in $U(1)$. In the case of electromagnetism we would say that A_μ is trivializable if there is a gauge transformation $g(x)$ that simplifies it to 0. (For valid gauge transformations $g(x)$ must be a single-valued function on spacetime.) If we are presented with $A_\mu(x)$ and we want to know if it is trivializable then we should check whether gauge invariant quantities vanish. One such quantity is the fieldstrength tensor $F_{\mu\nu} := \partial_\mu A_\nu - \partial_\nu A_\mu$, but this is not a complete gauge invariant. The isomorphism class of a field is completely specified by the holonomies $\exp \mathrm{i} \oint_\gamma A$ around all the closed cycles γ in spacetime. Even when $A_\mu(x)$ is not trivializable, it is very often useful to use gauge transformations to try to simplify A_μ. In the next remark we do the same for cocycles.

5. *Simplifying Cocycles Using Coboundaries.* Using a coboundary one can usefully simplify cocycles. Since this topic will be unfamiliar to some readers we explain this in excruciating detail. Those who are familiar with cohomology can safely skip the rest of this remark. To begin, note that a coboundary modification takes a cochain f to $f^{(1)}$ satisfying:

$$f^{(1)}(1,1) = f(1,1) \frac{t(1)t(1)}{t(1 \cdot 1)} = f(1,1)t(1) \tag{14.120}$$

so by choosing any function t such that $t(1) = f(1,1)^{-1}$ we get a new cochain satisfying $f^{(1)}(1,1) = 1$. Choose any such function. (The simplest thing to do is set $t(g) = 1$ for all other $g \neq 1$. We will make this choice, but it is really not necessary.) Now recall that if f is a cocycle then a modification of f by any coboundary produces a new cochain $f^{(1)}$ that is also a cocycle. So now, if f is a cocycle and we have set $f^{(1)}(1,1) = 1$ then, by (14.92) we have $f^{(1)}(g,1) = f^{(1)}(1,g) = 1$ for all g. Now, we can continue to make modifications by coboundaries to simplify further our cocycle $f^{(1)}$. In order not to undo what we have done we require that the new coboundaries we use, say, $\tilde{t}$ satisfy $\tilde{t}(1) = 1$. We may say that we are "partially choosing a gauge" by choosing representatives so that $f^{(1)}(1,1) = 1$ and then the further coboundaries $\tilde{t}$ must "preserve that gauge." Now suppose that $g \neq 1$. Then (using our particular choice of t above):

$$f^{(1)}(g,g^{-1}) = f(g,g^{-1})\frac{1}{t(1)} = f(g,g^{-1})f(1,1) \tag{14.121}$$

is not particularly special. (Remember that we are making the somewhat arbitrary choice that $t(g) = 1$ for $g \neq 1$.) So we have not simplified these quantities. However, we still have plenty of gauge freedom left and we can try to simplify the values as follows: Suppose, first, that $g \neq g^{-1}$, equivalently, suppose $g^2 \neq 1$ so g is not an involution. Then we can make another "gauge transformation" by a coboundary function $\tilde{t}$ to produce:

$$f^{(2)}(g,g^{-1}) = f^{(1)}(g,g^{-1})\frac{\tilde{t}(g)\tilde{t}(g^{-1})}{\tilde{t}(g\cdot g^{-1})} = \hat{f}(g,g^{-1})\tilde{t}(g)\tilde{t}(g^{-1}) \tag{14.122}$$

where in the second equality we used the "gauge-preserving" property that $\tilde{t}(1) = 1$. Now, in any way you like, divide the non-involution elements of G into two disjoint sets $S_1 \amalg S_2$ so that no two group elements in S_1 are related by $g \to g^{-1}$. Then, if $g \in S_2$ we have $g^{-1} \in S_1$ and vice versa. Then we can choose a function $\tilde{t}$ so that for every $g \in S_2$ we have

$$\tilde{t}(g) = (\tilde{t}(g^{-1}))^{-1}(f^{(1)}(g,g^{-1}))^{-1} \tag{14.123}$$

Consequently:

$$f^{(2)}(g,g^{-1}) = 1 \qquad\qquad \forall g \in S_2 \tag{14.124}$$

It doesn't really matter what we choose for $\tilde{t}$ on S_1. For definiteness we choose it to be $= 1$. But if we had made another choice the above procedure would still lead to equation (14.124). Now recall from (14.93) that any cocycle f satisfies $f(g,g^{-1}) = f(g^{-1},g)$ for all g. Since $f^{(2)}$ is a cocycle (if we started with a cocycle f) then we conclude that for all the non-involutions:

$$f^{(2)}(g,g^{-1}) = f^{(2)}(g^{-1},g) = 1 \qquad\qquad \forall g \in S_1 \amalg S_2 \tag{14.125}$$

Note that there is still a lot of "gauge freedom": We have not yet constrained $\tilde{t}(g)$ for $g \in S_1$, nor have we constrained $\tilde{t}(g)$ for the involutions, that is, the group elements

g with $g^2 = 1$. What can we say about $f^{(2)}(g,g)$ for g an involution? we have

$$f^{(2)}(g,g) = f^{(1)}(g,g)\frac{\tilde{t}(g)^2}{\tilde{t}(g^2)} = f^{(1)}(g,g)(\tilde{t}(g))^2 \tag{14.126}$$

Now, it might, or might not be the case that $f^{(1)}(g,g)$ is a perfect square in the group. If it is not a perfect square then we are out of luck: We cannot make any further gauge transformations to set $f^{(2)}(g,g) = 1$. Now one can indeed check that the property of $f(g,g)$ being a perfect square, or not, for an involution g is a truly "gauge invariant" condition. Therefore we have proven: *If $f(g,g)$ is not a perfect square for some nontrivial involution g then we know that f is not "gauge equivalent" - that is, is not cohomologous to - the trivial cocycle. That is, $[f]$ is a nontrivial cohomology class.* Such cocycles will define nontrivial central extensions.

Example 1 . *Extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2$.* WLOG we can take $f(1,1) = f(1,\sigma) = f(\sigma,1) = 1$. Then we have two choices: $f(\sigma,\sigma) = 1$ or $f(\sigma,\sigma) = \sigma$. Each of these choices satisfies the cocycle identity and they are not related by a coboundary. Indeed σ is an involution and also σ is not a perfect square, so by our discussion above a cocycle with $f(\sigma,\sigma) = \sigma$ cannot be gauged to the trivial cocycle. In other words $H^2(\mathbb{Z}_2,\mathbb{Z}_2) = \mathbb{Z}_2$. For the choice $f = 1$ we obtain $\tilde{G} = \mathbb{Z}_2 \times \mathbb{Z}_2$. For the nontrivial choice $f(\sigma,\sigma) = \sigma$ we obtain $\tilde{G} \cong \mathbb{Z}_4$. Let us see this in detail. We'll let $\sigma_1 \in A \cong \mathbb{Z}_2$ and $\sigma_2 \in G \cong \mathbb{Z}_2$ be the nontrivial elements so we should write $f(\sigma_2,\sigma_2) = \sigma_1$. Note that $(\sigma_1, 1)$ has order 2, but then

$$(1,\sigma_2)\cdot(1,\sigma_2) = (f(\sigma_2,\sigma_2),1) = (\sigma_1,1) \tag{14.127}$$

shows that $(1,\sigma_2)$ has order 4. Moreover $(\sigma_1,\sigma_2) = (\sigma_1,1)(1,\sigma_2) = (1,\sigma_2)(\sigma_1,1)$. Thus,

$$\begin{aligned}\Psi &: (\sigma_1,1) \to \omega^2 = -1\\ \Psi &: (1,\sigma_2) \to \omega\end{aligned} \tag{14.128}$$

where ω is a primitive 4^{th} root of 1 defines an isomorphism with the group of fourth roots of unity. In conclusion, the nontrivial central extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2$ is:

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{14.129}$$

Recall that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. The square of this extension is the trivial extension.

Example 2. *Extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_p$.* The generalization of the previous example to the extension of $\mathbb{Z}_p$ by $\mathbb{Z}_p$ for an odd prime p is extremely instructive. So, let us study in detail the extensions

$$1 \to \mathbb{Z}_p \to G \to \mathbb{Z}_p \to 1 \tag{14.130}$$

In this example we will write our cyclic groups multiplicatively. Now, using methods of topology one can show that [118]

$$H^2(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p. \tag{14.131}$$

The result (14.131) should puzzle you. After all we know that G must be a group of order p^2, and we know from the class equation and Sylow's theorems that there are exactly two groups of order p^2, up to isomorphism! How is that compatible with the p distinct extensions predicted by equation (14.131) !? The answer is that there can be nonisomorphic extensions (14.22) involving the same group $\tilde{G}$. Let us see how this works in the present example by examining in detail the possible extensions:

$$1 \to \mathbb{Z}_p \xrightarrow{\iota} \mathbb{Z}_{p^2} \xrightarrow{\pi} \mathbb{Z}_p \to 1 \tag{14.132}$$

We write the first, second and third groups in this sequence as

$$\begin{aligned} \mathbb{Z}_p &= \langle \sigma_1 | \sigma_1^p = 1 \rangle \\ \mathbb{Z}_{p^2} &= \langle \alpha | \alpha^{p^2} = 1 \rangle \\ \mathbb{Z}_p &= \langle \sigma_2 | \sigma_2^p = 1 \rangle \end{aligned} \tag{14.133}$$

respectively.

For the injection ι we have

$$\iota(\sigma_1) = \alpha^x \tag{14.134}$$

for some x. For this to be a well-defined homomorphism we must have

$$\iota(1) = \iota(\sigma_1^p) = \alpha^{px} = 1 \tag{14.135}$$

and therefore $px = 0 \bmod p^2$ and therefore $x = 0 \bmod p$. But since ι must be an injection it must be of the form

$$\iota_k(\sigma_1) := \alpha^{kp} \tag{14.136}$$

where k is relatively prime to p. We can take

$$1 \le k \le p-1 \tag{14.137}$$

or (preferably) we can regard $k \in \mathbb{Z}_p^*$.

Similarly, for π we must have $\pi(\alpha) = \sigma_2^y$ for some y. Now, since π has to be surjective, σ_2^y must be a generator and hence π must be of the form

$$\pi_r(\alpha) = \sigma_2^r \qquad\qquad 1 \le r \le p-1 \tag{14.138}$$

where again we should really regard r as an element of $\mathbb{Z}_p^*$.

Note that the kernel of π_r is the set of elements α^ℓ with $\sigma_2^{\ell r} = 1$. This implies $\ell r = 0 \bmod p$ and therefore $\ell = 0 \bmod p$ so

$$\ker(\pi_r) = \{1, \alpha^p, \alpha^{2p}, \ldots, \alpha^{(p-1)p}\} \tag{14.139}$$

[118] You can also show it by examining the cocycle equation directly. We will write down the nontrivial cocycles presently.

Since $k \in \mathbb{Z}_p^*$ we have

$$\ker(\pi_r) = \mathrm{im}(\iota_k) \tag{14.140}$$

so our sequence is exact for any choice of $r, k \in \mathbb{Z}_p^*$. We have now described all the extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_p$. Let us find a representative cocycle $f_{k,r}$ for each of these extensions.

To find the cocycle we choose a section of π_r. It is instructive to try to make it a homomorphism. Therefore we must take $s(1) = 1$. What about $s(\sigma_2)$? It must be of the form $s(\sigma_2) = \alpha^x$ for some x, and since $\pi_r(s(\sigma_2)) = \sigma_2$ we must have

$$\sigma_2^{xr} = \sigma_2 \tag{14.141}$$

so that

$$xr = 1 \mathrm{mod}\ p \tag{14.142}$$

Recall that $r \in \mathbb{Z}_p^*$ and let r^* be the integer $1 \le r^* \le p-1$ such that

$$rr^* = 1 \mathrm{mod}\ p \tag{14.143}$$

Then we have that $x = r^* + \ell p$ for any ℓ. That is, $s(\sigma_2)$ could be any of

$$\alpha^{r^*}, \alpha^{r^*+p}, \alpha^{r^*+2p}, \dots, \alpha^{r^*+(p-1)p} \tag{14.144}$$

Here we will make the simplest choice $s(\sigma_2) = \alpha^{r^*}$. The reader can check that the discussion is not essentially changed if we make one of the other choices. (After all, this will just change our cocycle by a coboundary!)

Now that we have chosen $s(\sigma_2) = \alpha^{r^*}$, if s were a homomorphism then we would be forced to take:

$$\begin{aligned} s(1) &= 1 \\ s(\sigma_2) &= \alpha^{r^*} \\ s(\sigma_2^2) &= \alpha^{2r^*} \\ \vdots \quad & \quad \vdots \\ s(\sigma_2^{p-1}) &= \alpha^{(p-1)r^*} \end{aligned} \tag{14.145}$$

But now we are stuck! The property that s is a homomorphism requires two contradictory things. On the one hand, we must have $s(1) = 1$ for any homomorphism. On the other hand, from the above equations we also must have $s(\sigma_2^p) = \alpha^{pr^*}$. But because $1 \le r^* \le p-1$ we know that $\alpha^{pr^*} \ne 1$. So the conditions for s being a homomorphism are impossible to meet. Therefore, with this choice of section we find a nontrivial cocycle as follows:

$$s(\sigma_2^x)s(\sigma_2^y)s(\sigma_2^{x+y})^{-1} = \begin{cases} 1 & x+y \le p-1 \\ \alpha^{r^*p} & p \le x+y \end{cases} \tag{14.146}$$

Here we computed:

$$\alpha^{r^*x}\alpha^{r^*y}\alpha^{-r^*(x+y-p)} = \alpha^{r^*p} \tag{14.147}$$

where you might note that if $p \le x + y \le 2p - 2$ then $0 \le x + y - p \le p - 2$. Therefore, our cocycle is $f_{k,r}$ where

$$f_{k,r}(\sigma_2^x, \sigma_2^y) := \begin{cases} 1 & x + y \le p - 1 \\ \sigma_1^{k^* r^*} & p \le x + y \end{cases} \tag{14.148}$$

since

$$\iota_k(\sigma_1^{k^* r^*}) = \alpha^{k^* r^* kp} = \alpha^{r^* p} \tag{14.149}$$

and here we have introduced an integer $1 \le k^* \le p - 1$ so that

$$kk^* = 1 \text{ mod } p \tag{14.150}$$

Although it is not obvious from the above formula for $f_{k,r}$, we know that $f_{k,r}$ will satisfy the cocycle equation because we constructed it from a section of a group extension.

Now, we know the cocycle is nontrivial because $\mathbb{Z}_p \times \mathbb{Z}_p$ is not isomorphic to $\mathbb{Z}_{p^2}$. But let us try to trivialize our cocycle by a coboundary. So we modify our section to

$$\tilde{s}(\sigma_2^x) = \iota(t(\sigma_2^x)) s(\sigma_2^x) \tag{14.151}$$

We can always write our function t in the form

$$t(\sigma_2^x) = \sigma_1^{\tau(x)} \tag{14.152}$$

for some function $\tau(x)$ valued in $\mathbb{Z}/p\mathbb{Z}$. We are trying to find a function $\tau(x)$ so that the new cocycle $f_{\tilde{s}}$ is identically 1. We certainly need $\tilde{s}(1) = 1$ and hence $\tau(\bar{0}) = \bar{0}$. But now, because $f(\sigma_2^x, \sigma_2^y) = 1$ already holds for $x + y \le p - 1$ don't want to undo that so we learn that

$$\tau(x) + \tau(y) - \tau(x + y) = 0 \text{mod} p \tag{14.153}$$

for $x + y \le p - 1$. This means we must take

$$\tau(x) = x\tau(1) \qquad\qquad 1 \le x \le p - 1 \tag{14.154}$$

So, our coboundary is completely fixed up to a choice of $\tau(1)$. But now let us compute for $x + y \ge p - 1$:

$$\tilde{s}(\sigma_2^x)\tilde{s}(\sigma_2^y)\tilde{s}(\sigma_2^{x+y})^{-1} = \alpha^{r^* p}\iota(\sigma_1^{\tau(x)+\tau(y)-\tau(x+y)}) = \alpha^{r^* p} \tag{14.155}$$

So, we cannot gauge the cocycle to one, confirming what we already knew: The cocycle is nontrivial.

Now let us see when the different extensions defined by $k, r \in \mathbb{Z}_p^*$ are actually equivalent. To see this let us try to construct φ so that

$$\begin{tikzcd}
 & & \langle \alpha \rangle \arrow[dd, "\varphi"] \arrow[dr, "\pi_{r_1}"] & & \\
1 \arrow[r] & \langle \sigma_1 \rangle \arrow[ur, "\iota_{k_1}"] \arrow[dr, "\iota_{k_2}"'] & & \langle \sigma_2 \rangle \arrow[r] & 1 \\
 & & \langle \alpha \rangle \arrow[ur, "\pi_{r_2}"'] & &
\end{tikzcd} \tag{14.156}$$

Now φ, being a homomorphism, must be of the form

$$\varphi(\alpha) = \alpha^y \tag{14.157}$$

for some y. We know this must be an isomorphism so y must be relatively prime to p. Moreover commutativity of the diagram implies

$$\pi_{r_2}(\varphi(\alpha)) = \pi_{r_1}(\alpha) \qquad \Rightarrow \qquad r_2 y = r_1 \text{ mod} p \tag{14.158}$$

$$\varphi(\iota_{k_1}(\sigma_1)) = \iota_{k_2}(\sigma_1) \qquad \Rightarrow \qquad k_1 p y = k_2 p \text{ mod} p^2 \qquad \Rightarrow \qquad k_1 y = k_2 \text{ mod } p \tag{14.159}$$

Putting these equations together, and remembering that y is multiplicatively invertible modulo p we find that there exists a morphism of extensions iff

$$k_1 r_1 = k_2 r_2 \text{mod} p \tag{14.160}$$

Note that the cocycles $f_{k,r}$ constructed in (14.148) indeed only depend on krmod$p$. Equivalently, we can label their cohomology class by $(kr)^* = k^* r^*$mod$p$.

The conclusion is that $kr \in \mathbb{Z}_p^*$ is the invariant quantity. Extensions with the same group $\tilde{G} = \mathbb{Z}_{p^2}$ in the middle, but with different $kr \in \mathbb{Z}_p^*$, define inequivalent extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_p$.

Now let us examine the group structure on the group cohomology. Just multiplying the cocycles we get:

$$(f_{k_1,r_1} \cdot f_{k_2,r_2})(\sigma_2^x, \sigma_2^y) = \begin{cases} 1 & x+y \leq p-1 \\ \sigma_1^{(k_1 r_1)^* + (k_2 r_2)^*} & p \leq x+y \end{cases} \tag{14.161}$$

Thus if we map

$$[f_{k,r}] \mapsto (kr)^* \text{mod} \mathbb{Z}_p \tag{14.162}$$

we have a homomorphism of $H^2(G,A)$ to the additive group $\mathbb{Z}/p\mathbb{Z}$, with the trivializable cocycle representing the direct product and mapping to $\bar{0} \in \mathbb{Z}/p\mathbb{Z}$.

In conclusion, we describe the *group* of isomorphism classes of central extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_p$ as follows: The identity element is the trivial extension

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \to 1 \tag{14.163}$$

and then there is an orbit of $(p-1)$ nontrivial extensions of the form

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 1 \tag{14.164}$$

acted on by $\text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^*$.

Example 3:*Prime Powers.* Once we start to look at prime powers things start to get more complicated. We will content ourselves with extensions of $\mathbb{Z}_4$ by $\mathbb{Z}_2$. Here it can be shown that

$$H^2(\mathbb{Z}_4, \mathbb{Z}_2) \cong \mathbb{Z}_2 \tag{14.165}$$

so there should be two inequivalent extensions. One is the direct product and the other is

♣Do this more systematically so show that there are precisely two extensions of $\mathbb{Z}_4$ by $\mathbb{Z}_2$. ♣

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_8 \to \mathbb{Z}_4 \to 1 \tag{14.166}$$

We will think of these as multiplicative groups of roots of unity, with generators $\sigma = -1$ for $\mathbb{Z}_2$, $\alpha = \exp[2\pi i/8]$ for $\mathbb{Z}_8$, and $\omega = \exp[2\pi i/4]$ for $\mathbb{Z}_4$.

The inclusion map $\iota : \sigma \to \alpha^4$, while the projection map takes $\pi : \alpha \to \alpha^2 = \omega$.

Let us try to find a section. Since we want a normalized cocycle we must choose $s(1) = 1$. Now, $\pi(s(\omega)) = \omega$ implies $s(\omega)^2 = \omega$, and this equation has two solutions: $s(\omega) = \alpha$ or $s(\omega) = \alpha^5$. Let us choose $s(\omega) = \alpha$. (The following analysis for α^5 is similar.) If we try to make s into a homomorphism then we are forced to choose

$$\begin{aligned} s(\omega) &= \alpha \\ s(\omega^2) &= \alpha^2 \\ s(\omega^3) &= \alpha^3 \end{aligned} \tag{14.167}$$

but now we have no choice - we *must* set $s(\omega^4) = s(1) = 1$. On the other hand, if s *were* to have been a homomorphism we would have wanted to set $s(\omega^4) = s(\omega)^4 = \alpha^4$, but, as we just said, we cannot do this. With the above choice of section we get the symmetric cocycle whose nontrivial entries are

$$f(\omega,\omega^3) = f(\omega^2,\omega^2) = f(\omega^2,\omega^3) = f(\omega^3,\omega^3) = \alpha^4 = \sigma. \tag{14.168}$$

♣Probably should just describe all extensions with $Q = \mathbb{Z}_n$ ♣

Example 4.. *Products Of Cyclic Groups.* Another natural generalization is to consider products of cyclic groups. For simplicity we will only consider the case

$$G = \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p \tag{14.169}$$

where there are k summands, but p is prime. We will think of our group additively and moreover we will think of $\mathbb{Z}_p$ as a ring in this example. If we write elements as $\vec{x} = (x_1, \dots, x_k)$ with $x_i \in \mathbb{Z}_p$ and our cocycle $f(\vec{x},\vec{y})$ is also valued in $\mathbb{Z}_p$, so that we are considering central extensions:

$$0 \to \mathbb{Z}_p \to \widetilde{G} \to \mathbb{Z}_p^{\oplus k} \to 0 \tag{14.170}$$

then the cocycle condition becomes:

$$f(\vec{x},\vec{y}) + f(\vec{x}+\vec{y},\vec{z}) = f(\vec{x},\vec{y}+\vec{z}) + f(\vec{y},\vec{z}) \tag{14.171}$$

An obvious way to satisfy this condition is to use a bilinear form:

$$f(\vec{x},\vec{y}) = A_{ij}x_i y_j \tag{14.172}$$

where the matrix elements $A_{ij} \in \mathbb{Z}_n$. We can modify by a coboundary:

$$f(\vec{x},\vec{y}) \to f(\vec{x},\vec{y}) + q(\vec{x}+\vec{y}) - q(\vec{x}) - q(\vec{y}) \tag{14.173}$$

Notice a linear term cancels out. It we want to restrict attention to expressions which are quadratic then we can modify

$$A_{ij} \to A_{ij} - (q_{ij} + q_{ji}) \tag{14.174}$$

where q_{ij} is any matrix with values in $\mathbb{Z}_p$.

Now we must distinguish the case $p = 2$ from p an odd prime. If $p = 2$ we can use the coboundary to make the off-diagonal part asymmetric, and WLOG we can agree that for each $i < j$ either $A_{ij} = A_{ji} = 0$ or $A_{ij} = 0$ and $A_{ji} = 1$. Note that the diagonal matrix elements are gauge invariant since $q_{ii} + q_{ii} = 2q_{ii} = 0$. Therefore we can produce in this way $\frac{1}{2}k(k+1)$ independent cocycles.

If p is an odd prime we can require that the matrix is "anti-symmetric" in the sense that $A_{ij} + A_{ji} = 0$ for all i, j, because 2 is invertible. In this way we only produce $\frac{1}{2}k(k-1)$ independent cocycles.

On the other hand, using methods of topology (See section **** below for hints) one can prove that

$$H^2(\mathbb{Z}_p^{\oplus k}, \mathbb{Z}_p) \cong \mathbb{Z}_p^{\frac{1}{2}k(k+1)} \tag{14.175}$$

for any prime p. What are the k "missing" cocycles for p an odd prime? They are exactly the extensions we discussed in detail in Example 2 above!

Example 5.. As a special case of the above, consider extensions of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ by $\mathbb{Z}_2$. This will be a group of order 8. As we will see, there are five groups of order 8 up to isomorphism:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2^3, \quad Q, \quad D_4 \tag{14.176}$$

where Q and D_4 are the quaternion and dihedral groups, respectively. Now $\mathbb{Z}_8$ cannot sit in an extension of $\mathbb{Z}_2 \times \mathbb{Z}_2$. (Why not? [119]) This leaves 4 isomorphisms classes of groups which do fit in extensions of $\mathbb{Z}_2 \times \mathbb{Z}_2$ by $\mathbb{Z}_2$ and it happens they are all central extensions. They are:

$$\begin{aligned}
&1 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\
&1 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\
&1 \to \mathbb{Z}_2 \to Q \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\
&1 \to \mathbb{Z}_2 \to D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1
\end{aligned} \tag{14.177}$$

where Q is the quaternion group and D_4 the dihedral group. We have already met Q and D_4 above. One can define a homomorphism $\pi : Q \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by

$$\begin{aligned}
\pi(\pm 1) &= 0 = (0,0) \\
\pi(\pm \mathrm{i}\sigma^1) &= v_1 = (1,0) \\
\pi(\pm \mathrm{i}\sigma^2) &= v_2 = (0,1) \\
\pi(\pm \mathrm{i}\sigma^3) &= v_1 + v_2 = (1,1)
\end{aligned} \tag{14.178}$$

[119] *Answer*: Because $\mathbb{Z}_2 \times \mathbb{Z}_2$ would have to be a quotient of $\mathbb{Z}_8$. But we can easily list the subgroups of $\mathbb{Z}_8$ and no quotient is of this form.

where we are thinking of $\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z}$ additively to make contact with the previous example. We can choose a section:

$$\begin{aligned} s(v_1) &= \mathrm{i}\sigma^1 \\ s(v_2) &= \mathrm{i}\sigma^2 \\ s(v_1+v_2) &= \mathrm{i}\sigma^3 \end{aligned} \tag{14.179}$$

and, computing the cocycle we find that it is given by the bilinear form (see the previous exercise):

$$A_Q = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{14.180}$$

Similarly, we can define a homomorphism $\pi : D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$\begin{aligned} \pi(\pm 1) &= 0 = (0,0) \\ \pi(\pm R(\pi/2)) &= v_1 = (1,0) \\ \pi(\pm P) &= v_2 = (0,1) \\ \pi(\pm PR(\pi/2)) &= v_1 + v_2 = (1,1) \end{aligned} \tag{14.181}$$

We can choose a section:

$$\begin{aligned} s(v_1) &= R(\pi/2) \\ s(v_2) &= P \\ s(v_1+v_2) &= PR(\pi/2) \end{aligned} \tag{14.182}$$

and, computing the cocycle we find that it is given by the bilinear form (see the previous exercise):

$$A_{D_4} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \tag{14.183}$$

Now, on the other hand, using methods of topology one can prove that

$$H^2(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \tag{14.184}$$

We can understand this group in terms of the bilinear quadratic forms mentioned in the previous example. Under $A_{ij} \to A_{ij} - (q_{ij} + q_{ji})$. Note that A_{11} and A_{22} are invariant, but we can modify the off-diagonal part of A_{ij} by a symmetric matrix. Thus, there are 8 possible values for $A_{11}, A_{22}, A_{12} \in \mathbb{Z}_2$.

In a way analogous to our discussion of extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_p$, while there are only four different isomorphism classes of groups, there can be different extensions. An extension with group cocycle $A_{ij}x_1^i x_2^j$ defines a group of elements $(z, \vec{x})$. If we only care about the isomorphism class of the group we are free to consider an isomorphism

$$(z, \vec{x}) \mapsto (z, S\vec{x}) \tag{14.185}$$

where $S \in GL(2, \mathbb{Z}_2)$. This maps $A \to SAS^{tr}$. In general that will produce an isomorphic group, but a different extension.

♣Explain in detail how this takes us from 8 extensions to four isomorphism classes of groups using the explicit transforms by elements of $GL(2,\mathbb{Z}_2) \cong S_3$. ♣

♣Should add an exercise showing that $f(g,g)$ for g an involution determines the entire cocycle in this case. There are

In all our examples up to now the group $\tilde{G}$ has been Abelian, but in this example we have produced two nonisomorphic nonabelian groups Q and D_4 of order 8.

Example 5.. Nonabelian groups can also have central extensions. Indeed, we already saw this for $G = SO(3)$. Here is an example with G a nonabelian finite group. We take G to be the symmetric group S_n. It turns out that it has one nontrivial central extension by $\mathbb{Z}_2$:

$$H^2(S_n;\mathbb{Z}_2) \cong \mathbb{Z}_2 \tag{14.186}$$

To define it we let $\sigma_i = (i, i+1)$, $1 \le i \le n-1$ be the transpositions generating S_n. Then $\hat{S}_n$ is generated by $\hat{\sigma}_i$ and a central element z satisfying the relations:

♣Should also consider central extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. ♣

$$\begin{aligned} z^2 &= 1 \\ \hat{\sigma}_i^2 &= z \\ \hat{\sigma}_i\hat{\sigma}_{i+1}\hat{\sigma}_i &= \hat{\sigma}_{i+1}\hat{\sigma}_i\hat{\sigma}_{i+1} \\ \hat{\sigma}_i\hat{\sigma}_j &= z\hat{\sigma}_j\hat{\sigma}_i \qquad\qquad j > i+1 \end{aligned} \tag{14.187}$$

When restricted to the alternating group A_n we get an extension of A_n that can be elegantly described using spin groups.

Remarks:

1. One generally associates cohomology with the subject of topology. There is indeed a beautiful topological interpretation of group cohomology in terms of "classifying spaces."

2. In the case where G is itself abelian we can use more powerful methods of homological algebra to classify central extensions.

3. The special case $H^2(G, U(1))$ (or sometimes $H^2(G, \mathbb{C}^*)$, they are the same) is known as the *Schur multiplier*. It plays an important role in the study of projective representations of G. We will return to this important point.

4. We mentioned that a general extension (14.1) can be viewed as a principal N bundle over Q. Let us stress that trivialization of $\pi : G \to Q$ as a principal bundle is completely different from trivialization of the extension (by choosing a splitting). These are different mathematical structures! For example, for finite groups the bundle is of course trivial because any global section is also continuous. However, as we have just seen the extensions might be nontrivial. It is true, quite generally, that if a central extension is trivial as a group extension then $\tilde{G} = A \times G$ and hence $\pi : \tilde{G} \to G$ is trivializable as an A-bundle.

♣In general a central extension by $U(1)$ is equivalent to a line bundle over the group and you should explain that here. ♣

Exercise

Suppose that the central extension (14.22) is equivalent to the trivial extension with $\tilde{G} = A \times G$, the direct product. Show that the possible splittings are in one-one correspondence with the set of group homomorphisms $\phi : G \to A$.

Exercise

Construct cocycles corresponding to each of the central extensions in (14.177) and show how the automorphisms of $\mathbb{Z}_2 \times \mathbb{Z}_2$ account for the the fact that there are only four entries in (14.177) while (14.184) is order 8.

Exercise *D_4 vs. Q*

a.) Show that D_4 and Q both fit in exact sequences

$$1 \to \mathbb{Z}_4 \to D_4 \to \mathbb{Z}_2 \to 1 \tag{14.188}$$

$$1 \to \mathbb{Z}_4 \to Q \to \mathbb{Z}_2 \to 1 \tag{14.189}$$

b.) Are these <u>central</u> extensions?

c.) Are D_4 and Q isomorphic? [120]

Exercise

Choosing the natural section $s : \sigma_i \to \hat{\sigma}_i$ in (14.187) and find the corresponding cocycle f_s.

Exercise *Due Diligence*

Show that the associative law for the twisted product (14.102) is equivalent to the cocycle condition on the 2-cochain f.

Exercise *Involution Criterion For A Nontrivial Cocycle*

[120] *Answer*: No. D_4 has 5 nontrivial involutions: The reflections in the four symmetry axes of the square and the rotation by π, while Q has only one nontrivial involution, namely -1.

Let g be a nontrvial involution. Show that the condition that $f(g,g)$ is, or is not, a perfect square is independent of which cocycle we use within a cohomology class.

Exercise *Group Commutator Criterion For A Nontrivial Cocycle*

a.) Show that if a central extension is defined by a cocycle f then the group commutator is:

$$[(a_1,g_1),(a_2,g_2)] = \left(\frac{f(g_1g_2, g_1^{-1}g_2^{-1})}{f(g_2g_1, g_1^{-1}g_2^{-1})} \frac{f(g_1,g_2)}{f(g_2,g_1)}, g_1g_2g_1^{-1}g_2^{-1} \right) \tag{14.190}$$

b.) Suppose G is abelian. Show that $\tilde{G}$ is abelian iff $f(g_1,g_2)$ is symmetric.

c.) In general the condition that f is symmetric: $f(g_1,g_2) = f(g_2,g_1)$ would not be preserved by a coboundary transformation. Show that it does make sense in this setting.

d.) Suppose $\tilde{G}$ is a central extension of a not-necessarily-Abelian group G by an Abelian group A. Show that if (g_1,g_2) is a commuting pair of elements in G and if $f(g_1,g_2)/f(g_2,g_1)$ is not the identity then the extension is nontrivial. [121]

14.4 Extended Example: Charged Particle On A Circle Surrounding A Solenoid

In the following extended example we will illustrate how classical symmetries can be centrally extended in the context of a very interesting quantum system. Along the way we will take the opportunity to introduce many ideas about quantum field theory in a very simple context.

14.4.1 Hamiltonian Analysis

Consider a particle of mass m confined to a ring of radius r in the xy plane. The position of the particle is described by an angle ϕ, so we identify $\phi \sim \phi + 2\pi$, and the action is

$$S = \int \frac{1}{2} m r^2 \dot{\phi}^2 = \int \frac{1}{2} I \dot{\phi}^2 \tag{14.191}$$

with $I = mr^2$ the moment of inertia.

Let us also suppose that our particle has electric charge e and that the ring is threaded by a solenoid with magnetic field B, so the particle moves in a zero B field, but there is a nonzero gauge potential [122]

$$A = \frac{B}{2\pi} d\phi \tag{14.192}$$

[121] *Answer*: This follows because, as we saw above, a split central extension is a direct product. But the group commutator of $(1,g_1)$ and $(1,g_2)$ must then be the identity. On the other hand, $f(g_1,g_2)/f(g_2,g_1)$ is gauge invariant, so if it is nontrivial then the group commutator cannot be the identity.

[122] For readers not familiar with differential form notation this means, in cylindrical coordinates that $A_z = 0$, $A_r = 0$ and $A_\phi = B/2\pi$.

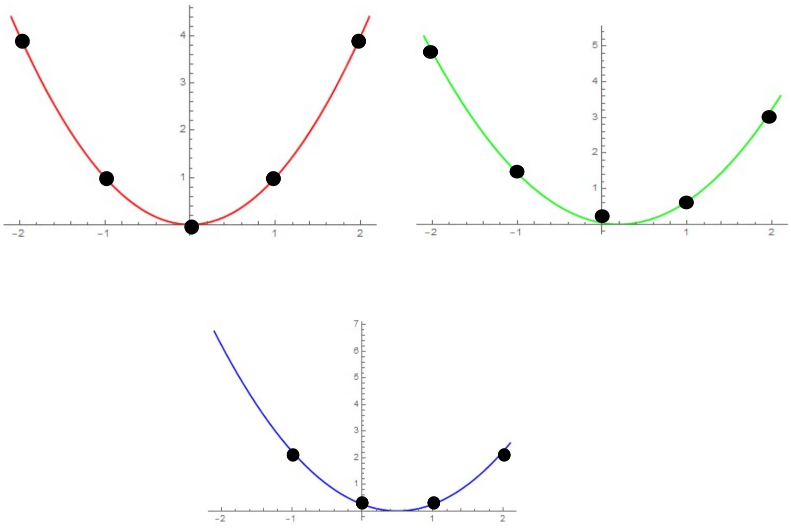

Figure 28: Spectrum of a particle on a circle as a function of $\mathcal{B} = eB/2\pi$. The upper left shows the low-lying spectrum for $\mathcal{B} = 0$. It is symmetric under $m \to -m$. The upper right shows the spectrum for $\mathcal{B} = 0.2$. There is no symmetry in the spectrum. The lower figure shows the spectrum for $\mathcal{B} = 1/2$. There is again a symmetry, but under $m \to 2\mathcal{B} - m = 1 - m$. In general there will be no symmetry unless $2\mathcal{B} \in \mathbb{Z}$. If $2\mathcal{B} \in \mathbb{Z}$ the spectrum is symmetric under $m \to 2\mathcal{B} - m$.

The action is therefore:

$$\begin{aligned} S &= \int \frac{1}{2} I \dot{\phi}^2 dt + \oint eA \\ &= \int \frac{1}{2} I \dot{\phi}^2 dt + \frac{eB}{2\pi} \dot{\phi} dt \end{aligned} \tag{14.193}$$

The second term is an example of a "topological term" or a "θ-term." Classically, the second term does not affect physical predictions, since it is a total derivative. However as we will soon see, quantum mechanically, it will have an important effect on physical predictions.

We are going to analyze the symmetries of this system and compare their realization in the classical and quantum theories.

Classical Symmetries:

We begin by analyzing the classical symmetries. Because the θ-term does not affect the classical dynamics the classical system has $O(2)$ symmetry. We can rotate: $R(\alpha) : e^{\mathrm{i}\phi} \to e^{\mathrm{i}\alpha} e^{\mathrm{i}\phi}$, or, if you prefer, translate $\phi \to \phi + \alpha$ (always bearing in mind that α and ϕ are only defined modulo addition of an integral multiple of 2π). If we think of the circle in the $x - y$ plane centered on the origin, with the solenoid along the z-axis then we could also take as usual:

$$R(\alpha) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \quad . \tag{14.194}$$

Also we can make a "parity" or "charge conjugation" transformation $P : \phi \to -\phi$. The second term in the Lagrangian is not invariant but this "doesn't matter" because it is a total derivative. Put differently: $\phi \to -\phi$ is a symmetry of the equations of motion, and hence it is a classical symmetry.

Note that these group elements in $O(2)$ satisfy

$$\begin{aligned} R(\alpha)R(\beta) &= R(\alpha+\beta) \\ P^2 &= 1 \\ PR(\alpha)P &= R(-\alpha) \end{aligned} \tag{14.195}$$

and indeed, as we have seen, $O(2)$ is a semidirect product:

$$O(2) = SO(2) \rtimes \mathbb{Z}_2 \tag{14.196}$$

with $\omega : \langle P\rangle \cong \mathbb{Z}_2 \to \mathrm{Aut}(SO(2)) \cong \mathbb{Z}_2$ acting by taking the nontrivial element of $\mathbb{Z}_2$ to the outer automorphism that sends $R(\alpha) \to R(-\alpha)$.

Diagonalizing The Hamiltonian

Now let us consider the quantum mechanics with the "θ-term" added to the Lagrangian. Our goal is to see how that term affects the quantum theory.

We will first analyze the quantum mechanics in the Hamiltonian approach. See the remark below for some remarks on the path integral approach. The conjugate momentum is

$$L = I\dot{\phi} + \frac{eB}{2\pi} \tag{14.197}$$

We denote it by L because it can be thought of as angular momentum.

Note that the coupling to the flat gauge field has altered the usual relation of angular momentum and velocity. Now we obtain the Hamiltonian from the Legendre transform:

$$\int L\dot{\phi}dt - S = \int \frac{1}{2I}(L - \frac{eB}{2\pi})^2 dt \tag{14.198}$$

Upon quantization $L \to -\mathrm{i}\hbar\frac{\partial}{\partial\phi}$, so the Hamiltonian is

$$H_{\mathcal{B}} := \frac{\hbar^2}{2I}\left(-\mathrm{i}\frac{\partial}{\partial\phi} - \mathcal{B}\right)^2 \tag{14.199}$$

where $\mathcal{B} := \frac{eB}{2\pi\hbar}$.

The eigenfunctions of the Hamiltonian $H_{\mathcal{B}}$ are just

$$\Psi_m(\phi) = \frac{1}{\sqrt{2\pi}} e^{\mathrm{i}m\phi} \qquad m \in \mathbb{Z} \tag{14.200}$$

They give energy eigenstates with energy

$$E_m = \frac{\hbar^2}{2I}(m - \mathcal{B})^2 \tag{14.201}$$

There is just one energy eigenstate for each $m \in \mathbb{Z}$.

Before moving on with the analysis of the symmetries in this quantum mechanical problem let us take the opportunity to make a long list of:

Remarks:

1. The action (14.193) makes good sense for ϕ valued in the real line or for $\phi \sim \phi + 2\pi$, valued in the circle. Making this choice is important in the choice of what theory we are describing. Where - in the above analysis - did we make the choice that the target space is a circle? [123]

2. Taking $\phi \sim \phi + 2\pi$, even though the θ-term is a total derivative it has a nontrivial effect on the quantum physics as we can see since B has shifted the spectrum of the quantum Hamiltonian in a physically observable fashion: *This is how we see that topological terms matter.*

3. Note that when $2\mathcal{B}$ is even the energy eigenspaces are two-fold degenerate, except for the ground state at $m = \mathcal{B}$. On the other hand, when $2\mathcal{B}$ is odd all the energy eigenspaces are two-fold degenerate, including the ground state. If $2\mathcal{B}$ is not an integer all the energy eigenspaces are one-dimensional. See Figure 28.

4. The total spectrum is *periodic* in $\mathcal{B}$, and shifting $\mathcal{B} \to \mathcal{B}+1$ is equivalent to $m \to m+1$. To be more precise, we can define a unitary operator on the Hilbert space by its action on a basis:

$$U\Psi_m = \Psi_{m+1} \tag{14.202}$$

and

$$UH_{\mathcal{B}}U^{-1} = H_{\mathcal{B}+1} \tag{14.203}$$

5. The quantum mechanics problem (14.193) and the spectrum (14.201) arise in the discussion of the "Coulomb blockade" in physics of quantum dots. See Yoshimasa Murayama, *Mesoscopic Systems*, Section 10.10.

6. *Viewing the system as a field theory.* We have introduced this system as describing the quantum mechanics of a particle. However, it is important to note that it can also be viewed as a special case of a quantum field theory. In general, in a field theory [124] we have a spacetime M and the fields ϕ are functions on M valued in some *target*

[123] *Answer*: If we took the case where ϕ is valued in $\mathbb{R}$ and not the circle then there would be no quantization on m and the spectrum of the Hamiltonian would be continuous. In this case the Chern-Simons term would not affect the physics in the quantum mechanical version as well.

[124] As traditionally conceived. The topic of topological field theory generalizes the next few lines considerably.

space $\mathcal{X}$. (So the term "target space" means nothing more or less than the codomain of the fields.) An important example is that of a nonrelativistic particle of mass m moving on a Riemannian manifold X with metric $ds^2 = g_{\mu\nu}(x)dx^\mu \otimes dx^\nu$. The action would be

$$S = \int dt \frac{m}{2} g_{\mu\nu}(x(t))\dot{x}^\mu \dot{x}^\nu dt \tag{14.204}$$

If, in addition, the particle has charge e and there is an electromagnetic potential $A_\mu(x)dx^\mu$ on X then the action is

$$S = \int dt \frac{m}{2} g_{\mu\nu}(x(t))\dot{x}^\mu \dot{x}^\nu dt + \int eA_\mu(x(t))\dot{x}^\mu dt \tag{14.205}$$

Here M is the manifold of time. It could be $M = \mathbb{R}$ if we describe the entire history of the particle, or $M = [t_{in}, t_{fin}]$ if we describe only the motion in a finite time interval. As we will soon see, it can also be interesting to let $M = S^1$. The "field" is a suitably differentiable map

$$x : M \to X \tag{14.206}$$

describing the position of the particle as a function of time. This is an example of a "$0+1$ dimensional field theory." A generalization would be a theory of maps from a d-dimensional spacetime with metric $h_{ab}d\sigma^a d\sigma^b$ and action

$$S = \int d^{d+1}\sigma \sqrt{|\det h|} h^{ab}(\sigma) \frac{1}{2} m g_{\mu\nu}(x(t))\partial_a x^\mu \partial_b x^\nu \tag{14.207}$$

and the "field" would be a suitably differentiable map:

$$x : M \to X \tag{14.208}$$

Equations (14.205) and (14.207) are examples of what is known as a "nonlinear sigma model." [125] In our case our fields are maps

$$e^{\mathrm{i}\phi} : M \to S^1 \tag{14.212}$$

We have been referring to $\phi \to -\phi$ as "parity" because that is the appropriate term in the context of the quantum mechanics of a particle constrained to a circle in the

[125] For the mathematically sophisticated reader we note that, for general nonlinear sigma models

$$dx : T_\sigma M \to T_{x(\sigma)} X \tag{14.209}$$

is a linear map between two inner-product spaces. We can use the inner products to define $(dx)^\dagger$ and then the kinetic term is

$$\int_M \mathrm{Tr}((dx)(dx)^\dagger)\mathrm{vol}\,(h) \tag{14.210}$$

More to the point dx is a section of $(TM)^\vee \otimes f^*(TX)$ and we can use the metric on this bundle to write $\int_M \parallel dx \parallel^2$. In the case of the charged particle moving on the Riemannian manifold X, there is also the data of a principal $U(1)$ bundle with connection $d + A$ and the topological term is based on the holonomy of the pulled back connection:

$$S = \int \frac{m}{2} \parallel dx \parallel^2 dt + \oint ex^*(A) \tag{14.211}$$

There are similar topological terms for the $d > 0$ sigma models.

plane. The parity operation is just reflection around some line in the plane. However, if we take the point of view that we are discussing a $0+1$ dimensional "field theory" then it would be better to refer to the operation as "charge conjugation" because it complex conjugates the $U(1)$-valued field $e^{\mathrm{i}\phi}$.

In addition there are (in the field theory interpretation) "worldvolume symmetries" of time translation invariance and time reversal. These form the group $\mathbb{R} \rtimes \mathbb{Z}_2$. We will put those aside. (Note that time reversal is not a symmetry of the second term in the Lagrangian but is a symmetry of the space of solutions of the equations of motion.)

7. *Relations to higher dimensional field theories and string theory.* The θ-term we have added has a very interesting analog in $1+1$ dimensional field theory, where it is known as a coupling to the B-field. It can also be obtained from a Kaluza-Klein reduction of $1+1$ dimensional Maxwell theory:

$$\begin{aligned} S &= \frac{1}{e^2}\int dx^0 dx^1 F_{01}^2 + \int \frac{\theta}{2\pi} F_{01} dx^0 \wedge dx^1 \\ &= \frac{1}{e^2}\int F * F + \int \frac{\theta}{2\pi} F \end{aligned} \tag{14.213}$$

In $1+1$ dimensional theory we can choose $A_0 = 0$ gauge and gauge away the x^1 dependence so that on $S^1 \times \mathbb{R}$ the only gauge invariant quantity is

$$e^{\mathrm{i}\phi(t)} = e^{\mathrm{i}\oint_{S^1} A} = e^{\mathrm{i}\oint_{S^1} A_1 dx^1} \tag{14.214}$$

With this in mind we can say

$$\theta = 2\pi\mathcal{B} \tag{14.215}$$

Remark: More generally, in $1+1$ dimensional Yang-Mills theory on $S^1 \times \mathbb{R}$ we can always go to $A_0 = 0$ gauge and then the only gauge invariant observable is the conjugacy class of the holonomy around the circle.

The theta term also has a close analog in $3+1$-dimensional gauge theory. In the case of $3+1$ dimensional Maxwell theory we can write

$$\begin{aligned} S &= \int d^4x \frac{1}{4e^2} F_{\mu\nu}F^{\mu\nu} + \int \frac{\theta}{8\pi}\epsilon^{\mu\nu\lambda\rho}F_{\mu\nu}F_{\lambda\rho}d^4x \\ &= \int \frac{1}{2e^2} F * F + \int \frac{\theta}{(4\pi)} F \wedge F \end{aligned} \tag{14.216}$$

In fact, in the effective theory of electromagnetism in the presence of an insulator a very similar action arises with a θ term. If a parity- and/or time-reversal symmetry is present then θ is zero or π, corresponding to our case $2\mathcal{B} \in \mathbb{Z}$. The difference between a normal and a topological insulator is then, literally, the difference between

$2\mathcal{B}$ being even (normal) and odd (topological), respectively. Finally, in the 3+1-dimensional Yang-Mills theories that describe the standard model of electro-weak and strong interactions one can add an analogous θ-term. Topological terms matter, and in this case the topological term for the strong gauge field leads to the prediction of an intrinsic electric dipole moment of the neutron. However, to excellent accuracy it is known that if the neutron dipole moment it is very small and

$$|\theta| < 10^{-9} \tag{14.217}$$

One of the great unsolved mysteries about nature is why the (effective) theta angle for the strong interactions in the standard model is so small. [126]

Now let us get back to the symmetries of the particle on the ring. We have seen that the classical "internal" symmetry group - the "internal" symmetry group of the equations of motion - is $O(2)$. Now let us analyze how the symmetries are implemented in the quantum theory:

In quantum mechanics the $SO(2)$ shift symmetry $\phi \to \phi + \alpha$ is realized by a translation operator $\rho(R(\alpha)) = \mathcal{R}(\alpha)$ and acting on Ψ_m we have

$$(\mathcal{R}(\alpha) \cdot \Psi_m) = e^{\mathrm{i}m\alpha}\Psi_m \tag{14.218}$$

Can we also represent $\rho(P) = \mathcal{P}$ on the Hilbert space? Classically, parity symmetry P just takes $\phi \to -\phi$. If we make this substitution in the Hamiltonian $H_{\mathcal{B}}$ we see that the naive parity operation takes

$$\mathcal{P} H_{\mathcal{B}} \mathcal{P}^{-1} = H_{-\mathcal{B}} \tag{14.219}$$

For general values of $\mathcal{B}$ the operator $H_{\mathcal{B}}$ is not unitarily equivalent to $H_{-\mathcal{B}}$. However, thanks to (14.203) it is clear that when $2\mathcal{B} \in \mathbb{Z}$ they are unitarily equivalent and the naive operation of taking $\phi \to -\phi$, which takes $m \to -m$ on eigenvectors of $H_{\mathcal{B}}$, should be accompanied by $U^{2\mathcal{B}}$. Therefore $\mathcal{P}$ should map the eigenspace associated with m to that associated with with $2\mathcal{B} - m$. As a sanity check note that indeed $E_m = E_{2\mathcal{B}-m}$. Therefore we should define a parity operation:

$$\mathcal{P} \cdot \Psi_m = \xi_m \Psi_{2\mathcal{B}-m} \tag{14.220}$$

where ξ_m is a phase which we can take to be 1. Note that the operator $\mathcal{P}$ so defined commutes with the Hamiltonian: Indeed, it takes eigenvectors to eigenvectors with the same eigenvalue.

♣You should allow the possibility of a phase in the definition of $\mathcal{P}$ and show in detail it doesn't matter. ♣

If $2\mathcal{B}$ is not an integer the parity symmetry is broken and the quantum symmetry group is just $SO(2)$.

Now consider the case when $2\mathcal{B} \in \mathbb{Z}$ and let us study the relations obeyed by the operators $\mathcal{R}(\alpha)$ and $\mathcal{P}$ and compare them with the classical relations (14.195). We still have $\mathcal{R}(\alpha)\mathcal{R}(\beta) = \mathcal{R}(\alpha + \beta)$ and $\mathcal{P}^2 = 1$ but now the third line of (14.195) is modified to:

$$\mathcal{P}\mathcal{R}(\alpha)\mathcal{P} = e^{\mathrm{i}2\mathcal{B}\alpha}\mathcal{R}(-\alpha) \tag{14.221}$$

[126] For much more about this see M. Dine's TASI lectures https://arxiv.org/pdf/hep-ph/0011376.pdf.

Exercise *Due Diligence*

a.) Check that (14.221) is well-defined, even though α is only defined up to a shift by an integral multiple of 2π.

b.) Check the operator relation (14.221)!

We now consider the group of operators generated by the operators $\mathcal{P}$, $\mathcal{R}(\alpha)$, and $z1_{\mathcal{H}}$ where $z \in U(1)$. (Do not forget that we identify $\alpha \sim \alpha + 2\pi$. This will be quite important in what follows.) Denote this group of operators by $\mathcal{G}_{\mathcal{B}}$. Naively we might have expected this group of operators on Hilbert space to be isomorphic to $U(1) \times O(2)$ where $O(2)$ is our classical symmetry group and $U(1)$ is just the group of phases acting on wavefunctions by scalar multiplication. However, equation (14.221) is not satisfied by a direct product. So, how is $\mathcal{G}_{\mathcal{B}}$ related to $U(1)$ and $O(2)$? General principles tell us it will be an extension

$$\begin{tikzcd} 1 \arrow[r] & U(1) \arrow[r] & \mathcal{G}_B \arrow[r] & O(2) \arrow[r] & 1 \end{tikzcd} \tag{14.222}$$

But what extension?

Now, when $\mathcal{B}$ is an integer we can indeed define an isomorphism of $\mathcal{G}_{\mathcal{B}}$ with $U(1) \times O(2)$ by setting

$$\tilde{\mathcal{R}}(\alpha) := e^{-\mathrm{i}\mathcal{B}\alpha}\mathcal{R}(\alpha) \tag{14.223}$$

We now recover the standard relations of $O(2)$, so the classical $O(2)$ symmetry is not modified quantum mechanically. However, when $\mathcal{B}$ is a half-integer, $\tilde{\mathcal{R}}$ is not well-defined since we must identify $\alpha \sim \alpha + 2\pi$. In this case the group $\mathcal{G}_{\mathcal{B}}$ is really different.

To understand what happens when $\mathcal{B}$ is half-integral we introduce a new group called Spin(2). As an abstract group it is isomorphic to $SO(2)$, and $U(1)$, and $\mathbb{R}/\mathbb{Z}$. The groups are all isomorphic. What makes Spin(2) nontrivial is its relation to $SO(2)$. The group elements in Spin(2) can be parametrized by $\hat{\alpha}$ with $\hat{\alpha} \sim \hat{\alpha} + 2\pi$. Let us call the elements of the spin group $\hat{R}(\hat{\alpha})$. You can think of it in terms of Pauli matrices as

$$\hat{R}(\hat{\alpha}) = \exp[\hat{\alpha}\sigma^1\sigma^2] = \cos(\hat{\alpha}) + \mathrm{i}\sin(\hat{\alpha})\sigma^3 \tag{14.224}$$

But it is called the *spin group* because it comes with a nontrivial double cover:

$$\pi : \mathrm{Spin}(2) \to SO(2) \tag{14.225}$$

the double covering is given by restricting our standard projection $\pi : SU(2) \to SO(3)$ to the subgroup of $SU(2)$ in (14.224). In this way we get a double cover of the rotation group around the z axis:

$$\pi : \hat{R}(\hat{\alpha}) \mapsto R(2\hat{\alpha}) \tag{14.226}$$

See equation (14.48) above.

Now, taking $\mathbb{Z}_2$ to act on Spin(2) by the nontrivial outer automorphism. So, denoting the nontrivial element of $\mathbb{Z}_2$ by $\hat{P}$ we use the homomorphism $\alpha : \mathbb{Z}_2 \to \mathrm{Aut}(\mathrm{Spin}(2))$ defined by

$$\alpha(\hat{P}) : \hat{R}(\hat{\alpha}) \to (R(\hat{\alpha}))^{-1} = \hat{R}(-\hat{\alpha}) \tag{14.227}$$

Then, one definition of the group $\mathrm{Pin}^+(2)$ is that it is the semidirect product:

$$\mathrm{Pin}^+(2) \cong \mathrm{Spin}(2) \rtimes_\alpha \mathbb{Z}_2 \tag{14.228}$$

(We will give a slightly different definition below.) There is a generalization of Spin and Pin groups to higher dimensions. They double cover $SO(d)$ and $O(d)$, respectively. See the remark below for a brief description and Chapters *** and **** for full details.

Now, when $2\mathcal{B}$ is an odd integer the group $\mathcal{G}_B$ is generated by

$$\begin{aligned} & z\mathbf{1}_{\mathcal{H}} \\ \rho(\hat{R}(\hat{\alpha})) &:= e^{-\mathrm{i}(2\mathcal{B})\hat{\alpha}}\mathcal{R}(2\hat{\alpha}) \qquad\qquad 0 \le \hat{\alpha} < 2\pi \\ \rho(\hat{P}) &:= \mathcal{P} \end{aligned} \tag{14.229}$$

where we take $\hat{P}$ to be the nontrivial element in $\mathbb{Z}_2$ in the semidirect product that defines $\mathrm{Pin}^+(2)$, so that $\hat{R}(\hat{\alpha})$ and $\hat{P}$ generate $\mathrm{Pin}^+(2)$. One checks that ρ is a homomorphism and the image under ρ is an isomorphic copy of $\mathrm{Pin}^+(2)$ inside $\mathcal{G}_B$, and we have:

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}_2 \arrow[r] \arrow[d] & \mathrm{Pin}^+(2) \arrow[r] \arrow[d, "\rho"] & O(2) \arrow[r] \arrow[d, "Id"] & 1 \\ 1 \arrow[r] & U(1) \arrow[r] & \mathcal{G}_B \arrow[r] & O(2) \arrow[r] & 1 \end{tikzcd} \tag{14.230}$$

where $\mathbb{Z}_2 \cong \{\pm 1\} \subset U(1)$. When $2\mathcal{B}$ is odd ρ has no kernel. (When $2\mathcal{B}$ is even there is a kernel.)

In conclusion:

1. The classical theory has an $O(2)$ symmetry.

2. In the quantum theory when $2\mathcal{B}$ is not an integer the symmetry is broken to $SO(2)$.

3. In the quantum theory, when $2\mathcal{B}$ is an even integer the theory still has $O(2)$ symmetry. The sequence
$$\begin{tikzcd} 1 \arrow[r] & U(1) \arrow[r] & \mathcal{G}_B \arrow[r] & O(2) \arrow[r] & 1 \end{tikzcd} \tag{14.231}$$
splits and $\mathcal{G}_B \cong U(1) \times O(2)$.

4. In the quantum theory, when $2\mathcal{B}$ is an odd integer,
$$\begin{tikzcd} 1 \arrow[r] & U(1) \arrow[r] & \mathcal{G}_B \arrow[r] & O(2) \arrow[r] & 1 \end{tikzcd} \tag{14.232}$$
does not split. When we try to realize the classical $O(2)$ symmetry on the Hilbert space we are forced to implement the pin double cover $\mathrm{Pin}^+(2)$, a central extension of $O(2)$ by $\mathbb{Z}_2$. It is related to $\mathcal{G}_\mathcal{B}$ as in (14.230).

We conclude with some remarks:

1. We stress that the particle we put on the ring did NOT have any intrinsic spin!! Having said that, if we define an angular momentum $\mathcal{L}$ so that $H = \frac{\mathcal{L}^2}{2I}$ then indeed when $\mathcal{B}$ is half-integral the angular momentum has half-integral eigenvalues, as one expects for a spin representation. So, what we are finding is that the half flux quantum is inducing a half-integral spin of the system so that the classical $O(2)$ symmetry of the classical system is implemented as a $\mathrm{Pin}^+(2)$ symmetry in the quantum theory. This is an intriguing phenomenon appearing in quantum symmetries with nontrivial gauge fields and topological terms: The statistics and spins of particles can be shifted from their classical values, often in ways that involve curious fractions.

2. *Spin And Pin Groups.* Enquiring minds will wonder about the definition of $\mathrm{Pin}^{\pm}(d)$. These groups are defined using Clifford algebras. For much more detail and motivation see the two chapters on Clifford algebras and Spin groups. In brief, consider the Clifford algebra generated by $\{\gamma_i, \gamma_j\} = 2Q_{ij}$ where Q_{ij} is an invertible $d \times d$ symmetric matrix. For a vector v^i define $\gamma(v) := v^i\gamma_i$. Assume that $Q_{ij} = \delta_{ij}$. Then $\mathrm{Pin}^+(d)$ is the group of expressions of the form

$$\pm\gamma(v_1)\cdots\gamma(v_r) \tag{14.233}$$

for some r. The group $\mathrm{Pin}^-(d)$ is similarly defined with $Q_{ij} = -\delta_{ij}$. The group $\mathrm{Spin}(d)$ is the subgroup of such expressions where r is even. The projection $\pi : \mathrm{Pin}^{\pm}(d) \to O(d)$ is defined by the equation:

$$\gamma(\pi(g)\cdot w) = (-1)^r g\gamma(w)g^{-1} \tag{14.234}$$

The key idea here is that

$$-\gamma(v)\gamma(w)\gamma(v)^{-1} = \gamma(R_v(w)) \tag{14.235}$$

where $R_v(w)$ is the reflection of w through the plane orthogonal to v, as the reader can easily check in an exercise below. Then use the fact that all elements of $O(d)$ are products of reflections. The restriction to $\mathrm{Spin}(d)$ defines $\pi : \mathrm{Spin}(d) \to SO(d)$. This is a generalization of our standard double-covering $\pi : SU(2) \to SO(3)$. Although $\mathrm{Spin}(3) \cong SU(2)$ for $d > 3$ $\mathrm{Spin}(d)$ is not isomorphic to a unitary or orthogonal group. The difference between $\mathrm{Pin}^+(d)$ and $\mathrm{Pin}^-(d)$ is whether the lift of a reflection will square to $+1$ or -1 respectively. As a group $\mathrm{Pin}^-(d)$ is isomorphic to $(\mathrm{Spin}(2) \rtimes \mathbb{Z}_4)/\mathbb{Z}_2$.

3. It is instructive to study the representation of $\mathrm{Pin}^+(2)$ on the two-dimensional space of ground states, $\mathcal{H}_{\mathrm{grnd}}$, when $\mathcal{B} = 1/2$. In this case we can choose the ordered basis $\{\Psi_0, \Psi_1\}$ for $\mathcal{H}_{\mathrm{grnd}}$, and, relative to this basis we have a matrix representation:

$$\begin{aligned} \rho(\widehat{R}(\hat{\alpha}))|_{\mathcal{H}_{\mathrm{grnd}}} &= \begin{pmatrix} e^{-\mathrm{i}\hat{\alpha}} & 0 \\ 0 & e^{\mathrm{i}\hat{\alpha}} \end{pmatrix} \\ \rho(\widehat{P})|_{\mathcal{H}_{\mathrm{grnd}}} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned} \tag{14.236}$$

We stress the appearance of $\hat{\alpha}$ in the representation matrix. This transformation corresponds to a translation of ϕ by $\alpha = 2\hat{\alpha}$. Had we tried to express the representation in terms of α we would encounter the phase $e^{\pm i\alpha/2}$ which is not well-defined because α is only defined modulo $\alpha \sim \alpha + 2\pi$.

4. As pointed out in a recent paper [127] this extension of the symmetry group at half-integral θ is an excellent baby model for how one can learn about nontrivial dynamics of quantum systems (in particular, QCD) by thinking carefully about group extensions. For example, if we were to add a potential $U(\phi)$ to the problem we just discussed we could no longer solve exactly for the eigenstates. Also, a generic potential would be of the form

$$U^{generic}(\phi) = \sum_{n\in\mathbb{Z}} c_n \cos(n\phi) + \sum_{n\in\mathbb{Z}} s_n \sin(n\phi) \tag{14.237}$$

Potentials with generic coefficients will explicitly break all of the $O(2)$ symmetry. Suppose however, that we can restrict attention to a special class of potentials with only cosine Fourier coefficients that are 0 mod 2:

$$U^{special}(\phi) = \sum_{n} u_n \cos(2n\phi) \tag{14.238}$$

Then, even though we cannot solve the spectrum of the Hamiltonian exactly we can make an interesting statement about it. For such potentials the classical $O(2)$ symmetry is explicitly broken to $\mathbb{Z}_2 \times \mathbb{Z}_2$ generated by $P : \phi \to -\phi$ and $r : \phi \to \phi + \pi$. We have shown that when $2\mathcal{B}$ is odd and the potential is zero the $O(2)$ symmetry is centrally extended and realized as the double-cover $\mathrm{Pin}^+(2)$ on the Hilbert space. The double cover of the subgroup group $\langle P, r\rangle \subset O(2)$ acting on Hilbert space is described by the pullback diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}_2 \arrow[r, "\iota"] \arrow[d, "\mathrm{Id}"] & D_4 \arrow[r, "\pi_1"] \arrow[d, "\iota"] & \mathbb{Z}_2 \times \mathbb{Z}_2 \arrow[r] \arrow[d, "\iota"] & 1 \\
1 \arrow[r] & \mathbb{Z}_2 \arrow[r] & \mathrm{Pin}^+(2) \arrow[r, "\pi_2"] & O(2) \arrow[r] & 1
\end{tikzcd} \tag{14.239}$$

To check this note that P lifts to the operators $\pm\mathcal{P}$ and $r = R(\pi)$ lifts to the operators

$$\pm\hat{r} = e^{i\mathcal{B}\pi}\mathcal{R}(\pi) \tag{14.240}$$

One checks that $\langle \mathcal{P}, \hat{r}\rangle$ generates a group isomorphic to D_4. Indeed, these operators satisfy the defining relations of D_4: $\mathcal{P}^2 = 1$, $\hat{r}^4 = 1$, and $\mathcal{P}\hat{r}\mathcal{P} = \hat{r}^{-1}$. Note that, in addition $\hat{r}^2 = -1$ on the entire Hilbert space. The representation on the Qbit groundstate in (14.236) (with $\hat{\alpha} = \pm\pi/2$) is a two-dimensional irrep of D_4. In fact all the doubly degenerate energy eigenspaces are two-dimensional irreps of D_4.

[127] D. Gaiotto, A. Kapustin, Z. Komargodski and N. Seiberg, "Theta, Time Reversal, and Temperature," https://arxiv.org/pdf/1703.00501.pdf

It is reasonable to assume that when we turn on a weak potential of the form (14.238) the classically preserved $\mathbb{Z}_2 \times \mathbb{Z}_2$ subgroup again lifts to a D_4 action on the Hilbert space, even though we can no longer construct the operators in the D_4 group explicitly. The cocycle is discrete: So if it is a continuous function of the parameters u_n at $u_n = 0$ (this is an assumption) then the classical $\mathbb{Z}_2 \times \mathbb{Z}_2$ symmetry must be realized by D_4 on the Hilbert space.

Now, we saw that, in the absence of the potential, there is a Qbit giving a two-dimensional representation of $\mathrm{Pin}^+(2)$. This representation restricts to an irreducible two-dimensional representation of D_4. (See equation (14.236) with $\hat{\alpha} = \pm\pi/2$.) Now, D_4 has four one-dimensional irreducible representations $\mathbf{1}_{\pm,\pm}$ and, we will show later, exactly one two-dimensional irreducible representation. In particular, the set of representations of D_4 is discrete. Again, it is reasonable to suppose that the representation is a continuous function of u_n. Again, this is an assumption. But granting this, turning on a weak potential cannot change the decomposition of the energy eigenspaces into irreducible representations. This leads to a striking prediction: The two-fold groundstate degeneracy is not broken by potentials of the form (14.238) when $2\mathcal{B}$ is odd! This is remarkable when one compares to the standard discussion of the double-well potential of one-dimensional quantum mechanics. In that standard case one has a two-fold classical degeneracy broken by tunneling (instanton) effects so that there is a unique ground state. For potentials of the form (14.238) there are (generically) four stationary points of the potential, at $\phi = 0, \pm\pi/2, \pi$. Generically, two will be maxima and two will be minima. So, classically, and perturbatively in quantum mechanics, for a generic potential of the form (14.238) there will be a two-fold degenerate groundstate. However, unlike the textbook discussion of the double-well potential, the degeneracy will not be lifted by nonperturbative tunneling effects.

Exercise

Show that the ground state energy is

$$E_{\text{ground}} = Min_{m\in\mathbb{Z}} \frac{\hbar^2}{2I} (m - \mathcal{B})^2 \tag{14.241}$$

and, using the floor function, give a formula for E_{ground} directly in terms of $\mathcal{B}$ (without requiring minimization).

Exercise *Pin Action*

a.) Show that (14.234) defines a homomorphism to $O(d)$. [128]

[128] *Answer*: The key equation to check is (14.235). To check this consider the two cases that w is parallel to v and that w is perpendicular to v. Then note that every element in $O(d)$ is a product of reflections.

b.) Show that the general definition of $\mathrm{Pin}^{+}(d)$ specializes to the definition of $\mathrm{Pin}^{+}(2)$ as a semidirect product. [129]

Exercise *One-Dimensional Representations Of D_4*
Show that there are four distinct one-dimensional representations of D_4. [130]

Exercise *A Cocycle Puzzle*
Note that had we defined $\mathcal{P}$ with an extra factor of i we would have concluded that it is order 4, not order 2. Now, we know that the sequence $1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1$ is not split and has a nontrivial cocycle. When then, can we define a parity operation of order two? [131]

14.4.2 Remarks About The Quantum Statistical Mechanics Of The Particle On The Ring

In quantum statistical mechanics a central object of study is the partition function:

$$Z := \mathrm{Tr}_{\mathcal{H}} e^{-\beta H} \qquad (14.243)$$

Here $\beta = 1/(kT)$ where k is Boltzmann's constant and T is the absolute temperature.

For simplicity we will henceforth set $\hbar = k = 1$ (as can always be done by a suitable choice of units).

Since we have diagonalized the Hamiltonian exactly we can immediately say that

$$Z = \sum_{m\in\mathbb{Z}} e^{-\frac{\beta}{2I}(m-\mathcal{B})^2} \qquad (14.244)$$

This is in fact a very interesting function of $\frac{\beta}{2I}$ and $\mathcal{B}$. Some immediate facts we can note are

[129] *Answer*: First reproduce Spin(2) using the general definition. We can represent the $d = 2$ Clifford algebra by σ^1, σ^2 and then the product of two vectors of the form $\gamma(v)$ with $v^2 = 1$ is a matrix of the form $(x^1\sigma^1 + x^2\sigma^2)(y^1\sigma^1 + y^2\sigma^2)$ where $v_1 = (x^1, x^2)$ and $v_2 = (y^1, y^2)$ are unit vectors in $\mathbb{R}^2$. Multiplying this out we get

$$\cos\theta + \sin\theta\sigma^1\sigma^2 \qquad (14.242)$$

where θ is the angle between v_1 and v_2. Now let $\hat{P}$ be represented by σ^1 (or $\gamma(w)$ for any unit vector w).

[130] *Answer*: D_4 has generators x, y with $x^2 = 1$ and $y^4 = 1$ and $xyx = y^{-1}$. In a one-dimensional representation x, y will be represented by complex numbers. So we solve the above equations with $x, y \in \mathbb{C}$. Clearly $x \in \{\pm 1\}$ and then $y^2 = 1$ so $y \in \{\pm 1\}$ and there is no correlation between the choice of sign for x and the choice of sign for y.

[131] *Hint*:It is important to think about which group the cocycle and coboundaries take values in.

1. The expression is manifestly periodic under integer shifts of $\mathcal{B}$, illustrating the general claim above that the theory is invariant under integral shifts of the "theta angle" $\mathcal{B}$.
2. Moreover, at low temperature, $\beta \to \infty$ there is a single dominant term from the sum, unless $\mathcal{B}$ is a half-integer, in which there are two equally dominant terms - this reflects the double degeneracy of the ground state when $2\mathcal{B}$ is odd: The ground state is a Qbit. A standard technique in field theory is to study the IR behavior of a partition function to learn about the ground states of the system.

We are going to see that this system in fact has a very interesting high/low temperature duality and use this to understand better the θ-dependence of the previous example in terms of path integrals.

To relate Z to a path integral we observe that we can write:

$$Z = \int_0^{2\pi} d\phi \langle \phi | e^{-\beta H} | \phi \rangle \tag{14.245}$$

Now, we can interpret $\langle \phi | e^{-\beta H} | \phi \rangle$ as a specialization of the matrix elements of the Euclidean time propagator

$$\langle \phi_2 | e^{-t_E H_{\mathcal{B}}} | \phi_1 \rangle = \frac{1}{2\pi} \sum_{m \in \mathbb{Z}} e^{-\frac{t_E}{2I}(m-\mathcal{B})^2 + \mathrm{i}m(\phi_1 - \phi_2)} \tag{14.246}$$

Indeed, the usual propagator in quantum mechanics is

$$U(t) = e^{-\mathrm{i}tH/\hbar} \tag{14.247}$$

Under good conditions this family of operators for $t \in \mathbb{R}$ has an "analytic continuation" to part of the complex plane. What this means is that there is a well-defined family of operators

$$e^{-\mathrm{i}zH/\hbar} \tag{14.248}$$

where z takes values in a region $\mathcal{R} \subset \mathbb{C}$. The region $\mathcal{R}$ should, at least contain the real axis of time on its boundary (or closure). To see that there might be restrictions on $\mathcal{R}$ suppose that $\mathcal{R} = \mathbb{C}$. Then we can consider the restriction to the imaginary axis, setting

$$z = -\mathrm{i}t_E \qquad t_E \in \mathbb{R} \tag{14.249}$$

Here t_E is called *Euclidean time* because if we were to make a substitution $t \to -\mathrm{i}t_E$ in the Lorentz metric then we would get a metric of definite signature. (If we take signature $(-, +^d)$ we would get the Euclidean metric.) If the Hamiltonian is bounded below $\exp[-t_E H]$ should make sense for t_E positive, but if the spectrum of H grows rapidly the operator will be unbounded and certainly not traceclass for t_E negative. So, for Hamiltonians, such as the one we are considering the region $\mathcal{R}$ can be taken to be the negative half-plane. Defining such an analytic family of operators and restricting to the negative imaginary axis (or some other part of the imaginary axis) is called *Wick rotation.*

Now, it is well-known that the propagator: $\langle \phi_2 | e^{-\frac{\mathrm{i}tH}{\hbar}} | \phi_1 \rangle$ can be represented by a Feynman path integral. After Wick rotation we still have a path integral representation.

Feynman's argument proceeds just as well with $e^{-t_E H/\hbar}$. In fact, formally, it is better since the integral has better (formal) convergence properties for Euclidean actions whose real part is bounded below.

Now, by setting $\phi_1 = \phi_2 = \phi$ and integrating over ϕ we are making Euclidean time periodic, with period β and computing the path integral on a compact spacetime, namely, the circle. The path integral for $\phi_1 = \phi_2$ is done with boundary conditions on the fields so that $\phi(0) = \phi(\beta)$. This is precisely the kind of boundary condition that says that $\phi(t)$ is defined on a circle. More details on path integrals are available in many textbooks. See, for examples:

1. Feynman and Hibbs, *Quantum Mechanics and Integrals*
2. Feynman, *Statistical Mechanics*
3. C. Itzykson and J.B. Zuber, *Quantum Field Theory*,
4. J. Zinn-Justin, *Quantum Field Theory and Critical Phenomena*,

In this subsubsection we will henceforth drop the subscript E on t_E and just use t for the real Euclidean time coordinate.

In the Wick rotation to Euclidean space the "θ-angle" $\oint eA$ remains real so the matrix elements of the Euclidean time propagator have the path integral representation:

$$\langle\phi_2|e^{-\beta H}|\phi_1\rangle = Z(\phi_2,\phi_1|\beta) := \int [d\phi(t)]_{\phi(0)=\phi_1}^{\phi(\beta)=\phi_2} e^{-\frac{1}{\hbar}\int_0^\beta \frac{1}{2}I\dot{\phi}^2 dt - \mathrm{i}\int \mathcal{B}\dot{\phi}dt} \tag{14.250}$$

(One must be careful with the sign of the imaginary term, and it matters.)

Viewed as a field theory, this is a free field theory and the path integral can be done exactly by semiclassical techniques:

The equation of motion is simply $\ddot{\phi} = 0$. Again, the θ-term has not changed it.

Thus, the classical solutions to the equations of motion with boundary conditions $\phi(0) = \phi_1, \phi(\beta) = \phi_2$ are:

$$\phi_{cl}(t) = \phi_1 + \left(\frac{\phi_2 - \phi_1 + 2\pi w}{\beta}\right)t \qquad w \in \mathbb{Z} \tag{14.251}$$

or more to the point:

$$e^{\mathrm{i}\phi_{cl}(t)} = e^{\mathrm{i}\left((1-\frac{t}{\beta})\phi_1 + \frac{t}{\beta}\phi_2\right) + \frac{2\pi \mathrm{i} t w}{\beta}} \tag{14.252}$$

These are solutions of the Euclidean equations of motion, and are known as "instantons" for historical reasons. Notice that because of the compact nature of the spacetime on which we define our $0+1$ dimensional field theory there are infinitely many solutions labeled by $w \in \mathbb{Z}$. There are two circles in the game: The spacetime of this $0+1$-dimensional field theory is the Euclidean time circle. Then the target space of the field theory is also a circle. The quantum field $e^{\mathrm{i}\phi(t)}$ is a map $M \to \mathcal{X}$. M, which is spacetime is S^1 and $\mathcal{X}$, which is the target space is also $\mathcal{X}$. As we saw: $\pi_1(S^1) \cong \mathbb{Z}$. There can be topologically inequivalent field configurations. That is the space of maps $Map(M \to \mathcal{X})$ has different connected components. The different topological sectors are uniquely labelled by the winding number of the map (14.252). In the path integral we sum over all field configurations so we should sum over all these instanton configurations.

We now write

$$\phi = \phi_{cl} + \phi_q \tag{14.253}$$

where ϕ_{cl} is an instanton solution, as in (14.251), and ϕ_q is the quantum fluctuation with $\phi_q(0) = \phi_q(\beta) = 0$, and, moreover, $\phi_q(t)$ is in the topologically trivial component of $Map(S^1, \mathcal{X})$. The action is a sum $S(\phi_{cl}) + S(\phi_q)$, precisely because ϕ_{cl} solves the equation of motion. Indeed the integral factorizes and we just get:

$$Z(\phi_2, \phi_1|\beta) = Z_q \sum_{w\in\mathbb{Z}} e^{-\frac{2\pi^2 I}{\beta}(w+\frac{\phi_2-\phi_1}{2\pi})^2 + 2\pi i\mathcal{B}(w+\frac{\phi_2-\phi_1}{2\pi})} \tag{14.254}$$

The summation runs over classical solutions, weighted by the value of the classical action on that solution.

Z_q is the path integral over ϕ_q:

$$Z_q = \int [d\phi_q(t)]^{\phi(\beta)=0}_{\phi_q(0)=0} e^{-\int_0^\beta \frac{1}{2}I\dot{\phi}^2 dt} \tag{14.255}$$

We are integrating over the space of "all" maps $\phi_q : [0,1] \to U(1)$ with $\phi_q(0) = \phi_q(1) = 0$ that are homotopically trivial. We can do it by noticing that this is a Gaussian integral.

Now in finite dimensions we have the integral

$$\int \prod_{i=1}^n \frac{dx^i}{\sqrt{2\pi}} e^{-\frac{1}{2}x^i A_{ij} x^j + b_i x^i} = \frac{1}{\sqrt{\det A}} e^{\frac{1}{2}b_i (A^{-1})^{ij} b_j} \tag{14.256}$$

where $Re(A) > 0$ is a symmetric matrix. When A can be diagonalized by a real orthogonal transformation we can replace

$$\det A = \prod_{i=1}^n \lambda_i \tag{14.257}$$

where the product runs over the eigenvalues of A. Thus, we need to generalize this expression to the determinant of an infinite-dimensional "matrix"

$$\int [d\phi_q] \exp[-\int_0^1 \phi_q(-\frac{I}{2\beta}\frac{d^2}{d\tau^2})\phi_q] = (2\pi)\mathrm{Det}'^{-1/2}(\mathcal{O}) \tag{14.258}$$

Here the prime on the determinant means that we have omitted the zero-mode and the analog of A is the operator $\mathcal{O} = -\frac{I}{2\hbar\beta}\frac{d^2}{d\tau^2}$.

One way to make sense of Det$\mathcal{O}$ for an operator $\mathcal{O}$ on Hilbert space is known as "ζ-function regularization." (It will only work for a suitable class of operators.) Note that

$$\frac{d}{ds}|_{s=0}\lambda^{-s} = -\log\lambda \tag{14.259}$$

So if we define

$$\zeta_{\mathcal{O}}(s) := \sum_\lambda \lambda^{-s} \tag{14.260}$$

where we take the sum over the spectrum of $\mathcal{O}$ (and we assume $\mathcal{O}$ is diagonalizable with discrete spectrum) then, formally:

$$\prod_\lambda \lambda = \exp[-\zeta'_{\mathcal{O}}(0)] \tag{14.261}$$

For good operators $\mathcal{O}$ the spectrum goes to infinity sufficiently fast that $\zeta_{\mathcal{O}}(s)$ exists as an analytic function of s in a half plane $Re(s) > N$ for some N. Moreover, $\zeta_{\mathcal{O}}(s)$ also admits an analytic continuation in s to an open region around $s = 0$. In this case, we can define the determinant by the RHS of (14.261).

For $\mathcal{O} = -\frac{I}{2\hbar\beta}\frac{d^2}{d\tau^2}$ we have $\zeta_{\mathcal{O}}(s) = 2\big(\frac{I\pi^2}{2\hbar\beta}\big)^s\zeta(2s)$ where $\zeta(s)$ is the standard Riemann ζ-function, and since

$$\zeta(s) = -\frac{1}{2} + s\log\big(\frac{1}{\sqrt{2\pi}}\big) + \mathcal{O}(s^2) \tag{14.262}$$

we have

$$\mathrm{Det}'(\mathcal{O}) := \exp[-\zeta'_{\mathcal{O}}(0)] = \frac{\beta}{I} \tag{14.263}$$

(There are some factors of 2 and π that need to be fixed in this equation.)

We can understand this result nicely as follows. Let us study the $\beta \to 0$ behavior of the path integral. Then for $|\phi_1 - \phi_2| < \pi$,

$$Z \to Z_q e^{-\frac{I}{2\beta}(\phi_2-\phi_1)^2 + i\mathcal{B}(\phi_2-\phi_1)}\left(1 + \mathcal{O}(e^{-\kappa/\beta})\right) \tag{14.264}$$

where $\kappa > 0$. In plain English: the instantons are only important at *large* β. This is intuitively very satisfying: At very small times β it must cost a lot of action for $\phi(t)$ to make a nonzero number of circuites around the circle because the velocity must then be large, and large velocity means large action. So for physical quantities based on such small fluctuations the topologically nontrivial field configurations must contribute subleading effects. Let us therefore compare $Z(\phi_2, \phi_1|\beta)$ as $\beta \to 0$ with the standard quantum mechanical propagator. For small ϕ we can remove the phase from the B-field via $\psi(\phi) \to e^{-i\mathcal{B}\phi}\psi(\phi)$, so Z_q should not depend on $\mathcal{B}$. (Note this transformation is not globally defined in ϕ for generic $\mathcal{B}$ so we cannot use it to remove $\mathcal{B}$ from the problem when we treat the full quantity Z exactly.) After this transformation we expect to recover the standard propagator of a particle of mass $M = I$ on the line. Rotated to Euclidean space this would be:

$$\sqrt{\frac{M}{2\pi\hbar\beta}}e^{-\frac{M(\phi_2-\phi_1)^2}{2\hbar\beta}} \tag{14.265}$$

so

$$Z_q = \sqrt{\frac{I}{2\pi\hbar\beta}} \tag{14.266}$$

The net result is that

$$Z(\phi_2, \phi_1|\beta) = \sqrt{\frac{I}{2\pi\beta}}\sum_{w\in\mathbb{Z}} e^{-\frac{2\pi^2 I}{\beta}(w+\frac{\phi_2-\phi_1}{2\pi})^2 - 2\pi \mathrm{i}\mathcal{B}(w+\frac{\phi_2-\phi_1}{2\pi})} \tag{14.267}$$

Now compare (14.246) (with $t_E = \beta$) with (14.267). These expressions look very different! One involves a sum of exponentials with β in the numerator and the other with β in the demoninator. One is well-suited to discussing the asymptotic behavior for $\beta \to \infty$ (low temperature) and the other for $\beta \to 0$ (high temperature), respectively. Nevertheless, we have computed the same physical quantity, just using two different methods. So they must be the same. But the mathematical identity that says they are the same appears somewhat miraculous. We now explain how to verify the two expressions are indeed identical using a direct mathematical argument.

The essential fact is the Poisson summation formula. For any function

$$\sum_{m\in\mathbb{Z}} f(m) = \sum_{w\in\mathbb{Z}} \widehat{f}(w) \tag{14.268}$$

where $\widehat{f}$ is the Fourier transform:

$$\widehat{f}(w) = \int_{\mathbb{R}} e^{-2\pi \mathrm{i} t w} f(t) \tag{14.269}$$

This is valid for functions such that

1. f decays rapidly enough so that the sum on the LHS converges.
2. The Fourier transform $\widehat{f}$ exists.
3. The Fourier transform $\widehat{f}$ decays rapidly enough so that the sum on the RHS converges.

We apply this to an important special function known as the Riemann theta function

$$\vartheta[\begin{smallmatrix}\theta\\ \phi\end{smallmatrix}](z|\tau) := \sum_{n\in\mathbb{Z}} e^{\mathrm{i}\pi\tau(n+\theta)^2+2\pi\mathrm{i}(n+\theta)(z+\phi)} \tag{14.270}$$

The Riemann theta function is an absolutely convergent analytic function of τ in the upper half-plane. It is also an entire function of z. Then one has (simply apply the Poisson summation formula):

$$\vartheta[\begin{smallmatrix}\theta\\ \phi\end{smallmatrix}](\frac{-z}{\tau}|\frac{-1}{\tau}) = (-i\tau)^{1/2} e^{2\pi i\theta\phi} e^{i\pi z^2/\tau} \vartheta[\begin{smallmatrix}-\phi\\ \theta\end{smallmatrix}](z|\tau) \tag{14.271}$$

In our case, the expression computed directly from the diagonalization of the Hamiltonian is

$$\begin{aligned} Z(\phi_2,\phi_1|\beta) &= \frac{1}{2\pi}\sum_{m\in\mathbb{Z}} e^{-\frac{\beta}{2I}(m-\mathcal{B})^2+\mathrm{i}m(\phi_1-\phi_2)} \\ &= \frac{1}{2\pi} e^{\mathrm{i}\mathcal{B}(\phi_1-\phi_2)} \vartheta[\begin{smallmatrix}\theta\\ \phi\end{smallmatrix}](0|\tau) \end{aligned} \tag{14.272}$$

with

$$\begin{aligned} \tau &= \mathrm{i}\frac{\beta}{2\pi I} \\ \theta &= -\mathcal{B} \\ \phi &= \frac{\phi_1-\phi_2}{2\pi} \end{aligned} \tag{14.273}$$

On the other hand, the expression that emerges naturally from the semiclassical evaluation of the Euclidean path integral is

$$\begin{aligned} Z(\phi_2,\phi_1|\beta) &= \sqrt{\frac{I}{2\pi\beta}}\sum_{w\in\mathbb{Z}} e^{-\frac{2\pi^2 I}{\beta}(w+\frac{\phi_2-\phi_1}{2\pi})^2-2\pi\mathrm{i}\mathcal{B}(w+\frac{\phi_2-\phi_1}{2\pi})} \\ &= \sqrt{\frac{I}{2\pi\beta}}\vartheta[{\theta' \atop \phi'}](0|\tau') \end{aligned} \tag{14.274}$$

$$\begin{aligned} \tau' &= \mathrm{i}\frac{2\pi I}{\beta} \\ \theta' &= -\frac{\phi_1-\phi_2}{2\pi} \\ \phi' &= -\mathcal{B} \end{aligned} \tag{14.275}$$

and the modular transformation law of the Riemann theta function is equivalent to the relation between the expressions naturally arising from the Hamiltonian and Lagrangian approaches to evaluation of the matrix elements of the Euclidean time propagator.

Note in particular that for the partition function proper we have, as $\beta\to 0$:

$$\begin{aligned} Z(S^1) &= \left(\frac{2\pi I}{\beta\hbar}\right)^{1/2}\sum_{n\in\mathbb{Z}} e^{-2\pi^2 n^2\frac{I}{\beta\hbar}+2\pi\mathrm{i}n\mathcal{B}} \\ &\sim_{\beta\to 0}\left(\frac{2\pi I}{\beta\hbar}\right)^{1/2}\left(1+2e^{-2\pi^2\frac{I}{\beta\hbar}}\cos(2\pi\mathcal{B})+\cdots\right) \end{aligned} \tag{14.276}$$

The overall factor of $\beta^{-1/2}$ gives the expected divergence. The first correction term to the factor in parentheses is an instanton effect.

Note that in the Hamiltonian version the only thing that is manifest about the high-temperature, $\beta\to 0$, limit is that Z diverges. Note that for $\beta\to 0$ all the terms in the sum contribute about equally and the sum diverges. The modular transformation reveals an interesting duality: Once we factor out this multiplicative divergence we discover another theta function.

Exercise *A Parity Puzzle*

Suppose $2\mathcal{B}$ is an odd integer.

a.) Show that as $\beta\to\infty$ we have

$$\langle\phi_2|e^{-\frac{\beta H}{\hbar}}|\phi_1\rangle \sim 2e^{\frac{\mathrm{i}}{2}(\phi_1-\phi_2)}\cos\left(\frac{\phi_1-\phi_2}{2}\right)e^{-\beta E_{\mathrm{ground}}}+\cdots \tag{14.277}$$

b.) Note that this expression is not invariant under $\phi\to-\phi$. But in $\mathrm{Pin}^+(2)$ there is an element P which corresponds to $\phi\to-\phi$. How is this compatible with our argument that $\mathrm{Pin}^+(2)$ is a valid symmetry of the quantum theory? [132]

[132] *Answer*: Show that

$$\mathcal{P}\cdot|\phi\rangle = e^{-\mathrm{i}\phi}|-\phi\rangle \tag{14.278}$$

You can prove this by expanding $|\phi\rangle = \sum_{m\in\mathbb{Z}}\langle\Psi_m|\phi\rangle\Psi_m$. Now, using this expression check that the propagator indeed transforms correctly.

Exercise *Poisson Summation And X-Ray Crystallography*

Although it is slightly formal (but valid in a distributional sense) one can apply the Poisson summation formula to the case that $f(x) = e^{\mathrm{i}xs}$ is an oscillatory exponential (with s real). Write out the resulting formula.

Interpret this as saying that the constructive interference of many plane waves results in a series of sharp peaks: That is the basis for X-ray crystallography.

14.4.3 Gauging The Global $SO(2)$ Symmetry, Chern-Simons Terms, And Anomalies

When a theory has a symmetry one can implement a procedure called "gauging the symmetry." This is a two-step process:

1. Make the symmetry local and couple to a gauge field.
2. Integrate over "all possible" gauge fields consistent with the symmetry.

It is not necessary to proceed to step (2) after completing step (1). In this case, we say that we are coupling to nondynamical external gauge fields. It makes perfectly good sense to introduce nondynamical, external gauge fields for a symmetry. We do this all the time in quantum mechanics courses where we couple our quantum system to an electromagnetic field, but do not try to quantize the electromagnetic field.

For the more mathematically sophisticated reader the two-step process can be summarized, somewhat more concisely and precisely, as saying that we:

1. Identify the symmetry group with the structure group of a principal bundle and we change the bordism category in the domain of the field theory functor to include G-bundles with connection (where G is the symmetry we are gauging).
2. Sum over isomorphism classes of principal bundles and integrate over the isomorphism classes of connections on those bundles.

In the present simple example of the charged particle on a ring surrounding a solenoid we can "gauge" the global $SO(2)$ symmetry $\phi \to \phi + \alpha$ that is present for all values of $\mathcal{B}$. It is then interesting to see how coupling to the external gauge field tells us about the subtleties of combining $SO(2)$ symmetry with charge conjugation symmetry that we studied above. (The following discussion was inspired by Appendix D of. [133])

[133] D. Gaiotto, A. Kapustin, Z. Komargodski and N. Seiberg, "Theta, Time Reversal, and Temperature," https://arxiv.org/pdf/1703.00501.pdf

So in our simple example we implement Step 1 above as follows: We seek to make the shift symmetry local, that is, we attempt to make

$$\phi(t) \to \phi(t) + \alpha(t) \tag{14.279}$$

into a symmetry where $\alpha(t)$ is not a constant but an "arbitrary" function of time. When $\alpha(t)$ is time dependent the action $\sim \int \dot{\phi}^2$ is not invariant under such transformations. To compensate for this we introduce an extra function of time into the problem, call it $A^{(e)}(t)$. Here the superscript e - for "external" - reminds us that this is an "external" or "background" field: We will <u>not</u> do a path integral over these functions (unless we proceed to Step 2 above). By contrast, we <u>will</u> do a path integral over the "dynamical" field $\phi(t)$ or $\Phi(t) = e^{\mathrm{i}\phi(t)}$.

The gauged action is

$$\begin{aligned} S &= \int \frac{1}{2} I (\dot{\phi} + A^{(e)})^2 dt + \oint \mathcal{B}(\dot{\phi} + A^{(e)}) dt \\ &= \int \frac{1}{2} I \left(\Phi(t)^{-1}(-\mathrm{i}\frac{d}{dt} + A^{(e)})\Phi(t) \right)^2 dt + \oint \mathcal{B}\Phi(t)^{-1}(-\mathrm{i}\frac{d}{dt} + A^{(e)})\Phi(t) dt \end{aligned} \tag{14.280}$$

This action is a functional of both the nondynamical field $A^{(e)}(t)$ and the dynamical field $\phi(t)$. Note that the action is invariant under the gauge transformation:

$$\begin{aligned} \phi(t) &\to \phi(t) + \alpha(t) \\ A^{(e)}(t) &\to A^{(e)}(t) - \partial_t \alpha(t) \end{aligned} \tag{14.281}$$

where, for the moment, we ignore boundary terms.

It turns out that it is better to regard the function $A^{(e)}(t)$ as a component of a 1-form:

$$A^{(e)} := A^{(e)}(t) dt \tag{14.282}$$

and, better still, $A^{(e)}$ is the local one-form associated to a connection on a (locally trivialized) principal $SO(2)$ bundle over the time manifold M. We stress that the gauge field $A^{(e)}$ is <u>NOT</u> the gauge field of electromagnetism. (That field has already produced our theta term.) Rather, it is a new field in our system: It is a gauge field for the shift symmetry of the field $\phi(t)$. [134]

Note that we could also write the gauge transformation in the form:

$$\begin{aligned} e^{\mathrm{i}\phi(t)} &\to e^{\mathrm{i}\phi(t)} e^{\mathrm{i}\alpha(t)} \\ d - \mathrm{i}A^{(e)} &\to e^{\mathrm{i}\alpha(t)}(d + \mathrm{i}A^{(e)}) e^{-\mathrm{i}\alpha(t)} \end{aligned} \tag{14.283}$$

This is better because is captures better the geometric content, Consequently, it makes more sense when working on topologically nontrivial spacetimes, such as the Euclidean

[134] The physical interpretation of the gauging process in terms of our original charged particle on a ring is not completely clear to the author. But the mathematical structure makes sense and is a good toy model for other field theoretic systems where the physical interpretation of the gauging is clear.

time circle. One can make choices of gauge group so that it becomes important that $e^{\mathrm{i}\alpha(t)}$ can be single-valued even when $\alpha(t)$ is not.

What about charge conjugation symmetry?

First consider the classical theory. In the absence of the external gauge field we noted that there is an $O(2)$ symmetry of the equations of motion, even though under $\phi(t) \to -\phi(t)$ the theta term in the action flips sign. In the presence of the external gauge field the equations of motion are modified, however, as we will see below, we can gauge $A^{(e)}(t)$ to be a constant, and in this case they are not modified. So we still have an $O(2)$ symmetry.

Now consider the quantum theory. One can show that, appropriately defined, the quantum Hamiltonian is still $H_{\mathcal{B}}$. Under charge conjugation we must flip $\mathcal{B}$ and then we change the Hamiltonian (unless $\mathcal{B} = 0$). But, as noted above, if $2\mathcal{B} \in \mathbb{Z}$ in that case $H_{\mathcal{B}}$ is unitarily equivalent to $H_{-\mathcal{B}}$ and we can implement a unitary operator $\mathcal{P}$ corresponding to the charge conjugation operation. In the path integral the value of the action matters. The action (14.280) is invariant under the charge conjugation transformation if we take

$$\begin{aligned} \phi(t) &\to -\phi(t) \\ A^{(e)} &\to -A^{(e)} \\ \mathcal{B} &\to -\mathcal{B} \end{aligned} \tag{14.284}$$

and consequently if we change $\mathcal{B} \to -\mathcal{B}$ we must also take $A^{(e)} \to -A^{(e)}$ as noted above. We will return to the quantum implementation of charge conjugation symmetry.

Now let us re-examine the periodicity of the physics as a function of $\mathcal{B}$. In the absence of the external gauge field $A^{(e)}$ we found that physical quantities are periodic functions of $\mathcal{B}$ with period one. However, in the presence of a nonzero $A^{(e)}$, the term $\int \mathcal{B}A^{(e)}(t)dt$ spoils the periodicity in $\mathcal{B}$, because the value of the action matters in the quantum theory.

We can restore a kind of periodicity in $\mathcal{B}$ by adding a Chern-Simons term to the action. We will comment in detail on the Chern-Simons term below. In Euclidean space the new action is:

$$e^{-S} = e^{-\int \frac{1}{2}I(\dot{\phi}+A_t^{(e)})^2 dt - \mathrm{i}\oint \mathcal{B}(\dot{\phi}+A_t^{(e)})dt} e^{\mathrm{i}k\int A_t^{(e)}dt} \tag{14.285}$$

and the last factor is the Chern-Simons term. By introducing the Chern-Simons term we have introduced yet another parameter, the level k, into our theory. Classically the action with $(\mathcal{B}, k)$ is equivalent to the action with $(\mathcal{B} + r, k + r)$ where $r \in \mathbb{R}$ is any real number.

Now that we have restored some kind of periodicity we can ask about quantum implementation of charge conjugation symmetry. We must take $\mathcal{B} \to -\mathcal{B}$, but quantum mechanically the theory with $\mathcal{B}$ is only equivalent to that with $-\mathcal{B}$ when $2\mathcal{B} \in \mathbb{Z}$. So, in the quantum theory we can only hope to have charge conjugation invariance if there is an integer N so that

$$(\mathcal{B} + N, k + N) = (-\mathcal{B}, -k) \tag{14.286}$$

In other words $k = \mathcal{B} = N/2 \in \mathbb{Z}/2$.

The introduction of the Chern-Simons term raises a new issue: When one sees gauge potentials in an action that do not enter through fieldstrengths or covariant derivatives it is important to ask about gauge invariance. In order to discuss the gauge invariance of the Chern-Simons term properly we need first to discuss more carefully the space of gauge fields and the group of gauge transformations.

The Space Of Gauge Fields And The Group Of Gauge Transformations

In our simple setting the space $\mathcal{A}$ of gauge fields can be identified with the space of single-valued, continuous real-valued functions $A^{(e)}(t)$ on M.

We now must choose a *gauge group* G. This will be a Lie group - typically finite-dimensional, although not necessarily connected. In our case, there are two natural choices: We could take $G = \mathbb{R}$ or we could take $G = U(1)$. Then the *group of gauge transformations* is a group of maps

$$\mathcal{G} = Map[M \to G] \tag{14.287}$$

If M and G have positive dimension the group of gauge transformations will be an infinite-dimensional Lie group.

Of particular interest in gauge theory is the quotient space $\mathcal{A}/\mathcal{G}$, the space of gauge orbits, or, equivalently, the space of gauge-inequivalent field configurations.

Let us examine a few examples of $\mathcal{A}/\mathcal{G}$:

1. Let us first consider what happens when $G = \mathbb{R}$ and M is an interval or the real line. Then the space $\mathcal{A}$ of gauge fields can be identified with the space of real-valued continuous functions on M. The group $\mathcal{G}$ is the space of real-valued C^1 functions on M, $t \mapsto \alpha(t) \in \mathbb{R}$. The group $\mathcal{G}$ acts on $\mathcal{A}$ via

$$A^{(e)}(t) \to A^{(e)}(t) - \partial_t \alpha(t) \tag{14.288}$$

If $M = [t_1, t_2]$ with free boundary conditions on $\mathcal{A}$ and $\mathcal{G}$ then we can always solve

$$\partial_t \alpha(t) = A^{(e)}(t) \tag{14.289}$$

for some $\alpha(t)$ and hence we can always gauge $A^{(e)}(t)$ to zero. So $\mathcal{A}/\mathcal{G}$ is just a point. [135]

For the discussion below it is useful to note here that the expression

$$\exp[\mathrm{i}\int_{t_1}^{t_2} A_t^{(e)}(t')dt'] \tag{14.290}$$

is in general not gauge invariant. Rather:

$$\exp[\mathrm{i}\int_{t_1}^{t_2} A_t^{(e)}(t')dt'] \to e^{\mathrm{i}\alpha(t_1)}\exp[\mathrm{i}\int_{t_1}^{t_2} A_t^{(e)}(t')dt']e^{-\mathrm{i}\alpha(t_2)} \tag{14.291}$$

[135] Actually, this is too naive: $\mathcal{A}/\mathcal{G}$ is more properly thought of as a stack. See the section below on groupoids.

2. Now, continuing to take $G = \mathbb{R}$ let us consider what happens if $M = \mathbb{R}$ and we impose boundary conditions that $\alpha(t) \to 0$ at $t \to \pm\infty$. In this case

$$\int_{-\infty}^{+\infty} A^{(e)}(t)dt \tag{14.292}$$

is gauge invariant. There are no "local" invariants. From the previous discussion we see that we can gauge $A^{(e)}(t)$ to zero in any compact region. In this case

$$\mathcal{A}/\mathcal{G} \cong \mathbb{R} \tag{14.293}$$

and the integral (14.292) fully determines the gauge equivalence class.

3. Now let us consider the case $G = U(1)$, and let us also take M to be the Euclidean time circle so

$$\mathcal{G} = \mathrm{Map}(S^1_{s.t.} \to U(1)) \tag{14.294}$$

Now, just viewing the gauge transformation as a set of continuous maps $S^1 \to S^1$ there is a winding number. If this winding number is nonzero there is an obstruction to finding a single-valued function $\alpha(t)$ so that $g(t) = e^{\mathrm{i}\alpha(t)}$.

There is a normal subgroup $\mathcal{G}_0$ of *small gauge transformations* for which $g(t)$ admits a well-defined logarithm. That is, the gauge transformations $g(t) \in \mathcal{G}_0$ are of the form $g(t) = e^{\mathrm{i}\alpha(t)}$ where $\alpha(t)$ is single-valued. Then

$$1 \to \mathcal{G}_0 \to \mathcal{G} \quad \overset{\pi}{\to} \quad \mathbb{Z} \to 1 \tag{14.295}$$

where the map π can be viewed as the winding number. Gauge transformations in $\mathcal{G}_0$ are known as *small gauge transformations*. Those which have nonzero winding numbers are known as *large gauge transformations*. It is worth noting that the above sequence splits: For $w \in \mathbb{Z}$ we can take $s(w) = g_w$ to be the gauge transformation:

$$g_w(t) = \exp[2\pi \mathrm{i} wt/\beta] \tag{14.296}$$

and $g_w(t)g_{w'}(t) = g_{w+w'}(t)$. Note that for these transformations if we tried to define $\alpha(t)$ it would be $\alpha(t) = 2\pi wt/\beta$ and would not be single-valued when M is the circle.

Now, referring to (14.299) it is clear that if $\alpha(t)$ is single valued then

$$\exp[\mathrm{i}\oint_{S^1} A^{(e)}_t(t')dt'] \tag{14.297}$$

is gauge invariant. However when we have a large gauge transformation $g_w(t)$ we can cut the circle say at $t = 0$ and $t = \beta$ and then, with $\alpha(t) = 2\pi wt/\beta$ with $w \in \mathbb{Z}$ the holonomy is still gauge invariant. Note that the large gauge transformations $g_w(t)$ take

$$A^{(e)}_t(t') \to A^{(e)}_t(t') + w/\beta \tag{14.298}$$

but preserves the holonomy (14.297). Put differently, (14.299) is generalized to

$$\exp[\mathrm{i}\int_{t_1}^{t_2} A^{(e)}_t(t')dt'] \to g(t_2)^{-1}\exp[\mathrm{i}\int_{t_1}^{t_2} A^{(e)}_t(t')dt']g(t_1) \tag{14.299}$$

so that on the circle the *holonomy* (14.297) is gauge invariant. Equation (14.299) generalizes nicely to the case of nonabelian groups on arbitrary spacetimes.

We can ask if there are other independent gauge invariant functions of $A^{(e)}(t)$ besides the holonomy. Since $A^{(e)}(t)$ is periodic we can decompose $A^{(e)}(t)$ in a Fourier expansion. Write $\tilde{A}_t^{(e)}(t)$ for the sum of the nonzero frequency modes. Then we can solve the differential equation

$$\partial_t \alpha(t) = \tilde{A}_t^{(e)}(t) \tag{14.300}$$

with a single-valued $\alpha(t)$ to choose a gauge so that

$$A^{(e)}(t) = \mu/\beta \tag{14.301}$$

is constant. Put differently, $\mathcal{A}/\mathcal{G}_0$ can be identified with the space of real numbers, given by the constant μ. We will denote $\mathcal{A}^{\mathrm{red}} = \mathcal{A}/\mathcal{G}_0$. Then the "large" gauge transformations $g_w(t)$ shift $\mu \to \mu + 2\pi w$, with $w \in \mathbb{Z}$. Therefore we have

$$\mathcal{A}/\mathcal{G} \cong \mathcal{A}^{\mathrm{red}}/\mathbb{Z} \cong \{[\mu] = [\mu + 2\pi w] \qquad w \in \mathbb{Z}\} \cong U(1) \tag{14.302}$$

and the holonomy $e^{\mathrm{i}\mu}$ around the circle is a complete gauge invariant.

4. Finally, let us take the gauge group to be $G = O(2) = SO(2) \rtimes \mathbb{Z}_2$. Let $\mathcal{G}_{SO(2)}$ be the group of gauge transformations when the gauge group is $SO(2)$ and $\mathcal{G}_{O(2)}$ be the group of gauge transformations when the gauge group is $O(2)$. Then $\mathcal{G}_{O(2)} = \mathcal{G}_{SO(2)} \rtimes \mathbb{Z}_2$ and we have the exact sequence

$$1 \to \mathcal{G}_0 \to \mathcal{G}_{O(2)} \to \mathbb{Z} \rtimes \mathbb{Z}_2 \cong D_\infty \to 1 \tag{14.303}$$

Again the sequence splits and the infinite dihedral group $D_\infty \cong \mathbb{Z} \rtimes \mathbb{Z}_2$ preserves the space $\mathcal{A}^{\mathrm{red}}$ of constant gauge fields with generators acting as

$$\begin{aligned} \sigma :&\mu \to -\mu \\ s :&\mu \to \mu + 2\pi \end{aligned} \tag{14.304}$$

Comments On The Chern-Simons Term

Now we are ready to discuss the gauge invariance of the Chern-Simons term. The Chern-Simons term on $M = S^1$ is invariant under $\mathcal{G}_0$ for any value of k. However, under the large gauge transformations $g_w(t)$ with $w \neq 0$:

$$\exp[\mathrm{i}k \oint_{S^1} A_t^{(e)}(t')dt'] \to e^{2\pi \mathrm{i} wk} \exp[\mathrm{i}k \oint_{S^1} A_t^{(e)}(t')dt'] \tag{14.305}$$

and therefore, if we are going to allow our theory to make sense on a circle with the gauge group $SO(2) \cong U(1)$ then k should be quantized to be an integer. Note there would be no such quantization of k if the gauge group is taken to be $\mathbb{R}$.

The above observation is related to two extremely important conceptual points that are essential to all discussions of the use of Chern-Simons terms in quantum physics:

It is not necessary for the action to be invariant. All that is necessary for a well-defined path integral is that the exponentiated action must be invariant.

Gauge invariance of the "Chern-Simons term" under large gauge transformations implies that the level k, one of the couplings of the theory, is quantized: $k \in \mathbb{Z}$.

In our case the action in equation (14.285) is <u>not</u> gauge invariant! Under large gauge transformations with winding number w we have $S \to S + 2\pi i k w$ with $w \in \mathbb{Z}$. However, having a well-defined measure in the path integral only requires e^{-S} to be well-defined, and this will be the case if, and only if, $k \in \mathbb{Z}$.

Note that

$$\exp[\mathrm{i}k \oint_{S^1} A_t^{(e)}(t')dt'] = e^{\mathrm{i}k\mu} \tag{14.306}$$

and, since $k \in \mathbb{Z}$ is quantized this is properly periodic under $\mu \to \mu + 2\pi$ and the exponentiated Chern-Simons term descends to a well-defined function on $\mathcal{A}/\mathcal{G}$. For the group $O(2)$ we would have to consider $\cos(\mu)$. (Of course, $\cos(n\mu)$ is a Tchebyshev polynomial of the basic invariant $\cos(\mu)$.)

<u>Anomalies</u>

We can now discuss, very generally, the notion of anomalies. In quantum systems we typically have both "dyanmical variables" such as dynamical fields, degrees of freedom, etc. as well as "external" or "background" or "control" variables. We will denote generic "background fields" by ϕ^{bck} and generic "dynamical fields" by ϕ^{dyn}. Any parameter of the theory should be considered a "field." The space of all fields is then fibered:

$$\begin{tikzcd}
\mathcal{F}^{dyn} \arrow[r] & \mathcal{F} \arrow[d] \\
 & \mathcal{F}^{bck}
\end{tikzcd} \tag{14.307}$$

In the very simple situation we are discussing here the fibration is just a Cartesian product.

In the computation of physical quantities we will typically integrate over $\mathcal{F}^{dyn}$ thus producing a function (or, more generally, a section of a bundle) on $\mathcal{F}^{bck}$. We then study the physical quantity as a function on $\mathcal{F}^{bck}$.

In our example $\mathcal{F}^{dyn}$ can be taken to be the set of functions $\Phi(t) : M \to U(1)$ and $\mathcal{F}^{bck}$ can be taken to be the set of functions $A^{(e)}(t)$, or better, the connections on a principal G-bundle over M where in our present examples $G = \mathbb{R}, SO(2)$ or $O(2)$. [136]

Now suppose that there is a group $\mathcal{G}$ acting on $\mathcal{F}$ so that physical quantities are formally invariant. For example, if we have an invariant action $S[\phi^{dyn}; \phi^{bck}]$ and a formally invariant measure, then the path integral will be formally invariant. Then, physical quantities such as the partition function:

$$Z[\phi^{bck}] = \int_{\mathcal{F}^{dyn}} e^{-S[\phi^{dyn};\phi^{bck}]} \mathrm{vol}\,(\phi^{dyn}) \tag{14.308}$$

will, formally define a $\mathcal{G}$-invariant function on $\mathcal{F}^{bck}$. However, it can happen that when one defines the path integral carefully the partition function fails to be $\mathcal{G}$-invariant. In that case we say that there is a *potential anomaly.* Sometimes potential anomalies can be removed by physically unimportant redefinitions. When this cannot be done we say there is an *anomaly.*

If we tried to consider the Chern-Simons term for $k \notin \mathbb{Z}$ we would say it has an *anomaly.* For any value of k it descends to a function on $\mathcal{A}/\mathcal{G}_0$. However, only when $k \in \mathbb{Z}$ does it desend to a well-defined function on $\mathcal{A}/\mathcal{G}$.

It can happen that there can be different subgroups $\mathcal{H}_1 \subset \mathcal{G}$ and $\mathcal{H}_2 \subset \mathcal{G}$ such that there are different definitions of the path integral so that it is invariant either under $\mathcal{H}_1$ or under $\mathcal{H}_2$ but there is no definition so that it is invariant simultaneously under both $\mathcal{H}_1$ and $\mathcal{H}_2$. In this case we say there is a *mixed anomaly.*

The Partition Function As Function On $\mathcal{A}$ And Its Behavior Under The Action Of $\mathcal{G}$

Let us now illustrate some of the above ideas about anomalies by examining the partition function in our example of the gauged particle on a ring.

There will not be any interesting anomalies under $\mathcal{G}_0$. As we have explained we can always use $\mathcal{G}_0$ to gauge $A^{(e)}$ to be a constant 1-form, and we will henceforth take our gauge field to be constant. Then the equation of motion is the same as before, and performing the path integral just as in the previous section we find

$$\begin{aligned} Z(\mu) &= e^{\mathrm{i}k\mu} Z_q \sum_{w\in\mathbb{Z}} e^{-\frac{2\pi^2 I}{\beta}(w+\frac{\mu}{2\pi})^2 - 2\pi\mathrm{i}\mathcal{B}(w+\frac{\mu}{2\pi})} \\ &= e^{\mathrm{i}k\mu} Z_q \vartheta[{}^{\mu/2\pi}_{-\mathcal{B}}](0|\tau) \end{aligned} \tag{14.309}$$

with $\tau = \mathrm{i}\frac{2\pi I}{\beta}$. All we need to do here is replace the value of the classical action for solutions with $\dot{\phi} = 2\pi w/\beta$ by making the substitution $w \to w + \mu/2\pi$.

[136] One can also promote $\mathcal{B}$ to be a field for fun and profit. This has been discussed in many places. See e-Print: 1905.09315 for a recent discussion.

As in the case without the external gauge field there is a Hamiltonian interpretation. Performing the Poisson summation (or using the modular transformation law of the theta function) we get:

$$Z(\mu) = e^{\mathrm{i}(k-\mathcal{B})\mu} \frac{1}{2\pi} \sum_{m\in\mathbb{Z}} e^{-\frac{\beta}{2I}(m-\mathcal{B})^2 - \mathrm{i}(m-\mathcal{B})\mu} \tag{14.310}$$

It can be shown that the Euclidean path integral with action (14.193) is in fact equal to

$$Z(\mu) = e^{\mathrm{i}k\mu} \mathrm{Tr} e^{-\beta H_{\mathcal{B}}} e^{\mathrm{i}\mu Q} \tag{14.311}$$

where Q is the operator measuring the charge of the $SO(2)$ symmetry we gauged. In our case $Q\Psi_m = m\Psi_m$. [137] As noted above we still have

$$H_{\mathcal{B}} = \frac{1}{2I}\left(-\mathrm{i}\frac{\partial}{\partial\phi} - \mathcal{B}\right)^2 \tag{14.312}$$

acting on $L^2(\mathcal{X}) = L^2(S^1)$. One easily checks the equality of (14.310) and (14.311).

From either point of view $Z(\mu)$ is a periodic function of μ and there is no anomaly under the group $\mathbb{Z}$ of large gauge transformations, so long as $k \in \mathbb{Z}$.

The Gauge Group $O(2)$ and Mixed Anomalies

What happens if we try to extend the gauge group to gauge the full $O(2)$? Then, as we have seen, the quotient group $\mathcal{G}/\mathcal{G}_0$ is the infinite dihedral group generated by σ and s defined in equation (14.304) above.

If $2\mathcal{B}$ is even then we can take $k = \mathcal{B} \in \mathbb{Z}$. The partition function is invariant under $\mu \to -\mu$ and has the expected periodicity $\mu \sim \mu + 2\pi$. In other words $Z(\mu)$ is invariant under the group of large gauge transformations isomorphic to D_∞ and generated by σ and s, so it descends to a function on $\mathcal{A}/\mathcal{G}$ and there is no anomaly.

Things are much more subtle when $2\mathcal{B}$ is odd. As we saw, we can only expect charge conjugation symmetry when

$$k = \mathcal{B} \in \mathbb{Z} + \frac{1}{2} \tag{14.313}$$

But this clashes with the constraint $k \in \mathbb{Z}$. So we see an example of a mixed anomaly.

It is interesting to see how the mixed anomaly is manifested in the partition function. The main point can be seen most easily by considering the leading term in the $\beta \to \infty$ expansion which is (taking $\mathcal{B} = 1/2$ for simplicity):

$$Z \to \frac{e^{-\beta E_{ground}}}{2\pi} e^{\mathrm{i}(k-\frac{1}{2})\mu}\left(e^{\mathrm{i}\mu/2} + e^{-\mathrm{i}\mu/2}\right) + \cdots \tag{14.314}$$

If $k = 0$ then

$$Z \to \frac{e^{-\beta E_{ground}}}{2\pi}\left(1 + e^{-\mathrm{i}\mu}\right) + \cdots \tag{14.315}$$

[137] To give a first-principles proof of why this should be so we gauge away $A^{(e)}$ in the path integral. The result is an identification of the fields at $t = 0$ with the fields at $t = \beta$ accompanied by a gauge transformation by the holonomy $e^{\mathrm{i}\mu}$ which takes $e^{\mathrm{i}\phi} \to e^{\mathrm{i}(\phi+\mu)}$. So $\Psi_m \to e^{\mathrm{i}m\mu}\Psi_m = e^{\mathrm{i}\mu Q}\Psi_m$.

the expression is properly periodic in μ, but not invariant under the analog of charge conjugation: $\mu \to -\mu$. This is not surprising since $k \neq \mathcal{B}$.

As we will discuss below, by changing the physical system (yet again!) there is a way to make sense of the half-integral level Chern-Simons term. If we just go ahead and mindlessly substitute $k = \mathcal{B} = 1/2$ in the above formula for $Z(\mu)$ we get:

$$Z \to \frac{e^{-\beta E_{ground}}}{2\pi} \left(e^{\mathrm{i}\mu/2} + e^{-\mathrm{i}\mu/2} \right) + \cdots \tag{14.316}$$

The action is now invariant under the generator $\sigma : \mu \to -\mu$ of D_∞ but it is no longer invariant under the generator $s : \mu \to \mu + 2\pi$.

Provided we view the different choices of Chern-Simons terms as different definitions of the theory, we can define the theory to be invariant under the group generated by s, but with that definition σ is anomalous, or we can define the theory to be invariant udner the group generated by σ, but then with that definition s is anomalous. So in this sense there is a mixed anomaly of $\mathbb{Z}$ and $\mathbb{Z}_2$ in the D_∞ subgroup of global gauge transformations.

Making sense of Chern-Simons terms with half-integer level

There is a way to make sense of the half-integer quantized Chern-Simons term by viewing the $0+1$ dimensional theory as the boundary of a well-defined $1+1$ dimensional theory. By Stokes' theorem we have:

$$\exp[ik \oint_{S^1} A_t^{(e)} dt] = \exp[\mathrm{i}k \int_\Sigma F^{(e)}] \tag{14.317}$$

where $F^{(e)} = dA^{(e)}$. The RHS makes sense even if k is not an integer, but now the expression depends on details of the gauge field in the "bulk" of the $1+1$ dimensional spacetime Σ.

A very analogous phenomenon is observed in real condensed matter systems where the boundary theory of a 3+1 dimensional topological insulator is described by a Chern-Simons theory with half-integral level. (That is, half the level allowed by naive gauge invariance.)

Such half-integral level Chern-Simons terms come up in many interesting physical systems. For example, half-integral (spin) Chern-Simons theory is needed to describe the topological features of the fractional quantum Hall effect. In supersymmetric field theories and string theories many of the supergravity effective actions and brane effective actions involve half-integrally quantized Chern-Simons terms.

Exercise *Puzzle*

Warning: This exercise requires some knowledge of topology.

Resolve the following paradox:

We first argued that, if $k \notin \mathbb{Z}$ then the LHS of (14.317) is not invariant under large gauge transformations. Then we proceeded to define the LHS by the expression on the RHS which is manifestly gauge invariant.

How can these two statements be compatible? [138]

14.5 Heisenberg Extensions

Consider again a central extension

$$1 \to A \to \widetilde{G} \to G \to 1 \tag{14.318}$$

In many of the examples above we had G Abelian and $\widetilde{G}$ was also Abelian. However, as our examples with Q and D_4 have shown, in general $\widetilde{G}$ need not be Abelian. (See equation (14.177).) In this section we focus on an important class of examples where G is Abelian and $\widetilde{G}$ is non-Abelian. They are known as *Heisenberg groups* and *Heisenberg extensions.* In fact in the literature closely related but slightly different things are meant by "Heisenberg extensions" and "Heisenberg groups." These kinds of extensions show up all the time in physics, in many different ways. They are very basic in quantum field theory and other areas of physics, so we are going to dwell upon them a bit.

14.5.1 Preliminary Remarks: Some Useful Formulae For Working With Exponentials Of Operators

In this section we will discuss some formulae that are very useful for working with exponentials of matrices (and linear operators). In particular we will derive the Baker-Campbell-Hausdorff formula. This formula is huge overkill for dealing with Heisenberg groups per se, but it's existence is very useful in a number of other contexts.

Let us recall that if A is a matrix or an operator then e^A is the matrix, or operator, defined by the exponential series. The following three identities are easily shown by direct use of the exponential series:

1. $$e^{\alpha A} e^{\beta A} = e^{(\alpha+\beta)A} \tag{14.319}$$

2. $$\frac{d}{dt} e^{tA} = A e^{tA} = e^{tA} A \tag{14.320}$$

3. $$e^A e^B e^{-A} = e^{e^A B e^{-A}} \tag{14.321}$$

Now we prove some identities that are not directly obvious from the exponential series:

Definition: For $A \in M_n(\kappa)$ we denote by $\mathrm{Ad}(A)$ the linear transformation $M_n(\kappa) \to M_n(\kappa)$ defined by

$$\mathrm{Ad}(A) : B \mapsto [A, B] \tag{14.322}$$

[138] *Answer*: The gauge transformation $e^{\mathrm{i}\alpha(t)}$ must extend to a continuous map $\Sigma \to U(1)$. If Σ is a smooth manifold whose only boundary is S^1, as we have tacitly assumed in writing equation (14.317), then such maps always restrict to small gauge transformations on the bounding S^1.

We also denote:

$$(\mathrm{Ad}(A))^m B = \overbrace{[A,[A,\cdots[A,B]\cdots]}^{m \text{ times}} \tag{14.323}$$

where there are m commutators on the RHS.

First we prove

$$e^A B e^{-A} = e^{\mathrm{Ad}(A)} B \tag{14.324}$$

in other words:

$$\begin{aligned} e^A B e^{-A} &= e^{\mathrm{Ad}(A)} B \\ &= B + \mathrm{Ad}(A)B + \frac{1}{2!}(\mathrm{Ad}(A))^2 B + \cdots \\ &= B + [A,B] + \frac{1}{2!}[A,[A,B]] + \cdots \end{aligned} \tag{14.325}$$

To prove this define $B(t) := e^{tA} B e^{-tA}$. So $B(0) = B$ and $B(1) = e^A B e^{-A}$ is the quantity we want. Now it is easy to derive the differential equation:

$$\frac{d}{dt} B(t) = \mathrm{Ad}(A) B(t) \tag{14.326}$$

so

$$B(t) = e^{t\mathrm{Ad}(A)} B(0) \tag{14.327}$$

Now set $t = 1$.

Combining with (14.321) we now have the somewhat less trivial identity:

$$e^A e^B e^{-A} = e^{e^{\mathrm{Ad}(A)} B} \tag{14.328}$$

All these identities follow from a much more nontrivial formula, known as the Baker-Campbell-Hausdorff formula that expresses the operator C defined by

$$e^A e^B = e^C \tag{14.329}$$

as a power series in A, B. We have

$$C = A + B + s(A,B) \tag{14.330}$$

where $s(A,B)$ is an infinite series and every term involves nested commutators.

We will give a complete statement and proof of the BCH formula below. In order to do that we first state the extremely useful

Lemma : Let

$$f(z) = \frac{e^z - 1}{z} = 1 + \frac{z}{2!} + \frac{z^2}{3!} + \cdots \tag{14.331}$$

Then

$$\left(\frac{d}{dt} e^{A(t)}\right) e^{-A(t)} = -e^{A(t)} \frac{d}{dt} e^{-A(t)} = f(\mathrm{Ad}(A(t))) \cdot \dot{A}(t) \tag{14.332}$$

where $A(t)$ is any differentiable matrix function of t.

Note that this is nontrivial because $\dot{A}(t)$ does not commute with $A(t)$ in general! Indeed, from the exponential series you can easily show that

$$\begin{aligned}\frac{d}{dt}e^{A(t)} - \dot{A}(t)e^{A(t)} &= \frac{1}{2}[A(t),\dot{A}(t)] + \cdots \\ \frac{d}{dt}e^{A(t)} - e^{A(t)}\dot{A}(t) &= -\frac{1}{2}[A(t),\dot{A}(t)] + \cdots\end{aligned} \tag{14.333}$$

Proof: Introduce a matrix function of two variables and take derivatives wrt s:

$$\begin{aligned}B(s,t) &:= e^{sA(t)}\frac{d}{dt}e^{-sA(t)} \\ \frac{\partial B}{\partial s} &= A(t)e^{sA(t)}\frac{d}{dt}e^{-sA(t)} - e^{sA(t)}\frac{d}{dt}\left[e^{-sA(t)}A(t)\right] \\ &= \mathrm{Ad}(A(t))B(s,t) - \dot{A}(t) \\ \frac{\partial^j B}{\partial s_j} &= (\mathrm{Ad}(A(t)))^j B(s,t) - (\mathrm{Ad}A(t))^{j-1}\dot{A}(t)\end{aligned} \tag{14.334}$$

$B(0,t) = 0$ therefore again by Taylor:

$$\frac{1}{j!}\frac{\partial^j}{\partial s^j}B(s,t)\mid_{s=0} = -\mathrm{Ad}(A(t))^{j-1}\dot{A}(t) \qquad j \geq 1 \tag{14.335}$$

So

$$e^{sA(t)}\frac{d}{dt}(e^{-sA(t)}) = -\sum_{j=1}^{\infty}\frac{s^j(\mathrm{Ad}(A(t)))^{j-1}}{j!}\dot{A}(t) \tag{14.336}$$

Now set s=1. ♠

Note: you can rewrite this lemma as the statement:

$$\frac{d}{dt}e^{A(t)} = \int_0^1 e^{sA(t)}\dot{A}(t)e^{(1-s)A(t)}ds \tag{14.337}$$

because:

$$\begin{aligned}\frac{d}{dt}e^{A(t)} &= \int_0^1 e^{sA(t)}\dot{A}(t)e^{(1-s)A(t)}ds \\ &= \int_0^1 e^{sAd(A(t))}ds\dot{A}(t)e^{A(t)} \\ &= \left[\left(\frac{e^{Ad(A(t))}-1}{Ad(A(t))}\right)\dot{A}(t)\right]e^{A(t)}\end{aligned} \tag{14.338}$$

Remark: Equation (14.337) is an intuitively appealing formula. For a finite product we have:

$$\begin{aligned}\frac{d}{dt}\left[M_1(t)M_2(t)M_3(t)\cdots M_n(t)\right] &= (\frac{d}{dt}M_1(t))M_2(t)M_3(t)\cdots \\ &+ (M_1(t))(\frac{d}{dt}M_2(t))M_3(t)\cdots \\ &+ (M_1(t))(M_2(t))(\frac{d}{dt}M_3(t))\cdots \\ &+ \cdots + M_1(t)M_2(t)\cdots(\frac{d}{dt}M_n(t))\end{aligned} \tag{14.339}$$

Now write

$$e^{A(t)} = \prod_{i=1}^{N}[e^{A(t)\Delta s}] \tag{14.340}$$

where $\Delta s = 1/N$. By equation (14.333), we can replace $\frac{d}{dt}e^{\Delta sA(t)}$ by $e^{\Delta sA(t)}\Delta s\dot{A}(t)$ up to order $(\Delta s)^2$. Then write the general term in the sum (14.339) as

$$\left(\prod_{i<s} e^{\Delta sA(t)}\right) e^{\Delta sA(t)}\dot{A}(t)\left(\prod_{s<i} e^{\Delta sA(t)}\right)\Delta s \tag{14.341}$$

up to terms of order $(\Delta s)^2$. Next we sum over these terms and take $N \to \infty$ to get (14.337).

Now we are finally ready to state the main theorem:

Theorem: (Baker-Campbell-Hausdorff formula)
Let:

$$g(w) = \frac{\log w}{w-1} = \sum_{j=0}^{\infty}\frac{(1-w)^j}{j+1} = 1 + \frac{1-w}{2} + \frac{(1-w)^2}{3} + \cdots \tag{14.342}$$

be a power series in w about 1. Then when A, B are $n \times n$ matrices with $\parallel A \parallel$, $\parallel B \parallel$ sufficiently small, the matrix C given by the expansion:

$$\boxed{C = B + \int_0^1 g(e^{t\mathrm{Ad}A}e^{\mathrm{Ad}B})(A)dt} \tag{14.343}$$

satisfies $C = \log(e^A e^B)$.

Proof:

Introduce the matrix-valued function $C(t)$ via:

$$e^{C(t)} = e^{tA}e^B \tag{14.344}$$

and note that $C(0) = B$, and $C(1)$ is the matrix we want. We derive a differential equation for $C(t)$. By our lemma we have:

$$e^{C(t)}\frac{d}{dt}e^{-C(t)} = -f(\mathrm{Ad}C(t))\dot{C}(t) \tag{14.345}$$

with

$$f(z) = \frac{e^z - 1}{z} \tag{14.346}$$

On the other hand, plugging in the definition (14.344) we compute directly the simple result

$$e^{C(t)} \frac{d}{dt} e^{-C(t)} = e^{tA} \frac{d}{dt} e^{-tA} = -A \tag{14.347}$$

Therefore we get a differential equation:

$$f(\mathrm{Ad}C(t))\dot{C}(t) = A \tag{14.348}$$

Now, f is a power series about 1 so it immediately follows that

$$\dot{C}(t) = f(Ad(C(t)))^{-1} A \tag{14.349}$$

Let us make this more explicit: Using the power series $g(w)$ above with $w = e^z$ note that

$$f(z)g(e^z) = \frac{e^z - 1}{z} \cdot \frac{z}{e^z - 1} = 1 \tag{14.350}$$

regarded as an identity of power series in z. Now we can substitute for z any operator $\mathcal{O}$, and use

$$g(e^{\mathcal{O}}) = f(\mathcal{O})^{-1}, \tag{14.351}$$

and therefore we can solve for $\dot{C}$:

$$\begin{aligned} \dot{C}(t) &= f(\mathrm{Ad}(C(t)))^{-1} \cdot A \\ &= g(\exp(\mathrm{Ad}(C(t))) \cdot A \end{aligned} \tag{14.352}$$

where we applied (14.351) with $\mathcal{O} = \mathrm{Ad}(C(t)$. This hardly seems useful, since we still don't know $C(t)$, but now since we have power series we can say

$$e^{\mathcal{O}} = e^{Ad(C(t))} = e^{\mathrm{Ad}(tA)} e^{\mathrm{Ad}(B)} \tag{14.353}$$

To prove (14.353) note that for all H we have:

$$\begin{aligned} e^{\mathrm{Ad}C(t)} H &= e^{C(t)} H e^{-C(t)} \\ &= e^{tA} e^B H e^{-B} e^{-tA} \\ &= e^{\mathrm{Ad}(tA)} e^{\mathrm{Ad}(B)} H \\ \Rightarrow e^{\mathrm{Ad}(C(t))} &= e^{\mathrm{Ad}(tA)} e^{\mathrm{Ad}(B)} \end{aligned} \tag{14.354}$$

Therefore:

$$\dot{C}(t) = g(e^{\mathrm{Ad}(tA)} e^{\mathrm{Ad}(B)}) \cdot A \tag{14.355}$$

Now we integrate equation (14.355)

$$C(t) = C(0) + \int_0^t g(e^{\mathrm{Ad}(sA)} e^{\mathrm{Ad}(B)}) A ds \tag{14.356}$$

but $C(0) = B$, so

$$C = C(1) = \log(e^A e^B) = B + \int_0^1 g(e^{\mathrm{Ad}(s\ A)} e^{\mathrm{Ad}(B)}) A\ ds \tag{14.357}$$

which is what we wanted to show. ♠.

Remarks:

1. To evaluate $g(e^{\mathcal{O}})$ for an operator $\mathcal{O}$ we expand $e^{\mathcal{O}}$ around 0 so $e^{\mathcal{O}} = 1 + \mathcal{O} + \cdots$ and then we expand around 1 to get an expansion of $g(e^{\mathcal{O}})$ around $\mathcal{O} = 0$. A similar remark applies to $g(e^{\mathcal{O}_1} e^{\mathcal{O}_2})$.

2. Explicitly the first few terms are: [139]

$$\boxed{C = A + B + \frac{1}{2}[A, B] + \frac{1}{12}[A, [A, B]] + \frac{1}{12}[B, [B, A]] + \frac{1}{24}[A, [B, [A, B]]] + \cdots} \tag{14.358}$$

   where the next terms are order ϵ^5 if we scale A, B by ϵ.[140]

3. For suitable operators A, B on Hilbert space the BCH formula continues to hold. But the series has a finite radius of convergence: See the exercises below.

4. *A preview of the relation of Lie groups and Lie algebras.* This subject is covered in much more detail in Chapter 8. But here is a preview. Suppose that $\mathfrak{g} \subset M_n(\kappa)$ is a vector subspace of matrices that is closed under matrix commutation, so that $\mathfrak{g}$ is a Lie subalgebra of $M_n(\kappa)$. It might be helpful to keep in mind the classical matrix Lie algebras:

   a.) $\mathfrak{g} = \mathfrak{gl}(n, \kappa) = M_n(\kappa)$.

   b.) $\mathfrak{g} = A_{n-1} = \mathfrak{su}(n)$ is the real Lie algebra of traceless, antihermitian, $n \times n$ matrices in $M_n(\mathbb{C})$.

   c.) $\mathfrak{g} = B_n = \mathfrak{so}(2n+1)$ and $\mathfrak{g} = D_n = \mathfrak{so}(2n)$ is the real Lie algebra of real antisymmetric matrices in $M_{2n+1}(\mathbb{R})$ and $M_{2n}(\mathbb{R})$, respectively.

   d.) $\mathfrak{g} = C_n = \mathfrak{sp}(n) = \mathfrak{usp}(2n)$ is the Lie algebra of matrices $a \in M_{2n}(\mathbb{C})$ such that $(Ja)^{tr} = Ja$.

   Then, provided the BCH series converges it follows that if $A, B \in \mathfrak{g}$ then

$$e^A e^B = e^C \tag{14.359}$$

[139] It is useful to note that $[A, [B, [A, B]]] = -[B, [A, [B, A]]] = B^2 A^2 - A^2 B^2$

[140] One can find an algorithm for generating the higher order terms in Varadarajan's book on group theory.

with $C \in \mathfrak{g}$. Thus, up to convergence issues, the invertible operators e^A with $A \in \mathfrak{g}$ will close to form a group. One can show that for compact connected Lie groups the exponential map

$$\exp : \mathfrak{g} \to G \tag{14.360}$$

is indeed surjective, although it will not be injective. So, taking the closure of the set of matrices $\exp[A]$ with $A \in \mathfrak{g}$ will give the compact Lie group. Conversely, from a matrix Lie group one can recover the Lie algebra by considering the general one-parameter subgroups $g(t)$ with $g(0) = 1$ and computing $g^{-1}(t)\frac{d}{dt}g(t)$ at $t = 0$. In other words, the Lie algebra of G can be associated, as a vector space, with the tangent space at the identity:

$$\mathfrak{g} = T_1 G \tag{14.361}$$

The main theorem in the subject is

Theorem:

a.) Every finite dimensional Lie algebra $\mathfrak{g}$ over $\kappa = \mathbb{R}$ arises from a unique (up to isomorphism) connected and simply connected Lie group G.

b.) Under this correspondence, Lie group homomorphisms $f : G_1 \to G_2$ are in $1 - 1$ correspondence with Lie algebra homomorphisms $\mu : T_1 G_1 \to T_1 G_2$.

Exercise
Work out the BCH series to order 5 in A, B.

Exercise
Show that we can also write:

$$C = \log(e^A e^B) = A + \int_0^1 g(e^{-\mathrm{Ad}(s\ B)} e^{-\mathrm{Ad}(A)})B\ ds \tag{14.362}$$

Exercise *All Orders In B, First Order in A*
Write $A = \epsilon$ and consider it to be small. Show that the formula for C given by BCH to all orders in B and first order in ϵ is

$$\begin{aligned} C &= B + \frac{\mathrm{Ad}B}{e^{\mathrm{Ad}B} - 1}(\epsilon) \\ &= B + \epsilon - \frac{1}{2}[B, \epsilon] + \frac{1}{12}[B, [B, \epsilon]] - \frac{1}{720}[B, [B, [B, [B, \epsilon]]]] + \cdots \end{aligned} \tag{14.363}$$

Note:

$$\begin{aligned}\frac{x}{e^x-1} &= 1-\frac{1}{2}x+\frac{1}{12}x^2-\frac{x^4}{720}+\frac{x^6}{30240}-\frac{x^8}{1209600}+\frac{x^{10}}{47900160}\\ &-\frac{691}{1307674368000}x^{12}+\cdots \\ &\equiv \sum_{n=0}^{\infty}\frac{B_n x^n}{n!}\end{aligned} \tag{14.364}$$

is an important expansion in classical function theory -the numbers B_n are known as the Bernoulli numbers

There are many applications of this formula. One in particle physics is to spontaneous symmetry breaking where the formula above gives the chiral transformation law of the pion field. Here $B=\pi(x)$ is the pion field and ϵ is the chiral transformation parameter.

Exercise *Eigenvalues of* Ad(A) *For Diagonalizable* A

a.) Show that if $A\in M_n(\kappa)$ is diagonalizable $A\sim \text{Diag}\{\lambda_1,\dots,\lambda_n\}$ then the eigenvalues of Ad(A) acting on $M_n(\kappa)$ are $\lambda_i-\lambda_j$.

b.) Using (a) and the previous exercise conclude that the BCH formula has finite radius of convergence.

Exercise *Group Commutators And Lie Algebra Commutators*

a.) Use the BCH theorem to show that if

$$g_1=e^{t_1A_1}, \quad g_2=e^{t_2A_2} \tag{14.365}$$

the <u>*group commutator*</u>, $g_1g_2g_1^{-1}g_2^{-1}$ corresponds to the Lie algebra commutator:

$$g_1\cdot g_2\cdot g_1^{-1}\cdot g_2^{-1}=1+t_1t_2[A_1,A_2]+\mathcal{O}(t_1^2,t_2^2) \tag{14.366}$$

b.) We say a Lie algebra is "Abelian" if $[A_1,A_2]=0$ for all $A_1,A_2\in\mathfrak{g}$. That that such a Lie algebra exponentiates to form an Abelian group.

c.) If $A_i=\frac{d}{dt}|_0 g_i(t)$ then $[A_1,A_2]$ is the Lie algebra element associated to the curve

$$g_{12}(t)=g_1(\sqrt{t})\cdot g_2(\sqrt{t})\cdot g_1^{-1}(\sqrt{t})\cdot g_2^{-1}(\sqrt{t}) \tag{14.367}$$

Exercise *BCH And Representation Theory* a.) A *representation of a Lie algebra* is a linear map

$$\rho : \mathfrak{g} \to \mathrm{End}(V) \tag{14.368}$$

for some vector space V (sometimes called the *carrier space*) such that

$$[\rho(x), \rho(y)] = \rho([x, y]) \tag{14.369}$$

for all $x, y \in \mathfrak{g}$. Recall a *representation of a Lie group* is a group homomorphism

$$\rho : G \to GL(V) \tag{14.370}$$

Given a representation $\dot{\rho}$ of a Lie algebra $\mathfrak{g}$ show that we get a representation of the corresponding Lie group [141] G by setting

$$\rho(e^x) := e^{\dot{\rho}(x)} \tag{14.371}$$

b.) Given a Lie algebra $\mathfrak{g}$ show [142] that it has a canonical representation with $V = \mathfrak{g}$ and

$$\dot{\rho}(x) : y \mapsto \mathrm{Ad}(x)(y) = [x, y] \tag{14.372}$$

c.) Show that for $G = GL(n, \kappa)$ the corresponding Lie algebra is $\mathfrak{gl}(n, \kappa)$. [143]

d.) Consider the adjoint representation of $GL(n, \kappa)$: It acts on $\mathfrak{g} = M_n(\kappa)$ via

$$\rho(g)(x) = gxg^{-1} \tag{14.373}$$

Interpret equation (14.324) as a special case of (14.371) for the adjoint representation. Use this to derive (14.353) from the group homomorphism property of ρ.

14.5.2 Heisenberg Groups: The Basic Motivating Example

Those who have taken quantum mechanics will be familiar with the relation between position and momentum operators for the quantum mechanics of a particle on the real line:

$$[\hat{q}, \hat{p}] = \mathrm{i}\hbar \tag{14.374}$$

One realization of these operator relations is in terms of normalizable wavefunctions $\psi(q)$ where we write:

$$\begin{aligned} (\hat{q} \cdot \psi)(q) &= q\psi(q) \\ (\hat{p} \cdot \psi)(q) &= -\mathrm{i}\hbar \frac{d}{dq}\psi(q) \end{aligned} \tag{14.375}$$

[141] We are assuming there is a corresponding Lie group. Some Lie algebras can, in fact, not be exponentiated to form Lie groups.

[142] *Answer*: Show that the equation $[\dot{\rho}(x), \dot{\rho}(y)] = \dot{\rho}([x, y])$ is equivalent to the Jacobi identity.

[143] *Answer*: Consider the 1-parameter subgroups $\exp[te_{ij}]$ where e_{ij} are the matrix units.

Now, let us consider the operators

$$\begin{aligned} U(\alpha) &:= \exp[\mathrm{i}\alpha\hat{p}] \\ V(\beta) &:= \exp[\mathrm{i}\beta\hat{q}] \end{aligned} \tag{14.376}$$

These are unitary when α, β are real. When α is real $U(\alpha)$ implements translation in position space by $\hbar\alpha$. When β is real $V(\beta)$ implements translation in momentum space by $-\hbar\beta$.

The group of operators $\{U(\alpha)|\alpha \in \mathbb{R}\}$ is isomorphic to $\mathbb{R}$ because $U(\alpha_1)U(\alpha_2) = U(\alpha_1 + \alpha_2)$. A similar statement holds for the group of operators $V(\beta)$. But when we take products of both $U(\alpha)$ and $V(\beta)$ operators we do not get the group $\mathbb{R} \oplus \mathbb{R}$ of translations in position and momentum, separately. Rather, one can show in a number of ways that:

$$U(\alpha)V(\beta) = e^{\mathrm{i}\hbar\alpha\beta} V(\beta)U(\alpha) \tag{14.377}$$

This is an extremely important equation. We can understand it in many different ways. We will explain three ways to derive it. First, it immediately follows from the BCH formula since $[\hat{q}, \hat{p}]$ is central.

A second way to derive (14.377) is to evaluate both operators on a wavefunction in the position representation. So, on the one hand:

$$\begin{aligned} \left((U(\alpha)V(\beta)) \cdot \psi\right)(q) &= \left(V(\beta) \cdot \psi\right)(q + \hbar\alpha) \\ &= e^{\mathrm{i}\beta(q+\hbar\alpha)}\psi(q + \hbar\alpha) \end{aligned} \tag{14.378}$$

On the other hand

$$\begin{aligned} \left((V(\beta)U(\alpha)) \cdot \psi\right)(q) &= e^{\mathrm{i}\beta q}\left(U(\alpha) \cdot \psi\right)(q + \hbar\alpha) \\ &= e^{\mathrm{i}\beta q}\psi(q + \hbar\alpha) \end{aligned} \tag{14.379}$$

Comparing (14.378) with (14.379) we arrive at (14.379). The reader should compare this with our discussion of quantum mechanics with a finite number of degrees of freedom, especially the derivation of (10.77).

Here is a third derivation of (14.377): Using (14.324) it follows that

$$U(\alpha)\hat{q}U(\alpha)^{-1} = e^{\mathrm{i}\alpha\mathrm{Ad}(\hat{p})}\hat{q} = \hat{q} + \hbar\alpha \tag{14.380}$$

$$V(\beta)\hat{p}V(\beta)^{-1} = e^{\mathrm{i}\beta\mathrm{Ad}(\hat{q})}\hat{p} = \hat{q} - \hbar\beta \tag{14.381}$$

Now using (14.328) we obtain (14.377).

Returning to the group generated by the operators $U(\alpha)$ and $V(\alpha)$ for $\alpha \in \mathbb{R}$, which we'll denote $\mathrm{Heis}(\mathbb{R} \times \mathbb{R})$, it fits in a central extension:

$$1 \to U(1) \to \mathrm{Heis}(\mathbb{R} \times \mathbb{R}) \to \mathbb{R} \times \mathbb{R} \to 1 \tag{14.382}$$

With one (nice) choice of cocycle we can write the group law as:

$$(z_1, (\alpha_1, \beta_1)) \cdot (z_2, (\alpha_2, \beta_2)) = (z_1 z_2 e^{\frac{i}{2}\hbar(\alpha_1\beta_2 - \alpha_2\beta_1)}, (\alpha_1 + \alpha_2, \beta_1 + \beta_2)) \tag{14.383}$$

Notice that the cocycle is expressed in terms of the anti-symmetric form

$$\omega(v_1,v_2) := \alpha_1\beta_2 - \alpha_2\beta_1 = \begin{pmatrix}\alpha_1 & \beta_1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = v_1^{tr} J v_2 \tag{14.384}$$

where

$$v = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \tag{14.385}$$

and the matrix

$$J = \begin{pmatrix}0 & 1_n\\ -1_n & 0\end{pmatrix} \tag{14.386}$$

was used at the very beginning of the course (see equation (2.21)) to define the symplectic group $Sp(2n,\kappa)$ as the group of matrices such that $A^{tr}JA = J$.

ω is called a *symplectic form* Note that

$$\omega(A\vec{v}_1, A\vec{v}_2) = \omega(\vec{v}_1,\vec{v}_2) \tag{14.387}$$

for $A \in Sp(2,\mathbb{R})$. We say that ω is invariant under symplectic transformations.

Exercise

Referring to equations (14.377) and (14.375) et. seq.

a.) Show that the choice of section

$$s(\alpha,\beta) = U(\alpha)V(\beta) \tag{14.388}$$

leads to the cocycle

$$f((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{i\hbar(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_1\beta_2)} \tag{14.389}$$

b.) Show that the choice of section

$$s(\alpha,\beta) = \exp[\mathrm{i}(\alpha\hat{p}+\beta\hat{q})] \tag{14.390}$$

leads to the cocycle

$$f((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{\frac{i}{2}\hbar(\alpha_1\beta_2-\alpha_2\beta_1)} \tag{14.391}$$

c.) Find an explicit coboundary that relates the cocycle (14.389) to (14.391).

♣NEED TO PROVIDE ANSWER HERE. ♣

Exercise *Generalization To* Heis$(\mathbb{R}^n \oplus \mathbb{R}^n)$

Consider the group generated by exponentiating linear combinations of $\hat{q}^i$ and $\hat{p}_i$, $i = 1,\dots,n$ with the nonzero commutators being:

$$[\hat{q}^i,\hat{p}_j] = \mathrm{i}\hbar\delta^i{}_j \tag{14.392}$$

Then for

$$\vec{v} = \begin{pmatrix} \alpha_i \\ \beta^j \end{pmatrix} \tag{14.393}$$

we can choose section:

$$s(\vec{v}) = \exp\left[\mathrm{i}(\alpha^i \hat{p}_i + \beta_i \hat{q}^i)\right] \tag{14.394}$$

Show that the resulting group is

$$(z_1, \vec{v}_1) \cdot (z_2, \vec{v}_2) = (z_1 z_2 e^{\mathrm{i}\frac{\hbar}{2}\omega(\vec{v}_1, \vec{v}_2)}, \vec{v}_1 + \vec{v}_2) \tag{14.395}$$

with ω defined by equation (14.353).

14.5.3 The Commutator Function And The Definition Of A General Heisenberg Group

Let us now step back and think more generally about central extensions of G by A where G is *also abelian.* From the exercise (14.190) we know that for G abelian the commutator is

$$[(a_1, g_1), (a_2, g_2)] = \left(\frac{f(g_1, g_2)}{f(g_2, g_1)}, 1\right) \tag{14.396}$$

(We are writing $1/f(g_2, g_1)$ for $f(g_2, g_1)^{-1}$ and since A is abelian the order doesn't matter, so we write a fraction as above.)

The function $\kappa : G \times G \to A$ defined by

$$\kappa(g_1, g_2) = \frac{f(g_1, g_2)}{f(g_2, g_1)} \tag{14.397}$$

is known as the *commutator function.*

Note that:

1. The commutator function is *gauge invariant*, in the sense that it does not change under the change of 2-cocycle f by a coboundary. (Check that! This uses the property that G is abelian). It is therefore a more intrinsic quantity associated with the central extension.

2. $\kappa(g, 1) = \kappa(1, g) = 1$. (This follows from exercise (14.92) above.)

3. The extension $\tilde{G}$ is abelian iff $\kappa(g_1, g_2) = 1$, that is, iff there exists a symmetric cocycle f. [144]

4. κ is *skew*:

$$\kappa(g_1, g_2) = \kappa(g_2, g_1)^{-1} \tag{14.398}$$

5. κ is *alternating*:

$$\kappa(g, g) = 1 \tag{14.399}$$

[144] Note that in our example of Q, D_4 as extensions the cocycle we computed was not symmetric.

6. κ is *bimultiplicative*:

$$\kappa(g_1g_2, g_3) = \kappa(g_1, g_3)\kappa(g_2, g_3) \tag{14.400}$$

$$\kappa(g_1, g_2g_3) = \kappa(g_1, g_2)\kappa(g_1, g_3) \tag{14.401}$$

All of these properties except, perhaps, the last, are obvious. To prove the bimultiplicative properties (it suffices to prove just one) we rewrite (14.400) as

$$f(g_1g_2, g_3)f(g_3, g_2)f(g_3, g_1) = f(g_2, g_3)f(g_1, g_3)f(g_3, g_1g_2) \tag{14.402}$$

Now multiply the equation by $f(g_1, g_2)$ and use the fact that A is abelian to write

$$(f(g_1, g_2)f(g_1g_2, g_3))f(g_3, g_2)f(g_3, g_1) = f(g_2, g_3)f(g_1, g_3)(f(g_1, g_2)f(g_3, g_1g_2)) \tag{14.403}$$

We apply the cocycle identity on both the LHS and the RHS (and also use the fact that G is abelian) to get

$$f(g_2, g_3)f(g_1, g_2g_3)f(g_3, g_2)f(g_3, g_1) = f(g_2, g_3)f(g_1, g_3)f(g_3, g_1)f(g_3g_1, g_2) \tag{14.404}$$

Now canceling some factors and using that A is abelian we have

$$f(g_1, g_2g_3)f(g_3, g_2) = f(g_1, g_3)f(g_3g_1, g_2) \tag{14.405}$$

Now use the fact that G is abelian to write this as

$$f(g_1, g_3g_2)f(g_3, g_2) = f(g_1, g_3)f(g_1g_3, g_2) \tag{14.406}$$

which is the cocycle identity. This proves the bimultiplicative property (14.400). ♠

We now define the *Heisenberg extensions*. The function κ is said to be *nondegenerate* if for all $g_1 \neq 1$ there is a g_2 with $\kappa(g_1, g_2) \neq 1$. When this is the case the center of $\tilde{G}$ is precisely A:

$$Z(\widetilde{G}) \cong A\ . \tag{14.407}$$

This follows immediately from equation (14.396). If κ is degenerate the center will be larger. In the extreme case that $\kappa(g_1, g_2) = 1$ for all g_1, g_2 we get the direct product $\widetilde{G} = A \times G$ and

$$Z(\widetilde{G}) = \widetilde{G}\ . \tag{14.408}$$

In general, we will have an intermediate situation and A will be a proper subgroup of $Z(\tilde{G})$.

One definition which is used in the literature is

Definition: A *Heisenberg extension* is a central extension of an *abelian* group G by an *abelian* group A where the commutator function κ is nondegenerate.

Exercise *Alternating implies skew*

Show that a map $\kappa : G \times G \to A$ which satisfies the bimultiplicative identity (14.400) and the alternating identity (14.399) is also skew, that is, satisfies (14.398).

Exercise *Commutator function for* Heis($\mathbb{R} \oplus \mathbb{R}$)

a.) Show that both of the cocycles (14.389) and (14.391) defining groups isomorphic to Heis($\mathbb{R} \oplus \mathbb{R}$) have the same commutator function

$$\kappa((\alpha_1, \beta_1), (\alpha_2, \beta_2) = e^{i\hbar(\alpha_1\beta_2 - \alpha_2\beta_1)} = e^{i\hbar\omega(v_1,v_2)} \tag{14.409}$$

b.) Similarly show that for Heis($\mathbb{R}^n \oplus \mathbb{R}^n$) we have

$$\kappa(v_1, v_2) = \exp\left(i\hbar\omega(v_1, v_2)\right) \tag{14.410}$$

where

$$\omega(v_1, v_2) = v_1^{tr} J v_2 \tag{14.411}$$

14.5.4 Classification Of $U(1)$ Central Extensions Using The Commutator Function

For a large class of abelian groups G, there is a nice theorem regarding arbitrary central extensions by $U(1)$. We consider

1. Finitely generated Abelian groups. As we will prove in sections 15.2 and 15.3 below, these can be (noncanonically) written as products of cyclic groups $\mathbb{Z}_n$, for various n, and a lattice $\mathbb{Z}^d$ for some d (possibly $d = 0$).
2. Vector spaces. [145]
3. Tori. These are isomorphic to $V/\mathbb{Z}^d$ where V is a d-dimensional real vector space.
4. Direct products of the above three.

Remark: This class of groups can be characterized as the set of Abelian groups A which are topological groups so there is an exact sequence:

$$0 \to \pi_1(A) \to \text{Lie}(A) \to A \to \pi_0(A) \to 0 \tag{14.412}$$

where Lie(A) is a vector space that projects to A by an exponential map.

For this class of groups we have the following theorem:

[145] Topological, separable.

Theorem Let G be a topological Abelian group of the above class. The isomorphism classes of central extensions of G by $U(1)$ are in one-one correspondence with continuous bimultiplicative maps

$$\kappa : G \times G \to U(1) \tag{14.413}$$

which are alternating (and hence skew).

I do not know who originally proved this theorem, but one proof can be found in [146]

Remarks

1. In other words, given the commutator function κ one can always find a corresponding cocycle f. This theorem is useful because κ is invariant under change of f by a coboundary, and moreover the bimultiplicative property is simpler to check than the cocycle identity. (In fact, one can show that it is always possible to find a cocycle f which is bimultiplicative. This property automatically ensures the cocycle relation.)
2. It is important to realize that κ only characterizes $\tilde{G}$ up to *noncanonical* isomorphism: to give a definite group one must choose a definite cocycle.

♣Explain this comment more. ♣

3. In this theorem we can replace $U(1)$ by any subgroup of $U(1)$, such as $\mathbb{Z}_n$ realized as the group of n^{th} roots of unity.

14.5.5 Pontryagin Duality

Using the notion of the *Pontryagin dual* of an Abelian group we can give a very general construction of interesting Heisenberg extensions. [147] We already encountered Pontryagin duality briefly in section 10.2. We will review and extend it here.

Definition: Let S be an Abelian group. The *Pontryagin dual* group $\widehat{S}$ is defined to be the group of homomorphisms $\mathrm{Hom}(S, U(1))$. Note that if $\chi_1, \chi_2 \in \mathrm{Hom}(S, U(1))$ then the pointwise product

$$(\chi_1 \cdot \chi_2)(s) := \chi_1(s)\chi_2(s) \tag{14.414}$$

is again a homomorphism $S \to U(1)$, thus making $\widehat{S}$ into an Abelian group.

Remarks:

1. The Pontryagin dual group $\widehat{S}$ can also be thought of as the group of all complex one-dimensional unitary representations of S. It follows from Schur's lemma that all irreducible finite dimensional complex representations of an Abelian group are

[146] D. Freed, G. Moore, G. Segal, "The uncertainty of fluxes," Commun.Math.Phys. 271 (2007) 247-274, arXiv:hep-th/0605198, Proposition A.1.

[147] The transliteration from the Cyrillic to the Latin alphabets takes various forms. Another common one is Pontrjagin.

one-dimensional. [148] Note that the adjective complex is essential here. After all the defining representation of the Abelian group $SO(2)$ is $\mathbb{R}^2$ and is irreducible as a representation over $\mathbb{R}$.

2. Elements of the group $\widehat{S}$ are also called characters.

3. It is best to discuss Pontryagin duality in the context of topological groups. In this case we should only consider the continuous characters $\chi : S \to U(1)$. For the duality theorem below we should consider *locally compact Abelian groups.* A topological space X is *locally compact* if, for every $x \in X$ there is a compact neighborhood of x. That is, there is a compact subspace $K \subset X$ so that $x \in U \subset K$ for some open neighborhood U of x. Examples of locally compact Abelian groups are $\mathbb{R}^n$, tori, lattices, and finite Abelian groups with compact topology. An infinite-dimensional Hilbert space is a topological Abelian group under addition, but it is not locally compact.

Note that, for a fixed $s \in S$ we can define a homomorphism $\mathrm{Hom}(\widehat{S}, U(1))$ by

$$\hat{s} : \chi \mapsto \chi(s) \tag{14.415}$$

The map $s \mapsto \hat{s}$ is a homomorphism $S \to \widehat{\widehat{S}}$. The main theorem is:

Theorem[Pontryagin-van Kampen duality]. If G is a locally compact Abelian group then the canonical homomorphism $S \to \widehat{\widehat{S}}$ is in fact an isomorphism:

$$\widehat{\widehat{S}} \cong S \tag{14.416}$$

For a proof see, for example, the book on representation theory by A.A. Kirillov.

Example 1: Consider $S = \mathbb{Z}/n\mathbb{Z}$, thought of additively. To determine $\chi \in \mathrm{Hom}(S, U(1))$ it suffices to determine $\chi(\bar{1})$, since $\chi(\bar{\ell}) = \chi(\bar{1})^\ell$ for any $\ell \in \mathbb{Z}$. Put $\chi(\bar{1}) = \omega \in U(1)$. But now we need to impose the relation $\chi(\bar{n}) = \chi(\bar{0}) = 1$. This implies $\omega^n = 1$, so ω is an n^{th} root of unity. So the most general element of $\widehat{\mathbb{Z}/n\mathbb{Z}}$ is

$$\chi(\bar{\ell}) = \chi_\omega(\bar{\ell}) := \omega^\ell \tag{14.417}$$

where ω is an n^{th} root of unity. Moreover $\chi_{\omega_1}\chi_{\omega_2} = \chi_{\omega_1\omega_2}$ so $\widehat{\mathbb{Z}/n\mathbb{Z}}$ is identified in this way with the multiplicative group of n^{th} roots of unity. In this way we see that, as abstract groups

$$\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z} \tag{14.418}$$

[148] See Chapter four. Here is a brief summary of the argument: Suppose (ρ, V) is a finite-dimensional irreducible representation of a group G on a complex vector space V. Suppose an operator A commutes with $\rho(g)$ for all g. Any operator on a complex vector space has at least one eigenvalue because $\det(A - x)$ has at least one complex root. Let $V_\lambda \subset V$ be the corresponding eigenspace. Note that this is a nonzero invariant subspace so $V_\lambda = V$, that is $A = \lambda\mathbf{1}$. Now, for an Abelian group for any $g_0 \in G$, the operator $\rho(g_0)$ commutes with all the operator $\rho(g)$. So $\rho(g_0) = \chi(g_0)\mathbf{1}$.

Example 2: Consider $\mathbb{R}$, additively. Then if $\chi \in \widehat{\mathbb{R}}$ we have $\chi(x+y) = \chi(x)\chi(y)$ so $\chi(x) = e^{ax}$ for some constant a. For χ to be valued in $U(1)$ we must have $a = \mathrm{i}k$ with $k \in \mathbb{R}$ and hence

$$\chi(x) = \chi_k(x) := e^{\mathrm{i}kx} \tag{14.419}$$

moreover,

$$\chi_k \chi_\ell = \chi_{k+\ell} \tag{14.420}$$

and hence $\widehat{\mathbb{R}} \cong \mathbb{R}$. In an entirely similar way $\widehat{\mathbb{R}^n} \cong \mathbb{R}^n$

Example 3: Consider $S = \mathbb{Z}$. To determine $\chi \in \mathrm{Hom}(S, U(1))$ it suffices to determine $\chi(1)$. Choose any phase $\xi \in U(1)$ and set $\chi(1) = \xi$. Then it must be that, for all $n \in \mathbb{Z}$:

$$\chi(n) = \chi_\xi(n) := \xi^n \tag{14.421}$$

Moreover $\chi_{\xi_1}\chi_{\xi_2} = \chi_{\xi_1\xi_2}$. Thus,

$$\widehat{\mathbb{Z}} \cong U(1) \tag{14.422}$$

Example 4: Consider $S = U(1)$. To determine $\chi \in \mathrm{Hom}(S, U(1))$ it might help to think of $U(1) \cong \mathbb{R}/\mathbb{Z}$. We know from the Pontryagin dual of $\mathbb{R}$ that χ should be of the form

$$\chi(x + \mathbb{Z}) = \exp[\mathrm{i}k(x + \mathbb{Z})] \tag{14.423}$$

for some real number k. However, for this to be well-defined we must have $k = 2\pi n$ with $n \in \mathbb{Z}$. Therefore χ must be of the form

$$\chi_n(x + \mathbb{Z}) = \exp[2\pi \mathrm{i} n x] \tag{14.424}$$

Or, if we think of $S = U(1)$ multiplicatively as complex numbers of modulus one, then we can say that every character on $U(1)$ is of the form:

$$\chi_n(\xi) := \xi^n \tag{14.425}$$

for some $n \in \mathbb{Z}$. Therefore,

$$\widehat{U(1)} \cong \mathbb{Z} \tag{14.426}$$

Comparing (14.422) and (14.426) we verify the general result (14.416).

Example 5: *Tori.* Consider the group $G = \mathbb{Z}^d$. It will be useful to consider a free G action on affine Euclidean space $\mathbb{E}^d$. This defines a subset $\Gamma \subset \mathbb{E}^d$ known as a *lattice* (sometimes called an *embedded lattice*). The quotient space $\mathbb{E}^d/\Gamma$ has a natural basepoint, namely the coset of Γ and, as a group it is isomorphic to $U(1)^d$. By the same arguments as above its Pontryagin dual will be isomorphic to $\mathbb{Z}^d$.

There is a nice way to think about the Pontryagin duality between lattices and tori. Suppose Γ is a lattice in $\mathbb{R}^d$. Using the Euclidean norm we can define another lattice, the *dual lattice*

♣Really we should do this using the dual vector space... ♣

$$\Gamma^\vee = \{k \in \mathbb{R}^d | k \cdot \gamma \in \mathbb{Z} \qquad \forall \gamma \in \Gamma\} \tag{14.427}$$

As a group $\Gamma^\vee \cong \mathrm{Hom}(\Gamma, \mathbb{Z})$.

The unitary irreps of Γ are represented by points in the torus $\bar{k} \in \mathbb{R}^d/\Gamma^\vee$. Indeed we can write:

$$\chi_{\bar{k}}(\gamma) = \exp[2\pi \mathrm{i} k \cdot \gamma] \tag{14.428}$$

where k is any representative of $\bar{k}$, that is $\bar{k} = k + \Gamma^\vee$. Note that the above formula is well-defined. So

$$\widehat{\Gamma} \cong \mathbb{R}^d/\Gamma^\vee \cong U(1)^d \tag{14.429}$$

Conversely, the Pontryagin dual of the torus $\mathbb{R}^d/\Gamma^\vee$ can be identified with Γ by the same formula:

$$\chi_\gamma(\bar{k}) = \exp[2\pi \mathrm{i} k \cdot \gamma] \tag{14.430}$$

Exercise *Pontryagin Dual Of The Prüfer Groups*

Recall that the Prüfer groups $Pr(p)$ are defined for each prime p as the union over all n of roots of unity of order p^n.

What is the Pontryagin dual of $Pr(p)$? (Give it the discrete topology.) [149]

14.5.6 An Application Of Pontryagin Duality: Bloch's Theorem And Band Structure

The Pontryagin duality between an embedded lattice $\Gamma \subset \mathbb{R}^d$ and the torus $\mathbb{R}^d/\Gamma^\vee$ has a very significant application in condensed matter physics known as *Bloch's theorem.*

In the one-electron approximation to the Schrodinger problem of electrons in a crystal one considers the Schrödinger Hamiltonian on $L^2(\mathbb{R}^d)$ of the form:

$$H = -\frac{\hbar^2}{2m}\nabla^2 + U(x) \tag{14.432}$$

where the potential $U : \mathbb{R}^d \to \mathbb{R}$ is assumed to be invariant under some crystallographic group (see below). In particular, it is invariant under translation by a lattice $\Gamma \subset \mathbb{R}^d$. For exampe, if we take into account the Coulomb interaction between the electron and a collection of ions of charge $Z_i e$ at positions $x_i \in C$, where C is a crystal then

$$U(x) = \sum_i \frac{-Z_i e^2}{|x - x_i|} \tag{14.433}$$

[149] *Answer*: Use the isomorphism $U(1) \cong \mathbb{R}/\mathbb{Z}$. One needs to say what is the image of p^{-n}. So $\chi(\frac{1}{p^n}) = \exp[2\pi \mathrm{i} a_n/p^n]$, for some integer a_n because $\chi(p^{-n})$ must itself be a $(p^n)^{th}$ root of unity. Note we can regard $a_n \in \mathbb{Z}/p^n\mathbb{Z}$. Now note that

$$\exp[2\pi \mathrm{i}\frac{a_{n-1}}{p^{n-1}}] = \chi(\frac{1}{p^{n-1}}) = \chi(\frac{1}{p^n})^p = \exp[2\pi \mathrm{i}\frac{a_n}{p^{n-1}}] \tag{14.431}$$

So the Pontryagin dual is the subgroup of $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ consisting of sequences a_n so that a_n projects to a_{n-1}. This is known as the group of p-adic integers.

But for the statement we are going to make all we need is that $U(x+\gamma)=U(x)$ for $\gamma\in\Gamma$. Now the group Γ acts on the Hilbert space through unitary operators commuting with H. Explicitly:

$$\rho(\gamma)=\exp[\mathrm{i}\gamma\cdot\hat{p}] \tag{14.434}$$

Note that in this case there is no nontrivial central extension. It follows that the Hilbert space is a representation of Γ, and the Hamiltonian acts within each representation space.

We have classified the one-dimensional representations above so if $\psi\in\mathcal{H}$ were to be in a one-dimensional representation then it would have to be quasi-periodic:

$$\psi(x+\gamma)=\chi_{\bar{k}}\psi(x) \tag{14.435}$$

where $\bar{k}\in\mathbb{R}^d/\Gamma^\vee$. In this context Pontryagin dual torus is known as the *Brillouin torus.* It follows that eigenfunctions can be written (noncanonically!!!) as

$$\psi(x)=e^{\mathrm{i}k\cdot x}u_k(x) \tag{14.436}$$

where $k/2\pi\in\Gamma^\vee$ is known as a *reciprocal vector* and $u_k(x)$ is periodic in x, i.e. invariant under shifts of $x\to x+\gamma$ for $\gamma\in\Gamma$.

There is a technical point here usually glossed over in physics textbooks. A quasiperiodic fuction (14.435) cannot also be L^2. For each point $\bar{k}$ in the Brillouin torus define the Hilbert space

$$\mathcal{H}_{\bar{k}}:=\{\psi(x)|\psi(x+\gamma)=\chi_{\bar{k}}(\gamma)\psi(x) \qquad \int_{\mathbb{R}^d/\Gamma}|\psi(x)|^2dx<\infty\} \tag{14.437}$$

Then there is a measure on the torus so that we have an isomorphism

$$\mathcal{H}\cong\oint_{\mathbb{R}^d/\Gamma^\vee}d\bar{k}\mathcal{H}_{\bar{k}} \tag{14.438}$$

Now, the Hamiltonian acts within $\mathcal{H}_{\bar{k}}$. It is useful to write the eigenvalue problem as

$$H_ku_k(x)=E_ku_k(x) \tag{14.439}$$

where

$$H_k=e^{-\mathrm{i}k\cdot x}He^{\mathrm{i}k\cdot x} \tag{14.440}$$

Note that we had to make a choice of k that projects to $\bar{k}$ to write the Hamiltonian H_k. However, if $k'=k+g$ where $g\in\Gamma^\vee$ then $H_{k'}$ is unitarily equivalent to H_k.

♣Should be possible to give the explicit unitary transformation - exercise? ♣

H_k is an Hermitian elliptic operator acting on the functions on a compact manifold. It is a compact perturbation of a Laplace operator and therefore has a discrete spectrum of eigenvalues $\{E_n(k)\}$. Note that while H_k depends on k, the spectrum itself only depends on $\bar{k}$.

♣You should explain in more detail why the spectrum is discrete. ♣

The eigenvalues vary continuously as functions of $\bar{k}\in\mathbb{R}^d/\Gamma^\vee$ to give what is called a *band structure.* See Figure 29.

Remark: *Magnetic translation group.* In the presence of an electromagnetic field the group of translations acting on charged particles definitely becomes centrally extended.

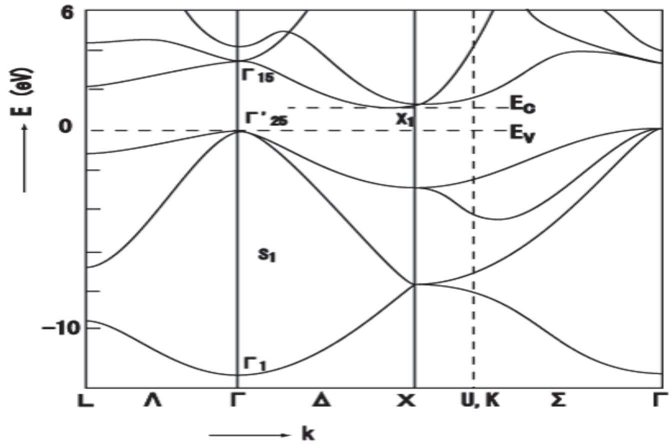

Figure 29: Example of a bandstructure. (For silicon.) On the horizontal axis the structure is plotted as a function of k along lines inside the Brillouin torus. The letters refer to points where the (cubic) crystallographic group has fixed points. Γ denotes the identity element $\bar{k} = 0$ where the full cubic symmetry group is restored.

This shows up naturally when discussing a charged nonrelativistic particle confined to two spatial dimensions and moving in a constant magnetic field B. In one convenient gauge the Hamiltonian is

$$H = \frac{1}{2m}\left((p_1 + \frac{eBx_2}{2})^2 + (p_2 - \frac{eBx_1}{2})^2\right) = \frac{1}{2m}(\tilde{p}_1^2 + \tilde{p}_2^2) \tag{14.441}$$

where the gauge invariant momenta are $\tilde{p}_i := p_i - eA_i$ are

$$\begin{aligned}\tilde{p}_1 &= p_1 + \frac{eB}{2}x_2 \\ \tilde{p}_2 &= p_2 - \frac{eB}{2}x_1\end{aligned} \tag{14.442}$$

Ordinary translations are generated by p_1, p_2 and do not commute with the Hamitonian: We have lost translation invariance. Nevertheless we can define the *magnetic translation operators*:

$$\pi_1 := p_1 - \frac{eBx_2}{2} \qquad\qquad \pi_2 := p_2 + \frac{eBx_1}{2} \tag{14.443}$$

Compare this carefully with the definitions of $\tilde{p}_i$. Note the relative signs! These operators satisfy $[\pi_i, \tilde{p}_j] = 0$. In particular they are translation-like operators that commute with the Hamiltonian: $[\pi_i, H] = 0$. Hence the name. While they are called "translation operators" note that they do not commute:

$$[\pi_1, \pi_2] = -i\hbar eB \tag{14.444}$$

The "magnetic translation group" is generated by the operators

$$\begin{aligned} U(a_1) &= \exp[i a_1 \pi_1/\hbar] \\ V(a_2) &= \exp[i a_2 \pi_2/\hbar] \end{aligned} \tag{14.445}$$

The operators $U(a_1), V(a_2)$ satisfy the relations:

$$U(a_1)V(a_2) = \exp[\mathrm{i}eBa_1a_2/\hbar]V(a_2)U(a_1) \tag{14.446}$$

If we are interested in quantized values of a_1, a_2 (as, for example, if the charged particle is moving in a lattice, or is confined to a torus) then we obtain the basic relations (14.642). Note that

$$\exp[\mathrm{i}eBa_1a_2/\hbar] = \exp[2\pi\mathrm{i}\Phi/\Phi_0] \tag{14.447}$$

where $\Phi = Ba_1a_2$ is the flux through an area element a_1a_2 and $\Phi_0 = h/e$ is known as the *magnetic flux quantum.* [150]

Remark: The group generated by the operators $U = U(a_1)$ and $V = V(a_2)$ is a Heisenberg group, but it is also interesting to consider the *algebra* of operators generated by U, V. This algebra admits a $C*$-algebra structure and is sometimes referred to as the *algebra of functions on the noncommutative torus* or the *irrational rotation algebra.* Abstractly it is the C^* algebra generated by unitary operators U, V satisfying $UV = e^{2\pi i\theta}VU$ for some θ. The properties of the algebra are very different for θ rational and irrational. The algebra $\mathcal{A}_\theta$ figures prominantly in applications of noncommutative geometry to the QHE and in applications of noncommutative geometry to toroidal compactifications of string theory.

14.5.7 Pontryagin Duality And The Stone-von Neumann-Mackey Theorem

The theorem of section 14.5.4 is nicely illustrated by the Heisenberg of extension of the Abelian group $G = S \times \widehat{S}$ by $A = U(1)$. Here S is any locally compact Abelian group and $\widehat{S}$ is the Pontryagin dual.

Now, there is a very natural alternating, skew, bilinear map on the product $S \times \widehat{S}$ defined by

$$\kappa\left((s_1,\chi_1),(s_2,\chi_2)\right) := \frac{\chi_2(s_1)}{\chi_1(s_2)} \tag{14.448}$$

and according to the above theorem this defines a general Heisenberg extension

$$1 \to U(1) \to \mathrm{Heis}(S\times\widehat{S}) \to S\times\widehat{S} \to 1 \tag{14.449}$$

at least up to isomorphism.

Remarks

1. Note that one natural cocycle giving the commutator function (14.448) is

$$f\left((s_1,\chi_1),(s_2,\chi_2)\right) := \frac{1}{\chi_1(s_2)} \tag{14.450}$$

[150] One should be careful about a factor of two here since in superconductivity the condensing field has charge $2e$ and hence the official definition of the term "flux quantum" used, for example, by NIST is $\Phi_0 = h/2e$, half the value we use.

2. There is a very natural representation of (14.449). We need a Haar measure on S so that we can define $V = L^2(S)$, a Hilbert space of complex-valued functions on S. For our key examples we have

$$\begin{aligned}\langle\psi_1,\psi_2\rangle &= \int_{\mathbb{R}} \psi_1^*(x)\psi_2(x)dx \qquad S=\mathbb{R}\\ &= \sum_{n\in\mathbb{Z}} \psi_1^*(n)\psi_2(n) \qquad S=\mathbb{Z}\\ &= \frac{1}{2\pi}\int_0^{2\pi} \psi_1^*(e^{\mathrm{i}\theta})\psi_2(e^{\mathrm{i}\theta})d\theta \qquad S=U(1)\\ &= \frac{1}{n}\sum_{k=0}^{n-1}\psi_1^*(\bar{k})\psi_2(\bar{k}) \qquad S=\mathbb{Z}/n\mathbb{Z}\end{aligned} \tag{14.451}$$

We represent $s_0 \in S$ as a translation operator:

$$(T_{s_0}\cdot\Psi)(s) := \Psi(s+s_0) \tag{14.452}$$

and we represent $\chi_0 \in \widehat{S}$ as a multiplication operator

$$(M_{\chi_0}\cdot\Psi)(s) := \chi_0(s)\Psi(s) \tag{14.453}$$

Then one checks that this does not define a representation of the direct product $S\times\widehat{S}$ but rather we have the operator equation:

$$T_{s_0}M_{\chi_0} = \chi_0(s_0)M_{\chi_0}T_{s_0} \tag{14.454}$$

If $\mathcal{O}$ is the group of operators generated by T_s, M_χ and $z\in U(1)$ acting on V then the map

$$(z;(s,\chi)) \to zT_sM_\chi \tag{14.455}$$

is a homomorphism, and in fact an isomorphism of $\mathrm{Heis}(S\times\widehat{S})$ with $\mathcal{O}$ where we use the cocycle (14.450).

3. This construction is extremely important in quantum mechanics and also in the description of free quantum field theories. In these cases we take S to be a vector space. For example, for the quantum mechanics of a particle in $\mathbb{R}^n$ we have $V=\mathbb{R}^n$ as an Abelian group. For the quantum field theory of a free real scalar field in $d+1$ dimensions we would take V to be a suitable space of real-valued functions on a d-dimensional spatial slice. [151] Then we introduce the dual vector space $V^\vee \cong \widehat{S}$, and the canonical pairing $V\times V^\vee \to \mathbb{R}$ gives the character:

$$\chi_k(v) = e^{\mathrm{i}k\cdot v} \tag{14.456}$$

Then, T_s in our general discussion is the operator $U(s)$ of the basic motivating example, and M_{χ_k} is the operator $V(k)$ of the basic motivating example and the general identity (14.454) becomes our starting point:

$$U(s)V(k) = e^{\mathrm{i}k\cdot s}V(k)U(s) \tag{14.457}$$

[151] Technical point: This will not be locally compact. So, if one wishes to be rigorous, further considerations are required.

4. *Stone-von Neumann-Mackey Theorem.* Up to isomorphism (equivalence) there is a unique irreducible unitary representation of $\mathrm{Heis}(S \times \widehat{S})$ such that $A = U(1)$ acts by scalar multiplication. That is, if $\xi \in U(1)$ then we require $\rho(\xi) = \xi \mathbf{1}_V$. In addition we need some further technical hypotheses. [152] This is called the Stone-von Neumann theorem or sometimes the Stone-von Neumann-Mackey theorem. For a relatively short proof see. [153] The main idea is to consider the maximal Abelian subgroups of $\mathrm{Heis}(S \times \widehat{S})$. One such subgroup is isomorphic to $U(1) \times S$, another is $U(1) \times \widehat{S}$. Let us consider $U(1) \times \widehat{S}$. Over the subgroup $\{1\} \times \widehat{S}$ we can split the sequence and consider the elements:

$$M_\chi := \rho(1, (0, \chi)) \tag{14.458}$$

where $1 \in U(1)$, $0 \in S$, and $\chi \in \widehat{S}$. These operators commute for different choices of χ and are simultaneously diagonalizable so we have a complete basis ψ_α of simultaneous eigenvectors for the representation with eigenvalues: [154]

$$M_\chi \psi_\alpha = \lambda_\alpha(\chi) \psi_\alpha \tag{14.459}$$

Clearly $\chi \mapsto \lambda_\alpha(\chi)$ must be a character on $\widehat{S}$, so the eigenvalues can be identified with characters on $\widehat{S}$ and therefore, by Pontryagin duality, can be identified with elements $s_\alpha \in S$. So there is some set $\{s_\alpha\}$ whose elements are drawn from S with corresponding eigenbasis ψ_α with

$$M_\chi \psi_\alpha = \chi(s_\alpha) \psi_\alpha \tag{14.460}$$

Now, for any $s \in S$ define the operator

$$T_s := \rho(1, (s, 1)) \tag{14.461}$$

Choose some particular α_0 and consider the vectors $T_s \psi_{\alpha_0}$ for $s \in S$. Using the Heisenberg relations and the fact that the central $U(1)$ group just acts by scalars we know that:

$$M_\chi \left(T_s \psi_{\alpha_0}\right) = \chi(s - s_{\alpha_0}) \left(T_s \psi_{\alpha_0}\right) \tag{14.462}$$

Therefore the span of $\{T_s \psi_{\alpha_0}\}_{s \in S}$, which is the span of $\{T_{s+s_{\alpha_0}} \psi_{\alpha_0}\}_{s \in S}$ is a copy of the representation constructed above. So if (V, ρ) is irreducible, it must be equivalent to our representation constructed above. This demonstrates uniqueness of the irreducible representation.

5. *Simple Proof Of Irreducibility for $S = \mathbb{R}^n$.* For $v = (\alpha, \beta) \in \mathbb{R}^{2n}$ we introduced the section

$$s(v) := \exp[\mathrm{i}(\alpha \hat{q} + \beta \hat{p})] \tag{14.463}$$

Now, consider the standard representation of $\mathrm{Heis}(\mathbb{R}^n \times \widehat{\mathbb{R}^n})$ on $\mathcal{H} = L^2(\mathbb{R}^n)$. For

♣This remark assumes at least a little bit of knowledge from the linear algebra chapter 2 and the idea of an irreducible representation, from chapter 4. ♣

♣The α, β here are reversed from the convention in previous section. ♣

[152] We need the representation to be continuous in the norm topology and we need S to have a translation-invariant measure so that $L^2(A)$ makes sense. Then we replace V above by the Hilbert space $L^2(S)$.

[153] A. Prasad, "An easy proof of the Stone-von Neumann-Mackey Theorem," arXiv:0912.0574.

[154] It is exactly at this point that we are using unitarity, and a careful discussion requires more functional analysis.

any two vectors $\psi_1, \psi_2 \in \mathcal{H}$ define the *Wigner function*:

$$W(\psi_1, \psi_2)(v) := \langle s(v)\psi_1, \psi_2 \rangle \tag{14.464}$$

This is a function on the phase space $v \in \mathbb{R}^{2n}$. Now we compute:

$$(s(v)\psi_1)(q) = e^{\mathrm{i}\frac{\alpha\beta}{2}} e^{\mathrm{i}\alpha q} \psi_1(q + \beta) \tag{14.465}$$

Shifting the integration variable by $\beta/2$ in the inner product we have

$$W(\psi_1, \psi_2)(v) = \int_{\mathbb{R}^n} e^{-\mathrm{i}\alpha q} \psi_1^*(q + \beta/2)\psi_2(q - \beta/2) dq \tag{14.466}$$

Now, an elementary computation shows that, on $L^2(\mathbb{R}^{2n})$ with the standard measure we have

$$\parallel W(\psi_1, \psi_2) \parallel^2 = \parallel \psi_1 \parallel^2 \parallel \psi_2 \parallel^2 \tag{14.467}$$

Here are some details

♣Need to clean up some 2π's here... ♣

$$\begin{aligned}
\parallel W(\psi_1, \psi_2) \parallel^2 &= \int_{\mathbb{R}^{2n}} |W(\psi_1, \psi_2)|^2 d^{2n} v \\
&= \int d\alpha d\beta dq_1 dq_2 e^{\mathrm{i}\alpha(q_1 - q_2)} \psi_1(q_1 + \beta/2)\psi_2^*(q_1 - \beta/2)\psi_1^*(q_2 + \beta/2)\psi_2(q_2 - \beta/2) \\
&= \int dq d\beta \psi_1^*(q + \beta/2)\psi_1(q + \beta/2)\psi_2^*(q - \beta/2)\psi_2(q - \beta/2) \\
&= \parallel \psi_1 \parallel^2 \parallel \psi_2 \parallel^2
\end{aligned} \tag{14.468}$$

Now with the key result (14.467) we can show that $\mathcal{H}$ is irreducible. [155] Suppose that $\mathcal{H}_0 \subset \mathcal{H}$ is preserved preserved by the Heisenberg group. Suppose there is a vector $\psi_\perp \notin \mathcal{H}_0$. WLOG we can take $\psi_\perp$ to be perpendicular to $\mathcal{H}_0$ (hence the notation). But then,

$$W(\psi, \psi_\perp)(v) = \langle s(v)\psi, \psi_\perp \rangle = 0 \tag{14.469}$$

for all $v \in \mathbb{R}^{2n}$ and all $\psi \in \mathcal{H}_0$, because $s(v)\psi \in \mathcal{H}_0$. But then by (14.467) we know that $\parallel \psi \parallel^2 \parallel \psi_\perp \parallel^2 = 0$. Therefore either $\psi = 0$ or $\psi_\perp = 0$. If $\mathcal{H}_0$ is not the zero vector space then we can always choose $\psi \neq 0$ and hence $\psi_\perp = 0$. But if $\mathcal{H}_0$ were proper then there would be a nonzero choice for $\psi_\perp$. Therefore, there is no nonzero and proper subspace $\mathcal{H}_0 \subset \mathcal{H}$ preserved by the group action of Heis. Therefore $\mathcal{H}$ is irreducible.

6. *Stone von-Neumann And Fourier* Now let us combine the Stone-von-Neumann theorem with Pontryagin duality. Because $\widehat{\widehat{S}} \cong S$ we can write

$$\mathrm{Heis}(S \times \widehat{S}) \cong \mathrm{Heis}(\widehat{S} \times \widehat{\widehat{S}}) \tag{14.470}$$

[155] See chapter 4 for a thorough discussion of reducible vs. irreducible representations. Briefly - if a representation $\mathcal{H}$ has a nonzero and proper subspace $\mathcal{H}_0$ preserved by the group action then it is said to be *reducible*. A representation which is not reducible is said to be *irreducible*.

so, we could equally well give a unitary representation of the group by taking $\widehat{V} := Fun(\widehat{S} \to \mathbb{C})$ with inner product

$$\langle \hat{\psi}_1, \hat{\psi}_2 \rangle := \int_{\widehat{S}} d\chi \hat{\psi}_1^*(\chi)\hat{\psi}_2(\chi) \tag{14.471}$$

Now we represent translation and multiplication operators by

$$(\hat{T}_{\chi_0}\hat{\psi})(\chi) := \hat{\psi}(\chi_0\chi) \tag{14.472}$$

$$(\hat{M}_{s_0}\hat{\psi})(\chi) := \chi(s_0)\hat{\psi}(\chi) \tag{14.473}$$

and check the commutator function. So, by SvN there must be a unitary isomorphism

$$\mathcal{S} : V \to \widehat{V} \tag{14.474}$$

mapping

$$\begin{aligned} \mathcal{S}T_{s_0}\mathcal{S}^{-1} &= \hat{M}_{s_0} \\ \mathcal{S}M_{\chi_0}\mathcal{S}^{-1} &= \hat{T}_{\chi_0} \end{aligned} \tag{14.475}$$

Indeed there is: It is the Fourier transform:

$$\psi \mapsto \hat{\psi}(\chi) := \int_S \chi(s)^*\psi(s)ds \tag{14.476}$$

Moreover, $\mathcal{S}$ is an isometry:

$$\langle \psi_1, \psi_2 \rangle_{L^2(S)} = \langle \hat{\psi}_1, \hat{\psi}_2 \rangle_{L^2(\widehat{S})} \tag{14.477}$$

a result known as either the *Plancherel theorem* or the *Parseval theorem.* [156] Note that this is equivalent to the relations:

$$\int_{\widehat{S}} \chi(s_1)^*\chi(s_2)d\chi = \delta_S(s_1 - s_2) \tag{14.478}$$

$$\int_S \chi_1(s)^*\chi_2(s)ds = \delta_{\widehat{S}}(\chi_1 - \chi_2) \tag{14.479}$$

These in turn can be viewed as the orthogonality relations for the matrix elements of irreducible representations of the group. For a general compact group the matrix elements of irreducible representations satisfy orthogonality relations. See Chapter 4. These generalize to suitable noncompact groups, and the above relations are an example of that generalization.

Exercise *Bimultiplicative cocycle*

[156] The original statements by Plancherel and Parseval concerned special cases and the two terms are not consistently used in the literature.

a.) Check that (14.450) satisfies the cocycle relation.

b.) Show that, in fact, (14.450) is bimultiplicative.

Exercise *Irreducibility Of The Stone-von Neumann Representation Of* Heis$(S \times \widehat{S})$

Generalize the proof of irreducibility for $S = \mathbb{R}^n$ to other locally compact Abelian groups. [157]

Exercise *The Poisson Summation Formula*

a.) Write out the orthogonality relations (14.478) and (14.479) explicitly for the important special cases of locally compact groups we have discussed.

b.) Show, in particular, that if $\Gamma \subset \mathbb{R}^n$ is an embedded lattice that the relation implies

$$\sum_{\gamma\in\Gamma} e^{-2\pi i k\cdot\gamma} = \sum_{\gamma^\vee\in\Gamma^\vee} \delta_{\mathbb{R}^n}(\gamma^\vee - k) \tag{14.480}$$

which in turn implies the Poisson summation formula.

14.5.8 Some More Examples Of Heisenberg Extensions

For this section the reader might wish to consult section [**** 2.1 *** ?] of chapter two for the definition of a ring. The reader won't lose much by taking $R = \mathbb{Z}$ or $R = \mathbb{Z}/N\mathbb{Z}$ with abelian group structure $+$ and extra multiplication structure $\bar{n}_1\bar{n}_2 = \overline{n_1 n_2}$.

Example 1: Suppose R is a commutative ring with identity. Then we can consider the group of 3×3 matrices over R of the form

$$M(a,b,c) := \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \tag{14.481}$$

The multiplication law is easily worked out to be

$$M(a,b,c)M(a',b',c') = M(a+a', b+b', c+c'+ab') \tag{14.482}$$

Therefore, if we define Heis$(R \times R)$ to be the group of matrices $M(a,b,c)$ and take

$$\pi : M(a,b,c) \to (a,b) \tag{14.483}$$

[157] *Answer* For the general case define the Wigner function as the function $W(\psi_1,\psi_2) : S \times \widehat{S} \to \mathbb{C}$ by $W(\psi_1,\psi_2)(s,\chi) := \langle T_s M_\chi \psi_1, \psi_2\rangle$. Show that (14.467) continues to hold. You will need to use the orthogonality relation for characters.

and

$$\iota : c \mapsto M(0,0,c) \tag{14.484}$$

we have an extension

$$0 \to R \to \mathrm{Heis}(R \times R) \to R \oplus R \to 0 \tag{14.485}$$

with cocycle $f((a,b),(a',b')) = ab'$. Note that we are writing our Abelian group R additively so the cocycle identity becomes

$$f(v_1,v_2) + f(v_1+v_2,v_3) = f(v_1,v_2+v_3) + f(v_2,v_3) \tag{14.486}$$

where $v = (a,b) \in \mathbb{R} \oplus \mathbb{R}$. In this additive notation the commutator function is

$$\kappa((a,b),(a',b')) = ab' - a'b \tag{14.487}$$

In the literature one will sometimes find the above class of groups defined as the "Heisenberg groups." It is a special case of what we have defined as general Heisenberg groups.

As a special case of the above construction let us take $R = \mathbb{Z}/n\mathbb{Z}$. We will now show that we recover the group $\mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n)$ discussed in section 10.2 in the context of a particle on a discrete approximation to a circle.

First consider $\mathbb{Z}_n$ written additively. So if $a \in \mathbb{Z}$, then $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is just $\bar{a} = a + n\mathbb{Z}$ is the coset. Then we define

$$U = \begin{pmatrix} \bar{1} & \bar{1} & 0 \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad V = \begin{pmatrix} \bar{1} & 0 & 0 \\ 0 & \bar{1} & \bar{1} \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad q = \begin{pmatrix} \bar{1} & 0 & \bar{1} \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \tag{14.488}$$

We easily check that for $a \in \mathbb{Z}$,

$$U^a = \begin{pmatrix} \bar{1} & \bar{a} & 0 \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad V^a = \begin{pmatrix} \bar{1} & 0 & 0 \\ 0 & \bar{1} & \bar{a} \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad q^a = \begin{pmatrix} \bar{1} & 0 & \bar{a} \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \tag{14.489}$$

so

$$U^n = V^n = q^n = 1 \tag{14.490}$$

Moreover:

$$UV = qVU \qquad qU = Uq \qquad qV = Vq \tag{14.491}$$

Thus we obtain the presentation:

$$\mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n) = \langle U, V, q | U^n = V^n = q^n = 1, \quad UV = qVU, \quad Uq = qU, \quad Vq = qV \rangle \tag{14.492}$$

we saw before.

A simple and useful generalization of the previous construction is to take any bilinear map $c : R \times R \to \mathcal{Z}$ where $\mathcal{Z}$ is Abelian. Thus $c(a_1 + a_2, b) = c(a_1, b) + c(a_2, b)$ and $c(a, b_1 + b_2) = c(a, b_1) + c(a, b_2)$. Then we can define a central extension

$$0 \to \mathcal{Z} \to \tilde{G} \to R \oplus R \to 0 \tag{14.493}$$

by the law

$$(z_1, (a, b)) \cdot (z_2, (a', b')) = (z_1 + z_2 + c(a, b'), (a + a', b + b')) \tag{14.494}$$

The corresponding group cocycle is $f((a, b), (a', b')) = c(a, b')$. The cocycle relation is satisfied simply by virtue of c being bilinear. It will be a Heisenberg extension if $\kappa : (R \times R) \times (R \times R) \to \mathcal{Z}$ given by $\kappa((a, b), (a', b')) = c(a, b') - c(a', b)$ is nondegenerate. In particular, if we take $\mathcal{Z} = R$ and $c(a, b') = ab'$ using the ring multiplication then we recover (14.481).

Example 2: *Clifford algebra representations and Extra-special groups.* Suppose we have a set of matrices γ_i, $1 \leq i \leq n$ such that

$$\{\gamma_i, \gamma_j\} = 2\delta_{ij} \tag{14.495}$$

Such a set of matrices can indeed be constructed, by taking suitable tensor products of Pauli matrices. They are called "gamma matrices." They form a matrix representation of what is called a *Clifford algebra* and we will study them in more detail and more abstractly in chapter ****. For the moment the reader should be content with the explicit representation: [158]

$$\begin{aligned} \gamma_1 &= \sigma^1 \\ \gamma_2 &= \sigma^2 \end{aligned} \tag{14.496}$$

for $n = 2$,

$$\begin{aligned} \gamma_1 &= \sigma^1 \\ \gamma_2 &= \sigma^2 \\ \gamma_3 &= \sigma^3 \end{aligned} \tag{14.497}$$

for $n = 3$,

$$\begin{aligned} \gamma_1 &= \sigma^1 \otimes \sigma^1 \\ \gamma_2 &= \sigma^1 \otimes \sigma^2 \\ \gamma_3 &= \sigma^1 \otimes \sigma^3 \\ \gamma_4 &= \sigma^2 \otimes 1 \end{aligned} \tag{14.498}$$

for $n = 4$,

$$\begin{aligned} \gamma_1 &= \sigma^1 \otimes \sigma^1 \\ \gamma_2 &= \sigma^1 \otimes \sigma^2 \\ \gamma_3 &= \sigma^1 \otimes \sigma^3 \\ \gamma_4 &= \sigma^2 \otimes 1 \\ \gamma_5 &= \sigma^3 \otimes 1 \end{aligned} \tag{14.499}$$

[158] See Chapter 2, section 5.3 for a detailed discussion of tensor product $\otimes$.

for $n = 5$,

$$\begin{aligned}
\gamma_1 &= \sigma^1 \otimes \sigma^1 \otimes \sigma^1 \\
\gamma_2 &= \sigma^1 \otimes \sigma^1 \otimes \sigma^2 \\
\gamma_3 &= \sigma^1 \otimes \sigma^1 \otimes \sigma^3 \\
\gamma_4 &= \sigma^1 \otimes \sigma^2 \otimes 1 \\
\gamma_5 &= \sigma^1 \otimes \sigma^3 \otimes 1 \\
\gamma_6 &= \sigma^2 \otimes 1 \otimes 1
\end{aligned} \tag{14.500}$$

for $n = 6$, and so on. So for the Clifford algebra with n generators we have constructed a representation by $2^{[n/2]} \times 2^{[n/2]}$ matrices.

Of course, the above choice of matrices is far from a unique choice of matrices satisfying the Clifford relations (14.495). If the $\gamma_i \in \mathrm{Mat}_d(\mathbb{C})$ then for any $S \in GL(d, \mathbb{C})$ we can change $\gamma_i \to S\gamma_i S^{-1}$. These give *equivalent* representations of the Clifford algebra. We could also modify $\gamma_i \to \epsilon_i \gamma_i$ where $\epsilon_i \in \{\pm 1\}$ and still get a representation, although it might not be an equivalent one.

For example, note that for $n = 3$

$$\gamma_1\gamma_2\gamma_3 = \mathrm{i}\mathbf{1}_{2\times 2} \tag{14.501}$$

and for $n = 5$

$$\gamma_1 \cdots \gamma_5 = -\mathbf{1}_{4\times 4} \tag{14.502}$$

We cannot change the sign on the RHS by conjugating with S. So in this case we conclude that there are at least two inequivalent representations of the Clifford algebra.

The general story, proved in detail in Chapters 11-12 is that

1. If n is even there is a unique irreducible representation of dimension $d = 2^{n/2}$.
2. If n is odd there are precisely two irreducible representation of dimension $d = 2^{(n-1)/2}$ and they are distinguished by the sign of the "Clifford volume element" $\omega = \gamma_1 \cdots \gamma_n$.

In Chapter 11 these statements, and more are generalized to real Clifford algebras for a quadratic form of any signature,

For $w \in \mathbb{Z}_2^n$ (where we will think of $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ as a ring in this example) we define

$$\gamma(w) := \gamma_1^{w_1} \cdots \gamma_n^{w_n} \tag{14.503}$$

Then

$$\gamma(w)\gamma(w') = \epsilon(w, w')\gamma(w + w') = \kappa(w, w')\gamma(w')\gamma(w) \tag{14.504}$$

where

$$\epsilon(w, w') = (-1)^{\sum_{i>j} w_i w'_j} \tag{14.505}$$

defines a cocycle with commutator function

$$\kappa(w,w') = (-1)^{\sum_{i\neq j} w_i w'_j} \tag{14.506}$$

When is the commutator function κ nondegenerate? We need to consider two cases:

Case 1a $\sum_i w_i = 1 \text{mod } 2$ and there is an i_0 so that $w_{i_0} = 0$. Then $\gamma(w)$ anticommutes with γ_{i_0}.

Case 1b $\sum_i w_i = 1 \text{mod } 2$ and $w_i = 1$ for all i. In this case n must be odd. Then in fact $\gamma_1 \cdots \gamma_n$ commutes with all the γ_i and the commutator function is degenerate.

Case 2. $\sum_i w_i = 0 \bmod 2$ and some $w_{i_0} \neq 0$. Then γ_{i_0} anticommutes with $\gamma(w)$.

We conclude that for the even degree Clifford algebras κ is nondegenerate and the group generated by taking products of the matrices $\pm\gamma(w)$ defined by an irreducible representation in fact defines a Heisenberg extension:

$$1 \to \mathbb{Z}_2 \to \mathcal{E}_{2m} \to \mathbb{Z}_2^{2m} \to 1 \tag{14.507}$$

In finite group theory this group is an example of what is known as an "extra-special group" and is denoted $\mathcal{E}_{2m} = 2_+^{1+2m}$. [159]

In the case when n is odd then in fact the Clifford volume form $\gamma_1 \cdots \gamma_n$ commutes with all the γ_i and the cocycle is degenerate.

Example 3: *Heisenberg Construction Of Nontrivial $U(1)$ Bundle Over Symplectic Tori.* Consider a torus $T := \mathbb{R}^n/\Gamma$ where Γ is an integral lattice. Suppose we have an integral-valued symplectic form on Γ. This is a blinear, anti-symmetric, nondegenerate map:

$$\Omega : \Gamma \times \Gamma \to \mathbb{Z} \tag{14.508}$$

It is shown in the Linear Algebra User's Manual that we can choose an ordered basis $\{\gamma_1, \dots, \gamma_n\}$ for Γ so that the matrix $\Omega(\gamma_i, \gamma_j)$ is of the form

$$\begin{pmatrix} 0 & d_1 \\ -d_1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & d_2 \\ -d_2 & 0 \end{pmatrix} \cdots \tag{14.509}$$

where the d_i are integers. We will assume that Ω is nondegenerate so therefore $n = 2m$ is even and all the integer d_i are nonzero.

If Γ is full rank we can extend Ω to a bilinear antisymmetric form on [160]

$$V = \Gamma \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^{2m}$$

[159] For any prime p an *extra-special group* is a group G that fits in a central extension $1 \to \mathbb{Z}_p \to G \to \mathbb{Z}_p^n \to 1$ where the center is minimal, that is, is isomorphic to $\mathbb{Z}_p$. For example, for $p = 2$ we have seen that both D_4 and Q are extra-special groups. Up to isomorphism there are two such groups, sometimes denoted $p_\pm^{1+n}$.

[160] The symbol $\otimes_{\mathbb{Z}}$ is explained in the Linear Algebra User's Manual. It means we are taking a tensor product of $\mathbb{Z}$-modules, i.e. Abelian groups.

to get an antisymmetric bilinear form:

$$\Omega : V \times V \to \mathbb{R} \tag{14.510}$$

If all the d_i are nonzero then this is a symplectic form. Using an invertible matrix S we can bring $S^{tr}\Omega S$ to the standard form J. We can define a commutator function on $\mathbb{R}^n$:

$$\kappa(v_1, v_2) = e^{2\pi i \Omega(v_1,v_2)} \tag{14.511}$$

and this defines the isomorphism class of a Heisenberg extension of $V \cong \mathbb{R}^{2m}$. To be concrete our extension is

$$1 \to U(1) \to \mathrm{Heis}(V,\Omega) \to V \to 0 \tag{14.512}$$

where we make the explicit choice of cocycle $f(v_1, v_2) = e^{i\pi\Omega(v_1,v_2)}$. So, $\mathrm{Heis}(V,\Omega)$ is the group of pairs (z, v) with $z \in U(1)$ and $v \in V$ with multiplication:

$$(z_1, v_1) \cdot (z_2, v_2) := (z_1 z_2 e^{i\pi\Omega(v_1,v_2)}, v_1 + v_2) \tag{14.513}$$

We stress that this gives a Heisenberg group and in particular the sequence does not split.

Now consider the pullback of the sequence under the inclusion $\iota : \Gamma \to V$. We claim that the pulled-back sequence splits: Let us try to choose a section

$$s(\gamma) = (\epsilon_\gamma, \gamma) \tag{14.514}$$

then to split the sequence we will need

$$\begin{aligned}(\epsilon_{\gamma_1+\gamma_2}, \gamma_1 + \gamma_2) &= s(\gamma_1 + \gamma_2)\\ &= s(\gamma_1)s(\gamma_2)\\ &= (\epsilon_{\gamma_1}\epsilon_{\gamma_2} e^{i\pi\Omega(\gamma_1,\gamma_2)}, \gamma_1 + \gamma_2)\end{aligned} \tag{14.515}$$

In other words, to split the sequence over Γ we need to find a function $\epsilon : \Gamma \to U(1)$ so that

$$\epsilon_{\gamma_1}\epsilon_{\gamma_2} = e^{-i\pi\Omega(\gamma_1,\gamma_2)}\epsilon_{\gamma_1+\gamma_2} \tag{14.516}$$

It is indeed possible to find such functions. See the exercise.

Since the sequence splits over Γ we consider the Abelian subgroup $s(\Gamma) \subset \tilde{V}$. Then define the quotient space:

$$P(T, \Omega, \epsilon) := \mathrm{Heis}(V,\Omega)/s(\Gamma) \tag{14.517}$$

Explicitly $P(T, \Omega, \epsilon)$ is the quotient $(U(1) \times V)/\Gamma$ with the equivalence relation

$$(z, v) \sim (z, v) \cdot (\epsilon_\gamma, \gamma) = (z\epsilon_\gamma e^{i\pi\Omega(v,\gamma)}, v + \gamma) \tag{14.518}$$

for all $\gamma \in \Gamma$.

Note that there is a continuous map

$$\pi : P(T, \Omega, \epsilon) \to T \tag{14.519}$$

whose fiber is $U(1)$. This space, together with its projection map is an example of a principal $U(1)$ bundle over the torus T: Each fiber is a principal homogeneous space for the group $U(1)$, under the natural action of $U(1)$ on $P(T,\Omega,\epsilon)$. (Since the $U(1)$ is central we can consider it either as a left- or right- action.) Our construction of the bundle depended on a choice of splitting ϵ_γ, but a change of splitting defines isomorphic bundles.

Remarks

1. The above construction comes up, either explicitly or implicitly in discussions of the quantum Hall efect, Chern-Simons theory, and the quantization of p-form gauge theories.

2. Note that while $s(\Gamma)$ is a subgroup of $\mathrm{Heis}(V,\Omega)$ it is <u>not</u> a normal subgroup, so that, while, $P(T,\Omega,\epsilon)$ is a bundle, it is not a group.

3. If we view $\mathrm{Heis}(V,\Omega)$ as a principal $U(1)$ bundle over V then we can construct a very natural connection on this bundle. Parallel transport of the point $(z,v_0)\in P(T,\Omega,\epsilon)$ over a straightline path $\wp_{v_0,w} := \{v_0+tw|0\le t\le 1\}$ in V is defined by left-multiplication by $(1,w)$:

$$U(\wp_{v_0,w}) : (z,v_0)\to (1,w)\cdot(z,v_0) = (ze^{\mathrm{i}\pi\Omega(w,v_0)}, w+v_0) \tag{14.520}$$

Now, if one considers parallel transport around a small square loop starting at v_0 by composing paths

$$\wp_{v,w_1,w_2} := \wp_{v_0,w_1}\star\wp_{v_0+w_1,w_2} * \wp_{v_0+w_1+w_2,-w_1} * \wp_{v_0+w_2,-w_2} \tag{14.521}$$

one obtains the holonomy

$$U(\wp_{v_0,w_1,w_2}) : (z,v_0)\to (ze^{2\pi\mathrm{i}\Omega(w_1,w_2)}, v_0) \tag{14.522}$$

showing that the curvature of this connection is Ω regarded as a 2-form on V. The connection and 2-form descend to the principal $U(1)$ bundle $P(T,\Omega,\epsilon)$. The cohomology class of $[\Omega]$, which is the first Chern class of $P(T,\Omega,\epsilon)$ is characterized by the integers $\vec{d}=(d_1,d_2,\dots)$. A nonzero value of $\vec{d}$ obstructs topological triviality.

Exercise

We illustrated how Q and D_4 are the only two non-Abelian groups that sit in an extension of $\mathbb{Z}_2\times\mathbb{Z}_2$ by $\mathbb{Z}_2$. Which one is the Heisenberg extension?

Exercise *Finite Heisenberg group in multiplicative notation*

It is interesting to look at the Heisenberg extension

$$1 \to \mathbb{Z}_n \to \mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n) \to \mathbb{Z}_n \times \mathbb{Z}_n \to 1 \tag{14.523}$$

where we think of $\mathbb{Z}_n$ as the *multiplicative* group of n^{th} roots of unity. Let $\omega = \exp[2\pi \mathrm{i}/n]$. We distinguish the three $\mathbb{Z}_n$ factors by writing generators as $\omega_1, \omega_2, \omega_3$.

a.) Show that one natural choice of cocycle is:

$$f\left((\omega_1^s, \omega_2^t), (\omega_1^{s'}, \omega_2^{t'})\right) := \omega_3^{st'} \tag{14.524}$$

b.) Compute the commutator function

$$\kappa\left((\omega_1^s, \omega_2^t), (\omega_1^{s'}, \omega_2^{t'})\right) := \omega_3^{st'-ts'} \tag{14.525}$$

c.) Connect to our general theory of extensions by defining $U := (1, (\omega_1, 1))$, $V := (1, (1, \omega_2))$ and computing

$$\begin{aligned} UV &= (f((\omega_1, 1), (1, \omega_2)), (\omega_1, \omega_2)) \\ &= (\omega_3, (\omega_1, \omega_2)) \\ VU &= (f((1, \omega_2), (\omega_1, 1)), (\omega_1, \omega_2)) \\ &= (1, (\omega_1, \omega_2)) \end{aligned} \tag{14.526}$$

or in other words, since the center is generated by $q = (\omega_3, (1,1))$ we can write:

$$UV = qVU \tag{14.527}$$

Exercise *Degenerate Heisenberg extensions*

Suppose $n = km$ is composite and suppose we use the function $c_k(a, b') = kab'$ in defining an extension of $\mathbb{Z}_n \times \mathbb{Z}_n$.

a.) Show that the commutator function is now degenerate.

b.) Show that the center of the central extension is larger than $\mathbb{Z}_n$. Compute it. [161]

While these are not - strictly speaking - Heisenberg extensions people will often refer to them as Heisenberg extensions. We might call them “degenerate Heisenberg extensions.”

Exercise *Constructing The Splitting* (14.516)

[161] *Answer*: The center is generated by q, U^m, V^m and is $\mathbb{Z}_n \times \mathbb{Z}_k \times \mathbb{Z}_k$.

Give an explicit construction of a function $\epsilon : \Gamma \to U(1)$ satisfying (14.516). [162]

Exercise *Different Splittings Give Isomorphic Bundles*

a.) Describe the relation between two splittings of the pullback of the sequence (14.512) to Γ.

b.) Let ϵ_1, ϵ_2 denote two splittings of the pullback of the sequence (14.512) to Γ. Show that the bundles $P(T, \Omega, \epsilon_1)$ with $P(T, \Omega, \epsilon_2)$.

Exercise *Two Dimensions*

a.) Suppose $T = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ with $\mathrm{Im}\tau > 0$. So $\Gamma = \mathbb{Z} + \tau\mathbb{Z}$. Choose

$$\Omega(1, \tau) = -\Omega(\tau, 1) = k \in \mathbb{Z}. \tag{14.529}$$

b.) Show that

$$\Omega(z_1, z_2) = k \frac{\mathrm{Im}(\bar{z}_1 z_2)}{\mathrm{Im}\tau} \tag{14.530}$$

14.5.9 Lagrangian Subgroups And Induced Representations

Let us compare the general Heisenberg extension

$$1 \to \mathcal{Z} \to \tilde{G} \to G \to 0 \tag{14.531}$$

with (14.449) and (14.493) with $\mathcal{Z}$ any subgroup of $U(1)$. The difference from the general case is that in these examples G is explicitly presented as a product of subgroups $G = L \times L'$ where L and L' are *maximal Lagrangian subgroups*. A subgroup $L \subset G$ is said to be a *Lagrangian subgroup* if $\kappa(g_1, g_2) = 1$ for all pairs $(g_1, g_2) \in L$ and similarly for L'.

When discussing Heisenberg groups of the form $\mathrm{Heis}(S \times \widehat{S})$ the group $S \times \widehat{S}$ has two canonical Lagrangian subgroups, namely S and $\widehat{S}$. With the choice of κ we made above these are maximal Lagrangian subgroups.

The case of $G = S \times \widehat{S}$ should be contrasted with other examples where G is $\mathbb{R}^{2n}$ or $\mathbb{Z}_2^{2n}$. These groups certainly can be presented as products of maximal Lagrangian subgroups, but there is no canonical decomposition. Consider, for example the Heisenberg extension $\mathrm{Heis}(\mathbb{Z}_2^{2n})$ constructed using the gamma-matrices. Note that $\mathbb{Z}_2 = \mathbb{F}_2$ is a field, and we can

[162] *Answer*: Choose an ordered basis $\gamma_1, \dots, \gamma_n$ for Γ and define

$$\epsilon_\gamma := e^{-\mathrm{i}\pi \sum_{i<j} n_i n_j \Omega_{ij}} \tag{14.528}$$

where $\gamma = \sum_i n_i \gamma_i$ and $\Omega_{ij} = \Omega(\gamma_i, \gamma_j)$. One can check this satisfies the desired identity. Note that it is crucial that Ω_{ij} and n_i are integral.

consider $\mathbb{F}_2^{2n}$ to be a vector space over $\kappa = \mathbb{F}_2$. We could take L to be any half-dimensional Lagrangian subspace.

In the general situation, with no canonical choice of L one would often like to construct an explicit unitary representation of the Heisenberg group. One way to do this is the following:

Choose a maximal Lagrangian subgroup $L \subset G$. The inverse image $\tilde{L} \subset \tilde{G}$ is a maximal commutative subgroup of $\tilde{G}$.

We now choose a character of $\tilde{L}$ such that $\rho(z,x) = z\rho(x)$. Note that such a character must satisfy

$$\rho(x)\rho(x') = f(x,x')\rho(x+x') \qquad \forall x,x' \in L \tag{14.532}$$

♣This is bad notation, because $\rho(z,x)$ is later used for the full SvN representation. The letter here should be changed and it propagates through the discussion. ♣

Note that f need not be trivial on L, but it does define an Abelian extension $\tilde{L}$ which must therefore be isomorphic to a product $L \times U(1)$, albeit noncanonically. Different choices of ρ are different choices of splitting. Indeed note that (14.532) says that, when restricted to $L \times L$ the cocycle is trivialized by ρ.

The carrier space of our representation will be the space $\mathcal{F}$ of functions $\psi : \tilde{G} \to \mathbb{C}$ such that

$$\psi\left((z,x)(z',x')\right) = \rho(z',x')^{-1}\psi\left(z,x\right) \qquad \forall (z',x') \in \tilde{L} \tag{14.533}$$

Setting $(z',x') = (z^{-1},0)$ we note that equation (14.533) implies $\psi(z,x) = z^{-1}\psi(1,x)$, so defining $\Psi(x) := \psi(1,x)$ we can simplify the description of $\mathcal{F}$ by identifying it with the space of functions $\Psi : G \to \mathbb{C}$ such that:

$$\Psi\left(x + x'\right) = \frac{f(x,x')}{\rho(x')}\Psi(x) \qquad \forall x' \in L. \tag{14.534}$$

If our group is continuous or noncompact we should state an L^2 condition. We take ρ to be a unitary character so that $|\Psi(x)|^2$ descends to a function on G/L and we demand:

$$\int_{G/L} |\Psi(x)|^2 dx < +\infty. \tag{14.535}$$

The group action is simply left-action of $\tilde{G}$ on the functions $\psi(z,x)$. When written in terms of $\Psi(x)$ the representation of $(x,z) \in \tilde{G}$ is:

$$\begin{aligned}(\rho(z,x)\cdot\Psi)(y) &= (\rho(z,x)\cdot\psi)(1,y)\\ &= \psi\left((z,x)^{-1}\cdot(1,y)\right)\\ &= \psi\left((z^{-1}f(x,-x)^{-1}f(-x,y), y-x)\right)\\ &= zf(x,y-x)\Psi(y-x)\end{aligned} \tag{14.536}$$

where in the last line we assumed that f is a normalized cocycle so that $f(0,y) = 1$.

Let us see how we recover the standard Stone-von Neumann representation of $\mathrm{Heis}(S \times \widehat{S})$ from this viewpoint. Let us choose $L = \widehat{S}$. Then the equivariance condition (14.534) becomes

$$\Psi(s,\chi\chi') = \frac{1}{\rho(\chi')}\Psi(s,\chi) \tag{14.537}$$

Now set $\chi' = 1/\chi$ and conclude that

$$\Psi(s, \chi) = \frac{1}{\rho(\chi)} \Psi(s, 1) \tag{14.538}$$

So the dependence on $\chi \in \widehat{S}$ is completely fixed by equivariance. Defining $\tilde{\psi}(s) := \Psi(s, 1)$ we obtain a vector $\tilde{\psi} \in L^2(S)$, and thus if we take $L = \widehat{S}$ then our space of equivariant functions is naturally identified with $L^2(S)$.

We can now work out the representations of

$$\begin{aligned} T_s &= \rho(1, (s, 1)) \\ M_\chi &= \rho(1, (0, \chi)) \end{aligned} \tag{14.539}$$

on $L^2(S)$. Working through the above definitions it should not be surprising that one recovers:

$$\begin{aligned} (T_s \tilde{\psi})(s_0) &= \tilde{\psi}(s_0 - s) \\ (M_\chi \tilde{\psi})(s_0) &= \frac{\rho(\chi)}{\chi(s_0)} \tilde{\psi}(s_0) \end{aligned} \tag{14.540}$$

Example. Consider $\mathbb{F}_2^{2m}$ with $\kappa(w, w') = (-1)^{\sum_{i \neq j} w_i w'_j}$. We can give a Lagrangian decomposition

$$\mathbb{F}_2^{2m} \cong L \oplus N \tag{14.541}$$

in many different ways. For special values of m there are special Lagrangian subspaces provided by classical error correcting codes. A Heisenberg representation can be given by taking V to be the space of functions $\psi : L \to \mathbb{C}$. This has complex dimension 2^m. N can be identified with the group of characters on L since we can set

$$\chi_n(\ell) = \kappa(n, \ell) \tag{14.542}$$

The usual translation and multiplication operators T_ℓ and M_n generate an algebra isomorphic to $Mat_d(\mathbb{C})$. V is also a representation of the Clifford algebra (and hence the extra-special group). So the Clifford representation matrices γ_i can be expressed in terms of these, and vice versa.

Remarks

1. The representation is, geometrically, just the space of L^2-sections of the associated line bundle $\tilde{G} \times_{\tilde{L}} \mathbb{C}$ defined by ρ. The representation is independent of the choice of ρ, and any two choices are related by an automorphism of L given by the restriction of an inner automorphism of $\tilde{G}$.

2. This is an example of an *induced representation*, $Ind_{\tilde{L}}^{\tilde{G}}(\mathbb{C})$ which we will study more systematically in chapter 4, although we will give a brief account here.

3. *Induced Representations.* Let G be a group and H a subgroup. Suppose that $\rho : H \to \mathrm{End}(V)$ is a representation of the *subgroup* H. Then, as we have seen $\mathrm{Map}(G,V)$ is canonically a $G \times H$-space. To keep the notation under control we denote a general function in $\mathrm{Map}(G,V)$ by Ψ. A left-action of $G \times H$ on $\mathrm{Map}(G,V)$ is defined by declaring that for $(g,h) \in G \times H$ and $\Psi \in \mathrm{Map}(G,V)$ the new function $(g,h) \cdot \Psi \in \mathrm{Map}(G,V)$ is the function $G \to V$ defined by:

$$((g,h) \cdot \Psi)(g_0) := \rho(h) \cdot \Psi(g^{-1} g_0 h) \tag{14.543}$$

for all $g_0 \in G$. Now, we can consider the subspace of functions *fixed by the action of* $1 \times H$. That is, we consider the H-equivariant functions which satisfy

$$\boxed{\Psi(gh^{-1}) = \rho(h)\Psi(g)} \tag{14.544}$$

for every $g \in G$ and $h \in H$. Put differently: There are two natural left-actions on $\mathrm{Map}(G,V)$ and we consider the subspace where they are equal. Note that the space of such functions is a linear subspace of $\mathrm{Map}(G,V)$. We will denote it by $\mathrm{Ind}_H^G(V)$. Moreover, it is still a representation of G since if Ψ is equivariant so is $(g,1) \cdot \Psi$.

The subspace $\mathrm{Ind}_H^G(V) \subset \mathrm{Map}(G,V)$ of H-equivariant functions, i.e. functions satisfying (14.544) is called the *induced representation of G, induced by the representation V of the subgroup H*. This is an important construction with a beautiful underlying geometrical interpretation. In some sense all the representations of compact groups follow from this construction, as well as the representations of many important non-compact and infinite-dimensional groups. For this reason it appears in many places in physics.

4. *The geometrical interpretation.* Note that there is a right H-action on the set $G \times V$:

$$\phi_h : (g,v) \mapsto (gh, \rho(h^{-1})v) \tag{14.545}$$

we can therefore form the quotient space of orbits. In this case it is usually denoted $G \times_H V$, but it is just the set of equivalence classes under the above right H-action. There is a natural map

$$\pi : G \times_H V \to G/H \tag{14.546}$$

given by $\pi : [(g,v)] \mapsto gH$. When G, H are Lie groups and ρ is a continous representation the map π is continuous. Moreover, the fiber above any coset gH is the vector space V. We therefore have an example of a vector bundle over G/H with fiber V. The sections of the vector bundle are, by definition, continuous maps

$$s : G/H \to G \times_H V \tag{14.547}$$

that are a right-inverse to π, that is $\pi \circ s = Id_{G/H}$. To construct such a section we have to identify, for each coset gH an equivalence class of the form

$$\{(gh, v(gh)) | h \in H\} \tag{14.548}$$

where $v(gh) \in V$. On the other hand, since this is an equivalence class it must be that $(gh, v(gh)) \sim (g, v(g))$, but we also know that

$$(gh, v(gh)) \sim (ghh^{-1}, \rho(h)v(gh)) = (g, \rho(h)v(gh)) \tag{14.549}$$

by the definition of the right H-action on $G \times V$. We conclude that

$$v(gh) = \rho(h^{-1})v(g) \tag{14.550}$$

This must hold for all $g \in G$, and hence $g \mapsto v(g)$ is an equivariant function: Thus, *the space of sections of the homogeneous vector bundle $\pi : G \times_H V \to G/H$ is canonically identified with the space of H-equivariant functions $G \to V$ satisfying* (14.544).

5. In physics, using the one-dimensional representations of $U(1)$ one can induce to produce all the irreducible representations of $SU(2)$. For example, we have seen that the Pontryagin dual of $U(1)$ is $\mathbb{Z}$ so let ρ_k be the irreducible representation $\rho_k(z) = z^k$ of $U(1)$ where $k \in \mathbb{Z}$. Then for the induced representation we take functions $F : SU(2) \to U(1)$ satisfying the equivariance condition

$$F(\begin{pmatrix} u & -\bar{v} \\ v & \bar{u} \end{pmatrix} \begin{pmatrix} e^{\mathrm{i}\theta} & \\ & e^{-\mathrm{i}\theta} \end{pmatrix}) = e^{-\mathrm{i}k\theta} F(\begin{pmatrix} u & -\bar{v} \\ v & \bar{u} \end{pmatrix}) \tag{14.551}$$

(Where we chose to induce from the diagonal $U(1)$ subgroup of $SU(2)$.) We can abbreviate

$$F(\begin{pmatrix} u & -\bar{v} \\ v & \bar{u} \end{pmatrix}) \Rightarrow F(u, v) \tag{14.552}$$

so we just have

$$F(ue^{\mathrm{i}\theta}, ve^{\mathrm{i}\theta}) = e^{-\mathrm{i}k\theta} F(u, v) \tag{14.553}$$

There is an infinite-dimensional space of such L^2 functions on $SU(2)$, and this construction becomes much more useful if we can cut it down to a finite dimensional representation. Here it turns out to be extremely useful to introduce ideas of algebraic geometry. For us, we will relax the constraint that $|u|^2 + |v|^2 = 1$, and rather consider $(u, v) \in \mathbb{C}^2$ and then consider the subspace of functions are that *holomorphic* in $u, v \in \mathbb{C}$. Holomorphy requires that $-k \geq 0$ and our functions will just be polynomials in u, v. It is convenient to set $-k = 2j \in \mathbb{Z}_+$. The restriction to the holomorphic equivariant functions gives the finite dimensional space $\mathcal{H}_{2j}$ of homogeneous polynomials in u, v of degree $2j$. A basis for $\mathcal{H}_{2j}$ is

♣Need to point them to a more sophisticated discussion with G_c/B. ♣

$$\tilde{f}_m(u, v) := u^{j+m} v^{j-m} \tag{14.554}$$

for $m = -j, -j+1, -j+2, \cdots, j-1, j$. Note that m increases in steps of $+1$ and hence $j \pm m$ is always an integer even though j, m might be half-integer.

Now, for

$$g = \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \qquad |\alpha|^2 + |\beta|^2 = 1 \tag{14.555}$$

we compute the matrix elements for this representation of $SU(2)$ relative to this basis via:

$$\begin{aligned}(g\cdot\tilde{f}_m)(u,v) &:= \tilde{f}_m(\bar{\alpha}u+\bar{\beta}v,-\beta u+\alpha v)\\ &= (\bar{\alpha}u+\bar{\beta}v)^{j+m}(-\beta u+\alpha v)^{j-m}\\ &:= \sum_{m'}\tilde{D}^j_{m'm}(g)\tilde{f}_{m'}\end{aligned} \tag{14.556}$$

Note that for $g=\exp[-\frac{i}{2}\phi\sigma^3]=\exp[\phi J^3]$ (with our unconventional normalization of J^3) we have

$$g\cdot\tilde{f}_m = e^{im\phi}\tilde{f}_m \tag{14.557}$$

More generally, we can derive an explicit formula for the matrix elements $\tilde{D}^j_{m'm}(g)$ as functions on $SU(2)$ by expanding out the two factors in (14.556) using the binomial theorem and collecting terms:

$$\tilde{D}^j_{m'm}(g)=\sum_{s+t=j+m'}\binom{j+m}{s}\binom{j-m}{t}\bar{\alpha}^s\alpha^{j-m-t}\bar{\beta}^{j+m-s}(-\beta)^t \tag{14.558}$$

It turns out that the $\mathcal{H}_{2j}$ give the full set of irreducible representations of $SU(2)$, so the above matrix elements - also known as Wigner functions - form a complete basis for $L^2(SU(2))$. [163] The Wigener functions are related to many important special functions in mathematical physics such as spherical harmonics and associated Legendre polynomials. The representation is also unitarizable and after a suitable rescaling the $\tilde{f}_m$ correspond to the usual ket vectors $|m,j\rangle$ found in quantum mechanics textbooks. For the continuation of this discussion see Chapter 4.

Note that, from the above discussion we can identify the full representation $\mathrm{Ind}_{U(1)}^{SU(2)}(\rho_k)$ with the span of $\tilde{D}^j_{m',-k}$ Therefore $j\geq|k|/2$ and $j+k/2\in\mathbb{Z}$. So

$$\mathrm{Ind}_{U(1)}^{SU(2)}(\rho_k)\cong\oplus_{j\geq|k|/2,j+k/2\in\mathbb{Z}}V_j \tag{14.559}$$

as $SU(2)$ representations.

6. *Representations Of Lorentz, Poincaré, and Affine Euclidean Groups.* Also, the construction of the irreducible unitary representations of Lorentz groups, and affine Euclidean and Poincaré groups proceeds using this method. (That observation goes back to Wigner and Bargmann.) Briefly, for a representation of the Poincaré group one induces from a representation of the translation group (or the translation group semidirect product with a compact rotation group). For a representation of the Lorentz group one considers the homogeneous spaces from orbits of $SO(1,d)$ in momentum space. For example, the mass shell $p^2=m^2$ with $p^0>0$ can be identified with $SO(1,d)/SO(d)$. Then one induces from a representation of $SO(d)$ to produce a unitary representation of $SO(1,d)$.

[163] Warning: The functions $\tilde{D}^j_{m_L m}$ differ from the Wigner functions $D^j_{m_L m}$ by a normalization factor. They are orthogonal, but not orthonormal.

7. Of course, there are many different Lagrangian subgroups of G. For example, if G is a symplectic vector space there will be many different Lagrangian subspaces, all related by the linear action of the symplectic group. Each choice of Lagrangian subspace gives a representation of the Heisenberg group, but they all must be isomorphic, by the Stone-von Neumann-Mackey theorem. This leads to interesting isomorphisms between seemingly different representations and interesting (projective) actions of symplectic groups. These kinds of considerations are central to some simple examples of "duality symmetries" in quantum field theory. We will next investigate how the groups of symplectic automorphisms lift to automorphism groups of Heisenberg groups.

Exercise

Construct explicit Lagrangian subspaces of $\mathbb{F}_2^{2m}$ for small values of m and write out the matrices of the Heisenberg representation. [164]

14.5.10 Automorphisms Of Heisenberg Extensions

In several of our examples above, such as $\mathrm{Heis}(V, \Omega)$ and the extraspecial group we have noted that to define a representation one must make a choice of a Lagrangian subgroup, where κ restricts to 1. On the other hand, we also noted that in some situations there is no natural choice of such a Lagrangian group. There are many such Lagrangian subgroups and they are related by "symplectic automorphisms" of G.

We say that *an automorphism $\alpha \in \mathrm{Aut}(G)$ is symplectic* if it preserves the commutator function:

$$\begin{aligned} \alpha^*\kappa(g_1, g_2) &:= \kappa(\alpha(g_1), \alpha(g_2)) \\ &= \kappa(g_1, g_2) \end{aligned} \tag{14.560}$$

In the first line we defined the general notion of pullback $\kappa \to \alpha^*\kappa$ and the second line is the invariance condition. In physics, such symplectic transformations are relevant to canonical transformations. We can ask whether such automorphisms of "phase space" actually lift to automorphisms of the full Heisenberg group, and then whether and how this lifted group acts on the representations of the Heisenberg group. This would be the "quantum mechanical implementation of symplectic transformations." In this section we will investigate those questions from the group-theoretical viewpoint.

Quite generally, (there is no need for G to be Abelian in this paragraph), if $\pi : \widetilde{G} \to G$ is a homomorphism and $\alpha \in \mathrm{Aut}(G)$ is an automorphism of G we say that α *lifts to an*

[164] *Answer.* Start with $m = 1$. Any vector is isotropic so let L be spanned by $\ell = (1, 0)$ and N spanned by $n = (0, 1)$. Choose a basis for V by taking the delta function supported on basis vector e_i. Then $T_\ell = \sigma^1$ and $M_n = \sigma_3$ relative to this basis.*********** CONTINUE ***********.

automorphism of $\widetilde{G}$ if there is an automorphism $\widetilde{\alpha} \in \mathrm{Aut}(\widetilde{G})$ that completes the diagram:

$$\begin{tikzcd}
\widetilde{G} \arrow[r, "\pi"] \arrow[d, dashed, "\widetilde{\alpha}"] & G \arrow[d, "\alpha"] \\
\widetilde{G} \arrow[r, "\pi"] & G
\end{tikzcd} \tag{14.561}$$

Or, in equations, for every $\alpha \in \mathrm{Aut}(G)$ we seek a corresponding $\widetilde{\alpha} \in \mathrm{Aut}(\widetilde{G})$ such that

$$\pi(\widetilde{\alpha}(\widetilde{g})) = \alpha(\pi(\widetilde{g})) \tag{14.562}$$

for all $\widetilde{g} \in \widetilde{G}$.

Some General Theory [165]

Consider a group extension

$$1 \to A \to \widetilde{G} \to G \to 1 \tag{14.563}$$

where A and G are Abelian and we write the group operations on both A and G additively so $\widetilde{G}$ is the group of pairs (a, g) with group multiplication

$$(a_1, g_1)(a_2, g_2) = (a_1 + a_2 + f(g_1, g_2), g_1 + g_2) \tag{14.564}$$

and $f(g_1, g_2)$ is a cocycle satisfying the additive version of the cocycle identity:

$$f(g_1 + g_2, g_3) + f(g_1, g_2) = f(g_1, g_2 + g_3) + f(g_2, g_3) \tag{14.565}$$

Now suppose $\alpha \in \mathrm{Aut}(G)$. If α preserves the commutator function then we can hope to lift it to an automorphism T_α of $\widetilde{G}$. As explained above, "lifting" means that

$$\pi(T_\alpha(a, g)) = \alpha(\pi(a, g)) = \alpha(g) \ . \tag{14.566}$$

Therefore, T_α must be of the form:

$$T_\alpha(a, g) = (\xi_\alpha(a, g), \alpha(g)) \tag{14.567}$$

where ξ_α is some function $\xi_\alpha : A \times G \to A$. We can write constraints on this function from the requirement that T_α must be an automorphism with the group law defined by the cocycle f. In particular T_α must be a group homomorphism:

$$T_\alpha((a_1, g_1), (a_2, g_2)) = T_\alpha(a_1, g_1) \cdot T_\alpha(a_2, g_2) \tag{14.568}$$

which is true iff

$$\xi_\alpha(a_1 + a_2 + f(g_1, g_2), g_1 + g_2) = \xi_\alpha(a_1, g_1) + \xi_\alpha(a_2, g_2) + f(\alpha(g_1), \alpha(g_2)) \tag{14.569}$$

[165] What follows is an elaboration of the ideas from Appendix A of arXiv:1707.08888. I also got some useful help from Graeme Segal.

Now, specialize this equation by putting $g_1 = 0$ and assuming (WLOG) that we have a normalized cocycle, so that $f(g,0) = f(0,g) = 0$. Then equation (14.569) simplifies to

$$\xi_\alpha(a_1 + a_2, g) = \xi_\alpha(a_1, 0) + \xi_\alpha(a_2, g) \tag{14.570}$$

Putting $a_2 = 0$ in (14.570) we now learn that

$$\xi_\alpha(a, g) = \xi_\alpha(a, 0) + \xi_\alpha(0, g) \tag{14.571}$$

On the other hand, putting $g = 0$ in (14.570) we now learn that $a \mapsto \xi_\alpha(a, 0)$ is just an automorphism of A. Composing lifts of α with such automorphisms is an inherent ambiguity in lifting α. Thus, it is useful to make the simplifying assumption that $\xi_\alpha(a, 0) = a$, since we can always arrange this by composition with an automorphism of A. Therefore we can write equation (14.571) in the general form

$$T_\alpha(a, g) = (a + \tau_\alpha(g), \alpha(g)) \tag{14.572}$$

If we restrict to automorphisms of the type (14.572) then one easily checks that T_α is indeed a group homomorphism iff

$$(\alpha^* f - f)(g_1, g_2) = \tau_\alpha(g_1 + g_2) - \tau_\alpha(g_1) - \tau_\alpha(g_2) \tag{14.573}$$

where

$$\alpha^* f(g_1, g_2) := f(\alpha(g_1), \alpha(g_2)) \tag{14.574}$$

is known as the "pulled-back cocycle." The conceptual meaning of this equation is the following: $\alpha \in \mathrm{Aut}(G)$ is a "symmetry of G." We are asking how badly the cocycle f breaks that symmetry. We say that "f is invariant under pullback" if $\alpha^* f = f$ and in that case we can take $\tau_\alpha = 0$ and we can easily lift the group $\mathrm{Aut}(G)$ to a group of automorphisms of $\widetilde{G}$. The more general condition (14.573) says that the amount by which f is not symmetric under α, that is $\alpha^* f - f$, must be a trivializable cocycle. Put this way, it is clear that the condition is unchanged under shifting f by a coboundary. Indeed, if we change f by a coboundary so

$$\tilde{f}(g_1, g_2) = f(g_1, g_2) + b(g_1 + g_2) - b(g_1) - b(g_2) \tag{14.575}$$

then we can solve (14.573) by taking

$$\tilde{\tau}_\alpha(g) = \tau_\alpha(g) + (\alpha^* b - b)(g) \tag{14.576}$$

so the existence of a solution to (14.573) is gauge invariant. Put more simply, *the cohomology class $[f] \in H^2(G, A)$ must be invariant under the action of α^* on $H^2(G, A)$.*

♣The above paragraph should be said more succinctly. ♣

Thus, in general we cannot lift all automorphisms of G, only those for which (14.573) holds. The set of such automorphisms forms a subgroup of $\mathrm{Aut}(G)$ that we will denote as $\mathrm{Aut}_0(G)$. Note that, in our additive notation we have

$$\kappa(g_1, g_2) = f(g_1, g_2) - f(g_2, g_1) \tag{14.577}$$

which, as mentioned above, is a generalization of a symplectic form. Any automorphism satisfying (14.573) automatically satisfies $\alpha^*(\kappa) = \kappa$ and is therefore a "symplectic automorphism." However, $\mathrm{Aut}_0(G)$ is in general a subgroup of the group of symplectic automorphisms of G. We will give an example with $G = SL(2, \mathbb{Z}_n)$ below.

We now restrict attention to $\alpha \in \mathrm{Aut}_0(G)$. If, in addition

$$\tau_{\alpha_1 \circ \alpha_2}(g) = \tau_{\alpha_1}(\alpha_2(g)) + \tau_{\alpha_2}(g) \tag{14.578}$$

that is,

$$\tau_{\alpha_1 \circ \alpha_2} = \alpha_2^* \tau_{\alpha_1} + \tau_{\alpha_2} \tag{14.579}$$

then in fact $T_{\alpha_1} \circ T_{\alpha_2} = T_{\alpha_1 \circ \alpha_2}$ generate a subgroup of $\mathrm{Aut}(\widetilde{G})$ isomorphic to $\mathrm{Aut}(G)$.

♣ Relate this to equation (14.662)) the condition for a twisted homomorphism $\tau : \mathrm{Aut}(G) \to A$. ♣

In general, even if we can find a solution to (14.573) the criterion (14.579) will not hold. Nevertheless, the automorphisms T_α will generate a subgroup of $\mathrm{Aut}(\widetilde{G})$. To see what subgroup it is we introduce, for $\ell \in \mathrm{Hom}(G, A)$, the automorphism

$$P_\ell(a, g) = (a + \ell(g), g) \tag{14.580}$$

Then we note that

$$T_{\alpha_1} \circ T_{\alpha_2}(a, g) = T_{\alpha_1 \circ \alpha_2} \circ P_{\ell_{\alpha_1, \alpha_2}} \tag{14.581}$$

where

$$\ell_{\alpha_1, \alpha_2}(g) := \tau_{\alpha_1}(\alpha_2(g)) + \tau_{\alpha_2}(g) - \tau_{\alpha_1 \circ \alpha_2}(g) \tag{14.582}$$

A little computation shows that $\ell_{\alpha_1, \alpha_2} \in \mathrm{Hom}(G, A)$ is indeed a homomorphism from G to A. A little more computation reveals

$$\begin{aligned} P_{\ell_1} \circ P_{\ell_2} &= P_{\ell_1 + \ell_2} \\ T_\alpha \circ P_\ell &= P_{\alpha^*(\ell)} \circ T_\alpha \end{aligned} \tag{14.583}$$

Therefore, we can write any word in P's and T's in the form $P_{\ell'} \circ T_{\alpha'}$ for some (ℓ', α'). Altogether, equations (14.581), (14.582), and (14.583) mean that T_α generate a subgroup of $\mathrm{Aut}(\widetilde{G})$. Including all transformations P_ℓ defines a subgroup $\widetilde{\mathrm{Aut}(G)}$ of $\mathrm{Aut}(\widetilde{G})$ which fits in an exact sequence:

$$1 \to \mathrm{Hom}(G, A) \to \widetilde{\mathrm{Aut}(G)} \to \mathrm{Aut}_0(G) \to 1 \tag{14.584}$$

Finally, restoring $\mathrm{Hom}(G, A) \to \mathrm{Hom}(G, A) \rtimes \mathrm{Aut}(A)$ gives the group of (possible) lifts of automorphisms of G to automorphisms of $\tilde{G}$.

Example: $\mathrm{Heis}(\mathbb{R} \oplus \mathbb{R})$

Let us consider the basic example from quantum mechanics based on a phase space $\mathbb{R} \oplus \mathbb{R}$ with symplectic form defined by J. In this case there is a very nice way of thinking of the matrix group $Sp(2, \mathbb{R})$. We note that if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{14.585}$$

then

$$\begin{aligned} A^{tr} J A &= \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= (ad - bc) J \end{aligned} \tag{14.586}$$

Therefore, $A \in Sp(2,\mathbb{R})$ iff $ad - bc = 1$. But this is precisely the condition that defines $SL(2,\mathbb{R})$. Therefore

$$SL(2,\mathbb{R}) = Sp(2,\mathbb{R}) \tag{14.587}$$

are identical as matrix groups. The same argument applies if we replace $\mathbb{R}$ by any ring R. This kind of isomorphism is definitely not true if we consider higher rank groups $SL(n,\mathbb{R})$ and $Sp(2n,\mathbb{R})$.

Now, as we have seen, the section $s(\alpha,\beta) = \exp[\mathrm{i}(\alpha\hat{p} + \beta\hat{q})]$ leads to the choice of section, written additively

$$f\left((\alpha_1,\beta_1),(\alpha_2,\beta_2)\right) = \frac{\hbar}{2}(\alpha_1\beta_2 - \alpha_2\beta_1) \tag{14.588}$$

This is symplectic invariant, so we can take $\tau_\alpha(g) = 0$ in the equation (14.573) and we conclude that the symplectic group acts as a group of automorphisms on the Heisenberg group $\mathrm{Heis}(\mathbb{R}^{2n})$.

It is interesting however, that the symplectic group only acts projectively on the Stone-von-Neumann representation of the Heisenberg group. We now explain this point.

As we will discuss in detail in the chapter on Lie groups, $SL(2,\mathbb{R})$ and $Sp(2,\mathbb{R})$ are examples of Lie groups. It is useful to look at group elements infinitesimally close to the identity matrix. These can be written as

$$A = 1 + \epsilon m + \mathcal{O}(\epsilon^2) \tag{14.589}$$

We learn from the defining equation that

$$\mathrm{Tr}(m) = 0 \tag{14.590}$$

is required to satisfy the defining conditions to order ϵ. (Exercise: Prove this using both the definition of $Sp(2,\mathbb{R})$ and of $SL(2,\mathbb{R})$.)

The infinitesimal group elements are thus characterized by the vector space $\mathfrak{sp}(2,\mathbb{R}) = \mathfrak{sl}(2,\mathbb{R})$, which is the vector space of 2×2 real traceless matrices. These form a Lie algebra with the standard matrix commutator. Generic (but not all) group elements are obtained by exponentiating such matrices. In particular, in a neighborhood of the identity all group elements are obtained by exponentiating elements of the Lie algebra.

A basis of $\mathfrak{sl}(2,\mathbb{R})$ satisfying these relations is

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad h = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad f = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \tag{14.591}$$

(Check the signs carefully!) Compute:

$$[h,e] = -2e \qquad [e,f] = h \qquad [h,f] = +2f \tag{14.592}$$

From this one can in principle multiply exponentiated matrices using the BCH formula.

We now consider the quantum implementation of these operators on $L^2(\mathbb{R})$ with $\rho(e) = \hat{e}$ etc. with:

$$\hat{e} := \frac{\mathrm{i}}{2\hbar}\hat{p}^2 \qquad \hat{h} := \frac{\mathrm{i}}{2\hbar}(\hat{q}\hat{p} + \hat{p}\hat{q}) \qquad \hat{f} := \frac{\mathrm{i}}{2\hbar}\hat{q}^2 \tag{14.593}$$

Now, using the useful identities: [166]

$$\begin{aligned} [AB, CD] &= A[B, C]D + [A, C]BD + CA[B, D] + C[A, D]B \\ &= AC[B, D] + A[B, C]D + C[A, D]B + [A, C]DB \end{aligned} \tag{14.595}$$

we can check that this is indeed a representation:

$$[\hat{h}, \hat{e}] = -2\hat{e} \qquad [\hat{e}, \hat{f}] = \hat{h} \qquad [\hat{h}, \hat{f}] = +2\hat{f} \tag{14.596}$$

However, we have to be careful about exponentiating these operators.

Let us consider the one-parameter subgroup of $SL(2, \mathbb{R})$:

$$\exp[\theta(e + f)] = \cos\theta + \sin\theta \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{14.597}$$

This is in fact a maximal compact subgroup of $SL(2, \mathbb{R})$. (See chapter **** on 2x2 matrix groups.) Note carefully that it has period $\theta \sim \theta + 2\pi$.

The quantum implementation of $e + f$ is just the standard harmonic oscillator Hamiltonian!

$$\hat{e} + \hat{f} = \frac{\mathrm{i}}{2}(\hat{p}^2 + \hat{q}^2) = \mathrm{i}(\bar{a}a + \frac{1}{2}) \tag{14.598}$$

where

$$\begin{aligned} a &= \frac{1}{\sqrt{2}}(q + \mathrm{i}p) \\ \bar{a} &= \frac{1}{\sqrt{2}}(q - \mathrm{i}p) \end{aligned} \tag{14.599}$$

Now, in the Stone-von-Neumann representation $\frac{\mathrm{i}}{2}(\hat{p}^2 + \hat{q}^2)$ has the spectrum $\mathrm{i}(n + \frac{1}{2})$, $n = 0, 1, 2, \dots$. Therefore, the one-parameter subgroup $\exp[\theta(\hat{e} + \hat{f})]$ has period $\theta \sim \theta + 4\pi$. We see that the group generated by $\hat{e}, \hat{f}, \hat{h}$ is at least a double cover of $Sp(2, \mathbb{R})$. In fact, it turns out to be exactly a double cover, and it is known as the *metaplectic group*.

One very interesting aspect of the metaplectic group is that this is a Lie group with no finite-dimensional faithful representation. We now explain that fact, [167] and a few other important things in the following remarks:

Remarks

[166] These identities are very useful, but a bit hard to remember. If you are on a desert island you can easily reconstruct them from the special cases:

$$\begin{aligned} [AB, C] &= A[B, C] + [A, C]B \\ [A, CD] &= C[A, D] + [A, C]D \end{aligned} \tag{14.594}$$

both of which are easy to remember.

[167] Our demonstration of this surprising fact follows the discussion in G. Segal in *Lectures On Lie Groups and Lie Algebras.*

1. *The finite-dimensional representations of* $\mathfrak{sl}(2,\mathbb{R})$. The Lie algebra of the metaplectic group is $\mathfrak{sl}(2,\mathbb{R})$. Any finite dimensional representation of the metaplectic group would give a finite-dimensional representation of the Lie algebra $\mathfrak{sl}(2,\mathbb{R})$ so we should find out what these are. Thus, we are supposing we have a finite-dimensional complex vector space V and linear operators $\rho(e),\rho(f),\rho(h)$ on V satisfying the commutation relations (14.592).

   As shown in Chapter two, any linear operator on a complex vector space has at least one eigenvector. (It might have only one eigenvector.)

   Suppose we choose an eigenvector v of $\rho(h)$ and suppose the eigenvalue is λ. Then, we claim that, so long as $\rho(e)^n v \neq 0$ the vector $\rho(e)^n v$ has eigenvalue $\lambda - 2n$. To prove this apply the general identity

$$[A, B^n] = \sum_{i=0}^{n-1} B^i [A,B] B^{n-1-i} \tag{14.600}$$

   to conclude:

$$[\rho(h), \rho(e)^n] = -2n\rho(e)^n \tag{14.601}$$

   and the result follows. Now, it is general fact of linear algebra that if we nonzero vectors $v_1,\dots,v_n$ with <u>distinct</u> eigenvalues $\lambda_1,\dots,\lambda_n$ for some operator then the $v_1,\dots,v_n$ are linearly independent. (Prove this as an exercise.) Therefore, if $\rho(e)^n v \neq 0$ then the vectors $v,\rho(e)v,\dots,\rho(e)^n v$ are linearly independent. Therefore, since we have a finite-dimensional representation there must be a nonnegative integer n so that $\rho(e)^n v \neq 0$ but $\rho(e)^{n+1} v = 0$. Let us denote $v_0 := \rho(e)^n v$. So $\rho(e)v_0 = 0$ with $\rho(h)v_0 = \lambda_0 v_0$ and $v_0 \neq 0$. Now, using (14.600) again we get:

$$[\rho(h), \rho(f)^k] = 2k\rho(f)^k \tag{14.602}$$

   and therefore

$$\rho(h)(\rho(f)^k v_0) = (\lambda_0 + 2k)\rho(f)^k v_0 \tag{14.603}$$

   By a similar argument to that above, we know that if $\rho(f)^n v_0$ is nonzero then the vectors $v_0,\rho(f)v_0,\dots,\rho(f)^n v_0$ are linearly independent, and therefore there must exist an integer N so that $\rho(f)^N v_0 \neq 0$ but $\rho(f)^{N+1} v_0 = 0$. Therefore

$$[\rho(e), \rho(f)^{N+1}]v_0 = 0 \tag{14.604}$$

   Now, using

$$[\rho(e), \rho(f)^{N+1}] = \sum_{i=0}^{N} \rho(f)^i [\rho(e),\rho(f)] \rho(f)^{N-i} = \sum_{i=0}^{N} \rho(f)^i \rho(h) \rho(f)^{N-i} \tag{14.605}$$

   and applying this identity to v_0 we get:

$$0 = \left(\sum_{i=0}^{N} (\lambda_0 + 2(N-i)) \right) \rho(f)^N v_0 \tag{14.606}$$

But $\rho(f)^N v_0 \neq 0$, by the definition of N so

$$\left(\sum_{i=0}^{N} (\lambda_0 + 2(N-i)) \right) = 0 \tag{14.607}$$

which implies $\lambda_0 = -N$. Thus, we have produced a set of vectors

$$v_0, \rho(f)v_0, \cdots, \rho(f)^N v_0 = v_0, v_1, \dots, v_N \tag{14.608}$$

spanning an $(N{+}1)$-dimensional representation of $\mathfrak{sl}(2,\mathbb{R})$ inside any finite-dimensional representation. If V is irreducible this must be a basis for V.

Since $SL(2,\mathbb{R})$ is noncompact we should worry about the possibility that V is reducible but indecomposable. However, the relation of the Lie algebra to that of the compact group $SU(2)$ explained below rules out that possibility. The representation of $\mathfrak{sl}(2,\mathbb{R})$ is fully reducible into a direct sum of irreducible representations. Note that in this basis the representation matrices are: (See chapter 2 for the proper way to associate a matrix to a linear transformation on a basis with an ordered basis.)

$$\rho(f) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \tag{14.609}$$

$$\rho(h) = \begin{pmatrix} -N & 0 & 0 & \cdots & 0 & 0 \\ 0 & -N+2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -N+4 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & N-2 & 0 \\ 0 & 0 & 0 & \cdots & 0 & N \end{pmatrix} \tag{14.610}$$

One computes $\rho(e)\rho(f)^\ell v_0 = -\ell(N+1-\ell)\rho(f)^{\ell-1}v_0$ so

$$\rho(e) = \begin{pmatrix} 0 & -N & 0 & \cdots & 0 & 0 \\ 0 & 0 & -2(N-1) & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -N \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \tag{14.611}$$

2. *Relation of* $\mathfrak{sl}(2,\mathbb{R})$ *and* $\mathfrak{su}(2)$. The above representation should remind the reader of the spin $j = N/2$ representation of $\mathfrak{su}(2)$. The relation is this: As real Lie algebras $\mathfrak{sl}(2,\mathbb{R})$ and $\mathfrak{su}(2)$ are inequivalent.

However, if we allow ourselves to multiply by complex numbers, that is, if we consider $\mathfrak{sl}(2,\mathbb{R})\otimes\mathbb{C}$ and $\mathfrak{su}(2)\otimes\mathbb{C}$ then we obtain a single Lie algebra $\mathfrak{sl}(2,\mathbb{C})$. If we take $T^j = -\frac{\mathrm{i}}{2}\sigma^j$ as a basis for $\mathfrak{su}(2)$ then, in the complexification, we have

$$\begin{aligned} e &= \mathrm{i}T^1 - T^2 \\ h &= -2\mathrm{i}T^3 \\ f &= -\mathrm{i}T^1 - T^2 \end{aligned} \tag{14.612}$$

3. *Application to the metaplectic group.* Note that $e+f$ corresponds to $\mathrm{i}J^1$. So: In <u>any</u> finite-dimensional complex representation of $\mathfrak{sl}(2,\mathbb{R})$, the operator $\rho(e)+\rho(f)$ is diagonalizable and all the eigenvalues are of the form $\mathrm{i}\ell$, where ℓ is an integer. So $\exp[\theta\rho(e+f)]$ has period $\theta\sim\theta+2\pi$. Therefore no finite dimensional representation of Mpl can be faithful. In particular, Mpl is an example of a Lie group which is not a matrix group: It cannot be embedded as a subgroup of $GL(N,\mathbb{C})$ for any N.

4. It is very interesting to consider the action of the one-parameter family $\exp[\theta(\hat{e}+\hat{f})]$ in the standard "position space" representation $L^2(\mathbb{R})$ with $\hat{p} = -\mathrm{i}\frac{d}{dq}$. Let us compute the integral kernel:

$$\langle x|\exp[\theta(\hat{e}+\hat{f})]|y\rangle \tag{14.613}$$

since

$$\left(e^{\theta(\hat{e}+\hat{f})}\psi\right)(x) = \int_{-\infty}^{+\infty}\langle x|\exp[\theta(\hat{e}+\hat{f})]|y\rangle\psi(y)dy \tag{14.614}$$

Clearly, to evaluate (14.613) we should insert a complete set of eigenstates of the harmonic oscillator Hamiltonian. So we introduce the *Hermite functions*: [168]

$$\psi_n(x) := (2^n n!\sqrt{\pi})^{-1/2}e^{-\frac{x^2}{2}}H_n(x) \qquad n\in\mathbb{Z}_+ \tag{14.615}$$

where $H_n(x)$ is the Hermite polynomial

$$H_n(x) = e^{x^2}\left(-\frac{d}{dx}\right)^n e^{-x^2} \tag{14.616}$$

The Hermite functions $\psi_n(x)$ satisfy

$$\left(-\frac{d^2}{dx^2}+x^2\right)\psi_n = (2n+1)\psi_n \tag{14.617}$$

and we have normalized them so that so that

$$\int_{-\infty}^{+\infty}\psi_n(x)\psi_m(x)dx = \delta_{n,m} \tag{14.618}$$

Now we have

$$\sum_{n=0}^{\infty}u^n\psi_n(x)\psi_m(x) = \frac{1}{\sqrt{\pi(1-u^2)}}\exp\left[-\frac{1-u}{1+u}\left(\frac{x+y}{2}\right)^2 - \frac{1+u}{1-u}\left(\frac{x-y}{2}\right)^2\right] \tag{14.619}$$

[168] What follows here are completely standard facts. We used Wikipedia.

To prove this write

$$H_n(x) = e^{x^2}\left(-\frac{d}{dx}\right)^n e^{-x^2} = e^{x^2}\left(-\frac{d}{dx}\right)^n \left(\frac{1}{\sqrt{4\pi}}\int_{-\infty}^{+\infty} e^{-\frac{1}{4}s^2+\mathrm{i}sx}ds\right) \tag{14.620}$$

Apply this to both $\psi_n(x)$ and $\psi_n(y)$ apply the derivatives, exchange integration and sum and get

$$\begin{aligned}\sum_{n=0}^{\infty} u^n\psi_n(x)\psi_m(x) &= \frac{e^{\frac{1}{2}(x^2+y^2)}}{4\pi^{3/2}}\int dsdte^{-\frac{1}{4}(s^2+t^2)-\frac{1}{2}stu+\mathrm{i}sx+\mathrm{i}ty} \\ &= \frac{1}{\sqrt{\pi(1-u^2)}}\exp\left[-\frac{1-u}{1+u}\left(\frac{x+y}{2}\right)^2 - \frac{1+u}{1-u}\left(\frac{x-y}{2}\right)^2\right]\end{aligned} \tag{14.621}$$

Now we have

$$\langle x|\exp[\theta(\hat{e}+\hat{f})]|y\rangle = e^{\mathrm{i}\theta/2}\sum_{n=0}^{\infty} e^{\mathrm{i}n\theta}\psi_n(x)\psi_n(y) \tag{14.622}$$

so we apply the above identity with $u = e^{\mathrm{i}\theta}$. We should be careful about convergence: The Gaussian integral in (14.621) has quadratic form

$$A = \frac{1}{4}\begin{pmatrix} 1 & u \\ u & 1 \end{pmatrix} \tag{14.623}$$

which has eigenvalues $\frac{1}{4}(1 \pm u)$. The zero-modes at $u = \pm 1$ indicate a divergent Gaussian. In fact we have

$$\begin{aligned}\sum_{n=0}^{\infty}\psi_n(x)\psi_n(y) &= \delta(x-y) \\ \sum_{n=0}^{\infty}(-1)^n\psi_n(x)\psi_n(y) &= \delta(x+y)\end{aligned} \tag{14.624}$$

The second line follows easily from the first since the parity of $\psi_n(x)$ as a function of x is the parity of n.

The quadratic form A has a positive definite real part for $|u| \le 1$ except for $u = \pm 1$. The values for $|u| > 1$ have to be defined by analytic continuation and there is a branch point at $u = \pm 1$. Note that at $\theta = \pi/2$ we have

$$\langle x|\exp[\frac{\pi}{2}(\hat{e}+\hat{f})]|y\rangle = \frac{e^{\mathrm{i}\pi/4}}{\sqrt{2\pi}}e^{\mathrm{i}xy} \tag{14.625}$$

and we recognize the kernel for the Fourier transform:

$$e^{\frac{\pi}{2}(\hat{e}+\hat{f})}\psi = e^{\mathrm{i}\pi/4}\mathcal{F}(\psi) \tag{14.626}$$

where $\mathcal{F} : L^2(\mathbb{R}) \to L^2(\mathbb{R})$ is the Fourier transform. This is the quantum implementation of the canonical transformation exchanging position and momenta. Note that

$\theta = \pi$ is the square of the Fourier transform (up to a scalar multiplication by i) but this is not a scalar operator on the space of functions. Indeed at $\theta = \pi$ we have

$$\left(e^{\pi(\hat{e}+\hat{f})}\psi\right)(x) = \mathrm{i}\psi(-x) \tag{14.627}$$

The Fourier transform is of order four not order two. Also note that at $\theta = 2\pi$ the operator is just multiplication by -1.

5. We note that there are beautiful general formulae for expectation value operators defined by exponentiating general quadratic forms in the $\hat{p}_i$ and $\hat{q}^i$, or, equivalently in a's and $a^\dagger$'s. This is useful when working with coherent states and squeezed states. But it is best presented in the Bargmann or geometric quantization formalism. ♣say more? ♣

Exercise

a.) Check that, for 2×2 matrices the condition $\mathrm{Tr}(m) = 0$ is identical to the condition $(mJ)^{tr} = mJ$.

b.) Show that for any $n \times n$ matrix, the infinitesimal version of the condition $\det A = 1$ is that $A = 1 + \epsilon m + \mathcal{O}(\epsilon^2)$ with $\mathrm{Tr}(m) = 0$.

c.) Show that for any $n \times n$ matrix, the infinitesimal version of the condition $A^{tr} J A = J$ is that $A = 1 + \epsilon m + \mathcal{O}(\epsilon^2)$ with $(mJ)^{tr} = mJ$.

d.) Show that the conditions $\mathrm{Tr}(m) = 0$ and $(mJ)^{tr} = mJ$ are inequivalent different for $n > 2$.

♣Following exercise belongs in the Linear Algebra chapter. ♣

Exercise *Linear independence of eigenvectors with distinct eigenvalues*

Suppose a set of nonzero vectors $v_1, \dots, v_n$ are eigenvectors of some operator A with distinct eigenvalues. Show that they are linearly independent. [169]

Exercise $\mathfrak{su}(2)$ *vs.* $\mathfrak{sl}(2,\mathbb{R})$

A basis for the real Lie algebra of 2×2 traceless anti-Hermitian matrices is

$$T^i = -\frac{\mathrm{i}}{2}\sigma^i \qquad i = 1,2,3 \tag{14.628}$$

[169] *Answer*: Suppose $\sum_s c_s v_s = 0$ for some coefficients c_s. Applying powers of A we determine that $\sum c_s \lambda_s^k v_s = 0$. If all the c_s are nonzero then we learn that the matrix the matrix VC must have determinant zero where $V_{ij} = \lambda_i^j$ and C is the diagonal matrix with entries $c_1, \dots, c_n$. If some of the c_s are nonzero then we have a minor of the matrix V times the diagonal matrix of the nonzero c_s. In any case, none of the minors of V_{ij} have zero determinant, provided the λ_i are distinct. Therefore, VC (or the appropriate minor) has nonzero determinant and hence no kernel. So $\{v_s\}$ is a linearly independent set.

with Lie algebra

$$[T^i, T^j] = \epsilon^{ijk} T^k \tag{14.629}$$

Can one make real linear combinations of T^i to produce the generators e, h, f of $\mathfrak{sl}(2, \mathbb{R})$ above?

Exercise *Representation matrices*

a.) Show that if v_0 is the vector used above with $\rho(e)v_0 = 0$ and $\rho(h)v_0 = -Nv_0$ then [170]

$$\rho(e)\rho(f)^{\ell} v_0 = -\ell(N + 1 - \ell)\rho(f)^{\ell-1} v_0 \tag{14.630}$$

b.) Suppose that we choose a highest weight vector v_h so that $\rho(f)w = 0$ and $\rho(h)w = +Nw$. Write the representation matrices in the ordered basis

$$w, \rho(e)w, \dots, \rho(e)^N w \tag{14.631}$$

c.) Put a unitary structure on the vector space V so that $\rho(T^j)$ are anti-Hermitian matrices and relate the above bases to the standard basis $|j, m\rangle$, $m = -N/2, -N/2 + 1, \dots, N/2 - 1, N/2$ appearing in quantum-mechanics textbooks. That is, find a rescaling of the vectors $\rho(f)^k v_0$ so that in the new basis, after defining $\rho(T^i)$ using (14.612) one obtains anti-Hermitian matrices for $\rho(T^i)$.

Example: $SL(2, \mathbb{Z})$ action on $Heis(\mathbb{Z}_n \times \mathbb{Z}_n)$.

Consider again the example of the quantum mechanics of a particle on a discrete approximation to a ring.

1. Because the position is periodic, the momentum is quantized.
2. Because the position is quantizied, the momentum is periodic.

So, the momentum is both periodic and discrete, just like the position. Recall the position operator Q and the momentum operator P both had a spectrum which is given by n^{th} roots of unity.

So there is a symmetry between momentum and position. This is part of a kind of symplectic symmetry in this discrete system related to $SL(2, \mathbb{Z}_n)$. All such matrices arise from reduction modulo n of matrices in $SL(2, \mathbb{Z})$. Recall from Section [**** 8.3 ****] that $SL(2, \mathbb{Z})$ is generated by S and T with relations

$$(ST)^3 = S^2 = -1 \tag{14.632}$$

[170] *Hint*: Use $[\rho(e), \rho(f)^{\ell}] = \sum_{i=0}^{\ell-1} \rho(e)^i [\rho(e), \rho(f)] \rho(e)^{\ell-1-i}$.

Therefore, S and T (reduced modulo n) will generate $SL(2,\mathbb{Z}_n)$, although there will be further relations, such as $T^n = 1$. The $SL(2,\mathbb{Z}_n)$ symmetry plays and important role in string theory and Chern-Simons theory and illustrates nicely some ideas of duality.

We now take the cocycle for Heis$(\mathbb{Z}_n \times \mathbb{Z}_n)$ to be

$$f((a_1,b_1),(a_2,b_2)) = a_1 b_2 \in \mathbb{Z}_n \tag{14.633}$$

so the commutator function is

$$\kappa((a_1,b_1),(a_2,b_2)) = a_1 b_2 - a_2 b_1 = v_1^{tr} J v_2 \tag{14.634}$$

which we can recognize as a symplectic form on $\mathbb{Z}_n \oplus \mathbb{Z}_n$.

Now an important subtlety arises. In general we cannot find an equivalent cocycle so that

$$\tilde{f}((a_1,b_1),(a_2,b_2)) = \frac{1}{2}(a_1 b_2 - a_2 b_1) \tag{14.635}$$

because, in general, we are not allowed to divide by 2 in $\mathbb{Z}_n$. After all, $x = \frac{1}{2}(a_1 b_2 - a_2 b_1)$ should be the solution to $2x = (a_1 b_2 - a_2 b_1)$, but, if n is even, then if x is a solution $x + n/2$ is a different solution, so the expression is ambiguous. If n is odd then 2 is invertible and we can divide by 2. Therefore, it is not obvious if $Sp(2,\mathbb{Z}_n)$ will lift to automorphisms of the finite Heisenberg group.

Consider the transformation:

$$S : (a,b) \to (b,-a) \tag{14.636}$$

This is a symplectic transformation: $S^*\kappa = \kappa$, and it satisfies $S^2 = -1$. Now we compute

$$(S^* f - f)((a_1,b_1),(a_2,b_2)) = -(a_1 b_2 + b_1 a_2) \tag{14.637}$$

Although the cocycle is not invariant under S nevertheless the difference $S^* f - f$ can indeed be trivialized by

$$\tau_S(a,b) = -ab \tag{14.638}$$

Now consider the transformation

$$T : (a,b) \to (a+b,b) \tag{14.639}$$

We compute

$$(T^* f - f)((a_1,b_1),(a_2,b_2)) = b_1 b_2 \tag{14.640}$$

This can be trivialized by

$$\tau_T(a,b) = \frac{1}{2}b^2 \tag{14.641}$$

PROVIDED we are able to divide by 2!! This is possible if n is odd, but not when n is even. Indeed, when $n = 2$ the cocycle $(T^* f - f)$ is not even a trivializable cocycle! (Why not? Apply the triviality test described in [**** Remark 5, section 11.3 ****] above.)

One way to determine the lifted group, and how the group lifts when n is even is the following. Suppose we have any two operators U, V that satisfy

$$UV = e^{2\pi \mathrm{i}\theta} VU \tag{14.642}$$

for some θ (which, at this point, need not even be rational). If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \tag{14.643}$$

then

$$\widetilde{U} := U^a V^c \qquad\qquad \widetilde{V} = U^b V^d \tag{14.644}$$

♣Need to add phases here to get a proper group action. These don't compose properly yet. ♣

also satisfy

$$\widetilde{U}\widetilde{V} = e^{2\pi \mathrm{i}\theta} \widetilde{V}\widetilde{U} \tag{14.645}$$

Now suppose, in addition that $\theta = 1/n$ and $U^n = V^n = 1$. Then we can compute

$$\begin{aligned} \widetilde{U}^n &= e^{-\mathrm{i}\pi\theta n(n-1)ac} = e^{-\mathrm{i}\pi(n-1)ac} \\ \widetilde{V}^n &= e^{-\mathrm{i}\pi\theta n(n-1)bd} = e^{-\mathrm{i}\pi(n-1)bc} \end{aligned} \tag{14.646}$$

Now, when n is odd, the conditions (14.646) place no restriction on A. In that case, the group $SL(2,\mathbb{Z})$ acts on $\mathrm{Heis}(\mathbb{Z}_n \oplus \mathbb{Z}_n)$ as a group of automorphisms, but the normal subgroup

$$\Gamma(n) := \{A \in SL(2,\mathbb{Z}) | A = \mathbf{1} \mathrm{mod} n\} \tag{14.647}$$

acts trivially so that

$$SL(2,\mathbb{Z})/\Gamma(n) \cong SL(2,\mathbb{Z}_n) \tag{14.648}$$

indeed acts as a group of automorphisms.

However, when n is even, we must consider the subgroup of $SL(2,\mathbb{Z})$ with the extra conditions $ac = bd = 0\mathrm{mod}2$. Only this subgroup acts as a group of automorphisms. Again a finite quotient group acts effectively.

Lifting Symplectomorphisms In Geometric Quantization

****

****

TO BE WRITTEN OUT IN DETAIL: A good example of the general problem of lifting automorphisms is to consider a line bundle with connection (L, ∇) over a symplectic manifold such that the curvature of the connection is the symplectic form Ω. Then, in geometric quantization we can attempt to lift the symplectomorphisms which preserve the line bundle with connection. We will see all the above phenomena, and only the "Hamiltonian automorphisms" will lift. For some discussion see section 6 of:

https://arxiv.org/pdf/hep-th/0605200.pdf

IN PARTICULAR EXPLAIN THE RELATION OF $\mathrm{Aut}_0(G)$ to the kernel of a homomorphism $\mathrm{Aut}(G) \to \mathrm{Hom}(G, H^1(G,A))$.

****

****

14.5.11 Coherent State Representations Of Heisenberg Groups: The Bargmann Representation

EXPLAIN BARGMANN REPRESENTATION.

NICE FORMULAE FOR COHERENT STATES AND VEV'S OF EXPONENTIATED QUADRATIC EXPRESSIONS IN OSCILLATORS.

14.5.12 Some Remarks On Chern-Simons Theory

In Chern-Simons theory (and similar topological field theories) it is quite typical for the Wilson line operators to generate finite Heisenberg groups. For example for $U(1)$ Chern-Simons of level k on a torus we have an action

$$S = \frac{k}{4\pi}\int_{\mathbb{R}} dt \int_{T^2} A_1 \partial_t A_2 + \cdots \tag{14.649}$$

so upon quantization $A_2 \sim \frac{4\pi}{k}\frac{\delta}{\delta A_1}$. The consequence is that Wilson lines along the a- and b-cycles generate a finite Heisenberg group with $q = e^{2\pi \mathrm{i}/k}$. The Hilbert space of states is a finite-dimensional irreducible representation of this group.

****

EXPLAIN MORE. THETA FUNCTIONS AND METAPLECTIC REPRESENTATION.

****

14.6 Non-Central Extensions Of A General Group G By An Abelian Group A: Twisted Cohomology

Let us now generalize central extensions to extensions of the form:

$$1 \to A \overset{\iota}{\to} \tilde{G} \overset{\pi}{\to} G \to 1 \tag{14.650}$$

Here G can be any group, not necessarily Abelian. We continue to assume that $N = A$ is Abelian, but now we no longer assume $\iota(A)$ is central in $\tilde{G}$. So we allow for the possibility of non-central extensions by an Abelian group.

Much of our original story goes through, but now the map

$$\omega : G \to \mathrm{Aut}(A) \tag{14.651}$$

of our general discussion (defined in equations (14.12) and (14.14)) is canonically defined and is actually a group homomorphism. As we stressed below (14.14), in general it is not a group homomorphism. There are two ways to understand that:

1. $\tilde{G}$ acts on A by conjugation on the isomorphic image of A in $\tilde{G}$ which, because the sequence is exact, is still a normal subgroup. In equations, we can define
$$\iota(\tilde{\omega}_{\tilde{g}}(a)) := \tilde{g}\iota(a)\tilde{g}^{-1} \tag{14.652}$$
But now $\tilde{\omega}_{\tilde{g}}$ only depends on the equivalence class $[\tilde{g}] \in \tilde{G}/\iota(A)$ beccause
$$(\tilde{g}\iota(a_0))\,\iota(a)\,(\tilde{g}\iota(a_0))^{-1} = \tilde{g}\iota(a)\tilde{g}^{-1} \tag{14.653}$$
so $\tilde{\omega}_{\tilde{g}\iota(a_0)} = \tilde{\omega}_{\tilde{g}}$ and since $\tilde{G}/\iota(A) \cong G$ we can use this to define ω_g. However, from this definition it is clear that $g \mapsto \omega_g$ is a group homomorphism.

2. Or you can just choose a section and define ω_g exactly as in (14.14). To stress the dependence on s we write
$$\iota(\omega_{g,s}(a)) = s(g)\iota(a)s(g)^{-1} \tag{14.654}$$
However, now if we change section so that [171] $\hat{s}(g) = \iota(t(g))s(g)$ is another section then we compute
$$\begin{aligned}\iota\left(\omega_{g,\hat{s}}(a)\right) &:= \{\iota(t(g))s(g)\} \cdot \iota(a) \cdot \{\iota(t(g))s(g)\}^{-1} \\ &= \iota(t(g)) \cdot \iota(\omega_{g,s}(a)) \cdot \iota(t(g))^{-1} \\ &= \iota\left\{t(g) \cdot \omega_{g,s}(a) \cdot (t(g))^{-1}\right\} \\ &= \iota(\omega_{g,s}(a))\end{aligned} \tag{14.655}$$
and since ι is injective $\omega_{g,s}$ is independent of section and we can just denote it as ω_g. Note carefully that only in the very last line did we use the assumption that A is Abelian. We will come back to this when we discuss general extensions in section 14.7.

   Moreover, given a choice of section we can define $f_s(g_1, g_2)$ just as we did in equation (14.90). This definition works for all group extensions:
$$s(g_1)s(g_2) = \iota(f_s(g_1, g_2))s(g_1g_2) \tag{14.656}$$
We can now compute, just as in (14.15):
$$\begin{aligned}\iota\left(\omega_{g_1} \circ \omega_{g_2}(a)\right) &= s(g_1)\iota(\omega_{g_2}(a))s(g_1)^{-1} \\ &= s(g_1)s(g_2)\iota(a)(s(g_1)s(g_2))^{-1} \\ &= \iota(f_s(g_1, g_2)) \cdot \iota(\omega_{g_1g_2}(a)) \cdot \iota(f_s(g_1, g_2))^{-1} \\ &= \iota\left\{f_s(g_1, g_2))\omega_{g_1g_2}(a)f_s(g_1, g_2))^{-1}\right\} \\ &= \iota\left(\omega_{g_1g_2}(a)\right)\end{aligned} \tag{14.657}$$
and again notice that only in the very last line did we use the hypothesis that A is Abelian. Again, since ι is injective, we conclude that $\omega_{g_1} \circ \omega_{g_2} = \omega_{g_1g_2}$ so that the map ω is a group homomorphism.

[171] Note that here the order of the two factors on the RHS matters, since $\iota(A)$ is not necessarily central in $\tilde{G}$

Now, computing $s(g_1)s(g_2)s(g_3)$ in two ways, just as before, we derive the *twisted cocycle relation*:

$$\omega_{g_1}(f_s(g_2, g_3))f_s(g_1, g_2g_3) = f_s(g_1, g_2)f_s(g_1g_2, g_3) \tag{14.658}$$

Conversely, given a homomorphism $\omega : G \to \mathrm{Aut}(A)$ and a twisted cocycle for ω we can define a group law on the set $A \times G$:

$$(a_1, g_1) \cdot (a_2, g_2) = (a_1\omega_{g_1}(a_2)f(g_1, g_2), g_1g_2) \tag{14.659}$$

The reader should check that this really does define a valid group law on the set $A \times G$.

Remark: Note that (14.659) simultaneously generalizes the twisted product of a semidirect product (13.2) and the twisted product of a central extension (14.102).

Now suppose that we change section from s to $\hat{s}(g) := \iota(t(g))s(g)$ using some arbitrary function $t : G \to A$. Then one can compute that the new cocycle is related to the old one by

$$f_{\hat{s}}(g_1, g_2) = t(g_1)\omega_{g_1}(t(g_2))f_s(g_1, g_2)t(g_1g_2)^{-1} \tag{14.660}$$

Note that since A is Abelian the order of the factors on the RHS do not matter, but in the analogous formula for general extensions, equation (14.761) below, the order definitely does matter.

We say two different twisted cocycles are related by a twisted coboundary if they are related as in (14.660) for some function $t : G \to A$. One can check that if f is a twisted cocycle and we define f' as in (14.660) then f' is also a twisted cocycle. We again have an equivalence relation and we define the *twisted cohomology group* $H^{2+\omega}(G, A)$ to be the abelian group of equivalence classes. It is again an Abelian group, as in the untwisted case, as one shows by a similar argument.

The analog of the main theorem of section 14.3 above is:

Theorem: Let $\omega : G \to \mathrm{Aut}(A)$ be a fixed group homomorphism. Denote the set of isomorphism classes of extensions of the form

$$1 \to A \to \tilde{G} \to G \to 1 \tag{14.661}$$

which induce ω by $\mathrm{Ext}^{\omega}(G, A)$. Then the set $\mathrm{Ext}^{\omega}(G, A)$ is in 1-1 correspondence with the twisted cohomology group $H^{2+\omega}(G, A)$.

The proof is very similar to the untwisted case and we will skip it. Now the trivial element of the Abelian group $H^{2+\omega}(G, A)$ corresponds to the semidirect product determined by ω.

Now we can observe an interesting phenomenon which happens often in cohomology theory: Suppose that a twisted cocyle f is trivializable so that $[f] = 0$. Then our group extension is equivalent to a semidirect product. Nevertheless, the sequence (14.650) can be split in many different ways: There are many distinct trivializations and the different trivializations have meaning. Equivalently, there are many different coboundary transformations that preserve the trivial cocycle. A glance at (14.660) reveals that this will happen when

$$t(g_1 g_2) = t(g_1)\omega_{g_1}(t(g_2)) \tag{14.662}$$

This is known as a *twisted homomorphism*. Of course, in the case that $\omega : G \to \mathrm{Aut}(A)$ takes every $g \in G$ to the identity automorphism of $\mathrm{Aut}(A)$ (that is, the identity element of $\mathrm{Aut}(A)$, the condition specializes to the definition of a homomorphism.

For the later discussion of group cohomology is useful:

A 1-cochain $t \in C^1(G,A)$ is simply a map $t : G \to A$.

A twisted homomorphism is also known as a *twisted one-cocycle*. That is, a 1-cocycle $t \in Z^{1+\omega}(G,A)$ with twisting ω is a 1-cochain that satisfies (14.662).

To define group cohomology $H^{1+\omega}(G,A)$ we need an appropriate notion of equivalence of one-cocycles. This is motivated by noting that if $s : G \to \tilde{G}$ is a section that is also a homomorphism (that is, a splitting) then for any $a \in A$ we can produce a new splitting

$$\tilde{s}(g) = \iota(a)s(g)\iota(a)^{-1} \tag{14.663}$$

This corresponds to the change of section $\tilde{s}(g) = \iota(t(g))s(g)$ where the function $t(g)$ is:

$$t(g) = t_a(g) := a\omega_g(a)^{-1} \quad . \tag{14.664}$$

To check this you write

$$\begin{aligned} \tilde{s}(g) &= \iota(a)s(g)\iota(a)^{-1} \\ &= \iota(a)\cdot\left(s(g)\iota(a)^{-1}s(g)^{-1}\right)\cdot s(g) \\ &= \iota(a)\cdot\left(\iota(\omega_g(a^{-1}))\right)\cdot s(g) \\ &= \left(\iota(a\omega_g(a^{-1}))\right)\cdot s(g) \end{aligned} \tag{14.665}$$

One easily checks that if t is a one-cocycle, then $t \cdot t_a$ is also a one-cocycle. So, in defining the cohomology group $H^{1+\omega}(G,A)$ we use the equivalence relation $t \sim t'$ if there exists an a so that $t = t' t_a$.

Theorem: When the sequence (14.650) splits, that is, when the cohomology class of the twisted cocycle is trivial $[f] = 0$, then the inequivalent splittings are in one-one correspondence with the inequivalent trivializations of a trivializable cocycle, and these are in one-one correspondence with the cohomology group $H^{1+\omega}(G,A)$.

Example 1: Consider the sequence associated with the Euclidean group

$$0 \to \mathbb{R}^d \xrightarrow{\iota} \mathrm{Euc}(d) \xrightarrow{\pi} O(d) \to 1 \tag{14.666}$$

Recall that if $v \in \mathbb{R}^d$ then $\iota(v) = T_v$ is the translation operator on affine space $\mathbb{A}^d$. We have $T_v(p) = p+v$. As we saw in (13.76) and (13.77) and the discussion preceding that exercise, for any $p \in \mathbb{A}^d$ we have a section $R \mapsto s_p(R) \in \mathrm{Euc}(d)$ where $s_p(R)$ is the transformation that takes

$$s_p(R) : p + v \mapsto p + Rv \tag{14.667}$$

In other words, we define rotation-reflections by choosing p as the origin. Then from

$$T_{\omega_R(v_0)} = s_p(R) T_{v_0} s_p(R)^{-1} \tag{14.668}$$

we compute that

$$\omega_R(v_0) = R v_0 \tag{14.669}$$

thus $\omega_R \in \mathrm{Aut}(\mathbb{R}^d)$, and indeed $R \mapsto \omega_R$ is a group homomorphism. If we have two difference sections $s_{p'}$ and s_p then

$$s_{p'}(R) = T_{t(R)} s_p(R) \tag{14.670}$$

where

$$t(R) = (1 - R)(p' - p) = (1 - R)w \tag{14.671}$$

where we have put $p' = p + w$, $w \in \mathbb{R}^d$.

Note that One easily checks that for fixed $w \in \mathbb{R}^d$

$$R \mapsto t(R) := (1 - R)w \tag{14.672}$$

is indeed a twisted homomorphism $O(d) \to \mathbb{R}^d$. (It is not a homomorphism.) However, one also checks that it is of the form $t_w(R) = w - \omega_R(w)$, so it is a trivial one-cocycle: All the splittings are equivalent in the sense defined above.

Example 2: Now restrict the sequence (14.666) to

$$0 \to \mathbb{Z}^d \to G \to \{1, \sigma\} \to 1 \tag{14.673}$$

where $\{1, \sigma\} \subset O(d)$ is a subgroup isomorphic to $\mathbb{Z}_2$ with $\sigma = -\mathbf{1}_{d\times d}$. Then $\omega : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}^d)$ is inherited from ω_R in (14.666) and $\omega_\sigma(\vec{n}) = -\vec{n}$. Now the sequence splits and the most general possible splitting is $s_{\vec{n}_0}$ where $s_{\vec{n}_0}(1) = \{0|\mathbf{1}\}$ and

$$s_{\vec{n}_0}(\sigma) = \{\vec{n}_0|\sigma\} \tag{14.674}$$

for some $\vec{n}_0 \in \mathbb{Z}^d$. Indeed one checks $s_{\vec{n}_0}(\sigma)^2 = 1$. Now for $\vec{a} \in \mathbb{R}^d$ we have

$$t_{\vec{a}}(\sigma) = \vec{a} - \omega_\sigma(\vec{a}) = 2\vec{a} \in 2\mathbb{Z}^d \tag{14.675}$$

So not all splittings are equivalent! The equivalent ones have $\vec{n}_0 - \vec{n}_0' \in 2\mathbb{Z}^d$. Therefore

$$H^{1+\omega}(\mathbb{Z}_2, \mathbb{Z}^d) \cong \mathbb{Z}^d / 2\mathbb{Z}^d \cong (\mathbb{Z}_2)^d \tag{14.676}$$

Remarks

1. Different trivializations of something trivializable can have physical meaning. In the discussion on crystallographic groups below the different trivializations are related to a choice of origin for rotation-reflection symmetries of the crystal.

2. An analogy to bundle theory might help some readers: Let G be a compact Lie group. Then the isomorphism classes of principal G-bundles over S^3 are in 1-1 correspondence with $\pi_2(G)$ and a theorem states that $\pi_2(G) = 0$ for all compact Lie groups. Therefore, every principal G-bundle over S^3 is trivializable. Distinct trivializations differ by maps $t : S^3 \to G$ and the set of inequivalent trivializations is classified by $\pi_3(G)$, which is, in general nontrivial. This can have physical meaning. For example, in Yang-Mills theory in $3 + 1$ dimensions on $S^3 \times \mathbb{R}$ the principal G-bundle on space S^3 is trivializable. But if there is an instanton between two time slices then the trivialization jumps by an element of $\pi_3(G)$.

Exercise *Due diligence*

Derive equation (14.658) and show that if we change f by a coboundary using (14.660) then indeed we produce another twisted cocycle.

Exercise

Suppose that a twisted cocycle $f(g_1, g_2)$ can be trivialized by two different functions $t_1, t_2 : G \to A$. Show that $t_{12}(g) := t_1(g)/t_2(g)$ is a trivialization that preserves the trivial cocycle. That is, show that t_{12} is a twisted 1-cocycle.

14.6.1 Crystallographic Groups

A *crystal* is a subset of affine space $C \subset \mathbb{A}^d$ that is invariant under translations by a lattice $L \subset \mathbb{R}^d$ (actually, that's an embedded lattice). As an example, see Figure 30. Then restricting the exact sequence of the Euclidean group (equation (14.666) above) to the subgroup $G(C) \subset \mathrm{Euc}(d)$ of those transformations that preserve C we have an exact sequence

$$1 \to L(C) \to G(C) \to P(C) \to 1 \tag{14.677}$$

where $P(C) \cong G(C)/L(C)$ is a subgroup of $O(d)$ known as the *point group of the crystal.*

Remark: In solid state physics when the sequence (14.677) does not split the crystallographic group $G(C)$ is said to be *nonsymmorphic.*

Example 1: Take $C = \mathbb{Z} \amalg (\mathbb{Z} + \delta) \subset \mathbb{R}$ where $0 < \delta < 1$. Then of course $L(C) = \mathbb{Z}$ acts by translations, preserving the crystal. But note that it is also true that

$$\begin{aligned} \{\delta|\sigma\} &: n \mapsto \delta - n = -n + \delta \\ &: n + \delta \mapsto \delta - (n + \delta) = -n \end{aligned} \tag{14.678}$$

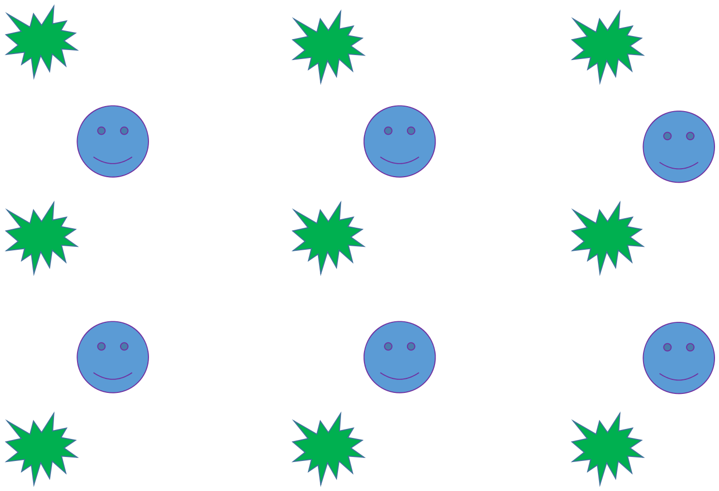

Figure 30: A portion of a crystal in the two-dimensional plane.

where $\sigma \in O(1)$ is the reflection around 0, $\sigma : x \to -x$ in $\mathbb{R}$. The transformation $\{\delta|\sigma\}$ maps $\mathbb{Z}$ to $\mathbb{Z} + \delta$ and $\mathbb{Z} + \delta$ to $\mathbb{Z}$ so that the whole crystal is preserved. Since $O(1) = \mathbb{Z}_2$, this is all we can do. We thus find that $G(C)$ fits in a sequence

$$0 \to L(C) \cong \mathbb{Z} \to G(C) \to O(1) \cong \mathbb{Z}_2 \to 1 \tag{14.679}$$

But we can split this sequence by choosing a section $s(\sigma) = \{\delta| - 1\}$. Note that

$$\{\delta|\sigma\} \cdot \{\delta|\sigma\} = \{0|1\} \tag{14.680}$$

so $s : O(1) \to G(C)$ is a homomorphism. Another way of thinking about this is that $s(\sigma)$ is just reflection, not around the origin, but around the point $\frac{1}{2}\delta$. So, by a shift of origin for defining our rotation-inversion group $O(1)$ we just have reflections and integer translations. In any case we can recognize $G(C)$ as the infinite dihedral group.

Example 2: More generally, consider a lattice $L \subset \mathbb{R}^d$ and a generic vector $\vec{\delta} \in \mathbb{R}^d$. Consider the crystal

$$C = L \amalg (L + \vec{\delta}) \tag{14.681}$$

If L and $\vec{\delta}$ are generic then the point group is just $\mathbb{Z}_2$ generated by $-1 \in O(d)$. Denoting the action of -1 on $\mathbb{R}^d$ by σ we can lift this to the involution

$$\{\vec{\delta}|\sigma\} \in G(C) \tag{14.682}$$

which exchanges L with $(L+\vec{\delta})$. This group is symmorphic (because $\{\vec{\delta}|\sigma\}$ is an involution). In fact, this operation is just inversion about the new origin $\frac{1}{2}\vec{\delta}$:

$$\{\vec{\delta}|\sigma\} : \frac{1}{2}\vec{\delta}+\vec{y} \to \frac{1}{2}\vec{\delta}-\vec{y} \tag{14.683}$$

♣NEED TO HAVE A FIGURE HERE. THIS WOULD HELP. ♣

Example 3: For another very similar example consider

$$C = L \amalg (L+\vec{\delta}) \subset \mathbb{R}^2 \tag{14.684}$$

where

$$L = a_1\mathbb{Z} \oplus a_2\mathbb{Z} \subset \mathbb{R}^2 \tag{14.685}$$

As we have just discussed, for generic a_1, a_2 and $\vec{\delta}$ the symmetry group will be isomorphic to the semidirect product $\mathbb{Z}^2 \rtimes \mathbb{Z}_2$.

However, now let $0 < \delta < \frac{1}{2}$ and specialize $\vec{\delta}$ to $\vec{\delta} = (\delta a_1, \frac{1}{2}a_2)$. Then the crystal has more symmetry and in particular the point group is enhanced from $\mathbb{Z}_2$ to $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$$1 \to \mathbb{Z}^2 \to G(C) \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \tag{14.686}$$

To see this let σ_1, σ_2 be generators of $\mathbb{Z}_2 \times \mathbb{Z}_2$ acting by reflection around the x_2 and x_1 axes, respectively. Then the operations:

$$\hat{\sigma}_1 : (x_1, x_2) \mapsto \vec{\delta} + (-x_1, x_2) \tag{14.687}$$

$$\hat{\sigma}_2 : (x_1, x_2) \mapsto (x_1, -x_2) \tag{14.688}$$

are symmetries of the crystal $G(C)$. In Seitz notation (or rather, its improvement - see equations (13.33) and (13.34) above) we have:

$$\hat{\sigma}_1 = \{\vec{\delta}| \begin{pmatrix} -1 & \\ & 1 \end{pmatrix} \} \tag{14.689}$$

$$\hat{\sigma}_2 = \{0| \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \} \tag{14.690}$$

Now, we can define a section $s(\sigma_1) = \hat{\sigma}_1$ and $s(\sigma_2) = \hat{\sigma}_2$. Note that the square of the lift

$$\hat{\sigma}_1^2 = \{(0, a_2)|1\} \tag{14.691}$$

is a nontrivial translation. Thus $\sigma_i \to \hat{\sigma}_i$ is *not* a splitting. Moreover, $\hat{\sigma}_1$ does not have finite order. Therefore, it cannot be in a discrete group of rotations about any point!

Just because we chose a section that wasn't a splitting doesn't mean that a splitting doesn't actually exist. Here is how we can prove that in fact no splitting exists: The most general section is of the form

$$s(\sigma_1) = \{\vec{\delta}+\vec{v}|\sigma_1\} \tag{14.692}$$

where $\vec{v} = (n_1 a_1, n_2 a_2) \in L$ where $n_1, n_2 \in \mathbb{Z}$. Now consider the square:

$$s(\sigma_1)^2 = \{(0, a_2(1 + 2n_2)|1\}. \tag{14.693}$$

Since $n_2 \in \mathbb{Z}$ there is no lifting that makes this an involution. Therefore, there is no section. Therefore the sequence (14.686) does not split.

Example 4: It is interesting to see what happens to the previous example when $a_1 = a_2 = a$ and we take $\delta = a(\frac{1}{2}, \frac{1}{2})$. Then, clearly

$$C = L \amalg (L + \vec{\delta}) \subset \mathbb{R}^2 \tag{14.694}$$

has a point group symmetry D_4. So this becomes a symmorphic crystal. In fact, this is just a square lattice in disguise! We can take basis vectors δ and $R(\pi/2)\delta$.

****

NEED TO RELATE THE ABOVE FACTS MORE DIRECTLY TO THE PREVIOUS DISCUSSION OF GROUP COHOMOLOGY. SHOULD DO MORE ON CASE WHERE THE SEQUENCE SPLITS BUT THERE ARE INEQUIVALENT SPLITTINGS: PROBABLY A good example is Zincblend structure with tetrahedral symmetry. For example GaAs has this structure. There are two tetrahedra around the Ga and As but they are rotated.

****

Exercise

Why does the argument of example 3 fail in the special case of example 4? [172]

Exercise *Honeycomb*

Consider a honeycomb crystal in the plane. Discuss the crystal group, the point group, and decide if it is symmorphic or not.

♣Need to provide answer in a footnote ♣

14.6.2 Time Reversal

A good example of a physical situation in which it is useful to know about how twisted cocycles define non-central extensions is when there are anti-unitary symmetries in a quantum mechanical system. A typical example where this happens is when there is a time-orientation-reversing symmetry. In this case there is a homomorphism

$$\tau : G \to \{\pm 1\} \cong \mathbb{Z}_2 \tag{14.695}$$

[172] *Answer*: The wrong step is in equation (14.692). When δ takes the special form $\frac{1}{2}(a, a)$ this is not the most general lifting. One has now translation symmetry by multiples of $\vec{\delta}$, so there is an obvious lifting of σ_1.

telling us whether the symmetry $g \in G$ preserves or reverses the orientation of time.

In quantum mechanics it is often (but not always! - see below) the case that time-reversal is implemented as an anti-unitary operator (see Chapter 2 below for a precise definition of this term) and therefore when looking at the way the symmetry is implemented quantum mechanically we should consider the nontrivial automorphism of $U(1)$ defined by complex conjugation.

Recall that

$$\mathrm{Aut}(U(1)) \cong \mathrm{Out}(U(1)) \cong \mathbb{Z}_2 \tag{14.696}$$

and the nontrivial element of $\mathrm{Aut}(U(1)$ is the automorphism $z \to z^* = z^{-1}$.

So, when working with a symmetry group G that includes time-orientation-reversing symmetries we will need to consider the group homomorphism

$$\omega : G \to \mathrm{Aut}(U(1)) \tag{14.697}$$

where:

$$\omega(g)(z) = \begin{cases} z & \tau(g) = +1 \\ z^{-1} & \tau(g) = -1 \end{cases} \tag{14.698}$$

Example 1. The simplest example is where we have a symmetry group $G = \mathbb{Z}_2$ interpreted as time reversal. It will be convenient to denote $M_2 = \{1, \bar{T}\}$, with $\bar{T}^2 = 1$. Of course, $M_2 \cong \mathbb{Z}_2$. In quantum mechanics the representation of $\bar{T}$ will be an operator $\rho(T) := \tilde{T}$ on the Hilbert space and we will get a possibly twisted central extension of M_2. Let $\omega : M_2 \to \mathrm{Aut}(U(1))$. There are two possibilities: $\omega(\bar{T}) = 1$ (so the operation is unitary) and $\omega(\bar{T})$ is the complex conjugation automorphism (so the operation is anti-unitary). Assuming the anti-unitary case is the relevant one, so that ω is the nontrivial homomorphis $M_2 \to \mathrm{Aut}(U(1))$ (both are isomorphic to $\mathbb{Z}_2$ so ω is just the identity homomorphism of $\mathbb{Z}_2$) we need the group cohomology:

$$H^{2+\omega}(\mathbb{Z}_2, U(1)) = \mathbb{Z}_2 \tag{14.699}$$

To prove this we look at the twisted cocycle identity. Exactly the same arguments as in Remark 5 of section 14.3 show that we can choose a gauge with $f(g,1) = f(1,g) = 1$ for all g. This leaves only $f(\bar{T}, \bar{T})$ to be determined. Now, the twisted cocycle relation for the case $g_1 = g_2 = g_3 = \bar{T}$ says that

$$f(\bar{T}, \bar{T})^* = \omega_{\bar{T}}(f(\bar{T}, \bar{T})) = f(\bar{T}, \bar{T}) \tag{14.700}$$

and since $f(\bar{T}, \bar{T}) \in U(1)$ this means $f(\bar{T}, \bar{T}) \in \{\pm 1\}$. We need to check that we can't gauge $f(\bar{T}, \bar{T})$ to one using a twisted coboundary relation. That relation says that we can gauge f to

$$\tilde{f}(\bar{T}, \bar{T}) = t(\bar{T}) \omega_{\bar{T}}(t(\bar{T})) f(\bar{T}, \bar{T}) / t(1) \tag{14.701}$$

Now $t(1) = 1$ since we want to preserve the gauge $f(g,1) = f(1,g) = 1$ and $t(\bar{T})\omega_{\bar{T}}(t(\bar{T})) = |t(\bar{T})|^2 = 1$ so $f(\bar{T}, \bar{T})$ is gauge invariant.

(Note that $\bar{T}$ is an involution so our old criterion from Remark 5 of section 14.3 would ask us to find a square root of $f(\bar{T},\bar{T}) = -1$. Indeed such a square root exists, it is $\pm\mathrm{i}$, but our old criterion no longer applies because we are in the twisted case.)

So, choosing ω to be the nontrivial homomorphism $M_2 \to \mathrm{Aut}(U(1))$ there are two extensions:

$$\begin{tikzcd} 1 \arrow[r] & U(1) \arrow[r] & M_2^{\pm} \arrow[r, "\tilde{\pi}"] & M_2 \arrow[r] & 1 \end{tikzcd} \tag{14.702}$$

Let us write these out more explicitly:

Choose a lift $\tilde{T}$ of $\bar{T}$. Then $\pi(\tilde{T}^2) = 1$, so $\tilde{T}^2 = z \in U(1)$. But, then

$$\tilde{T}z = \tilde{T}\tilde{T}^2 = \tilde{T}^2\tilde{T} = z\tilde{T} \tag{14.703}$$

On the other hand, since we take $\omega(\bar{T})$ to be the nontrivial automorphism of $U(1)$ then

$$\tilde{T}z = z^{-1}\tilde{T} \tag{14.704}$$

Therefore $z^2 = 1$, so $z = \pm 1$, and therefore $\tilde{T}^2 = \pm 1$. Thus the two groups are

$$M_2^{\pm} = \{z\tilde{T} | z\tilde{T} = \tilde{T}z^{-1} \qquad \& \qquad \tilde{T}^2 = \pm 1\} \tag{14.705}$$

These possibilities are really distinct: If $\tilde{T}'$ is another lift of $\bar{T}$ then $\tilde{T}' = \mu\tilde{T}$ for some $\mu \in U(1)$ and so

$$(\tilde{T}')^2 = (\mu\tilde{T})^2 = \mu\bar{\mu}\tilde{T}^2 = \tilde{T}^2 \tag{14.706}$$

So the sign of the square of the lift of the time-reversing symmetry is an invariant.

The extension corresponding to the identity element of $H^{2+\omega}(\mathbb{Z}_2, U(1))$ is the semidirect product. This is just $O(2)$, using $SO(2) \cong U(1)$:

$$O(2) = SO(2) \rtimes \mathbb{Z}_2 \tag{14.707}$$

But the nontrivial extension is a new group for us. It double-covers $O(2)$ and is known as $\mathrm{Pin}^-(2)$. Indeed we can define homomorphisms

$$\pi^{\pm} : M_2^{\pm} \to O(2) \tag{14.708}$$

where $\pi^{\pm}(\tilde{T}) = P \in O(2)$ and $\pi^{\pm}(z = e^{\mathrm{i}\alpha}) = R(2\alpha)$. Note that $-1 = e^{\mathrm{i}\pi} \mapsto R(e^{2\mathrm{i}\pi}) = +\mathbf{1}$. In $\mathrm{Pin}^+(2)$ the double cover of a reflection, $\tilde{T} = (\pi^+)^{-1}(P)$, squares to one. In $\mathrm{Pin}^-(2)$ the double cover of a reflection, $\tilde{T} = (\pi^-)^{-1}(P)$ squares to -1.

Remark: In QM textbooks it is shown that if we write Schrödinger equation for an electron in a potential with spin-orbit coupling then there is a time-reversal symmetry:

$$(\tilde{T} \cdot \Psi)(\vec{x}, t) = \mathrm{i}\sigma^2(\Psi(\vec{x}, -t)^* \tag{14.709}$$

where here Ψ is a 2-component spinor function of $(\vec{x}, t)$. [173] Note that this implies:

$$\begin{aligned} (\tilde{T}^2 \cdot \Psi)(\vec{x}, t) &= \mathrm{i}\sigma^2 \cdot \Big((\tilde{T} \cdot \Psi)(\vec{x}, -t)\Big)^* \\ &= \mathrm{i}\sigma^2 \cdot \big(\mathrm{i}\sigma^2 \cdot (\Psi(\vec{x}, t))^*\big)^* \\ &= \mathrm{i}\sigma^2\mathrm{i}\sigma^2\Psi(\vec{x}, t) \\ &= -\Psi(\vec{x}, t) \end{aligned} \tag{14.710}$$

[173] This is most elegantly derived from the time-reversal transformation on the Dirac equation.

So, in this example, $\tilde{T}^2 = -1$. More generally, in analogous settings for spin j particles $\tilde{T}^2 = (-1)^{2j}$. See section 14.6.3 below for an explanation. The fact that $\tilde{T}^2 = (-1)^{2j}$ in the spin j representation has a very important consequence known as *Kramer's theorem*: In these situations the energy eigenspaces must have even degeneracy. For if Ψ is an energy eigenstate $H\Psi = E\Psi$ and we have a time-reversal invariant system then $\tilde{T} \cdot \Psi$ is also an energy eigenstate. We can prove that it is linearly independent of Ψ as follows: Suppose to the contrary that

$$\tilde{T} \cdot \Psi = z\Psi \tag{14.711}$$

for some complex number z. Then act with $\tilde{T}$ again and use the fact that it is anti-unitary and squares to -1:

$$-\Psi = z^* \tilde{T} \cdot \Psi \tag{14.712}$$

but this implies that $z = -1/z^*$ which implies $|z|^2 = -1$, which is impossible. Therefore, (14.711) is impossible. Therefore Ψ and $\tilde{T} \cdot \Psi$ are independent energy eigenstates. A slight generalization of the argument shows that the dimension of the energy eigenspace must be even. A more conceptual way of understanding this is that the energy eigenspace must be a quaternionic vector space because we have an anti-linear operator on it that squares to -1. See the discussion of real, complex, and quaternionic vector spaces in Chapter 2 below.

Example 2: In general a system can have time-orientation reversing symmetries but the simple transformation $t \to -t$ is not a symmetry. Rather, it must be accompanied by other transformations so that the symmetry group is <u>not</u> of the simple form $G = G_0 \times \mathbb{Z}_2$ where G_0 is a group of time-orientation-preserving symmetries. (Such a structure is often assumed in the literature.) As a simple example consider a crystal

$$C = \left(\mathbb{Z}^2 + (\delta_1, \delta_2)\right) \amalg \left(\mathbb{Z}^2 + (-\delta_2, \delta_1)\right) \amalg \left(\mathbb{Z}^2 + (-\delta_1, -\delta_2)\right) \amalg \left(\mathbb{Z}^2 + (\delta_2, -\delta_1)\right) \tag{14.713}$$

where $\vec{\delta}$ is generic so, as we saw above we have a symmorphic crystal with $P(C) \cong D_4$. The action of D_4 is just given by rotation around the origin $\{0|R(\frac{\pi}{2})\}$ which we will denote by R and reflection, say, in the y-axis, which we will denote by P. So $R^4 = 1$, $P^2 = 1$, and $PRP = R^{-1}$. We have

$$G(C) = \mathbb{Z}^2 \rtimes D_4 \tag{14.714}$$

But now suppose there is a dipole moment, or spin S. We model this with a set of two elements $\mathcal{S} = \{S, -S\}$ for dipole moment up and down and now our crystal with spin is a subset of $\mathbb{R}^2 \times \mathcal{S}$. This subset is of the form

$$\widehat{C} = \widehat{C}_+ \amalg \widehat{C}_- \tag{14.715}$$

with

$$\widehat{C}_+ = \left(\mathbb{Z}^2 + (\delta_1, \delta_2)\right) \times \{S\} \amalg \left(\mathbb{Z}^2 + (-\delta_1, -\delta_2)\right) \times \{S\} \tag{14.716}$$

but a spin $-S$ on points of the complementary sub-crystal

$$\widehat{C}_- = \left(\mathbb{Z}^2 + (-\delta_2, \delta_1)\right) \times \{-S\} \amalg \left(\mathbb{Z}^2 + (\delta_2, -\delta_1)\right) \times \{-S\} \tag{14.717}$$

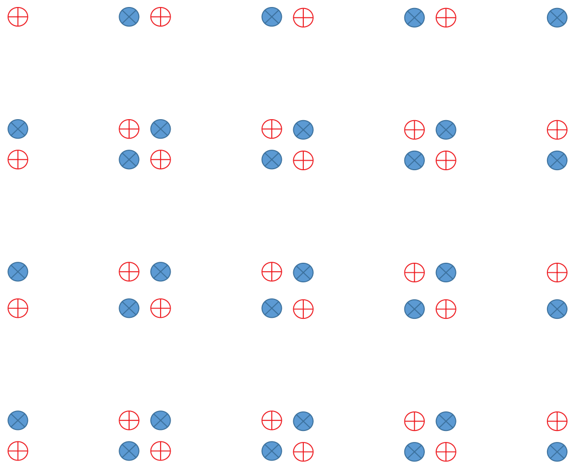

Figure 31: In this figure the blue crosses represent an atom with a local magnetic moment pointing up while the red crosses represent an atom with a local magnetic moment pointing down. The magnetic point group is isomorphic to D_4 but the homomorphism τ to $\mathbb{Z}_2$ has a kernel $\mathbb{Z}_2 \times \mathbb{Z}_2$ (generated by π rotation around a lattice point together with a reflection in a diagonal). Since D_4 is nonabelian the sequence $1 \to \widehat{P}_0 \to \widehat{P} \xrightarrow{\tau} \mathbb{Z}_2 \to 1$ plainly does not split.

Now let $\mathbb{Z}_2 = \{1, \sigma\}$ act on $\mathbb{R}^2 \times \mathcal{S}$ by acting trivially on the first factor and $\sigma : S \to -S$ on the second factor. Now reversal of time orientation exchanges S with $-S$. So the symmetries of the crystal with dipole is a subgroup $\widehat{G(C)} \subset \mathrm{Euc}(2) \times \mathbb{Z}_2$ known as the *magnetic crystallographic group*. The subgroup of translations by the lattice is still a normal subgroup and the quotient by the lattice of translations is the *magnetic point group*. In the present example:

$$0 \to \mathbb{Z}^2 \to \widehat{G(C)} \to \widehat{P(C)} \to 1 \qquad (14.718)$$

The elements in $\widehat{P(C)}$ are

$$\{(1,1), (R,\sigma), (R^2,1), (R^3,\sigma), (P,\sigma), (PR,1), (PR^2,\sigma), (PR^3,1)\} \qquad (14.719)$$

This magnetic point group is isomorphic to D_4 but the time reversal homomorphism takes $\tau(R,\sigma) = -1$ and $\tau(P,\sigma) = -1$ so that we have

$$1 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to \widehat{P(C)} \xrightarrow{\tau} \mathbb{Z}_2 \to 1 \qquad (14.720)$$

The induced automorphism on $\mathbb{Z}_2 \times \mathbb{Z}_2$ is trivial so clearly this sequence does not split, since $\widehat{P(C)} \cong D_4$ is nonabelian.

Remarks:

1. With the possible exception of exotic situations in which quantum gravity is important, physics takes place in space and time. Except in unusual situations associated with nontrivial gravitational fields we can assume our spacetime is time-orientable. Then, any physical symmetry group G must be equipped with a homomorphism

   $$\tau : G \to \mathbb{Z}_2 \tag{14.721}$$

   telling us whether the symmetry operations preserve or reverse the orientation of time. That is $\tau(g) = +1$ are symmetries which preserve the orientation of time while $\tau(g) = -1$ are symmetries which reverse it.

   Now, suppose that G is a symmetry of a quantum system. Then Wigner's theorem gives G another grading $\phi : G \to \mathbb{Z}_2$, telling us whether the operator $\rho(g)$ implementing the symmetry transformation g on the Hilbert space is unitary or anti-unitary. Thus, on very general grounds, a symmetry of a quantum system should be *bigraded* by a pair of homomorphisms (ϕ, τ), or what is the same, a homomorphism to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   It is natural to ask whether ϕ and τ are related. A natural way to try to relate them is to study the dynamical evolution.

   In quantum mechanics, time evolution is described by unitary evolution of states. That is, there should be a family of unitary operators $U(t_1, t_2)$, strongly continuous in both variables and satisfying composition laws $U(t_1, t_3) = U(t_1, t_2)U(t_2, t_3)$ so that the density matrix ϱ evolves according to:

   $$\varrho(t_1) = U(t_1, t_2)\varrho(t_2)U(t_2, t_1) \tag{14.722}$$

   Let us - for simplicity - make the assumption that our physical system has time-translation invariance so that $U(t_1, t_2) = U(t_1 - t_2)$ is a strongly continuous group of unitary transformations. [174]

   By Stone's theorem, $U(t)$ has a self-adjoint generator H, the Hamiltonian, so that we may write

   $$U(t) = \exp\left(-\frac{it}{\hbar}H\right) \tag{14.723}$$

   ♣There is an obvious generalization of this statement for $U(t_1, t_2)$. Is it proved rigorously somewhere? ♣

   Now, suppose we have a group [175] of operators on the Hilbert space: $\rho : G \to \mathrm{Aut}_{\mathbb{R}}(\mathcal{H})$. We say this group action is a *symmetry of the dynamics* if for all $g \in G$:

   $$\rho(g)U(t)\rho(g)^{-1} = U(\tau(g)t) \tag{14.724}$$

   where $\tau : G \to \mathbb{Z}_2$ is the indicator of time-orientation-reversal.

[174] In the more general case we would need an analog of Stone's theorem to assert that there is a family of self-adjoint operators with $U(t_1, t_2) = \mathrm{Pexp}[-\frac{i}{\hbar}\int_{t_1}^{t_2} H(t')dt']$. Then, the argument we give below would lead to $\rho(g)H(t)\rho(g)^{-1} = \phi(g)\tau(g)H(t)$ for all t.

[175] As explained in the 2012 article of Freed and Moore, this group might be an extension of the original group of quantum symmetries $\bar{\rho} : \bar{G} \to \mathrm{Aut}_{\mathrm{qtm}}(\mathbb{P}\mathcal{H})$.

Now, substituting (14.723) and paying proper attention to ϕ we learn that the condition for a symmetry of the dynamics (14.724) is equivalent to

$$\phi(g)\rho(g)H\rho(g)^{-1} = \tau(g)H \tag{14.725}$$

in other words,

$$\rho(g)H\rho(g)^{-1} = \phi(g)\tau(g)H \tag{14.726}$$

Thus, the answer to our question is that ϕ and τ are *unrelated* in general. We should therefore define a third homomorphism $\chi : G \to \mathbb{Z}_2$

$$\chi(g) := \phi(g)\tau(g) \in \{\pm 1\} \tag{14.727}$$

Note that

$$\phi \cdot \tau \cdot \chi = 1 \tag{14.728}$$

2. It is very unusual for physical systems to have nontrivial homomorphisms χ. That is, it is very unusual to have physical systems with time-orientation-reversing symmetries which are $\mathbb{C}$-linear or time-orientation-preserving symmetries which act $\mathbb{C}$-anti-linearly. But it is not impossible. To see why it is unusual note that:

$$\rho(g)H\rho(g)^{-1} = \chi(g)H \tag{14.729}$$

implies that if any group element has $\chi(g) = -1$ then the spectrum of H must be symmetric around zero. In particular, if the spectrum is bounded below but not above this condition must fail. In many problems, e.g. in the standard Schrödinger problem with potentials which are bounded below, or in relativistic QFT with H bounded below we must have $\chi(g) = 1$ for all g and hence $\phi(g) = \tau(g)$, which is what one reads in virtually every physics textbook: "A symmetry is anti-unitary iff it reverses the orientation of time." Not true, in general.

3. However, there *are* physical examples where $\chi(g)$ can be non-trivial, that is, there can be symmetries which are both anti-unitary and time-orientation preserving. An example are the so-called "particle-hole" symmetries in free fermion systems.

14.6.3 Digression: Clebsch-Gordon Decomposition And $T^2 = (-1)^{2j}$ On Spin j Particles

Above we checked that $T^2 = -1$ on spin 1/2 particles whose wavefunction obeys the usual Schrödinger equation with spin-orbit coupling. The generalization to spin j particles is $T^2 = (-1)^{2j}$.

One simple way to see this is to note that the spin j representation is obtained by decomposing the tensor product of $(2j)$ copies of the spin 1/2 representation. In general we have the very important Clebsch-Gordon decomposition:

$$V(j_1) \otimes V(j_2) \cong V(|j_1 - j_2|) \oplus V(|j_1 - j_2| + 1) \oplus \cdots\cdots \oplus V(j_1 + j_2) \tag{14.730}$$

Note that every representation on the RHS has the same parity of $(-1)^{2j}$. Also note the triangular structure of the Clebsch-Gordon decomposition of $V(\frac{1}{2})^{\otimes n}$ allowing for an inductive proof. Finally $\tilde{T}^2$ on $V(\frac{1}{2})^{\otimes n}$ is just $(-1)^n$, so it is $(-1)^n$ on the highest summand $V(n/2)$.

Let us give a proof of (14.730). We need some general facts about representation theory. See Chapter 4 for full explanations:

First set of general facts:

Denote a representation $\rho : G \to \mathrm{Aut}(V)$ simply by $V(\rho)$. For any finite-dimensional representation $V(\rho)$ of any group G we can definite the *character of the representation*, denoted χ_ρ. It is a function

$$\chi_\rho : G \to \mathbb{C} \tag{14.731}$$

and it is defined by

$$\chi_\rho(g) := \mathrm{Tr}_{V(\rho)}(\rho(g)) \tag{14.732}$$

Some useful general remarks about characters:

1. $\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$
2. $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} \chi_{\rho_2}$
3. $\chi_\rho(h^{-1}gh) = \chi_\rho(g)$ for all $g, h \in G$. In other words, $\chi_\rho(g)$ only depends on g via its conjugacy class. In general, a function $F : G \to \mathbb{C}$ that only depends on conjugacy class, that is, that satisfies $F(h^{-1}gh) = F(g)$ for all $g, h \in G$ is known as a *class function*.
4. If $V(\rho)$ is unitary then $\chi_\rho(g^{-1}) = \chi_\rho(g)^*$.

Second set of general facts:

If G is compact, there is a notion of invariant integration. Given a (reasonable) function $F : G \to \mathbb{C}$ we can define the integral

$$\int_G F(g)[dg] \in \mathbb{C} \tag{14.733}$$

such that, for all $h \in G$:

$$\int_G F(g)[dg] = \int_G F(gh)[dg] = \int_G F(hg)[dg] \tag{14.734}$$

This property is called left- and right-invariance. If we normalize the measure so $\int_G [dg] = 1$ then it is unique. For finite groups,

$$\int_G F(g)[dg] := \frac{1}{|G|} \sum_{g \in G} F(g) \tag{14.735}$$

For $G = U(1)$:

$$\int_G F(g)[dg] := \frac{1}{2\pi} \int_0^{2\pi} F(e^{\mathrm{i}\theta}) d\theta \tag{14.736}$$

For $G = SU(2)$: ♣Need to check ♣

$$\int_G F(g)[dg] := \frac{1}{16\pi^2}\int F(u)\sin^2\theta d\theta d\phi d\psi \tag{14.737}$$

where we use the Euler angle parametrization of $SU(2)$

$$u = e^{i\frac{\phi}{2}\sigma^3}e^{i\frac{\theta}{2}\sigma^1}e^{i\frac{\psi}{2}\sigma^3} \tag{14.738}$$

with range $\phi \sim \phi + 2\pi$, $\psi \sim \psi + 4\pi$, $0 \leq \theta \leq \pi$. A "reasonable function" means one for which the above integrals exist.

A consequence of the existence of invariant integration is that every finite-dimensional representation is equivalent to a unitary representation. This follows because you can use a suitable averaging procedure over the group to make the matrices unitary. Therefore, every finite-dimensional is fully reducible: This follows from the unitarization and finite-dimensionality: If the representation is reducible then the orthogonal complement to an invariant subspace is another invariant subspace. So we may use induction on the dimension of the representation. Therefore, for any representation $V(\rho)$ we can always write:

$$V(\rho) \cong \oplus_i V(\rho_i) \tag{14.739}$$

where each ρ_i is irreducible and the sum on the RHS is finite. It is better to write this as

$$V(\rho) \cong \oplus_\alpha D_\alpha \otimes V(\rho_\alpha) \tag{14.740}$$

where now the ρ_α is a complete set of inequivalent irreducible representations. For a compact group the set of irreducible representations is in a natural way a discrete set. The D_α are degeneracy spaces (which might be zero). This is called an *isotypical decomposition* and one can identify D_α as the space of linear operators $T : V(\rho_\alpha) \to V(\rho)$ that commute with the G action. (Such operators are known as *intertwiners* and the above statement follows from Schur's lemma.)

If G is compact there is a notion of invariant integration of functions on G. In particular, one can normalize the measure so that, on the set of characters of irreducible representations $V(\rho_\alpha)$ we have

$$\int_G \chi_{\rho_{\alpha_1}}(g^{-1})\chi_{\rho_{\alpha_2}}(g)[dg] = \int_G \chi_{\rho_{\alpha_1}}(g)^*\chi_{\rho_{\alpha_2}}(g)[dg] = \delta_{\alpha_1,\alpha_2} \tag{14.741}$$

Putting these facts together it follows that

A representation of a compact group is completely determined, up to equivalence, by its character function.

Now let us apply these general facts to $SU(2)$. For the spin j representation denote the character by χ_j. Every $u \in SU(2)$ is diagonalizable so we can say

$$u \sim u(\theta) := \begin{pmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{pmatrix} \tag{14.742}$$

and parametrize all the conjugacy classes uniquely by $\theta \sim \theta + \pi$. [176] On the other hand,

$$\begin{pmatrix} e^{\mathrm{i}\theta} & \\ & e^{-\mathrm{i}\theta} \end{pmatrix} = \exp[-2\theta\left(-\frac{\mathrm{i}}{2}\sigma^3\right)] \tag{14.743}$$

so, in the standard basis that diagonalizes $T^3 = -\frac{\mathrm{i}}{2}\sigma^3$ we have

$$\rho(u) \sim \mathrm{Diag}\{z^{-2j}, z^{-2j+2}, \dots, z^{2j-2}, z^{2j}\} \tag{14.744}$$

where $z = e^{\mathrm{i}\theta}$. Therefore

$$\chi_j(u) = z^{-2j} + z^{-2j+2} + \cdots + z^{2j-2} + z^{2j} = \frac{z^{2j+1} - z^{-2j-1}}{z - z^{-1}} \tag{14.745}$$

Now, because a representation is uniquely determined by its character we can consider the character of $V(j_1) \otimes V(j_2)$. If we can write this as a linear combination of characters χ_j with nonnegative integer coefficients we can uniquely determine the decomposition into irreps.

Therefore, let's write:

$$\begin{aligned} \chi_{j_1}(z)\chi_{j_2}(z) &= \left(\frac{z^{2j_1+1} - z^{-2j_1-1}}{z - z^{-1}}\right) \cdot \left(\frac{z^{2j_2+1} - z^{-2j_2-1}}{z - z^{-1}}\right) \\ &= \frac{1}{z - z^{-1}}\left(\frac{z^{2j_1+2j_2+2} - z^{2(j_1-j_2)}}{z - z^{-1}} + \frac{z^{-2j_1-2j_2-2} - z^{-2(j_1-j_2)}}{z - z^{-1}}\right) \end{aligned} \tag{14.746}$$

Now, WLOG assume that $j_1 \geq j_2$. Then we use the identity:

$$\frac{z^{a+2} - z^b}{z - z^{-1}} = z^{b+1}\frac{z^{a-b+2} - 1}{z^2 - 1} = z^{b+1} + z^{b+3} + \cdots + z^{a+1} \tag{14.747}$$

for each of the two terms in the sum above, then realize that the two terms are related by $z \to 1/z$ and we directly obtain:

$$\chi_{j_1}\chi_{j_2} = \chi_{j_1+j_2} + \chi_{j_1+j_2-1} + \cdots + \chi_{|j_1-j_2|} \tag{14.748}$$

It is instructive to give a proof using the orthogonality of characters. The properly normalized measure on $SU(2)$ is such that on a class function F we have:

$$\int_{SU(2)} F(u)[du] = \frac{1}{\pi}\int_0^{2\pi} f(\theta)\sin^2\theta d\theta = -\frac{1}{4\pi\mathrm{i}}\oint g(z)(z - z^{-1})^2\frac{dz}{z} \tag{14.749}$$

where

$$f(\theta) = F(\begin{pmatrix} e^{\mathrm{i}\theta} & \\ & e^{-\mathrm{i}\theta} \end{pmatrix}) = g(z) \tag{14.750}$$

with $z = e^{\mathrm{i}\theta}$.

[176] The identification is period π, and not 2π, because $u(-\theta) = vu(\theta)v^{-1}$ where, for example, we can take $v = \mathrm{i}\sigma^1$.

Now one checks directly by contour integration that

$$-\frac{1}{4\pi i}\oint \chi_{j_1}(z)\chi_{j_2}(z)\chi_j(z)(z-z^{-1})^2\frac{dz}{z} = \begin{cases} +1 & |j_1-j_2| \le j \le j_1+j_2 \qquad \& \qquad 2j = 2j_1+2j_2 \mathrm{mod} 2 \\ 0 & \text{else} \end{cases} \tag{14.751}$$

Exercise *Recovering Dimension*

As a nice check of the expression on the far RHS in (14.745) show that the limit $u \to 1$ reproduces the dimension of V_j.

14.7 General Extensions

Let us briefly return to the general extension (14.1). Thus, we are now not assuming that N or Q is abelian. We might ask what happens if we try to continue following the reasoning of section (14.1) in this general case, but now keeping in mind the nice classification of central extensions using group cohomology.

What we showed is that for *any* group extension a choice of a section $s : Q \to G$ automatically gives us two maps:

1. $\omega_s : Q \to \mathrm{Aut}(N)$
2. $f_s : Q \times Q \to N$

These two maps are defined by

$$\iota(\omega_{s,q}(n)) := s(q)\iota(n)s(q)^{-1} \tag{14.752}$$

and

$$s(q_1)s(q_2) := \iota(f_s(q_1,q_2))s(q_1 \cdot q_2) \tag{14.753}$$

respectively.

Now (14.752) defines an element of Aut(N) for fixed s and q, but the map $q \mapsto \omega_{s,q}$ need not be a homomorphism, as we have repeatedly stressed. Rather, using (14.752) and (14.753) we can derive a twisted version of the homomorphism rule:

$$\omega_{s,q_1} \circ \omega_{s,q_2} = I(f_s(q_1,q_2)) \circ \omega_{s,q_1q_2} \tag{14.754}$$

Recall that for $a \in N$, $I(a) \subset \mathrm{Aut}(N)$ denotes the inner automorphism given by conjugation by a. The proof of (14.754) follows exactly the same steps as (14.657), except for the very last line.

Moreover, using (14.753) to relate $s(q_1)s(q_2)s(q_3)$ to $s(q_1q_2q_3)$ in two ways gives a twisted cocycle relation:

$$\omega_{s,q_1}(f_s(q_2,q_3))f_s(q_1,q_2q_3) = f_s(q_1,q_2)f_s(q_1q_2,q_3) \tag{14.755}$$

Note this is the same as (14.658), but unlike that equation now order of the terms is very important since we no longer assume that N is abelian.

To summarize: Given a general extension (14.1) there exist maps (ω_s, f_s), associated with any section s and defined by (14.752) and (14.753). The maps (ω_s, f_s) automatically satisfy the identities (14.754) and (14.755).

We now consider, more generally, functions satisfying identities (14.754) and (14.755). That is, we assume we are given two maps (not necessarily derived from some section):

1. A map $f : Q \times Q \to N$
2. A map $\omega : Q \to \mathrm{Aut}(N)$

And we suppose the data (ω, f) satisfy the two conditions

$$\omega_{q_1} \circ \omega_{q_2} = I(f(q_1, q_2)) \circ \omega_{q_1 q_2} \tag{14.756}$$

$$\omega_{q_1}(f(q_2, q_3))f(q_1, q_2 q_3) = f(q_1, q_2)f(q_1 q_2, q_3) \tag{14.757}$$

then we can construct an extension (14.1) with the multiplication law:

$$(n_1, q_1) \cdot_{f,\omega} (n_2, q_2) := (n_1 \omega_{q_1}(n_2) f(q_1, q_2), q_1 q_2) \tag{14.758}$$

This is very similar to (14.659) but we stress that since N might be nonabelian, the order of the factors in the first entry on the RHS matters!

With a few lines of algebra, using the identities (14.756) and (14.757) one can check the associativity law and the other group axioms. We have already seen this simultaneous generalization of the semidirect product (13.2) and the twisted product of a central extension (14.102) in our discussion of the case where $N = A$ is abelian. (See equation (14.659) above.) The new thing we have now learned is that this is the most general way of putting a group structure on a product $N \times Q$ so that the result fits in an extension of Q by N.

Now, suppose again that we are given a group extension. As we showed, a choice of section s gives us a pair of functions (ω_s, f_s) satisfying (14.756) and (14.757). Any other section $\tilde{s}$ is related to s by a function $t : Q \to N$. Indeed that function t is defined by:

$$\tilde{s}(q) = \iota(t(q))s(q) \tag{14.759}$$

and one easily computes that we now have

$$\omega_{\tilde{s},q} = I(t(q)) \circ \omega_{s,q} \tag{14.760}$$

$$f_{\tilde{s}}(q_1, q_2) = t(q_1)\omega_{s,q_1}(t(q_2)) f_s(q_1, q_2) t(q_1 q_2)^{-1} \tag{14.761}$$

The proof of (14.760) follows exactly the same steps as (14.655). To prove (14.761) we patiently combine the definition (14.759) with the definition (14.753).

♣We also skipped this proof for $N = A$ abelian. Probably should show the steps. ♣

These formulae for how (ω_s, f_s) change as we change the section now motivate the following:

Suppose we are given a pair (ω, f) satisfying (14.756) and (14.757) and an arbitrary function $t : Q \to N$. We can now define a new pair (ω', f') by the equations:

$$\omega'_q = I(t(q)) \circ \omega_q \tag{14.762}$$

$$f'(q_1, q_2) = t(q_1)\omega_{q_1}(t(q_2))f(q_1, q_2)t(q_1 q_2)^{-1} \tag{14.763}$$

Now, with some algebra (DO IT!) one can check that indeed (ω', f') really do satisfy (14.756) and (14.757) as well. Equations (14.762) and (14.763) generalize the coboundary relation (14.97) of central extension theory. Note that the equations relating ω and f back to ω' and f' are of the same form with $t(q) \to t(q)^{-1}$.

The relations (14.762) and (14.763) define an equivalence relation on the set of pairs (ω, f) satisfying (14.756) and (14.757). Moreover, if (ω, f) and (ω', f') are related by (14.762) and (14.763) then we can define a group structure on the set $N \times Q$ in two ways using the equation (14.758) for each pair. Nevertheless, there is a morphism between these two extensions in the sense of (14.4) above where we define

$$\varphi(n, q) := (nt(q)^{-1}, q) \tag{14.764}$$

So, to check this you need to check

$$\varphi((n_1, q_1) \cdot_{f,\omega} (n_2, q_2)) = \varphi(n_1, q_1) \cdot_{f',\omega'} \varphi(n_2, q_2) \tag{14.765}$$

Then note that $\varphi^{-1}(n, q) = (nt(q), q)$ is an inverse morphism of extensions, and hence we have an isomorphism of extensions.

Now we would like to state all this a little more conceptually. The first point to note is that a map $q \mapsto \omega_q \in \mathrm{Aut}(N)$ that satisfies (14.756) in fact canonically defines a homomorphism $\bar{\omega} : Q \to \mathrm{Out}(N)$ of Q into the group of outer automorphisms of N. This homomorphism is defined more conceptually as the unique map that makes the diagram:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota"] \arrow[d, "I"] & G \arrow[r, "\pi"] \arrow[d, "\psi"] & Q \arrow[r] \arrow[d, "\varpi"] & 1 \\
1 \arrow[r] & \mathrm{Inn}(N) \arrow[r] & \mathrm{Aut}(N) \arrow[r] & \mathrm{Out}(N) \arrow[r] & 1
\end{tikzcd} \tag{14.766}$$

Here $I : N \to \mathrm{Inn}(N)$ is the map that takes n to the inner automorphism $I(n) : n' \mapsto nn'n^{-1}$ and ψ is the map from $G \to \mathrm{Aut}(N)$ defined by

$$\iota(\psi(g)(n)) = g\iota(n)g^{-1} \tag{14.767}$$

Now, we can ask the converse question: *Given an arbitrary homomorphism $\bar{\omega} : Q \to \mathrm{Out}(N)$ is there an extension of Q by N that induces it as in* (14.766)*?*

The most obvious thing to try when trying to answer this question is to use $\bar{\omega} : Q \to \mathrm{Out}(N)$ and the pullback construction (14.34) of the canonical exact sequence given by the lower line of (14.766). But this will only give an extension of Q by $\mathrm{Inn}(N)$. Note that $\mathrm{Inn}(N) \cong N/Z(N)$, and so the center of N might cause some trouble. That is in fact what happens: The answer to the above question is, in general, "NO," and the obstruction has to do with the third cohomology group $H^{3+\bar{\omega}}(Q, Z(N))$ where $Z(N)$ is the center of N. See section 14.8.5 below.

But for now, let us suppose we have a choice of $\bar{\omega}$ such that extensions inducing it do exist. What can we say about the set $\mathrm{Ext}^{\bar{\omega}}(Q, N)$ of equivalence classes of such extensions?

To answer this we choose a lifting of the homomorphism, that is, a map $q \mapsto \omega_q \in \mathrm{Aut}(N)$. Now, if we have two extensions both inducing $\bar{\omega}$ and we choose two liftings $\omega_q^{(1)}$ and $\omega_q^{(2)}$ then they will be related by

$$\omega_q^{(1)} = I(t(q)) \circ \omega_q^{(2)} \tag{14.768}$$

for some function $t : Q \to N$. Note, please, that while this equation is formally very similar to (14.760) it is conceptually different. Nothing has been said about the relation of the two extensions, other than that they induce the same $\bar{\omega}$.

Now we try to relate the corresponding functions $f^{(1)}(q_1, q_2)$ and $f^{(2)}(q_1, q_2)$. To do that we compute

$$\begin{aligned}
\omega_{q_1}^{(1)} \circ \omega_{q_2}^{(1)}(n) &= t(q_1)\omega_{q_1}^{(2)}\left(t(q_2)\omega_{q_2}^{(2)}(n)t(q_2)^{-1}\right)t(q_1)^{-1} \\
&= t(q_1)\omega_{q_1}^{(2)}(t(q_2))\left(\omega_{q_1}^{(2)} \circ \omega_{q_2}^{(2)}(n)\right)\omega_{q_2}^{(2)}(t(q_2)^{-1})t(q_1)^{-1} \\
&= t(q_1)\omega_{q_1}^{(2)}(t(q_2))\left(f^{(2)}(q_1, q_2)\omega_{q_1 q_2}^{(2)}(n)f^{(2)}(q_1, q_2)^{-1}\right)\omega_{q_2}^{(2)}(t(q_2)^{-1})t(q_1)^{-1} \\
&= \left\{t(q_1)\omega_{q_1}^{(2)}(t(q_2))f^{(2)}(q_1, q_2)t(q_1q_2)^{-1}\right\} \cdot \omega_{q_1q_2}^{(1)}(n)\left\{t(q_1)\omega_{q_1}^{(2)}(t(q_2))f^{(2)}(q_1, q_2)t(q_1q_2)^{-1}\right\}^{-1} \\
&= \hat{f}^{(2)}(q_1, q_2) \cdot \omega_{q_1q_2}^{(1)}(n)\hat{f}^{(2)}(q_1, q_2)^{-1}
\end{aligned} \tag{14.769}$$

where we define

$$\hat{f}^{(2)}(q_1, q_2) := t(q_1)\omega_{q_1}^{(2)}(t(q_2))f^{(2)}(q_1, q_2)t(q_1q_2)^{-1} \tag{14.770}$$

On the other hand, we know that

$$\omega_{q_1}^{(1)} \circ \omega_{q_2}^{(1)}(n) = f^{(1)}(q_1, q_2)\omega_{q_1q_2}^{(1)}(n)f^{(1)}(q_1, q_2)^{-1} \tag{14.771}$$

Can we conclude that $\hat{f}^{(2)}(q_1, q_2) = f^{(1)}(q_1, q_2)$? Certainly not! Provided $\omega_{q_1q_2}^{(1)}(n)$ is sufficiently generic all we can conclude is that

$$\hat{f}^{(2)}(q_1, q_2) = f^{(1)}(q_1, q_2)\zeta(q_1, q_2) \tag{14.772}$$

for some function $\zeta : Q \times Q \to Z(N)$. These two functions are not necessarily related by a coboundary and the extensions are not necessarily equivalent!

What is true is that if $\hat{f}^{(2)}$ and $f^{(1)}$ satisfy the twisted cocycle relation then $\zeta(q_1, q_2)$ in (14.772) also satisfies the twisted cocycle relation. (This requires a lot of patient algebra....) It follows that

$$\zeta \in Z^{2+\bar{\omega}}(Q, Z(N)) \tag{14.773}$$

Moreover, going the other way, given one extension and corresponding $(\omega^{(1)}, f^{(1)})$, and a $\zeta \in Z^{2+\bar{\omega}}(Q, Z(N))$ we can change f as in (14.772). If $[z] \in H^{2+\bar{\omega}}(Q, Z(N))$ is nontrivial we will in general get a new, nonequivalent extension.

All this is summarized by the theorem:

Theorem: Let $\mathrm{Ext}^{\bar{\omega}}(Q,N)$ be the set of inequivalent extensions of Q by N inducing $\bar{\omega}$. Then either this set it is empty or it is a torsor [177] for $H^{2+\bar{\omega}}(Q,Z(N))$.

****

NEED SOME EXAMPLES HERE. AND NEED SOME MORE INTERESTING EXERCISES.

****

Exercise *Checking the group laws*

Show that (14.758) really defines a group structure.

a.) Check the associativity relation.

b.) What is the identity element? [178]

c.) Check that every element has an inverse.

Exercise

a.) Check that (14.764) really does define a homomorphism of the group laws (14.758) defined by (ω, f) and (ω', f') if (ω', f') is related to (ω, f) by (14.762) and (14.763).

b.) Check that the diagram (14.4) really does commute if we use (14.764).

14.8 Group cohomology in other degrees

Motivations:

a.) The word "cohomology" suggests some underlying chain complexes, so we will show that there is such a formulation.

b.) There has been some discussion of higher degree group cohomology in physics in

1. The theory of anomalies (Faddeev-Shatashvili; Segal; Carey et. al.; Mathai et. al.; ...)

2. Classification of rational conformal field theories (Moore-Seiberg; Dijkgraaf-Vafa-Verlinde-Verlinde; Dijkgraaf-Witten; Kapustin-Saulina)

3. Chern-Simons theory and topological field theory (Dijkgraaf-Witten,...)

4. Condensed matter/topological phases of matter (Kitaev; Wen et. al.; Kapustin et. al.; Freed-Hopkins;....)

[177] A *torsor* X for a group G is a set X with a G-action on it so that given any pair $x, x' \in X$ there is a unique $g \in G$ that maps x to x'. In this chapter we have discussed an important example of a torsor quite extensively: Affine space $\mathbb{A}^d$ is a torsor for $\mathbb{R}^d$ with the natural action of $\mathbb{R}^d$ on $\mathbb{A}^d$ by translation.

[178] *Answer*: $(f(1,1)^{-1}, 1_Q)$.

5. Three-dimensional supersymmetric gauge theory.

Here we will be brief and just give the basic definitions:

14.8.1 Definition

Suppose we are given any group G and an Abelian group A (written additively in this sub-section) and a homomorphism

$$\omega : G \to \mathrm{Aut}(A) \tag{14.774}$$

Definition: An n-cochain is a function $\phi : G^{\times n} \to A$. The space of n-cochains is denoted $C^n(G, A)$. It is also useful to speak of 0-cochains. We interpret a 0-cochain ϕ_0 to be some element $\phi_0 = a \in A$.

Note that $C^n(G, A)$, for $n \geq 0$, is an abelian group using the abelian group structure of A on the values of ϕ, that is: $(\phi_1 + \phi_2)(\vec{g}) := \phi_1(\vec{g}) + \phi_2(\vec{g})$.

Define a group homomorphism: $d : C^n(G, A) \to C^{n+1}(G, A)$

$$\begin{gathered}(d\phi)(g_1, \dots, g_{n+1}) := \omega_{g_1}\left(\phi(g_2, \dots, g_{n+1})\right) \\ -\phi(g_1g_2, g_3, \dots, g_{n+1}) + \phi(g_1, g_2g_3, \dots, g_{n+1}) \pm \cdots + (-1)^n\phi(g_1, \dots, g_{n-1}, g_ng_{n+1}) \\ + (-1)^{n+1}\phi(g_1, \dots, g_n)\end{gathered} \tag{14.775}$$

Then we have, for $n = 0$:

$$(d\phi_0)(g) = \omega_g(a) - a \tag{14.776}$$

For $n = 1$, $n = 2$ and $n = 3$ the formula written out looks like:

$$(d\phi_1)(g_1, g_2) = \omega_{g_1}\left(\phi_1(g_2)\right) - \phi_1(g_1g_2) + \phi_1(g_1) \tag{14.777}$$

$$(d\phi_2)(g_1, g_2, g_3) = \omega_{g_1}\left(\phi_2(g_2, g_3)\right) - \phi_2(g_1g_2, g_3) + \phi_2(g_1, g_2g_3) - \phi_2(g_1, g_2) \tag{14.778}$$

$$(d\phi_3)(g_1, g_2, g_3, g_4) = \omega_{g_1}\left(\phi_3(g_2, g_3, g_4)\right) - \phi_3(g_1g_2, g_3, g_4) + \phi_3(g_1, g_2g_3, g_4) - \phi_3(g_1, g_2, g_3g_4) + \phi_3(g_1, g_2, g_3) \tag{14.779}$$

Next, one can check that for any ϕ, we have the absolutely essential equation:

$$\boxed{d(d\phi) = 0} \tag{14.780}$$

We will give a simple proof of (14.780) below but let us just look at how it works for the lowest degrees: If $\phi_0 = a \in A$ is a 0-cochain then

$$\begin{aligned}(d^2\phi_0)(g_1, g_2) &= \omega_{g_1}(d\phi_0(g_2)) - d\phi_0(g_1 \cdot g_2) + d\phi_0(g_1) \\ &= \omega_{g_1}\left(\omega_{g_2}(a) - a\right) - \left(\omega_{g_1g_2}(a) - a\right) + \left(\omega_{g_1}(a) - a\right) \\ &= \omega_{g_1}(\omega_{g_2}(a)) - \omega_{g_1g_2}(a) \\ &= 0\end{aligned} \tag{14.781}$$

if ϕ_1 is any 1-cochain then we compute:

$$\begin{aligned}(d^2\phi_1)(g_1,g_2,g_3) &= \omega_{g_1}(d\phi_1(g_2,g_3)) - (d\phi_1)(g_1g_2,g_3) + (d\phi_1)(g_1,g_2g_3) - (d\phi_1)(g_1,g_2)\\ &= \omega_{g_1}\left(\omega_{g_2}(\phi_1(g_3)) - \phi_1(g_2g_3) + \phi_1(g_2)\right)\\ &- \left(\omega_{g_1g_2}(\phi_1(g_3)) - \phi_1(g_1g_2g_3) + \phi_1(g_1g_2)\right)\\ &+ \left(\omega_{g_1}(\phi_1(g_2g_3) - \phi_1(g_1g_2g_3) + \phi_1(g_1)\right)\\ &- \left(\omega_{g_1}(\phi_1(g_2)) - \phi_1(g_1g_2) + \phi_1(g_1)\right)\\ &= 0\end{aligned} \tag{14.782}$$

where you can check that all terms cancel in pairs, once you use $\omega_{g_1}\circ\omega_{g_2} = \omega_{g_1g_2}$.

The set of (ω-twisted) n-cocycles is defined to be the subgroup $Z^{n+\omega}(G,A) \subset C^n(G,A)$ of cochains that satisfy $d\phi_n = 0$.

Thanks to (14.780) we can define a subgroup $B^{n+\omega}(G,A) \subset Z^{n+\omega}(G,A)$, called the subgroup of coboundaries:

$$B^{n+\omega}(G,A) := \{\phi_n | \exists \phi_{n-1} \qquad s.t. \qquad d\phi_{n-1} = \phi_n\} \tag{14.783}$$

then, since $d^2 = 0$ we have $B^{n+\omega}(G,A) \subset Z^{n+\omega}(G,A)$.

Then the group cohomology is defined to be the quotient

$$H^{n+\omega}(G,A) = Z^{n+\omega}(G,A)/B^{n+\omega}(G,A) \tag{14.784}$$

Example: Let us take $G = \mathbb{Z}_2 = \{1,\sigma\}$ and $A = \mathbb{Z}$. Recall that

$$\mathrm{Aut}(A) = \mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}, \mathcal{P}\} \cong \mathbb{Z}_2 \tag{14.785}$$

where $\mathcal{P}$ is the automorphism that takes $\mathcal{P}: n \to -n$. Now $\mathrm{Hom}(G, \mathrm{Aut}(\mathbb{Z})) \cong \mathbb{Z}_2$. Of course, $\omega_1 = \mathrm{Id}_{\mathbb{Z}}$ always and now we have two possibilities for ω_σ. Either $\omega_\sigma = \mathrm{Id}_{\mathbb{Z}}$ in which case we denote $\omega = T$ ("T" for trivial) or $\omega_\sigma = \mathcal{P}$ which we will denote $\mathcal{I}$. Let us compute $H^{1+\omega}(\mathbb{Z}_2,\mathbb{Z})$ for these two possibilities. First look at the subgroup of coboundaries. If $\phi_0 = n_0 \in \mathbb{Z}$ is some integer then

$$\begin{aligned}&(d\phi_0)(1) = 0\\ &(d\phi_0)(\sigma) = \omega_\sigma(n_0) - n_0 = \begin{cases}0 & \omega = T\\ -2n_0 & \omega = \mathcal{I}\end{cases}\end{aligned} \tag{14.786}$$

Now consider the differential of a one-cochain:

$$\begin{aligned}(d\phi_1)(1,1) &= \omega_1(\phi_1(1)) - \phi_1(1) + \phi_1(1) = \phi_1(1)\\ (d\phi_1)(1,\sigma) &= \omega_1(\phi_1(\sigma)) - \phi_1(\sigma) + \phi_1(1) = \phi_1(1)\\ (d\phi_1)(\sigma,1) &= \omega_\sigma(\phi_1(1)) - \phi_1(\sigma) + \phi_1(\sigma) = \omega_\sigma(\phi_1(1))\\ (d\phi_1)(\sigma,\sigma) &= \omega_\sigma(\phi_1(\sigma)) - \phi_1(1) + \phi_1(\sigma)\end{aligned} \tag{14.787}$$

Now the cocycle condition implies $\phi_1(1) = 0$, making the first three lines of (14.787) vanish. Using this the fourth line becomes:

$$(d\phi_1)(\sigma, \sigma) = \omega_\sigma(\phi_1(\sigma)) + \phi_1(\sigma) = \begin{cases} 2\phi_1(\sigma) & \omega = T \\ 0 & \omega = \mathcal{I} \end{cases} \tag{14.788}$$

Now, when is ϕ_1 a cocycle? When $\omega = T$ is trivial then we must take $\phi_1(\sigma) = 0$ and hence $\phi_1 = 0$ moreover, there are no coboundaries. We find $H^{1+T}(\mathbb{Z}_2, \mathbb{Z}) = 0$ in this case, reproducing the simple fact that there are no nontrivial group homomorphisms from $\mathbb{Z}_2$ to $\mathbb{Z}$.

On the other hand, when $\omega = \mathcal{I}$ we can take $\phi_1(\sigma) = a$ to be any integer $a \in \mathbb{Z}$. The group of twisted cocycles is isomorphic to $\mathbb{Z}$. However, now there are nontrivial coboundaries, as we see from (14.786). We can shift a by any even integer $a \to a - 2n_0$. So

$$H^{1+\mathcal{I}}(\mathbb{Z}_2, \mathbb{Z}) \cong \mathbb{Z}_2 \tag{14.789}$$

In addition to the interpretation in terms of splittings, this has a nice interpretation in topology in terms of the unorientability of even-dimensional real projective spaces.

Remarks:

1. Previously we were denoting the cohomology groups by $H^{n+\omega}(G, A)$. In the equations above the ω is still present, (see the first term in the definition of $d\phi$) but we leave the ω implicit in the notation. Nevertheless, we are talking about the same groups as before, but now generalizing to arbitrary degree n.

2. Remembering that we are now writing our abelian group A additively, we see that the equation $(d\phi_2) = 0$ is just the twisted 2-cocycle conditions, and $\phi_2' = \phi_2 + d\phi_1$ are two different twisted cocycles related by a coboundary. See equations (14.658) and (14.660) above. Roughly speaking, you should "take the logarithm" of these equations.

3. *Homological Algebra*: What we are discussing here is a special case of a topic known as homological algebra. Quite generally, a *chain complex* is a sequence of Abelian groups $\{C_n\}_{n\in\mathbb{Z}}$ equipped with group homomorphisms

$$\partial_n : C_n \to C_{n-1} \tag{14.790}$$

such that $\partial_n \circ \partial_{n+1} = 0$ for all $n \in \mathbb{Z}$. A *cochain complex* is similarly a sequence of Abelian groups $\{C^n\}_{n\in\mathbb{Z}}$ with group homomorphisms $d_n : C^n \to C^{n+1}$ so that $d_{n+1} \circ d_n = 0$ for all $n \in \mathbb{Z}$. Note that these are NOT exact sequences. Indeed the failure to be an exact sequence is measured by the *homology groups* of the chain complex

$$H_n(C_*, \partial_*) := \ker(\partial_n)/\mathrm{im}(\partial_{n+1}) \tag{14.791}$$

and the *cohomology groups* of the cochain complex:

$$H^n(C^*, d_*) := \ker(d_n)/\mathrm{im}(d_{n-1}) \tag{14.792}$$

4. *Homogeneous cocycles*: A nice way to prove that $d^2 = 0$ is the following. We define *homogeneous* n-cochains to be maps $\varphi : G^{n+1} \to A$ which satisfy

$$\varphi(hg_0, hg_1, \dots, hg_n) = \omega_h \left(\varphi(g_0, g_1, \dots, g_n)\right) \tag{14.793}$$

Let $\mathcal{C}^n(G, A)$ denote the abelian group of such homogeneous group cochains. (Warning! Elements of $\mathcal{C}^n(G, A)$ have $(n + 1)$ arguments!) Define

$$\delta : \mathcal{C}^n(G, A) \to \mathcal{C}^{n+1}(G, A) \tag{14.794}$$

by

$$\delta\varphi(g_0, \dots, g_{n+1}) := \sum_{i=0}^{n+1} (-1)^i \varphi(g_0, \dots, \widehat{g_i}, \dots, g_{n+1}) \tag{14.795}$$

where $\widehat{g_i}$ means the argument is omitted. Clearly, if φ is homogeneous then $\delta\varphi$ is also homogeneous. It is then very straightforward to prove that $\delta^2 = 0$. Indeed, if $\varphi \in \mathcal{C}^{n-1}(G, A)$ we compute:

$$\begin{aligned}
\delta^2\varphi(g_0, \dots, g_{n+1}) &= \sum_{i=0}^{n+1} (-1)^i \Bigg\{ \sum_{j=0}^{i-1} (-1)^j \varphi(g_0, \dots, \widehat{g_j}, \dots, \widehat{g_i}, \dots, g_{n+1}) \\
&\qquad - \sum_{j=i+1}^{n+1} (-1)^j \varphi(g_0, \dots, \widehat{g_i}, \dots, \widehat{g_j}, \dots, g_{n+1}) \Bigg\} \\
&= \sum_{0 \le j < i \le n+1} (-1)^{i+j} \varphi(g_0, \dots, \widehat{g_j}, \dots, \widehat{g_i}, \dots, g_{n+1}) \\
&\qquad - \sum_{0 \le i < j \le n+1} (-1)^{i+j} \varphi(g_0, \dots, \widehat{g_i}, \dots, \widehat{g_j}, \dots, g_{n+1}) \\
&= 0
\end{aligned} \tag{14.796}$$

Now, we can define an isomorphism $\psi : \mathcal{C}^n(G, A) \to C^n(G, A)$ by defining

$$\phi_n(g_1, \dots, g_n) := \varphi_n(1, g_1, g_1 g_2, \dots, g_1 \cdots g_n) \tag{14.797}$$

That is, when ϕ_n and φ_n are related this way we say $\phi_n = \psi(\varphi_n)$. Now one can check that the simple formula (14.795) becomes the more complicated formula (14.775). Put more formally: there is a unique d so that $d\psi = \psi\delta$, or even more formally, there is a unique group homomorphism d such that we have a commutative diagram:

$$\begin{tikzcd}
\mathcal{C}^n(G, A) \arrow[r, "\delta"] \arrow[d, "\psi"] & \mathcal{C}^{n+1}(G, A) \arrow[d, "\psi"] \\
C^n(G, A) \arrow[r, "d"] & C^{n+1}(G, A)
\end{tikzcd} \tag{14.798}$$

For example, if

$$\phi_1(g) = \psi(\varphi_1)(g) = \varphi_1(1, g) \tag{14.799}$$

then we can check that

$$\begin{aligned}(d\phi_1)(g_1,g_2) &= d(\psi(\varphi_1))(g_1,g_2)\\ &= \psi(\delta\varphi_1)(g_1,g_2)\\ &= \delta\varphi_1(1,g_1,g_1g_2)\\ &= \varphi_1(g_1,g_1g_2) - \varphi_1(1,g_1g_2) + \varphi_1(1,g_1)\\ &= \omega_{g_1}(\varphi_1(1,g_2)) - \varphi_1(1,g_1g_2) + \varphi_1(1,g_1)\\ &= \omega_{g_1}(\phi_1(g_2)) - \phi_1(g_1g_2) + \phi_1(g_1)\end{aligned} \tag{14.800}$$

in accord with the previous definition!

5. Where do all these crazy formulae come from? The answer is in topology. We will indicate it briefly in our discussion of categories and groupoids below.
6. The reader will probably find these formulae a bit opaque. It is therefore good to stop and think about what the cohomology is measuring, at least in low degrees.

Exercise
Derive the formula for the differential on an inhomogeneous cochain $d\phi_2$ starting with the definition on the analogous homogeneous cochain φ_3

Exercise
If (C_n, ∂_n) is a chain complex show that one can define a cochain complex with groups:

$$C^n := \mathrm{Hom}(C_n, \mathbb{Z}) \tag{14.801}$$

14.8.2 Interpreting the meaning of $H^{0+\omega}$

A zero-cocycle is an element $a \in A$ so that for all g

$$\omega_g(a) = a \tag{14.802}$$

There are no coboundaries to worry about, so $H^0(G,A)$ is just the set of fixed points of the G action on A.

14.8.3 Interpreting the meaning of $H^{1+\omega}$

We have interpreted $H^{1+\omega}(G,A)$ above as the set of nontrivial splittings of the semidirect product defined by ω:

$$0 \to A \to A \rtimes G \to G \to 1 \tag{14.803}$$

14.8.4 Interpreting the meaning of $H^{2+\omega}$

Again, we have interpreted $H^{2+\omega}(G, A)$ as $\mathrm{Ext}^{\omega}(G, A)$, the set of equivalence classes of extensions

$$0 \to A \to \tilde{G} \to G \to 1 \tag{14.804}$$

inducing a fixed $\omega : G \to \mathrm{Aut}(A)$. The trivial element of the cohomology group corresponds to the semi-direct product and the set of inequivalent trivializations is the group $H^{1+\omega}(G, A)$ of splittings of the semi-direct product.

More generally, $\mathrm{Ext}^{\bar{\omega}}(Q, N)$ is a torsor for $H^{2+\bar{\omega}}(Q, Z(N))$.

14.8.5 Interpreting the meaning of H^3

To see one interpretation of H^3 in terms of extension theory let us return to the analysis of general extensions in §14.7.

Recall that, as we have discussed using (14.766), a general extension (14.1) has a canonically associated homomorphism

$$\bar{\omega} : Q \to \mathrm{Out}(N) \tag{14.805}$$

where $\mathrm{Out}(N)$ is the group of outer automorphisms of N.

The natural question arises: *Given a homomorphism $\bar{\omega}$ as in (14.805) is there a corresponding extension of Q by N inducing $\bar{\omega}$ as in equation (14.766) ?*

To answer this question we could proceed by *choosing* for each $q \in Q$ an automorphism $\xi_q \in \mathrm{Aut}(N)$ such that $[\xi_q] = \bar{\omega}_q$ in $\mathrm{Out}(N)$. To do this, choose a section s of $\pi : \mathrm{Aut}(N) \to \mathrm{Out}(N)$ and let $\xi_q := s(\bar{\omega}_q)$. If we cannot split the sequence

$$1 \to \mathrm{Inn}(N) \to \mathrm{Aut}(N) \to \mathrm{Out}(N) \to 1 \tag{14.806}$$

then $q \mapsto \xi_q$ will not be a group homomorphism. But we do know that for all $q_1, q_2 \in Q$

$$\xi_{q_1} \circ \xi_{q_2} \circ \xi^{-1}_{q_1 q_2} \in \mathrm{Inn}(N) \tag{14.807}$$

Therefore, for every q_1, q_2 we may *choose* an element $f(q_1, q_2) \in N$ so that

$$\xi_{q_1} \circ \xi_{q_2} \circ \xi^{-1}_{q_1 q_2} = I(f(q_1, q_2)) \tag{14.808}$$

i.e.

$$\xi_{q_1} \circ \xi_{q_2} = I(f(q_1, q_2)) \circ \xi_{q_1 q_2} \tag{14.809}$$

Of course, the choice of $f(q_1, q_2)$ is ambiguous by an element of $Z(N)$!

Equation (14.809) is of course just (14.756) written in slightly different notation. Therefore, as we saw in §14.7, if $f(q_1, q_2)$ were to satisfy the the "twisted cocycle condition" (14.757) then we could use (14.758) to define an extension inducing $\bar{\omega}$.

Therefore, let us check if some choice of $f(q_1, q_2)$ actually does satisfy the twisted cocycle condition (14.757). Looking at the RHS of (14.757) we compute:

$$\begin{aligned} I(f(q_1, q_2) f(q_1 q_2, q_3)) &= I(f(q_1, q_2)) I(f(q_1 q_2, q_3)) \\ &= \left(\xi_{q_1} \circ \xi_{q_2} \circ \xi^{-1}_{q_1 q_2}\right) \circ \left(\xi_{q_1 q_2} \circ \xi_{q_3} \circ \xi^{-1}_{q_1 q_2 q_3}\right) \\ &= \xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_3} \circ \xi^{-1}_{q_1 q_2 q_3} \end{aligned} \tag{14.810}$$

On the other hand, looking at the LHS of (14.757) we compute:

$$\begin{aligned} I(\xi_{q_1}(f(q_2,q_3))f(q_1,q_2q_3)) &= I(\xi_{q_1}(f(q_2,q_3)))I(f(q_1,q_2q_3)) \\ &= \xi_{q_1} \circ I((f(q_2,q_3))) \circ \xi_{q_1}^{-1} \circ I(f(q_1,q_2q_3) \\ &= \xi_{q_1} \circ \left(\xi_{q_2} \circ \xi_{q_3} \circ \xi_{q_2q_3}^{-1}\right) \circ \xi_{q_1}^{-1} \circ \left(\xi_{q_1} \circ \xi_{q_2q_3} \circ \xi_{q_1q_2q_3}^{-1}\right) \\ &= \xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_3} \circ \xi_{q_1q_2q_3}^{-1} \end{aligned} \tag{14.811}$$

Therefore, comparing (14.810) and (14.811) we conclude that

$$I(\xi_{q_1}(f(q_2,q_3))f(q_1,q_2q_3)) = I(f(q_1,q_2)f(q_1q_2,q_3)) \tag{14.812}$$

We cannot conclude that f satisfies the twisted cocycle equation from this identity because inner transformations are trivial for elements in the center $Z(N)$. Rather, what we can conclude is that for every q_1, q_2, q_3 there is an element $z(q_1,q_2,q_3) \in Z(N)$ such that

$$f(q_1,q_2)f(q_1q_2,q_3) = z(q_1,q_2,q_3)\xi_{q_1}(f(q_2,q_3))f(q_1,q_2q_3) \tag{14.813}$$

Now, one can check (with a lot of algebra) that

1. z is a cocycle in $Z^{3+\bar{\omega}}(Q,Z(N))$. (We are using $\mathrm{Aut}(Z(N)) \cong \mathrm{Out}(Z(N))$.)
2. Changes in choices of ξ_q and $f(q_1,q_2)$ lead to changes in z by a coboundary.

and therefore we conclude:

Theorem 14.8.5.1 : Given $\bar{\omega} : Q \to \mathrm{Out}(N)$ there exists an extension of Q by N iff the cohomology class $[z] \in H^3(Q,Z(N))$ vanishes.

Moreover, as we have seen, if $[z]=0$ then the trivializations of z are in 1-1 correspondence with elements $H^2(Q,Z(N))$ and are hence in 1-1 correspondence with isomorphism classes of extensions of Q by N. This is the analogue, one step up in degree, of our interpretation of $H^1(G,A)$.

Examples: As an example [179] where a degree three cohomology class obstructs the existence of an extension inducing a homomorphism $\bar{\omega} : Q \to \mathrm{Out}(N)$ we can take N to be the generalized quaternion group of order 16. It is generated by x and y satisfying:

$$x^4 = y^2 \qquad x^8 = 1 \qquad yxy^{-1} = x^{-1} \tag{14.814}$$

Using these relations every word in $x^{\pm 1}$ and $y^{\pm 1}$ can be reduced to either x^m, or yx^m, with $m = 0, \dots, 7$, and these words are all different. One can show the outer automorphism group $\mathrm{Out}(N) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ with generators α, β acting by

$$\alpha(x) = x^3, \alpha(y) = y \qquad\qquad \beta(x) = x, \beta(y) = yx \tag{14.815}$$

Then there is is no group extension with group G fitting in

$$1 \to N \to G \to \mathbb{Z}_2 \to 1 \tag{14.816}$$

[179] I learned these nice examples from Clay Cordova. They will appear in a forthcoming paper with Po-Shen Hsin and Francesco Benini.

inducing the homomorphism $\bar{\omega} : \mathbb{Z}_2 \to \mathrm{Out}(N)$ defined by $\bar{\omega}(\sigma) = \alpha \circ \beta$ where σ is the nontrivial element of $\mathbb{Z}_2$. One way to prove this is to look up the list of groups of order 32 and search for those with maximal normal subgroup given by N. [180] There are five such. Then one computes $\bar{\omega}$ for each such extension and finds that it is never of the above type. A similar example can be constructed by taking N to be a dihedral group of order 16.

♣Really should explain four-term sequences and crossed modules here.... ♣

Remark There is an interpretation of $H^3(Q, Z(N))$ as a classification of four-term exact sequences, and there are generalizations of this to higher degree. See

1. K. Brown, *Group Cohomology.*
2. C. A. Weibel, *An introduction to homological algebra*, chapter 6

14.9 Some references

Some online sources with links to further material are

1. http://en.wikipedia.org/wiki/Group-extension
2. http://ncatlab.org/nlab/show/group+extension

3 http://terrytao.wordpress.com/2010/01/23/some-notes-on-group-extensions/

4. Section 14.8.5, known as the Artin-Schreier theory, is based on a nice little note by P.J. Morandi,

http://sierra.nmsu.edu/morandi/notes/GroupExtensions.pdf

5. Jungmann, Notes on Group Theory

6. S. MacLane, "Topology And Logic As A Source Of Algebra," Bull. Amer. Math. Soc. 82 (1976), 1-4.

Textbooks:

1. K. Brown, Group Cohomology
2. Karpilovsky, The Schur Multiplier
3. C. A. Weibel, *An introduction to homological algebra*, chapter 6

15. Overview of general classification theorems for finite groups

In general if a mathematical object proves to be useful then there is always an associated important problem, namely the *classification* of these objects.

For example, with groups we can divide them into classes: finite and infinite, abelian and nonabelian producing a four-fold classication:

Finite abelian	Finite nonabelian
Infinite abelian	Infinite nonabelian

[180] See, for example, B. Shuster, "Morava K-theory of groups of order 32," Algebr. Geom. Topol. **11** (2011) 503-521.

But this is too rough, it does not give us a good feeling for what the examples really are.

Once we have a "good" criterion we often can make a nontrivial statement about the general structure of objects in a given class. Ideally, we should be able to construct all the examples algorithmically, and be able to distinguish the ones which are not isomorphic. Of course, finding such a "good" criterion is an art. For example, classification of infinite nonabelian groups is completely out of the question. But in Chapter *** we will see that an important class of infinite nonabelian groups, the simply connected compact simple Lie groups, have a very beautiful classification: There are four infinite sequences of classical matrix groups: $SU(n), Spin(n), USp(2n)$ and then five exceptional cases with names G_2, F_4, E_6, E_7, E_8. [181]

One might well ask: Can we classify finite groups? In this section we survey a little of what is known about this problem.

15.1 Brute force

If we just start listing groups of low order we soon start to appreciate what a jungle is out there.

But let us try, if only as an exercise in applying what we have learned so far. First, let us note that for groups of order p where p is prime we automatically have the unique possibility of the cyclic group $\mathbb{Z}/p\mathbb{Z}$. Similarly, for groups of order p^2 there are precisely two possibilities: $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. This gets us through many of the low order cases.

Given this remark the first nontrivial order to work with is $|G| = 6$. By Cauchy's theorem there are elements of order 2 and 3. Call them b, with $b^2 = 1$ and a with $a^3 = 1$. Then $(bab)^3 = 1$, so either

1. $bab = a$ which implies $ab = ba$ which implies $G = \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_6$
2. $bab = a^{-1}$ which implies $G = D_3$.

This is the first place we meet a nonabelian group. It is the dihedral group, the first of the series we saw before

$$D_n = \langle a, b | a^n = b^2 = 1, bab = a^{-1} \rangle \tag{15.1}$$

and has order $2n$. There is a special isomorphism $D_3 \cong S_3$ with the symmetric group on three letters.

The next nontrivial case is $|G| = 8$. Here we can invoke Sylow's theorem: If $p^k||G|$ then G has a subgroup of order p^k. Let us apply this to 4 dividing $|G|$. Such a subgroup has index two and hence must be a normal subgroup, and hence fits in a sequence

$$1 \to N \to G \to \mathbb{Z}_2 \to 1 \tag{15.2}$$

Now, N is of order 4 so we know that $N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $N \cong \mathbb{Z}_4$. If we have

$$1 \to \mathbb{Z}_4 \to G \to \mathbb{Z}_2 \to 1 \tag{15.3}$$

[181] $Spin(n)$ double covers the classical matrix group $SO(n)$.

then we have $\alpha : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$ and there are exactly two such homomorphisms. Moreover, for a fixed α there are two possibilities for the square $\tilde{\sigma}^2 \in \mathbb{Z}_4$ where $\tilde{\sigma}$ is a lift of the generator of $\mathbb{Z}_2$. Altogether this gives four possibilities:

♣Need to explain more here. ♣

$$1 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{15.4}$$

$$1 \to \mathbb{Z}_4 \to \mathbb{Z}_8 \to \mathbb{Z}_2 \to 1 \tag{15.5}$$

$$1 \to \mathbb{Z}_4 \to D_4 \to \mathbb{Z}_2 \to 1 \tag{15.6}$$

$$1 \to \mathbb{Z}_4 \to \widetilde{D}_2 \to \mathbb{Z}_2 \to 1 \tag{15.7}$$

Here we meet the first of the series of *dicyclic* or *binary dihedral* groups defined by

$$\widetilde{D_n} := \langle a, b | a^{2n} = 1, a^n = b^2, b^{-1}ab = a^{-1} \rangle \tag{15.8}$$

It has order $4n$. There is a special isomorphism of $\widetilde{D}_2$ with the quaternion group.

The other possibility for N is $\mathbb{Z}_2 \times \mathbb{Z}_2$ and here one new group is found, namely $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Thus there are 5 inequivalent groups of order 8.

The next few cases are trivial until we get to $|G| = 12$. By Cauchy's theorem there are subgroups isomorphic to $\mathbb{Z}_2$, so we can view G as an extension of D_3 or $\mathbb{Z}_6$ by $\mathbb{Z}_2$. There is also a subgroup isomorphic to $\mathbb{Z}_3$ so we can view it as an extension of an order 4 group by an order 3 group. We skip the analysis and just present the 5 distinct order 12 groups. In this way we find the groups forming the pattern at lower order:

♣Check this reasoning is correct. You need to know the subgroups are normal to say there is an extension. ♣

$$\mathbb{Z}_{12}, \quad , \mathbb{Z}_2 \times \mathbb{Z}_6, \quad , D_6, \quad , \tilde{D}_3 \tag{15.9}$$

And we find one "new" group: $A_4 \subset S_4$.

We can easily continue the table until we get to order $|G| = 16$. At order 16 there are 14 inequivalent groups! So we will stop here. [182]

[182] See, however, M. Wild, "Groups of order 16 made easy," American Mathematical Monthly, Jan 2005

Order	Presentation	name
1	$\langle a \vert a = 1\rangle$	Trivial group
2	$\langle a \vert a^2 = 1\rangle$	Cyclic $\mathbb{Z}/2\mathbb{Z}$
3	$\langle a \vert a^3 = 1\rangle$	Cyclic $\mathbb{Z}/3\mathbb{Z}$
4	$\langle a \vert a^4 = 1\rangle$	Cyclic $\mathbb{Z}/4\mathbb{Z}$
4	$\langle a, b \vert a^2 = b^2 = (ab)^2 = 1\rangle$	Dihedral $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, Klein
5	$\langle a \vert a^5 = 1\rangle$	Cyclic $\mathbb{Z}/5\mathbb{Z}$
6	$\langle a, b \vert a^3 = 1, b^2 = 1, bab = a\rangle$	Cyclic $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
6	$\langle a, b \vert a^3 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral $D_3 \cong S_3$
7	$\langle a \vert a^7 = 1\rangle$	Cyclic $\mathbb{Z}/7\mathbb{Z}$
8	$\langle a \vert a^8 = 1\rangle$	Cyclic $\mathbb{Z}/8\mathbb{Z}$
8	$\langle a, b \vert a^2 = 1, b^4 = 1, aba = b\rangle$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
8	$\langle a, b, c \vert a^2 = b^2 = c^2 = 1, [a, b] = [a, c] = [b, c] = 1\rangle$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
8	$\langle a, b \vert a^4 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_4
8	$\langle a, b \vert a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1}\rangle$	Dicyclic $\widetilde{D_2} \cong Q$, quaternion
9	$\langle a \vert a^9 = 1\rangle$	Cyclic $\mathbb{Z}/9\mathbb{Z}$
9	$\langle a, b \vert a^3 = b^3 = 1, [a, b] = 1\rangle$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	$\langle a \vert a^{10} = 1\rangle$	Cyclic $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
10	$\langle a \vert a^5 = b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_5
11	$\langle a \vert a^{11} = 1\rangle$	Cyclic $\mathbb{Z}/11\mathbb{Z}$
12	$\langle a \vert a^{12} = 1\rangle$	Cyclic $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
12	$\langle a, b \vert a^2 = 1, b^6 = 1, [a, b] = 1\rangle$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
12	$\langle a, b \vert a^6 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_6
12	$\langle a, b \vert a^6 = 1, a^3 = b^2, b^{-1}ab = a^{-1}\rangle$	Dicyclic $\widetilde{D_3}$
12	$\langle a, b \vert a^3 = 1, b^2 = 1, (ab)^3 = 1\rangle$	Alternating A_4
13	$\langle a \vert a^{13} = 1\rangle$	Cyclic $\mathbb{Z}/13\mathbb{Z}$
14	$\langle a \vert a^{14} = 1\rangle$	Cyclic $\mathbb{Z}/14\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$
14	$\langle a, b \vert a^7 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_7
15	$\langle a \vert a^{15} = 1\rangle$	Cyclic $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Remarks:

1. Explicit tabulation of the isomorphism classes of groups was initiated by by Otto Holder who completed a table for $|G| \leq 200$ about 100 years ago. Since then there has been much effort in extending those results. For surveys see

   1. J.A. Gallan, "The search for finite simple groups," Mathematics Magazine, vol. 49 (1976) p. 149. (This paper is a bit dated.)

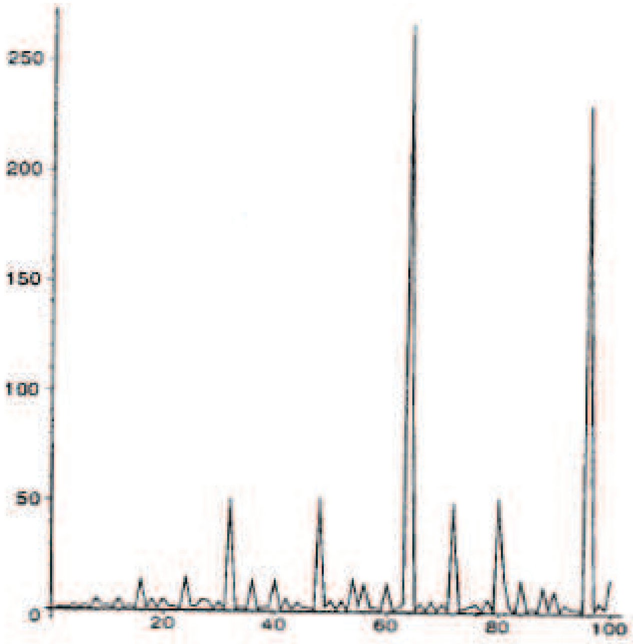

Figure 32: A plot of the number of nonisomorphic groups of order n. This plot was taken from the book by D. Joyner, *Adventures in Group Theory*.

2. H.U. Besche, B. Eick, E.A. O'Brian, "A millenium project: Constructing Groups of Small Order,"

2. There are also nice tables of groups of low order, in Joyner, *Adventures in Group Theory*, pp. 168-172, and Karpilovsky, *The Schur Multiplier* which go beyond the above table.

3. There are also online resources:

   1. http://www.gap-system.org/ for GAP
   2. http://hobbes.la.asu.edu/groups/groups.html for groups of low order.
   3. http://www.bluetulip.org/programs/finitegroups.html
   4. http://en.wikipedia.org/wiki/List-of-small-groups

4. The number of isomorphism types of groups jumps wildly. Apparently, there are $49,487,365,422$ isomorphism types of groups of order $2^{10} = 1024$. (Besche et. al. loc. cit.) The remarkable plot of Figure 32 from Joyner's book shows a plot of the number of isomorphism classes vs. order up to order 100. Figure 33 shows a log plot of the number of groups up to order 2000.

5. There is, however, a formula giving the asymptotics of the number $f(n,p)$ of isomorphism classes of groups of order p^n for $n \to \infty$ for a fixed prime p. (Of course, there are $p(n)$ Abelian groups, where $p(n)$ the the number of partitions of n. Here we are

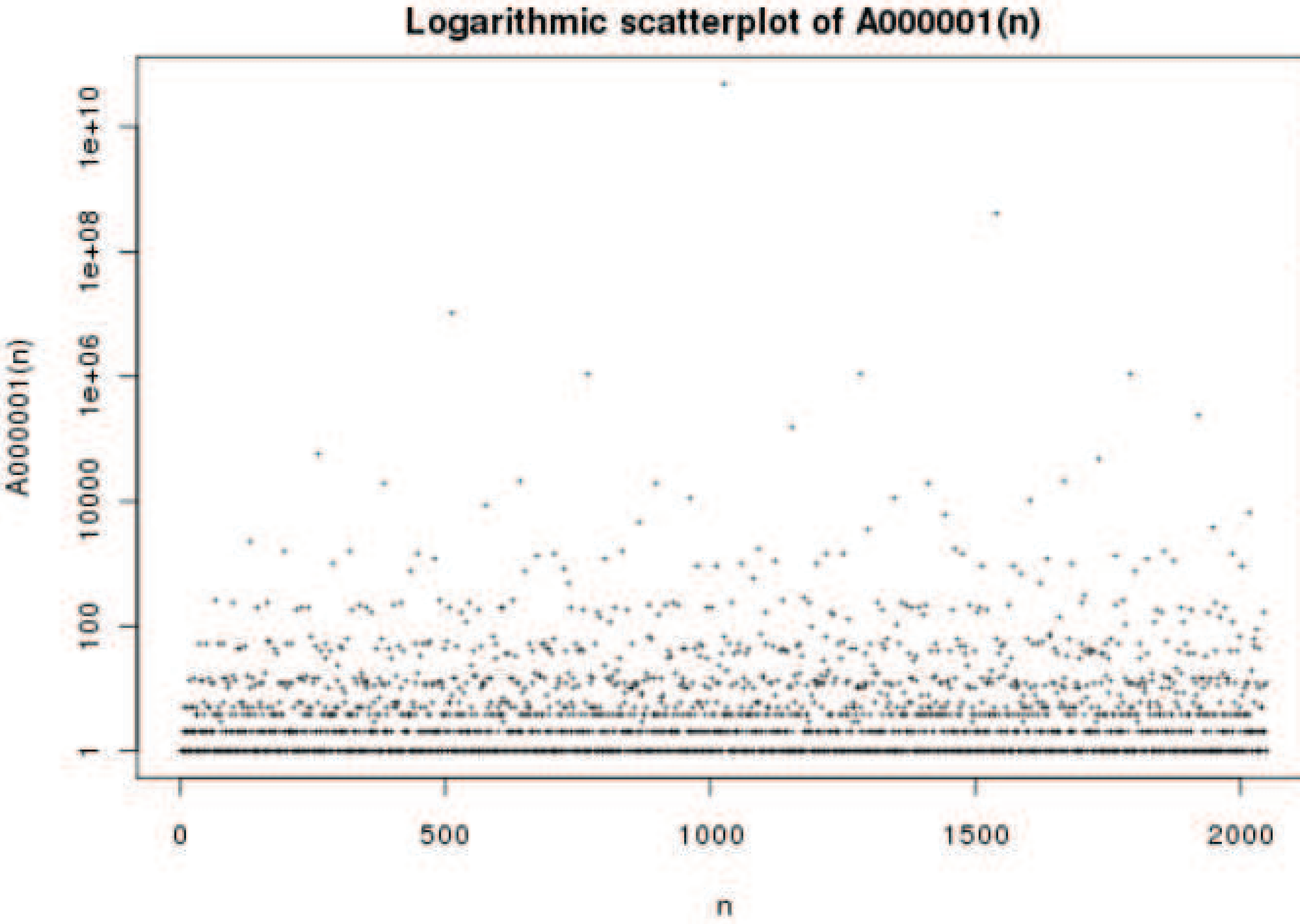

Figure 33: A logarithmic plot of the number of nonisomorphic groups of order n out to $n \leq 2000$. This plot was taken from online encyclopedia of integer sequences, OEIS.

talking about the number of all groups.) This is due to G. Higman [183] and C. Sims [184] and the result states that:

$$f(n,p) \sim p^{\frac{2}{27}n^3} \tag{15.10}$$

Note that the asymptotics we derived for $p(n)$ before had a growth like $e^{const.n^{1/2}}$ so, unsurprisingly, most of the groups are nonabelian.

Exercise *Relating the binary dihedral and dihedral groups*

[183] G. Higman, "Enumerating p-Groups," Proc. London Math. Soc. 3) 10 (1960)

[184] C. Sims, "Enumerating p-Groups," Proc. London Math. Soc. (3) IS (1965) 151-66

Show that $\widetilde{D}_n$ is a double-cover of D_n which fits into the exact sequence:

$$\begin{tikzcd}
 & \mathbb{Z}_2 \arrow[r, equal] \arrow[d] & \mathbb{Z}_2 \arrow[d] & & \\
1 \arrow[r] & \mathbb{Z}_{2n} \arrow[r] \arrow[d, equal] & \widetilde{D}_n \arrow[r] \arrow[d] & \mathbb{Z}_2 \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathbb{Z}_n \arrow[r] & D_n \arrow[r] & \mathbb{Z}_2 \arrow[r] & 1
\end{tikzcd} \tag{15.11}$$

15.2 Finite Abelian Groups

The upper left box of our rough classification can be dealt with thoroughly, and the result is extremely beautiful.

In this subsection we will write our abelian groups *additively.*

Recall that we have shown that if p and q are positive integers then

$$0 \to \mathbb{Z}/gcd(p,q)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/lcm(p,q)\mathbb{Z} \to 0 \tag{15.12}$$

and in particular, if p, q are relatively prime then

$$\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}. \tag{15.13}$$

It thus follows that if n has prime decomposition

$$n = \prod_i p_i^{e_i} \tag{15.14}$$

then

$$\mathbb{Z}/n\mathbb{Z} \cong \oplus_i \mathbb{Z}/p_i^{e_i}\mathbb{Z} \tag{15.15}$$

This decomposition has a beautiful generalization to an arbitrary finite abelian group:

Kronecker Structure Theorem. Any finite abelian group is a direct product of cyclic groups of order a prime power. That is, we firstly have the decomposition:

$$\begin{aligned} G &= G_2 \oplus G_3 \oplus G_5 \oplus G_7 \oplus \cdots \\ &= \oplus_{p \text{ prime}} G_p \end{aligned} \tag{15.16}$$

where G_p has order p^n for some $n \geq 0$ (n can depend on p, and for all but finitely many p, $G_p = \{0\}$.) And, secondly, each nonzero factor G_p can be written:

$$G_p = \oplus_i \mathbb{Z}/(p^{n_i}\mathbb{Z}) \tag{15.17}$$

for some finite collection of positive integers n_i (depending on p).

Proof: The proof proceeds in two parts. The first, easy, part shows that we can split G into a direct sum of "p-groups" (defined below). The second, harder, part shows that an arbitrary abelian p-group is a direct sum of cyclic groups.

For part 1 of the proof let us consider an arbitrary finite abelian group G. We will write the group multiplication additively. Suppose n is an integer so that $ng = 0$ for all $g \in G$. To fix ideas let us take $n = |G|$. Suppose $n = m_1 m_2$ where m_1, m_2 are relatively prime integers. Then there are integers s_1, s_2 so that

$$s_1 m_1 + s_2 m_2 = 1 \tag{15.18}$$

Therefore any element g can be written as

$$g = s_1(m_1 g) + s_2(m_2 g) \tag{15.19}$$

Now $m_1 G$ and $m_2 G$ are subgroups and we claim that $m_1 G \cap m_2 G = \{0\}$. If $a \in m_1 G \cap m_2 G$ then $m_1 a = 0$ and $m_2 a = 0$ and hence (15.19) implies $a = 0$. Thus,

$$G = m_1 G \oplus m_2 G \tag{15.20}$$

Moreover, we claim that $m_1 G = \{g \in G | m_2 g = 0\}$. It is clear that every element in $m_1 G$ is killed by m_2. Suppose on the other hand that $m_2 g = 0$. Again applying (15.19) we see that $g = s_1 m_1 g = m_1(s_1 g) \in m_1 G$.

Thus, we can decompose

$$G = \oplus p \text{ prime} G_p \tag{15.21}$$

where G_p is the subgroup of G of elements whose order is a power of p.

If p is a prime number then a *p-group* is a group all of whose elements have order a power of p. Now for part 2 of the proof we show that any abelian p-group is a direct sum of the form (15.17). The proof of this statement proceeds by induction and is based on a systematic application of Cauchy's theorem: If p divides $|G|$ then there is an element of G of order precisely p. (Recall we proved this theorem in Section 9.

Now, note that any p-group G has an order which is a power p^n for some n. If not, then $|G| = p^n m$ where m is relatively prime to p. But then - by Cauchy's theorem - there would have to be an element of G whose order is a prime divisor of m.

Next we claim that if an abelian p-group has a *unique* subgroup H of order p then G itself is cyclic.

To prove this we again proceed by induction on $|G|$. Consider the subgroup defined by:

$$H = \{g | pg = 0\} \tag{15.22}$$

From Cauchy's theorem we see that H cannot be the trivial group, and hence this must be the unique subgroup of order p. On the other hand, H is manifestly the kernel of the homomorphism $\phi : G \to G$ given by $\phi(g) = pg$. Again by Cauchy, $\phi(G)$ has a subgroup of order p, but this must also be a subgroup of G, which contains $\phi(G)$, and hence $\phi(G)$ has a unique subgroup of order p. By the induction hypothesis, $\phi(G)$ is cyclic. But now $\phi(G) \cong G/H$, so let $g_0 + H$ be a generator of the cyclic group G/H. Next we claim that $H \subset \langle g_0 \rangle$. Since G is a p-group the subgroup $\langle g_0 \rangle$ is a p-group and hence contains a subgroup of order p (by Cauchy) but (by hypothesis) there is a unique such subgroup in G and any subgroup of $\langle g_0 \rangle$ is a subgroup of G, so $H \subset \langle g_0 \rangle$. But now take any element $g \in G$. On the one hand it must project to an element $[g] \in G/H$. Thus must be of the form $[g] = kg_0 + H$, since $g_0 + H$ generates G/H. That means $g = kg_0 + h$, $h \in H$, but since $H \subset \langle g_0 \rangle$ we must have $h = \ell g_0$ for some integer ℓ. Therefore $G = \langle g_0 \rangle$ is cyclic.

The final step proceeds by showing that if G is a finite abelian p-group and M is a cyclic subgroup of maximal order then $G = M \oplus N$ for some subgroup N. Once we have established this the desired result follows by induction.

So, now suppose that that G has a cyclic subgroup of maximal order M. If G is cyclic then $N = \{0\}$. If G is not cyclic then we just proved that there must be at least two distinct subgroups of order p. One of them is in M. Choose another one, say K. Note that K must not be in M, because M is cyclic and has a unique subgroup of order p. Therefore $K \cap M = \{0\}$. Therefore $(M + K)/K \cong M$. Therefore $(M + K)/K$ is a cyclic subgroup of G/K. Any element $g + K$ has an order which divides $|g|$, and $|g| \le |M|$ since M is a maximal cyclic subgroup. Therefore the cyclic subgroup $(M + K)/K$ is a maximal order cyclic subgroup of G/K. Now the inductive hypothesis implies $G/K = (M+K)/K \oplus H/K$ for some subgroup $K \subset H \subset G$. But this means $(M+K) \cap H = K$ and hence $M \cap H = \{0\}$ and hence $G = M \oplus H$. ♠

For other proofs see

1. S. Lang, *Algebra*, ch. 1, sec. 10.
2. I.N. Herstein, Ch. 2, sec. 14.
3. J. Stillwell, *Classical Topology and Combinatorial Group Theory.*
4. Our proof is based on G. Navarro, "On the fundamental theorem of finite abelian groups," Amer. Math. Monthly, Feb. 2003, vol. 110, p. 153.

One class of examples where we have a finite Abelian group, but it's Kronecker decomposition is far from obvious is the following: Consider the Abelian group $\mathbb{Z}^d$. Choose a set of d vectors $v_i \in \mathbb{Z}^d$, linearly independent as vectors in $\mathbb{R}^d$.

$$L := \{\sum_{i=1}^{d} n_i v_i | n_i \in \mathbb{Z}\} \tag{15.23}$$

is a subgroup. Then

$$A = \mathbb{Z}^d/L \tag{15.24}$$

is a finite Abelian group. For example if $v_i = ke_i$ where e_i is the standard unit vector in the i^{th} direction then obviously $A \cong (\mathbb{Z}/k\mathbb{Z})^d$. But for a general set of vectors the decomposition is not obvious.

So, here is an algorithm for giving the Kronecker decomposition of a finite Abelian group:

1. Compute the orders of the various elements.

2. You need only consider the elements whose order is a prime power. (By the Bezout manipulation all the others will be sums of these.)

3. Focusing on one prime at a time. Take the element g_1 whose order is maximal. Then $G_p = \langle g_1 \rangle \oplus N$.

♣Have to say how to get N. ♣

4. Repeat for N.

Exercise

Show that an alternative of the structure theorem is the statement than any finite abelian group is isomorphic to

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k} \tag{15.25}$$

where

$$n_1 | n_2 \quad \& \quad n_2 | n_3 \quad \& \quad \cdots \quad \& \quad n_{k-1} | n_k \tag{15.26}$$

Write the n_i in terms of the prime powers in (15.17).

Exercise *p-groups*

a.) Show that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

b.) Show more generally that if p is prime $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_{p^{n-m}} \oplus \mathbb{Z}_{p^m}$ are not isomorphic if $0 < m < n$.

c.) How many nonisomorphic abelian groups have order p^n?

Exercise

Suppose $e_1, e_2 \in \mathbb{Z}^2$ are two linearly independent vectors (over $\mathbb{Q}$). Let $\Lambda = \langle e_1, e_2 \rangle \subset \mathbb{Z}^2$ be the sublattice generated by these vectors. Then $\mathbb{Z}^2/\Lambda$ is a finite abelian group. Compute its Kronecker decomposition in terms of the coordinates of e_1, e_2.

15.3 Finitely Generated Abelian Groups

It is hopeless to classify all infinite abelian groups, but a "good" criterion that leads to an interesting classification is that of *finitely generated* abelian groups.

Any abelian group has a canonically defined subgroup known as the *torsion subgroup*, and denoted Tors(G). This is the subgoup of elements of *finite order*:

$$\mathrm{Tors}(G) := \{ g \in G | \exists n \in \mathbb{Z} \qquad ng = 0 \} \tag{15.27}$$

where we are writing the group G additively, so $ng = g + \cdots + g$.

One can show that any *finitely generated abelian group* fits in an exact sequence

$$0 \to \mathrm{Tors}(G) \to A \to \mathbb{Z}^r \to 0 \tag{15.28}$$

where $\mathrm{Tors}(G)$ is a *finite abelian group.*

For a proof, see, e.g., S. Lang, *Algebra* .

Moreover (15.28) is a split extension, that is, it is isomorphic to

$$\mathbb{Z}^r \oplus \mathrm{Tors}(G) \tag{15.29}$$

The integer r, called the *rank of the group*, and the finite abelian group $\mathrm{Tors}(G)$ are invariants of the finitely generated abelian group. Since we have a general picture of the finite abelian groups we have now got a general picture of the finitely generated abelian groups.

Remark:

Remarks

1. The groups $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ under addition are abelian but not finitely generated. This is obvious for $\mathbb{C}$ and $\mathbb{R}$ since these are uncountable sets. To see that $\mathbb{Q}$ is not finitely generated consider any finite set of fractions $\{\frac{p_1}{q_1}, \dots, \frac{p_s}{q_s}\}$. This set will will only generate rational numbers which, when written in lowest terms, have denominator at most $q_1 q_2 \cdots q_s$.

2. Note that a torsion abelian group need not be finite in general. For example $\mathbb{Q}/\mathbb{Z}$ is entirely torsion, but is not finite.

3. A rich source of finitely generated abelian groups are the integral cohomology groups $H^n(X;\mathbb{Z})$ of smooth compact manifolds.

4. We must stress that the presentation (15.29) of a finitely generated abelian group is not canonical! There are many distinct splittings of (15.28). They are in 1-1 correspondence with the group homomorphisms $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{Tors}(G))$. For a simple example consider $\mathbb{Z}^d/\Lambda$ where Λ is a general sublattice of rank less than d.

5. In a nonabelian group the product of two finite-order elements can very well have infinite order. Examples include free products of cyclic groups and simple rotations by $2\pi/n$ around different axes in $SO(3)$. So, there is no straightforward generalization of $\mathrm{Tors}(G)$ to the case of nonabelian groups.

Exercise

Consider the finitely generated Abelian group [185]

$$L = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 | \sum_i x_i = 0\mathrm{mod}2\} \tag{15.30}$$

and consider the subgroup S generated by

$$\begin{aligned} v_1 &= (1, 1, 1, 1) \\ v_2 &= (1, 1, -1, -1) \end{aligned} \tag{15.31}$$

a.) What is the torsion group of L/S ?

b.) Find a splitting of the sequence (15.28) and compare with the one found by other students in the course. Are they the same?

Exercise

Given a set of finite generators of an Abelian group A try to find an algorithm for a splitting of the sequence (15.28).

15.4 The Classification Of Finite Simple Groups

Kronecker's structure theorem is a very satisfying, beautiful and elegant answer to a classification question. The generalization to nonabelian groups is very hard. It turns out that a "good" criterion is that a finite group be a *simple* group. This idea arose from the Galois demonstration of (non)solvability of polynomial equations by radicals.

A key concept in abstract group theory is provided by the notion of a *composition series*. This is a sequence of subgroups

$$1 = G_{s+1} \triangleleft G_s \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 = G \tag{15.32}$$

which have the property that G_{i+1} is a maximal normal subgroup of G_i. (Note: G_{i+1} need not be normal in G. Moreover, there might be more than one maximal normal subgroup in G_i.) As a simple example we shall see that we have

♣should give an example of this.... ♣

$$1 = G_4 \triangleleft G_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \triangleleft G_2 = A_4 \triangleleft G_1 = S_4 \tag{15.33}$$

but

$$G_3 = 1 \triangleleft G_2 = A_n \triangleleft G_1 = S_n \qquad\qquad n \geq 5 \tag{15.34}$$

Not every group admits a composition series. For example $G = \mathbb{Z}$ does not admit a composition series. (Explain why!) However, it can be shown that every <u>finite</u> group admits a composition series.

♣Give a reference. ♣

[185] It is the root lattice of $\mathfrak{so}(8)$.

It follows that in a composition series the quotient groups G_i/G_{i+1} are *simple groups*: By definition, a simple group is one whose only normal subgroups are 1 and itself. From what we have learned above, that means that a simple group has no nontrivial homomorphic images. It also implies that the center is trivial or the whole group.

Let us prove that the G_i/G_{i+1} are simple: In general, if $N \triangleleft G$ is a normal subgroup then there is a 1-1 correspondence:

Subgroups H between N and G: $N \subset H \subset G \Leftrightarrow$ Subgroups of G/N

Moreover, under this correspondence:

Normal subgroups of $G/N \Leftrightarrow$ Normal subgroups $N \subset H \triangleleft G$. If $H/G_{i+1} \subset G_i/G_{i+1}$ were normal and $\neq 1$ then $G_{i+1} \subset H \subset G_i$ would be normal and and properly contain G_{i+1}, contradicting maximality of G_{i+1}. ♠

♣Make this an exercise in an earlier section. ♣

A composition series is a nonabelian generalization of the Kronecker decomposition. It is not unique (see exercise below) but the the following theorem, known as the Jordan-Hölder theorem states that there are some invariant aspects of the decomposition:

Theorem: Suppose there are two different composition series for G:

$$1 = G_{s+1} \triangleleft G_s \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 = G \tag{15.35}$$

$$1 = G'_{s'+1} \triangleleft G'_s \triangleleft \cdots \triangleleft G'_2 \triangleleft G'_1 = G \tag{15.36}$$

Then $s = s'$ and there is a permutation $i \to i'$ so that $G_i/G_{i+1} \cong G'_{i'}/G'_{i'+1}$. That is: The length and the unordered set of quotients are both invariants of the group and do not depend on the particular composition series.

For a proof see Jacobsen, Section 4.6.

The classification of all finite groups is reduced to solving the extension problem in general, and then classifying finite simple groups. The idea is that if we know $G_i/G_{i+1} = S_i$ is a finite simple group then we construct G_i from G_{i+1} and the extension:

$$1 \to G_{i+1} \to G_i \to S_i \to 1 \tag{15.37}$$

We have discussed the extension problem thoroughly above. One of the great achievements of 20th century mathematics is the complete classification of finite simple groups, so let us look at the finite simple groups:

First consider the abelian ones. These cannot have nontrivial subgroups and hence must be of the form $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

So, now we search for the nonabelian finite simple groups. A natural source of nonabelian groups are the symmetric groups S_n. Of course, these are not simple because $A_n \subset S_n$ are normal subgroups. Could the A_n be simple? The first nonabelian example is A_4 and it is not a simple group! Indeed, consider the cycle structures $(2)^2$. There are three nontrivial elements: (12)(34), (13)(24), and (14)(23), they are all involutions, and

$$((12)(34)) \cdot ((13)(24)) = ((13)(24)) \cdot ((12)(34)) = (14)(23) \tag{15.38}$$

and therefore together with the identity they form a subgroup $K \subset A_4$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Since cycle-structure is preserved under conjugation, this is obviously a normal subgroup of A_4!. After this unpromising beginning you might be surprised to learn:

Theorem A_n is a simple group for $n \geq 5$.

Sketch of the proof:

We first observe that A_n is generated by cycles of length three: (abc). The reason is that $(abc) = (ab)(bc)$, so any word in an even number of distinct transpositions can be rearranged into a word made from a product of cycles of length three. Therefore, the strategy is to show that any normal subgroup $K \subset A_n$ which is larger than 1 must contain at least one three-cycle (abc). WLOG let us say it is (123). Now we claim that the entire conjugacy class of three-cycles must be in K. We consider a permutation ϕ which takes

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix} \tag{15.39}$$

Then $\phi(123)\phi^{-1} = (ijk)$. If $\phi \in A_n$ we are done, since K is normal in A_n so then $(ijk) \in K$. If ϕ is an odd permutation then $\tilde{\phi} = \phi(45)$ is even and $\tilde{\phi}(123)\tilde{\phi}^{-1} = (ijk)$.

Thus, we need only show that some 3-cycle is in K. For $n = 5$ this can be done rather explicitly. See the exercise below. Once we have established that A_5 is simple we can proceed by induction as follows.

We first establish a lemma: If $n \geq 5$ then for any $\sigma \in A_n$, $\sigma \neq 1$ there is a conjugate element (in A_n) σ' with $\sigma' \neq \sigma$ such that there is an $i \in \{1, \dots, n\}$ so that $\sigma(i) = \sigma'(i)$.

To prove the lemma choose any $\sigma \neq 1$ and for σ choose a cycle of maximal length, say r so that $\sigma = (12 \dots r)\pi$ with π fixing $\{1, \dots, r\}$. If $r \geq 3$ then consider the conjugate:

$$\sigma' = (345)\sigma(345)^{-1} = (345)(123\cdots)\pi(354) \tag{15.40}$$

We see that $\sigma(1) = \sigma'(1) = 2$, while $\sigma(2) = 3$ and $\sigma'(2) = 4$. We leave the case $r = 2$ to the reader.

Now we proceed by induction: Suppose A_j is simple for $5 \leq j \leq n$. Consider A_{n+1} and let $N \lhd A_{n+1}$. Then choose $\sigma \in N$ and using the lemma consider $\sigma' \in A_{n+1}$ with $\sigma' \neq \sigma$ and $\sigma'(i) = \sigma(i)$ for some i. Let $H_i \subset A_{n+1}$ be the subgroup of permutations fixing i. It is isomorphic to A_n. Now, $\sigma' \in N$ since it is a conjugate of $\sigma \in N$ and N is assumed to be normal. Therefore $\sigma^{-1}\sigma' \in N$, and $\sigma^{-1}\sigma' \neq 1$. Therefore $N \cap H_i \neq 1$. But $N \cap H_i$ must be normal in H_i. Since $H_i \cong A_n$ it follows that $N \cap H_i = H_i$. But H_i contains 3-cycles. Therefore N contains 3-cycles and hence $N \cong A_{n+1}$. ♠

Remark: For several other proofs of the same theorem and other interesting related facts see

http://www.math.uconn.edu/kconrad/blurbs/grouptheory/Ansimple.pdf.

Digressive Remark: A group is called *solvable* if the G_i/G_{i+1} are abelian (and hence $\mathbb{Z}/p\mathbb{Z}$ for some prime p). The term has its origin in Galois theory, which in turn was the original genesis of group theory. Briefly, in Galois theory one considers a polynomial $P(x)$ with coefficients drawn from a field F. (e.g. consider $F = \mathbb{Q}$ or $\mathbb{R}$). Then the roots of the polynomial θ_i can be adjoined to F to produce a bigger field $K = F[\theta_i]$. The *Galois group of the polynomial* $Gal(P)$ is the group of automorphisms of K fixing F. Galois theory sets up a beautiful 1-1 correspondence between subgroups $H \subset Gal(P)$ and subfields $F \subset K_H \subset K$. The intuitive notion of solving a polynomial by radicals corresponds to finding a series of subfields $F \subset F_1 \subset F_2 \subset \cdots \subset K$ so that F_{i+1} is obtained from F_i by adjoining the solutions of an equation $y^d = z$. Under the Galois correspondence this translates into a composition series where $Gal(P)$ is a solvable group - hence the name. If we take $F = \mathbb{C}[a_0, \dots, a_{n-1}]$ for an n^{th} order polynomial

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{15.41}$$

then the roots θ_i are such that a_j are the j^{th} elementary symmetric polynomials in the θ_i (See Chapter 2 below). The Galois group is then S_n. For $n \geq 5$ the only nontrivial normal subgroup of S_n is A_n, and this group is simple, hence certainly not solvable. That is why there is no solution of an n^{th} order polynomial equation in radicals for $n \geq 5$.

Returning to our main theme, we ask: What other finite simple groups are there? The full list is known. The list is absolutely fascinating: [186]

1. $\mathbb{Z}/p\mathbb{Z}$ for p prime.
2. The subgroup $A_n \subset S_n$ for $n \geq 5$.
3. "Simple Lie groups over finite fields."
4. 26 "sporadic oddballs"

We won't explain example 3 in great detail, but it consists of a few more infinite sequences of groups, like 1,2 above. To get a flavor of what is involved note the following: The additive group $\mathbb{Z}/p\mathbb{Z}$ where p is prime has more structure: One can multiply elements, and if an element is nonzero then it has a multiplicative inverse, in other words, it is a *finite field.* One can therefore consider the group of invertible matrices over this field $GL(n,p)$, and its subgroup $SL(n,p)$ of matrices of unit determinant. Since $\mathbb{Z}/p\mathbb{Z}$ has a finite number of elements it is a finite group. This group is not simple, because it has a nontrivial center, in general. For example, if n is even then the group $\{\pm 1\}$ is a normal subgroup isomorphic to $\mathbb{Z}_2$. If we divide by the center the we get a group $PSL(n,p)$ which, it turns out, is indeed a simple group. This construction can be generalized in a few directions. First, there is a natural generalization of $\mathbb{Z}/p\mathbb{Z}$ to finite fields $\mathbb{F}_q$ of order a prime power $q = p^k$. Then we can similarly define $PSL(n,q)$ and it turns out these are simple groups except for some low values of n, q. Just as the Lie groups $SL(n,\mathbb{C})$ have counterparts $O(n), Sp(n)$ etc. one can generalize this construction to groups of type B, C, D, E. This construction can be used to obtain the third class of finite simple groups.

♣Double check. Does this figure leave out a subgroup relation? ♣

[186] See the *Atlas of Finite Simple Groups*, by Conway and Norton

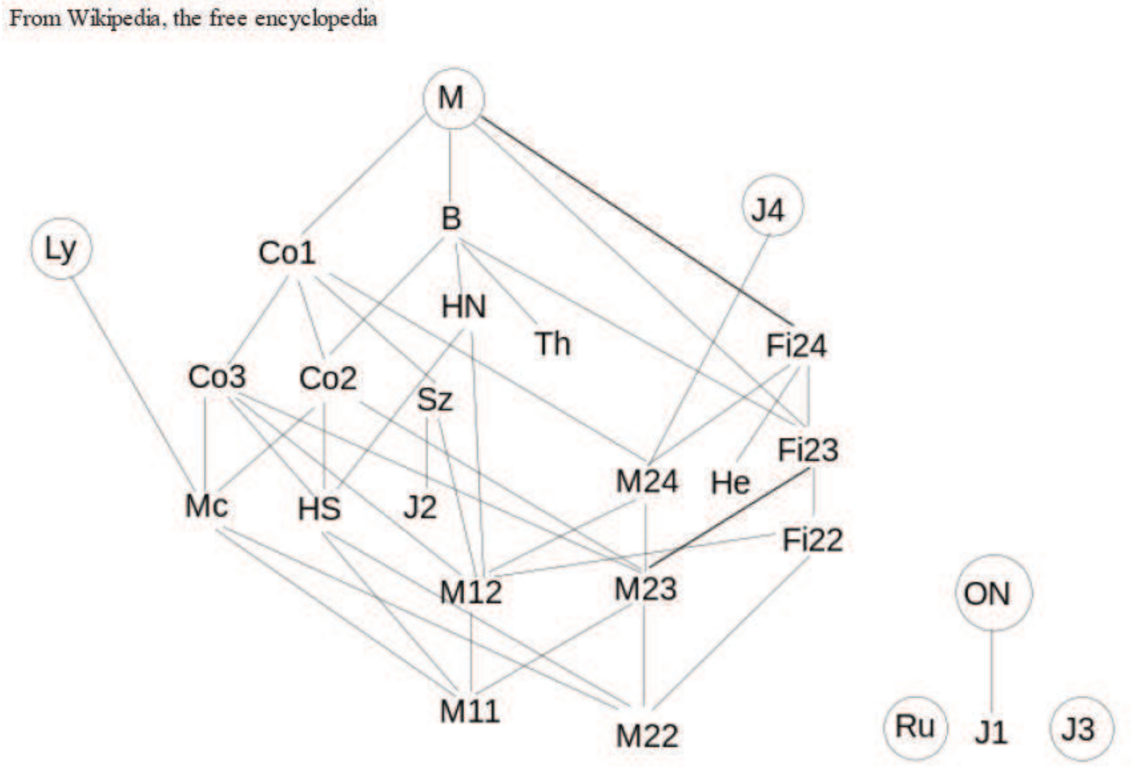

Figure 34: A table of the sporadic groups including subgroup relations. Source: Wikipedia.

It turns out that there are exactly 26 oddballs, known as the "sporadic groups." Some relationships between them are illustrated in Figure 34. The sporadic groups first showed up in the 19^{th} century via the Mathieu groups

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}. \tag{15.42}$$

M_n is a subgroup of the symmetric group S_n. M_{11}, which has order $|M_{11}| = 7920$ was discovered in 1861. We met M_{12} when discussing card-shuffling. The last group M_{24}, with order $\sim 10^9$ was discovered in 1873. All these groups may be understood as automorphisms of certain combinatorial objects called "Steiner systems."

It was a great surprise when Janko constructed a new sporadic group J_1 of order $175,560$ in 1965, roughly 100 years after the discovery of the Mathieu groups. The list of sporadic groups is now thought to be complete. The largest sporadic group is called the Monster group and its order is:

$$\begin{aligned}|Monster| &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &= 808017424794512875886459904961710757005754368000000000 \\ &\cong 8.08 \times 10^{53}\end{aligned} \tag{15.43}$$

but it has only 194 conjugacy classes! (Thus, by the class equation, it is "very" nonabelian. The center is trivial and $Z(g)$ tends to be a small order group.)

The history and status of the classification of finite simple groups is somewhat curious: [187]

1. The problem was first proposed by Hölder in 1892. Intense work on the classification begins during the 20th century.
2. Feit and Thompson show (1963) that any finite group of odd order is solvable. In particular, it cannot be a simple group.
3. Janko discovers (1965) the first new sporadic group in almost a century.
4. Progress is then rapid and in 1972 Daniel Gorenstein (of Rutgers University) announces a detailed outline of a program to classify finite simple groups.
5. The largest sporadic group, the Monster, was first shown to exist in 1980 by Fischer and Griess. It was explicitly constructed (as opposed to just being shown to exist) by Griess in 1982.
6. The proof is completed in 2004. It uses papers from hundreds of mathematicians between 1955 and 2004, and largely follows Gorenstein's program. The proof entails tens of thousands of pages. Errors and gaps have been found, but so far they are just "local."

Compared to the simple and elegant proof of the classification of simple Lie algebras (to be covered in Chapter **** below) the proof is obviously terribly unwieldy.

It is conceivable that physics might actually shed some light on this problem. The simple groups are probably best understood as automorphism groups of some mathematical, perhaps even geometrical object. For example, the first nonabelian simple group, A_5 is the group of symmetries of the icosahedron, as we will discuss in detail below. A construction of the monster along these lines was indeed provided by Frenkel, Lepowsky, Meurman, (at Rutgers) using vertex operator algebras, which are important in the description of perturbative string theory. More recently the mystery has deepened with interesting experimental discoveries linking the largest Mathieu group M_{24} to nonlinear sigma models with K3 target spaces. For more discussion about the possible role of physics in this subject see:

1. Articles by Griess and Frenkel et. al. in *Vertex Operators in Mathematics and Physics*, J. Lepowsky, S. Mandelstam, and I.M. Singer, eds.
2. J. Harvey, "Twisting the Heterotic String," in *Unified String Theories*, Green and Gross eds.

[187] Our source here is the Wikipedia article on the classification of finite simple groups. See also: Solomon, Ronald, "A brief history of the classification of the Finite simple groups," American Mathematical Society. Bulletin. New Series, 38 (3): 315-352 (2001).

3. L.J. Dixon, P.H. Ginsparg, and J.A. Harvey, "Beauty And The Beast: Superconformal Symmetry In A Monster Module," Commun.Math.Phys. 119 (1988) 221-241
4. M.C.N. Cheng, J.F.R. Duncan, and J.A. Harvey, "Umbral Moonshine," e-Print: arXiv:1204.2779 [math.RT]

Exercise *Completing the proof that A_5 is simple*

Show that any nontrivial normal subgroup of A_5 must contain a 3-cycle as follows:

a.) If $N \triangleleft A_5$ is a normal subgroup containing no 3-cycles then the elements must have cycle type $(ab)(cd)$ or $(abcde)$.

b.) Compute the group commutators (a, b, c, d, e are all distinct):

$$[(abe), (ab)(cd)] = (aeb) \tag{15.44}$$

$$[(abc), (abcde)] = (abd) \tag{15.45}$$

c.) Use these facts to conclude that N must contain a 3-cycle.

Legend has it that Galois discovered this theorem on the night before his fatal duel.

Exercise *Conjugacy classes in A_n*

Note that conjugacy classes in A_n are different from conjugacy classes in S_n. For example, (123) and (132) are not conjugate in A_3.

Describe the conjugacy classes in A_n.

Exercise *Jordan-Hölder decomposition*

Work out JH decompositions for the order 8 quaternion group $\widetilde{D}_2$ and observe that there are several maximal normal subgroups.

Exercise *The simplest of the Chevalley groups*

a.) Verify that $SL(2, \mathbb{Z}/p\mathbb{Z})$ is a group.

b.) Show that the order of $SL(2, \mathbb{Z}/p\mathbb{Z})$ is $p(p^2 - 1)$. [188]

[188] Break up the cases into $d = 0$ and $d \neq 0$. When $d = 0$ you can solve $ad - bc = 1$ for a. When $d = 0$ you can have arbitrary a but you must have $bc = -1$.

c.) Note that the scalar multiples of the 2×2 identity matrix form a normal subgroup of $SL(2, \mathbb{Z}/p\mathbb{Z})$. Show that the number of such matrices is the number of solutions of $x^2 = 1 \mathrm{mod} p$. Dividing by this normal subgroup produces the group $PSL(2, \mathbb{Z}/p\mathbb{Z})$. Jordan proved that these are simple groups for $p \neq 2, 3$.

It turns out that $PSL(2, \mathbb{Z}_5) \cong A_5$. (Check that the orders match.) Therefore the next simple group in the series is $PSL(2, \mathbb{Z}_7)$. It has many magical properties.

d.) Show that $PSL(2, \mathbb{Z}_7)$ has order 168.

---

16. Categories: Groups and Groupoids

A rather abstract notion, which nevertheless has found recent application in string theory and conformal field theory is the language of categories. Many physicists object to the high level of abstraction entailed in the category language. Some mathematicians even refer to the subject as "abstract nonsense." (Others take it very seriously.) However, it seems to be of increasing utility in the further formal development of string theory and supersymmetric gauge theory. It is also essential for reading any of the literature on topological field theory.

We briefly illustrate some of that language here. Our main point here is to introduce a different viewpoint on what groups are that leads to a significant generalization: groupoids. Moreover, this point of view also provides some very interesting insight into the meaning of group cohomology. Related constructions have been popular in condensed matter physics and topological field theory.

Definition A *category* $\mathcal{C}$ consists of

a.) A set $Ob(\mathcal{C})$ of "objects"

b.) A collection $Mor(\mathcal{C})$ of sets $\mathrm{hom}(X, Y)$, defined for any two objects $X, Y \in Ob(\mathcal{C})$. The elements of $\mathrm{hom}(X, Y)$ are called the "morphisms from X to Y." They are often denoted as arrows:

$$X \overset{\phi}{\to} Y \tag{16.1}$$

c.) A composition law:

$$\mathrm{hom}(X, Y) \times \mathrm{hom}(Y, Z) \to \mathrm{hom}(X, Z) \tag{16.2}$$

$$(\psi_1, \psi_2) \mapsto \psi_2 \circ \psi_1 \tag{16.3}$$

Such that

1. A morphism ϕ uniquely determines its source X and target Y. That is, $\mathrm{hom}(X, Y)$ are disjoint for distinct ordered pairs (X, Y).

2. $\forall X \in Ob(\mathcal{C})$ there is a distinguished morphism, denoted $1_X \in \mathrm{hom}(X, X)$ or $\mathrm{Id}_X \in \mathrm{hom}(X, X)$, which satisfies:

$$1_X \circ \phi = \phi \qquad \psi \circ 1_X = \psi \tag{16.4}$$

for all morphisms $\phi \in \mathrm{hom}(Y, X)$ and $\psi \in \mathrm{hom}(X, Y)$ for all $Y \in Ob(\mathcal{C})$. [189]

[189] As an exercise, show that these conditions uniquely determine the morphism 1_X.

3. Composition of morphisms is associative:

$$(\psi_1 \circ \psi_2) \circ \psi_3 = \psi_1 \circ (\psi_2 \circ \psi_3) \tag{16.5}$$

An alternative definition one sometimes finds is that a category is defined by two sets $\mathcal{C}_0$ (the objects) and $\mathcal{C}_1$ (the morphisms) with two maps $p_0 : \mathcal{C}_1 \to \mathcal{C}_0$ and $p_1 : \mathcal{C}_1 \to \mathcal{C}_0$. The map $p_0(f) = x_1 \in \mathcal{C}_0$ is the *range* map and $p_1(f) = x_0 \in \mathcal{C}_0$ is the *domain* map. In this alternative definition a category is then defined by a composition law on the set of *composable morphisms*

$$\mathcal{C}_2 = \{(f,g) \in \mathcal{C}_1 \times \mathcal{C}_1 | p_0(f) = p_1(g)\} \tag{16.6}$$

which is sometimes denoted $\mathcal{C}_{1p_1} \times_{p_0} \mathcal{C}_1$ and called the *fiber product.* The composition law takes $\mathcal{C}_2 \to \mathcal{C}_1$ and may be pictured as the composition of arrows. If $f : x_0 \to x_1$ and $g : x_1 \to x_2$ then the composed arrow will be denoted $g \circ f : x_0 \to x_2$. The composition law satisfies the axioms

1. For all $x \in X_0$ there is an identity morphism in X_1, denoted 1_x, or Id_x, such that $1_x f = f$ and $g 1_x = g$ for all suitably composable morphisms f, g.
2. The composition law is associative. If f, g, h are 3-composable morphisms then $(hg)f = h(gf)$.

Remarks:

1. When defining composition of arrows one needs to make an important notational decision. If $f : x_0 \to x_1$ and $g : x_1 \to x_2$ then the composed arrow is an arrow $x_0 \to x_2$. We will write $g \circ f$ when we want to think of f, g as functions and fg when we think of them as arrows.

♣Is this dual notation really a good idea?? ♣

2. It is possible to endow the data X_0, X_1 and p_0, p_1 with additional structures, such as topologies, and demand that p_0, p_1 have continuity or other properties.
3. A morphism $\phi \in \hom(X,Y)$ is said to be *invertible* if there is a morphism $\psi \in \hom(Y,X)$ such that $\psi \circ \phi = 1_X$ and $\phi \circ \psi = 1_Y$. If X and Y are objects with an invertible morphism between them then they are called *isomorphic objects.* One key reason to use the language of categories is that objects can have nontrivial automorphisms. That is, $\hom(X,X)$ can have invertible elements other than just 1_X in it. When this is true then it is tricky to speak of "equality" of objects, and the language of categories becomes very helpful. As a concrete example you might ponder the following question: "Are all real vector spaces of dimension n *the same*?"

Here are some simple examples of categories:

1. **SET**: The category of sets and maps of sets. [190]

[190] We take an appropriate collection of sets and maps to avoid the annoying paradoxes of set theory.

2. **TOP**: The category of topological spaces and continuous maps.

3. **TOPH**: The category of topological spaces and homotopy classes of continuous maps.

4. **MANIFOLD**: The category of manifolds and suitable maps. We could take topological manifolds and continuous maps of manifolds. Or we could take smooth manifolds and smooth maps as morphisms. The two choices lead to two (very different!) categories.

5. **BORD**(n): The bordism category of n-dimensional manifolds. Roughly speaking, the objects are n-dimensional manifolds without boundary and the morphisms are bordisms. A bordism Y from an n-manifold M_1 to and n-manifold M_2 is an $(n+1)$-dimensional manifold with a decomposition of its boundary $\partial Y = (\partial Y)_{in} \amalg (\partial Y)_{out}$ together with diffeomorphisms $\theta_1 : (\partial Y)_{in} \to M_1$ and $\theta_2 : (\partial Y)_{out} \to M_2$.

6. **GROUP**: the category of groups and homomorphisms of groups. Note that here if we took our morphisms to be isomorphisms instead of homomorphisms then we would get a very different category. All the pairs of objects in the category with nontrivial morphism spaces between them would be pairs of isomorphic groups.

7. **AB**: The (sub) category of abelian groups.

8. Fix a group G and let **G-SET** be the category of G-sets, that is, sets X with a G-action. For simplicity let us just write the G-action $\Phi(g, x)$ as $g \cdot x$ for x a point in a G-set X. We take the morphisms $f : X_1 \to X_2$ to satisfy satisfy $f(g \cdot x_1) = g \cdot f(x_1)$.

9. **VECT**$_\kappa$: The category of finite-dimensional vector spaces over a field κ with morphisms the linear transformations.

One use of categories is that they provide a language for describing precisely notions of "similar structures" in different mathematical contexts. When discussed in this way it is important to introduce the notion of "functors" and "natural transformations" to speak of interesting relationships between categories.

In order to state a relation between categories one needs a "map of categories." This is what is known as a functor:

Definition A *functor* between two categories $\mathcal{C}_1$ and $\mathcal{C}_2$ consists of a pair of maps $F_{\rm obj} : Obj(\mathcal{C}_1) \to Obj(\mathcal{C}_2)$ and $F_{\rm mor} : Mor(\mathcal{C}_1) \to Mor(\mathcal{C}_2)$ so that if

$$x \xrightarrow{f} y \ \in \hom(x, y) \tag{16.7}$$

then

$$F_{\rm obj}(x) \xrightarrow{F_{\rm mor}(f)} F_{\rm obj}(y) \ \in \hom(F_{\rm obj}(x), F_{\rm obj}(y)) \tag{16.8}$$

and moreover we require that $F_{\rm mor}$ should be compatible with composition of morphisms: There are two ways this can happen. If f_1, f_2 are composable morphisms then we say F is a *covariant functor* if

$$F_{\rm mor}(f_1 \circ f_2) = F_{\rm mor}(f_1) \circ F_{\rm mor}(f_2) \tag{16.9}$$

and we say that F is a *contravariant functor* if

$$F_{\rm mor}(f_1 \circ f_2) = F_{\rm mor}(f_2) \circ F_{\rm mor}(f_1) \tag{16.10}$$

In both cases we also require [191]

$$F_{\rm mor}({\rm Id}_X) = {\rm Id}_{F(X)} \tag{16.11}$$

We usually drop the subscript on F since it is clear what is meant from context.

Exercise

Using the alternative definition of a category in terms of data $p_{0,1} : X_1 \to X_0$ define the notion of a functor writing out the relevant commutative diagrams.

Exercise *Opposite Category*

If $\mathcal{C}$ is a category then the *opposite category* $\mathcal{C}^{\rm opp}$ is defined by just reversing all arrows. More formally: The set of objects is the same and

$$\hom_{\mathcal{C}^{\rm opp}}(X, Y) := \hom_{\mathcal{C}}(Y, X) \tag{16.12}$$

so for every morphism $f \in \hom_{\mathcal{C}}(Y, X)$ we associate $f^{\rm opp} \in \hom_{\mathcal{C}^{\rm opp}}(X, Y)$ such that

$$f_1 \circ_{\mathcal{C}^{\rm opp}} f_2 = (f_2 \circ_{\mathcal{C}} f_1)^{\rm opp} \tag{16.13}$$

a.) Show that if $F : \mathcal{C} \to \mathcal{D}$ is a contravariant functor then one can define in a natural way a covariant functor $F : \mathcal{C}^{\rm opp} \to \mathcal{D}$.

b.) Show that if $F : \mathcal{C} \to \mathcal{D}$ is a covariant functor then we can naturally define another covariant functor $F^{\rm opp} : \mathcal{C}^{\rm opp} \to \mathcal{D}^{\rm opp}$

Example 1: Every category has a canonical functor to itself, called the identity functor $Id_{\mathcal{C}}$.

Example 2: There is an obvious functor, the *forgetful functor* from **GROUP** to **SET**. This idea extends to many other situations where we "forget" some mathematical structure and map to a category of more primitive objects.

[191] Although we do have $F_{\rm mor}({\rm Id}_X) \circ F_{\rm mor}(f) = F_{\rm mor}(f)$ for all $f \in \hom(Y, X)$ and $F_{\rm mor}(f) \circ F_{\rm mor}({\rm Id}_X) = F_{\rm mor}(f)$ for all $f \in \hom(X, Y)$ this is not the same as the statement that $F_{\rm mor}({\rm Id}_X) \circ \phi = \phi$ for all $\phi \in \hom(F(Y), F(X))$, so we need to impose this extra axiom.

Example 3: Since **AB** is a subcategory of **GROUP** there is an obvious functor $\mathcal{F}$: **AB** → **GROUP**.

Example 4: In an exercise below you are asked to show that the abelianization of a group defines a functor $\mathcal{G}$: **GROUP** → **AB**.

Example 5: Fix a group G. Then in the notes above we have on several occasions used the functor

$$F_G : \mathbf{SET} \to \mathbf{GROUP} \tag{16.14}$$

by observing that if X is a set, then $F_G(X) = Maps[X \to G]$ is a group. Check this is a contravariant functor: If $f : X_1 \to X_2$ is a map of sets then

$$F_G(X_1) \xleftarrow{F_G(f)} F_G(X_2) \tag{16.15}$$

The map $F_G(f)$ is usually denoted f^* and is known as the *pull-back*. To be quite explicit: If Ψ is a map of $X_2 \to G$ then $f^*(\Psi) := \Psi \circ f$ is a map $X_1 \to G$.

This functor is used in the construction of certain *nonlinear sigma models* which are quantum field theories where the target space is a group G. The viewpoint that we are studying the representation theory of an infinite-dimensional group of maps to G has been extremely successful in a particular case of the *Wess-Zumino-Witten* model, a certain two dimensional quantum field theory that enjoys conformal invariance (and more).

Example 6: Now let us return to the category **G-SET**. Now fix any set Y. Then in the notes above we have on several occasions used the functor

$$F_{G,Y} : \mathbf{G\text{-}SET} \to \mathbf{G\text{-}SET} \tag{16.16}$$

by observing that if X is a G-set, then $F_Y(X) = Maps[X \to Y]$ is also a G-set. To check this is a contravariant functor we write:

$$\begin{aligned}
[g \cdot (f^*\Psi)](x_1) &= (f^*\Psi)(g^{-1} \cdot x_1) \\
&= \Psi(f(g^{-1} \cdot x_1)) \\
&= \Psi(g^{-1} \cdot (f(x_1))) \\
&= (g \cdot \Psi)(f(x_1)) \\
&= (f^*(g \cdot \Psi))(x_1)
\end{aligned} \tag{16.17}$$

and hence $\Psi \to g \cdot \Psi$ is a morphism of G-sets.

This functor is ubiquitous in quantum field theory: If a spacetime enjoys some symmetry (for example rotational or Poincaré symmetry) then the same group will act on the space of fields defined on that spacetime.

Example 7: Fix a nonnegative integer n and a group G. Then the group cohomology we discussed above (take the trivial twisting $\omega_g = \mathrm{Id}_A$ for all g) defines a covariant functor

$$H^n(G, \bullet) : \mathbf{AB} \to \mathbf{AB} \tag{16.18}$$

To check this is really a functor we need to observe the following: If $\varphi : A_1 \to A_2$ is a homomorphism of Abelian groups then there is an induced homomorphim, usually denoted

$$\varphi_* : H^n(G, A_1) \to H^n(G, A_2) \tag{16.19}$$

You have to check that $\mathrm{Id}_* = \mathrm{Id}$ and

$$(\varphi_1 \circ \varphi_2)_* = (\varphi_1)_* \circ (\varphi_2)_* \tag{16.20}$$

Strictly speaking we should denote φ_* by $H^n(G, \varphi)$, but this is too fastidious for the present author.

Example 8: Fix a nonnegative integer n and any group A. Then the group cohomology we discussed above (take the trivial twisting $\omega_g = \mathrm{Id}_A$ for all g) defines a contravariant functor

$$H^n(\bullet, A) : \mathbf{GROUP} \to \mathbf{AB} \tag{16.21}$$

To check this is really a functor we need to observe the following: If $\varphi : G_1 \to G_2$ is a homomorphism of Abelian groups then there is an induced homomorphim, usually denoted φ^*

$$\varphi^* : H^n(G_2, A) \to H^n(G_1, A) \tag{16.22}$$

Example 9: *Topological Field Theory.* The very definition of topological field theory is that it is a functor from a bordism category of manifolds to the category of vector spaces and linear transformations. For much more about this one can consult a number of papers. Two online resources are

http://www.physics.rutgers.edu/∼gmoore/695Fall2015/TopologicalFieldTheory.pdf
https://www.ma.utexas.edu/users/dafr/bordism.pdf

Note that in example 2 there is no obvious functor going the reverse direction. When there are functors both ways between two categories we might ask whether they might be, in some sense, "the same." But saying precisely what is meant by "the same" requires some care.

Definition If $\mathcal{C}_1$ and $\mathcal{C}_2$ are categories and $F_1 : \mathcal{C}_1 \to \mathcal{C}_2$ and $F_2 : \mathcal{C}_1 \to \mathcal{C}_2$ are two functors then a *natural transformation* $\tau : F_1 \to F_2$ is a rule which, for every $X \in Obj(\mathcal{C}_1)$ assigns an arrow $\tau_X : F_1(X) \to F_2(X)$ so that, for all $X, Y \in Obj(\mathcal{C}_1)$ and all $f \in \hom(X, Y)$,

$$\tau_Y \circ F_1(f) = F_2(f) \circ \tau_X \tag{16.23}$$

Or, in terms of diagrams.

$$\begin{tikzcd} F_1(X) \arrow[r, "F_1(f)"] \arrow[d, "\tau_X"] & F_1(Y) \arrow[d, "\tau_Y"] \\ F_2(X) \arrow[r, "F_2(f)"] & F_2(Y) \end{tikzcd} \tag{16.24}$$

Example 1: *The evaluation map.* Here is another tautological construction which nevertheless can be useful. Let S be any set and define a functor

$$F_S : \mathbf{SET} \to \mathbf{SET} \tag{16.25}$$

by saying that on objects we have

$$F_S(X) := Map[S \to X] \times S \tag{16.26}$$

and if $\varphi : X_1 \to X_2$ is a map of sets then

$$F_S(\varphi) : Map[S \to X_1] \times S \to Map[S \to X_2] \times S \tag{16.27}$$

is defined by $F_S(\varphi) : (f, s) \mapsto (\varphi \circ f, s)$. Then we claim there is a natural transformation to the identity functor. For every set X we have

$$\tau_X : F_S(X) = Map[S \to X] \times S \to \mathrm{Id}(X) = X \tag{16.28}$$

It is defined by $\tau_X(f, s) := f(s)$. This is known as the "evaluation map." Then we need to check

$$\begin{tikzcd} F_S(X) \arrow[r, "\tau_X"] \arrow[d, "F_S(\varphi)"] & X \arrow[d, "\varphi"] \\ F_S(Y) \arrow[r, "\tau_Y"] & Y \end{tikzcd} \tag{16.29}$$

commutes. If you work it out, it is just a tautology.

Example 2: *The determinant.* [192] Let **COMMRING** be the category of commutative rings with morphisms the ring morphisms. (So, $\varphi : R_1 \to R_2$ is a homomorphism of Abelian groups and moreover $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$.) Let us consider two functors

$$\mathbf{COMMRING} \to \mathbf{GROUP} \tag{16.30}$$

The first functor F_1 maps a ring R to the multiplicative group $U(R)$ of multiplicatively invertible elements. This is often called the group of units in R. If φ is a morphism of rings and $r \in U(R_1)$ then $\varphi(r) \in U(R_2)$ and the map $\varphi_* : U(R_1) \to U(R_2)$ defined by

$$\varphi_* : r \mapsto \varphi(r) \tag{16.31}$$

is a group homomorphism. So F_1 is a functor. The second functor F_2 maps a ring R to the matrix group $GL(n, R)$ of $n \times n$ matrices such that there exists an inverse matrix with values in R. Again, if $\varphi : R_1 \to R_2$ is a morphism then applying φ to each matrix element defines a group homomorphism $\varphi_* : GL(n, R_1) \to GL(n, R_2)$. Now consider the determinant of a matrix $g \in GL(n, R)$. The usual formula

$$\det(g) := \sum_{\sigma \in S_n} \epsilon(\sigma) g_{1,\sigma(1)} \cdot g_{2,\sigma(2)} \cdots g_{n,\sigma(n)} \tag{16.32}$$

[192] This example uses some terms from linear algebra which can be found in the "User's Manual," Chapter 2 below.

makes perfect sense for $g \in GL(n,R)$. Moreover,

$$\det(g_1 g_2) = \det(g_1)\det(g_2) \tag{16.33}$$

Now we claim that the determinant defines a natural transformation $\tau : F_1 \to F_2$. For each object $R \in Ob(\mathbf{COMMRING})$ we assign the morphism

$$\tau_R : GL(n,R) \to U(R) \tag{16.34}$$

defined by $\tau_R(g) := \det(g)$. Thanks to (16.33) this is indeed a morphism in the category **GROUP**, that is, it is a group homomorphism. Moreover, it satisfies the required commutative diagram because if $\varphi : R_1 \to R_2$ is a morphism of rings then

$$\varphi_*(\det(g)) = \det(\varphi_*(g)). \tag{16.35}$$

Example 3: *Natural transformations in cohomology theory.* Cohomology groups provide natural examples of functors, as we have stressed above. There are a number of interesting natural transformations between these different cohomology-group functors.

♣Can we explain an elementary example with group cohomology as developed so far??? ♣

Definition Two categories are said to be *equivalent* if there are functors $F : \mathcal{C}_1 \to \mathcal{C}_2$ and $G : \mathcal{C}_2 \to \mathcal{C}_1$ together with isomorphisms (via natural transformations) $FG \cong Id_{\mathcal{C}_2}$ and $GF \cong Id_{\mathcal{C}_1}$. (Note that FG and $Id_{\mathcal{C}_2}$ are both objects in the category of functors FUNCT$(\mathcal{C}_2, \mathcal{C}_2)$ so it makes sense to say that they are isomorphic.)

Many important theorems in mathematics can be given an elegant and concise formulation by saying that two seemingly different categories are in fact equivalent. Here is a (very selective) list: [193]

♣Should explain example showing category of finite-dimensional vector spaces over a field is equivalent to the catetgory of nonnegative integers. ♣

Example 1: Consider the category with one object for each nonnegative integer n and the morphism space $GL(n,\kappa)$ of invertible $n \times n$ matrices over the field κ. These categories are equivalent. That is one way of saying that the only invariant of a finite-dimensional vector space is its dimension.

Example 2: The basic relation between Lie groups and Lie algebras the statement that the functor which takes a Lie group G to its tangent space at the identity, $T_1 G$ is an equivalence of the category of connected and simply-connected Lie groups with the category of finite-dimensional Lie algebras. One of the nontrivial theorems in the theory is the existence of a functor from the category of finite-dimensional Lie algebras to the category of connected and simply-connected Lie groups. Intuitively, it is given by exponentiating the elements of the Lie algebra.

Example 3: Covering space theory is about an equivalence of categories. On the one hand we have the category of coverings of a pointed space (X, x_0) and on the other hand

[193] I thank G. Segal for a nice discussion that helped prepare this list.

the category of topological spaces with an action of the group $\pi_1(X, x_0)$. Closely related to this, Galois theory can be viewed as an equivalence of categories.

Example 4: The category of unital commutative C^*-algebras is equivalent to the category of compact Hausdorff topological spaces. This is known as Gelfand's theorem.

Example 5: Similar to the previous example, an important point in algebraic geometry is that there is an equivalence of categories of commutative algebras over a field κ (with no nilpotent elements) and the category of affine algebraic varieties.

Example 6: Pontryagin duality is a nontrivial self-equivalence of the category of locally compact abelian groups (and continuous homomorphisms) with itself.

Example 7: A generalization of Pontryagin duality is Tannaka-Krein duality between the category of compact groups and a certain category of linear tensor categories. (The idea is that, given an abstract tensor category satisfying certain conditions one can construct a group, and if that tensor category is the category of representations of a compact group, one recovers that group.)

Example 8: The Riemann-Hilbert correspondence can be viewed as an equivalence of categories of flat connections (a.k.a. linear differential equations, a.k.a. D-modules) with their monodromy representations.

♣This needs a lot more explanation. ♣

In physics, the statement of "dualities" between different physical theories can sometimes be formulated precisely as an equivalence of categories. One important example of this is mirror symmetry, which asserts an equivalence of (A_∞)-) categories of the derived category of holomorphic bundles on X and the Fukaya category of Lagrangians on $X^\vee$. But more generally, nontrivial duality symmetries in string theory and field theory have a strong flavor of an equivalence of categories.

Exercise *Playing with natural transformations*

a.) Given two categories $\mathcal{C}_1, \mathcal{C}_2$ show that the natural transformations allow one to define a category FUNCT$(\mathcal{C}_1, \mathcal{C}_2)$ whose objects are functors from $\mathcal{C}_1$ to $\mathcal{C}_2$ and whose morphisms are natural transformations. For this reason natural transformations are often called "morphisms of functors."

b.) Write out the meaning of a natural transformation of the identity functor $Id_{\mathcal{C}}$ to itself. Show that $End(Id_{\mathcal{C}})$, the set of all natural transformations of the identity functor to itself is a monoid.

Exercise *Freyd's theorem*

A "practical" way to tell if two categories are equivalent is the following:

By definition, a *fully faithful functor* is a functor $F : \mathcal{C}_1 \to \mathcal{C}_2$ where $F_{\rm mor}$ is a bijection on all the hom-sets. That is, for all $X, Y \in Obj(\mathcal{C}_1)$ the map

$$F_{\rm mor} : {\rm hom}(X, Y) \to {\rm hom}(F_{\rm obj}(X), F_{\rm obj}(Y)) \tag{16.36}$$

is a bijection.

Show that $\mathcal{C}_1$ is equivalent to $\mathcal{C}_2$ iff there is a fully faithful functor $F : \mathcal{C}_1 \to \mathcal{C}_2$ so that any object $\alpha \in Obj(\mathcal{C}_2)$ is isomorphic to an object of the form $F(X)$ for some $X \in Obj(\mathcal{C}_1)$.

Exercise

As we noted above, there is a functor **AB** → **GROUP** just given by inclusion.

a.) Show that the abelianization map $G \to G/[G, G]$ defines a functor **GROUP** → **AB**.

b.) Show that the existence of nontrivial perfect groups, such as A_5, implies that this functor cannot be an equivalence of categories.

In addition to the very abstract view of categories we have just sketched, very concrete objects, like groups, manifolds, and orbifolds can profitably be viewed as categories.

One may always picture a category with the objects constituting points and the morphisms directed arrows between the points as shown in Figure 35.

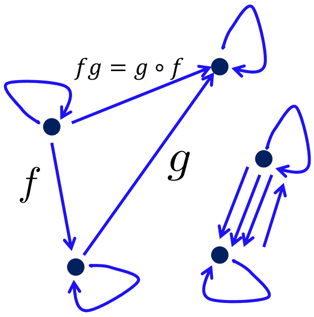

Figure 35: Pictorial illustration of a category. The objects are the black dots. The arrows are shown, and one must give a rule for composing each arrow and identifying with one of the other arrows. For example, given the arrows denoted f and g it follows that there must be an arrow of the type denoted $f \circ g$. Note that every object x has at least one arrow, the identity arrow in $Hom(x, x)$.

As an extreme example of this let us consider a category with only *one object*, but we allow the possibility that there are several morphisms. For such a category let us look carefully at the structure on morphisms $f \in Mor(\mathcal{C})$. We know that there is a binary operation, with an identity 1 which is associative.

But this is just the definition of a monoid!

If we have in addition inverses then we get a group. Hence:

Definition A *group* is a category with one object, all of whose morphisms are invertible.

To see that this is equivalent to our previous notion of a group we associate to each morphism a group element. Composition of morphisms is the group operation. The invertibility of morphisms is the existence of inverses.

We will briefly describe an important and far-reaching generalization of a group afforded by this viewpoint. Then we will show that this viewpoint leads to a nice geometrical construction making the formulae of group cohomology a little bit more intuitive.

****

CONSTRUCT EXERCISE HERE EXAMINING HOW CONCEPTS OF FUNCTORS AND NATURAL TRANSFORMATIONS TRANSLATE INTO GROUP THEORY LANGUAGE WHEN SPECIALIZED TO THE CATEGORIES CORRESPONDING TO GROUPS

****

16.1 Groupoids

Definition A *groupoid* is a category all of whose morphisms are invertible.

Note that for any object x in a groupoid, $\hom(x, x)$ is a group. It is called the *automorphism group* of the object x.

Example 1. Any equivalence relation on a set X defines a groupoid. The objects are the elements of X. The set $\mathrm{Hom}(a, b)$ has one element if $a \sim b$ and is empty otherwise. The composition law on morphisms then means that $a \sim b$ with $b \sim c$ implies $a \sim c$. Clearly, every morphism is invertible.

Example 2. Consider time evolution in quantum mechanics with a time-dependent Hamiltonian. There is no sense to time evolution $U(t)$. Rather one must speak of unitary evolution $U(t_1, t_2)$ such that $U(t_1, t_2)U(t_2, t_3) = U(t_1, t_3)$. Given a solution of the Schrodinger equation $\Psi(t)$ we may consider the state vectors $\Psi(t)$ as objects and $U(t_1, t_2)$ as morphisms. In this way a solution of the Schrodinger equation defines a groupoid.

♣Clarify this remark. ♣

Example 3. Let X be a topological space. The fundamental groupoid $\pi_{\leq 1}(X)$ is the category whose objects are points $x \in X$, and whose morphisms are homotopy classes of paths $f : x \to x'$. These compose in a natural way. Note that the automorphism group of a point $x \in X$, namely, $\hom(x, x)$ is the fundamental group of X based at x, $\pi_1(X, x)$.

Example 4. Gauge theory: Objects = connections on a principal bundle. Morphisms = gauge transformations. This is the right point of view for thinking about some more exotic (abelian) gauge theories of higher degree forms which arise in supergravity and string theories.

Example 5. In the theory of string theory orbifolds and orientifolds spacetime must be considered to be a groupoid. Suppose we have a right action of G on a set X, so we have a map

$$\Phi : X \times G \to X \tag{16.37}$$

such that

$$\Phi(\Phi(x, g_1), g_2) = \Phi(x, g_1 g_2) \tag{16.38}$$

$$\Phi(x, 1_G) = x \tag{16.39}$$

for all $x \in X$ and $g_1, g_2 \in G$. We can just write $\Phi(x, g) := x \cdot g$ for short. We can then form the category $X//G$ with

$$\begin{aligned} Ob(X//G) &= X \\ Mor(X//G) &= X \times G \end{aligned} \tag{16.40}$$

We should think of a morphism as an arrow, labeled by g, connecting the point x to the point $x \cdot g$. The target and source maps are:

♣FIGURE NEEDED HERE! ♣

$$p_0((x, g)) := x \cdot g \qquad\qquad p_1((x, g)) := x \tag{16.41}$$

The composition of morphisms is defined by

$$(xg_1, g_2) \circ (x, g_1) := (x, g_1 g_2) \tag{16.42}$$

or, in the other notation (better suited to a right-action):

$$(x, g_1)(xg_1, g_2) := (x, g_1 g_2) \tag{16.43}$$

Note that $(x, 1_G) \in \hom(x, x)$ is the identity morphism, and the composition of morphisms makes sense because we have a group action. Also note that $pt//G$ where G has the trivial action on a point realizes the group G as a category, as sketched above.

Example 6. In the theory of string theory orbifolds and orientifolds spacetime must be considered to be a groupoid. (This is closely related to the previous example.)

Exercise

For a group G let us define a groupoid denoted $G//G$ (for reasons explained later) whose objects are group elements $Obj(G//G) = G$ and whose morphisms are arrows defined by

$$g_1 \xrightarrow{h} g_2 \tag{16.44}$$

iff $g_2 = h^{-1} g_1 h$. This is the groupoid of principal G-bundles on the circle.

Draw the groupoid corresponding to S_3.

Exercise *The Quotient Groupoid*

a.) Show that whenever G acts on a set X one can canonically define a groupoid: The objects are the points $x \in X$. The morphisms are pairs (g, x), to be thought of as arrows $x \xrightarrow{g} g \cdot x$. Thus, $X_0 = X$ and $X_1 = G \times X$.

b.) What is the automorphism group of an object $x \in X$.

This groupoid is commonly denoted as $X//G$.

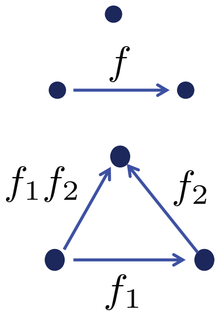

Figure 36: Elementary $0, 1, 2$ simplices in the simplicial space $|\mathcal{C}|$ of a category

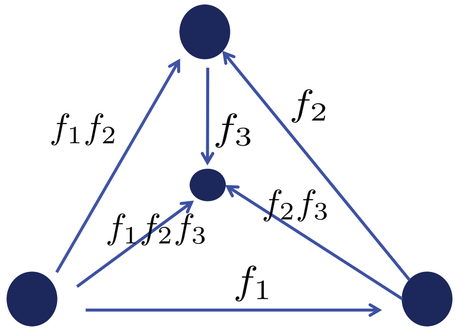

Figure 37: An elementary 3-simplex in the simplicial space $|\mathcal{C}|$ of a category

16.2 The topology behind group cohomology

Now, let us show that this point of view on the definition of a group can lead to a very nontrivial and beautiful structure associated with a group.

An interesting construction that applies to any category is its associated simplicial space $|\mathcal{C}|$.

This is a space made by gluing together simplices [194] whose simplices are:

- 0-simplices = objects
- 1-simplices = $\Delta_1(f)$ associated to each morphism $f : x_0 \to x_1 \in X_1$.
- 2-simplices: $\Delta(f_1, f_2)$ associated composable morphisms

$$(f_1, f_2) \in X_2 := \{(f_1, f_2) \in X_1 \times X_1 | p_0(f_1) = p_1(f_2)\} \tag{16.45}$$

- 3-simplices: $\Delta(f_1, f_2, f_3)$ associated to 3 composable morphisms, i.e. elements of:

$$X_3 = \{(f_1, f_2, f_3) \in X_1 \times X_1 \times X_1 | p_0(f_i) = p_1(f_{i+1}), i = 1, 2\} \tag{16.46}$$

- and so on. There are infinitely many simplices of arbitarily high dimension because we can keep composing morphisms as long as we like.

And so on. See Figures 36 and 37. The figures make clear how these simplices are glued together:

$$\partial\Delta_1(f) = x_1 - x_0 \tag{16.47}$$

$$\partial\Delta_2(f_1, f_2) = \Delta_1(f_1) - \Delta_1(f_1 f_2) + \Delta_1(f_2) \tag{16.48}$$

and for Figure 37 view this as looking down on a tetrahedron. Give the 2-simplices of Figure 36 the counterclockwise orientation and the boundary of the 3-simplex the induced orientation from the outwards normal. Then we have

$$\partial\Delta(f_1, f_2, f_3) = \Delta(f_2, f_3) - \Delta(f_1 f_2, f_3) + \Delta(f_1, f_2 f_3) - \Delta(f_1, f_2) \tag{16.49}$$

Note that on the three upper faces of Figure 37 the induced orientation is the ccw orientation for $\Delta(f_1, f_2 f_3)$ and $\Delta(f_2, f_3)$, but with the cw orientation for $\Delta(f_1 f_2, f_3)$. On the bottom fact the inward orientation is ccw and hence the outward orientation is $-\Delta(f_1, f_2)$.

Clearly, we can keep composing morphisms so the space $|\mathcal{C}|$ has simplices of arbitrarily high dimension, that is, it is an infinite-dimensional space.

Let look more closely at this space for the case of a group, regarded as a category with one object. Then in the above pictures we identify all the vertices with a single vertex.

For each group element g we have a one-simplex $\Delta_1(g)$ beginning and ending at this vertex.

For each ordered pair (g_1, g_2) we have an oriented 2-simplex $\Delta(g_1, g_2)$, etc. We simply replace $f_i \to g_i$ in the above formulae, with g_i now interpreted as elements of G:

$$\partial\Delta(g) = 0 \tag{16.50}$$

$$\partial\Delta(g_1, g_2) = \Delta_1(g_1) + \Delta_1(g_2) - \Delta_1(g_1 g_2) \tag{16.51}$$

[194] Technically, it is a *simplicial space.*

$$\partial\Delta(g_1,g_2,g_3) = \Delta(g_2,g_3) - \Delta(g_1g_2,g_3) + \Delta(g_1,g_2g_3) - \Delta(g_1,g_2) \tag{16.52}$$

See Figure 37.

Let us construct this topological space a bit more formally:

We begin by defining $n+1$ maps from $G^n \to G^{n-1}$ for $n \geq 1$ given by

$$\begin{aligned} d^0(g_1,\dots,g_n) &= (g_2,\dots,g_n) \\ d^1(g_1,\dots,g_n) &= (g_1g_2,g_3,\dots,g_n) \\ d^2(g_1,\dots,g_n) &= (g_1,g_2g_3,g_4,\dots,g_n) \\ &\cdots\cdots \\ &\cdots\cdots \\ d^{n-1}(g_1,\dots,g_n) &= (g_1,\dots,g_{n-1}g_n) \\ d^n(g_1,\dots,g_n) &= (g_1,\dots,g_{n-1}) \end{aligned} \tag{16.53}$$

On the other hand, we can view an n-simplex Δ_n as

$$\Delta_n := \{(t_0,t_1,\dots,t_n) | t_i \geq 0 \qquad \& \qquad \sum_{i=0}^{n} t_i = 1\} \tag{16.54}$$

Now, there are also $(n+1)$ *face maps* which map an $(n-1)$-simplex Δ_{n-1} into one of the $(n+1)$ faces of the n-simplex Δ_n:

$$\begin{aligned} d_0(t_0,\dots,t_{n-1}) &= (0,t_0,\dots,t_{n-1}) \\ d_1(t_0,\dots,t_{n-1}) &= (t_0,0,t_1,\dots,t_{n-1}) \\ &\cdots\cdots \\ &\cdots\cdots \\ d_n(t_0,\dots,t_{n-1}) &= (t_0,\dots,t_{n-1},0) \end{aligned} \tag{16.55}$$

d_i embeds the $(n-1)$ simplex into the face $t_i = 0$ which is opposite the i^{th} vertex $t_i = 1$ of Δ_n.

Now we identify [195]

$$(\amalg_{n=0}^{\infty} \Delta_n \times G^n) \,/\, \sim$$

via

$$(d_i(\vec{t}), \vec{g}) \sim (\vec{t}, d^i(\vec{g})). \tag{16.56}$$

The space we have constructed this way has a homotopy type denoted BG. This homotopy type is known as the *classifying space of the group G*. It can be characterized as the homotopy type of a topological space which is both contractible and admits a free G-action.

Note that for all $g \in G$, $\partial\Delta_1(g) = 0$, so for each group element there is a closed loop. On the other hand

$$\Delta_1(1_G) = \partial(\Delta_2(1_G,1_G)) \tag{16.57}$$

[195] This means we take the set of equivalence classes and impose the weakest topology on the set of equivalence classes so that the projection map is continuous.

so $\Delta_1(1_G)$ is a contractible loop. But all other loops are noncontractible. (Show this!) Therefore:

$$\pi_1(BG,*) \cong G \tag{16.58}$$

Moreover, if G is a finite group one can show that all the higher homotopy groups of BG are contractible. So then BG is what is known as an *Eilenberg MacLane space* $K(G,1)$.

Even for the simplest nontrivial group $G = \mathbb{Z}/2\mathbb{Z}$ the construction is quite nontrivial and BG has the homotopy type of $\mathbb{R}P^\infty$.

Now, an n-cochain in $C^n(G,\mathbb{Z})$ (here we take $A = \mathbb{Z}$ for simplicity) is simply an assignment of an integer for each n-simplex in BG. Then the coboundary and boundary maps are related by

$$\langle d\phi_n, \Delta\rangle = \langle \phi_n, \partial\Delta\rangle \tag{16.59}$$

and from the above formulae we recover, rather beautifully, the formula for the coboundary in group cohomology.

Remarks:

1. When we defined group cohomology we also used homogeneous cochains. This is based on defining G as a groupoid from its left action and considering the mapping of groupoids $G//G \to pt//G$.

♣Explain more here? ♣

2. A Lie group is a manifold and hence has its own cohomology groups as a manifold, $H^n(G;\mathbb{Z})$. There is a relation between these: There is a group homomorphism

$$H^{n+1}_{\text{group cohomology}}(G;\mathbb{Z}) \to H^n_{\text{topological space cohomology}}(G;\mathbb{Z}) \tag{16.60}$$

3. One can show that $H^n(BG;\mathbb{Z})$ is always a finite abelian group if G is a finite group. [GIVE REFERENCE].

4. The above construction of BG is already somewhat nontrivial even for the trivial group $G = \{1_G\}$. Indeed, following it through for the 2-cell, we need to identify the three vertices of a triangle to one vertex, and the three edges to a single edge, embedded as a closed circle. If you do this by first identifying two edges and then try to identify the third edge you will see why it is called the "dunce's cap." It is true, but hard to visualize, that this is a contractible space. Things only get worse as we go to higher dimensions. A better construction, due to Milnor, is to construct what is known as a "simplicial set," and then collapse all degenerate simplices to a point. This gives a nicer realization of BG, but one which is homotopy equivalent to the one we described above. For the trivial category with one object and one morphism one just gets a topological space consisting of a single point. [196]

5. The "space" BG is really only defined up to homotopy equivalence. For some G there are very nice realizations as infinite-dimensional homogeneous spaces. This is useful for defining things like "universal connections." For example, one model for

[196] I thank G. Segal for helpful remarks on this issue.

$B\mathbb{Z}$ is as the humble circle $\mathbb{R}/\mathbb{Z} = S^1$. This generalizes to lattices $B\mathbb{Z}^d = T^d$, the d-dimensional torus. On the other hand $B\mathbb{Z}_2$ must be infinite-dimensional but it can be realized as $\mathbb{RP}^\infty$, the quotient of the unit sphere in a real infinite-dimensional separable Hilbert space by the antipodal map. Similarly, $BU(1)$ is $\mathbb{CP}^\infty$, realized as the quotient of the unit sphere in a complex infinite-dimensional separable Hilbert space by scaling vectors by a phase: $\psi \to e^{\mathrm{i}\theta}\psi$.

17. Lattice Gauge Theory

As an application of some of the general concepts of group theory we discuss briefly lattice gauge theory.

Lattice gauge theory can be defined on any graph: There is a set of unoriented edges $\bar{\mathcal{E}}$. Each edge can be given either orientation and we denote the set of oriented edges by $\mathcal{E}$. The set of vertices is denoted $\mathcal{V}$ and source and target maps that tells us the vertex at the beginning and end of each oriented edge:

$$s : \mathcal{E} \to \mathcal{V} \qquad\qquad t : \mathcal{E} \to \mathcal{V} \tag{17.1}$$

We will view the union of edges $\bar{\mathcal{E}}$ (i.e. forgetting the orientation) as a topological space and denote it as Γ.

The original idea of Ken Wilson was that we could formulate Yang-Mills theory on a "lattice approximation to Euclidean spacetime" which we visualize as a cubic lattice in $\mathbb{R}^d$ for some d. Then, the heuristic idea is, that as the bond lengths are taken to zero we get a good approximation to a field theory in the continuum. Making this idea precise is highly nontrivial! For example, just one of the many issues that arise is that important symmetries such as Euclidean or Poincaré symmetries of the continuum models we wish to understand are broken, in this formulation, to crystallographic symmetries.

17.1 Some Simple Preliminary Computations

A rather trivial part of the idea is to notice the following: Suppose we have a field theory on $\mathbb{R}^d$ of fields

$$\phi : \mathbb{R}^d \to \mathcal{T} \tag{17.2}$$

where $\mathcal{T}$ is some "target space." Then if we consider the embedded hypercubic lattice:

$$\Lambda_a := \{a(n_1, \dots, n_d) \in \mathbb{R}^d | n_i \in \mathbb{Z}\} \tag{17.3}$$

and we restrict ϕ to Λ_a then at neighboring vertices the value of ϕ will converge as $a \to 0$:

$$\lim_{a\to 0} \phi(\vec{x}_0 + a\hat{e}_\mu) = \phi(\vec{x}_0) \tag{17.4}$$

where $\hat{e}_\mu$, $\mu = 1, \dots, d$ is a unit vector in the μ^{th} direction. Moreover, if $\phi : \mathbb{R}^d \to \mathcal{T}$ is differentiable and $\mathcal{T}$ is a linear space then

$$\lim_{a\to 0} a^{-1}(\phi(\vec{x}_0 + a\hat{e}_\mu) - \phi(\vec{x}_0)) = \partial_\mu \phi(\vec{x}_0) \tag{17.5}$$

and so on.

In lattice field theory we attempt to go the other way: We assume that we have fields defined on a sequence of lattices $\Lambda_a \subset \mathbb{R}^d$ and try to take an $a \to 0$ limit to define a continuum field theory.

Here is a simple paradigm to keep in mind: [197] Consider the one-dimensional lattice $\mathbb{Z}$, but it is embedded in the real line so that bond-length is a, so $\Lambda_a = \{an | n \in \mathbb{Z}\} \subset \mathbb{R}$. Our degrees of freedom will be a real number $\phi_\ell(n)$ at each lattice site $n \in \mathbb{Z}$, and it will evolve in time to give a motion $\phi_\ell(n,t)$ according to the action:

$$S = \int_{\mathbb{R}} dt \sum_{n\in\mathbb{Z}} \left(\frac{m}{2} \dot{\phi}_\ell(n,t)^2 - \frac{k}{2} \left(\phi_\ell(n,t) - \phi_\ell(n+1,t)\right)^2 \right) \tag{17.6}$$

We can think of this as a system of particles of mass m fixed at the vertices of Λ_a with neighboring particles connected by a spring with spring constant k. For the action to have proper units, $\phi_\ell(n,t)$ should have dimensions of length, suggesting it measures the displacement of the particle in some orthogonal direction to the real line. The equations of motion are of course:

$$m \frac{d^2}{dt^2} \phi_\ell(n,t) = k(\phi_\ell(n+1,t) - 2\phi_\ell(n,t) + \phi_\ell(n-1,t)) \tag{17.7}$$

Now we wish to take the $a \to 0$ limit. We assume that there is some differentiable function $\phi_{cont}(x,t)$ such that

$$\phi_{cont}(x,t)|_{x=an} = \phi_\ell(n,t) \tag{17.8}$$

so by Taylor expansion

$$\phi_\ell(n+1,t) - 2\phi_\ell(n,t) + \phi_\ell(n-1,t) = a^2 \frac{d^2}{dx^2} \phi_{cont}|_{x=an} + \mathcal{O}(a^3) \tag{17.9}$$

Now suppose we scale the parameters of the Lagrangian so that

$$m = aT \qquad k = \frac{v^2 T}{a} \tag{17.10}$$

then, if the limits really exist, the continuum function $\phi_{cont}(x,t)$ must satisfy the wave equation:

$$\frac{d^2}{dt^2}\phi_{cont} - v^2 \frac{d^2}{dx^2} \phi_{cont} = 0 \tag{17.11}$$

whose general solution is

$$\Phi_{left}(x+vt) + \Phi_{right}(x-vt) \tag{17.12}$$

The general solution is described by arbitrary wavepackets traveling to the left and right along the real line. (We took $v > 0$ here.) We can also see this at the level of the Lagrangian since if $\phi_\ell(n,t)$ is well-approximated by a continuum function $\phi_{cont}(x,t)$ then

$$S \to T \int_{\mathbb{R}} dt \int_{\mathbb{R}} dx \left[\frac{1}{2} \left(\frac{d}{dt} \phi_{cont} \right)^2 - \frac{v^2}{2} \left(\frac{d}{dx} \phi_{cont} \right)^2 \right] + \mathcal{O}(a) \tag{17.13}$$

Remarks

[197] Here we will just latticize the spatial dimension of a $1+1$ dimensional field theory. In the rest of the section we latticize spacetime with Euclidean signature.

1. In the lattice theory there will certainly be sequences of field configurations $\phi_{lattice}(n,t)$ that have no good continuum limit. The idea is that these are unimportant to the physics because they have huge actions whose contributions to the path integral is unimportant in the continuum limit.

2. Keeping in mind the interpretation of $\phi_{cont}(x,t)$ as a height in a direction orthogonal to the real axis, we see that we are describing a string of tension T.

17.2 Gauge Group And Gauge Field

In lattice gauge theory we choose a group G - known as the *gauge group*. For the moment it can be any group. The dynamical degree of freedom is a *gauge field*, or more precisely, the dynamical object is the *gauge equivalence class* or isomorphism class of the gauge field. This will be defined below.

In mathematics, a gauge field is called a *connection*.

To give the definition of a connection let $\mathcal{P}$ be the set of all connected open paths in Γ. For example, we can think of it as the set of continuous maps $\gamma : [0,1] \to \Gamma$. Since we are working on a graph you can also think of a path γ as a sequence of edges $e_1, e_2, \dots, e_k$ such that

$$t(e_i) = s(e_{i+1}) \qquad\qquad 1 \le i \le k-1 \tag{17.14}$$

(We also allow for the trivial path $\gamma_v(t) = v$ for some fixed vertex v which has no edges.) However, the former definition is superior because it generalizes to connections on other topological spaces.

Now, by definition, a connection is just a map

$$\mathbb{U} : \mathcal{P} \to G, \tag{17.15}$$

which satisfies the composition law: If we concatenate two paths γ_1 and γ_2 to make a path $\gamma_1 \circ \gamma_2$, so that the concatenated path begins at $\gamma_1(0)$ and ends at $\gamma_2(1)$ and such that $\gamma_1(1) = \gamma_2(0)$, that is, the end of γ_1 is the beginning of γ_2, then we must have:

$$\mathbb{U}(\gamma_1 \circ \gamma_2) = \mathbb{U}(\gamma_1)\mathbb{U}(\gamma_2) \tag{17.16}$$

If our path is the trivial path then

$$\mathbb{U}(\gamma_v) = 1_G \tag{17.17}$$

and if $\gamma^{-1}(t) = \gamma(1-t)$ is the path run backwards then

$$\mathbb{U}(\gamma^{-1}) = (\mathbb{U}(\gamma))^{-1} \tag{17.18}$$

♣Are these really independent conditions? ♣

Note that if the path γ is made by concatenating edges $e_1, e_2, \dots, e_k$ then

$$\mathbb{U}(\gamma) = \mathbb{U}(e_1)\mathbb{U}(e_2)\cdots\mathbb{U}(e_k) \tag{17.19}$$

so, really, in lattice gauge theory it suffices to know the $\mathbb{U}(e)$ for the edges. If e^{-1} is the edge e with the opposite orientation then

$$\mathbb{U}(e^{-1}) = \mathbb{U}(e)^{-1} \tag{17.20}$$

We will denote the space of all connections by $\mathcal{A}(\Gamma)$.

Remark: *Background heuristics*: For those who know something about gauge fields in field theory we should think of $\mathbb{U}(e)$ as the parallel transport (in some trivialization of our principal bundle) along the edge e. From these parallel transports along edges we can recover the components of the gauge field. To explain more let us assume for simplicity that $G = U(N)$ is a unitary group, or some matrix subgroup of $U(N)$.

Recall some elementary ideas from the theory of Lie groups: If α is any anti-Hermitian matrix then $\exp[\alpha]$ is a unitary matrix. Moreover, if α is "small" then $\exp[\alpha]$ is close to the identity. Conversely, if U is "close" to the identity then it can be uniquely written in the form $U = \exp[\alpha]$ for a "small" anti-Hermitian matrix α. Put more formally: The tangent space to $U(N)$ at the identity is the (real!) vector space of $N \times N$ anti-Hermitian matrices. (This vector space is a real Lie algebra, because the commutator of anti-Hermitian matrices is an anti-Hermitian matrix.) Moreover, the exponential map gives a good coordinate chart in some neighborhood of the identity of the topological group $U(N)$.

The poor man's way of understanding the relation between Lie algebras and Lie groups is to use the very useful Baker-Campbell-Hausdorf formula: If A, B are $n \times n$ matrices then the formula gives an expression for an $n \times n$ matrix C so that

$$e^A e^B = e^C \tag{17.21}$$

The formula is a (very explicit) infinite set of terms all expressed in terms of multiple commutators. The first few terms are:

$$\boxed{C = A + B + \frac{1}{2}[A, B] + \frac{1}{12}[A, [A, B]] + \frac{1}{12}[B, [B, A]] + \frac{1}{24}[A, [B, [A, B]]] + \cdots} \tag{17.22}$$

The series is convergent as long as A, B are small enough (technically, such that the characteristic values of $\mathrm{Ad}(A)$ and $\mathrm{Ad}(B)$ are less than 2π in magnitude). See Chapter 8 for a full explanation. Note in particular that if we expand in small parameters ϵ_1, ϵ_2 then

$$e^{\epsilon_1 A} e^{\epsilon_2 B} e^{-\epsilon_1 A} e^{-\epsilon_2 B} = e^{\epsilon_1 \epsilon_2 [A,B] + \cdots} \tag{17.23}$$

Now, returning to lattice gauge theory: In the usual picture of "approximating" Euclidean $\mathbb{R}^d$ by $\mathbb{Z}^d$ with bond-length a we can write a fundamental edge $e_\mu(\vec{n})$ as the straight line in $\mathbb{R}^d$ from $\vec{n}$ to $\vec{n} + a\hat{e}_\mu$. If a is small and we have some suitable continuity then $\mathbb{U}(e_\mu(\vec{n}))$ will be near the identity and we can write:

$$\mathbb{U}(e_\mu(\vec{n})) = \exp[a A_\mu^{lattice}(\vec{n})] \tag{17.24}$$

for some anti-Hermitian matrix $A_\mu(a\vec{n})$. In lattice gauge theory, the connections with a good continuum limit are those such that there is a locally defined 1-form valued in $N \times N$ anti-Hermitian matrices $A_\mu^{cont}(\vec{x}) dx^\mu$ so that $A_\mu^{cont}(a\vec{n}) = A_\mu^{lattice}(\vec{n})$.

Now, the gauge field $\mathbb{U}$ has redundant information in it. The reason it is useful to include this redundant information is that many aspects of locality become much clearer when working with $\mathcal{A}(\Gamma)$ as we will see when trying to write actions below. The redundant information is reflected in a *gauge transformation* which is simply a map

$$f : \mathcal{V} \to G \tag{17.25}$$

The idea is that if γ is a path then the gauge fields $\mathbb{U}$ and $\mathbb{U}'$ related by the rule

$$\mathbb{U}'(\gamma) = f(s(\gamma))\mathbb{U}(\gamma)f(t(\gamma))^{-1} \tag{17.26}$$

are deemed to be gauge equivalent, i.e. isomorphic. We denote the set of gauge transformations by $\mathcal{G}(\Gamma)$. Note that, being a function space whose target is a group, this set is a group in a natural way. It is called *the group of gauge transformations.* [198] The group of gauge transformations $\mathcal{G}(\Gamma)$ acts on $\mathcal{A}(\Gamma)$. The moduli space of gauge inequivalent fields is the set of equivalence classes: $\mathcal{A}(\Gamma)/\mathcal{G}(\Gamma)$. Mathematicians would call these isomorphism classes of connections.

It might seem like there is no content here. Can't we always choose $f(s(\gamma))$ to set $\mathbb{U}'(\gamma)$ to 1? Yes, in general, except when $s(\gamma) = t(\gamma)$, that is, when γ is a closed loop based at a vertex, say v_0. For such closed loops we are stuck, all we can do by gauge transformations is conjugate:

$$\mathbb{U}'(\gamma) = g\mathbb{U}(\gamma)g^{-1} \tag{17.27}$$

where g is the gauge transformation at v_0. Moreover, if we start the closed loop at another vertex on the loop then the parallel transport is again in the same conjugacy class. Thus there is gauge invariant information associated to a loop γ: The conjugacy class of the $\mathbb{U}(\gamma)$. That is: The *holonomy function*:

$$\mathrm{Hol}_{\mathbb{U}} : L\Gamma \to \mathrm{Conj}(G) \tag{17.28}$$

that maps the loops in Γ to the conjugacy class:

$$\mathrm{Hol}_{\mathbb{U}} : \gamma \mapsto C(\mathbb{U}(\gamma)) \tag{17.29}$$

is gauge invariant: If $\mathbb{U}' \sim \mathbb{U}$ are gauge equivalent then

$$\mathrm{Hol}_{\mathbb{U}'} = \mathrm{Hol}_{\mathbb{U}} \tag{17.30}$$

In fact, one can show that $\mathrm{Hol}_{\mathbb{U}}$ is a complete invariant, meaning that we have the converse: If $\mathrm{Hol}_{\mathbb{U}'} = \mathrm{Hol}_{\mathbb{U}}$ then $\mathbb{U}'$ is gauge equivalent to $\mathbb{U}$. Put informally:

> *The gauge invariant information in a gauge field, or connection, is encoded in the set of conjugacy classes associated to the closed loops in Γ.*

Exercise

[198] AND IS NOT TO BE CONFUSED WITH THE gauge group G!!!!

Show that if γ is a closed loop beginning and ending at v_0 and if v_1 is another vertex on the path γ then if γ' describes the "same" loop but starting at v_1 then $\mathbb{U}(\gamma)$ and $\mathbb{U}(\gamma')$ are in the same conjugacy class in G.

Exercise

Consider a graph Γ which forms a star: There is one central vertex, and r "legs" each consisting or N_i edges radiating outward, where $i = 1, \dots, r$.

a.) Show explicitly that any gauge field can be gauged to $\mathbb{U} = 1$.

b.) What is the unbroken subgroup of the group of gauge transformations? (That is, what is the automorphism group of the gauge field $\mathbb{U} = 1$?)

Exercise

Consider a d-dimensional hypercubic lattice with periodic boundary conditions, so that we are "approximating a torus" which is a product of "circles" of length Na.

What is the maximal number of edges so that we can set $\mathbb{U}(e) = 1$?

17.3 Defining A Partition Function

Next, to do physics, we need to define a gauge invariant action. At the most general level this is simply a function $F : \mathcal{A}(\Gamma)/\mathcal{G}(\Gamma) \to \mathbb{C}$ so that we can define a "partition function":

$$Z = \sum_{[\mathbb{U}]\in\mathcal{A}(\Gamma)/\mathcal{G}(\Gamma)} F([\mathbb{U}]) \tag{17.31}$$

If Γ is finite and G is finite this sum is just a finite sum. If Γ is finite and G is a finite-dimensional Lie group then $\mathcal{A}(\Gamma)/\mathcal{G}(\Gamma)$ is a finite-dimensional topological space and the "sum" needs to be interpreted as some kind of integral. Since a connection on Γ is completely determined by its values on the elementary edges (for a single orientation) we can, noncanonically, identity the space of all connections as

$$\mathcal{A}(\Gamma) \cong G^{|\bar{\mathcal{E}}|}. \tag{17.32}$$

Similarly

$$\mathcal{G}(\Gamma) \cong G^{|\mathcal{V}|} \tag{17.33}$$

Now we need a way of integrating over the group. If G is a finite group and $F : G \to \mathbb{C}$ is a function then

$$\int_G F d\mu := \frac{1}{|G|}\sum_{g\in G} F(g) \tag{17.34}$$

This basic idea can be generalized to Lie groups. A Lie group is a manifold and we define a measure on it $d\mu$. (If G is a simple Lie group then there is a canonical choice of measure up to an overall scale.) As a simple example, coonsider $U(1) = \{e^{i\theta}\}$ then the integration is

$$\int_0^{2\pi} F(e^{i\theta})\frac{d\theta}{2\pi} \tag{17.35}$$

In all cases, the crucial property of the group integration is that, for all h we have

$$\int_G F(gh)d\mu(g) = \int_G F(hg)d\mu(g) = \int_G F(g)d\mu(g) \tag{17.36}$$

This property defines what is called a *left-right-invariant measure*. It is also known as the *Haar measure*.

In general the Haar measure is only defined up to an overall scale. In the above examples we chose the normalization so that the volume of the group is 1.

Now, choosing a left-right-invariant measure we can define:

$$Z = \frac{1}{\mathrm{vol}\,(\mathcal{G}(\Gamma))}\int_{\mathcal{A}(\Gamma)} \hat{F}(\mathbb{U})d\mu_{\mathcal{A}(\Gamma)} \tag{17.37}$$

where $\hat{F}$ is a lifting of F to a $\mathcal{G}(\Gamma)$-invariant function on $\mathcal{A}(\Gamma)$ and $d\mu_{\mathcal{G}(\Gamma)}$ is the Haar measure on $G^{|\vec{\mathcal{E}}|}$ induced by a choice of Haar measure on G. It is gauge invariant because the Haar measure is left- and right- invariant.

If we want to impose locality then it is natural to have $\hat{F}(\mathbb{U})$ depend only on the local gauge invariant data. This motivates us to consider "small" loops and consider a *class function*.

In general, a class function on a group G is a function $F : G \to \mathbb{C}$ such that $F(hgh^{-1}) = F(g)$ for all $h \in G$. We should clearly take $\hat{F}$ to be some kind of class function. A natural source of class functions are traces in representations, for if $\rho : G \to GL(N,\mathbb{C})$ is a matrix representation then $\chi(g) := \mathrm{Tr}\rho(g)$ is a class function by cyclicity of the trace. (This class function is called the *character of the representation*.)

The smallest closed loops we can make are the "plaquettes." For $\Lambda_a \subset \mathbb{R}^d$ these would be labeled by a pair of directions μ, ν with $\mu \neq \nu$ and would be the closed loop

$$a\vec{n} \to a\vec{n} + a\hat{e}_\mu \to a\vec{n} + a\hat{e}_\mu + a\hat{e}_\nu \to a\vec{n} + a\hat{e}_\nu \to a\vec{n} \tag{17.38}$$

Let us denote this plaquette as $p_{\mu\nu}(\vec{n})$. ♣FIGURE NEEDED HERE! ♣

Given a class function $F : G \to \mathbb{C}$ we can form a partition function by taking

$$\hat{F}(\mathbb{U}) := e^{-S(\mathbb{U})} := e^{-\sum_p S(p)} \tag{17.39}$$

where we have summed over all plaquettes in the exponential to make this look more like a discrete approximation to a field theory path integral, and the action $S(p)$ of a plaquette p is some class function applied to $\mathbb{U}(p)$. If G is a continuous group then we need to interpret the sum over $\mathcal{A}(\Gamma)/\mathcal{G}(\Gamma)$ as some kind of integral, as discussed above.

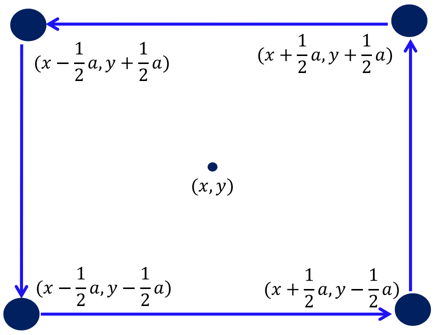
$(x-\frac{1}{2}a, y+\frac{1}{2}a)$
$(x+\frac{1}{2}a, y+\frac{1}{2}a)$
(x,y)
$(x-\frac{1}{2}a, y-\frac{1}{2}a)$
$(x+\frac{1}{2}a, y-\frac{1}{2}a)$

Figure 38: A small plaquette, centered on a surface element in a tangent plane with coordinates (x, y) and centered on a point with coordinates (x, y). The holonomy around the plaquette, to leading order in an expansion in small values of bond-length a is governed by the curvature tensor evaluated on that area element.

Remark: *More background heuristics*: For those who know something about gauge fields in field theory we should think of the parallel transport $\mathbb{U}(p)$ around a plaquette p as defining the components of the curvature on a small area element $dx^\mu \wedge dx^\nu$ at some point $\vec{x}_0 = a\vec{n}$ (in some framing). Indeed, using the idea that

$$\mathbb{U}(e_\mu(\vec{n})) \sim \exp[aA_\mu^{cont}|_{\vec{x}=a\vec{n}}] \tag{17.40}$$

we can try to take a "limit" where $a \to 0$. The plaquette $p_{\mu\nu}(\vec{n})$ is two-dimensional so, temporarily choosing coordinates so that $\mu = 1$ and $\nu = 2$ we can write the plaquette gauge group element as

$$e^{aA_1(x,y-\frac{1}{2}a)} e^{aA_2(x+\frac{1}{2}a,y)} e^{-aA_1(x,y+\frac{1}{2}a)} e^{-aA_2(x-\frac{1}{2}a,y)} \tag{17.41}$$

See Figure 38. Now, using the BCH formula [199] we define the *fieldstrength of the gauge field* or, equivalently, the *curvature of the connection* by

$$\mathbb{U}(p_{\mu\nu}(\vec{n})) = \exp[a^2 F_{\mu\nu} + \mathcal{O}(a^4)] \tag{17.44}$$

Here in the continuum we would have the relation:

$$F_{\mu\nu}(\vec{x}) = \partial_\mu A_\nu(\vec{x}) - \partial_\nu A_\mu(\vec{x}) + [A_\mu(\vec{x}), A_\nu(\vec{x})] \tag{17.45}$$

[199] Warning: If you are not careful the algebra can be extremely cumbersome here! Taylor expansion in to order a^2 gives:

$$e^{aA_1 - \frac{a^2}{2}\partial_2 A_1} e^{aA_2 + \frac{a^2}{2}\partial_1 A_2} e^{-aA_1 - \frac{a^2}{2}\partial_2 A_1} e^{-aA_2 + \frac{a^2}{2}\partial_1 A_2} \tag{17.42}$$

We only need to keep the first commutator term in the BCH formula if we are working to order a^2 so we get

$$e^{a^2(\partial_1 A_2 - \partial_2 A_1 + [A_1, A_2]) + \mathcal{O}(a^3)} \tag{17.43}$$

A standard action used in lattice gauge theory in the literature is constructed as follows:

First, choose a finite-dimensional unitary representation of G, that is, a group homomorphism

$$\rho : G \to U(r) \tag{17.46}$$

Next, define the action for a plaquette to be

$$S(p) = K(r - \mathrm{Re}[\mathrm{Tr}\rho(\mathbb{U}(p))]) \tag{17.47}$$

for some constant K. Note that the trivial gauge field has action $S(p) = 0$. Moreover, every unitary matrix can be diagonalized, by the spectral theorem, with eigenvalues $e^{\mathrm{i}\theta_i(p)}$, $i = 1, \dots, r$ and then

$$S(p) = K \sum_{i=1}^{r} (1 - \cos\theta_i(p)) = 2K \sum_{i=1} \sin^2(\theta_i(p)/2) \tag{17.48}$$

is clearly positive definite for $K > 0$. This is good for unitarity (or its Euclidean counterpart - "reflection positivity.")

Remarks:

1. *Correlation Functions*: The typical physical quantities we might want to compute are expectation values of products of gauge invariant operators. In view of our discussion of gauge equivalence classes of gauge fields above one very natural way to make such gauge invariant operators is via *Wilson loop operators.* For these one chooses a matrix representation $R : G \to GL(N, \mathbb{C})$ of G (totally unrelated to the choice we made in defining the action) and a particular loop γ and defines:

$$W(R, \gamma)(\mathbb{U}) := \mathrm{Tr}_{\mathbb{C}^N} R(\mathbb{U}(\gamma)) \tag{17.49}$$

   So, $W(R, \gamma)$ should be regarded as a gauge invariant function

$$W(R, \gamma) : \mathcal{A}(\Gamma) \to \mathbb{C} \tag{17.50}$$

   and therefore we can consider the expectation values:

$$\langle \prod_i W(R_i, \gamma_i) \rangle := \frac{\int_{\mathcal{A}(\Gamma)} \prod_i W(R_i, \gamma_i) e^{-S(\mathbb{U})} d\mu_{\mathcal{A}(\Gamma)}}{\int_{\mathcal{A}(\Gamma)} e^{-S(\mathbb{U})} d\mu_{\mathcal{A}(\Gamma)}} \tag{17.51}$$

2. *Yet more background heuristics*: For those who know something about gauge fields in field theory we can begin to recognize something like the Yang-Mills action if we use (17.44) and write

$$S(p) = K \sum_{p_{\mu\nu}(\vec{n})} (r - \mathrm{Re}[\mathrm{Tr}\rho(\mathbb{U}(p_{\mu\nu}(\vec{n})))]) \to -\frac{1}{2} K a^4 \sum_{\vec{n} \in \mathbb{Z}^d} \sum_{\mu \neq \nu} \mathrm{Tr}\rho(F_{\mu\nu}(a\vec{n}))^2 \tag{17.52}$$

♣There is a bit of a cheat here since you did not work out the plaquette to order a^4. ♣

The heuristic limit (17.52) is to be compared with the Yang-Mills action

$$S_{YM} = -\frac{1}{2g_0^2}\int_X d^dx\sqrt{\det g}g^{\mu\lambda}g^{\nu\rho}\mathrm{Tr}F_{\mu\nu}F_{\lambda\rho} \tag{17.53}$$

where here we wrote it in Euclidean signature on a Riemannian manifold M. The trace is in some suitable representation and the normalization of the trace can be absorbed in a rescaling of the coupling constant g_0. If we use the representation $\rho : G \to U(r)$ then

$$\frac{1}{g_0^2} = Ka^{4-d} \qquad \Rightarrow \qquad K = \frac{a^{d-4}}{g_0^2} \tag{17.54}$$

The constant K must be dimensionless so that $d = 4$ dimensions is selected as special. For $d = 4$ the Yang-Mills coupling g_0^2 is dimensionless. It has dimensions of length to a positive power for $d > 4$ and length to a negative power for $d < 4$. To take the continuum limit we should hold g_0^2 fixed and scale K as above as $a \to 0$.

3. *Very important subtlety in the case $d = 4$* Actually, if one attempts to take the limit more carefully, the situation becomes more complicated in $d = 4$, because in quantum mechanics there are important effects known as *vacuum fluctuations.* What is expected to happen (based on continuum field theory) is that, if we replace K by $g^{-2}(a)$ and allow a-dependence then we can get a good limit of, say, correlation functions of Wilson loop vev's if we scale $g^2(a)$ so that

$$\frac{8\pi^2}{g^2(a_1)} = \frac{8\pi^2}{g^2(a_2)} + \beta\log\frac{a_1}{a_2} + \mathcal{O}(g^2(a_2)) \tag{17.55}$$

where there are higher order terms in the RHS in an expansion in $g^2(a_2)$. Here β is a constant, depending on the gauge group G and other fields in the theory. For $G = SU(n)$ we have the renowned result of D. Gross and F. Wilczek, and of D. Politzer that

$$\beta = -\frac{11}{3}n \tag{17.56}$$

As long as $\beta < 0$ we see that $g^2(a_2) \to 0$ as $a_2 \to 0$. This is known as *asymptotic freedom.* It has the good property that as we attempt to take $a_2 \to 0$ the higher order terms on the RHS are at least formally going to zero.

4. One can therefore ask, to what extent is this continuum limit rigorously defined and how rigorously has (17.55) been established from the lattice gauge theory approach. My impression is that it is still open. Two textbooks on this subject are:

   1. C. Itzykson and J.-M. Drouffe, *Statistical Field Theory*, Cambridge

   2. M. Creutz, *Quarks, gluons, and lattices*, Cambridge

5. *Phases and confinement.* Many crucial physical properties can be deduced from Wilson loop vev's. In Yang-Mills theory a crucial question is whether, for large planar loops γ $\langle W(R,\gamma)\rangle$ decays like $\exp[-TArea(\gamma)]$ or $\exp[-\mu Perimeter(\gamma)]$. If it decays like the area one can argue that quarks will be confined. For a nice explanation see S. Coleman, *Aspects Of Symmetry*, for a crystal clear explanation.

6. *Including quarks and QCD.* The beta function is further modified if there are "matter fields" coupling to the gauge fields. If we introduce n_f Dirac fermions in the fundamental representation of $SU(n)$ then (17.56) is modified to:

$$\beta = -\left(\frac{11}{3}n - \frac{2}{3}n_f\right) \tag{17.57}$$

   The theory of the strong nuclear force between quarks and gluons is based on $n = 3$ and $n_f = 6$. Actually, there is a strong hierarchy of quark masses so for low energy questions $n_f = 2$ (for "up" and "down" quarks) is more relevant.

7. There are very special situations in which $\beta = 0$ and in fact all the higher terms on the RHS of the "renormalization group equation" (17.55) vanish. These lead to scale-invariant theories, and in good cases, to conformal field theories. In the modern viewpoint on field theory, these conformal field theories are the basic building blocks of all quantum field theories.

17.4 Hamiltonian Formulation

EXPLAIN HILBERT SPACE FOR 1+1 CASE IS $L^2(G)$.

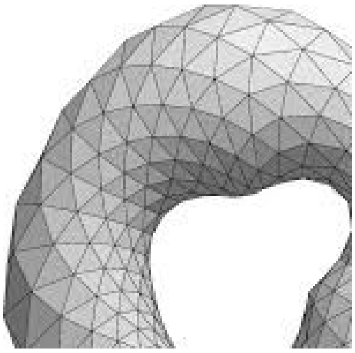

Figure 39: A triangulated surface. Figure from Wikipedia.

17.5 Topological Gauge Theory

A very popular subject in discussions of topological phases of matter is a set of models known as "topological gauge theories." In general, topological field theories are special classes of field theories that are independent of distances in spacetime. They focus on the topological aspects of physics. A formal mathematical definition is that it is a functor from some bordism category to, say, the category $\mathbf{Vect}_\kappa$.

If G is a finite group and we are working on a smooth manifold then there can be no curvature tensor, so all gauge fields are "flat." They can still be nontrivial since $\mathbb{U}(\gamma)$ can still be nontrivial for homotopically nontrivial loops. The simplest example would be $0+1$ dimensional Yang-Mills theory on a circle. If the action is literally zero then the partition function is just

$$Z = \frac{1}{|G|}\sum_{g\in G} 1 \tag{17.58}$$

Recalling our discussion of the class equation we recognize that the partition function can be written as:

$$Z = \sum_{c.c.} \frac{1}{|Z(g)|} \tag{17.59}$$

where we sum over conjugacy classes in the group and weight each class by one over the order of the centralizer of some (any) representative of that class. This second form of the sum can be interpreted as a sum over the isomorphism classes of principal G-bundles over the circle, weighted by one over the automorphism group of the bundle.

For those who know something about gauge theory note that this illustrates a very general principle: *In the partition function of a gauge theory we sum over all the isomorphism classes of bundles with connection: We weight the bundle with connection by a gauge invariant functional divided by the order of the automorphism group of the bundle with connection.*

It is also worth remarking that, quite generally in field theory, the partition function on a manifold of the form $X \times S^1$ can be interpreted as a trace in a Hilbert space. With proper boundary conditions for the "fields" around S^1 we simply have

$$Z(X \times S^1) = \mathrm{Tr}_{\mathcal{H}(X)} e^{-\beta H} \tag{17.60}$$

where β is the length of the circle. In a topological theory the Hamiltonian $H = 0$, so we just get the dimension of the Hilbert space associated to the spatial slice X. In the case of Yang-Mills in $0+1$ dimensions we see that the Hilbert space associated to a point is just $\mathcal{H} = \mathbb{C}$.

In lattice models of topological gauge theories in higher dimensions we insert the gauge-invariant function

$$\prod_p \delta(\mathbb{U}(p)) \tag{17.61}$$

where $\delta(g)$ is the Dirac delta function relative to the measure $d\mu(g)$ we chose on G, and is concentrated at $g = 1_G$. Here we take the product over all plaquettes that are meant to be "filled in" in the continuum limit. That means that the parallel transport around "small" loops defined by plaquettes will be trivial. This does not mean that the gauge field is trivial! For example if we consider a triangulation of a compact surface or higher dimensional manifold with nontrivial fundamental group then there can be nontrivial holonomy around homotopically nontrivial loops. In general, a connection, or gauge field, such that $\mathbb{U}(\gamma) = 1$ for homotopically nontrivial loops (this is equivalent to the vanishing of the curvature 2-form $F_{\mu\nu}$) is known as a *flat connection* or *flat gauge field.* In topological gauge theories we sum over (isomorphism classes of) flat connections.

Note that (17.61) is just part of the definition of a topological gauge theory. We want to do this so that physical quantities only depend on topological aspects of the theory. In standard Yang-Mills theory $\langle W(R, \gamma)\rangle$ will depend on lots of details of γ. Indeed, one definition of the curvature is how $W(R, \gamma)$ responds to small deformations of γ. In topological gauge theories we want

$$\langle \prod_i W(R_i, \gamma_i)\rangle \tag{17.62}$$

to be independent of (nonintersecting!) γ_i under homotopy. Therefore, our measure should be concentrated on flat gauge fields, at least in some heuristic sense. In lattice topological gauge theory we do this by hand.

Remark: In general, flat gauge fields for a group G on a manifold M are classified, up to gauge equivalence by the conjugacy classes of homomorphisms $\mathrm{Hom}(\pi_1(M, x_0), G)$.

For a flat gauge field, the standard Wilson action we discussed above will simply vanish. We can get a wider class of models by using group cocycles. This was pointed out in the paper

R. Dijkgraaf and E. Witten, "Topological Gauge Theory And Group Cohomology," Commun.Math.Phys. 129 (1990) 39.

and topological gauge theories that make use of group cocycles for the action are now known as *Dijkgraaf-Witten models.*

For simplicity we now take our group G to be a finite group. Let us start with a two-dimensional model. We can view Γ as a triangulation of an oriented surface M as in Figure 39. We want a local action, so let us restrict to a flat gauge field on a triangle as in Figure 36. We want to assign the local "Boltzman weight." It will be a function:

$$W : G \times G \to \mathbb{C}^* \tag{17.63}$$

(If we wish to match to some popular physical theories we might take it to be $U(1)$-valued. The distinction will not matter for anything we discuss here.) Now referring to Figure 36 we assign the weight

$$W(g_1, g_2) \tag{17.64}$$

to this triangle. But now we have to decide if we are to use this, or $W(g_2, (g_1 g_2)^{-1})$ or $W((g_1 g_2)^{-1}, g_1)$. In general these complex numbers will not be equal to each other. So we number the vertices $1, \dots, |\mathcal{V}|$ and then for any triangle T we start with the vertices with the two smallest numbers. Call this $W(T)$. This will define an orientation that might or might not agree with that on the surface M. Let $\epsilon(T) = +1$ if it agrees and $\epsilon(T) = -1$ if it does not. Then the Boltzman weight for a flat gauge field configuration $\mathbb{U}$ on the entire surface is defined to be

$$W(\mathbb{U}) := \prod_T W(T)^{\epsilon(T)} \tag{17.65}$$

Now, if this weight is to be at all physically meaningful we definitely want the dependence on all sorts of choices to drop out.

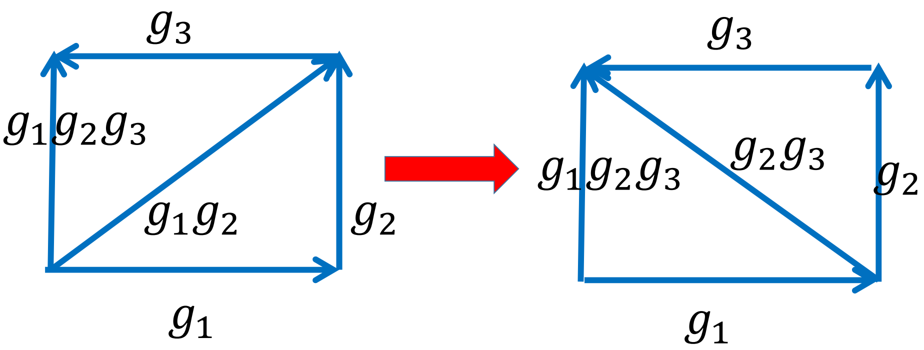

Figure 40: A local change of triangulation of type I.

Now, one thing we definitely want to have is independence of the choice of triangulation. A theorem of combinatorial topology states that any two triangulations can be related by a sequence of local changes of type I and type II illustrated in Figure 40 and 41, respectively. We see that the invariance of the action under type I requires:

$$W(g_1,g_2)W(g_1g_2,g_3) = W(g_1,g_2g_3)W(g_2,g_3) \tag{17.66}$$

and this is the condition that W should be a 2-cocycle. Similarly, the change of type II doesn't matter provided

$$W(g_1,g_2) = W(g_1,g_2g_3)W(g_2,g_3)W(g_1g_2,g_3)^{-1} \tag{17.67}$$

which is again guaranteed by the cocycle equation! This strongly suggests we can get a good theory by using a 2-cocycle, and that is indeed the case. But we need to check some things first:

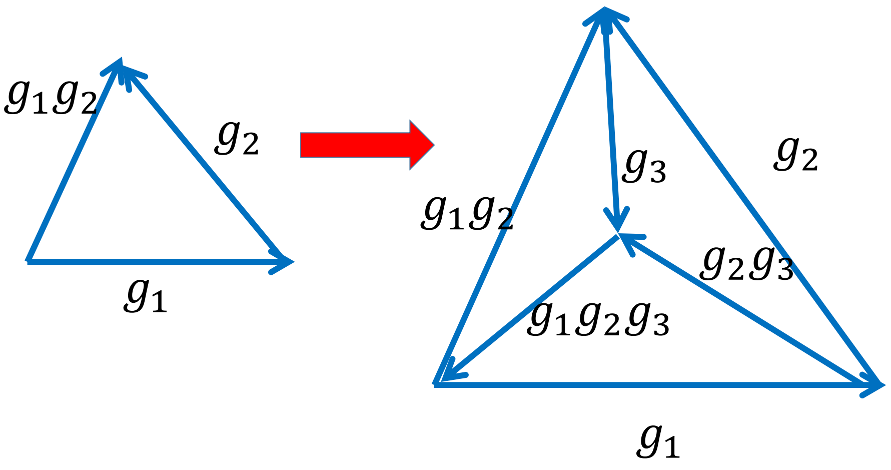

Figure 41: A local change of triangulation of type II.

1. The dependence on the labeling of the vertices drops out using an argument based on topology we haven't covered. This can be found in the Dijkgraaf-Witten paper. Similarly, if W is changed by a coboundary then we modify

$$W(g_1, g_2) \to W(g_1, g_2)\frac{t(g_1)t(g_2)}{t(g_1g_2)} \tag{17.68}$$

that is, we modify the weight by a factor based on a product around the edges. When multiplying the contributions of the individual triangles to get the total weight (17.65) the edge factors will cancel out from the two triangles sharing a common edge.

2. The action is not obviously gauge invariant, since it is certainly not true in general that $W(g_1, g_2)$ is equal to

$$W(h(v_1)^{-1}g_1h(v_2), h(v_2)^{-1}g_2h(v_3)) \tag{17.69}$$

for all group elements $h(v_1), h(v_2), h(v_3) \in G$. The argument that, nevertheless, the total action (17.65) is invariant is given (for the $d = 3$ case) in the Dijkgraaf-Witten paper around their equation (6.29).

3. The idea above generalizes to define a topological gauge theory on oriented manifolds in d-dimensions for any d, where one uses a d-cocycle on G with values in $\mathbb{C}^*$ (or $U(1)$). These topological gauge theories are known as "Dijkgraaf-Witten theories." The Boltzmann weight W represents a topological term in the action that exists and is nontrivial even for flat gauge fields.

♣Cop out. Give a better argument. Explain that Chern-Simons actions change by boundary terms and it is too much to hope for exact local gauge invariance. ♣

4. The invariance under the change of type II in Figure 41, which can be generalized to all dimensions is particularly interesting. It means that the action is an "exact renormalization group invariant" in the sense reminiscent of block spin renormalization. [200] This fits in harmoniously with the alleged the metric-independence of the topological gauge theory.

5. The case $d = 3$ is of special interest, and was the main focus of the original Dijkgraaf-Witten paper. In this case we have constructed a "lattice Chern-Simons invariant," and the theory with a cocycle $[W] \in H^3(BG, U(1)) = H^3_{\text{groupcohomology}}(G, U(1))$ is a Chern-Simons theory for gauge group G. In the case of G finite one can show that $H^3(BG, U(1)) \cong H^4(BG; \mathbb{Z})$. In general the level of a Chern-Simons theory is valued in $H^4(BG; \mathbb{Z})$ for all compact Lie groups G.

ALSO DISCUSS HAMILTONIAN VIEWPOINT!

18. Example: Symmetry Protected Phases Of Matter In $1+1$ Dimensions

[200] The idea of block spin renormalization, invented by Leo Kadanoff, is that we impose some small lattice spacing a as a UV cutoff and try to describe an effective theory at ever larger distances. So, we block spins together in some way, define an effective spin, and then an effective action

$$e^{-S_{eff}} := \sum_{fixed-effective-spins} e^{-S(spins)} \tag{17.70}$$

The hope is that at long distances, with ever larger blocks, the "relevant" parts of S_{eff} converge to a useful infrared field theory description.