Preprint typeset in JHEP style - HYPER VERSION

Chapter 1: Abstract Group Theory

Gregory W. Moore

Abstract: Very Abstract.March 30, 2018

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

[1] See the romantic stories of the life of Galois

groups were crucial in transformation laws of tensors and in describing and constructing 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.

Now, in the late 20th and early 21st century group theory is 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* G is a set with a multiplication:

$\forall a, b \in G$ there exists a unique element in G, called the product, and denoted $a \cdot b \in G$

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:
$$\forall a \in G \qquad a \cdot e = e \cdot a = a \tag{2.1}$$
3. Existence of inverses: $\forall a \qquad \exists a^{-1} \in G \qquad a \cdot a^{-1} = a^{-1} \cdot a = e$

Remarks

1. We will often denote e by 1, or by 1_G, when discussing more than one group at a time. 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 defined by dropping the existence of inverses. Nevertheless, the definition of a group seems to be in that Goldilocks region of being not too sparse to give too little structure, but not too rigid to allow only limited examples. It is *just right* to have a deep and rich mathematical theory.

Exercise

a.) Show that e unique.

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

c.) Show that in axiom (2) above we need only say $a \cdot e = a$, or $e \cdot a = a$. It is not necessary to postulate both equations.

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

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n) \tag{2.2}$$

Example 2.3: $G = \mathbb{R}^* := \mathbb{R} - \{0\}$ or $G = \mathbb{C}^* := \mathbb{C} - \{0\}$ operation $= \times$.

Definition 2.2: If G is a group, a subset $H \subseteq G$ which is also a group is called, naturally enough, a *subgroup*.

Exercise *Subgroups*

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

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

c.) Let $\mathbb{R}^*_{\pm}$ denote the positive and negative real numbers, respectively. Which of these are subgroups 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.

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

Example 2.4: The residue classes modulo N, also called "The cyclic group of order N."

Choose a natural number [2] N. As a set we can take $G = \{0, 1, \dots, N-1\}$. [3] 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, denoted abstractly as $r_1 \cdot r_2$, is defined to be the residue of $(r_1 + r_2)$ modulo N. [4] 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.

Exercise

Does $\mathbb{Z}_{137}$ have any nontrivial subgroups? [5]

Exercise

In example 4 show that if N is even then the subset of classes of even integers forms a proper subgroup of $\mathbb{Z}_N$. 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. [6]

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

$$a \cdot b = b \cdot a \tag{2.3}$$

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

[3] It is conceptually better to think of G as the integers modulo N, using the notation of equivalence relation of §6.2 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 $\overline{r_1} + \overline{r_2} := \overline{r_1 + r_2}$.

[4] It is also possible to define a ring structure where one multiplies r_1 and r_2 as integers and then takes the residue. This is *NOT* what is meant here by $r_1 \cdot r_2$!!

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

[6] 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.

When (2.3) holds we say "a and b commute." Such groups are very special and baptised as *abelian groups*:

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

Note: When working with abelian groups we will often - but not always! - use additive notation and write, for example $a + b$ rather than the abstract $a \cdot b$. In this case we will write the identity element as 0. So that $a + 0 = 0 + a = a$. (Writing "$a + 1 = a$" would look extremely wierd.)

There are certainly examples of nonabelian groups.

Example 2.5: *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. ♣

$$GL(n, \kappa) = \{A | A = n \times n \text{ invertible matix over } \kappa\} \tag{2.4}$$

$GL(n, \kappa)$ 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 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:

$$Z(G) := \{z \in G | zg = gz \qquad \forall g \in G\} \tag{2.5}$$

$Z(G)$ is an abelian subgroup of G. 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 2.6: *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:

$$SL(n, \kappa) \equiv \{A \in GL(n, \kappa) : \det A = 1\} \tag{2.6}$$

The orthogonal groups:

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

$$
\begin{aligned}
O(n,\mathbb{R}) &:= \{A \in GL(n,\mathbb{R}) : AA^{tr} = 1\} \\
SO(n,\mathbb{R}) &:= \{A \in O(n,\mathbb{R}) : \det A = 1\}
\end{aligned}
\tag{2.7}
$$

Another natural class are the unitary and special unitary groups:

$$
U(n) := \{A \in GL(n,\mathbb{C}) : AA^{\dagger} = 1\} \tag{2.8}
$$

$$
SU(n) := \{A \in U(n) : \det A = 1\} \tag{2.9}
$$

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

$$
J = \begin{pmatrix} 0 & 1_{n\times n} \\ -1_{n\times n} & 0 \end{pmatrix} \in M_{2n}(\mathbb{R}) \tag{2.10}
$$

Note that the matrix J satisfies the properties:

$$
J = J^{*} = -J^{tr} = -J^{-1} \tag{2.11}
$$

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

$$
A^{tr} J A = J \tag{2.12}
$$

We define the symplectic groups:

$$
\begin{aligned}
Sp(2n,\mathbb{R}) &:= \{A \in GL(2n,\mathbb{R}) | A^{tr} J A = J\} \\
Sp(2n,\mathbb{C}) &:= \{A \in GL(2n,\mathbb{C}) | A^{tr} J A = J\}
\end{aligned}
\tag{2.13}
$$

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

$$
\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \qquad x^2 + y^2 = 1 \tag{2.14}
$$

where the matrix elements x, y are real. Thus we recognize that $SO(2,\mathbb{R})$ can be identified with the circle. 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:

$$
R(\phi) := \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \tag{2.15}
$$

This is familiar from the implementation of rotations of the Euclidean plane in Cartesian coordinates. 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, and the groups act naturally on various linear spaces. 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. Lie groups will be discussed in Chapters **** below.

Exercise

a.) Check that each of the above sets (2.6),(2.7),(2.8), (2.13), are indeed subgroups of the general linear group.

b.) In (2.13) we could have defined $Sp(2n, \kappa)$ to be matrices in $M_{2n}(\kappa)$ such that $A^{tr} J A = J$. Why?

Exercise $O(2, \mathbb{R})$

Show from the definition above of $O(2, \mathbb{R})$ that the most general element of this group is the form of (2.14) above, OR, of the form

$$\begin{pmatrix} x & y \\ y & -x \end{pmatrix} \qquad x^2 + y^2 = 1 \tag{2.16}$$

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

$$\{f, g\} = \sum_{i=1}^{n} \left(\frac{\partial f}{\partial q^i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial q^i} \right) \tag{2.17}$$

a.) Show that

$$\{q^i, q^j\} = \{p_i, p_j\} = 0 \qquad \{q^i, p_j\} = \delta^i{}_j \tag{2.18}$$

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

$$\begin{pmatrix} Q^1 \\ \vdots \\ Q^n \\ P_1 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1,2n} \\ \vdots & \ddots & \vdots \\ a_{2n,1} & \cdots & a_{2n,2n} \end{pmatrix} \cdot \begin{pmatrix} q^1 \\ \vdots \\ q^n \\ p_1 \\ \vdots \\ p_n \end{pmatrix} \tag{2.19}$$

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

b.) Show that

$$\{Q^i, Q^j\} = \{P_i, P_j\} = 0 \qquad \{Q^i, P_j\} = \delta^i_j \tag{2.20}$$

if and only if A is a symplectic matrix.

Example 2.7 *Function spaces as groups.*

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

$$\mathcal{F}[X \to G] = \{f : f \text{ is a function from } X \to G\} \tag{2.21}$$

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:

$$(f_1 \cdot f_2)(x) := f_1(x) \cdot f_2(x) \tag{2.22}$$

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

If X or G has an infinite set of points then this is an infinite order group. If X is a 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:

$$LG = \{Maps : f : S^1 \to G\} \tag{2.23}$$

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.*

Example 2.8: *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. 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 group of manifolds. One can ask simple questions about them whose answers are unknown.

Example 2.9: *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

$$Y_1 + Y_2 := (Y_1 - Y_2) \cup (Y_2 - Y_1) \tag{2.24}$$

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

$$2Y = \emptyset = 0 \tag{2.25}$$

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:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2') \tag{2.26}$$

Check the group axioms.

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:

$$\sigma^1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.27}$$

$$\sigma^2 := \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \tag{2.28}$$

$$\sigma^3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.29}$$

a.) Show that they satisfy the identity

$$\boxed{\boxed{\sigma^i \sigma^j = \delta^{ij} + \mathrm{i}\epsilon^{ijk}\sigma^k}} \tag{2.30}$$

b.) Show that the set of matrices

$$Q = \{\pm 1, \pm \mathrm{i}\sigma^1, \pm \mathrm{i}\sigma^2, \pm \mathrm{i}\sigma^3\} \tag{2.31}$$

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

c.) Show that the set of matrices

$$P = \{\pm 1, \pm \mathrm{i}, \pm\sigma^1, \pm\sigma^2, \pm\sigma^3, \pm \mathrm{i}\sigma^1, \pm \mathrm{i}\sigma^2, \pm \mathrm{i}\sigma^3\} \tag{2.32}$$

forms a group of order 16. It is known as the *Pauli group.*

The Pauli group is used in quantum information theory. Note that if we have a chain of N spin 1/2 particles then the N^{th} direct product

$$P^N = \underbrace{P \times \cdots \times P}_{N \text{ times}} \tag{2.33}$$

acts naturally on this chain of particles. [8]

---

[8] See Chapter 3 for the formal definition of a group action on a space.

3. Homomorphism and Isomorphism

Definition 3.1: Let G, G' be two groups,

1.) A *homomorphism* $\mu : G \to G'$ is a mapping that preserves the group law

$$\mu(\underbrace{g_1 g_2}_{\text{product in G}}) = \overbrace{\mu(g_1)\mu(g_2)}^{\text{product in G}'} \tag{3.1}$$

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 $G = G'$.

Remarks

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

2. 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 $\mu(\bar{r})\overline{kr}$ where kr is ordinary multiplication of integers. 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 $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ this exchanges $\bar{1}$ and $\bar{2}$. We will discuss this kind of example in greater detail in Section §9 below.

3. One kind of homomomorphism is especially important:

   Definition 3.2: A *matrix representation* of a group G is a homomorphism $T : G \to GL(n, k)$ for some positive integer n and field k.

Exercise *Some simple isomorphisms*

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

b.) Consider the group of N^{th} roots of unity $\{1, \omega, \dots, \omega^{N-1}\}$, $\omega = \exp(2\pi i/N)$, with multiplication of complex numbers as the group operation. Show that this group is isomorphic to $\mathbb{Z}_N$.

Exercise

Show that:

$$\mu(1_G) = 1_{G'} \tag{3.2}$$

$$\mu(g^{-1}) = \mu(g)^{-1} \tag{3.3}$$

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 the group $\{e, \sigma\}$ with group multiplication $\sigma^2 = e$. (As we will see in the next section, this is just the symmetric group on two letters.) Consider the group:

$$\hat{S}_2 = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \} \tag{3.4}$$

with multiplication being matrix multiplication.
Define $\mu : S_2 \to \hat{S}_2$

$$\begin{aligned} \mu(e) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \mu(\sigma) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned} \tag{3.5}$$

Show this is an isomorphism, and hence a matrix representation of S_2. The main thing to check is:

$$\mu(\sigma \cdot \sigma) \overset{?}{=} \mu(\sigma) \cdot \mu(\sigma) \tag{3.6}$$

Exercise

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

$$\mu : \omega^j \mapsto \begin{pmatrix} \cos(\frac{2\pi j}{N}) & \sin(\frac{2\pi j}{N}) \\ -\sin(\frac{2\pi j}{N}) & \cos(\frac{2\pi j}{N}) \end{pmatrix} \tag{3.7}$$

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

3.1 Group Actions On Sets

Recall that we defined:

Definition 1: 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. Another way to say it 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:

$$\phi(g_1, \phi(g_2, x)) = \phi(g_1 g_2, x) \tag{3.8}$$

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

$$\phi(1_G, \phi(1_G, x)) = \phi(1_G, x) \tag{3.9}$$

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

$$\phi(1_G, x) = x \qquad \forall x \in X. \tag{3.10}$$

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 (3.8). 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 identity transformation. This follows from (3.10). 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 ****

The following general idea is of great importance in 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. We can also impose various conditions, e.g. if X and Y are manifolds we could ask our maps to be continuous, differentiable, etc. 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 the function whose values are:

$$\tilde{\phi}(g, F)(x) := F(\phi(g^{-1}, x)) \tag{3.11}$$

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

$$\begin{aligned}
\tilde{\phi}(g_1, \tilde{\phi}(g_2, F))(x) &= \tilde{\phi}(g_2, F)(\phi(g_1^{-1}, x)) \\
&= F(\phi(g_2^{-1}, \phi(g_1^{-1}, x)) \\
&= F(\phi(g_2^{-1} g_1^{-1}, x)) \\
&= F(\phi((g_1 g_2)^{-1}, x)) \\
&= \tilde{\phi}(g_1 g_2, F)(x)
\end{aligned} \tag{3.12}$$

and hence $\tilde{\phi}(g_1, \tilde{\phi}(g_2, F)) = \tilde{\phi}(g_1 g_2, F)$ as required for a group action. As just one 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.

4. The Symmetric Group.

The symmetric group is an important example of a finite group. As we shall see later all finite groups are 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:

$$\begin{aligned} (\phi_1 \cdot_L \phi_2)(i) &:= \phi_2(\phi_1(i)) \\ (\phi_1 \cdot_R \phi_2)(i) &:= \phi_1(\phi_2(i)) \end{aligned} \tag{4.1}$$

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

$$\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix} \tag{4.2}$$

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:

$$\phi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p_{a_1} & p_{a_2} & \cdots & p_{a_n} \end{pmatrix} \tag{4.3}$$

where $a_1, \dots, a_n$ is any permutation of $1, \dots, n$. With this understood, suppose

$$\begin{aligned} \phi_1 &= \begin{pmatrix} q_1 & \cdots & q_n \\ 1 & \cdots & n \end{pmatrix} \\ \phi_2 &= \begin{pmatrix} 1 & \cdots & n \\ p_1 & \cdots & p_n \end{pmatrix} \end{aligned} \tag{4.4}$$

Then

$$\phi_1 \cdot_L \phi_2 = \begin{pmatrix} q_1 & \cdots & q_n \\ p_1 & \cdots & p_n \end{pmatrix} \tag{4.5}$$

On the other hand, to compute $\phi_1 \cdot_R \phi_2$ we should represent

$$
\begin{aligned}
\phi_1 &= \begin{pmatrix} 1 & \cdots & n \\ q'_1 & \cdots & q'_n \end{pmatrix} \\
\phi_2 &= \begin{pmatrix} p'_1 & \cdots & p'_n \\ 1 & \cdots & n \end{pmatrix}
\end{aligned}
\tag{4.6}
$$

and then

$$
\phi_1 \cdot_R \phi_2 = \begin{pmatrix} p'_1 & \cdots & p'_n \\ q'_1 & \cdots & q'_n \end{pmatrix} \tag{4.7}
$$

Exercise
a.) Show that the order of the group is $|S_n| = n!$.
b.) Show that if $n_1 \leq n_2$ 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?
d.) In how many ways can you consider S_{n_1} to be a subgroup of S_{n_2} when $n_1 \leq n_2$?

Exercise Show that the inverse of (4.2) is the permutation:

$$
\phi = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ 1 & 2 & \cdots & n \end{pmatrix} \tag{4.8}
$$

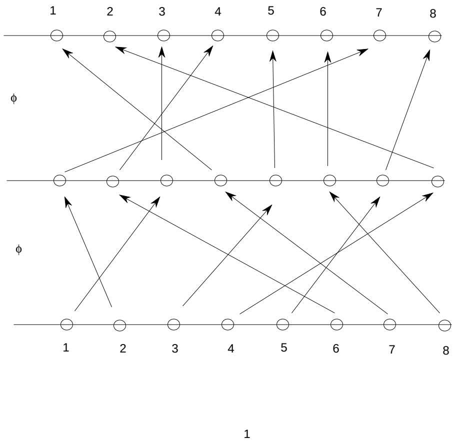

Figure 1: A pictorial view of the composition of two permutations ϕ_1, ϕ_2 in S_8. Thus $1 \to 3, 2 \to 7$ etc. for the group product $\phi_2 \cdot \phi_1$.

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

Exercise *Left versus right*

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

$$\phi_1 \cdot_L \phi_2 = (\phi_1^{-1} \cdot_R \phi_2^{-1})^{-1} \tag{4.9}$$

c.) Interpret (4.9) pictorially by running time backwards. [9]

4.1 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,s observation known as the

The rearrangement lemma: Consider a finite group

$$G = \{g_1, \dots, g_n\} \tag{4.10}$$

(consider this as an ordered set). Then, for any $h \in G$ consider the set

$$\{h \cdot g_1, \dots, h \cdot g_n\}. \tag{4.11}$$

(again, as an ordered set), is a list of distinct elements which is just a rearrangement, i.e. a permutation of (4.10).

You should find it easy to prove the rearrangement lemma. We will come back to this point several times, so prove it carefully.

By considering the left-multiplication of G on itself we see that any group element $a \in G$ defines a permutation of G, denoted $L(a)$, by:

$$L(a) : g \mapsto a \cdot g \tag{4.12}$$

Note that $L(a_1) \circ L(a_2) = L(a_1 \cdot a_2)$ so $a \to L(a)$ is a homomorphism. This is an example of a group action on a set. In this case $X = G$ and G is acting on itself.

Now consider any finite group G. We take $N = |G|$ and prove (the proof is easy) that $a \to L(a)$ is an isomorphism to a subgroup of S_N.

[9] Hint: The notion of inverse is convention-independent, so ϕ^{-1} is the same permutation whether we use $\cdot_L$ or $\cdot_R$. So now write $(\phi_1 \cdot_L \phi_2)^{-1} = \phi_1^{-1} \cdot_R \phi_2^{-1}$.

Exercise *Right action*

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

$$R(a) : g \mapsto g \cdot a \tag{4.13}$$

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 <u>not</u> 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.

4.2 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:

$$a_1 \to a_2 \to \cdots \to a_\ell \to a_1 \tag{4.14}$$

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

$$\phi = (a_1 a_2 \dots a_\ell). \tag{4.15}$$

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

$$(a_1 a_2 \dots a_\ell) = (a_2 a_3 \dots a_\ell a_1) = (a_3 \dots a_\ell a_1 a_2) = \cdots = (a_\ell a_1 a_2 \dots a_{\ell-1}) \tag{4.16}$$

So:

$$S_2 = \{1, (12)\} \tag{4.17}$$

$$S_3 = \{1, (12), (13), (23), (123), (132)\} \tag{4.18}$$

$$\begin{aligned} S_4 = \{1, (12), (13), (14),&(23), (24), (34), (12)(34), (13)(24), (14)(23), \\ (123), (132), (124), (142),&(134), (143), (234), (243) \\ &(1234),(1243), (1324), (1342), (1423), (1432)\} \end{aligned} \tag{4.19}$$

Note that every permutation above is a product of cyclic permutations on disjoint sets of integers. A little thought shows that this is quite general:

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

$$\sigma = (12)(34)(10,11)(56789) \tag{4.20}$$

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[10]

$$\begin{aligned}(12)\cdot(13) &= (132)\\ (13)\cdot(12) &= (123)\end{aligned} \tag{4.21}$$

4.3 Transpositions

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

$$\begin{gathered}(ij)\cdot(jk)\cdot(ij) = (ik) = (jk)\cdot(ij)\cdot(jk)\\ (ij)^2 = 1\\ (ij)\cdot(kl) = (kl)\cdot(ij) \qquad\qquad \{i,j\}\cap\{k,l\} = \emptyset\end{gathered} \tag{4.22}$$

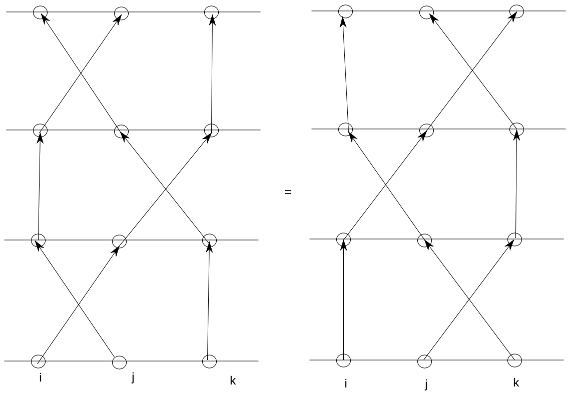

Figure 2: Pictorial illustration of equation (4.21) line one for transpositions. Note that the identity is suggested by "moving the time lines" holding the endpoints fixed. Reading time from bottom to top corresponds to reading the composition from left to right in the $\cdot_R$ convention.

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

$$(1,k)(1,k-1)\cdots(1,4)(1,3)(1,2) = (1,2,3,4,\dots,k) \tag{4.23}$$

Now, consider a permutation that takes

$$1 \to a_1, \quad 2 \to a_2, \quad 3 \to a_3, \cdots, k \to a_k \tag{4.24}$$

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

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

$$\phi \circ (1\ 2\ \cdots\ k) \circ \phi^{-1} = (a_1\ a_2\ \cdots\ a_k) \tag{4.25}$$

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* (4.21). We say that the transpositions *generate* the permutation group. Taking products of various transitions – 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 §5 below.

Of course, a given permutation can be written as a product of transpositions in many ways. This clearly follows because of the identities (4.22). A nontrivial fact is that the transpositions together with the above relations generate precisely the symmetric group. 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 (4.22) 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
a.) What is the order of A_n ?
b.) Write out the even elements of S_4, that is, write out A_4.

Exercise
When do two transpositions commute? Illustrate the answer with pictures, as above.

Exercise *Smaller set of generators*

Show that from the transpositions $\sigma_i := (i, i+1)$, $1 \le i \le n-1$ 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 $(1\ 2\ \cdots\ n)$. [11]

Exercise *Center of S_n*
What is the center of S_n?

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

♣Need to provide answer in a footnote to above exercise, which is a little hard. ♣

Example 3.2 *The sign homomorphism.*
This is a very important example of a homomorphism:

$$\epsilon : S_n \to \mathbb{Z}_2 \tag{4.26}$$

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:

$$\epsilon_{i_1 \cdots i_n} \tag{4.27}$$

Its value is:

1. $\epsilon_{i_1 \cdots i_n} = 0$ if two indices are repeated.
2. $\epsilon_{i_1 \cdots i_n} = +1$ if

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{4.28}$$

[11] *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.

is an even permutation.

3. $\epsilon_{i_1 \cdots i_n} = -1$ if

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{4.29}$$

is an odd permutation.

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

$$\begin{aligned} \epsilon_{123} &= 1 \\ \epsilon_{132} &= -1 \\ \epsilon_{231} &= +1 \\ \epsilon_{221} &= 0 \end{aligned} \tag{4.30}$$

and so forth.

Exercise

Show that

$$\epsilon_{i_1 i_2 \cdots i_n} \epsilon_{j_1 j_2 \cdots j_n} = \sum_{\sigma \in S_n} \epsilon(\sigma) \delta_{i_1 j_{\sigma(1)}} \delta_{i_2 j_{\sigma(2)}} \cdots \delta_{i_n j_{\sigma(n)}} \tag{4.31}$$

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 $\mathbb{R}^3$:

$$\vec{A} \times (\vec{B} \times \vec{C}) = \vec{B}(\vec{A} \cdot \vec{C}) - \vec{C}(\vec{A} \cdot \vec{B}) \tag{4.32}$$

Exercise *A Matrix Representation Of S_n*

Consider the standard Euclidean vector space 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: $T(\phi) : \vec{e}_i \to \vec{e}_{\phi(i)}$. Thus to any permutation $\phi \in S_n$ we can associate a linear transformation $T(\phi)$.

a.) Write out the matrices $A(\phi)$ of $T(\phi)$ relative to the basis $\vec{e}_i$ explicitly for small values of n:

$$T(\phi)\vec{e}_i = \sum_{j=1}^{n} A(\phi)_{ji} \vec{e}_j \tag{4.33}$$

b.) Write a general formula for the matrix elements of $A(\phi)$. [12]

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

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

$$\left(A(\phi) B A(\phi)^{-1}\right)_{i,j} = B_{\phi(i),\phi(j)} \tag{4.34}$$

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 $W(B_n) \to S_n$.

See chapter 2 below for any terms in linear algebra that might not be familiar.

4.4 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

$$0, n, 1, n+1, 2, n+2, \dots, n+2, 2n-2, n-1, 2n-1 \tag{4.35}$$

Another way to express this is that the Out-shuffle defines a permutation of $\{0, 1, \dots, 2n-1\}$ defined by the formula:

$$\mathcal{O}(x) = \begin{cases} 2x & x \leq n-1 \\ 2x - (2n-1) & n \leq x \leq 2n-1 \end{cases} \tag{4.36}$$

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 $2^k = 1 \mathrm{mod}(2n-1)$ 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:

$$\begin{aligned} \mathcal{O} = {} & (0)(1,2,4,8,16,32,13,26)(3,6,12,24,48,45,39,27) \\ & (5,10,20,40,29,7,14,28)(9,18,36,21,42,33,15,30) \\ & (11,22,44,37,23,46,41,31)(17,34)(19,38,25,50,49,47,43,35)(51) \end{aligned} \tag{4.37}$$

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

$$\mathcal{D}(2n) \to \mathcal{D}(2n+2) \tag{4.38}$$

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

$$\mathcal{I}(x) = \begin{cases} 2(x+1)-1 & x+1 \leq n \\ 2(x+1)-(2n+1)-1 & n \leq x \leq 2n-1 \end{cases} \tag{4.39}$$

One can check that this is given by the uniform formula

$$\mathcal{I}(x) = (2x+1) \,\mathrm{mod}(2n+1) \tag{4.40}$$

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

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

$$\begin{gathered} (0,1,3,7,15,31,10,21,43,34,16,33,14,29,6,13,27,2,5, \\ 11,23,47,42,32,12,25,51,50,48,44,36,20,41,30,8,17, \\ 35,18,37,22,45,38,24,49,46,40,28,4,9,19,26) \end{gathered} \tag{4.41}$$

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:

$$\ell = 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2^1 + a_0 \tag{4.42}$$

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: $1a_{k-1}a_{k-2}\cdots a_1a_0$.

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

$$\begin{aligned}
0 &\to 1 \\
&\to 2\cdot 1 + a_{k-1} \\
&\to 2\cdot(2\cdot 1 + a_{k-1}) + a_{k-2} = 2^2 + 2a_{k-1} + a_{k-2} \\
&\to 2\cdot(2^2 + 2a_{k-1} + a_{k-2}) + a_{k-3} = 2^3 + 2^2a_{k-1} + 2a_{k-2} + a_{k-3} \\
\vdots &\quad \vdots \\
&\to 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2^1 + a_0 = \ell
\end{aligned} \tag{4.43}$$

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

$$\phi : W(B_n) \to S_n \tag{4.44}$$

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 §12.4 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:

$$m : \{1,2,\dots,2n\} \to \{2n, 2n-2, \dots, 4, 2, 1, 3, 5, \dots, 2n-3, 2n-1\} \tag{4.45}$$

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

$$m(x) = \mathrm{Min}[2x, 2n+1-2x] \tag{4.46}$$

In particular for $2n = 12$ we have

$$\{1,2,3,4,5,6,7,8,9,10,11,12\} \to \{12,10,8,6,4,2,1,3,5,7,9,11\} \tag{4.47}$$

which has cycle decomposition (check!)

$$(3\ 8) \cdot (1\ 12\ 11\ 9\ 5\ 4\ 6\ 2\ 10\ 7) \tag{4.48}$$

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

$$|M_{12}| = 2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95040 \tag{4.49}$$

Compare this with the order of S_{12}:

$$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 = 479001600 \tag{4.50}$$

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?

---

5. Generators and relations

The presentation (4.22) of the symmetric group is an example of presenting a group by *generators and relations.*

Definition 5.1 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

$$g = s_{i_1} \cdots s_{i_r} \tag{5.1}$$

where, for each $1 \le k \le r$ 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. [13]

In general if we have a finitely generated group we write

$$G = \langle g_1, \dots, g_n | R_1, \cdots R_r \rangle \tag{5.2}$$

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 $\mathcal{S}$. Also, it is sometimes convenient to include s^{-1} in $\mathcal{S}$ if $s \in \mathcal{S}$. Such generating sets are said to be *symmetric*. Then we should add the relation $s \cdot s^{-1} = 1$. Otherwise it is understood, in making our words that we can raise s to an integer power s^n where, if $n < 0$, this means $(s^{-1})^{|}n|$.

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

$$\langle a | a^N = 1 \rangle \tag{5.3}$$

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

$$\begin{gathered} a^{n_1} b^{m_1} \cdots a^{n_k} \\ a^{n_1} b^{m_1} \cdots b^{m_k} \\ b^{n_1} a^{m_1} \cdots a^{n_k} \\ b^{n_1} a^{m_1} \cdots b^{m_k} \end{gathered} \tag{5.4}$$

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.

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

From Wikipedia, the free encyclopedia

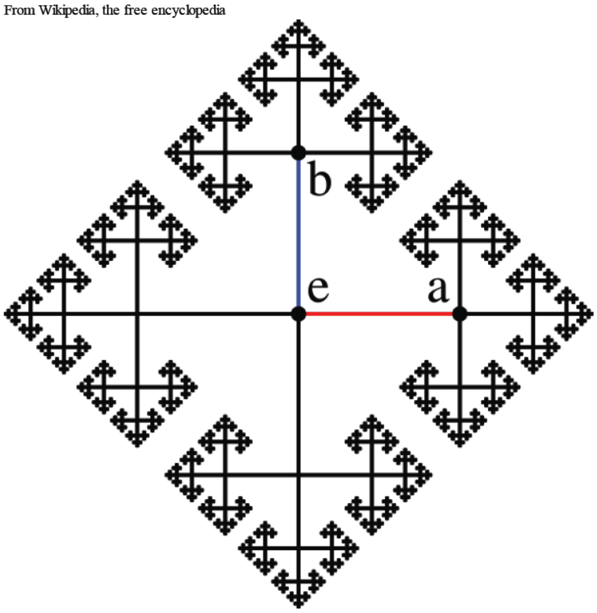

Figure 3: The Cayley graph for the free group on 2 generators a and b.

Example 2.4: *Coxeter groups*: Let m_{ij} by an $n \times n$ symmetric matrix whose entries are positive integers or ∞, such that $m_{ii} = 1$, $1 \le i \le n$, and $m_{ij} \ge 2$ or $m_{ij} = \infty$ for $i \neq j$. Then a *Coxeter group* is the group with generators and relations:

$$\langle s_1, \dots, s_n | \forall i, j : (s_i s_j)^{m_{ij}} = 1 \rangle \tag{5.5}$$

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

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

$$s_i^2 = 1 \tag{5.6}$$

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:

$$s_i s_j s_i = s_j s_i s_j \tag{5.7}$$

These groups have nice geometrical interpretations as groups of reflections (note $s_i^2 = 1$!!) in higher-dimensional spaces. In particular, we will see that all the Weyl groups of simple Lie algebras are Coxeter groups. Coxeter's main theorem (from the 1930's) was a classification of the finite Coxeter groups. He 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 $m_{ij} \ge 3$. 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

Coxeter's theorem states that all finite Coxeter groups are groups of *reflections* in some Euclidean space. That is, there is some vector space $\mathbb{R}^N$ with vectors v_i and inner product

$$v_i \cdot v_j = -\cos(\frac{\pi}{m_{i,j}}) \tag{5.8}$$

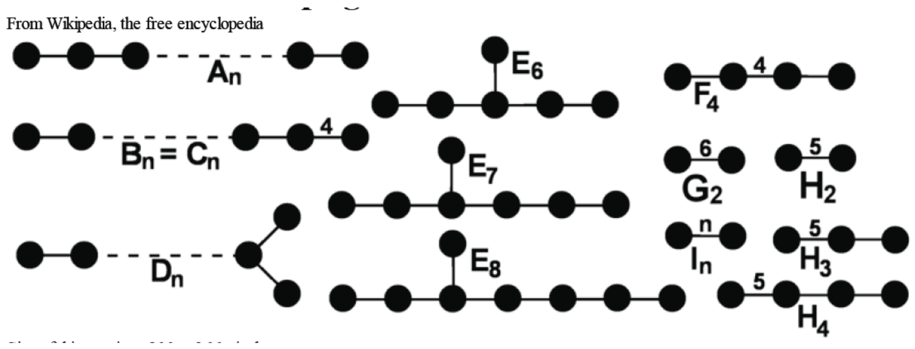

Figure 4: Coxeter's list of finite Coxeter groups.

so that the group is the group of reflections in the vectors v_i.

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 just the symmetric group S_{n+1}. That is clear from some of the presentations we have given of the symmetric group. The case $B_n = C_n$ is the group of centrally symmetric permutations $\mathcal{W}B_n \subset S_{2n}$ discussed in card-shuffling. (These statements are not meant to be obvious.)

♣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, $g_i' = \phi(g_i)$. Moreover, the images g_i' must satisfy the same relations as the g_i. This puts useful constraints on what homomorphisms you can write down. For example 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! [GIVE REF!] However, for many important finitely presented groups the word problem can be solved.

2. 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.

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 $\mu : \mathbb{Z}_N \to \mathbb{Z}$. [14]

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 Show that

$$\langle a, b | a^3 = 1, b^2 = 1, abab = 1 \rangle \tag{5.9}$$

is a presentation of S_3

Exercise

Show that S_n is a Coxeter group: There are generators σ_i, $i = 1, \dots, n-1$ with $\sigma_i^2 = 1$, $1 \le i \le (n-1)$, $(\sigma_i \sigma_{i+1})^3 = 1$, $1 \le i \le n-2$, $(\sigma_i \sigma_j)^2 = 1$ for $|i - j| > 1$.

Exercise

Consider the group with presentation:

$$\langle T, S | (ST)^3 = 1, S^2 = 1 \rangle \tag{5.10}$$

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 <u>minimal</u> set of generators $\mathcal{S}_1 \subset \mathcal{S}_2 \subset \cdots$ of cardinality $|\mathcal{S}_k| = k$. Show that $2|G_k| \le |G_{k+1}|$ and hence as $k \to \infty$ the order $|G_k|$ must grow at least as fast as 2^k.

[14] *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.

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

$$d(G) \leq C \frac{n}{\sqrt{\log n}} \tag{5.11}$$

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 $n \geq 3$:

$$d(G) \leq C \frac{\log n}{\sqrt{\log \log n}} \tag{5.12}$$

Moreover, these results are asymptotically the best possible. For a review of such results see. [15]

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 $G_1 \times G_2$. [16]

5.1 Fundamental Groups In Topology

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

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.

Consider a surface, perhaps with punctures as shown in Figure 5. By cutting along the paths shown there the surface unfolds to a presentation by gluing as in Figure 6:

From these kinds of constructions one can prove [17] that the fundamental group of an orientable surface with g handles and p punctures will be

$$\pi_1(S, x_0) = \langle a_i, b_i, c_s | \prod_{i=1}^{g} [a_i, b_i] \prod_{s=1}^{p} c_s = 1 \rangle \tag{5.13}$$

There is only one relation so this is very close to a free group! In fact, for $g = 0$, and p punctures it is a free group on $p - 1$ generators. Groups of the form (5.13) are sometimes called *surface groups.*

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

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

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

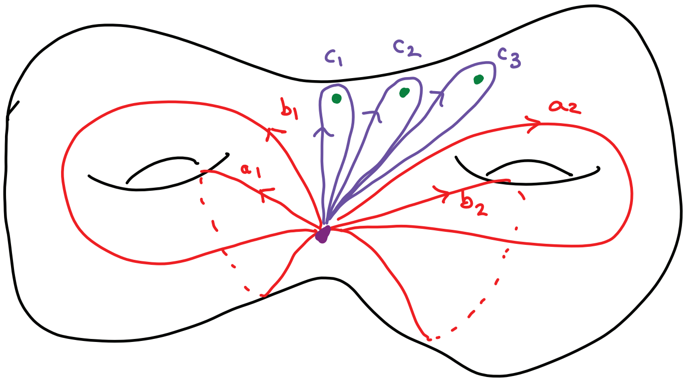

Figure 5: A collection of closed paths at x_0 which generate the fundamental group of a two-dimensional surface with two handles and three (green) holes.

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

$$\langle a, b | a^2 = b^2 \rangle \tag{5.14}$$

and the other is

$$\langle g_1, g_2 | g_1 g_2 g_1 g_2^{-1} = 1 \rangle \tag{5.15}$$

Show that these two presentations are equivalent.

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 7. Note that $\tilde{\sigma}_i^{-1}$ is the undercrossing.

Now one verifies the relations

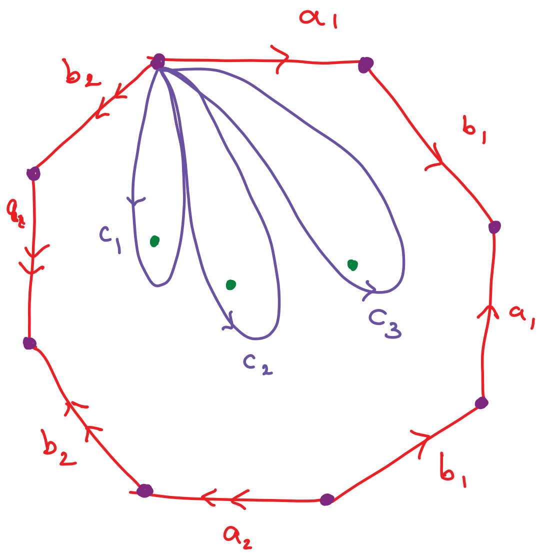

Figure 6: When the directed edges are identified according to their labels the above surface reproduces the genus two surface with three punctures. Since the disk is simply connected we derive one relation on the curves shown here.

$$\tilde{\sigma}_i \tilde{\sigma}_j = \tilde{\sigma}_j \tilde{\sigma}_i \qquad\qquad |i-j| \geq 2 \tag{5.16}$$

and

$$\tilde{\sigma}_i \tilde{\sigma}_{i+1} \tilde{\sigma}_i = \tilde{\sigma}_{i+1} \tilde{\sigma}_i \tilde{\sigma}_{i+1} \tag{5.17}$$

where the relation (5.17) is illustrated in Figure 8.

The braid group $\mathcal{B}_n$ may be defined as the group generated by $\tilde{\sigma}_i$ subject to the relations (5.16)(5.17):

$$\mathcal{B}_n := \langle \tilde{\sigma}_1, \dots, \tilde{\sigma}_{n-1} | \tilde{\sigma}_i \tilde{\sigma}_j \tilde{\sigma}_i^{-1} \tilde{\sigma}_j^{-1} = 1, |i-j| \geq 2; \tilde{\sigma}_i \tilde{\sigma}_{i+1} \tilde{\sigma}_i = \tilde{\sigma}_{i+1} \tilde{\sigma}_i \tilde{\sigma}_{i+1} \rangle \tag{5.18}$$

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.

♣say more? return to it in section on group actions on spaces. ♣

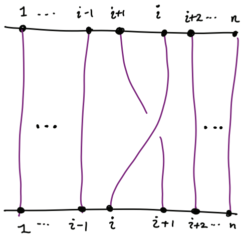

Figure 7: Pictorial illustration of the generator σ_i of the braid group B_n.

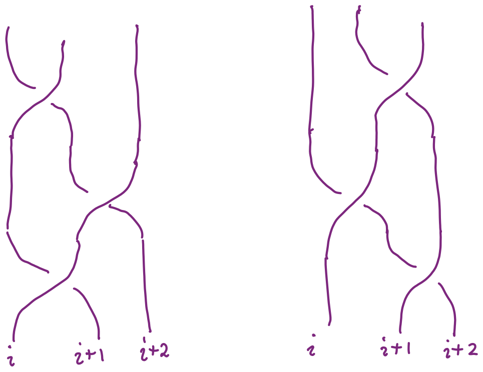

Figure 8: Pictorial illustration of the Yang-Baxter relation.

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
Define a homomorphism $\mu : \mathcal{B}_n \to S_n$.
Can you define a homomorphism $s : S_n \to \mathcal{B}_n$ so that $\mu \circ s$ is the identity transforma-

tion?

Remarks

1. In the theory of integrable systems the relation (5.17) 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. Intuitively, a system of n *identical* particles should have an S_n symmetry. We will make this notion more precise later. 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. In nonrelativistic systems the rotational group of space $SO(d)$ and its projective representations are important. Again 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. [18] 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. There can be interesting 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:

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

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

[18] 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.

6. Cosets and conjugacy

6.1 Equivalence Relations

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

Definition 6.1.1 . 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 6.1.1 : $\sim$ is $=$.

Example 6.1.2 : $X = \mathbb{Z}$, $a \sim b$ if $a - b$ is even.

Definition 6.1.2: Let $\sim$ be an equivalence relation on X. The *equivalence class* of an element a is

$$[a] \equiv \{x \in X : x \sim a\} \tag{6.1}$$

In the above two examples we have

Example 6.1.1' : $[a] = \{a\}$

Example 6.1.2' :
$[1] = \{n : n \text{ is an odd integer}\}$
$[4] = \{n : n \text{ is an even integer}\}$.
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.

6.2 Lagrange Theorem

Definition 6.2.1: Let $H \subseteq G$ be a subgroup. The set

$$gH \equiv \{gh | h \in H\} \subset G \tag{6.2}$$

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:

$$\begin{aligned} 1 \cdot H &= \{1, (12)\} \\ (12) \cdot H &= \{(12), 1\} = \{1, (12)\} \\ (13) \cdot H &= \{(13), (123)\} \\ (23) \cdot H &= \{(23), (132)\} \\ (123) \cdot H &= \{(123), (13)\} = \{(13), (123)\} \\ (132) \cdot H &= \{(132), (23)\} = \{(23), (132)\} \end{aligned} \tag{6.3}$$

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. [19]

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

$$|G|/|H| \in \mathbb{Z}_+ \tag{6.4}$$

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:

$$|g_i H| = |H| \tag{6.5}$$

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

This theorem is simple, but powerful: for example, we can conclude immediately that $\mathbb{Z}_p$ has no nontrivial subgroups for p prime. In particular, $\mathbb{Z}_{137}$ has no nontrivial subgroups.

Definition 6.2.2: If G is any group and H any subgroup then the *set of left cosets* is denoted G/H. It 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

$$G/H = \{H, (13)(24) \cdot H, (123) \cdot H, (132) \cdot H, (124) \cdot H, (142) \cdot H\} \tag{6.6}$$

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

Remark Note well! If $H \subset G$ is a subgroup and $g_1 H = g_2 H$ it does not 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. [20]

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

Theorem 6.2.2: (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 6.5 below. Actually, Sylow has more to say. We will say a bit 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. It is very easy to give examples of elements with infinite order in infinite groups. Some infinite groups have no elements of finite order

[20] *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. An infinite class of counterexamples is in fact provided by A_n, for $n \geq 4$. As we describe below, A_n for $n \geq 5$ are all simple groups. Moreover, $|A_n|$ 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 nonabelian 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.

(other than the identity) while some infinite groups have elements both of finite and infinite order.

Exercise *Subgroups of A_4*
a.) Write down all the subgroups of A_4.
b.) Write down the 2-Sylow and 3-Sylow subgroups of A_4.

6.3 Conjugacy

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

Definition 6.3.1 :

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:

$$C(h) := \{ghg^{-1} : g \in G\} \tag{6.7}$$

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

$$K = gHg^{-1} := \{ghg^{-1} : h \in H\} \tag{6.8}$$

Example 6.3.1 : 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.

Groups which are self-conjugate are very special:

Definition 6.3.2: A subgroup $N \subseteq G$ is called a *normal* subgroup, or an *invariant* subgroup if

$$gNg^{-1} = N \qquad \forall g \in G \tag{6.9}$$

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. [21] However, if H is normal something special happens:

[21] 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.

Theorem 6.3.1. 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:

$$(g_1 N) \cdot (g_2 N) := (g_1 \cdot g_2) N \tag{6.10}$$

Proof- left as an exercise:

The main thing to check is that the produce law defined by (6.10) is actually well defined. If $g_1 N = g_1' N$ do you get the same answer from (6.10) ? Show this carefully.

Once we see that (6.10) 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. ♠

Example 6.3.1 . All subgroups N of abelian groups A are normal, and moreover the quotient group A/N is abelian. For example $N\mathbb{Z} \subset \mathbb{Z}$ is normal, and the quotient group is $\mathbb{Z}/N\mathbb{Z}$, explaining the previous notation. So $\bar{r}$ is the equivalence class of an integer $r \in \mathbb{Z}$.

Example 6.3.2 . Consider the abelian group $\mathbb{C}$ of complex numbers with normal addition as the group operation. If τ is a complex number with nonzero 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 $\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$. This is a very interesting Abelian group related to the theory of "elliptic curves." 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. Thus we have an abelian group that is a compact manifold.

Example 6.3.3.

$$A_3 \equiv \{1, (123), (132)\} \subset S_3 \tag{6.11}$$

is normal. What group is S_3/A_3?

Example 6.3.4. 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*.

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 *Normal subgroups*

a.) Check the details of the proof of Theorem 6.3.1 !

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

c.) Warning! Equation (6.9) does *not* mean that $gng^{-1} = n$ for all $n \in N$! Construct a counterexample using a normal subgroup of S_3.

d.) 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? [22]

Exercise

Look at the 3 examples of homogeneous spaces G/H in section 6.2. Decide which of the subgroups H is normal and what the group G/H would be.

Exercise *Even permutations*

Example 6.3.2 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. Show that the even permutations, A_n, form a normal subgoup of S_n. (Hint: use the above exercise.) What is S_n/A_n?

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.

[22] *Answer* (d): 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 $G/H \cong \mathbb{Z}_2$.

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 (5.13). The abelianization of this group is called the *homology group* $H_1(S)$ where S is the punctured surface. Compute this group.

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.

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

Exercise

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

6.4 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 $i_1, i_2, \ldots$ by their images under g. That is, if $g(i_a) = j_a$, $a = 1, \ldots, k$, 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:

$$(12)(123)(12)^{-1} = (213) = (132) \tag{6.12}$$

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

3. *Therefore, the conjugacy classes in S_n are labeled by specifying the number, denoted ℓ_j of distinct cycles of length j we have 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 $(ab)(cd)$:

$$(12)(34), \qquad (13)(24), \qquad (14)(23) \tag{6.13}$$

Note that these can be conjugated into each other by suitable transpositions.

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

$$(1)^{\ell_1}(2)^{\ell_2}\cdots(n)^{\ell_n} \tag{6.14}$$

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

$$n = 1\cdot\ell_1 + 2\cdot\ell_2 + \cdots n\cdot\ell_n = \sum_{j=1}^{n} j\cdot\ell_j \tag{6.15}$$

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 $p(n)$. [23]

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

[23] 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 (6.14).

Exercise *Order of the conjugacy class*

Given a conjugacy class of type (6.14) compute the order $|C(g)|$. [24]

6.4.1 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. ♣

Conjugacy classes of the symmetric group come up in several ways in string theory and conformal field theory. We'll give a taste of how that happens here. Suppose we have a system (such as a string) which is described by an infinite collection of harmonic oscillators:

$$[a_j, a_k] = 0 \qquad [a_j^\dagger, a_k^\dagger] = 0 \qquad [a_j, a_k^\dagger] = \delta_{j,k} \qquad j, k = 1, \dots \tag{6.16}$$

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 $\omega, 2\omega, 3\omega, \dots$. The Hamiltonian is, formally,

$$H^{\text{formal}} = \sum_{j=1}^{\infty} j\omega(a_j^\dagger a_j + \frac{1}{2}) \tag{6.17}$$

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

$$a_j|vac\rangle = 0 \qquad\qquad \forall j \tag{6.18}$$

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

the groundstate energy is infinite. This is typical of the divergences of quantum field theory: 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 identifying

$$\sum_{j=1}^{\infty} \frac{j}{2}\omega = \frac{\omega}{2}\sum_{j=1}^{\infty}\frac{1}{j^{-1}} \to \frac{\omega}{2}\zeta(-1) = -\frac{\omega}{24} \tag{6.19}$$

This can be justified much more rigorously and indeed it gives the correct Casimir energy for a massless scalar field on a circle. In our units above the spatial circle has length 2π. Restoring the radius of the circle so that the length is $2\pi L$ the ground state energy is:

$$E_{\text{ground}} = -\frac{1}{24L} = -\frac{\hbar c}{24L} \tag{6.20}$$

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.

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

$$H = \sum_{j=1}^{\infty} j\omega a_j^\dagger a_j - \frac{\omega}{24} \tag{6.21}$$

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:

$$(a_1^\dagger)^{\ell_1}(a_2^\dagger)^{\ell_2}\cdots(a_n^\dagger)^{\ell_n}|0\rangle \tag{6.22}$$

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:

$$\frac{1}{\prod_{j=1}^{\infty}(1-q^j)} = 1 + \sum_{n=1}^{\infty} p(n)q^n \tag{6.23}$$

Indeed, note that this is the physical partition function of our system of oscillators!

$$Z(\beta) = \text{Tr}e^{-\beta H} = \frac{1}{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)}, \tag{6.24}$$

where we trace over the Hilbert space of states of our collection of oscillators. Here we identify $q = e^{-\beta\omega}$. Expanding out (6.23) gives the first few values of $p(n)$:

$$\begin{aligned}&1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + 11q^6 + 15q^7 + 22q^8 + 30q^9 + \\ &+ 42q^{10} + 56q^{11} + 77q^{12} + 101q^{13} + 135q^{14} + \cdots\end{aligned} \tag{6.25}$$

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

It turns out the generating series has a remarkable "modular transformation property" relating $Z(\beta)$ to $Z(1/\beta)$: [25]

$$\beta^{1/4}Z(\beta) = \tilde{\beta}^{1/4}Z(\tilde{\beta}) \tag{6.26}$$

$$\beta\tilde{\beta} = \left(\frac{2\pi}{\omega}\right)^2 \tag{6.27}$$

which, when combined with the method of stationary phase, allows one to derive the Hardy-Ramanujan formula giving an asymptotic formula for large values of n:

$$p(n) \sim \frac{1}{\sqrt{2}}\big(\frac{1}{24}\big)^{3/4}n^{-1}\text{exp}\left(2\pi\sqrt{\frac{n}{6}}\right) \tag{6.28}$$

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!

Analogs of equation (6.28) 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 $\text{Re}(\beta) > 0$. Note that $q^{1/24}Z(\beta)$ is periodic under imaginary shifts $\beta \to \beta + \frac{2\pi\text{i}}{\omega}$.

Write

$$p(n) = \int_{\beta_0}^{\beta_0 + \frac{2\pi\text{i}}{\omega}} d\beta e^{-n\beta\omega} q^{1/24} Z(\beta) \tag{6.29}$$

and use the above transformation formula, together with the stationary phase method to derive (6.28).

6.4.2 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: $\lambda_i \geq \lambda_{i+1}$.

[25] This is proven in textbooks on analytic number theory. From the physics viewpoint it is quite natural for the following reason: We note that $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ is a torus with a flat metric where τ is a complex number in the upper half-plane. To relate this to our discussion we set $q = e^{2\pi\text{i}\tau} = e^{-\beta\omega}$ so $\tau = \text{i}\frac{\beta\omega}{2\pi}$. Now one considers the path integral of a massless scalar field on this torus. One can easily (and rigorously) compute that path integral and show that it is $(\text{Im}\tau)^{-1/2}|\eta(\tau)|^{-2}$ where $\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$. 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 $z = x + \text{i}y$ 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 field is a conformal field theory, and for a flat metric the path integral will be invariant. Therefore $(\text{Im}\tau)^{-1/2}|\eta(\tau)|^{-2}$ is invariant under $\tau \to -1/\tau$ and since $\eta(\tau)$ is holomorphic one can deduce $\eta(-1/\tau) = (-\text{i}\tau)^{1/2}\eta(\tau)$. This equation is equivalent to the identity stated above.

b.) The λ_i eventually become zero.

Given a partition, we define $|\lambda| = \sum_i \lambda_i$ so that a partition of n can be written:

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_k \tag{6.30}$$

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.

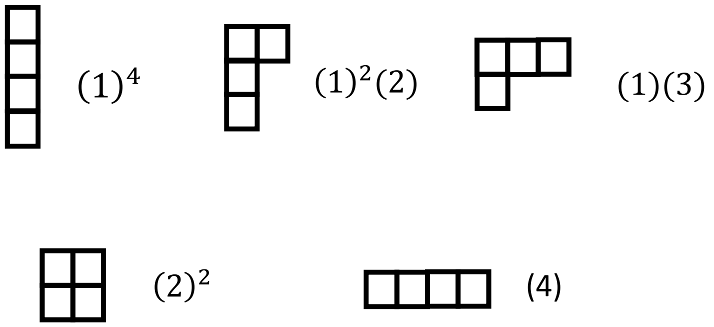

Figure 9: Young diagrams corresponding to the 5 different partitions of 4.

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. We will talk much more about these when discussing representations of the symmetric group and representations of $SU(n)$. To make contact with the other way of thinking about partitions of n you look at the rows with λ_1 boxes. There are ℓ_{λ_1} of these so we have $\ell_j = 0$ for $j > \lambda_1$ and $(\lambda_1)^{\ell_{\lambda_1}}$ then we look at the next longest row. So the parts λ_i are the cycles with nonzero ℓ arranged in order of the longest cycles first. See Figure 9 for an example.

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 (6.30)). The generating function is

$$\sum_{n=1}^{\infty} p_k(n) x^n = \prod_{j=1}^{k} \frac{x}{1-x^j} \tag{6.31}$$

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. [26] 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

$$\bar{k}(n) := \frac{\sqrt{6}}{2\pi}\sqrt{n}\log n \tag{6.32}$$

See Figure 10 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.

6.5 Centralizer And Counting Conjugacy Classes

Definition 6.5.1: Let $g \in G$, the *centralizer subgroup* of g, (also known as the *normalizer subgroup*), denoted, $Z(g)$, is defined to be:

$$Z(g) := \{h \in G | hg = gh\} \tag{6.33}$$

Exercise
Check that $Z(g) \subset G$ is a subgroup. Note that $g^n \in Z(g)$ for any integer n.

Recall that $C(g)$ denotes the conjugacy class of g. Then we have

$$|C(g)| = \frac{|G|}{|Z(g)|} \tag{6.34}$$

The proof is given by constructing a map $\psi : G/Z(g) \to C(g)$ by

$$\psi : g_i Z(g) \to g_i g g_i^{-1} \tag{6.35}$$

1. First, check that this is well-defined.

2. Then note that ψ is 1-1 and onto $C(g)$. (This statement is a special case of the "stabilizer-orbit theorem" discussed below.)

Now, G has a disjoint decomposition into conjugacy classes because conjugacy is an equivalence relation, so we get a very useful counting rule sometimes called the *class equation*:

[26] 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.

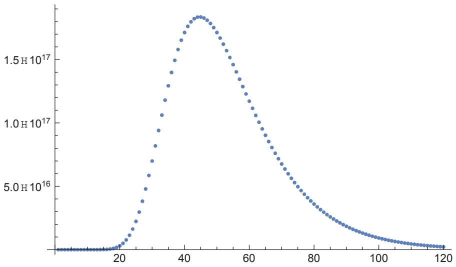

Figure 10: Showing the distribution of $p_k(n)$ as a function of k for $n = 400$ and $1 \leq k \leq 120$. Note that the Erdös-Lehner mean value of k is $\bar{k} = \frac{\sqrt{6}}{2\pi} 20 \log(20) \cong 46.7153$ is a very good approximation to where the distribution has its sharp peak. The actual maximum is at $k = 45$.

$$|G| = \sum_{classes} \frac{|G|}{|Z(g)|} \tag{6.36}$$

The sum is over distinct conjugacy classes. We may choose any element g from a given class 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.

Remarks:

1. In chapter 5 (???) we will study group actions on sets and orbits. The above result is nicely interpreted in terms of the transitive action of G on the conjugacy class $C(g)$.

♣Move this remark to section on lattice gauge theories below. ♣

2. Gauge theories can be formulated for discrete groups just as well as for compact Lie groups. 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
$$Z(S^1) = \frac{1}{|G|}\sum_{g\in G} 1 \tag{6.37}$$
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 $Z(S^1) = 1$, but let us rewrite this using the class equation. We organize the sum into conjugacy classes:
$$Z(S^1) = \frac{1}{|G|}\sum_{cc} |C(g)| = \sum_{cc}\frac{1}{|Z(g)|} \tag{6.38}$$
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. 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!

♣If you don't understand this remark. Don't panic! We will not use it later. ♣

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:
$$|G| = |Z(G)| + \sum_{classes}{}' \frac{|G|}{|Z(a)|} \tag{6.39}$$
where the sum with a prime is over over conjugacy classes bigger than 1. 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 (6.39) 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: We prove it using induction on the order of G.

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.

Now suppose $|G| > p$. We first prove the statement when G is abelian. 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.

Now assume that G is not abelian. By the class equation we can write

$$|G| = |Z(G)| + {\sum}' \frac{|G|}{|Z(g_i)|} \tag{6.40}$$

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. ♠

♣There is a very cool proof using the cyclic action of $\mathbb{Z}/p\mathbb{Z}$ on the set $S = \{(g_1, \dots, g_p)|g_1 \cdots g_p$ $1\}$. Revisit this with the stabilizer-orbit theorem below. ♣

Application 3: *Sylow's theorem*:

Finally, as a third application we give a simple proof of Sylow's first theorem by induction on the order of G: The theorem is clearly OK for $|G| = 1$. Now we use induction on the order of G. Suppose $|G| = p^k m$ with $(m, p) = 1$. We divide the proof into two cases:

1. Suppose 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 so G/N is a group 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.

2. Suppose p does not divide the order of $Z(G)$. Then by the class equation it must not divide $|C(g)| = |G|/|Z(g)|$ for some nontrivial conjugacy class $C(g)$. But that means p^k must divide $|Z(g)| < |G|$. 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? [27]

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 $G = \mathbb{Z}/15\mathbb{Z}$.

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 $\mathbb{Z}_{pq}$.

b.) Why is it important to say that p does not divide $q - 1$?

[27] *Answer*: NO! $\mathbb{Z}_p^k$ is a counterexample: It has order p^k and every element has order p.

Warning!! This is hard. [28]

---

7. Kernel, Image, And Exact Sequence

Given an arbitrary homomorphism

$$\mu : G \to G' \tag{7.1}$$

there is automatically a "God-given" subgroup of both G and G':

Definition 7.1:

a.) The *kernel* of μ is

$$K = \mathrm{ker}\mu := \{g \in G | \mu(g) = 1_{G'}\} \tag{7.2}$$

b.) The *image* of μ is

$$\mathrm{im}\mu := \mu(G) \subset G' \tag{7.3}$$

Exercise

a.) Check that $\mu(G) \subseteq G'$ is indeed a subgroup.

b.) Is $\mu(G)$ always a normal subgroup?

---

[28] *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 $1 \le j_1, j_2 \le (q-1)$ and $j_1 \ne j_2$. So we have to have $b^j ab^{-j} = a$ for some $1 \le j \le (q-1)$. But then $b^j \ne 1$. 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 $s \ge 1$ the RHS is too large. So $s = 0$ but then p would have to divide $q - 1$.

In mathematics one often encounters the notation of an *exact sequence*: Suppose we have three groups and two homomorphisms f_1, f_2

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \tag{7.4}$$

$$\boxed{\text{We say the sequence is } \textit{exact at } G_2 \text{ if } \mathrm{im} f_1 = \ker f_2.}$$

This generalizes to sequences of several groups and homomorphisms

$$\cdots G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots \tag{7.5}$$

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

$$1 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow 1 \tag{7.6}$$

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 (7.6) 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:

$$1 \to K \to G \xrightarrow{\mu} \mathrm{im}(\mu) \to 1 \tag{7.7}$$

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 7.1: Let $K \subseteq G$ be the kernel of a homomorphism (7.1). Then K is a normal subgroup of G.

Proof: $k_1, k_2 \in K \Rightarrow$

$$\begin{aligned} \mu(k_1 k_2) &= \mu(k_1)\mu(k_2) = 1_{G'} \\ \mu(k^{-1}) &= \mu(k)^{-1} = 1_{G'} \end{aligned} \tag{7.8}$$

$\Rightarrow K$ is a subgroup
$\mu(gkg^{-1}) = \mu(g)\mu(k)\mu(g^{-1}) = \mu(g)1_{G'}\mu(g)^{-1} = 1_{G'} \Rightarrow K$ is normal. ♠

It follows by Theorem 6.3.1, that G/K has a group structure. Note that $\mu(G)$ is also naturally a group.

These two groups are closely related because

$$\mu(g) = \mu(g') \qquad \leftrightarrow \qquad gK = g'K \tag{7.9}$$

Thus we have

Theorem 7.2:

$$\boxed{\mu(G) \cong G/K} \tag{7.10}$$

Proof: We associate the coset gK to the element $\mu(g)$ in G'.

$$\psi : gK \mapsto \mu(g) \tag{7.11}$$

Claim: ψ is an isomorphism. You have to show three things:

1. ψ is a well defined map:

$$gK = g'K \Rightarrow \exists k \in K, g' = gk \Rightarrow \mu(g') = \mu(gk) = \mu(g)\mu(k) = \mu(g) \tag{7.12}$$

2. ψ is in fact a homomorphism of groups

$$\psi(g_1K \cdot g_2K) = \psi(g_1K) \cdot \psi(g_2K) \tag{7.13}$$

   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.

3. ψ is one-one, i.e. ψ is onto and invertible. The surjectivity should be clear. To prove injectivity note that:

$$\mu(g') = \mu(g) \Rightarrow \exists k \in K, g' = gk \Rightarrow g'K = gK \qquad ♠ \tag{7.14}$$

Remarks:

1. If we have a short exact sequence

$$1 \to N \to G \to Q \to 1 \tag{7.15}$$

   then it automatically follws 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 [29] 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.

[29] notably, S. MacLane, one of the inventors of group cohomology,

2. In quantum mechanics physical states are actually represented by “rays” in Hilbert space (better, by projection operators, or more generally 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 §11 below. For the moment we quote three important examples:

Example 1: Consider $\mathbb{Z}_4$ as the multiplicative group of fourth roots of unity and $\pi(g) = g^2$. Then

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{7.16}$$

Exercise: Describe this extension thinking of $\mathbb{Z}_4$ additively as $\mathbb{Z}/4\mathbb{Z}$.

Example 2:*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

$$P_{i,j} = \delta_{j=i+1 \mathrm{mod} N} \tag{7.17}$$

$$Q_{i,j} = \delta_{i,j}\omega^j \tag{7.18}$$

Note that $P^N = Q^N = 1$ and no smaller power is equal to 1. Further note that

$$PQ = \omega QP \tag{7.19}$$

For $N = 4$ the matrices look like

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad Q = \begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 \\ 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{7.20}$$

with $\omega = e^{2\pi i/4}$. The group of matrices generated by P, Q is a finite subgroup of $GL(N, \mathbb{C})$ isomorphic to a *finite Heisenberg group*, denoted Heis. It is an extension

$$1 \to \mathbb{Z}_N \to \mathrm{Heis}_N \overset{\pi}{\to} \mathbb{Z}_N \times \mathbb{Z}_N \to 1 \tag{7.21}$$

and has many pretty applications to physics. Exercise: What is π in this sequence?

Example 3: There is a standard homomorphism

$$\pi : SU(2) \to SO(3) \tag{7.22}$$

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:

$$u\vec{x} \cdot \vec{\sigma} u^{-1} = (R\vec{x}) \cdot \vec{\sigma} \tag{7.23}$$

where $R \in SO(3)$.

To prove (7.23) we being 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

$$(\vec{x} \cdot \vec{\sigma})^2 = \vec{x}^2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{7.24}$$

(PROVE THIS FORMULA!!) and hence $\vec{x}^2 = \vec{y}^2$. Alternatively, note that $\det \vec{x} \cdot \vec{\sigma} = -\vec{x}^2$, so, taking the determinant of on both sides of $u\vec{x} \cdot \vec{\sigma}u^{-1} = \vec{y} \cdot \vec{\sigma}$ we get again $\vec{x}^2 = \vec{y}^2$. Either way, we 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

$$u\sigma^i u^{-1} = R_{ji}\sigma^j \quad . \tag{7.25}$$

It should be clear from the definition that $\pi(u_1u_2) = \pi(u_1)\pi(u_2)$, that is that π is a homomorhpism of groups. Now to show that actually $R \in SO(3) \subset O(3)$ note that

$$\begin{aligned} 2\mathrm{i} &= \mathrm{tr}\ \left(\sigma^1\sigma^2\sigma^3\right) \\ &= \mathrm{tr}\ \left(u\sigma^1u^{-1}u\sigma^2u^{-1}u\sigma^3u^{-1}\right) \\ &= R_{j_1,1}R_{j_2,2}R_{j_3,3}\mathrm{tr}\ \left(\sigma^{j_1}\sigma^{j_2}\sigma^{j_3}\right) \\ &= 2\mathrm{i}\epsilon^{j_1j_2j_3}R_{j_1,1}R_{j_2,2}R_{j_3,3} \end{aligned} \tag{7.26}$$

and hence $\det R = 1$. Alternatively, if you know about Lie groups, you can use the fact that π is continuous, and $SU(2)$ is a connected manifold.

In our chapter on 2×2 matrix groups we will prove that:

1. Every proper rotation R comes from some $u \in SU(2)$: This follows from the Euler angle parametrization.

2. $\ker(\pi) = \{\pm 1\}$. To prove this we write the general $SU(2)$ element as $\cos\chi + \sin\chi\vec{n}\cdot\vec{\sigma}$. This only commutes with all the σ^i if $\sin\chi = 0$ so $\cos\chi = \pm 1$.

Thus we have the extremely important extension:

$$1 \to \mathbb{Z}_2 \overset{\iota}{\to} SU(2) \overset{\pi}{\to} SO(3) \to 1 \tag{7.27}$$

Thus, $SU(2)$ is a two-fold cover of $SO(3)$. This is arguably the most important exact sequence in physics.

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 §8.2: Suppose $\mu : G_1 \to G_2$ is a homomorphism and $H_2 \subset G_2$ is a subgroup.

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

$$1 \to \mu^{-1}(H_2)/H_1 \to G_1/H_1 \to G_2/H_2 \tag{7.28}$$

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

$$\bar{\phi} : A/A_1 \to B/B_1 \tag{7.29}$$

b.) Show that if $\phi : A_1 \to B_1$ is *surjective* then

$$\ker\{\bar{\phi} : A/A_1 \to B/B_1\} \cong \frac{\ker\{\phi : A \to B\}}{\ker\{\phi : A_1 \to B_1\}} \tag{7.30}$$

Exercise

Let n be a natural number and let

$$\psi : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^d \tag{7.31}$$

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 (7.17) and (7.18) show that the word

$$P^{n_1}Q^{m_1}P^{n_2}Q^{m_2}\cdots P^{n_k}Q^{m_k} \tag{7.32}$$

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

$$1 \to \mathbb{Z}^{n-1} \to \mathcal{B}_n \to S_n \to 1 \tag{7.33}$$

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

$$1 \to \mathbb{Z}_2^n \to W(B_n) \to S_n \to 1 \tag{7.34}$$

and therefore $|W(B_n)| = 2^n n!$.

7.1 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.

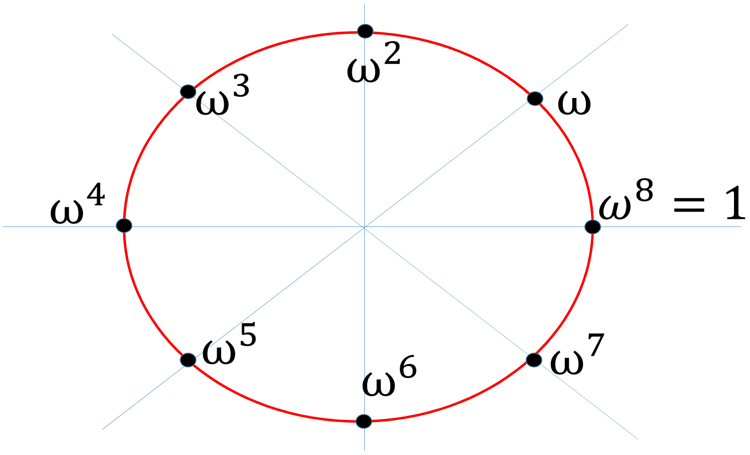

Figure 11: Roots of unity on the unit circle in the complex plane. Here $\omega = e^{2\pi \mathrm{i}/8}$ is a primitive eighth root of 1.

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 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:

$$\delta_j(\omega^k) = \delta_{\bar{j},\bar{k}} \tag{7.35}$$

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 expresses as

$$\Psi = \sum_{j=0}^{N-1} z_j \delta_j \tag{7.36}$$

where $z_j \in \mathbb{C}$.

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:

$$\langle \Psi_1, \Psi_2 \rangle := \sum_{g \in G} \Psi_1^*(g) \Psi_2(g) \tag{7.37}$$

Put differently, we can declare δ_j, $j = 0, \dots, N-1$, to be an orthonormal basis of $\mathcal{H}$.

Now, recall the general definition from section 3.1. 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:

$$\begin{aligned}\tilde{\phi}(\omega,\Psi)(\omega^k) &:= \Psi(\phi(\omega^{-1},\omega^k)) \\ &= \Psi(\omega^{k-1})\end{aligned} \tag{7.38}$$

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 (7.38) as

$$(P \cdot \Psi)(\omega^k) := \Psi(\omega^{k-1}) \tag{7.39}$$

Thus, P can be viewed as translation 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

$$(T(a)\cdot\Psi)(x) = \Psi(x-a) = (\exp[\mathrm{i}a\hat{p}])\Psi(x) = (\exp[-a\frac{d}{dx}]\cdot\Psi)(x) \tag{7.40}$$

This equation makes sense also for a particle on the circle. So our P is $T(a)$ for translation by $2\pi/N$ times around the circle clockwise.

Now let Q be the position operator:

$$(Q\cdot\Psi)(\omega^k) := \omega^k\Psi(\omega^k) \tag{7.41}$$

Now note that

$$\begin{aligned}(P\circ Q\cdot\Psi)(\omega^k) &= (Q\cdot\Psi)(\omega^{k-1}) \\ &= \omega^{k-1}\Psi(\omega^{k-1})\end{aligned} \tag{7.42}$$

while

$$\begin{aligned}(Q\circ P\cdot\Psi)(\omega^k) &= \omega^k(P\cdot\Psi)(\omega^k) \\ &= \omega^k\Psi(\omega^{k-1})\end{aligned} \tag{7.43}$$

and therefore we conclude that we have the operator equation:

$$Q\circ P = \omega P\circ Q \tag{7.44}$$

Now, let us choose the basis δ_j. Then we easily compute

$$P\cdot\delta_j = \delta_{j+1} \tag{7.45}$$

and therefore the matrix for P relative to the basis $\{\delta_j\}$, is the matrix with matrix elements

$$P_{i,j} = \delta_{i,j+1} \tag{7.46}$$

so, for $N=3$ it is

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \tag{7.47}$$

♣THIS IS THE TRANSPOSE OF WHAT WE CALLED P ABOVE. NEED TO FIX THAT!! ♣

Similarly, in the basis δ_j we have

$$Q_{i,j} = \omega^j \delta_{i,j} \tag{7.48}$$

and since $j = 0, 1, \dots, N-1$ we have for $N = 3$:

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \tag{7.49}$$

Note that P and Q are unitary matrices. For Q this is obvious. For P view it as the linear transformation that translates the wavefunction, so it preserves the norm. If you prefer, in the matrix form of both P and Q the columns are orthonormal basis vectors for $\mathbb{C}^N$. So the matrices are unitary.

Moreover, 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

$$SPS^{-1} = Q \tag{7.50}$$

where S is the finite Fourier transform matrix

$$S_{j,k} = \frac{1}{\sqrt{N}} e^{2\pi \mathrm{i} \frac{jk}{N}} \tag{7.51}$$

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.

Remark: As we will see in Chapter 4, there is a more conceptual way to think about S_{jk}. Let $\widehat{G}$ be the set of homomorphisms $\chi : G \to U(1)$. It is itself a group and in fact for $G = \mathbb{Z}_N$ we have $\widehat{G} \cong \mathbb{Z}_N$. If χ is a homomorphism we can define the Fourier transform

$$\widehat{\Psi}(\chi) := \frac{1}{|G|} \sum_{g \in G} \chi(g) \Psi(g) \tag{7.52}$$

Then identifying $L^2(\widehat{G})$ with $L^2(G)$ gives the matrix S.

8. Group theory And Elementary Number Theory

8.1 Reminder On gcd And The Euclidean Algorithm

Let us recall some basic facts from arithmetic.

First, if $A > B$ are two positive integers then we can write

$$A = qB + r \qquad 0 \le r < B \tag{8.1}$$

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:

$$\begin{aligned} A &= q_1 B + r_1 \qquad 0 < r_1 < B \\ B &= q_2 r_1 + r_2 \qquad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \qquad 0 < r_3 < r_2 \\ \vdots \quad & \quad \vdots \\ r_{j-2} &= q_j r_{j-1} + r_j \qquad 0 < r_j < r_{j-1} \\ r_{j-1} &= q_{j+1} r_j \end{aligned} \tag{8.2}$$

Examples

$A = 96$ and $B = 17$:

$$\begin{aligned} 96 &= 5 \cdot 17 + 11 \\ 17 &= 1 \cdot 11 + 6 \\ 11 &= 1 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 \end{aligned} \tag{8.3}$$

$A = 96$ and $B = 27$:

$$\begin{aligned} 96 &= 3 \cdot 27 + 15 \\ 27 &= 1 \cdot 15 + 12 \\ 15 &= 1 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 \end{aligned} \tag{8.4}$$

Note well: In (8.1) 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:

$$(m_1, m_2) = (m_2, m_1) = (m_2, m_1 - x m_2) \tag{8.5}$$

for any integer x. Applying this to the Euclidean algorithm above we get:

$$(A, B) = (B, r_1) = (r_1, r_2) = \cdots = (r_{j-1}, r_j) = (r_j, 0) = r_j. \tag{8.6}$$

A corollary of this algorithm is that if $g = (A, B)$ is the greatest common divisor then there exist integers (x, y) so that

$$Ax + By = g \tag{8.7}$$

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

$$m_1 x + m_2 y = 1. \tag{8.8}$$

Of course x, y are not unique. Equation (8.8) is sometimes known as "Bezout's theorem."

Remark: A theorem of Lamé asserts that the Euclidean algorithm is very efficient. The number of steps never exceeds $5\log_{10}B$ (recall that $A > B$). This is important for RSA (see below).

Exercise

Given one solution for (8.7), 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:

$$\frac{A}{B} = q_1 + \cfrac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_j}}} := [q_1, q_2, q_3, \cdots, q_j] \tag{8.9}$$

b.) The fractions $[q_1], [q_1, q_2], [q_1, q_2, q_3], \ldots$ are known as the *convergents* of the continued fraction. Write $[q_1, \ldots, q_k] = N_k / D_k$ where N_k and D_k are polynomials in $q_1, \ldots, q_k$.

Note that if we eliminate from equations (8.41) $r_{j-1}, \ldots, r_1$ (in that order) in terms of the $q's$ and r_j then we can substitute into the first two equations and the result is that we express A and B as a polynomial in $q's$ times r_j Of course these polynomials are N_j and D_j, respectively: $A = N_j[q_1, \ldots, q_j] r_j$ and $B = D_j[q_1, \ldots, q_j] r_j$. Using this observation give an explicit formula for the integers x, y in Bezout's theorem: [30]

$$AD_{j-1} - BN_{j-1} = (-1)^{j-1}(A, B) \tag{8.10}$$

8.2 The Direct Product Of Two Cyclic Groups

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:

$$(h_1, g_1) \cdot (h_2, h_2) = (h_1 \cdot h_2, g_1 \cdot g_2) \tag{8.11}$$

[30] *Answer*: Consult Hardy and Wright.

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. When we do this we should write the abelian group law additively.

Let us begin with the question: Is it true that

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \overset{?}{\cong} \mathbb{Z}_{m_1 m_2}. \tag{8.12}$$

In general (8.12) 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.)

b.) Examine some other examples.

However, there is a natural exact sequence

$$0 \to \mathbb{Z}_g \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \to \mathbb{Z}_\ell \to 0 \tag{8.13}$$

where we write $g = \gcd(m_1, m_2)$ and $\ell = \mathrm{lcm}(m_1, m_2)$. Then 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.

Now, let us prove (8.13). Recall that if we write the prime factors of m_1, m_2 as

$$m_a = \prod_i p_i^{e_{i,a}}, \qquad a = 1, 2 \tag{8.14}$$

then

♣Do we use this prime factorization in the argument? ♣

$$\begin{aligned} g = \gcd(m_1, m_2) &= \prod_i p_i^{\min[e_{i,1}, e_{i,2}]} \\ \ell = \mathrm{lcm}(m_1, m_2) &= \prod_i p_i^{\max[e_{i,1}, e_{i,2}]} \end{aligned} \tag{8.15}$$

Note that $g\ell = m_1 m_2$. 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

$$\mu_1 \nu_1 + \mu_2 \nu_2 = 1 \tag{8.16}$$

and hence $m_1 \nu_1 + m_2 \nu_2 = g$.

To prove (8.13) think of $\mathbb{Z}_m$ as the multiplicative group of m^{th} roots of 1 and let $\omega_1 = e^{\frac{2\pi i}{m_1}}$ and $\omega_2 = e^{\frac{2\pi i}{m_2}}$. Then the projection map is simply given by multiplication:

$$\pi : (\omega_1^{r_1}, \omega_2^{r_2}) \to \omega_1^{r_1} \omega_2^{r_2}. \tag{8.17}$$

Note that the product is an ℓ^{th} root of unity. Moreover, since $\nu_1 m_1 + \nu_2 m_2 = g$ then π maps $(\omega_1^{\nu_2}, \omega_2^{\nu_1})$ to $e^{\frac{2\pi i}{\ell}}$ which is a generator of $\mathbb{Z}_\ell$, and hence the homomorphism is onto.

On the other hand the injection map is defined by taking the generator $e^{2\pi i/g}$ of $\mathbb{Z}_g$ to $(\exp[2\pi i\frac{\mu_1}{m_1}], \exp[-2\pi i\frac{\mu_2}{m_2}])$. Note this maps into the kernel of π. This proves (8.13) ♠

A second proof gives some additional insight. It is related to the first by "taking a logarithm" and involves exact sequences of infinite groups which induce sequences on quotients.

Consider the sublattice of $\mathbb{Z}\oplus\mathbb{Z}$ given by

$$\Lambda = m_1\mathbb{Z}\oplus m_2\mathbb{Z} = \{\begin{pmatrix} m_1\alpha \\ m_2\beta \end{pmatrix} |\alpha,\beta\in\mathbb{Z}\} \tag{8.18}$$

Then

$$\mathbb{Z}^2/\Lambda = \mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2} \tag{8.19}$$

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

$$\begin{pmatrix} \mu_2 & \mu_1 \\ -\nu_1 & \nu_2 \end{pmatrix} \in SL(2,\mathbb{Z}) \tag{8.20}$$

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

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \mu_2 & \mu_1 \\ -\nu_1 & \nu_2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \tag{8.21}$$

that is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \nu_2 & -\mu_1 \\ \nu_1 & \mu_2 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix} \tag{8.22}$$

which we prefer to write as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = x'\begin{pmatrix} \nu_2 \\ \nu_1 \end{pmatrix} + y'\begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \tag{8.23}$$

Thus, we are using the basis vectors

$$v_1 = \begin{pmatrix} \nu_2 \\ \nu_1 \end{pmatrix} \qquad v_2 = \begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \tag{8.24}$$

as a different basis for $\mathbb{Z}^2$ which has the nice property that the smallest multiple of v_1 in Λ is ℓv_1 and the smallest multiple of v_2 in Λ is gv_2.

Define a homomorphism $\psi:\mathbb{Z}^2\to\mathbb{Z}$ that takes $\begin{pmatrix} x \\ y \end{pmatrix}$ to x'. That is, we have projection on the v_1 axis. This defines a surjective homomorphism onto $\mathbb{Z}$. (Explain why.) On the other hand, using (8.21) 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 (7.28) ψ descends to a map

$$\bar{\psi}:\mathbb{Z}^2/\Lambda\to\mathbb{Z}/\ell\mathbb{Z} \tag{8.25}$$

Now note from (8.23) that

$$\begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \mathrm{mod}\Lambda \tag{8.26}$$

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

$$0 \to \mathbb{Z}_g \to \mathbb{Z}^2/\Lambda \to \mathbb{Z}_\ell \to 0 \tag{8.27}$$

This concludes our second proof. ♠

Now, a corollary of (8.13) is that if m_1, m_2 are relatively prime then indeed we have

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \cong \mathbb{Z}_{m_1 m_2}. \tag{8.28}$$

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

$$(\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \cong \mathbb{Z}/M\mathbb{Z} \tag{8.29}$$

where $M = m_1 m_2 \cdots m_r$.

Proof: We construct a homomorphism

$$\psi : \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \tag{8.30}$$

by

$$\psi(x) = (x \mathrm{mod} m_1, x \mathrm{mod} m_2, \dots, x \mathrm{mod} m_r) \tag{8.31}$$

We first claim that $\psi(x)$ is *onto*. That is, for any values $a_1, \dots, a_r$ we can solve the simultaneous congruences:

$$\begin{aligned} x &= a_1 \mathrm{mod} m_1 \\ x &= a_2 \mathrm{mod} m_2 \\ \vdots & \quad \vdots \\ x &= a_r \mathrm{mod} m_r \end{aligned} \tag{8.32}$$

for some common value $x \in \mathbb{Z}$.

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

$$x_i m_i + y_i \hat{m}_i = 1 \tag{8.33}$$

Let $g_i = y_i \hat{m}_i$. Note that

$$g_i = \delta_{i,j} \text{mod} m_j \qquad \forall 1 \leq i, j \leq r \tag{8.34}$$

Therefore if we set

$$x = \sum_{i=1}^{r} a_i g_i \tag{8.35}$$

then x is a desired solution to (8.32) and hence is a preimage under ψ.

On the other hand, the kernel of ψ is clearly $M\mathbb{Z}$. Therefore:

$$0 \to M\mathbb{Z} \to \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \to 0 \tag{8.36}$$

and hence the desired isomorphism follows. ♠

Remarks

1. (8.28) 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 (8.28).

2. 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 to Sun Tzu, who was active about 2000 years ago. (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 [31] 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. 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.

[31] Kang Sheng Shen, "Historical development of the Chinese remainder theorem," Arch. Hist. Exact Sci. 38 (1988), no. 4, 285305.

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? [32]

8.3 Application: Expressing elements of $SL(2,\mathbb{Z})$ as words in S and T

The group $SL(2,\mathbb{Z})$ is generated by

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \& \qquad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{8.37}$$

Here is an algorithm for decomposing an arbitrary element

$$h = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL(2,\mathbb{Z}) \tag{8.38}$$

as a word in S and T.

First, note the following simple

Lemma Suppose $h \in SL(2,\mathbb{Z})$ as in (8.38). Suppose moreover that $g \in SL(2,\mathbb{Z})$ satisfies:

$$g \cdot \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8.39}$$

Then

$$gh = T^n \tag{8.40}$$

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

$$\begin{aligned} A &= q_1 C + r_1 \qquad 0 < r_1 < C \\ C &= q_2 r_1 + r_2 \qquad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \qquad 0 < r_3 < r_2 \\ &\vdots \quad \vdots \\ r_{N-2} &= q_N r_{N-1} + r_N \qquad 0 < r_N < r_{N-1} \\ r_{N-1} &= q_{N+1} r_N \end{aligned} \tag{8.41}$$

[32] 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 $3 \times 286 - 2 \times 65 - 1 \times 220 = 508 \mathrm{mod} 715$. Therefore there are 508 soldiers.

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:

$$\begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} r_1 \\ C \end{pmatrix} \tag{8.42}$$

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:

$$\sigma^1 \begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} C \\ r_1 \end{pmatrix} \tag{8.43}$$

Now the Euclidean algorithm implies the matrix identity:

$$\tilde{g} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8.44}$$

$$\tilde{g} = (\sigma^1 T^{-q_{N+1}}) \cdots (\sigma^1 T^{-q_1}) \tag{8.45}$$

Now, to apply the Lemma we need g to be in $SL(2, \mathbb{Z})$, but

$$\det \tilde{g} = (-1)^{N+1} \tag{8.46}$$

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

$$\begin{aligned} (\sigma^1 T^{-q_{2\ell}})(\sigma^1 T^{-q_{2\ell-1}}) &= (\sigma^1 \sigma^3)(\sigma^3 T^{-q_{2\ell}} \sigma^3)(\sigma^3 \sigma^1) T^{-q_{2\ell-1}} \\ &= -S T^{q_{2\ell}} S T^{-q_{2\ell-1}} \end{aligned} \tag{8.47}$$

   where we used that $\sigma^1 \sigma^3 = -\mathrm{i}\sigma^2 = S$. Therefore, we can write

$$\tilde{g} = g = (-1)^s \prod_{\ell=1}^{s} (S T^{q_{2\ell}} S T^{-q_{2\ell-1}}) \tag{8.48}$$

2. Now suppose that $N + 1 = 2s + 1$ is odd. Then we rewrite the identity (8.44) as:

$$\sigma^1 \tilde{g} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8.49}$$

   so now we simply take

$$g = \sigma^1 \tilde{g} = (-1)^{s+1} (S T^{-q_{2s+1}}) \prod_{\ell=1}^{s} (S T^{q_{2\ell}} S T^{-q_{2\ell-1}}) \tag{8.50}$$

Thus we can summarize both cases by saying that

$$g = (-1)^{\lfloor \frac{N+1}{2} \rfloor} \prod_{\ell=1}^{N+1} (ST^{(-1)^\ell q_\ell}) \tag{8.51}$$

Then we can finally write

$$h = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = g^{-1} T^n \tag{8.52}$$

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

$$\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ C + mA & D + mB \end{pmatrix} \tag{8.53}$$

while

$$\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} = ST^m S \tag{8.54}$$

This takes care of all cases except $A = C = 1$ and $A = -C = 1$.

♣CHECK!! ♣

♣DEAL WITH THESE CASES ♣

9. 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, $\mathrm{Aut}(G)$, 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

$$I(a) : g \to aga^{-1} \tag{9.1}$$

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:

$$\mathrm{Inn}(G) \cong G/Z(G). \tag{9.2}$$

Moreover, $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$, since for any automorphism $\phi \in \mathrm{Aut}(G)$:

$$\phi \circ I(a) \circ \phi^{-1} = I(\phi(a)). \tag{9.3}$$

Therefore we have another group

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G) \tag{9.4}$$

known as the group of "outer automorphisms." Thus

$$1 \to \mathrm{Inn}(G) \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1 \tag{9.5}$$

Note we can also write and exact sequence of length four:

$$1 \to Z(G) \to G \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1 \tag{9.6}$$

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 (9.4). These notes will engage in this abuse of terminology.

2. Note that for any abelian group G all nontrivial automorphisms are outer automorphisms.

Example 9.1: 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

$$(123) \to (132) \tag{9.7}$$

So: $Aut(\mathbb{Z}_3) \cong \mathbb{Z}_2$.

Example 9.2: 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 9.3: 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

$$\phi_2^2 = \phi_4 \qquad \phi_2^3 = \phi_3 \qquad \phi_2^4 = \phi_4^2 = \phi_1 = 1 \tag{9.8}$$

So $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$. The explicit isomorphism is

$$\begin{aligned} \phi_2 &\to \bar{1} \\ \phi_4 &\to \bar{2} \\ \phi_3 &\to \bar{3} \end{aligned} \tag{9.9}$$

Example 9.4: Consider $\mathrm{Aut}(\mathbb{Z}_N)$, 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

$$rs = 1 \mathrm{mod} N \tag{9.10}$$

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 §9.1 below.

Example 9.5: *Automorphisms Of The Symmetric Group S_n*: There are no outer automorphisms of S_n so

$$Aut(S_n) \cong Inn(S_n) \cong S_n, \qquad n \neq 2, 6 \tag{9.11}$$

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

$$\phi((ab)) = (xy) \qquad \phi((ac)) = (zw) \tag{9.12}$$

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

$$\phi((ab)) = (xy) \qquad \phi((ac)) = (xz) \tag{9.13}$$

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

$$\binom{n}{2} = \frac{n!}{(n-2)!2!} \tag{9.14}$$

The size of a conjugacy class of the form $(1)^k(2)^\ell$ with $k + 2\ell = n$ is

$$\frac{n!}{(n-2\ell)!\ell!2^\ell} \tag{9.15}$$

Setting these equal results in the identity

$$\frac{(n-2)!}{(n-2\ell)!} = \ell!2^{\ell-1} \qquad n \geq 2\ell \tag{9.16}$$

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 $n = 2\ell$:

$$(2\ell-2)! = \ell! 2^{\ell-1} \tag{9.17}$$

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 9.6: *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

$$(12)(123)(12)^{-1} = (132) \tag{9.18}$$

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 permtutation 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.

Example 9.7: Consider $G = GL(n, \mathbb{C})$. Then $A \to A^*$ is an outer automorphism. Similarly, $A \to A^{tr,-1}$ is an outer automorphism. Consider $G = SU(2)$. Is $A \to A^*$ an outer automorphism?

Exercise *Automorphisms of* $\mathbb{Z}$

Show that $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$. [33]

Exercise

Although $\mathbb{Z}_2$ does not have any automorphisms the product group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ certainly does.

[33] *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.

a.) Show that an automorphism of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ must be of the form

$$\phi(x_1, x_2) = (a_1 x_1 + a_2 x_2, a_3 x_3 + a_4 x_4) \tag{9.19}$$

where we are writing the group additively, and

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in GL(2, \mathbb{Z}_2) \tag{9.20}$$

b.) Show that $GL(2, \mathbb{Z}_2) \cong S_3$. [34]

c.) Now describe $\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_4)$. [35]

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 [36]

$$|\mathrm{Aut}(\mathbb{Z}_p^N)| = (p^N - 1)(p^N - p)(p^N - p^2) \cdots (p^N - p^{N-1}) \tag{9.21}$$

9.1 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

$$\bar{n}_1 + \bar{n}_2 = \overline{n_1 + n_2}, \tag{9.22}$$

and $\bar{0}$ is the unit element.

However, note that since

$$(n_1 + N\ell_1)(n_2 + N\ell_2) = n_1 n_2 + N\ell'' \tag{9.23}$$

we do have a well-defined operation on $\mathbb{Z}/N\mathbb{Z}$ inherited from *multiplcation* in $\mathbb{Z}$:

$$\bar{n}_1 \cdot \bar{n}_2 := \overline{n_1 \cdot n_2}. \tag{9.24}$$

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

[34] *Hint*: Consider what the group does to the three nontrivial elements $(1,0)$, $(0,1)$, and $(1,1)$.

[35] *Answer*: This group has a homomorphism onto $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ with a kernel isomorphic to $\mathbb{Z}_2^4$.

[36] *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 $\mathbb{Z}_p^N$. There are $p^N - 1$ nonzero vectors for the first element e_1. The span of e_1 is then a one-dimensional subpsace of p elements. That leaves $p^N - p$ choices for the next basis vector e_2, and so on.

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* $\mathbb{Z}/N\mathbb{Z}$:

$$(\mathbb{Z}/N\mathbb{Z})^* := \{\bar{m} : 1 \leq m \leq N-1, \gcd(m,N) = 1\} \tag{9.25}$$

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 (9.24) ! Clearly the multiplication is closed and $\bar{1}$ is the unit. The existence of multiplicative inverses follows from (8.8).

Moreover, as we have seen above, we can identify

$$\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^* \tag{9.26}$$

The isomorphism is that $a \in (\mathbb{Z}/N\mathbb{Z})^*$ is mapped to the transformation

$$\phi_a : n \mathrm{mod} N \to a n \mathrm{mod} N \tag{9.27}$$

if we think of $\mathbb{Z}/N\mathbb{Z}$ additively or

$$\phi_a : \omega \to \omega^a \tag{9.28}$$

if we think of it multiplicatively. Note that $\phi_{a_1} \circ \phi_{a_2} = \phi_{a_1 a_2}$.

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*. One can check that

$$\begin{aligned} \phi(2) &= 1 \\ \phi(3) &= 2 \\ \phi(4) &= 2 \end{aligned} \tag{9.29}$$

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

$$\begin{aligned} v_1 &\to \alpha v_1 + \beta v_2 \\ v_2 &\to \gamma v_1 + \delta v_2 \end{aligned} \tag{9.30}$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Now impose the conditions $n v_1 = 0$ and $m v_2 = 0$ 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 $\bar{\beta} = \bar{\gamma} = 0$. So 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:

$$\mathbb{Z}_{nm}^* \cong \mathbb{Z}_n^* \times \mathbb{Z}_m^* \tag{9.31}$$

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

$$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \cdots (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^* \tag{9.32}$$

Moreover, $(\mathbb{Z}/p^e\mathbb{Z})^*$ is of order $\phi(p^e) = p^e - p^{e-1}$, as is easily shown [37] and hence

$$\phi(N) = \prod_i (p_i^{e_i} - p_i^{e_i-1}) = N \prod_{p|N} (1 - \frac{1}{p}) \tag{9.33}$$

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

$$\frac{\phi(N)}{N} = \prod_{p|N} (1 - \frac{1}{p}) \tag{9.34}$$

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.

♣Should provide a proof here. ♣

On the other hand, if $p = 2$

$$(\mathbb{Z}/4\mathbb{Z})^* \cong \{\pm 1\} \tag{9.35}$$

is cyclic but

$$(\mathbb{Z}/2^e\mathbb{Z})^* = \{(-1)^a 5^b | a = 0, 1, 0 \le b < 2^{e-2}\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{e-2}\mathbb{Z}) \tag{9.36}$$

when $e \ge 3$.

Examples

1. $(\mathbb{Z}/7\mathbb{Z})^* = \{1,2,3,4,5,6\}\text{mod}7 \cong \mathbb{Z}_6$. Note that 3 and 5 are generators:

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1 \qquad \text{mod}7 \tag{9.37}$$

$$5^1 = 5, \quad 5^2 = 4, \quad 5^3 = 6, \quad 5^4 = 2, \quad 5^5 = 3, \quad 5^6 = 1 \qquad \text{mod}7 \tag{9.38}$$

However, $2 = 3^2\text{mod}7$ 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 $2,3,4$.

[37] 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.

2. $(\mathbb{Z}/9\mathbb{Z})^* = \{1,2,4,5,7,8\}\text{mod}9 \cong \mathbb{Z}_6$. It is a cyclic group generated by 2 and $2^5 = 5\text{mod}9$, but it is not generated by $2^2 = 4$, $2^3 = 8$ or $2^4 = 7\text{mod}9$, because $2, 3, 4$ are not relatively prime to 6.

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.

Remarks

1. A good reference for this material is Ireland and Rosen, *A Classical Introduction to Modern Number Theory* Springer GTM

2. *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 $1\text{mod}4$ then Artin predicts the density of primes for which a is a generator to be

$$\prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.37.... \tag{9.39}$$

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

$$\{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 293, 3 \tag{9.40}$$

3. *Factoring Integers.* Suppose N is a positive integer and a is a positive integer so that $(a, N) = 1$ so that $\bar{a} \in (\mathbb{Z}/N\mathbb{Z})^*$. Let r be the order of $\bar{a}$. Suppose that r is <u>even</u> so that we can define $b = a^{r/2}$. Note that $b \neq 1\text{mod}N$, by the definition of the order of a group element. Note that $b^2 = 1\text{mod}N$ so $\bar{b}$ is a squareroot of $\bar{1} \in (\mathbb{Z}/N\mathbb{Z})^*$. Suppose that $b \neq -1\text{mod}N$ as well. 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 α, β so that

$$(b \pm 1)\alpha + N\beta = 1 \tag{9.41}$$

But then multiply the equation by $b \mp 1$ to get

$$(b^2 - 1)\alpha + N\beta(b \mp 1) = b \mp 1 \tag{9.42}$$

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 $105 = 5 \cdot 21$.

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, $g.c.d(a, N) = 1$,

$$a^{\phi(N)} = 1 \text{mod} N \tag{9.43}$$

Note that a special case of this is Fermat's little theorem: If a is an integer and p is prime then

$$a^p = a \text{mod} p \tag{9.44}$$

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

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, \dots, \tag{9.45}$$

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

$$C(X) < X \text{exp} \left(- \frac{\kappa \text{log} X \text{logloglog} X}{\text{loglog} X} \right) \tag{9.46}$$

where κ is a positive real number.

Exercise *Periodic Functions*

a.) Consider the function

$$f(x) = 2^x \text{mod } N \tag{9.47}$$

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 $N = 15, 21, 105$. [38]

c.) More generally, if $(a, N) = 1$ show that $f(x) = a^x \bmod N$ is a periodic function.

9.2 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:

$$a \leftrightarrow \bar{0}, b \leftrightarrow \bar{1}, c \leftrightarrow \bar{2}, \ldots \tag{9.48}$$

Exercise *Simple 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 Ceasar. Using this decode the message:

$$ZOLPPQEBORYFZLK! \tag{9.49}$$

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 10^{500} divisors. Bear in mind that our universe is about $\pi \times 10^7 \times 13.77 \times 10^9 \cong 4 \times 10^{17}$ seconds old. [39] 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. [40]

[38] *Answer*: $r = 4, 6, 12$ divides $\phi(N) = 8, 12, 48$.

[39] There are $\pi \times 10^7$ seconds in a year, to 0.3% accuracy.

[40] 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 $\pi(x) \sim \frac{x}{\text{log}x}$. Equivalently, the n^{th} prime is asymptotically like $p_n \sim n\text{log}n$. This means that the density of primes for large x is $\sim 1/\text{log}x$, so if $x \sim 10^n$ then the density is $1/n$ so if we work with thousand-digit primes that after about one thousand random choices we will find a prime.

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

$$d_A e_A - f\phi(n_A) = 1 \tag{9.50}$$

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:

$$c := m^{e_A} \mathrm{mod} n_A \tag{9.51}$$

Bob sends the ciphertext c to Alice over the internet. Anyone can read it.

Then Alice can decode the message by computing

$$\begin{aligned} c^{d_A} \mathrm{mod} n_A &= m^{e_A d_A} \mathrm{mod} n_A \\ &= m^{1+f\phi(n_A)} \mathrm{mod} n_A \\ &= m \mathrm{mod} n_A \end{aligned} \tag{9.52}$$

Thus, to decode the message Alice just needs one piece of private information, namely the integer d_A.

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.

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}.

2. *How to break RSA with a quantum computer: Shor's algorithm.* 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 $\bar{b} = \bar{a}^{r/2} \neq \bar{-1}$ 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 $(a, N) = 1$.

   2. Compute the period r.

   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 $f(x) = a^x \bmod N$ 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.

Exercise *Your turn to play Eve*
Alice has published the key

$$(n = 661643, e = 325993) \tag{9.53}$$

Bob sends her the ciphertext in four batches:

$$c_1 = 541907 \quad c_2 = 153890 \quad c_3 = 59747 \quad c_4 = 640956 \tag{9.54}$$

What is Bob's message? [41]

10. Products And 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

$$\alpha : G \to \text{Aut}(H). \tag{10.1}$$

[41] 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 $x = 1 \text{mod} \phi$ and $x = 0 \text{mod} e$. This gives $x = 735766201 = de$ and hence $d = 2257$. Now you can compute the message from the ciphertext $m = c^d \text{mod} n$.

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. This group is the Cartesian product $H \times G$ as a *set* but has the “twisted” multiplication law:

$$(h_1, g_1) \cdot (h_2, g_2) := (h_1 \alpha_{g_1}(h_2), g_1 g_2) \tag{10.2}$$

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.”

Example 10.1: 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:

$$\begin{aligned}(x_1, e)(x_2, e) &= (x_1 + x_2, e)\\ (x_1, e)(x_2, \sigma) &= (x_1 + x_2, \sigma)\\ (x_2, \sigma)(x_1, e) &= (x_2 - x_1, \sigma)\\ (x_1, \sigma)(x_2, \sigma) &= (x_1 - x_2, e)\end{aligned} \tag{10.3}$$

and hence the resulting group is nonabelian with this twisted multiplication law. In fact $Aut(\mathbb{Z}) \cong \mathbb{Z}_2$, so this is the only nontrivial semidirect product we can form. This group is known as the *infinite dihedral group*. It has a presentation:

$$\mathbb{Z} \rtimes \mathbb{Z}_2 \cong \langle r, s | s^2 = 1 \qquad srs = r^{-1} \rangle \tag{10.4}$$

(e.g. take $s = (0, \sigma)$ and $r = (1, e)$) from which we also see it has a presentation as a Coxeter group:

$$\mathbb{Z} \rtimes \mathbb{Z}_2 \cong \langle x, y | x^2 = 1 \qquad y^2 = 1 \rangle \tag{10.5}$$

It is also the Weyl group for the affine Lie group $LSU(2)$.

Example 10.2: 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

$$\alpha_\sigma : \bar{n} \to -\bar{n} \tag{10.6}$$

where we are writing $\mathbb{Z}/N\mathbb{Z}$ additively. This defines the *finite dihedral group D_N*. Note that the presentation is now

$$(\mathbb{Z}/N\mathbb{Z}) \rtimes \mathbb{Z}_2 \cong \langle r, s | s^2 = 1, \qquad r^N = 1, \qquad srs = r^{-1} \rangle \tag{10.7}$$

Note that the group has order $2N$:

$$|D_N| = 2N. \tag{10.8}$$

We will meet this group again as the group of symmetries of the regular N-gon in the plane. Briefly, think of the N-gon centered on the origin of the plane. Then you can think of the generator r is a rotation by $2\pi/N$ and s as a reflection in any symmetry axis of the N-gon.

♣SHOULD ADD A FIGURE HERE. ♣

It is also worth noting that D_N is a quotient of the infinite dihedral group. Indeed, note that $\mathcal{N} = \{(x,e)|x = 0\text{mod}N\} \subset \mathbb{Z} \rtimes \mathbb{Z}_2$ is a normal subgroup and

$$(\mathbb{Z}/N\mathbb{Z}) \rtimes \mathbb{Z}_2 \cong (\mathbb{Z} \rtimes \mathbb{Z}_2)/\mathcal{N}. \tag{10.9}$$

Example 10.3: An affine space 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. For the case $d = 2$ think of a map: You can translate by two-dimensional vectors but there is no natural choice of origin. If we do choose an origin (this choice is arbitrary) then we can identify $\mathbb{E}^d \cong \mathbb{R}^d$. There is a distance between points which we take to be the Euclidean norm of the vector. Now we can study the group of transformations $\mathbb{E}^d \to \mathbb{E}^d$ that preserves these distances. It turns out (this is a nontrivial theorem) that the most general length-preserving transformation can be described as follows: To a pair $R \in O(d)$ and $v \in \mathbb{R}^d$ we can associate the isometry: [42]

$$\{v|R\} : x \mapsto v + Rx \tag{10.10}$$

In this notation the group multiplication law is

$$\{v_1|R_1\}\{v_2|R_2\} = \{v_1 + R_1 v_2|R_1 R_2\} \tag{10.11}$$

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 $O(d)$. Thus, there is 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

$$\{v|R\}\{w|1\} = \{Rw|1\}\{v|R\} \tag{10.12}$$

and hence:

$$\{v|R\}\{w|1\}\{v|R\}^{-1} = \{Rw|1\} \tag{10.13}$$

Note that, again, thanks to the group law, $\pi : \{v|R\} \to R$ is a surjective homomorphism $\text{Euc}(d) \to O(d)$. We conclude that

$$\text{Euc}(d) \cong \mathbb{M}^{1,d-1} \rtimes O(1, d-1) \tag{10.14}$$

Almost identical considerations show that the Poincaré group is the semidirect product of the translation and Lorentz group:

$$\text{Poincare}(\mathbb{M}^{1,d-1})) = \mathbb{M}^{1,d-1} \rtimes O(1, d-1) \tag{10.15}$$

[42] 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 $\{R|v\} : x \mapsto Rx + v$.

Example 10.4: *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.

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

$$\alpha : G_2 \to \mathrm{Aut}(\mathcal{F}[X \to G_1]) \tag{10.16}$$

be the canonical G_2 action on the function space, so $\phi : G_2 \times X \to X$ is the action on X and the induced action on the function space is

$$\alpha_g(F)(x) = F(\phi(g^{-1}, x)) \qquad \forall g \in G_2, x \in X \tag{10.17}$$

Then we can form the semidirect product

$$\mathcal{F}[X \to G_1] \rtimes G_2 \tag{10.18}$$

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

$$(h_1, \dots, h_n; \phi) \tag{10.19}$$

with $h_i \in G_1$ and $\phi \in S_n$ and the product is

$$(h_1, \dots, h_n; \phi)(h'_1, \dots, h'_n; \phi') = (h_1 h_{\phi^{-1}(1)}, h_2 h_{\phi^{-1}(2)}, \dots, h_n h_{\phi^{-1}(n)}, \phi \circ \phi') \tag{10.20}$$

Example 10.5: *Kaluza-Klein theory.* In Kaluza-Klein theory we study general relativity on a product manifold $X \times Y$ and partially rigidify the situation by putting some structure on Y. We then regard Y as "small" and study the physics as "effectively" taking place on X.

The canonical example of this idea is the case where $X = \mathbb{M}^{1,d-1}$ is d-dimensional Minkowski space and $Y = S^1$ is the circle. We rigidify the situation by putting a metric on the circle S^1 so that the metric on space-time is

$$ds^2 = \eta_{\mu\nu} dx^\mu dx^\nu + R^2 (d\theta)^2 \tag{10.21}$$

where R is the radius of the circle, $\theta \sim \theta + 2\pi$ and $0 \le \mu \le d-1$. Our signature is mostly plus. Now we consider a <u>massless</u> particle in $(d+1)$ dimensions on this spacetime. In field theory it is described by a field satisfying the wave equation:

$$\left[\eta^{\mu\nu} \frac{\partial}{\partial x^\mu} \frac{\partial}{\partial x^\nu} + \frac{1}{R^2} \left(\frac{\partial}{\partial \theta} \right)^2 \right] \phi = 0 \tag{10.22}$$

we can, of course Fourier-decompose the field to obtain the interpretation in terms of particles. The Fourier modes are like

$$e^{\mathrm{i}p_M x^M} = e^{\mathrm{i}p_\mu x^\mu} e^{\mathrm{i}p_\theta \theta} \tag{10.23}$$

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:

$$E^2 - \vec{p}^2 = \frac{n^2}{R^2} \tag{10.24}$$

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. If R is very small they are very massive for any $n \neq 0$ and therefore 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. Moreover, 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, if $M = 0, \dots, d+1$ and $\mu = 0, \dots, d$ then we postulate a metric

$$ds^2 = g_{MN} dx^M dx^N = g_{\mu\nu} dx^\mu dx^\nu + \Omega^2(x)(d\theta + A_\mu dx^\mu)^2 \tag{10.25}$$

where A_μ is only a function of x (that is the restriction to zero Fourier modes). Then the Riemann scalar is

$$\mathcal{R}[g_{MN}] = \mathcal{R}[g_{\mu\nu}] - \frac{\Omega^2}{4} F_{\mu\nu} F^{\mu\nu} - 2(\nabla \mathrm{log}\Omega)^2 - 2\nabla^2 \mathrm{log}\Omega \tag{10.26}$$

so the Einstein-Hilbert action for GR in $(d+1)$ dimensions reduces to that of Einstein-Hilbert-Maxwell-Scalar in d dimensions.

It is interesting to understand how gauge symmetries in theories on X arise in this point of view. Suppose $\mathcal{D} \cong Diff(X)$ is a subgroup of diffeomorphisms of $X \times Y$ of the form

$$\psi_f : (x, y) \to (f(x), y) \qquad f \in Diff(X). \tag{10.27}$$

We also consider a subgroup $\mathcal{G}$ of $Diff(X \times Y)$ where $\mathcal{G}$ is isomorphic to a subgroup of $Map(X, Diff(Y))$. For the moment just take $\mathcal{G} = Map(X, Diff(Y))$, so an element $g \in \mathcal{G}$ is a <u>family</u> of diffeomorphisms of Y parametrized by X: For each x we have a diffeomorphism of Y: $g_x : y \to g(y; x)$. Then we take $\mathcal{G}$ to be the subgroup of diffeomorphisms of $Diff(X \times Y)$ of the form

$$\psi_g : (x, y) \to (x, g(y; x)) \qquad g \in \mathcal{G} \tag{10.28}$$

Note that within $Diff(X \times Y)$ we can write the subgroup

$$\mathcal{G}\mathcal{D} \tag{10.29}$$

and $\mathcal{D}$ acts as a group of automorphisms of $\mathcal{G}$ via

$$\begin{aligned}\psi_f \psi_g \psi_f^{-1} : (x, y) &\to (f^{-1}(x), y) \\ &\to (f^{-1}(x), g(y; f^{-1}(x))) \\ &\to (x, g(y; f^{-1}(x)))\end{aligned} \tag{10.30}$$

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. This is a model for the group of gauge transformations in Kaluza-Klein theory. So X is the "large", possibly noncompact, spacetime where we have general relativity, while 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 X. Typically, Y is endowed with a fixed metric ds_Y^2 and the diffeomorphism symmetry of Y is (spontaneously) broken down to the group of isometries of Y, $Isom(Y, ds_Y^2)$. So in the above construction we take $\mathcal{G}$ to be the unbroken subgroup $Map(X, Isom(Y, ds_Y^2)) \subset Map(X, Diff(Y))$. This subgroup $Map(X, Isom(Y, ds_Y^2))$ is interpreted as a group of gauge transformations of a gauge theory on X coupled to general relativity on X.

Exercise

a.) Show that (10.2) defines an associative group law.

b.) Show that $(1_H, 1_G)$ defines the unit and

$$(h, g)^{-1} = \left(\alpha_{g^{-1}}(h^{-1}), g^{-1}\right) \tag{10.31}$$

c.) Let 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 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 (10.2) still defines a monoid. When is it a group?

Exercise *Internal definition of semidirect products*

Suppose there is a homomorphism $G \to \mathrm{Aut}(H)$ so that we can form the semidirect product $H \rtimes G$.

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. [43] This explains the funny product

[43] 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

$$(h_1, g_1)(1, g)(h_1, g_1)^{-1} = (h_1 \alpha_{g_1 g g_1^{-1}}(h_1^{-1}), g_1 g g_1^{-1}). \tag{10.32}$$

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:

$$1 \to N \to H \rtimes G \to Q \to 1 \tag{10.33}$$

d.) Show that $H \rtimes G = NQ = QN$ and show that $Q \cap N = \{1\}$.

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

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 $\mathbb{Z}_3$.

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

$$Z(g) \cong \prod_{i=1}^{n} \left(\mathbb{Z}_i^{\ell_i} \rtimes S_{\ell_i} \right) \tag{10.34}$$

where $\prod_i$ is a direct product.

b.) Use this to compute the order of a conjugacy class in the symmetric group.

Exercise *Holomorph*

Given a finite group G a canonical semidirect product group is $G \rtimes \mathrm{Aut}(G)$ known as the holomorph of G. Show that this is the normalizer of the copy of G in the symmetric group $S_{|G|}$ given by Cayley's theorem.

Exercise *Equivalence of semidirect products*

A nontrivial automorphism α 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 [44]

$$\Psi : H \rtimes_\alpha G \to H \times G \tag{10.35}$$

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. [45]

Exercise *Manipulating the Seitz notation*

a.) Show that:

$$\begin{aligned}
\{v|R\}^{-1} &= \{-R^{-1}v|R^{-1}\} \\
\{0|R\}\{v|1\} &= \{Rv|R\} \\
\{v|1\}\{0|R\} &= \{v|R\} \\
\{w|1\}\{v|R\} &= \{w+v|R\} \\
\{v_1|R_1\}\{v_2|R_2\}\{v_1|R_1\}^{-1} &= \{R_1v_2 + (1 - R_1R_2R_1^{-1})v_1|R_1R_2R_1^{-1}\} \\
[\{v_1|R_1\},\{v_2|R_2\}] &= \{(1 - R_1R_2R_1^{-1})v_1 - R_1R_2R_1^{-1}R_2^{-1}(1 - R_2R_1R_2^{-1})v_2|R_1R_2R_1^{-1}R_2^{-1}\}
\end{aligned} \tag{10.36}$$

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 $O(d) \to \mathrm{Euc}(d)$?

---

11. Group Extensions and Group Cohomology

11.1 Group Extensions

♣Add: Pushforward extensions ♣

Recall that an extension of Q by a group N is an exact sequence of the form:

$$1 \to N \overset{\iota}{\to} G \overset{\pi}{\to} Q \to 1 \tag{11.1}$$

[44] *Answer*: $\Psi(h,g) = (h\phi(g), g)$.

[45] *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.

There is a notion of *homomorphism of two group extensions*

$$1 \to N \overset{\iota_1}{\to} G_1 \overset{\pi_1}{\to} Q \to 1 \tag{11.2}$$

$$1 \to N \overset{\iota_2}{\to} G_2 \overset{\pi_2}{\to} Q \to 1 \tag{11.3}$$

This means that there is a group homomorphism $\varphi : G_1 \to G_2$ so that the following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota_1"] \arrow[d, "\mathrm{Id}"] & G_1 \arrow[r, "\pi_1"] \arrow[d, "\varphi"] & Q \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\iota_2"] & G_2 \arrow[r, "\pi_2"] & Q \arrow[r] & 1
\end{tikzcd} \tag{11.4}$$

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 (11.4) is completely equivalent to the pair of equations:

$$\begin{aligned} \pi_1 &= \pi_2 \circ \varphi \\ \iota_2 &= \varphi \circ \iota_1 \end{aligned} \tag{11.5}$$

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 11.5 below.

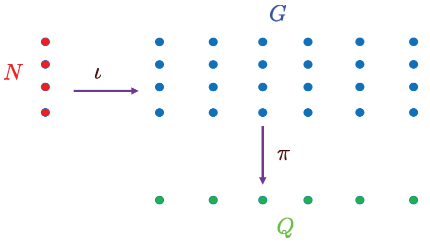

Figure 12: Illustration of a group extension $1 \to N \to G \to Q \to 1$ as an N-bundle over Q.

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 12. 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.[46] Note that in general $s(\pi(g)) \neq g$. This is obvious from Figure 12. The inverse $\pi^{-1}(q)$ is called *the fiber of π over q*. The map π projects the entire fiber over q to q. The section s chooses just one point above q in that fiber.

In order to justify the picture of Figure 12 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:

$$g(s(\pi(g)))^{-1} \tag{11.6}$$

maps to 1 under π (check this). Therefore, since the sequence is exact

$$g(s(\pi(g)))^{-1} = \iota(n) \tag{11.7}$$

for some $n \in N$. That is, every $g \in G$ can be written as

$$g = \iota(n)s(q) \tag{11.8}$$

for some $n \in N$ and some $q \in Q$. In fact, this decomposition is *unique*: Suppose that:

$$\iota(n_1)s(q_1) = \iota(n_2)s(q_2) \tag{11.9}$$

Then we rewrite this as

$$\iota(n_2^{-1}n_1) = s(q_2)s(q_1)^{-1} \tag{11.10}$$

Now, applying π we learn that $1 = q_2\pi(s(q_1)^{-1}) = q_2\left(\pi(s(q_1))\right)^{-1} = q_2 q_1^{-1}$, 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 (11.8) 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

$$\begin{aligned}\varphi(g) &= \varphi(\iota_1(n)s_1(q)) \\ &= \varphi(\iota_1(n))\varphi(s_1(q)) \\ &= \iota_2(n)s_2(q)\end{aligned} \tag{11.11}$$

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

$$\omega : Q \to \mathrm{Aut}(N) \tag{11.12}$$

denoted by

$$q \mapsto \omega_q \tag{11.13}$$

[46] 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

$$\iota(\omega_q(n)) = s(q)\iota(n)s(q)^{-1} \tag{11.14}$$

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 $\omega_q(n_1n_2) = \omega_q(n_1)\omega_q(n_2)$, and ω_q is one-one on N. Therefore we really have a map of sets (11.12). 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:

$$\begin{aligned}\iota\left(\omega_{q_1} \circ \omega_{q_2}(n)\right) &= s(q_1)\iota(\omega_{q_2}(n))s(q_1)^{-1} \\ &= s(q_1)s(q_2)\iota(n)(s(q_1)s(q_2))^{-1}\end{aligned} \tag{11.15}$$

We want to compare this to $\iota\left(\omega_{q_1q_2}(n)\right)$. In general they will be different unless $s(q_1q_2) = s(q_1)s(q_2)$, 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 (11.15) we know that

$$\omega_{q_1} \circ \omega_{q_2} = \omega_{q_1q_2} \tag{11.16}$$

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 (11.8) 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 (11.8). Write

$$\iota(n)s(q)\iota(n')s(q') = \iota(n)\left(s(q)\iota(n')s(q)^{-1}\right)s(qq') \tag{11.17}$$

Note that

$$s(q)\iota(n')s(q)^{-1} = \iota(\omega_q(n')) \tag{11.18}$$

so

$$\iota(n_1)s(q_1)\iota(n_2)s(q_2) = \iota\left(n_1\omega_{q_1}(n_2)\right)s(q_1q_2) \tag{11.19}$$

But this just means that

$$\Psi(n,q) = \iota(n)s(q) \tag{11.20}$$

is in fact an isomorphism $\Psi : N \rtimes_\omega Q \to G$. Indeed equation (11.19) just says that:

$$\Psi(n_1,q_1)\Psi(n_2,q_2) = \Psi((n_1,q_1)\cdot_\omega(n_2,q_2)) \tag{11.21}$$

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 §11.5 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.

♣Do the general case first and then specialize? ♣

Example And Remark: Let us return to the very important exact sequence (7.27):

$$1 \to \mathbb{Z}_2 \overset{\iota}{\to} SU(2) \overset{\pi}{\to} SO(3) \to 1 \tag{11.22}$$

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 $\pi_1(SU(2)) = 1$. [47] Moreover, as a manifold $H_1(SO(3);\mathbb{Z}_2) \cong \mathbb{Z}_2$ 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 (11.1) generalizes to

$$1 \to \mathbb{Z}_2 \overset{\iota}{\to} \mathrm{Spin}(d) \overset{\pi}{\to} SO(d) \to 1 \tag{11.24}$$

as well as the two Pin groups which extend $O(d)$:

$$1 \to \mathbb{Z}_2 \overset{\iota}{\to} \mathrm{Pin}^{\pm}(d) \overset{\pi}{\to} O(d) \to 1 \tag{11.25}$$

[47] Every $SU(2)$ matrix can be written as

$$\begin{pmatrix} \alpha & \beta \\ -\bar\beta & \bar\alpha \end{pmatrix} \tag{11.23}$$

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.

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 $q \in Q$,

$$s(q^{-1}) = s(q)^{-1}n = n's(q)^{-1} \tag{11.26}$$

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

$$\begin{tikzcd} 1 \arrow[r] & H' \arrow[r, "\iota"] & H \arrow[r, "\pi"] & H'' \arrow[r] & 1 \end{tikzcd} \tag{11.27}$$

and a homomorphism

$$\rho : G'' \to H'' \tag{11.28}$$

Then the *pullback extension* is defined by a subgroup of the Cartesian product $G \subset H \times G''$:

$$G := \{(h, g'')|\pi(h) = \rho(g'')\} \subset H \times G'' \tag{11.29}$$

and is an extension of the form

$$\begin{tikzcd} 1 \arrow[r] & H' \arrow[r, "\iota"] & G \arrow[r, "\tilde{\pi}"] & G'' \arrow[r] & 1 \end{tikzcd} \tag{11.30}$$

where $\tilde{\pi}(h, g'') := g''$. Show that this extension fits in the commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & H' \arrow[r] \arrow[d, equal] & G \arrow[r, "\tilde{\pi}"] \arrow[d, "\tilde{\rho}"] & G'' \arrow[r] \arrow[d, "\rho"] & 1 \\ 1 \arrow[r] & H' \arrow[r] & H \arrow[r, "\pi"] & H'' \arrow[r] & 1 \end{tikzcd} \tag{11.31}$$

Moreover, show that this diagram can be used to define the pullback extension.

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.

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 $R \mapsto \{R|(1-R)v\}$, and verify that this is also a splitting.

11.2 Central Extensions

Now we study an important class of extensions. We change the notation from the previous section to emphasize this.

Let A be an abelian group and G any group.

Definition A *central extension* of G by A, [48] is a group $\tilde{G}$ such that

$$1 \rightarrow A \quad \overset{\iota}{\rightarrow} \quad \tilde{G} \quad \overset{\pi}{\rightarrow} \quad G \rightarrow 1 \tag{11.32}$$

such that $\iota(A) \subset Z(\tilde{G})$.

We stress again that what we called G in the previous section is here called $\tilde{G}$, and what we called Q in the previous section is here called G.

Example . An example familiar from the quantum mechanical theory of angular momentum, and which we will discuss later is:

$$1 \rightarrow \mathbb{Z}_2 \rightarrow SU(2) \rightarrow SO(3) \rightarrow 1 \tag{11.33}$$

Here the $\mathbb{Z}_2 \cong \{\pm 1\}$ is the center of $SU(2)$.

Remarks:

1. Central extensions are important in the theory of projective representations and occur quite frequently in quantum mechanics. Recall that a matrix representation of a group G is a group homomorphism

$$\rho : G \rightarrow GL(d, \kappa) \tag{11.34}$$

A *projective representation* is a map

$$\rho : G \rightarrow GL(d, \kappa) \tag{11.35}$$

which is "almost a homomorphism" in the sense that

$$\rho(g_1)\rho(g_2) = f(g_1, g_2)\rho(g_1, g_2) \tag{11.36}$$

for some function $f : G \times G \rightarrow \kappa^*$. A simple example is the spin representation of the rotation group where one attempts to define a map:

$$\rho : SO(3) \rightarrow SU(2) \tag{11.37}$$

[48] Some authors say an extension of A by G.

that attempts to describe the effects of a rotation on - say - a spin 1/2 particle. [49] We will explain this relation in more detail later, but for the moment there are two general ways central extensions appear

a.) G is a group of classical symmetries of a physical system and $\tilde{G}$ as a group of corresponding operators in the quantum mechanical description of that physical system.

b.) Related to this, physical (pure) states are "rays" in Hilbert space $\mathcal{H}$, or better, one-dimensional projection operators. The group of transformations of one-dimensional projection operators (or rays) that preserves overlaps $\mathrm{Tr}(P_1 P_2)$ called $\mathrm{Aut}(QM))$ is the universal symmetry group of a quantum system. Any symmetry of the system will be a subgroup of this group. *Wigner's theorem* states that $\mathrm{Aut}(QM))$ is a quotient of the group $\mathrm{Aut}(\mathcal{H})$ of the norm-preserving unitary and anti-unitary operators on Hilbert space. 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 g:

$$1 \;\to\; U(1) \;\to\; \mathrm{Aut}(\mathcal{H}) \;\to \mathrm{Aut}(QM)) \;\to 1 \tag{11.38}$$

All of this is explained in detail in Chapter **** below. For now, speaking roughly, the idea is, given a classical symmetry group G of a physical system we associate a unitary operator $U(g)$ acting on a Hilbert space. As we will see, quantum mechanics only guarantees that

$$U(g_1)U(g_2) = c(g_1, g_2)U(g_1, g_2) \tag{11.39}$$

for some phase factor $c(g_1, g_2)$. This should remind you of the failure of a map $g \mapsto U(g)$ to be a group homomorphism. For a more detailed account of this see Chapter *** below.

2. Central extensions appear naturally in quantization of bosons and fermions. The Heisenberg group is an extension of a translation group. The symplectic group of linear canonical transformations gets quantum mechanically modified by a central extension to define something called the metaplectic group.

3. Central extensions are important in the theory of anomalies in quantum field theory.

4. Central extensions are very important in conformal field theory. The Virasoro group, and the Kac-Moody groups are both nontrivial central extensions of simpler objects.

[49] One way to try to do this is to use Euler angles. Under the standard homomorphism $\pi : SU(2) \to SO(3)$ one recognizes that $\exp[\mathrm{i}\frac{\theta}{2}\sigma^i]$ maps to a rotation by angle θ around the the i^{th} axis. 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. So one attempts to define ρ by assigning to R three Euler angles (ψ, θ, ϕ), respectively, and defining $g = e^{\mathrm{i}\frac{\phi}{2}\sigma^3} e^{\mathrm{i}\frac{\theta}{2}\sigma^1} e^{\mathrm{i}\frac{\psi}{2}\sigma^3}$. The problem is that the Euler angle coordinates on $SO(3)$ are sometimes singular. Similarly, it is true that 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 *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 $s(\pi(\tilde{g})) = \iota t(\tilde{g}^{-1}))\tilde{g}$.)

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

$$\pi(s(g)) = g \qquad \forall g \in G \tag{11.40}$$

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

$$\iota(a)s(g) \to (a, g) \tag{11.41}$$

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 (11.32) 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:

$$s(g_1)s(g_2)\left(s(g_1g_2)\right)^{-1}. \tag{11.42}$$

Now the quantity (11.42) 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

$$\iota(f_s(g_1, g_2)) := s(g_1)s(g_2)\left(s(g_1g_2)\right)^{-1}. \tag{11.43}$$

That is, we can write:

$$s(g_1)s(g_2) = \iota(f_s(g_1, g_2))s(g_1g_2) \tag{11.44}$$

The function f_s satisfies the important *cocycle identity*

$$\boxed{\boxed{f(g_2, g_3)f(g_1, g_2g_3) = f(g_1, g_2)f(g_1g_2, g_3)}} \tag{11.45}$$

Exercise

Verify (11.45) by using (11.43) to compute $s(g_1g_2g_3)$ in two different ways.

(Note that simply substituting (11.43) into (11.45) 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:

$$f(g,1) = f(1,g) = f(1,1) \qquad \forall g \in G \tag{11.46}$$

b.) Show that

$$f(g,g^{-1}) = f(g^{-1},g). \tag{11.47}$$

Now we introduce some fancy terminology:

Definition: In general
1. A *2-cochain on G with values in A* is a function

$$f : G \times G \to A \tag{11.48}$$

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 (11.45). 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 §11.6 and Section §13.2 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 (11.43).

Now, if we choose a different section $\hat{s}$ then [50]

$$\hat{s}(g) = \iota(t(g))s(g) \tag{11.49}$$

for some function $t : G \to A$. It is easy to check that

$$f_{\hat{s}}(g_1,g_2) = f_s(g_1,g_2)t(g_1)t(g_2)t(g_1g_2)^{-1} \tag{11.50}$$

where we have used that $\iota(A)$ is central in $\tilde{G}$.

[50] 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.

Definition: In general two 2-cochains f and $\hat{f}$ are said to *differ by a coboundary* if they satisfy

$$\hat{f}(g_1,g_2) = f(g_1,g_2)t(g_1)t(g_2)t(g_1g_2)^{-1} \tag{11.51}$$

for some function $t : G \to A$.

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:

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: From (11.43)(11.45)(11.50) we learn that given a central extension we can unambiguously form a group cohomology class which is independent of the choice of section. Moreover, if $\tilde{G} \cong \tilde{G}'$ are isomorphic central extensions and $\psi : \tilde{G} \to \tilde{G}'$ is an isomorphism, then ψ can be used to map sections of $\tilde{G} \to G$ to sections of $\tilde{G}' \to G$: $s'(g) = \psi(s(g))$. Then

$$\begin{aligned} s'(g_1)s'(g_2) &= \psi(s(g_1))\psi(s(g_2)) \\ &= \psi(s(g_1)s(g_2)) \\ &= \psi(\iota(f_s(g_1,g_2))s(g_1g_2)) \\ &= \psi(\iota(f_s(g_1,g_2)))\psi(s(g_1g_2)) \\ &= \iota'(f_s(g_1,g_2))s'(g_1g_2) \end{aligned} \tag{11.52}$$

and hence we assign precisely the same 2-cocycle $f(g_1,g_2)$ to the section s'. Hence the isomorphism class of a central extension maps unambiguously to a cohomology class $[f]$.

Conversely, given a cohomology class $[f]$ we may construct a corresponding central extension as follows. Choose a representative 2-cocycle f. With such an f we may define $\tilde{G} = A \times G$ as a set and we use f to *define* the multiplication law:

$$(a_1,g_1)(a_2,g_2) := (a_1a_2f(g_1,g_2), g_1g_2) \tag{11.53}$$

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 (11.51) above. Then we claim that the map $\psi : \tilde{G} \to \tilde{G}'$ defined by

$$\psi : (a,g) \to (at(g)^{-1}, g) \tag{11.54}$$

is an isomorphism of groups. (Check this!) On the other hand, we just showed above that if $[f] \neq [f']$ then $\tilde{G}$ cannot be isomorphic to $\tilde{G}'$. ♠

Remarks:

1. *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.

2. *Group Structure.* 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:

$$(f_1 \cdot f_2)(g, g') = f_1(g, g') \cdot f_2(g, g') \tag{11.55}$$

where we are writing the product in A multiplicatively. Again using the fact that A is abelian this descends to a well-defined muiltiplication 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 divide by the anti-diagonal of $A \times A$. In more detail: Suppose we have two extensions:

$$1 \to A \overset{\iota_1}{\to} \tilde{G}_1 \overset{\pi_1}{\to} G \to 1 \tag{11.56}$$

$$1 \to A \overset{\iota_2}{\to} \tilde{G}_2 \overset{\pi_2}{\to} G \to 1 \tag{11.57}$$

We can describe the "product" extension of G by A as follows: Let

$$\Delta : G \to G \times G \tag{11.58}$$

be the diagonal homomorphism: $\Delta : g \mapsto (g, g)$. Then construct the pull-back (see equation (11.31)) under Δ of the Cartesion product of extensions (11.56) and (11.57). (The Cartesian product is the obvious extension of $G \times G$ by $A \times A$.) In concrete terms we have an extension:

$$1 \to A \times A \overset{(\iota_1, \iota_2)}{\to} \widehat{G_{12}} \overset{\pi_{12}}{\to} G \to 1 \tag{11.59}$$

where

$$\widehat{G_{12}} := \{(\tilde{g}_1, \tilde{g}_2) | \pi_1(\tilde{g}_1) = \pi_2(\tilde{g}_2)\} \subset \tilde{G}_1 \times \tilde{G}_2 \tag{11.60}$$

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"

$$A^{\text{anti}} := \{(a, a^{-1})\} \subset A \times A \tag{11.61}$$

and its image:

$$N := \{(\iota_1(a), \iota_2(a^{-1}))|a \in A\} \subset \widehat{G_{12}} \tag{11.62}$$

Because we are working with <u>central</u> extensions this will be a normal subgroup. Then we let

$$\tilde{G}_{12} := \widehat{G_{12}}/N \tag{11.63}$$

Since N is in the kernel of π and since it is central the homomorphism π_{12} descends to a surjective homomorphism $\pi_{12} : \tilde{G}_{12} \to G$. Now we have an exact sequence

$$1 \to A \overset{\iota_{12}}{\to} \tilde{G}_{12} \overset{\pi_{12}}{\to} G \to 1 \tag{11.64}$$

where $\iota_{12}(a) := [(\iota_1(a), \iota_2(a))]$. 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 (11.64) represents the product of extensions (11.56) and (11.57).

3. *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 $\hat{f}$ satisfying:

$$\hat{f}(1,1) = f(1,1)\frac{t(1)t(1)}{t(1 \cdot 1)} = f(1,1)t(1) \tag{11.65}$$

so by choosing any function t such that $t(1) = f(1,1)^{-1}$ we get a new cochain satisfying $\hat{f}(1,1) = 1$. 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 $\hat{f}$ that is also a cocycle. So now, if f is a cocycle and we have set $\hat{f}(1,1) = 1$ then, by (11.46) we have $\hat{f}(g,1) = \hat{f}(1,g) = 1$ for all g. Now, we can continue to make modifications by coboundaries to simplify further our cocycle $\hat{f}$. 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 "choosing a gauge" by choosing representatives so that $\hat{f}(1,1) = 1$ 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):

$$\hat{f}(g,g^{-1}) = f(g,g^{-1})\frac{1}{t(1)} = f(g,g^{-1})f(1,1) \tag{11.66}$$

is not particularly special. (Remember that we are making the somewhat arbitrary choice that $t(g) = 1$ for $g \neq 1$.) Now suppose 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:

$$\hat{\hat{f}}(g,g^{-1}) = \hat{f}(g,g^{-1})\frac{\tilde{t}(g)\tilde{t}(g^{-1})}{\tilde{t}(g \cdot g^{-1})} = \hat{f}(g,g^{-1})\tilde{t}(g)\tilde{t}(g^{-1}) \tag{11.67}$$

where in the second equality we used the "gauge-preserving" property that $\tilde{t}(1) = 1$. Now, in some arbitrary way, divide the non-involutions 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 $g^{-1} \in S_1$. Then we can choose a $\tilde{t}$ function so that for every $g \in S_2$ we have

$$\tilde{t}(g) = (\tilde{t}(g^{-1}))^{-1}(\hat{f}(g, g^{-1}))^{-1} \tag{11.68}$$

so that

$$\hat{\hat{f}}(g, g^{-1}) = 1 \qquad \forall g \in S_1 \tag{11.69}$$

Now recall from (11.47) that any cocycle f satisfies $f(g, g^{-1}) = f(g^{-1}, g)$ for all g. Since $\hat{\hat{f}}$ is a cocycle (if we started with a cocycle f) then we conclude that for all the non-involutions:

$$\hat{\hat{f}}(g, g^{-1}) = \hat{\hat{f}}(g^{-1}, g) = 1 \qquad \forall g \in S_1 \amalg S_2 \tag{11.70}$$

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 $g^2 = 1$. What can we say about $\hat{\hat{f}}(g, g)$ for g an involution? we have

$$\hat{\hat{f}}(g, g) = \hat{f}(g, g)\frac{\tilde{t}(g)^2}{\tilde{t}(g^2)} = \hat{f}(g, g)(\tilde{t}(g))^2 \tag{11.71}$$

Now, it might, or might not be the case that $\hat{f}(g, g)$ 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 $\hat{\hat{f}}(g, g) = 1$. So this is truly gauge invariant information in the cocycle: *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

$$(1, \sigma_2) \cdot (1, \sigma_2) = (f(\sigma_2, \sigma_2), 1) = (\sigma_1, 1) \tag{11.72}$$

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,

$$\begin{aligned} \Psi &: (\sigma_1, 1) \to \omega^2 = -1 \\ \Psi &: (1, \sigma_2) \to \omega \end{aligned} \tag{11.73}$$

where ω is a primitive 4^{th} root of 1 defines an isomorphism. In conclusion, the nontrivial central extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2$ is:

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{11.74}$$

Recall that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

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

$$1 \to \mathbb{Z}_p \to G \to \mathbb{Z}_p \to 1 \tag{11.75}$$

where we will write our groups multiplicatively. Now, using methods of topology one can show that [51]

$$H^2(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p. \tag{11.76}$$

On the other hand, 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 (11.76)? The answer is that there can be nonisomorphic extensions (11.32) involving the same group $\tilde{G}$. To see this, let us examine in detail the possible extensions:

$$1 \to \mathbb{Z}_p \xrightarrow{\iota} \mathbb{Z}_{p^2} \xrightarrow{\pi} \mathbb{Z}_p \to 1 \tag{11.77}$$

We write the first, second and third groups in this sequence as

$$\begin{aligned} \mathbb{Z}_p &= \langle \sigma_1 | \sigma_1^p = 1 \rangle \\ \mathbb{Z}_{p^2} &= \langle \alpha | \alpha^{p^2} = 1 \rangle \\ \mathbb{Z}_p &= \langle \sigma_2 | \sigma_2^p = 1 \rangle \end{aligned} \tag{11.78}$$

respectively.

For the injection ι we have

$$\iota(\sigma_1) = \alpha^x \tag{11.79}$$

for some x. For this to be a well-defined homomorphism we must have

$$\iota(1) = \iota(\sigma_1^p) = \alpha^{px} = 1 \tag{11.80}$$

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

$$\iota_k(\sigma_1) := \alpha^{kp} \tag{11.81}$$

[51] You can also show it by examining the cocycle equation directly. We will write down the nontrivial cocycles presently.

where k is relatively prime to p. We can take

$$1 \leq k \leq p-1 \tag{11.82}$$

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

$$\pi_r(\alpha) = \sigma_2^r \qquad\qquad 1 \leq r \leq p-1 \tag{11.83}$$

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 $\ell r = 0 \text{ mod } p$ and therefore $\ell = 0 \text{ mod } p$ so

$$\ker(\pi_r) = \{1, \alpha^p, \alpha^{2p}, \dots, \alpha^{(p-1)p}\} \tag{11.84}$$

Since $k \in \mathbb{Z}_p^*$ we have

$$\ker(\pi_r) = \text{im}(\iota_k) \tag{11.85}$$

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 intstructive 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

$$\sigma_2^{xr} = \sigma_2 \tag{11.86}$$

so that

$$xr = 1 \text{mod } p \tag{11.87}$$

Recall that $r \in \mathbb{Z}_p^*$ and let r^* be the integer $1 \leq r^* \leq p-1$ such that

$$rr^* = 1 \text{mod } p \tag{11.88}$$

Then we have that $x = r^* + \ell p$ for any ℓ. That is, $s(\sigma_2)$ could be any of

$$\alpha^{r^*}, \alpha^{r^*+p}, \alpha^{r^*+2p}, \dots, \alpha^{r^*+(p-1)p} \tag{11.89}$$

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:

$$\begin{aligned} s(1) &= 1 \\ s(\sigma_2) &= \alpha^{r^*} \\ s(\sigma_2^2) &= \alpha^{2r^*} \\ \vdots \quad & \quad \vdots \\ s(\sigma_2^{p-1}) &= \alpha^{(p-1)r^*} \end{aligned} \tag{11.90}$$

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 $1 \leq r^* \leq p-1$ we know that $\alpha^{pr^*} \neq 1$. 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:

$$s(\sigma_2^x)s(\sigma_2^y)s(\sigma_2^{x+y})^{-1} = \begin{cases} 1 & x+y \leq p-1 \\ \alpha^{r^*p} & p \leq x+y \end{cases} \tag{11.91}$$

Here we computed:

$$\alpha^{r^*x}\alpha^{r^*y}\alpha^{-r^*(x+y-p)} = \alpha^{r^*p} \tag{11.92}$$

where you might note that if $p \leq x+y \leq 2p-2$ then $0 \leq x+y-p \leq p-2$. Therefore, our cocycle is $f_{k,r}$ where

$$f_{k,r}(\sigma_2^x, \sigma_2^y) := \begin{cases} 1 & x+y \leq p-1 \\ \sigma_1^{k^*r^*} & p \leq x+y \end{cases} \tag{11.93}$$

since

$$\iota_k(\sigma_1^{k^*r^*}) = \alpha^{k^*r^*kp} = \alpha^{r^*p} \tag{11.94}$$

and here we have introduced an integer $1 \leq k^* \leq p-1$ so that

$$kk^* = 1 \text{ mod } p \tag{11.95}$$

Although it is not obvious from the above formula for $f_{k,r}$, we know that $f_{k,r}$ will satisfy the cocycle equation becuase 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

$$\tilde{s}(\sigma_2^x) = \iota(t(\sigma_2^x))s(\sigma_2^x) \tag{11.96}$$

We can always write our function t in the form

$$t(\sigma_2^x) = \sigma_1^{\tau(x)} \tag{11.97}$$

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 $f(\sigma_2^x, \sigma_2^y) =$ already holds for $x+y \leq p-1$ we learn that

$$\tau(x) + \tau(y) - \tau(x+y) = 0 \text{mod} p \tag{11.98}$$

for $x+y \leq p-1$. This means we must take

$$\tau(x) = x\tau(1) \qquad\qquad 1 \leq x \leq p-1 \tag{11.99}$$

So, our coboundary is completely fixed up to a choice of $\tau(1)$. But now let us compute for $x+y \geq p-1$:

$$\tilde{s}(\sigma_2^x)\tilde{s}(\sigma_2^y)\tilde{s}(\sigma_2^{x+y})^{-1} = \alpha^{r^*p}\iota(\sigma_1^{\tau(x)+\tau(y)-\tau(x+y)}) = \alpha^{r^*p} \tag{11.100}$$

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

$$\begin{tikzcd}
 & & \langle\alpha\rangle \arrow[dd, "\varphi"] \arrow[dr, "\pi_{r_1}"] & & \\
1 \arrow[r] & \langle\sigma_1\rangle \arrow[ur, "\iota_{k_1}"] \arrow[dr, "\iota_{k_2}"'] & & \langle\sigma_2\rangle \arrow[r] & 1 \\
 & & \langle\alpha\rangle \arrow[ur, "\pi_{r_2}"'] & &
\end{tikzcd} \tag{11.101}$$

Now φ, being a homomorphism, must be of the form

$$\varphi(\alpha) = \alpha^y \tag{11.102}$$

for some y. We know this must be an isomorphism so y must be relatively prime to p. Moreover commutativity of the diagram implies

$$\pi_{r_2}(\varphi(\alpha)) = \pi_{r_1}(\alpha) \qquad \Rightarrow \qquad r_2 y = r_1 \ \mathrm{mod} p \tag{11.103}$$

$$\varphi(\iota_{k_1}(\sigma_1) = \iota_{k_2}(\sigma_1) \qquad \Rightarrow \qquad k_1 p y = k_2 p \ \mathrm{mod} p^2 \qquad \Rightarrow \qquad = k_1 y = k_2 \bmod p \tag{11.104}$$

Putting these equations together, and remembering that y is multiplicatively invertible modulo p we find that there exists a morphism of extensions iff

$$k_1 r_1 = k_2 r_2 \mathrm{mod} p \tag{11.105}$$

Note that the cocycles $f_{k,r}$ constructed in (11.93) indeed only depend on $kr\mathrm{mod}p$. Equivalently, we can label their cohomology class by $(kr)^* = k^* r^* \mathrm{mod} p$.

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:

$$(f_{k_1,r_1} \cdot f_{k_2,r_2})\,(\sigma_2^x, \sigma_2^y) = \begin{cases} 1 & x + y \le p - 1 \\ \sigma_1^{(k_1 r_1)^* + (k_2 r_2)^*} & p \le x + y \end{cases} \tag{11.106}$$

Thus if we map

$$[f_{k,r}] \mapsto (kr)^* \mathrm{mod} \mathbb{Z}_p \tag{11.107}$$

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

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \to 1 \tag{11.108}$$

and then there is an orbit of $(p-1)$ nontrivial extensions of the form

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 1 \tag{11.109}$$

acted on by $\mathrm{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^*$.

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

$$H^2(\mathbb{Z}_4, \mathbb{Z}_2) \cong \mathbb{Z}_2 \tag{11.110}$$

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 $\mathbb{Z}_2$. ♣

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_8 \to \mathbb{Z}_4 \to 1 \tag{11.111}$$

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

$$\begin{aligned} s(\omega) &= \alpha \\ s(\omega^2) &= \alpha^2 \\ s(\omega^3) &= \alpha^3 \end{aligned} \tag{11.112}$$

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

$$f(\omega, \omega^3) = f(\omega^2, \omega^2) = f(\omega^2, \omega^3) = f(\omega^3, \omega^3) = \alpha^4 = \sigma. \tag{11.113}$$

♣Probably should just describe all extensions with $Q = \mathbb{Z}_n$ ♣

Example 4.. *Products Of Cyclic Groups.* Things also get more interesting when we start to consider products of cyclic groups. Using methods of topology one can prove that

$$H^2(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \tag{11.114}$$

There are 4 isomorphisms classes of groups which fit in the central extensions of $\mathbb{Z}_2 \times \mathbb{Z}_2$ by $\mathbb{Z}_2$. They are:

$$\begin{aligned} &1 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\ &1 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\ &1 \to \mathbb{Z}_2 \to Q \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\ &1 \to \mathbb{Z}_2 \to D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \end{aligned} \tag{11.115}$$

where Q is the quaternion group and D_4 the dihedral group defined in future chapters. For now we can take Q to be the group of 2×2 matrices generated by

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \& \qquad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \tag{11.116}$$

(If you know about quaternions then another useful description is: $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, as we describe in Chapter *** below.)

D_4 is dihedral group defined above. It can also be thought of as the group of 2×2 matrices generated by

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \& \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{11.117}$$

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.

Exercise: Construct cocycles corresponding to each of these central extensions 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 (11.115) while (11.114) is order 8.

♣Probably better to give the answer, and write out the cocycles as $(-1)^{quadratic form}$. Then we can see how the automorphism group acts. Also we should say how the 4 groups above split up into inequivalent extensions. ♣

♣Should also do $H^2(\mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2)$ and get $\mathbb{Z}_8$. ♣

Example 5.. Nonabelian groups can also have central extensions. For example the symmetric group S_n has one nontrivial central extension by $\mathbb{Z}_2$:

$$H^2(S_n; \mathbb{Z}_2) \cong \mathbb{Z}_2 \tag{11.118}$$

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:

$$\begin{aligned} z^2 &= 1 \\ \hat{\sigma}_i^2 &= z \\ \hat{\sigma}_i \hat{\sigma}_{i+1} \hat{\sigma}_i &= \hat{\sigma}_{i+1} \hat{\sigma}_i \hat{\sigma}_{i+1} \\ \hat{\sigma}_i \hat{\sigma}_j &= z \hat{\sigma}_j \hat{\sigma}_i \qquad\qquad j > i+1 \end{aligned} \tag{11.119}$$

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 (11.1) 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 (11.32) 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

Choosing the natural section $s : \sigma_i \to \hat{\sigma}_i$ in (11.119) and find the corresponding cocycle f_s.

Exercise

Show that the associative law for the twisted product (11.53) is equivalent to the cocycle condition on the 2-cochain f.

Exercise

a.) Show that if a central extension is defined by a cocycle f then the group commutator is:

$$[(a_1, g_1), (a_2, g_2)] = \left(\frac{f(g_1 g_2, g_1^{-1} g_2^{-1})}{f(g_2 g_1, g_1^{-1} g_2^{-1})} \frac{f(g_1, g_2)}{f(g_2, g_1)}, g_1 g_2 g_1^{-1} g_2^{-1} \right) \tag{11.120}$$

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.

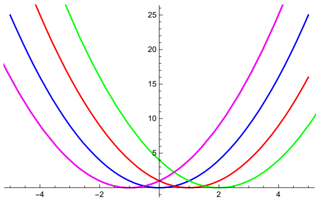

Figure 13: Spectrum of a particle on a circle as a function of $eB/2\pi$.

11.2.1 Example: Charged Particle On A Circle Surrounding A Solenoid

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

$$S = \int \frac{1}{2} m r^2 \dot{\phi}^2 = \int \frac{1}{2} I \dot{\phi}^2$$

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

$$A = \frac{B}{2\pi} d\phi$$

The action is therefore:

$$\begin{aligned} S &= \int \frac{1}{2} I \dot{\phi}^2 dt + \oint eA \\ &= \int \frac{1}{2} I \dot{\phi}^2 dt + \frac{eB}{2\pi} \dot{\phi} dt \end{aligned} \tag{11.121}$$

The second term is an example of a Chern-Simons term. [52] Classically, the second term does not affect physical predictions, since it is a total derivative. However, quantum mechanically, it will have an important effect on physical predictions.

The classical system clearly 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 $\phi \to \phi + \alpha$. 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

$$R(\alpha) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \tag{11.122}$$

as usual. Also we can make a "parity" or "charge conjugation" transformation $P : \phi \to -\phi$. Note that these group elements in $O(2)$ satisfy

$$\begin{aligned} R(\alpha)R(\beta) &= R(\alpha+\beta) \\ P^2 &= 1 \\ PR(\alpha)P &= R(-\alpha) \end{aligned} \tag{11.123}$$

and indeed $O(2)$ is a semidirect product:

$$O(2) = SO(2) \rtimes \mathbb{Z}_2 \tag{11.124}$$

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 $R(\alpha) \to R(-\alpha)$.

We will analyze the quantum mechanics in the Hamiltonian approach. [53] The conjugate momentum is

$$L = I\dot{\phi} + \frac{eB}{2\pi} \tag{11.125}$$

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:

$$\int L\dot{\phi}dt - S = \int \frac{1}{2I}(L - \frac{eB}{2\pi})^2 dt \tag{11.126}$$

Upon quantization $L \to -\mathrm{i}\hbar\frac{\partial}{\partial\phi}$, so the eigenfunctions of the Hamiltonian are just

$$\Psi_m(\phi) = \frac{1}{\sqrt{2\pi}}e^{\mathrm{i}m\phi} \qquad m \in \mathbb{Z} \tag{11.127}$$

They give energy eigenstates states with energy

$$E_m = \frac{\hbar^2}{2I}(m - \mathcal{B})^2 \tag{11.128}$$

where $\mathcal{B} := \frac{eB}{2\pi\hbar}$. There is just one state for each $m \in \mathbb{Z}$.

Remarks:

[52] This problem turns out to be closely related to quantum dots. See Yoshimasa Murayama, *Mesoscopic Systems*, Section 10.10

[53] Evaluating path integrals in this system is also extremely instructive, but we will not do that here.

1. The action (11.121) 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 the circle?
2. Although the Chern-Simons 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 Hamiltonian.
3. The total spectrum is *periodic* in $\mathcal{B}$, and shifting $\mathcal{B} \to \mathcal{B} + 1$ is equivalent to $m \to m + 1$. See Figure 13. The groundstate is two-fold degenerate for $\mathcal{B} = \frac{1}{2}\mathrm{mod}\mathbb{Z}$ and nondegenerate otherwise.
4. COMMENT ON "PARITY" vs. "CHARGE CONJUGATION" - and how this is "parity" in "field space" if we view this as a $0+1$ dimensional "field theory."

In quantum mechanics the shift symmetry is realized by a translation operator $\rho(R(\alpha)) = \mathcal{R}(\alpha)$ and acting on Ψ_m we have

$$(\mathcal{R}(\alpha) \cdot \Psi_m) = e^{\mathrm{i}m\alpha}\Psi_m \tag{11.129}$$

Can we also represent $\rho(P) = \mathcal{P}$ on the Hilbert space? Naively, the parity symmetry P takes $\phi \to -\phi$ so $\mathcal{P}$ takes $m \to -m$ and the symmetry would appear to be broken except when $\mathcal{B} = 0$ since $\Psi_m(\phi)$ and $\Psi_m(-\phi) = \Psi_{-m}(\phi)$ only have the same energy when $\mathcal{B} = 0$. But clearly, given the periodicity of the spectrum in $\mathcal{B}$ such a conclusion would be unwarranted. In fact, if $\mathcal{B}$ is an integer then we can define a parity symmetry

$$\mathcal{P} \cdot \Psi_m = \Psi_{2\mathcal{B}-m} \tag{11.130}$$

Note that there is also a symmetry when $\mathcal{B}$ is half-integer, and in that case, the above definition of $\mathcal{P}$ continues to make sense and commutes with the Hamiltonian.

Now we still have $\mathcal{R}(\alpha)\mathcal{R}(\beta) = \mathcal{R}(\alpha+\beta)$ and $\mathcal{P}^2 = 1$ but now the third line of (11.123) is modified to:

$$\mathcal{P}\mathcal{R}(\alpha)\mathcal{P} = e^{\mathrm{i}2\mathcal{B}\alpha}\mathcal{R}(-\alpha) \tag{11.131}$$

Letting $z(\alpha) := e^{\mathrm{i}2\mathcal{B}\alpha}$ be the c-number operator on Hilbert space we see that the operators $\mathcal{P}, \mathcal{R}(\alpha), z(\alpha)$ where $\alpha \sim \alpha + 2\pi$ generate a group of operators, denoted $\mathcal{G}_{\mathcal{B}}$, acting on Hilbert space. Naively we might have expected this group of operators on Hilbert space to be $U(1) \times O(2)$ where $O(2)$ is our classical symmetry group and $U(1)$ is just the group of phases, but equation (11.131) is not satisfied by a direct product. So, what is the group $\mathcal{G}_{\mathcal{B}}$?

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

$$\tilde{\mathcal{R}}(\alpha) := e^{-\mathrm{i}\mathcal{B}\alpha}\mathcal{R}(\alpha) \tag{11.132}$$

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 Spin(2). As an abstract group it is isomorphic to $SO(2)$, so group elements 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

$$\hat{R}(\hat{\alpha}) = \exp[\hat{\alpha}\sigma^1\sigma^2] = \cos(\hat{\alpha}) + \mathrm{i}\sin(\hat{\alpha})\sigma^3 \tag{11.133}$$

But it is called the *spin group* because it comes with a nontrivial double cover:

$$\pi : \mathrm{Spin}(2) \to SO(2) \tag{11.134}$$

the double covering is given by restricting our standard projection $\pi : SU(2) \to SO(3)$ to these matrices, so we get a double cover of the rotation group around the z axis:

$$\pi : \hat{R}(\hat{\alpha}) \mapsto R(2\hat{\alpha}) \tag{11.135}$$

(Similarly, Spin(3) is isomorphic to the group $SU(2)$.)

Now, taking $\mathbb{Z}_2$ to act on Spin(2) by the nontrivial automorphism we define the Pin group $\mathrm{Pin}^+(2)$ to be the semidirect product:

$$\mathrm{Pin}^+(2) \cong \mathrm{Spin}(2) \rtimes \mathbb{Z}_2 \tag{11.136}$$

(Just the way Spin(d) double covers $SO(d)$, so the $\mathrm{Pin}^{\pm}(d)$ groups are double covers of $O(d)$.)

Now, when $\mathcal{B}$ is half-integer, that is, when $2\mathcal{B}$ is odd we can define an isomorphism of $U(1) \times \mathrm{Pin}^+(2)$ with $\mathcal{G}_{\mathcal{B}}$ by

$$\begin{aligned} z &\mapsto z \\ \hat{R}(\hat{\alpha}) &\mapsto e^{-\mathrm{i}(2\mathcal{B})\hat{\alpha}}\mathcal{R}(2\hat{\alpha}) \\ \hat{P} &\mapsto \mathcal{P} \end{aligned} \tag{11.137}$$

(When $\mathcal{B}$ is integer this map is not an isomorphism.)

1. We stress that the particle on the ring is <u>NOT</u> a spin one-half!! 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.

2. It is straightforward to compute the propagator

$$\langle\phi_2|e^{-\frac{TH}{\hbar}}|\phi_1\rangle = \frac{1}{2\pi}\sum_{m\in\mathbb{Z}} e^{-\frac{T\hbar}{2I}(m-\mathcal{B})^2 + \mathrm{i}m(\phi_1-\phi_2)} \tag{11.138}$$

and the partition function:

$$Z(S^1) = \sum_{m\in\mathbb{Z}} e^{-\frac{T\hbar}{2I}(m-\mathcal{B})^2} \tag{11.139}$$

These are examples of Riemann's theta function and, using the Poisson summation formula, you can prove an intriguing high-low temperature duality.

♣Say more, related to ground state degeneracy, and the Pin-rep ♣

3. As pointed out in a recent paper [54] this extension of the symmetry group at half-integral Chern-Simons term 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 could no longer solve exactly for the eigenstates, but if the potential has a Fourier series only involving even Fourier coefficients then the $\phi \to -\phi$ symmetry is preserved, classically, and, quantum mechanically, we know from the $\mathrm{Pin}^+(2)$ group that the two-fold ground state degeneracy at $\mathcal{B} = \frac{1}{2}\mathrm{mod}\mathbb{Z}$ is unbroken by nonperturbative effects.

11.3 Heisenberg extensions

In all the examples above (except for Q and D_4 in (11.115)) the group $\tilde{G}$ in the central extension is abelian when G is abelian. But this need not be the case, as we will see in the present section.

In this section we focus attention on some special central extensions known as *Heisenberg extensions*. In fact in the literature two 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.

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:

$$[\hat{q}, \hat{p}] = \mathrm{i}\hbar \tag{11.140}$$

One realization of these operator relations is in terms of normalizable wavefunctions $\psi(q)$ where we write:

$$\begin{aligned} (\hat{q} \cdot \psi)(q) &= q\psi(q) \\ (\hat{p} \cdot \psi)(q) &= -\mathrm{i}\hbar \frac{d}{dq}\psi(q) \end{aligned} \tag{11.141}$$

Now, let us consider the unitary operators

$$\begin{aligned} U(\alpha) &:= \exp[\mathrm{i}\alpha\hat{p}] \\ V(\beta) &:= \exp[\mathrm{i}\beta\hat{q}] \end{aligned} \tag{11.142}$$

where $\alpha \in \mathbb{R}$. Of course $U(\alpha_1)U(\alpha_2) = U(\alpha_1 + \alpha_2)$ and similarly for $V(\alpha)$ so, separately, the group of operators $U(\alpha)$ is isomorphic to $\mathbb{R}$ as is the group of operators $V(\alpha)$. However, one can show in a number of ways that:

$$U(\alpha)V(\beta) = e^{\mathrm{i}\hbar\alpha\beta}V(\beta)U(\alpha) \tag{11.143}$$

[54] D. Gaiotto, A. Kapustin, Z. Komargodski and N. Seiberg, "Theta, Time Reversal, and Temperature," https://arxiv.org/pdf/1703.00501.pdf

Here is one way to demonstrate the extremely important relation (11.143): We just evaluate both operators on a wavefunction in the position representation. So, on the one hand:

$$\begin{aligned} \left((U(\alpha)V(\beta))\cdot\psi\right)(q) &= \left(V(\beta)\cdot\psi\right)(q+\hbar\alpha) \\ &= e^{\mathrm{i}\beta(q+\hbar\alpha}\psi(q+\hbar\alpha) \end{aligned} \tag{11.144}$$

On the other hand

$$\begin{aligned} \left((V(\beta)U(\alpha))\cdot\psi\right)(q) &= e^{\mathrm{i}\beta q}\left(U(\alpha)\cdot\psi\right)(q+\hbar\alpha) \\ &= e^{\mathrm{i}\beta q}\psi(q+\hbar\alpha) \end{aligned} \tag{11.145}$$

Comparing (11.144) with (11.145) we arrive at (11.145). The reader should compare this with our discussion of quantum mechanics with a finite number of degrees of freedom, especially the derivation of (7.44).

Therefore, the group generated by the operators $U(\alpha)$ and $V(\alpha)$ for $\alpha \in \mathbb{R}$, which we'll denote Heis($\mathbb{R}\times\mathbb{R}$) fits in a central extension:

$$1 \to U(1) \to \mathrm{Heis}(\mathbb{R}\times\mathbb{R}) \to \mathbb{R}\times\mathbb{R} \to 1 \tag{11.146}$$

Let us now step back and think more generally about central extensions of G by A where G is *also abelian*. From the exercise (11.120) we know that for G abelian the commutator is

$$[(a_1,g_1),(a_2,g_2)] = \left(\frac{f(g_1,g_2)}{f(g_2,g_1)},1\right) \tag{11.147}$$

(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

$$\kappa(g_1,g_2) = \frac{f(g_1,g_2)}{f(g_2,g_1)} \tag{11.148}$$

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. The extension $\tilde{G}$ is abelian iff $\kappa(g_1,g_2) = 1$, that is, iff there exists a symmetric cocycle f.

3. κ is *skew*:

$$\kappa(g_1,g_2) = \kappa(g_2,g_1)^{-1} \tag{11.149}$$

4. κ is *alternating*:
$$\kappa(g,g) = 1 \tag{11.150}$$

5. κ is *bimultiplicative*:
$$\kappa(g_1g_2,g_3) = \kappa(g_1,g_3)\kappa(g_2,g_3) \tag{11.151}$$
$$\kappa(g_1,g_2g_3) = \kappa(g_1,g_2)\kappa(g_1,g_3) \tag{11.152}$$

All of these properties except perhaps the last are obvious. To prove the bimultiplicative properties (it suffices to prove just one) we rewrite (11.151) as

$$f(g_1g_2,g_3)f(g_3,g_2)f(g_3,g_1) = f(g_2,g_3)f(g_1,g_3)f(g_3,g_1g_2) \tag{11.153}$$

Now multiply the equation by $f(g_1,g_2)$ and use the fact that A is abelian to write

$$(f(g_1,g_2)f(g_1g_2,g_3))f(g_3,g_2)f(g_3,g_1) = f(g_2,g_3)f(g_1,g_3)(f(g_1,g_2)f(g_3,g_1g_2)) \tag{11.154}$$

We apply the cocycle identity on both the LHS and the RHS (and also use the fact that G is abelian) to get

$$f(g_2,g_3)f(g_1,g_2g_3)f(g_3,g_2)f(g_3,g_1) = f(g_2,g_3)f(g_1,g_3)f(g_3,g_1)f(g_3g_1,g_2) \tag{11.155}$$

Now canceling some factors and using that A is abelian we have

$$f(g_1,g_2g_3)f(g_3,g_2) = f(g_1,g_3)f(g_3g_1,g_2) \tag{11.156}$$

Now use the fact that G is abelian to write this as

$$f(g_1,g_3g_2)f(g_3,g_2) = f(g_1,g_3)f(g_1g_3,g_2) \tag{11.157}$$

which is the cocycle identity. This proves the bimultiplicative property (11.151). ♠

For a large class of abelian groups G, there is a nice theorem. We consider

1. Finitely generated Abelian groups. These can be (noncanonically) written (See next chapter on classification) as products of $\mathbb{Z}_n$ for various n and $\mathbb{Z}^d$.

2. Vector spaces. [55]

3. Tori. These are isomorphic to $V/\mathbb{Z}^d$ where V is a d-dimensional real vector space.

4. Products of the above three.

This class of groups can be characterized as the set of Abelian groups A which are topological groups so there is an exact sequence:

$$0 \to \pi_1(A) \to \mathrm{Lie}(A) \to A \to \pi_0(A) \to 0 \tag{11.158}$$

where $\mathrm{Lie}(A)$ is a vector space that projects to A by an exponential map.

[55] Topological, separable.

For this class of groups we have the following theorem:

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

$$\kappa : G \times G \to U(1) \tag{11.159}$$

which are alternating (and hence skew).

For a proof of the theorem see[56]

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.) 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. ♣

Now let us turn to a special class of central extensions of an abelian group G by an abelian group A, the *Heisenberg extensions*. By the above theorem, a central extension is characterized by a commutator function κ. 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. If κ is degenerate the center will be larger.

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.

The reader should beware that in the literature there is another and narrower definition of the term “Heisenberg group.” Suppose R is a commutative ring with identity. (See the next chapter, or just take $R = \mathbb{Z}/N\mathbb{Z}$ with abelian group structure $+$ and extra multiplication structure $\bar{n}_1\bar{n}_2 = \overline{n_1 n_2}$.) Then we can consider the group of 3×3 matrices over R of the form

$$M(a,b,c) := \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \tag{11.160}$$

The multiplication law is easily worked out to be

$$M(a,b,c)M(a',b',c') = M(a+a', b+b', c+c'+ab') \tag{11.161}$$

Therefore, as abelian groups we have an extension

$$0 \to R \to \text{Heis}(R \times R) \to R \times R \to 0 \tag{11.162}$$

[56] D. Freed, G. Moore, G. Segal, “The uncertainty of fluxes,” Commun.Math.Phys. 271 (2007) 247-274, arXiv:hep-th/0605198, Proposition A.1.

with cocycle $f((a,b),(a',b')) = ab'$ and commutator

$$\kappa((a,b),(a',b')) = ab' - a'b \tag{11.163}$$

We now relate this narrower notion of Heisenberg group to the general definition of a Heisenberg group that we just gave. First, let us generalize the Heisenberg groups (11.160) slightly: If we have a bilinear map $c : R \times R \to \mathcal{Z}$ where $\mathcal{Z}$ is abelian, and written additively, then we can define a central extension

$$0 \to \mathcal{Z} \to \tilde{G} \to R \times R \to 0 \tag{11.164}$$

by the law

$$(z_1,(a,b)) \cdot (z_2,(a',b')) = (z_1 + z_2 + c(a,b'),(a+a',b+b')) \tag{11.165}$$

The corresponding group cocycle is $f((a,b),(a',b')) = c(a,b')$ and 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 non-degenerate. In particular, if we take $\mathcal{Z} = R$ and $c(a,b') = ab'$ using the ring multiplication then we recover (11.160).

Example 1: *The group* $\mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n)$. Let us specialize the above discussion to $R = \mathbb{Z}/n\mathbb{Z}$, written additively. Then we define

$$U = \begin{pmatrix} \bar{1} & \bar{1} & 0 \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad V = \begin{pmatrix} \bar{1} & 0 & 0 \\ 0 & \bar{1} & \bar{1} \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad q = \begin{pmatrix} \bar{1} & 0 & \bar{1} \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \tag{11.166}$$

We easily check that for $a \in \mathbb{Z}$,

$$U^a = \begin{pmatrix} 1 & \bar{a} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad V^a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \bar{a} \\ 0 & 0 & 1 \end{pmatrix} \qquad q^a = \begin{pmatrix} 1 & 0 & \bar{a} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{11.167}$$

And moreover,

$$UV = qVU \qquad qU = Uq \qquad qV = Vq \tag{11.168}$$

Thus we obtain a presentation:

$$\mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n) = \langle U, V, q | U^n = V^n = q^n = 1, \quad UV = qVU, \quad Uq = qU, \quad Vq = qV \rangle \tag{11.169}$$

It is interesting to look at the Heisenberg extension

$$1 \to \mathbb{Z}_n \to \mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n) \to \mathbb{Z}_n \times \mathbb{Z}_n \to 1 \tag{11.170}$$

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 $\omega_1, \omega_2, \omega_3$. Then the cocycle is

$$f\left((\omega_1^s, \omega_2^t),(\omega_1^{s'}, \omega_2^{t'})\right) := \omega_3^{st'} \tag{11.171}$$

The corresponding commutator function is

$$\kappa\left((\omega_1^s,\omega_2^t),(\omega_1^{s'},\omega_2^{t'})\right) := \omega_3^{st'-ts'} \tag{11.172}$$

To connect with our general theory of extensions let $U := (1,(\omega_1,1))$, $V := (1,(1,\omega_2))$ and compute

$$\begin{aligned} UV &= (f((\omega_1,1),(1,\omega_2)),(\omega_1,\omega_2)) \\ &= (\omega_3,(\omega_1,\omega_2)) \\ VU &= (f((1,\omega_2),(\omega_1,1)),(\omega_1,\omega_2)) \\ &= (1,(\omega_1,\omega_2)) \end{aligned} \tag{11.173}$$

or in other words, since the center is generated by $q = (\omega_3,(1,1))$ we can write:

$$UV = qVU \tag{11.174}$$

Example 2: Let S be an abelian group and consider the *Pontryagin dual* group $\widehat{S}$. It is the group of homomorphisms $\mathrm{Hom}(S,U(1))$, or equivalently, the group of all one-dimensional unitary representations. Elements of this group are also called characters. Note that if $\chi_1,\chi_2 \in \mathrm{Hom}(S,U(1)$ then the pointwise product

$$(\chi_1\cdot\chi_2)(s) := \chi_1(s)\chi_2(s) \tag{11.175}$$

is again a homomorphism $S \to U(1)$. There is a very natural cocycle on the product $S\times\widehat{S}$ defined by

$$f\left((s_1,\chi_1),(s_2,\chi_2)\right) := \frac{1}{\chi_1(s_2)} \tag{11.176}$$

with commutator function:

$$\kappa\left((s_1,\chi_1),(s_2,\chi_2)\right) := \frac{\chi_2(s_1)}{\chi_1(s_2)} \tag{11.177}$$

and this defines a general Heisenberg extension

$$1 \to U(1) \to \mathrm{Heis}(S\times\widehat{S}) \to S\times\widehat{S} \to 1 \tag{11.178}$$

Remarks

1. *Stone-von Neumann Theorem.* There is a very natural representation of (11.178). Let $V = Fun(S \to \mathbb{C})$ be the vector space of complex-valued functions on S. We represent $s_0 \in S$ as a translation operator:

$$(T_{s_0}\cdot\Psi)(s) := \Psi(s+s_0) \tag{11.179}$$

and we represent $\chi \in \widehat{S}$ as a multiplication operator

$$(M_\chi\cdot\Psi)(s) := \chi(s)\Psi(s) \tag{11.180}$$

Then one checks that this does <u>not</u> define a representation of the direct product $S \times \widehat{S}$ but rather we have the operator equation:

$$T_{s_0} M_\chi = \chi(s_0) M_\chi T_{s_0} \tag{11.181}$$

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

$$(z;(s,\chi)) \to z T_s M_\chi \tag{11.182}$$

is a homomorphism, and in fact an isomorphism of Heis$(S \times \widehat{S})$ with $\mathcal{O}$. Once we combine this with suitable analysis [57] it turns out that what we have described is the unique irreducible unitary representation of Heis$(S \times \widehat{S})$, up to isomorphism. This is called the Stone-von Neumann theorem. This remark implies a rather far-ranging generalization of Fourier analysis.

2. This construction is extremely important in quantum mechanics and in the description of free quantum field theories. In these cases we take a vector space $V = S$ and its dual $V^\vee \cong \widehat{S}$, via

$$\chi_k(v) = e^{\mathrm{i}k\cdot v} \tag{11.183}$$

and use the pairing to define a cocycle valued in $\mathcal{Z} = \sqrt{-1}\mathbb{R}$. We will discuss all that in detail in the chapter on representations.

3. Let us compare a general Heisenberg extension

$$1 \to \mathcal{Z} \to \tilde{G} \to G \to 0 \tag{11.184}$$

with (11.164),(11.165) and (11.178). The difference from the general case is that in all these examples G is a product of subgroups $G = L \times L'$ where L and L' are *Lagrangian subgroups* in the sense that $\kappa(g_1, g_2) = 1$ for all for all pairs $(g_1, g_2) \in L$ and similarly for L'. Since κ is nondegenerate they are in fact maximal Lagrangian subgroups. However, the maximal subgroup is in general *not* unique and so this decomposition of G is noncanonical. Good examples are $G = \mathbb{R}^{2n}$ and $2n$-dimensional tori.

♣Comment on the use of this in the study of duality symmetries. ♣

4. *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

$$S = \frac{k}{4\pi}\int_{\mathbb{R}} dt \int_{T^2} A_1 \partial_t A_2 + \cdots \tag{11.185}$$

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.

[57] 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 $L^2(S)$.

Exercise

Referring to equations (11.143) and (11.141) et. seq.

a.) Show that the choice of section

$$s(\alpha,\beta) = U(\alpha)V(\beta) \tag{11.186}$$

leads to the cocycle

$$f((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{i\hbar(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_1\beta_2)} \tag{11.187}$$

b.) Show that the choice of section

$$s(\alpha,\beta) = \exp[i\hbar(\alpha\hat{p}+\beta\hat{q})] \tag{11.188}$$

leads to the cocycle

$$f((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{\frac{i}{2}\hbar(\alpha_1\beta_2-\alpha_2\beta_1)} \tag{11.189}$$

c.) Show that in both cases the commutator function is

$$\kappa((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{i\hbar(\alpha_1\beta_2-\alpha_2\beta_1)} \tag{11.190}$$

Exercise *Alternating implies skew*

Show that a map $\kappa : G \times G \to A$ which satisfies the bimultiplicative identity (11.151) and the alternating identity (11.150) is also skew, that is, satisfies (11.149).

Exercise

In an exercise above we listed the extensions of $\mathbb{Z}_2 \times \mathbb{Z}_2$ by $\mathbb{Z}_2$. Which one is the Heisenberg extension?

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. [58]

While these are not - strictly speaking - Heisenberg extensions people will often refer to them as Heisenberg extensions. We might call them "degenerate Heisenberg extensions."

[58] The center is generated by q, U^m, V^m and is $\mathbb{Z}_n \times \mathbb{Z}_k \times \mathbb{Z}_k$.

11.4 General Extensions Of G By An Abelian Group A

Let us now generalize central extensions to extensions of the form:

$$1 \to A \overset{\iota}{\to} \tilde{G} \overset{\pi}{\to} G \to 1 \tag{11.191}$$

where we continue to assume that $N = A$ is abelian, but now $\iota(A)$ is not necessarily central in G.

Much of our original story goes through, but now the map

$$\omega : G \to \mathrm{Aut}(A) \tag{11.192}$$

of our general discussion (defined in equations (11.12) and (11.14)) is actually a group homomorphism. As we stressed below (11.14), in general it is not a group homomorphism. There are two ways to understand that:

1. $\tilde{G}$ acts on A by conjugation of the isomorphic image of A in $\tilde{G}$ which, because the sequence is exact, is still a normal subgroup. So we can define
$$\iota(\tilde{\omega}_{\tilde{g}}(a)) := \tilde{g}\iota(a)\tilde{g}^{-1} \tag{11.193}$$
But now $\tilde{\omega}_{\tilde{g}}$ only depends on the equivalence class $[\tilde{g}] \in \tilde{G}/\iota(A)$ beccause
$$(\tilde{g}\iota(a_0))\,\iota(a)\,(\tilde{g}\iota(a_0))^{-1} = \tilde{g}\iota(a)\tilde{g}^{-1} \tag{11.194}$$
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 (11.14). But now [59] if we change section so that $\hat{s}(g) = \iota(t(g))s(g)$ is another section then we compute
$$\begin{aligned}\iota\left(\omega_{g,\hat{s}}(a)\right) &:= \{\iota(t(g))s(g)\} \cdot \iota(a) \cdot \{\iota(t(g))s(g)\}^{-1} \\ &= \iota(t(g)) \cdot \iota(\omega_{g,s}(a)) \cdot \iota(t(g))^{-1} \\ &= \iota\left\{t(g) \cdot \omega_{g,s}(a) \cdot (t(g))^{-1}\right\} \\ &= \iota(\omega_{g,s}(a))\end{aligned} \tag{11.195}$$
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 11.5. Moreover, given a choice of section we can define $f_s(g_1, g_2)$ just as we did in equation (11.44) (the definition works for all group extensions), and we can now compute, just as in (11.15):
$$\begin{aligned}\iota\left(\omega_{g_1} \circ \omega_{g_2}(a)\right) &= s(g_1)\iota(\omega_{g_2}(a))s(g_1)^{-1} \\ &= s(g_1)s(g_2)\iota(a)(s(g_1)s(g_2))^{-1} \\ &= \iota(f_s(g_1,g_2)) \cdot \iota(\omega_{g_1g_2}(a)) \cdot \iota(f_s(g_1,g_2))^{-1} \\ &= \iota\left\{f_s(g_1,g_2))\omega_{g_1g_2}(a)f_s(g_1,g_2))^{-1}\right\} \\ &= \iota\left(\omega_{g_1g_2}(a)\right)\end{aligned} \tag{11.196}$$

[59] Note that here the order of the two factors on the RHS matters, since $\iota(A)$ is not necessarily central in $\widetilde{G}$

and again notice that only in the very last line did we use the hypothesis that A is Abelian. Now, since ι is injective we conclude that $\omega_{g_1} \circ \omega_{g_2} = \omega_{g_1 g_2}$ so that the map ω is a group homomorphism.

Now, computing $s(g_1)s(g_2)s(g_3)$ in two ways, just as before, we derive the *twisted cocycle relation*:

$$\omega_{s,g_1}(f_s(g_2, g_3)) f_s(g_1, g_2 g_3) = f_s(g_1, g_2) f_s(g_1 g_2, g_3) \tag{11.197}$$

Conversely, given a twisted cocycle for ω we can define a group law on the set $A \times G$:

$$(a_1, g_1) \cdot (a_2, g_2) = (a_1 \omega_{g_1}(a_2) f(g_1, g_2), g_1 g_2) \tag{11.198}$$

The reader should check that this really does define a valid group law on the set $A \times G$.

Remark: Note that (11.198) simultaneously generalizes the twisted product of a semidirect product (10.2) and the twisted product of a central extension (11.53).

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

$$f_{\tilde{s}}(g_1, g_2) = t(g_1) \omega_{s,g_1}(t(g_2)) f_s(g_1, g_2) t(g_1 g_2)^{-1} \tag{11.199}$$

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 (11.259) below, the order definitely does matter.

We say to twisted cocycles are related by a twisted coboundary if they are related as in (11.199). One can check that if f is a twisted cocycle and we define f' as in (11.199) 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 11.2 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

$$1 \to A \to \tilde{G} \to G \to 1 \tag{11.200}$$

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 <u>trivializable</u> so that $[f] = 0$. Then our group extension is equivalent to a semidirect product. Nevertheless, the sequence (11.191) can be split in many different ways: There are many distinct <u>trivializations</u> and the different trivializations have meaning. Equivalently, there are many different coboundary transformations that preserve the trivial cocycle. A glance at (11.199) reveals that this will happen when

$$t(g_1 g_2) = t(g_1)\omega_{g_1}(t(g_2)) \tag{11.201}$$

This is known as a *twisted homomorphism*, or a one cocycle:

A 1-cochain $t \in C^1(G, A)$ is simply a map $t : G \to A$.

A twisted 1-cocycle $t \in Z^{1+\omega}(G, A)$ with twisting ω is a 1-cochain that satisfies (11.201).

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

$$\tilde{s}(g) = \iota(a)s(g)\iota(a)^{-1} \tag{11.202}$$

This corresponds to the function

$$t_a(g) = a\omega_g(a)^{-1} \tag{11.203}$$

To check this you write

$$\begin{aligned} \tilde{s}(g) &= \iota(a)s(g)\iota(a)^{-1} \\ &= \iota(a) \cdot \left(s(g)\iota(a)^{-1}s(g)^{-1}\right) \cdot s(g) \\ &= \iota(a) \cdot \left(\iota(\omega_g(a^{-1}))\right) \cdot s(g) \\ &= \left(\iota(a\omega_g(a^{-1}))\right) \cdot s(g) \end{aligned} \tag{11.204}$$

One easily checks that if t is a one-cocycle, then $t \cdot t_a$ is also a one-cocycle.

Theorem: When the sequence (11.191) 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 $H^{1+\omega}(G, A)$.

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

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.

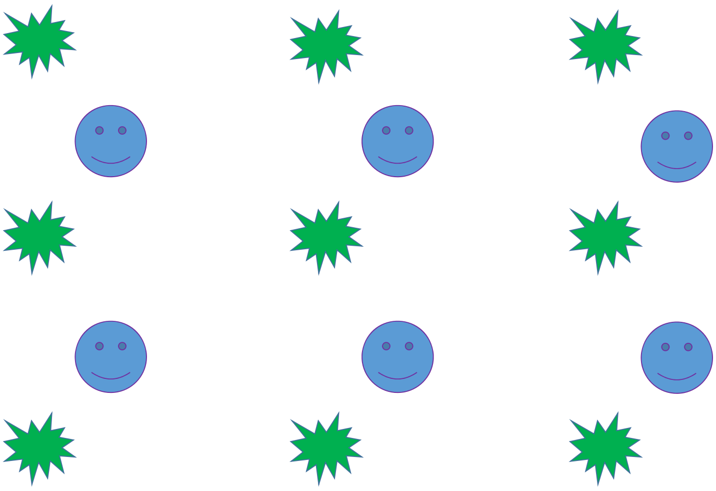

Figure 14: A portion of a crystal in the two-dimensional plane.

11.4.1 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 14. Then restricting the exact sequence of the Euclidean group to the subgroup, $G(C) \subset \text{Euc}(d)$, of those transformations that preserve C we have an exact sequence

$$1 \to L(C) \to G(C) \to P(C) \to 1 \tag{11.205}$$

where $P(C) \cong G(C)/L(C)$ is a subgroup of $O(d)$ known as the *point group of the crystal.*

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

$$\begin{aligned} \{\delta|\sigma\} &: n \mapsto \delta - n = -n + \delta \\ &: n + \delta \mapsto \delta - (n + \delta) = -n \end{aligned} \tag{11.206}$$

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

$$0 \to L(C) \cong \mathbb{Z} \to G(C) \to O(1) \cong \mathbb{Z}_2 \to 1 \tag{11.207}$$

But we can split this sequence by choosing a section $s(\sigma) = \{\delta| - 1\}$. Note that

$$\{\delta|\sigma\} \cdot \{\delta|\sigma\} = \{0|1\} \tag{11.208}$$

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: For another very similar example consider $\mathbb{Z}^2 \amalg (\mathbb{Z}^2 + \vec{\delta}) \subset \mathbb{R}^2$ for a generic vector δ the symmetry group will be isomorphic to the semidirect product $\mathbb{Z}^2 \rtimes \mathbb{Z}_2$, where we can lift the $\mathbb{Z}_2$ to, for example $\{\vec{\delta}|\sigma\}$ where $\sigma \in SO(2)$ is now inversion, $\vec{x} \to -\vec{x}$.

However, now let $0 < \delta < \frac{1}{2}$ and specialize $\vec{\delta}$ to $\vec{\delta} = (\delta, \frac{1}{2})$. Consider the crystal in two dimensions

$$C = \mathbb{Z}^2 \amalg (\mathbb{Z}^2 + \vec{\delta}) \tag{11.209}$$

then the point group is enhanced from $\mathbb{Z}_2$ to $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$$1 \to \mathbb{Z}^2 \to G(C) \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \tag{11.210}$$

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:

$$\hat{\sigma}_1 : (x_1, x_2) \mapsto (-x_1 + \delta, x_2 + \frac{1}{2}) \tag{11.211}$$

$$\hat{\sigma}_2 : (x_1, x_2) \mapsto (x_1, -x_2) \tag{11.212}$$

are symmetries of the crystal $G(C)$. In Seitz notation (or rather, its improvement - see above) we have:

$$\hat{\sigma}_1 = \{(\delta, \frac{1}{2})| \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}\} \tag{11.213}$$

$$\hat{\sigma}_2 = \{0| \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}\} \tag{11.214}$$

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

$$\hat{\sigma}_1^2 = \{(0,1)|1\} \tag{11.215}$$

is a nontrivial translation. Thus $\sigma_i \to \hat{\sigma}_i$ is *not* a splitting.

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

$$\begin{aligned} s(\sigma_1) &= \{(\delta, \frac{1}{2}) + v_1 | \sigma_1\} \\ s(\sigma_2) &= \{v_2 | \sigma_2\} \end{aligned} \tag{11.216}$$

where $v_1, v_2 \in \mathbb{Z}^2$. Now consider the group commutator

$$[s(\sigma_1), s(\sigma_2)] = \{(1 - \sigma_2)v_2 - (1 - \sigma_1)v_1 | 1\} \tag{11.217}$$

Doing the actual matrix multiplication on the most general vectors $v_1, v_2 \in \mathbb{Z}^2$ you can convince yourself that we always have:

$$(1 - \sigma_2)v_2 - (1 - \sigma_1)v_1 \neq 0 \tag{11.218}$$

for any v_1, v_2. But since the point group is commutative this means that no section exists which is a group homomorphism. That is, the sequence does not split.

♣ RELATE TO ACTUAL COHO GROUPS. CONSIDER CASE WITH BOTH δ_1, δ_2 HALF-INTEGRAL. ♣

In solid state physics when the sequence (11.205) does not split the crystallographic group $G(C)$ is said to be *nonsymmorphic*.

11.4.2 Time Reversal

A good example of where we need to use twisted cocycles to 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-reversal symmetry. In this case there is a homomorphism

$$\tau : G \to \{\pm 1\} \cong \mathbb{Z}_2 \tag{11.219}$$

telling us whether the symmetries $g \in G$ preserve or reverse 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 *** 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. So we consider the group homomorphism

$$\omega : G \to \mathrm{Aut}(U(1)) \cong \mathrm{Out}(U(1)) \cong \mathbb{Z}_2 \tag{11.220}$$

where:

$$\omega(g)(z) = \begin{cases} z & \tau(g) = +1 \\ z^{-1} & \tau(g) = -1 \end{cases} \tag{11.221}$$

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 $\bar{T}$ will act as an operator $\tilde{T}$ 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 we need the group cohomology:

$$H^{2+\omega}(\mathbb{Z}_2, U(1)) = \mathbb{Z}_2 \tag{11.222}$$

So there are two extensions:

♣Check and Explain that some more ♣

$$\begin{tikzcd} 1 \arrow[r] & U(1) \arrow[r] & M_2^{\pm} \arrow[r, "\tilde{\pi}"] & M_2 \arrow[r] & 1 \end{tikzcd} \tag{11.223}$$

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

$$\tilde{T}z = \tilde{T}\tilde{T}^2 = \tilde{T}^2\tilde{T} = z\tilde{T} \tag{11.224}$$

on the other hand if we take $\omega(\bar{T})$ to be the nontrivial automorphism of $U(1)$ then

$$\tilde{T}z = z^{-1}\tilde{T} \tag{11.225}$$

Therefore $z^2 = 1$, so $z = \pm 1$, and therefore $\tilde{T}^2 = \pm 1$. Thus the two groups are

$$M_2^{\pm} = \{z\tilde{T} | z\tilde{T} = \tilde{T}z^{-1} \qquad \& \qquad \tilde{T}^2 = \pm 1\} \tag{11.226}$$

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

$$(\tilde{T}')^2 = (\mu\tilde{T})^2 = \mu\bar{\mu}\tilde{T}^2 = \tilde{T}^2 \tag{11.227}$$

So the <u>sign</u> 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 $SO(2) \cong U(1)$:

$$O(2) = SO(2) \rtimes \mathbb{Z}_2 \tag{11.228}$$

But the nontrivial extension is a new group for us. It double-covers $O(2)$ and is known as $\mathrm{Pin}^-(2)$. We can take $T \to P$ and $z = e^{\mathrm{i}\alpha} \to R(2\alpha)$, so that $-1 \mapsto +1$. In $\mathrm{Pin}^+(2)$ the double cover of a reflection squared to one. Now, in $\mathrm{Pin}^-(2)$ the double cover of a reflection 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:

$$(\tilde{T} \cdot \Psi)(\vec{x}, t) = \mathrm{i}\sigma^2(\Psi(\vec{x}, -t)^* \tag{11.229}$$

where here Ψ is a 2-component spinor function of $(\vec{x}, t)$. [60] Note that this implies:

$$\begin{aligned} (\tilde{T}^2 \cdot \Psi)(\vec{x}, t) &= \mathrm{i}\sigma^2 \cdot \Big((\tilde{T} \cdot \Psi)(\vec{x}, -t)\Big)^* \\ &= \mathrm{i}\sigma^2 \cdot \big(\mathrm{i}\sigma^2 \cdot (\Psi(\vec{x}, t))^*\big)^* \\ &= \mathrm{i}\sigma^2\mathrm{i}\sigma^2\Psi(\vec{x}, t) \\ &= -\Psi(\vec{x}, t) \end{aligned} \tag{11.230}$$

[60] 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 $\tilde{T}^2 = (-1)^{2j}$. This 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

$$\tilde{T} \cdot \Psi = z\Psi \tag{11.231}$$

for some complex number z. Then act with $\tilde{T}$ again and use the fact that it is anti-unitary and squares to -1:

$$-\Psi = z^* \tilde{T} \cdot \Psi \tag{11.232}$$

but this implies that $z = -1/z^*$ which implies $|z|^2 = -1$, which is impossible. Therefore, (11.231) 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.

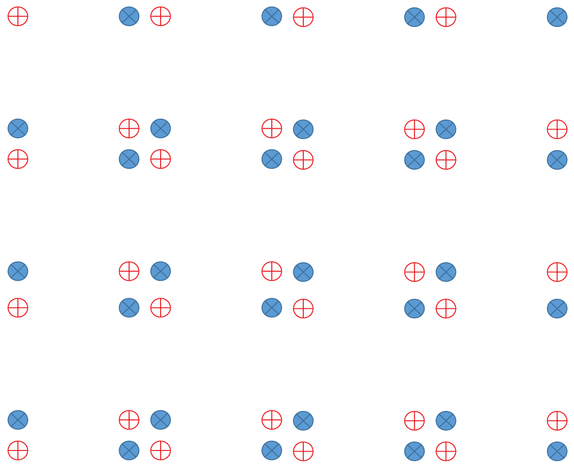

Figure 15: In this figure the blue crosses represent an atom with a local magnetic moment pointing up while the red crosses represent an atom with a local magnetic moment pointing down. The magnetic point group is isomorphic to D_4 but the homomorphism τ to $\mathbb{Z}_2$ has a kernel $\mathbb{Z}_2 \times \mathbb{Z}_2$ (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.

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

$$C = \left(\mathbb{Z}^2 + (\delta_1, \delta_2)\right) \amalg \left(\mathbb{Z}^2 + (-\delta_2, \delta_1)\right) \amalg \left(\mathbb{Z}^2 + (-\delta_1, -\delta_2)\right) \amalg \left(\mathbb{Z}^2 + (\delta_2, -\delta_1)\right) \tag{11.233}$$

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

$$G(C) = \mathbb{Z}^2 \rtimes D_4 \tag{11.234}$$

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

$$\widehat{C} = \widehat{C}_+ \amalg \widehat{C}_- \tag{11.235}$$

with

$$\widehat{C}_+ = \left(\mathbb{Z}^2 + (\delta_1, \delta_2)\right) \times \{S\} \amalg \left(\mathbb{Z}^2 + (-\delta_1, -\delta_2)\right) \times \{S\} \tag{11.236}$$

but a spin $-S$ on points of the complementary sub-crystal

$$\widehat{C}_- = \left(\mathbb{Z}^2 + (-\delta_2, \delta_1)\right) \times \{-S\} \amalg \left(\mathbb{Z}^2 + (\delta_2, -\delta_1)\right) \times \{-S\} \tag{11.237}$$

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 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:

$$0 \to \mathbb{Z}^2 \to \widehat{G(C)} \to \widehat{P(C)} \to 1 \tag{11.238}$$

The elements in $\widehat{P(C)}$ are

$$\{(1,1), (R,\sigma), (R^2,1), (R^3,\sigma), (P,\sigma), (PR,1), (PR^2,\sigma), (PR^3,1)\} \tag{11.239}$$

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

$$1 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to \widehat{P(C)} \xrightarrow{\tau} \mathbb{Z}_2 \to 1 \tag{11.240}$$

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

$$\tau : G \to \mathbb{Z}_2 \tag{11.241}$$

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

$$\rho(t_1) = U(t_1, t_2)\rho(t_2)U(t_2, t_1) \tag{11.242}$$

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. [61]

By Stone's theorem, $U(t)$ has a self-adjoint generator H, the Hamiltonian, so that we may write

$$U(t) = \exp\left(-\frac{it}{\hbar}H\right) \tag{11.243}$$

♣There is an obvious generalization of this statement for $U(t_1, t_2)$. Is it proved rigorously somewhere? ♣

Now, we say a quantum symmetry $\rho : G \to \mathrm{Aut}_{\mathrm{qtm}}(\mathbb{P}\mathcal{H})$ lifting to $\rho^{\mathrm{tw}} : G^{\mathrm{tw}} \to \mathrm{Aut}_{\mathbb{R}}(\mathcal{H})$ is a *symmetry of the dynamics* if for all $g \in G^{\mathrm{tw}}$:

$$\rho^{\mathrm{tw}}(g)U(t)\rho^{\mathrm{tw}}(g)^{-1} = U(\tau(g)t) \tag{11.244}$$

where $\tau : G^{\mathrm{tw}} \to \mathbb{Z}_2$ is inherited from the analogous homomorphism on G.

Now, substituting (11.243) and paying proper attention to ϕ we learn that the condition for a symmetry of the dynamics (11.244) is equivalent to

$$\phi(g)\rho^{\mathrm{tw}}(g)H\rho^{\mathrm{tw}}(g)^{-1} = \tau(g)H \tag{11.245}$$

[61] 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 $\rho^{\mathrm{tw}}(g)H(t)\rho^{\mathrm{tw}}(g)^{-1} = \phi(g)\tau(g)H(t)$ for all t.

in other words,

$$\rho^{\rm tw}(g) H \rho^{\rm tw}(g)^{-1} = \phi(g)\tau(g) H \tag{11.246}$$

Thus, the answer to our question is that ϕ and τ are *unrelated* in general. We should therefore define a third homomorphism $\chi : G \to \mathbb{Z}_2$

$$\chi(g) := \phi(g)\tau(g) \in \{\pm 1\} \tag{11.247}$$

Note that

$$\phi \cdot \tau \cdot \chi = 1 \tag{11.248}$$

2. It is very unusual to have a nontrivial homomorphism χ. Note that

$$\rho^{\rm tw}(g) H \rho^{\rm tw}(g)^{-1} = \chi(g) H \tag{11.249}$$

implies that if any group element has $\chi(g) = -1$ then the spectrum of H must be symmetric around zero. 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.

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.

11.5 General Extensions

Let us briefly return to the general extension (11.1). 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 (11.1) 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 automatically gives us two maps:

1. $\omega_s : Q \to {\rm Aut}(N)$

2. $f_s : Q \times Q \to N$

These two maps are defined by

$$\iota(\omega_{s,q}(n)) := s(q)\iota(n)s(q)^{-1} \tag{11.250}$$

and

$$s(q_1)s(q_2) := \iota(f_s(q_1, q_2))s(q_1 \cdot q_2) \tag{11.251}$$

respectively.

Now (11.250) defines an element of $\mathrm{Aut}(N)$ 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 (11.250) and (11.5) we can derive a twisted version of the homomorphism rule:

$$\omega_{s,q_1} \circ \omega_{s,q_2} = I(f_s(q_1, q_2)) \circ \omega_{s,q_1 q_2} \tag{11.252}$$

Recall that for $a \in N$, $I(a) \subset \mathrm{Aut}(N)$ denotes the inner automorphism given by conjugation by a. The proof of (11.252) follows exactly the same steps as (11.196), except for the very last line.

Moreover, using (11.5) 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:

$$\omega_{s,q_1}(f_s(q_2, q_3))f_s(q_1, q_2q_3) = f_s(q_1, q_2)f_s(q_1q_2, q_3) \tag{11.253}$$

Note this is the same as (11.197), 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 (11.1) there exist maps (ω_s, f_s), associated with any section s and defined by (11.250) and (11.5). The maps (ω_s, f_s) automatically satisfy the identities (11.252) and (11.253).

Conversely, suppose we are given two maps:

1. A map $f : Q \times Q \to N$
2. A map $\omega : Q \to \mathrm{Aut}(N)$

And suppose the data (ω, f) satisfy the two conditions

$$\omega_{q_1} \circ \omega_{q_2} = I(f(q_1, q_2)) \circ \omega_{q_1 q_2} \tag{11.254}$$

$$\omega_{q_1}(f(q_2, q_3))f(q_1, q_2q_3) = f(q_1, q_2)f(q_1q_2, q_3) \tag{11.255}$$

then we can construct an extension (11.1) with the multiplication law:

$$(n_1, q_1) \cdot_{f,\omega} (n_2, q_2) := (n_1\omega_{q_1}(n_2)f(q_1, q_2), q_1q_2) \tag{11.256}$$

This is very similar to (11.198) 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 (11.254) and (11.255) one can check the associativity law and the other group axioms. We have already seen this simultaneous generalization of the semidirect product (10.2) and the twisted product of a central extension (11.53) in our discussion of the case where $N = A$ is abelian. (See equation (11.198) 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 (11.254) and (11.255). Any other section $\tilde{s}$ is related to s by a function $t : Q \to N$. Indeed that function t is defined by:

$$\tilde{s}(q) = \iota(t(q))s(q) \tag{11.257}$$

and one easily computes that we now have

$$\omega_{\tilde{s},q} = I(t(q)) \circ \omega_{s,q} \tag{11.258}$$

$$f_{\tilde{s}}(q_1, q_2) = t(q_1)\omega_{s,q_1}(t(q_2))f_s(q_1, q_2)t(q_1q_2)^{-1} \tag{11.259}$$

The proof of (11.258) follows exactly the same steps as (11.195). To prove (11.258) we patiently combine the definition (11.257) with the definition .

♣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 (11.254) and (11.255) and an arbitrary function $t : Q \to N$. We can now define a new pair (ω', f') by the equations:

$$\omega'_q = I(t(q)) \circ \omega_q \tag{11.260}$$

$$f'(q_1, q_2) = t(q_1)\omega_{q_1}(t(q_2))f(q_1, q_2)t(q_1q_2)^{-1} \tag{11.261}$$

Now, with some algebra (DO IT!) one can check that indeed (ω', f') really do satisfy (11.254) and (11.255) as well. Equations (11.260) and (11.261) generalizes the coboundary relation (11.51) of central extension theory.

The relations (11.260) and (11.261) define an equivalence relation on the set of pairs (ω, f) satisfying (11.254) and (11.255). Moreover, if (ω, f) and (ω', f') are related by (11.260) and (11.261) then we can define a group structure on the set $N \times Q$ in two ways using the equation (11.256) for each pair. Nevertheless, there is a morphism between these two extensions in the sense of (11.4) above where we define

$$\varphi(n, q) := (nt(q)^{-1}, q) \tag{11.262}$$

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 (11.254) 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:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota"] \arrow[d, "I"] & G \arrow[r, "\pi"] \arrow[d, "\psi"] & Q \arrow[r] \arrow[d, "\varpi"] & 1 \\
1 \arrow[r] & \mathrm{Inn}(N) \arrow[r] & \mathrm{Aut}(N) \arrow[r] & \mathrm{Out}(N) \arrow[r] & 1
\end{tikzcd} \tag{11.263}$$

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

$$\iota(\psi(g)(n)) = g\iota(n)g^{-1} \tag{11.264}$$

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* (11.263)*?*

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 (11.31) of the canonical exact sequence given by the lower line of (11.263). 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 <u>third</u> cohomology group $H^{3+\bar{\omega}}(Q, Z(N))$ where $Z(N)$ is the center of N. See section 11.6.5 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

$$\omega_q^{(1)} = I(t(q)) \circ \omega_q^{(2)} \tag{11.265}$$

for some function $t : Q \to N$. Note, please, that while this equation is formally very similar to (11.258) 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

$$\begin{aligned}
\omega_{q_1}^{(1)} \circ \omega_{q_2}^{(1)}(n) &= t(q_1)\omega_{q_1}^{(2)}\left(t(q_2)\omega_{q_2}^{(2)}(n)t(q_2)^{-1}\right)t(q_1)^{-1} \\
&= t(q_1)\omega_{q_1}^{(2)}(t(q_2))\left(\omega_{q_1}^{(2)} \circ \omega_{q_2}^{(2)}(n)\right)\omega_{q_2}^{(2)}(t(q_2)^{-1})t(q_1)^{-1} \\
&= t(q_1)\omega_{q_1}^{(2)}(t(q_2))\left(f^{(2)}(q_1, q_2)\omega_{q_1q_2}^{(2)}(n)f^{(2)}(q_1, q_2)^{-1}\right)\omega_{q_2}^{(2)}(t(q_2)^{-1})t(q_1)^{-1} \\
&= \left\{t(q_1)\omega_{q_1}^{(2)}(t(q_2))f^{(2)}(q_1, q_2)t(q_1q_2)^{-1}\right\} \cdot \omega_{q_1q_2}^{(1)}(n)\left\{t(q_1)\omega_{q_1}^{(2)}(t(q_2))f^{(2)}(q_1, q_2)t(q_1q_2)^{-1}\right\}^{-1} \\
&= \hat{f}^{(2)}(q_1, q_2) \cdot \omega_{q_1q_2}^{(1)}(n)\hat{f}^{(2)}(q_1, q_2)^{-1}
\end{aligned} \tag{11.266}$$

where we define

$$\hat{f}^{(2)}(q_1, q_2) := t(q_1)\omega_{q_1}^{(2)}(t(q_2))f^{(2)}(q_1, q_2)t(q_1q_2)^{-1} \tag{11.267}$$

On the other hand, we know that

$$\omega_{q_1}^{(1)} \circ \omega_{q_2}^{(1)}(n) = f^{(1)}(q_1, q_2)\omega_{q_1q_2}^{(1)}(n)f^{(1)}(q_1, q_2)^{-1} \tag{11.268}$$

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

$$\hat{f}^{(2)}(q_1, q_2) = f^{(1)}(q_1, q_2)\zeta(q_1, q_2) \tag{11.269}$$

for some function $\zeta : Q \times Q \to Z(N)$. These two functions are <u>not</u> necessarily related by a coboundary and the extensions are <u>not</u> 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 (11.269) also satisfies the twisted cocycle relation. (This requires a lot of patient algebra....) It follows that

$$\zeta \in Z^{2+\bar{\omega}}(Q, Z(N)) \tag{11.270}$$

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 (11.269). 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 [62] 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 (11.256) really defines a group structure.

a.) Check the associativity relation.

b.) What is the identity element? [63]

c.) Check that every element has an inverse.

Exercise

a.) Check that (11.262) really does define a homomorphism of the group laws (11.256) defined by (ω, f) and (ω', f') if (ω', f') is related to (ω, f) by (11.260) and (11.261).

b.) Check that the diagram (11.4) really does commute if we use (11.262).

11.6 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,...)

[62] 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'.

[63] *Answer*: $(f(1,1)^{-1}, 1_Q)$.

4. Condensed matter/topological phases of matter (Kitaev; Wen et. al.; Kapustin et. al.; Freed-Hopkins;....)
5. Three-dimensional supersymmetric gauge theory.

Here we will be brief and just give the basic definitions:

11.6.1 Definition

Suppose we are given any group G and an Abelian group A (written additively in this sub-section) and a homomorphism

$$\omega : G \to \mathrm{Aut}(A) \tag{11.271}$$

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: $d : C^n(G, A) \to C^{n+1}(G, A)$

$$\begin{gathered}(d\phi)(g_1, \dots, g_{n+1}) := \omega_{g_1}\left(\phi(g_2, \dots, g_{n+1})\right) \\ -\phi(g_1g_2, g_3, \dots, g_{n+1}) + \phi(g_1, g_2g_3, \dots, g_{n+1}) \pm \cdots + (-1)^n \phi(g_1, \dots, g_{n-1}, g_ng_{n+1}) \\ + (-1)^{n+1}\phi(g_1, \dots, g_n)\end{gathered} \tag{11.272}$$

Then we have, for $n = 0$:

$$(d\phi_0)(g) = \omega_g(a) - a \tag{11.273}$$

For $n = 1$, $n = 2$ and $n = 3$ the formula written out looks like:

$$(d\phi_1)(g_1, g_2) = \omega_{g_1}\left(\phi_1(g_2)\right) - \phi_1(g_1g_2) + \phi_1(g_1) \tag{11.274}$$

$$(d\phi_2)(g_1, g_2, g_3) = \omega_{g_1}\left(\phi_2(g_2, g_3)\right) - \phi_2(g_1g_2, g_3) + \phi_2(g_1, g_2g_3) - \phi_2(g_1, g_2) \tag{11.275}$$

$$(d\phi_3)(g_1, g_2, g_3, g_4) = \omega_{g_1}\left(\phi_3(g_2, g_3, g_4)\right) - \phi_3(g_1g_2, g_3, g_4) + \phi_3(g_1, g_2g_3, g_4) - \phi_3(g_1, g_2, g_3g_4) + \phi_3(g_1, g_2, g_3) \tag{11.276}$$

Next, one can check that for any ϕ, we have the absolutely essential equation:

$$\boxed{d(d\phi) = 0} \tag{11.277}$$

We will give a simple proof of (11.277) 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

$$\begin{aligned}(d^2\phi_0)(g_1, g_2) &= \omega_{g_1}(d\phi_0(g_2)) - d\phi_0(g_1 \cdot g_2) + d\phi_0(g_1) \\ &= \omega_{g_1}\left(\omega_{g_2}(a) - a\right) - \left(\omega_{g_1g_2}(a) - a\right) + \left(\omega_{g_1}(a) - a\right) \\ &= \omega_{g_1}(\omega_{g_2}(a)) - \omega_{g_1g_2}(a) \\ &= 0\end{aligned} \tag{11.278}$$

if ϕ_1 is any 1-cochain then we compute:

$$\begin{aligned}(d^2\phi_1)(g_1,g_2,g_3) &= \omega_{g_1}(d\phi_1(g_2,g_3)) - (d\phi_1)(g_1g_2,g_3) + (d\phi_1)(g_1,g_2g_3) - (d\phi_1)(g_1,g_2)\\ &= \omega_{g_1}\left(\omega_{g_2}(\phi_1(g_3)) - \phi_1(g_2g_3) + \phi_1(g_2)\right)\\ &- \left(\omega_{g_1g_2}(\phi_1(g_3)) - \phi_1(g_1g_2g_3) + \phi_1(g_1g_2)\right)\\ &+ \left(\omega_{g_1}(\phi_1(g_2g_3) - \phi_1(g_1g_2g_3) + \phi_1(g_1)\right)\\ &- \left(\omega_{g_1}(\phi_1(g_2)) - \phi_1(g_1g_2) + \phi_1(g_1)\right)\\ &= 0\end{aligned} \tag{11.279}$$

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 (11.277) we can define a subgroup $B^{n+\omega}(G,A) \subset Z^{n+\omega}(G,A)$, called the subgroup of coboundaries:

$$B^{n+\omega}(G,A) := \{\phi_n | \exists \phi_{n-1} \qquad s.t. \qquad d\phi_{n-1} = \phi_n\} \tag{11.280}$$

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

$$H^{n+\omega}(G,A) = Z^{n+\omega}(G,A)/B^{n+\omega}(G,A) \tag{11.281}$$

Example: Let us take $G = \mathbb{Z}_2 = \{1,\sigma\}$ and $A = \mathbb{Z}$. Recall that

$$\mathrm{Aut}(A) = \mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}, \mathcal{P}\} \cong \mathbb{Z}_2 \tag{11.282}$$

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

$$\begin{aligned}(d\phi_0)(1) &= 0\\ (d\phi_0)(\sigma) &= \omega_\sigma(n_0) - n_0 = \begin{cases} 0 & \omega = T\\ -2n_0 & \omega = \mathcal{I}\end{cases}\end{aligned} \tag{11.283}$$

Now consider the differential of a one-cochain:

$$\begin{aligned}(d\phi_1)(1,1) &= \omega_1(\phi_1(1)) - \phi_1(1) + \phi_1(1) = \phi_1(1)\\ (d\phi_1)(1,\sigma) &= \omega_1(\phi_1(\sigma)) - \phi_1(\sigma) + \phi_1(1) = \phi_1(1)\\ (d\phi_1)(\sigma,1) &= \omega_\sigma(\phi_1(1)) - \phi_1(\sigma) + \phi_1(\sigma) = \omega_\sigma(\phi_1(1))\\ (d\phi_1)(\sigma,\sigma) &= \omega_\sigma(\phi_1(\sigma)) - \phi_1(1) + \phi_1(\sigma)\end{aligned} \tag{11.284}$$

Now the cocycle condition implies $\phi_1(1) = 0$, making the first three lines of (11.284) vanish. Using this the fourth line becomes:

$$(d\phi_1)(\sigma,\sigma) = \omega_\sigma(\phi_1(\sigma)) + \phi_1(\sigma) = \begin{cases} 2\phi_1(\sigma) & \omega = T \\ 0 & \omega = \mathcal{I} \end{cases} \tag{11.285}$$

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 <u>any</u> 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 (11.283). We can shift a by any even integer $a \to a - 2n_0$. So

$$H^{1+\mathcal{I}}(\mathbb{Z}_2, \mathbb{Z}) \cong \mathbb{Z}_2 \tag{11.286}$$

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 (11.197) and (11.199) 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

$$\partial_n : C_n \to C_{n-1} \tag{11.287}$$

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 <u>NOT</u> exact sequences. Indeed the failure to be an exact sequence is measured by the *homology groups* of the chain complex

$$H_n(C_*, \partial_*) := \ker(\partial_n)/\mathrm{im}(\partial_{n+1}) \tag{11.288}$$

and the *cohomology groups* of the cochain complex:

$$H^n(C^*, d_*) := \ker(d_n)/\mathrm{im}(d_{n-1}) \tag{11.289}$$

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

$$\varphi(hg_0, hg_1, \dots, hg_n) = \omega_h \left(\varphi(g_0, g_1, \dots, g_n)\right) \tag{11.290}$$

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

$$\delta : \mathcal{C}^n(G, A) \to \mathcal{C}^{n+1}(G, A) \tag{11.291}$$

by

$$\delta\varphi(g_0, \dots, g_{n+1}) := \sum_{i=0}^{n+1} (-1)^i \varphi(g_0, \dots, \widehat{g_i}, \dots, g_{n+1}) \tag{11.292}$$

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:

$$\begin{aligned}
\delta^2\varphi(g_0, \dots, g_{n+1}) &= \sum_{i=0}^{n+1} (-1)^i \left\{ \sum_{j=0}^{i-1} (-1)^j \varphi(g_0, \dots, \widehat{g_j}, \dots, \widehat{g_i}, \dots, g_{n+1}) \right. \\
&\qquad \left. - \sum_{j=i+1}^{n+1} (-1)^j \varphi(g_0, \dots, \widehat{g_i}, \dots, \widehat{g_j}, \dots, g_{n+1}) \right\} \\
&= \sum_{0 \le j < i \le n+1} (-1)^{i+j} \varphi(g_0, \dots, \widehat{g_j}, \dots, \widehat{g_i}, \dots, g_{n+1}) \\
&\qquad - \sum_{0 \le i < j \le n+1} (-1)^{i+j} \varphi(g_0, \dots, \widehat{g_i}, \dots, \widehat{g_j}, \dots, g_{n+1}) \\
&= 0
\end{aligned} \tag{11.293}$$

Now, we can define an isomorphism $\psi : \mathcal{C}^n(G, A) \to C^n(G, A)$ by defining

$$\phi_n(g_1, \dots, g_n) := \varphi_n(1, g_1, g_1g_2, \dots, g_1 \cdots g_n) \tag{11.294}$$

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 (11.292) becomes the more complicated formula (11.272). 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:

$$\begin{tikzcd}
\mathcal{C}^n(G, A) \arrow[r, "\delta"] \arrow[d, "\psi"] & \mathcal{C}^{n+1}(G, A) \arrow[d, "\psi"] \\
C^n(G, A) \arrow[r, "d"] & C^{n+1}(G, A)
\end{tikzcd} \tag{11.295}$$

For example, if

$$\phi_1(g) = \psi(\varphi_1)(g) = \varphi_1(1, g) \tag{11.296}$$

then we can check that

$$\begin{aligned}(d\phi_1)(g_1,g_2) &= d(\psi(\varphi_1))(g_1,g_2)\\ &= \psi(\delta\varphi_1)(g_1,g_2)\\ &= \delta\varphi_1(1,g_1,g_1g_2)\\ &= \varphi_1(g_1,g_1g_2) - \varphi_1(1,g_1g_2) + \varphi_1(1,g_1)\\ &= \omega_{g_1}(\varphi_1(1,g_2)) - \varphi_1(1,g_1g_2) + \varphi_1(1,g_1)\\ &= \omega_{g_1}(\phi_1(g_2)) - \phi_1(g_1g_2) + \phi_1(g_1)\end{aligned} \tag{11.297}$$

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:

$$C^n := \mathrm{Hom}(C_n, \mathbb{Z}) \tag{11.298}$$

11.6.2 Interpreting the meaning of $H^{0+\omega}$

A zero-cocycle is an element $a \in A$ so that for all g

$$\omega_g(a) = a \tag{11.299}$$

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.

11.6.3 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:

$$0 \to A \to A \rtimes G \to G \to 1 \tag{11.300}$$

11.6.4 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

$$0 \to A \to \tilde{G} \to G \to 1 \tag{11.301}$$

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 $H^{2+\bar{\omega}}(Q,Z(N))$.

11.6.5 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 §11.5.

Recall that, as we have discussed using (11.263), a general extension (11.1) has a canonically associated homomorphism

$$\bar{\omega} : Q \to \mathrm{Out}(N) \tag{11.302}$$

where $\mathrm{Out}(N)$ is the group of outer automorphisms of N.

The natural question arises: *Given a homomorphism $\bar{\omega}$ as in* (11.302) *is there a corresponding extension of Q by N inducing $\bar{\omega}$ as in equation* (11.263) *?*

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

$$1 \to \mathrm{Inn}(N) \to \mathrm{Aut}(N) \to \mathrm{Out}(N) \to 1 \tag{11.303}$$

then $q \mapsto \xi_q$ will not be a group homomorphism. But we do know that for all $q_1, q_2 \in Q$

$$\xi_{q_1} \circ \xi_{q_2} \circ \xi^{-1}_{q_1 q_2} \in \mathrm{Inn}(N) \tag{11.304}$$

Therefore, for every q_1, q_2 we may *choose* an element $f(q_1,q_2) \in N$ so that

$$\xi_{q_1} \circ \xi_{q_2} \circ \xi^{-1}_{q_1 q_2} = I(f(q_1,q_2)) \tag{11.305}$$

i.e.

$$\xi_{q_1} \circ \xi_{q_2} = I(f(q_1,q_2)) \circ \xi_{q_1 q_2} \tag{11.306}$$

Of course, the choice of $f(q_1,q_2)$ is ambiguous by an element of $Z(N)$!

Equation (11.306) is of course just (11.254) written in slightly different notation. Therefore, as we saw in §11.5, if $f(q_1,q_2)$ were to satisfy the the "twisted cocycle condition" (11.255) then we could use (11.256) 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 (11.255). Looking at the RHS of (11.255) we compute:

$$\begin{aligned} I(f(q_1,q_2)f(q_1q_2,q_3)) &= I(f(q_1,q_2))I(f(q_1q_2,q_3)) \\ &= \left(\xi_{q_1} \circ \xi_{q_2} \circ \xi^{-1}_{q_1q_2}\right) \circ \left(\xi_{q_1q_2} \circ \xi_{q_3} \circ \xi^{-1}_{q_1q_2q_3}\right) \\ &= \xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_3} \circ \xi^{-1}_{q_1q_2q_3} \end{aligned} \tag{11.307}$$

On the other hand, looking at the LHS of (11.255) we compute:

$$\begin{aligned} I(\xi_{q_1}(f(q_2,q_3))f(q_1,q_2q_3)) &= I(\xi_{q_1}(f(q_2,q_3)))I(f(q_1,q_2q_3)) \\ &= \xi_{q_1}\circ I((f(q_2,q_3)))\circ \xi_{q_1}^{-1}\circ I(f(q_1,q_2q_3) \\ &= \xi_{q_1}\circ \left(\xi_{q_2}\circ\xi_{q_3}\circ\xi_{q_2q_3}^{-1}\right)\circ\xi_{q_1}^{-1}\circ\left(\xi_{q_1}\circ\xi_{q_2q_3}\circ\xi_{q_1q_2q_3}^{-1}\right) \\ &= \xi_{q_1}\circ\xi_{q_2}\circ\xi_{q_3}\circ\xi_{q_1q_2q_3}^{-1} \end{aligned} \tag{11.308}$$

Therefore, comparing (11.307) and (11.308) we conclude that

$$I(\xi_{q_1}(f(q_2,q_3))f(q_1,q_2q_3)) = I(f(q_1,q_2)f(q_1q_2,q_3)) \tag{11.309}$$

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

$$f(q_1,q_2)f(q_1q_2,q_3) = z(q_1,q_2,q_3)\xi_{q_1}(f(q_2,q_3))f(q_1,q_2q_3) \tag{11.310}$$

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 11.6.5.1 : 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 [64] 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:

$$x^4 = y^2 \qquad x^8 = 1 \qquad yxy^{-1} = x^{-1} \tag{11.311}$$

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

$$\alpha(x)=x^3, \alpha(y)=y \qquad\qquad \beta(x)=x, \beta(y)=yx \tag{11.312}$$

Then there is is no group extension with group G fitting in

$$1\to N\to G\to\mathbb{Z}_2\to 1 \tag{11.313}$$

[64] 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. [65] 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.

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

♣Really should explain four-term sequences and crossed modules here.... ♣

1. K. Brown, *Group Cohomology.*
2. C. A. Weibel, *An introduction to homological algebra*, chapter 6

11.7 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 11.6.5, 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

12. 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

[65] 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. [66]

One might well ask: Can we classify finite groups? In this section we survey a little of what is known about this problem.

12.1 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

$$D_n = \langle a, b | a^n = b^2 = 1, bab = a^{-1} \rangle \tag{12.1}$$

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

$$1 \to N \to G \to \mathbb{Z}_2 \to 1 \tag{12.2}$$

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

$$1 \to \mathbb{Z}_4 \to G \to \mathbb{Z}_2 \to 1 \tag{12.3}$$

[66] $Spin(n)$ 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. ♣

$$1 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{12.4}$$

$$1 \to \mathbb{Z}_4 \to \mathbb{Z}_8 \to \mathbb{Z}_2 \to 1 \tag{12.5}$$

$$1 \to \mathbb{Z}_4 \to D_4 \to \mathbb{Z}_2 \to 1 \tag{12.6}$$

$$1 \to \mathbb{Z}_4 \to \widetilde{D}_2 \to \mathbb{Z}_2 \to 1 \tag{12.7}$$

Here we meet the first of the series of *dicyclic* or *binary dihedral* groups defined by

$$\widetilde{D_n} := \langle a, b | a^{2n} = 1, a^n = b^2, b^{-1}ab = a^{-1} \rangle \tag{12.8}$$

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. ♣

$$\mathbb{Z}_{12}, \quad ,\mathbb{Z}_2 \times \mathbb{Z}_6, \quad ,D_6, \quad ,\tilde{D}_3 \tag{12.9}$$

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. [67]

[67] See, however, M. Wild, "Groups of order 16 made easy," American Mathematical Monthly, Jan 2005

Order	Presentation	name
1	$\langle a \mid a = 1\rangle$	Trivial group
2	$\langle a \mid a^2 = 1\rangle$	Cyclic $\mathbb{Z}/2\mathbb{Z}$
3	$\langle a \mid a^3 = 1\rangle$	Cyclic $\mathbb{Z}/3\mathbb{Z}$
4	$\langle a \mid a^4 = 1\rangle$	Cyclic $\mathbb{Z}/4\mathbb{Z}$
4	$\langle a, b \mid a^2 = b^2 = (ab)^2 = 1\rangle$	Dihedral $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, Klein
5	$\langle a \mid a^5 = 1\rangle$	Cyclic $\mathbb{Z}/5\mathbb{Z}$
6	$\langle a, b \mid a^3 = 1, b^2 = 1, bab = a\rangle$	Cyclic $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
6	$\langle a, b \mid a^3 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral $D_3 \cong S_3$
7	$\langle a \mid a^7 = 1\rangle$	Cyclic $\mathbb{Z}/7\mathbb{Z}$
8	$\langle a \mid a^8 = 1\rangle$	Cyclic $\mathbb{Z}/8\mathbb{Z}$
8	$\langle a, b \mid a^2 = 1, b^4 = 1, aba = b\rangle$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
8	$\langle a, b, c \mid a^2 = b^2 = c^2 = 1, [a, b] = [a, c] = [b, c] = 1\rangle$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
8	$\langle a, b \mid a^4 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_4
8	$\langle a, b \mid a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1}\rangle$	Dicyclic $\widetilde{D_2} \cong Q$, quaternion
9	$\langle a \mid a^9 = 1\rangle$	Cyclic $\mathbb{Z}/9\mathbb{Z}$
9	$\langle a, b \mid a^3 = b^3 = 1, [a, b] = 1\rangle$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	$\langle a \mid a^{10} = 1\rangle$	Cyclic $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
10	$\langle a \mid a^5 = b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_5
11	$\langle a \mid a^{11} = 1\rangle$	Cyclic $\mathbb{Z}/11\mathbb{Z}$
12	$\langle a \mid a^{12} = 1\rangle$	Cyclic $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
12	$\langle a, b \mid a^2 = 1, b^6 = 1, [a, b] = 1\rangle$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
12	$\langle a, b \mid a^6 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_6
12	$\langle a, b \mid a^6 = 1, a^3 = b^2, b^{-1}ab = a^{-1}\rangle$	Dicyclic $\widetilde{D_3}$
12	$\langle a, b \mid a^3 = 1, b^2 = 1, (ab)^3 = 1\rangle$	Alternating A_4
13	$\langle a \mid a^{13} = 1\rangle$	Cyclic $\mathbb{Z}/13\mathbb{Z}$
14	$\langle a \mid a^{14} = 1\rangle$	Cyclic $\mathbb{Z}/14\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$
14	$\langle a, b \mid a^7 = 1, b^2 = 1, bab = a^{-1}\rangle$	Dihedral D_7
15	$\langle a \mid a^{15} = 1\rangle$	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.)

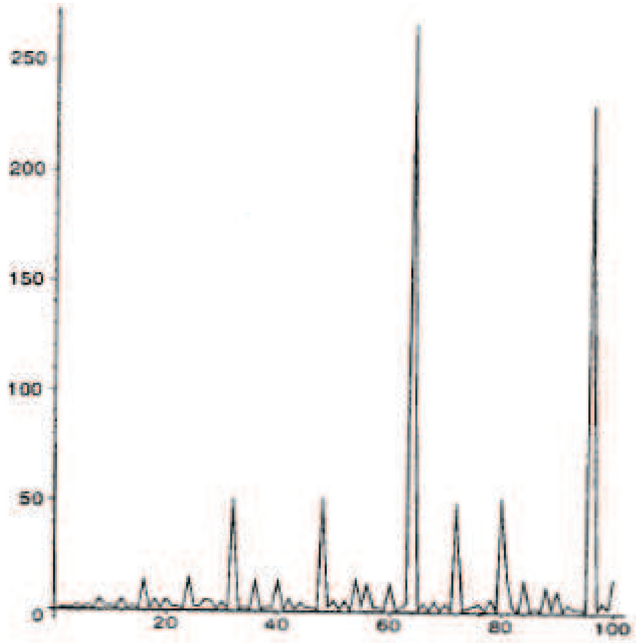

Figure 16: A plot of the number of nonisomorphic groups of order n. This plot was taken from the book by D. Joyner, *Adventures in Group Theory*.

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 16 from Joyner's book shows a plot of the number of isomorphism classes vs. order up to order 100. Figure 17 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

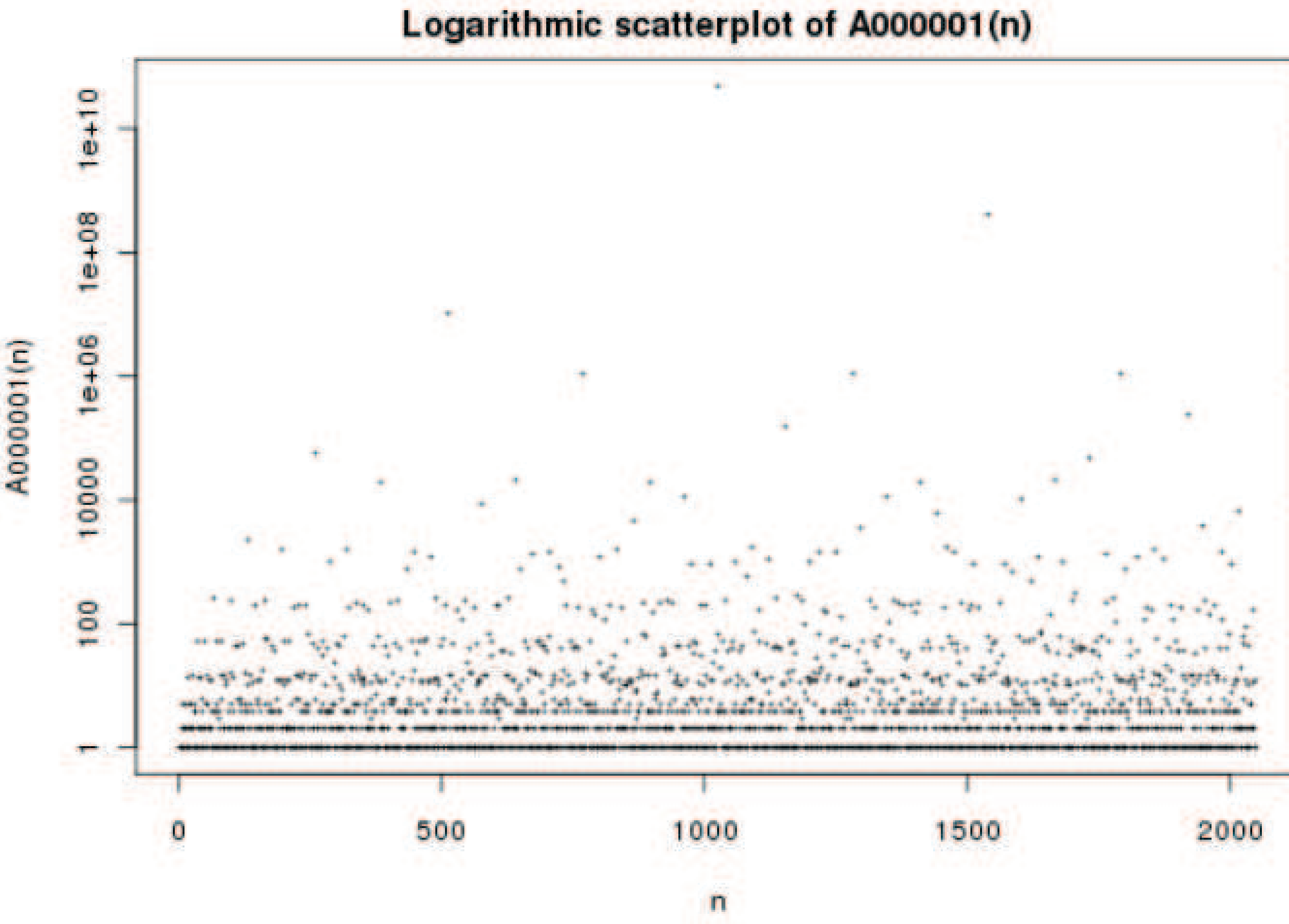

Figure 17: A logarithmic plot of the number of nonisomorphic groups of order n out to $n \leq 2000$. This plot was taken from online encyclopedia of integer sequences, OEIS.

talking about the number of all groups.) This is due to G. Higman [68] and C. Sims [69] and the result states that:

$$f(n,p) \sim p^{\frac{2}{27}n^3} \tag{12.10}$$

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*

[68] G. Higman, "Enumerating p-Groups," Proc. London Math. Soc. 3) 10 (1960)

[69] 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:

$$\begin{tikzcd}
& \mathbb{Z}_2 \arrow[r, equal] \arrow[d] & \mathbb{Z}_2 \arrow[d] & & \\
1 \arrow[r] & \mathbb{Z}_{2n} \arrow[r] \arrow[d, equal] & \widetilde{D}_n \arrow[r] \arrow[d] & \mathbb{Z}_2 \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathbb{Z}_n \arrow[r] & D_n \arrow[r] & \mathbb{Z}_2 \arrow[r] & 1
\end{tikzcd} \tag{12.11}$$

12.2 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

$$0 \to \mathbb{Z}/gcd(p,q)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/lcm(p,q)\mathbb{Z} \to 0 \tag{12.12}$$

and in particular, if p, q are relatively prime then

$$\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}. \tag{12.13}$$

It thus follows that if n has prime decomposition

$$n = \prod_i p_i^{e_i} \tag{12.14}$$

then

$$\mathbb{Z}/n\mathbb{Z} \cong \oplus_i \mathbb{Z}/p_i^{e_i}\mathbb{Z} \tag{12.15}$$

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:

$$\begin{aligned} G &= G_2 \oplus G_3 \oplus G_5 \oplus G_7 \oplus \cdots \\ &= \oplus_{p \text{ prime}} G_p \end{aligned} \tag{12.16}$$

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:

$$G_p = \oplus_i \mathbb{Z}/(p^{n_i}\mathbb{Z}) \tag{12.17}$$

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

$$s_1 m_1 + s_2 m_2 = 1 \tag{12.18}$$

Therefore any element g can be written as

$$g = s_1(m_1 g) + s_2(m_2 g) \tag{12.19}$$

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 (12.19) implies $a = 0$. Thus,

$$G = m_1 G \oplus m_2 G \tag{12.20}$$

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 (12.19) we see that $g = s_1 m_1 g = m_1(s_1 g) \in m_1 G$.

Thus, we can decompose

$$G = \oplus p \text{ prime} G_p \tag{12.21}$$

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 (12.17). 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 6.5.

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:

$$H = \{g | pg = 0\} \tag{12.22}$$

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 $|g| \leq |M|$ 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 $\mathbb{R}^d$.

$$L := \{\sum_{i=1}^{d} n_i v_i | n_i \in \mathbb{Z}\} \tag{12.23}$$

is a subgroup. Then

$$A = \mathbb{Z}^d / L \tag{12.24}$$

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

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k} \tag{12.25}$$

where

$$n_1 | n_2 \quad \& \quad n_2 | n_3 \quad \& \quad \cdots \quad \& \quad n_{k-1} | n_k \tag{12.26}$$

Write the n_i in terms of the prime powers in (12.17).

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.

12.3 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*:

$$\text{Tors}(G) := \{ g \in G | \exists n \in \mathbb{Z} \qquad ng = 0 \} \tag{12.27}$$

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

$$0 \to \mathrm{Tors}(G) \to A \to \mathbb{Z}^r \to 0 \tag{12.28}$$

where $\mathrm{Tors}(G)$ is a *finite abelian group*.

For a proof, see, e.g., S. Lang, *Algebra* .

Moreover (12.28) is a split extension, that is, it is isomorphic to

$$\mathbb{Z}^r \oplus \mathrm{Tors}(G) \tag{12.29}$$

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 (12.29) of a finitely generated abelian group is <u>not canonical</u>! There are many distinct splittings of (12.28). 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.

Exercise

Consider the finitely generated Abelian group [70]

$$L = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 | \sum_i x_i = 0 \mathrm{mod} 2\} \tag{12.30}$$

[70] It is the root lattice of $\mathfrak{so}(8)$.

and consider the subgroup S generated by

$$\begin{aligned} v_1 &= (1,1,1,1) \\ v_2 &= (1,1,-1,-1) \end{aligned} \tag{12.31}$$

a.) What is the torsion group of L/S ?

b.) Find a splitting of the sequence (12.28) 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 (12.28).

12.4 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

$$1 = G_{s+1} \triangleleft G_s \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 = G \tag{12.32}$$

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.... ♣

$$1 = G_4 \triangleleft G_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \triangleleft G_2 = A_4 \triangleleft G_1 = S_4 \tag{12.33}$$

but

$$G_3 = 1 \triangleleft G_2 = A_n \triangleleft G_1 = S_n \qquad\qquad n \geq 5 \tag{12.34}$$

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 finite group admits a composition series.

♣Give a reference. ♣

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:

$$1 = G_{s+1} \triangleleft G_s \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 = G \qquad (12.35)$$

$$1 = G'_{s'+1} \triangleleft G'_s \triangleleft \cdots \triangleleft G'_2 \triangleleft G'_1 = G \qquad (12.36)$$

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:

$$1 \to G_{i+1} \to G_i \to S_i \to 1 \qquad (12.37)$$

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

$$((12)(34)) \cdot ((13)(24)) = ((13)(24)) \cdot ((12)(34)) = (14)(23) \qquad (12.38)$$

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

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix} \tag{12.39}$$

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:

$$\sigma' = (345)\sigma(345)^{-1} = (345)(123\cdots)\pi(354) \tag{12.40}$$

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 $N \triangleleft A_{n+1}$. 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

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{12.41}$$

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: [71]

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? ♣

It turns out that there are exactly 26 oddballs, known as the "sporadic groups." Some relationships between them are illustrated in Figure 18. The sporadic groups first showed up in the 19^{th} century via the Mathieu groups

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}. \tag{12.42}$$

[71] See the *Atlas of Finite Simple Groups*, by Conway and Norton

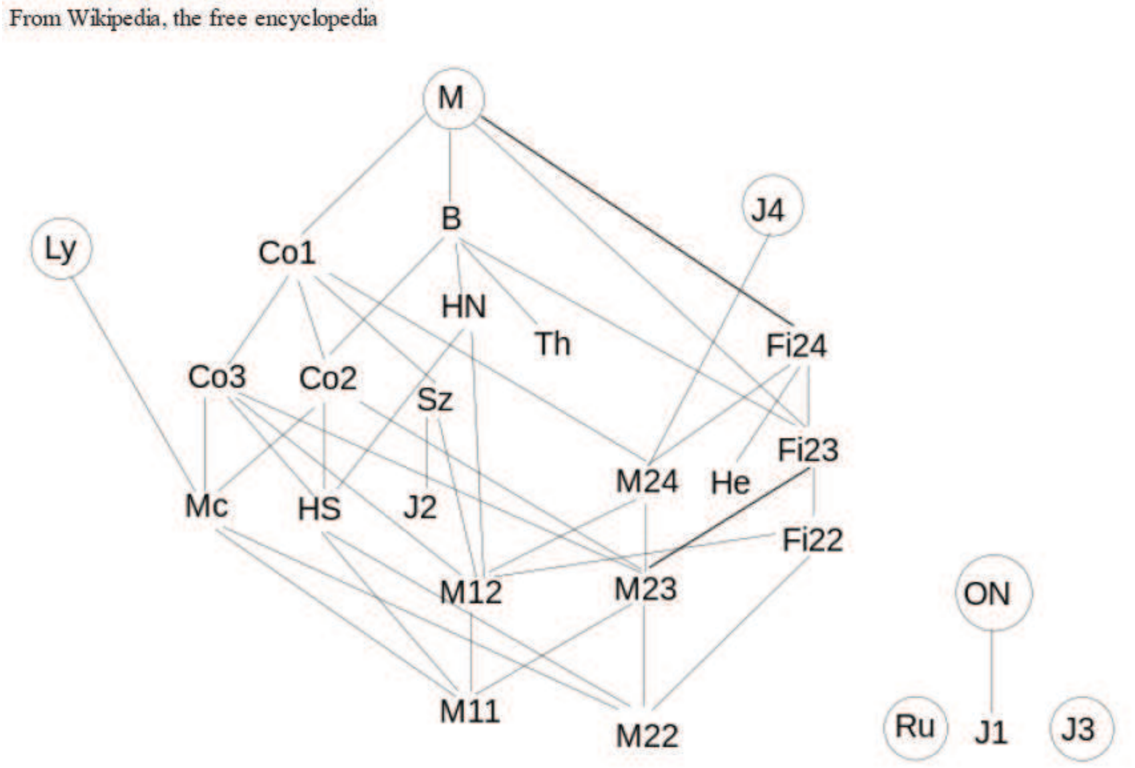

Figure 18: A table of the sporadic groups including subgroup relations. Source: Wikipedia.

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:

$$\begin{aligned} |Monster| &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &= 808017424794512875886459904961710757005754368000000000 \qquad (12.43) \\ &\cong 8.08 \times 10^{53} \end{aligned}$$

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: [72]

[72] Our source here is the Wikipedia article on the classification of finite simple groups. See also: Solomon,

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.

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]

Ronald, "A brief history of the classification of the Finite simple groups," American Mathematical Society. Bulletin. New Series, 38 (3): 315-352 (2001).

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):

$$[(abe), (ab)(cd)] = (aeb) \tag{12.44}$$

$$[(abc), (abcde)] = (abd) \tag{12.45}$$

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 $p(p^2 - 1)$. [73]

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.

[73] 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 $bc = -1$.

13. 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 $\hom(X,Y)$, defined for any two objects $X, Y \in Ob(\mathcal{C})$. The elements of $\hom(X,Y)$ are called the "morphisms from X to Y." They are often denoted as arrows:

$$X \overset{\phi}{\to} Y \tag{13.1}$$

c.) A composition law:

$$\hom(X,Y) \times \hom(Y,Z) \to \hom(X,Z) \tag{13.2}$$

$$(\psi_1, \psi_2) \mapsto \psi_2 \circ \psi_1 \tag{13.3}$$

Such that

1. A morphism ϕ uniquely determines its source X and target Y. That is, $\hom(X,Y)$ are disjoint for distinct ordered pairs (X,Y).

2. $\forall X \in Ob(\mathcal{C})$ there is a distinguished morphism, denoted $1_X \in \hom(X,X)$ or $\mathrm{Id}_X \in \hom(X,X)$, which satisfies:

$$1_X \circ \phi = \phi \qquad \psi \circ 1_X = \psi \tag{13.4}$$

for all morphisms $\phi \in \hom(Y,X)$ and $\psi \in \hom(X,Y)$ for all $Y \in Ob(\mathcal{C})$. [74]

3. Composition of morphisms is associative:

$$(\psi_1 \circ \psi_2) \circ \psi_3 = \psi_1 \circ (\psi_2 \circ \psi_3) \tag{13.5}$$

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

[74] As an exercise, show that these conditions uniquely determine the morphism 1_X.

this alternative definition a category is then defined by a composition law on the set of *composable morphisms*

$$\mathcal{C}_2 = \{(f,g) \in \mathcal{C}_1 \times \mathcal{C}_1 | p_0(f) = p_1(g)\} \tag{13.6}$$

which is sometimes denoted $\mathcal{C}_{1 p_1} \times_{p_0} \mathcal{C}_1$ 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. [75]

2. **TOP**: The category of topological spaces and continuous maps.

3. **TOPH**: The category of topological spaces and homotopy classes of continuous maps.

[75] We take an appropriate collection of sets and maps to avoid the annoying paradoxes of set theory.

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

$$x \xrightarrow{f} y \ \in \hom(x,y) \tag{13.7}$$

then

$$F_{\rm obj}(x) \xrightarrow{F_{\rm mor}(f)} F_{\rm obj}(y) \ \in \hom(F_{\rm obj}(x), F_{\rm obj}(y)) \tag{13.8}$$

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

$$F_{\rm mor}(f_1 \circ f_2) = F_{\rm mor}(f_1) \circ F_{\rm mor}(f_2) \tag{13.9}$$

and we say that F is a *contravariant functor* if

$$F_{\rm mor}(f_1 \circ f_2) = F_{\rm mor}(f_2) \circ F_{\rm mor}(f_1) \tag{13.10}$$

In both cases we also require [76]

$$F_{\text{mor}}(\mathrm{Id}_X) = \mathrm{Id}_{F(X)} \tag{13.11}$$

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* $\mathcal{C}^{\text{opp}}$ is defined by just reversing all arrows. More formally: The set of objects is the same and

$$\hom_{\mathcal{C}^{\text{opp}}}(X, Y) := \hom_{\mathcal{C}}(Y, X) \tag{13.12}$$

so for every morphism $f \in \hom_{\mathcal{C}}(Y, X)$ we associate $f^{\text{opp}} \in \hom_{\mathcal{C}^{\text{opp}}}(X, Y)$ such that

$$f_1 \circ_{\mathcal{C}^{\text{opp}}} f_2 = (f_2 \circ_{\mathcal{C}} f_1)^{\text{opp}} \tag{13.13}$$

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 $F : \mathcal{C}^{\text{opp}} \to \mathcal{D}$.

b.) Show that if $F : \mathcal{C} \to \mathcal{D}$ is a covariant functor then we can naturally define another covariant functor $F^{\text{opp}} : \mathcal{C}^{\text{opp}} \to \mathcal{D}^{\text{opp}}$

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.

Example 3: Since **AB** is a subcategory of **GROUP** there is an obvious functor $\mathcal{F}$: **AB** $\to$ **GROUP**.

Example 4: In an exercise below you are asked to show that the abelianization of a group defines a functor $\mathcal{G}$: **GROUP** $\to$ **AB**.

[76] Although we do have $F_{\text{mor}}(\mathrm{Id}_X) \circ F_{\text{mor}}(f) = F_{\text{mor}}(f)$ for all $f \in \hom(Y, X)$ and $F_{\text{mor}}(f) \circ F_{\text{mor}}(\mathrm{Id}_X) = F_{\text{mor}}(f)$ for all $f \in \hom(X, Y)$ this is not the same as the statement that $F_{\text{mor}}(\mathrm{Id}_X) \circ \phi = \phi$ for all $\phi \in \hom(F(Y), F(X))$, so we need to impose this extra axiom.

Example 5: Fix a group G. Then in the notes above we have on several occasions used the functor

$$F_G : \mathbf{SET} \to \mathbf{GROUP} \tag{13.14}$$

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

$$F_G(X_1) \xleftarrow{F_G(f)} F_G(X_2) \tag{13.15}$$

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

$$F_{G,Y} : \mathbf{G\text{-}SET} \to \mathbf{G\text{-}SET} \tag{13.16}$$

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:

$$\begin{aligned} [g \cdot (f^*\Psi)](x_1) &= (f^*\Psi)(g^{-1} \cdot x_1) \\ &= \Psi(f(g^{-1} \cdot x_1)) \\ &= \Psi(g^{-1} \cdot (f(x_1))) \\ &= (g \cdot \Psi)(f(x_1)) \\ &= (f^*(g \cdot \Psi))(x_1) \end{aligned} \tag{13.17}$$

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

$$H^n(G, \bullet) : \mathbf{AB} \to \mathbf{AB} \tag{13.18}$$

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

$$\varphi_* : H^n(G, A_1) \to H^n(G, A_2) \tag{13.19}$$

You have to check that $\mathrm{Id}_* = \mathrm{Id}$ and

$$(\varphi_1 \circ \varphi_2)_* = (\varphi_1)_* \circ (\varphi_2)_* \tag{13.20}$$

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

$$H^n(\bullet, A) : \mathbf{GROUP} \to \mathbf{AB} \tag{13.21}$$

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^*

$$\varphi^* : H^n(G_2, A) \to H^n(G_1, A) \tag{13.22}$$

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 $f \in \hom(X,Y)$,

$$\tau_Y \circ F_1(f) = F_2(f) \circ \tau_X \tag{13.23}$$

Or, in terms of diagrams.

$$\begin{tikzcd}
F_1(X) \arrow[r, "F_1(f)"] \arrow[d, "\tau_X"] & F_1(Y) \arrow[d, "\tau_Y"] \\
F_2(X) \arrow[r, "F_2(f)"] & F_2(Y)
\end{tikzcd} \tag{13.24}$$

Example 1: *The evaluation map.* Here is another tautological construction which nevertheless can be useful. Let S be any set and define a functor

$$F_S : \mathbf{SET} \to \mathbf{SET} \tag{13.25}$$

by saying that on objects we have

$$F_S(X) := Map[S \to X] \times S \tag{13.26}$$

and if $\varphi : X_1 \to X_2$ is a map of sets then

$$F_S(\varphi) : Map[S \to X_1] \times S \to Map[S \to X_2] \times S \tag{13.27}$$

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

$$\tau_X : F_S(X) = Map[S \to X] \times S \to \mathrm{Id}(X) = X \tag{13.28}$$

It is defined by $\tau_X(f, s) := f(s)$. This is known as the "evaluation map." Then we need to check

$$\begin{tikzcd} F_S(X) \arrow[r, "\tau_X"] \arrow[d, "F_S(\varphi)"] & X \arrow[d, "\varphi"] \\ F_S(Y) \arrow[r, "\tau_Y"] & Y \end{tikzcd} \tag{13.29}$$

commutes. If you work it out, it is just a tautology.

Example 2: *The determinant.* [77] 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

$$\mathbf{COMMRING} \to \mathbf{GROUP} \tag{13.30}$$

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

$$\varphi_* : r \mapsto \varphi(r) \tag{13.31}$$

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

$$\det(g) := \sum_{\sigma \in S_n} \epsilon(\sigma) g_{1,\sigma(1)} \cdot g_{2,\sigma(2)} \cdots g_{n,\sigma(n)} \tag{13.32}$$

makes perfect sense for $g \in GL(n, R)$. Moreover,

$$\det(g_1 g_2) = \det(g_1)\det(g_2) \tag{13.33}$$

[77] This example uses some terms from linear algebra which can be found in the "User's Manual," Chapter 2 below.

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

$$\tau_R : GL(n, R) \to U(R) \tag{13.34}$$

defined by $\tau_R(g) := \det(g)$. Thanks to (13.33) 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

$$\varphi_*(\det(g)) = \det(\varphi_*(g)). \tag{13.35}$$

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 $\mathrm{FUNCT}(\mathcal{C}_2, \mathcal{C}_2)$ so it makes sense to say that they are isomorphic.)

♣Should explain example showing category of finite-dimensional vector spaces over a field is equivalent to the catetgory of nonnegative integers. ♣

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: [78]

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_1G 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 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.

[78] I thank G. Segal for a nice discussion that helped prepare this list.

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

$$F_{\rm mor} : \hom(X, Y) \to \hom(F_{\rm obj}(X), F_{\rm obj}(Y)) \tag{13.36}$$

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 19.

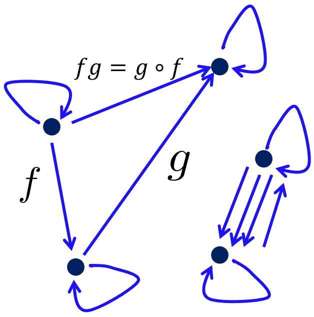

Figure 19: Pictorial illustration of a category. The objects are the black dots. The arrows are shown, and one must give a rule for composing each arrow and identifying with one of the other arrows. For example, given the arrows denoted f and g it follows that there must be an arrow of the type denoted $f \circ g$. 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.

13.1 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

$$\Phi : X \times G \to X \tag{13.37}$$

such that

$$\Phi(\Phi(x, g_1), g_2) = \Phi(x, g_1 g_2) \tag{13.38}$$

$$\Phi(x, 1_G) = x \tag{13.39}$$

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

$$\begin{aligned} Ob(X//G) &= X \\ Mor(X//G) &= X \times G \end{aligned} \tag{13.40}$$

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! ♣

$$p_0((x, g)) := x \cdot g \qquad\qquad p_1((x, g)) := x \tag{13.41}$$

The composition of morphisms is defined by

$$(xg_1, g_2) \circ (x, g_1) := (x, g_1g_2) \tag{13.42}$$

or, in the other notation (better suited to a right-action):

$$(x, g_1)(xg_1, g_2) := (x, g_1g_2) \tag{13.43}$$

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

$$g_1 \xrightarrow{h} g_2 \tag{13.44}$$

iff $g_2 = h^{-1}g_1h$. This is the groupoid of principal G-bundles on the circle.

Draw the groupoid corresponding to S_3.

13.2 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 [79] whose simplices are:

[79] Technically, it is a *simplicial space.*

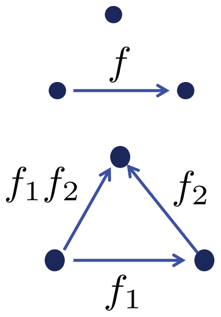

Figure 20: Elementary $0, 1, 2$ simplices in the simplicial space $|\mathcal{C}|$ of a category

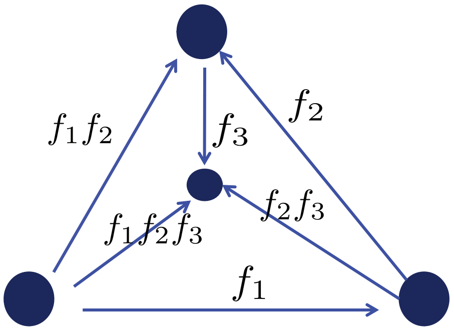

Figure 21: An elementary 3-simplex in the simplicial space $|\mathcal{C}|$ of a category

- 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

$$(f_1, f_2) \in X_2 := \{(f_1, f_2) \in X_1 \times X_1 | p_0(f_1) = p_1(f_2)\} \tag{13.45}$$

- 3-simplices: $\Delta(f_1, f_2, f_3)$ associated to 3 composable morphisms, i.e. elements of:

$$X_3 = \{(f_1, f_2, f_3) \in X_1 \times X_1 \times X_1 | p_0(f_i) = p_1(f_{i+1}), i = 1, 2\} \tag{13.46}$$

- 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 20 and 21. The figures make clear how these simplices are glued together:

$$\partial \Delta_1(f) = x_1 - x_0 \tag{13.47}$$

$$\partial\Delta_2(f_1,f_2) = \Delta_1(f_1) - \Delta_1(f_1f_2) + \Delta_1(f_2) \tag{13.48}$$

and for Figure 21 view this as looking down on a tetrahedron. Give the 2-simplices of Figure 20 the counterclockwise orientation and the boundary of the 3-simplex the induced orientation from the outwards normal. Then we have

$$\partial\Delta(f_1,f_2,f_3) = \Delta(f_2,f_3) - \Delta(f_1f_2,f_3) + \Delta(f_1,f_2f_3) - \Delta(f_1,f_2) \tag{13.49}$$

Note that on the three upper faces of Figure 21 the induced orientation is the ccw orientation for $\Delta(f_1,f_2f_3)$ and $\Delta(f_2,f_3)$, but with the cw orientation for $\Delta(f_1f_2,f_3)$. 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:

$$\partial\Delta(g) = 0 \tag{13.50}$$

$$\partial\Delta(g_1,g_2) = \Delta_1(g_1) + \Delta_1(g_2) - \Delta_1(g_1g_2) \tag{13.51}$$

$$\partial\Delta(g_1,g_2,g_3) = \Delta(g_2,g_3) - \Delta(g_1g_2,g_3) + \Delta(g_1,g_2g_3) - \Delta(g_1,g_2) \tag{13.52}$$

See Figure 21.

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

$$\begin{aligned}
d^0(g_1,\dots,g_n) &= (g_2,\dots,g_n)\\
d^1(g_1,\dots,g_n) &= (g_1g_2,g_3,\dots,g_n)\\
d^2(g_1,\dots,g_n) &= (g_1,g_2g_3,g_4,\dots,g_n)\\
&\cdots\cdots\\
&\cdots\cdots\\
d^{n-1}(g_1,\dots,g_n) &= (g_1,\dots,g_{n-1}g_n)\\
d^n(g_1,\dots,g_n) &= (g_1,\dots,g_{n-1})
\end{aligned} \tag{13.53}$$

On the other hand, we can view an n-simplex Δ_n as

$$\Delta_n := \{(t_0,t_1,\dots,t_n)|t_i \geq 0 \qquad \& \qquad \sum_{i=0}^n t_i = 1\} \tag{13.54}$$

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:

$$\begin{aligned} d_0(t_0,\dots,t_{n-1}) &= (0,t_0,\dots,t_{n-1}) \\ d_1(t_0,\dots,t_{n-1}) &= (t_0,0,t_1,\dots,t_{n-1}) \\ &\cdots\cdots \\ &\cdots\cdots \\ d_n(t_0,\dots,t_{n-1}) &= (t_0,\dots,t_{n-1},0) \end{aligned} \tag{13.55}$$

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 [80]

$$(\amalg_{n=0}^{\infty} \Delta_n \times G^n) \, / \sim$$

via

$$(d_i(\vec{t}), \vec{g}) \sim (\vec{t}, d^i(\vec{g})). \tag{13.56}$$

The space we have constructed this way has a homotopy type denoted BG.

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

$$\Delta_1(1_G) = \partial(\Delta_2(1_G, 1_G)) \tag{13.57}$$

so $\Delta_1(1_G)$ is a contractible loop. But all other loops are noncontractible. (Show this!) Therefore:

$$\pi_1(BG, *) \cong G \tag{13.58}$$

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

$$\langle d\phi_n, \Delta \rangle = \langle \phi_n, \partial\Delta \rangle \tag{13.59}$$

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? ♣

[80] 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.

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

$$H^{n+1}_{\text{group cohomology}}(G;\mathbb{Z}) \to H^n_{\text{topological space cohomology}}(G;\mathbb{Z}) \tag{13.60}$$

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. [81]

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 $B\mathbb{Z}$ 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: $\psi \to e^{\mathrm{i}\theta}\psi$.

14. 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:

$$s : \mathcal{E} \to \mathcal{V} \qquad\qquad t : \mathcal{E} \to \mathcal{V} \tag{14.1}$$

We will view the union of edges $\bar{\mathcal{E}}$ (i.e. forgetting the orientation) as a topological space and denote it as Γ.

[81] I thank G. Segal for helpful remarks on this issue.

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.

14.1 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

$$\phi : \mathbb{R}^d \to \mathcal{T} \tag{14.2}$$

where $\mathcal{T}$ is some "target space." Then if we consider the embedded hypercubic lattice:

$$\Lambda_a := \{a(n_1, \dots, n_d) \in \mathbb{R}^d | n_i \in \mathbb{Z}\} \tag{14.3}$$

and we restrict ϕ to Λ_a then at neighboring vertices the value of ϕ will converge as $a \to 0$:

$$\lim_{a\to 0} \phi(\vec{x}_0 + a\hat{e}_\mu) = \phi(\vec{x}_0) \tag{14.4}$$

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

$$\lim_{a\to 0} a^{-1}(\phi(\vec{x}_0 + a\hat{e}_\mu) - \phi(\vec{x}_0)) = \partial_\mu \phi(\vec{x}_0) \tag{14.5}$$

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: [82] 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:

$$S = \int_{\mathbb{R}} dt \sum_{n\in\mathbb{Z}} \left(\frac{m}{2}\dot{\phi}_\ell(n,t)^2 - \frac{k}{2}\left(\phi_\ell(n,t) - \phi_\ell(n+1,t)\right)^2 \right) \tag{14.6}$$

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:

$$m\frac{d^2}{dt^2}\phi_\ell(n,t) = k(\phi_\ell(n+1,t) - 2\phi_\ell(n,t) + \phi_\ell(n-1,t)) \tag{14.7}$$

[82] Here we will just latticize the <u>spatial</u> dimension of a $1 + 1$ dimensional field theory. In the rest of the section we latticize spacetime with Euclidean signature.

Now we wish to take the $a \to 0$ limit. We assume that there is some differentiable function $\phi_{cont}(x,t)$ such that

$$\phi_{cont}(x,t)|_{x=an} = \phi_\ell(n,t) \tag{14.8}$$

so by Taylor expansion

$$\phi_\ell(n+1,t) - 2\phi_\ell(n,t) + \phi_\ell(n-1,t) = a^2 \frac{d^2}{dx^2}\phi_{cont}|_{x=an} + \mathcal{O}(a^3) \tag{14.9}$$

Now suppose we scale the parameters of the Lagrangian so that

$$m = aT \qquad k = \frac{v^2 T}{a} \tag{14.10}$$

then, if the limits really exist, the continuum function $\phi_{cont}(x,t)$ must satisfy the wave equation:

$$\frac{d^2}{dt^2}\phi_{cont} - v^2 \frac{d^2}{dx^2}\phi_{cont} = 0 \tag{14.11}$$

whose general solution is

$$\Phi_{left}(x+vt) + \Phi_{right}(x-vt) \tag{14.12}$$

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

$$S \to T \int_{\mathbb{R}} dt \int_{\mathbb{R}} dx \left[\frac{1}{2}\left(\frac{d}{dt}\phi_{cont}\right)^2 - \frac{v^2}{2}\left(\frac{d}{dx}\phi_{cont}\right)^2 \right] + \mathcal{O}(a) \tag{14.13}$$

Remarks

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.

14.2 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 $e_1, e_2, \ldots, e_k$ such that

$$t(e_i) = s(e_{i+1}) \qquad 1 \le i \le k-1 \tag{14.14}$$

(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

$$\mathbb{U} : \mathcal{P} \to G, \tag{14.15}$$

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:

$$\mathbb{U}(\gamma_1 \circ \gamma_2) = \mathbb{U}(\gamma_1)\mathbb{U}(\gamma_2) \tag{14.16}$$

If our path is the trivial path then

$$\mathbb{U}(\gamma_v) = 1_G \tag{14.17}$$

and if $\gamma^{-1}(t) = \gamma(1-t)$ is the path run backwards then

$$\mathbb{U}(\gamma^{-1}) = (\mathbb{U}(\gamma))^{-1} \tag{14.18}$$

♣Are these really independent conditions? ♣

Note that if the path γ is made by concatenating edges $e_1, e_2, \ldots, e_k$ then

$$\mathbb{U}(\gamma) = \mathbb{U}(e_1)\mathbb{U}(e_2)\cdots\mathbb{U}(e_k) \tag{14.19}$$

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

$$\mathbb{U}(e^{-1}) = \mathbb{U}(e)^{-1} \tag{14.20}$$

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

$$e^A e^B = e^C \tag{14.21}$$

The formula is a (very explicit) infinite set of terms all expressed in terms of multiple commutators. The first few terms are:

$$\boxed{C = A + B + \frac{1}{2}[A,B] + \frac{1}{12}[A,[A,B]] + \frac{1}{12}[B,[B,A]] + \frac{1}{24}[A,[B,[A,B]]] + \cdots} \tag{14.22}$$

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

$$e^{\epsilon_1 A} e^{\epsilon_2 B} e^{-\epsilon_1 A} e^{-\epsilon_2 B} = e^{\epsilon_1 \epsilon_2 [A,B] + \cdots} \tag{14.23}$$

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:

$$\mathbb{U}(e_\mu(\vec{n})) = \exp[a A_\mu^{lattice}(\vec{n})] \tag{14.24}$$

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

$$f : \mathcal{V} \to G \tag{14.25}$$

The idea is that if γ is a path then the gauge fields $\mathbb{U}$ and $\mathbb{U}'$ related by the rule

$$\mathbb{U}'(\gamma) = f(s(\gamma))\mathbb{U}(\gamma)f(t(\gamma))^{-1} \tag{14.26}$$

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.* [83] The group of

[83] AND IS NOT TO BE CONFUSED WITH THE gauge group G!!!!

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, <u>except</u> 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:

$$\mathbb{U}'(\gamma) = g\mathbb{U}(\gamma)g^{-1} \tag{14.27}$$

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*:

$$\mathrm{Hol}_{\mathbb{U}} : L\Gamma \to \mathrm{Conj}(G) \tag{14.28}$$

that maps the loops in Γ to the conjugacy class:

$$\mathrm{Hol}_{\mathbb{U}} : \gamma \mapsto C(\mathbb{U}(\gamma)) \tag{14.29}$$

is gauge invariant: If $\mathbb{U}' \sim \mathbb{U}$ are gauge equivalent then

$$\mathrm{Hol}_{\mathbb{U}'} = \mathrm{Hol}_{\mathbb{U}} \tag{14.30}$$

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

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 $\mathbb{U}(e) = 1$?

14.3 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":

$$Z = \sum_{[\mathbb{U}] \in \mathcal{A}(\Gamma)/\mathcal{G}(\Gamma)} F([\mathbb{U}]) \tag{14.31}$$

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

$$\mathcal{A}(\Gamma) \cong G^{|\bar{\mathcal{E}}|}. \tag{14.32}$$

Similarly

$$\mathcal{G}(\Gamma) \cong G^{|\mathcal{V}|} \tag{14.33}$$

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

$$\int_G F d\mu := \frac{1}{|G|} \sum_{g \in G} F(g) \tag{14.34}$$

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 $U(1) = \{e^{\mathrm{i}\theta}\}$ then the integration is

$$\int_0^{2\pi} F(e^{\mathrm{i}\theta}) \frac{d\theta}{2\pi} \tag{14.35}$$

In all cases, the crucial property of the group integration is that, for all h we have

$$\int_G F(gh) d\mu(g) = \int_G F(hg) d\mu(g) = \int_G F(g) d\mu(g) \tag{14.36}$$

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:

$$Z = \frac{1}{\mathrm{vol}\,(\mathcal{G}(\Gamma))} \int_{\mathcal{A}(\Gamma)} \hat{F}(\mathbb{U}) d\mu_{\mathcal{A}(\Gamma)} \tag{14.37}$$

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

$$a\vec{n} \to a\vec{n} + a\hat{e}_\mu \to a\vec{n} + a\hat{e}_\mu + a\hat{e}_\nu \to a\vec{n} + a\hat{e}_\nu \to a\vec{n} \tag{14.38}$$

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

$$\hat{F}(\mathbb{U}) := e^{-S(\mathbb{U})} := e^{-\sum_p S(p)} \tag{14.39}$$

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.

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

$$\mathbb{U}(e_\mu(\vec{n})) \sim \exp[aA_\mu^{cont}|_{\vec{x}=a\vec{n}}] \tag{14.40}$$

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

$$e^{aA_1(x,y-\frac{1}{2}a)} e^{aA_2(x+\frac{1}{2}a,y)} e^{-aA_1(x,y+\frac{1}{2}a)} e^{-aA_2(x-\frac{1}{2}a,y)} \tag{14.41}$$

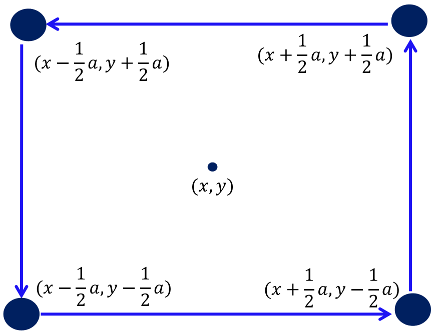
$(x-\frac{1}{2}a, y+\frac{1}{2}a)$
$(x+\frac{1}{2}a, y+\frac{1}{2}a)$
(x, y)
$(x-\frac{1}{2}a, y-\frac{1}{2}a)$
$(x+\frac{1}{2}a, y-\frac{1}{2}a)$

Figure 22: 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.

See Figure 22. Now, using the BCH formula [84] we define the *fieldstrength of the gauge field* or, equivalently, the *curvature of the connection* by

$$\mathbb{U}(p_{\mu\nu}(\vec{n})) = \exp[a^2 F_{\mu\nu} + \mathcal{O}(a^4)] \tag{14.44}$$

Here in the continuum we would have the relation:

$$F_{\mu\nu}(\vec{x}) = \partial_\mu A_\nu(\vec{x}) - \partial_\nu A_\mu(\vec{x}) + [A_\mu(\vec{x}), A_\nu(\vec{x})] \tag{14.45}$$

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

$$\rho : G \to U(r) \tag{14.46}$$

Next, define the action for a plaquette to be

$$S(p) = K(r - \mathrm{Re}[\mathrm{Tr}\rho(\mathbb{U}(p))]) \tag{14.47}$$

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 $e^{\mathrm{i}\theta_i(p)}$,

[84] Warning: If you are not careful the algebra can be extremely cumbersome here! Taylor expansion in to order a^2 gives:

$$e^{aA_1 - \frac{a^2}{2}\partial_2 A_1} e^{aA_2 + \frac{a^2}{2}\partial_1 A_2} e^{-aA_1 - \frac{a^2}{2}\partial_2 A_1} e^{-aA_2 + \frac{a^2}{2}\partial_1 A_2} \tag{14.42}$$

We only need to keep the first commutator term in the BCH formula if we are working to order a^2 so we get

$$e^{a^2(\partial_1 A_2 - \partial_2 A_1 + [A_1, A_2]) + \mathcal{O}(a^3)} \tag{14.43}$$

$i = 1, \dots, r$ and then

$$S(p) = K \sum_{i=1}^{r} (1 - \cos\theta_i(p)) = 2K \sum_{i=1} \sin^2(\theta_i(p)/2) \tag{14.48}$$

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:

$$W(R, \gamma)(\mathbb{U}) := \mathrm{Tr}_{\mathbb{C}^N} R(\mathbb{U}(\gamma)) \tag{14.49}$$

So, $W(R, \gamma)$ should be regarded as a gauge invariant function

$$W(R, \gamma) : \mathcal{A}(\Gamma) \to \mathbb{C} \tag{14.50}$$

and therefore we can consider the expectation values:

$$\langle \prod_i W(R_i, \gamma_i) \rangle := \frac{\int_{\mathcal{A}(\Gamma)} \prod_i W(R_i, \gamma_i) e^{-S(\mathbb{U})} d\mu_{\mathcal{A}(\Gamma)}}{\int_{\mathcal{A}(\Gamma)} e^{-S(\mathbb{U})} d\mu_{\mathcal{A}(\Gamma)}} \tag{14.51}$$

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 (14.44) and write

$$S(p) = K \sum_{p_{\mu\nu}(\vec{n})} (r - \mathrm{Re}[\mathrm{Tr}\rho(\mathbb{U}(p_{\mu\nu}(\vec{n})))]) \to -\frac{1}{2} K a^4 \sum_{\vec{n} \in \mathbb{Z}^d} \sum_{\mu \neq \nu} \mathrm{Tr}\rho(F_{\mu\nu}(a\vec{n}))^2 \tag{14.52}$$

♣There is a bit of a cheat here since you did not work out the plaquette to order a^4. ♣

The heuristic limit (14.52) is to be compared with the Yang-Mills action

$$S_{YM} = -\frac{1}{2g_0^2} \int_X d^d x \sqrt{\det g} g^{\mu\lambda} g^{\nu\rho} \mathrm{Tr} F_{\mu\nu} F_{\lambda\rho} \tag{14.53}$$

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

$$\frac{1}{g_0^2} = K a^{4-d} \qquad \Rightarrow \qquad K = \frac{a^{d-4}}{g_0^2} \tag{14.54}$$

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

$$\frac{8\pi^2}{g^2(a_1)} = \frac{8\pi^2}{g^2(a_2)} + \beta \log\frac{a_1}{a_2} + \mathcal{O}(g^2(a_2)) \tag{14.55}$$

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

$$\beta = -\frac{11}{3}n \tag{14.56}$$

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 (14.55) 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 $\exp[-T Area(\gamma)]$ 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 (14.56) is modified to:

$$\beta = -\left(\frac{11}{3}n - \frac{2}{3}n_f\right) \tag{14.57}$$

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" (14.55) 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.

14.4 Hamiltonian Formulation

EXPLAIN HILBERT SPACE FOR 1+1 CASE IS $L^2(G)$.

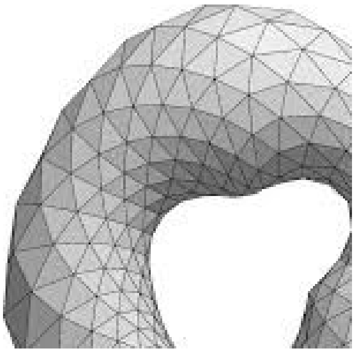

Figure 23: A triangulated surface. Figure from Wikipedia.

14.5 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

$$Z = \frac{1}{|G|} \sum_{g \in G} 1 \tag{14.58}$$

Recalling our discussion of the class equation we recognize that the partition function can be written as:

$$Z = \sum_{c.c.} \frac{1}{|Z(g)|} \tag{14.59}$$

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

$$Z(X \times S^1) = \mathrm{Tr}_{\mathcal{H}(X)} e^{-\beta H} \tag{14.60}$$

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

$$\prod_p \delta(\mathbb{U}(p)) \tag{14.61}$$

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 (14.61) 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

$$\langle \prod_i W(R_i, \gamma_i)\rangle \tag{14.62}$$

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 23. We want a local action, so let us restrict to a flat gauge field on a triangle as in Figure 20. We want to assign the local "Boltzman weight." It will be a function:

$$W : G \times G \to \mathbb{C}^* \tag{14.63}$$

(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 20 we assign the weight

$$W(g_1, g_2) \tag{14.64}$$

to this triangle. But now we have to decide if we are to use this, or $W(g_2, (g_1g_2)^{-1})$ or $W((g_1g_2)^{-1}, g_1)$. 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

$$W(\mathbb{U}) := \prod_T W(T)^{\epsilon(T)} \tag{14.65}$$

Now, if this weight is to be at all physically meaningful we definitely want the dependence on all sorts of choices to drop out.

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 24 and 25, respectively. We see that the invariance of the action under type I requires:

$$W(g_1, g_2)W(g_1g_2, g_3) = W(g_1, g_2g_3)W(g_2, g_3) \tag{14.66}$$

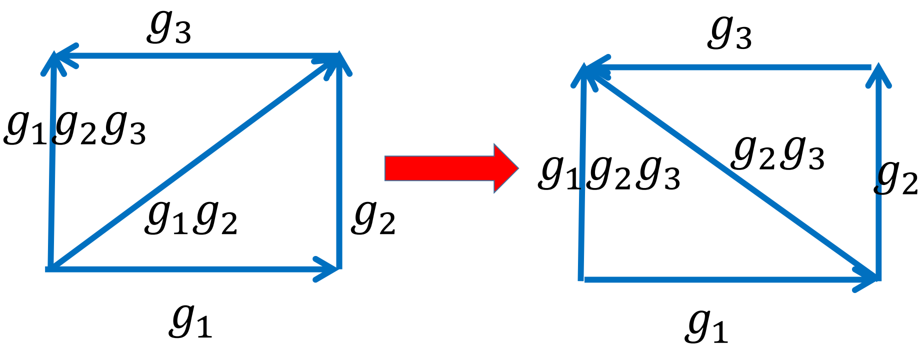

Figure 24: A local change of triangulation of type I.

and this is the condition that W should be a 2-cocycle. Similarly, the change of type II doesn't matter provided

$$W(g_1, g_2) = W(g_1, g_2g_3)W(g_2, g_3)W(g_1g_2, g_3)^{-1} \tag{14.67}$$

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:

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

$$W(g_1, g_2) \to W(g_1, g_2)\frac{t(g_1)t(g_2)}{t(g_1g_2)} \tag{14.68}$$

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 (14.65) 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

$$W(h(v_1)^{-1}g_1h(v_2), h(v_2)^{-1}g_2h(v_3)) \tag{14.69}$$

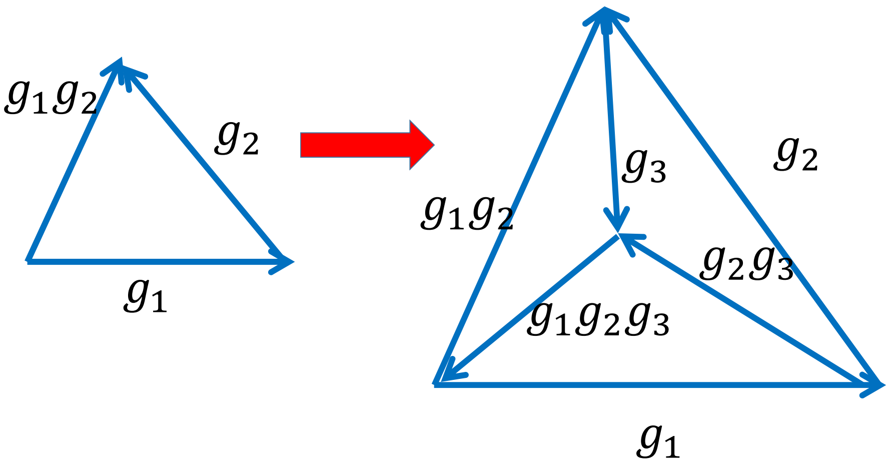

Figure 25: A local change of triangulation of type II.

for all group elements $h(v_1), h(v_2), h(v_3) \in G$. The argument that, nevertheless, the total action (14.65) is invariant is given (for the $d = 3$ case) in the Dijkgraaf-Witten paper around their equation (6.29).

♣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. ♣

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.

4. The invariance under the change of type II in Figure 25, 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. [85] This fits in harmoniously with the alleged the metric-independence of the topological gauge theory.

[85] 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

$$e^{-S_{eff}} := \sum_{fixed-effective-spins} e^{-S(spins)} \qquad (14.70)$$

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.

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 $[W] \in H^3(BG, U(1)) = H^3_{\rm groupcohomology}(G, U(1))$ 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!

15. Example: Symmetry Protected Phases Of Matter In $1 + 1$ Dimensions