Preprint typeset in JHEP style - HYPER VERSION

Chapter 1: Abstract Group Theory

Gregory W. Moore

Abstract: Very Abstract.December 6, 2014

Contents

1. Introduction **2**

2. Basic Definitions **3**

3. Homomorphism and Isomorphism **7**

4. The symmetric group. **9**
- 4.1 Cayley's Theorem 11
- 4.2 Cyclic Permutations and cycle decomposition 12
- 4.3 Transpositions 13
- 4.4 Diversion and Example: Card shuffling 16

5. Generators and relations **19**
- 5.1 Fundamental groups in topology 23

6. Cosets and conjugacy **27**
- 6.1 Equivalence Relations 27
- 6.2 Lagrange Theorem 28
- 6.3 Conjugacy 29
- 6.4 Conjugacy classes in S_n 32
- 6.5 Centralizer and counting conjugacy classes 36

7. Kernel, image, and exact sequence **38**

8. Group theory and elementary number theory **42**
- 8.1 Reminder on gcd and the Euclidean algorithm 42
- 8.2 The direct product of two cyclic groups 44
- 8.3 Application: Expressing elements of $SL(2,\mathbb{Z})$ as words in S and T 48

9. The Group of Automorphisms **50**
- 9.1 The group of units in $\mathbb{Z}_N$ 53
- 9.2 Group theory and cryptography 56

10. Products and Semidirect products **57**

11. Group Extensions and Group Cohomology **61**
- 11.1 Group Extensions 61
- 11.2 Central extensions 65
- 11.3 Heisenberg extensions 75
- 11.4 General Extensions 80
  - 11.4.1 Non-central extensions when N is abelian 82

11.5 Group cohomology in other degrees 83
11.5.1 Definition 83
11.5.2 Interpreting the meaning of H^0 85
11.5.3 Interpreting the meaning of H^1 85
11.5.4 Interpreting the meaning of H^3 85
11.6 Some references 87

12. Overview of general classification theorems for finite groups 87
12.1 Brute force 88
12.2 Finite Abelian Groups 92
12.3 Finitely generated abelian groups 96
12.4 The classification of finite simple groups 96

13. Categories: Groups and Groupoids 103
13.1 Groupoids 107
13.2 The topology behind group cohomology 108

---

1. Introduction

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

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

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 a unit: $\exists e \in G$ 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. Also, we sometimes denote the productof a and b simply by ab.

2. 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:

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) \equiv (x_1 + y_1, \ldots, x_n + y_n) \tag{2.2}$$

Example 2.3: $G = \mathbb{R}^* \equiv \mathbb{R} - \{0\}$ or $G = \mathbb{C}^* \equiv \mathbb{C} - \{0\}$ 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 number of elements in G. A group is G 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 N. As a set we can take $G = \{0, 1, \ldots, N-1\}$. [2] 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, $r \in G$. The group operation on G is that $r_1 \cdot r_2$ is defined to be the residue of $(r_1 + r_2)$ modulo N. [3] 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? [4]

---

[2] 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 $\overline{r_1} + \overline{r_2} := \overline{r_1 + r_2}$.

[3] 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 $r_1 \cdot r_2$!!

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

Exercise

In example 4 show that if N is even then the subset of classes of even integers forms a subgroup of $\mathbb{Z}_N$. What happens if N is odd?

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

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

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.*"

There are certainly examples of nonabelian groups.

Example 2.5: *The general linear group*

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

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

$GL(n, \kappa)$ is a group of infinite order. It is abelian if $n = 1$ and nonabelian if $n > 1$.

There are some important generalizations: We could let κ be any field. If κ is a finite field then we get a finite group. More generally, if R is an *ring* (defined in Chapter 2 below) $GL(n, R)$ is the subset of $n \times n$ matrices with entries in R with an inverse in $M_n(R)$. This set forms group.

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 $GL(n, k)$ is the subgroup of matrices proportional to the unit matrix.

Example 2.6: *Classical matrix groups*

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

The special linear group:

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

The orthogonal groups:

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

In particular

$$SO(2,\mathbb{R}) = \{R(\phi) := \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} : \phi \sim \phi + 2\pi\} \tag{2.8}$$

and $SO(3,\mathbb{R})$ is familiar from rotations in 3-space.

Another natural class are the unitary and special unitary groups:

$$U(n) := \{A \in GL(n,\mathbb{C}) : AA^\dagger = 1\} \tag{2.9}$$

$$SU(n) := \{A \in U(n) : \det A = 1\} \tag{2.10}$$

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

$$J = \begin{pmatrix} 0 & 1_{n\times n} \\ -1_{n\times n} & 0 \end{pmatrix} \in M_{2n}(\mathbb{R}) \tag{2.11}$$

Note that the matrix J satisfies the properties:

$$J = J^* = -J^{tr} = -J^{-1} \tag{2.12}$$

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

$$A^{tr} J A = J \tag{2.13}$$

We define the symplectic groups:

$$\begin{aligned} Sp(2n,\mathbb{R}) &:= \{A \in GL(2n,\mathbb{R}) | A^{tr} J A = J\} \\ Sp(2n,\mathbb{C}) &:= \{A \in GL(2n,\mathbb{C}) | A^{tr} J A = J\} \end{aligned} \tag{2.14}$$

Exercise

a.) Check that each of the above sets (2.6),(2.7),(2.9), (2.14), are indeed subgroups of the general linear group.

b.) In (2.14) we could have defined $Sp(2n,\kappa)$ to be matrices in $M_{2n}(\kappa)$ such that $A^{tr} J A = J$. Why?

Example 2.7 Function spaces as ∞-dimensional groups

Suppose G is a group. Suppose X is any set. Define a space of functions:

$$\mathcal{F}[X \to G] = \{f : f \text{ is a function from } X \to G\} \tag{2.15}$$

Claim: $\mathcal{F}[X \to G]$ is also a group: We define the product $f_1 \cdot f_2$ to be the function taking values:

$$(f_1 \cdot f_2)(x) \equiv f_1(x) \cdot f_2(x) \tag{2.16}$$

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:

$$LG = \{Maps : f : S^1 \to G\} \tag{2.17}$$

we have the famous "loop group" which has many wonderful properties. (It is also the beginning of string theory.)

Example 2.8: Let M be a smooth manifold. The group of diffeomorphisms of M, denoted Diff(M) is a group under composition. While much work has been done on these groups, it seems there is a lot left to discover about them. One can ask simple questions about them whose answers are unknown.

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:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2') \tag{2.18}$$

Check the group axioms.

---

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, $G = \mathbb{Z}/N\mathbb{Z}$ and consider the transformation $\mu(\bar{r}) = \overline{kr}$ where k is an integer relatively prime to N. 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 $\{1, \omega, \ldots, \omega^{N-1}\}$, $\omega = \exp(2\pi i/N)$, 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 of permutations on two letters $\{e, (12)\}$. (See the next section for the definition.) Denote $\sigma = (12)$. 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 $\mu : S_2 \to \hat{S}_2$

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

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

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

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 $\mathbb{Z}_N$.

---

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.

A *permutation* of a set 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.

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 $X = \{1, 2, \ldots, n\}$.

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

$$(\phi_1 \cdot_L \phi_2)(i) := \phi_2(\phi_1(i))$$
$$(\phi_1 \cdot_R \phi_2)(i) := \phi_1(\phi_2(i)) \tag{4.1}$$

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: $\phi(1) = p_1, \phi(2) = p_2, \ldots, \phi(n) = p_n$. 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 $a_1, \ldots, a_n$ is any permutation of $1, \ldots, n$. 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

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

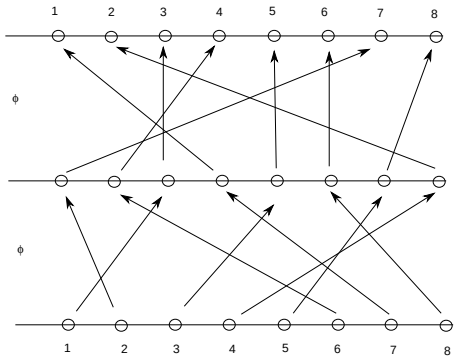
Exercise

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}.

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

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



1

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

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. [5]

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 observation known as the *The rearrangement lemma*:

Consider a finite group

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

[5] 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 $(\phi_1 \cdot_L \phi_2)^{-1} = \phi_1^{-1} \cdot_R \phi_2^{-1}$.

For any $h \in G$ consider the set

$$\{h \cdot g_1, \ldots, h \cdot g_n\} \tag{4.11}$$

Show that (4.11) is a list of distinct elements which is just a rearrangement, i.e. a *permutation* of (4.10). We will come back to this point several times.

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

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

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, another notion we will come back to and discuss more systematically in chapter ****.

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

4.2 Cyclic Permutations and cycle decomposition

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

$$a_1 \to a_2 \to \cdots \to a_\ell \to a_1 \tag{4.13}$$

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

$$\phi = (a_1 a_2 \ldots a_\ell). \tag{4.14}$$

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

$$(a_1 a_2 \ldots a_\ell) = (a_2 a_3 \ldots a_\ell a_1) = (a_3 \ldots a_\ell a_1 a_2) = \cdots = (a_\ell a_1 a_2 \ldots a_{\ell-1}) \tag{4.15}$$

So:

$$S_2 = \{1, (12)\} \tag{4.16}$$

$$S_3 = \{1, (12), (13), (23), (123), (132)\} \tag{4.17}$$

$$\begin{aligned} S_4 = \{&1, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), \\ &(123), (132), (124), (142), (134), (143), (234), (243) \\ &(1234), (1243), (1324), (1342), (1423), (1432)\} \end{aligned} \tag{4.18}$$

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

$$\sigma = (12)(34)(10,11)(56789) \tag{4.19}$$

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[6]

$$\begin{aligned}(12)\cdot(13) &= (132)\\ (13)\cdot(12) &= (123)\end{aligned} \tag{4.20}$$

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:

$$\begin{aligned}(ij)\cdot(jk)\cdot(ij) = (ik) &= (jk)\cdot(ij)\cdot(jk)\\ (ij)^2 &= 1\\ (ij)\cdot(kl) &= (kl)\cdot(ij) \qquad \{i,j\}\cap\{k,l\} = \emptyset\end{aligned} \tag{4.21}$$

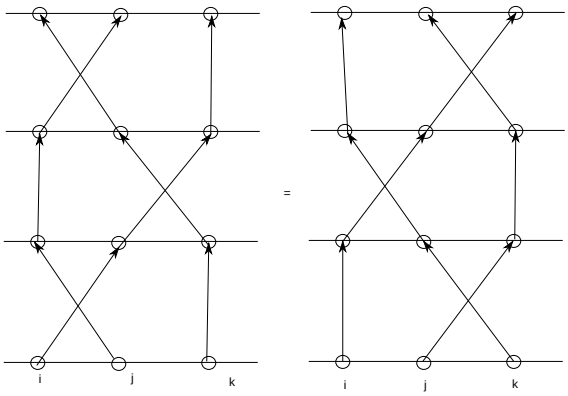


Figure 2: Pictorial illustration of equation (4.21) line one for transpositions. Note that the identity is suggested by "moving the time lines" holding the endpoints fixed. Reading time from bottom to top corresponds to reading the composition from left to right in the $\cdot_R$ convention.

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

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

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

$$(1,k)(1,k-1)\cdots(1,4)(1,3)(1,2) = (1,2,3,4,\ldots,k) \tag{4.22}$$

Now, if we conjugate this identity by the permutation taking $\{1,\ldots,k\} \to \{a_1,\ldots,a_k\}$ (say, holding everything else fixed) then we get an analogous identity for the cyclic permutation $(a_1, \cdots, a_k)$.

Therefore, *every element of* S_n *can be written as a product of transpositions, generalizing* (4.20). 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 (4.21). A nontrivial fact is that all relations between 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 (4.21) 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 $\sigma_i := (i, i+1)$, $1 \leq i \leq n-1$ we can generate all other transpositions in S_n. These are sometimes called the elementary generators.

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.

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

$$\epsilon : S_n \to \mathbb{Z}_2 \tag{4.23}$$

where we identify $\mathbb{Z}_2$ as the multiplicative group $\{\pm 1\}$. 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:

$$\epsilon_{i_1 \cdots i_n} \tag{4.24}$$

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

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{4.25}$$

is an even permutation.
3. $\epsilon_{i_1 \cdots i_n} = -1$ if

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{4.26}$$

is an odd permutation.
So, e.g. among the 27 entries of ϵ_{ijk}, $1 \leq i, j, k \leq 3$ we have

$$\begin{aligned}\epsilon_{123} &= 1\\ \epsilon_{132} &= -1\\ \epsilon_{231} &= +1\\ \epsilon_{221} &= 0\end{aligned} \tag{4.27}$$

and so forth.

Exercise
Show that

$$\epsilon_{i_1 i_2 \cdots i_n}\epsilon_{j_1 j_2 \cdots j_n} = \sum_{\sigma \in S_n} \epsilon(\sigma)\delta_{i_1 j_{\sigma(1)}}\delta_{i_2 j_{\sigma(2)}} \cdots \delta_{i_n j_{\sigma(n)}} \tag{4.28}$$

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 $\mathbb{R}^3$:

$$\vec{A} \times (\vec{B} \times \vec{C}) = \vec{B}(\vec{A} \cdot \vec{C}) - \vec{C}(\vec{A} \cdot \vec{B}) \tag{4.29}$$

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

$$0, n, 1, n+1, 2, n+2, \ldots, n+2, 2n-2, n-1, 2n-1 \tag{4.30}$$

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

$$\mathcal{O}(x) = \begin{cases} 2x & x \leq n-1 \\ 2x-(2n-1) & n \leq x \leq 2n-1 \end{cases} \tag{4.31}$$

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:

$$\begin{aligned} \mathcal{O} = &(0)(1,2,4,8,16,32,13,26)(3,6,12,24,48,45,39,27) \\ &(5,10,20,40,29,7,14,28)(9,18,36,21,42,33,15,30) \\ &(11,22,44,37,23,46,41,31)(17,34)(19,38,25,50,49,47,43,35)(51) \end{aligned} \tag{4.32}$$

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 $D_{2n} = \{0, 1, \ldots, 2n-1\}$ and we embed it in a Deck with $2n+2$ cards

$$D_{2n} \to D_{2n+2} \tag{4.33}$$

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

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

$$\mathcal{I}(x) = \begin{cases} 2(x+1)-1 & x+1 \leq n \\ 2(x+1)-(2n+1)-1 & n+1 \leq x+1 \end{cases} \tag{4.34}$$

One can check that this is given by the uniform formula

$$\mathcal{I}(x) = 2x + 1 \mathrm{mod}(2n+1) \tag{4.35}$$

for $x \in D_{2n}$.

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

$$\begin{aligned} &(0,1,3,7,15,31,10,21,43,34,16,33,14,29,6,13,27,2,5, \\ &11,23,47,42,32,12,25,51,50,48,44,36,20,41,30,8,17, \\ &35,18,37,22,45,38,24,49,46,40,28,4,9,19,26) \end{aligned} \tag{4.36}$$

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 n in its binary expansion:

$$\ell = 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2^1 + a_0 \tag{4.37}$$

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

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

$$\begin{aligned}
&0 \to 1 \\
&\quad \to 2 \cdot 1 + a_{k-1} \\
&\quad \to 2 \cdot (2 \cdot 1 + a_{k-1}) + a_{k-2} = 2^2 + 2a_{k-1} + a_{k-2} \\
&\quad \to 2 \cdot (2^2 + 2a_{k-1} + a_{k-2}) + a_{k-3} = 2^3 + 2^2 a_{k-1} + 2a_{k-2} + a_{k-3} \\
&\vdots \qquad \vdots \\
&\quad \to 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2^1 + a_0 = \ell
\end{aligned} \tag{4.38}$$

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

$$\phi : W(B_n) \to S_n \tag{4.39}$$

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 $\mathcal{S}_{2n}$. 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 a deck of 12 cards have some special properties. In fact, one can use it to generate a very interesting group known as the Mathieu group M_{12}. It was the first "sporadic" finite simple group. See section §12.4 below.

To describe M_{12} we consider the reverse shuffle $r(x) = 11 - x$. Here we take the deck of cards and simply transfer the top card to the bottom, the next on top etc. For the Mongean shuffle we start with our deck on the left. We place the top card on the right. Then alternately we put the next card on the top of the bottom of the right deck. This is the permutation

$$m : \{1, 2, \ldots, 2n\} \to \{2n, 2n-2, \ldots, 4, 2, 1, 3, 5, \ldots, 2n-3, 2n-1\} \tag{4.40}$$

In formulae, acting on D_{2n}

$$m(x) = \mathrm{Min}[2x, 2n + 1 - 2x] \tag{4.41}$$

For a pack of 12 cards r and m generate the Mathieu group M_{12}. It turns out to have order

$$|M_{12}| = 2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95040 \tag{4.42}$$

Compare this with

$$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 = 479001600 \tag{4.43}$$

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

Definition 5.1 A subset $S \subset G$ is a *generating set* for a group if every element $g \in G$ can be written as a "word" or product of elements of 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 $1 \leq k \leq r$ we have $s_{i_k} \in S$.

Finitely generated means that the generating set S is finite, that is, there is a finite list of elements $\{s_1, \ldots s_n\}$ so that all elements of the group can be obtained by taking products – "words" – in the "letters" drawn from 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. [7]

In general if we have a finitely generated group we write

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

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

where R_i are the words in the letters of S which will be set to 1.

Remark: It is convenient to exclude the unit 1 from S. Also, it is sometimes convenient to include s^{-1} in S if $s \in S$. Such generating sets are said to be *symmetric*.

Example 2.1: If S consists of one element a then $F(S) \cong \mathbb{Z}$. 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 S, denoted $F(S)$. If S consists of one element then we just get $\mathbb{Z}$, as above. However, things are completely different if S consists of two elements a, b. Then $F(S)$ is very complicated. A typical element looks like one of

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

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

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

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

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

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:

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

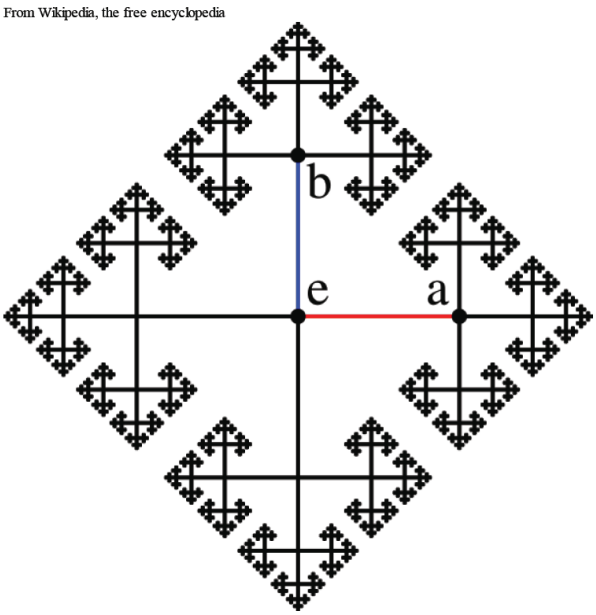


Figure 3: The Cayley graph for the free group on 2 generators a and b.

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 finite Coxeter groups are Weyl groups of simple Lie algebras. 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 $m_{ij} \geq 3$. By convention the edges are labeled by m_{ij} and if $m_{ij} = 3$ then the standard convention is to omit the label.

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

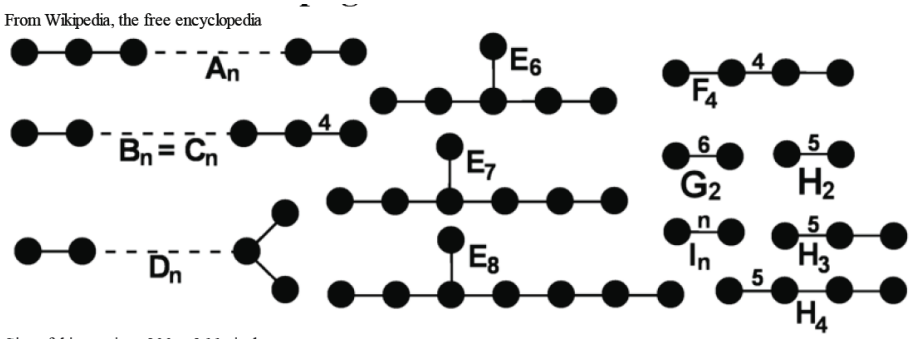


Figure 4: Coxeter's list of finite Coxeter groups.

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

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

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. 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.)

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.

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 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, $i = 1, \ldots, n-1$ with $\sigma_i^2 = 1$, $1 \leq i \leq (n-1)$, $(\sigma_i \sigma_{i+1})^3 = 1$, $1 \leq i \leq n-2$, $(\sigma_i \sigma_j)^2 = 1$ 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.

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. [8]

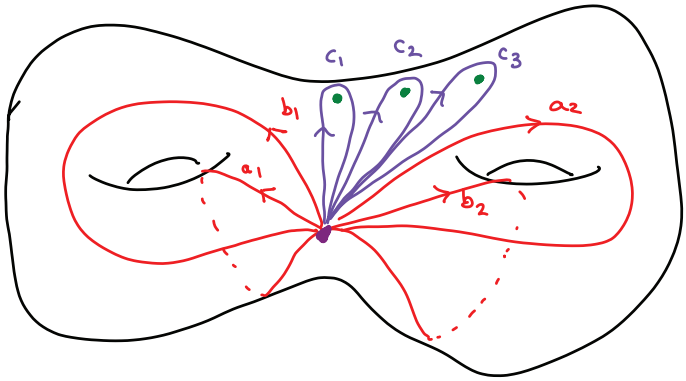


Figure 5: A collection of closed paths at x_0 which generate the fundamental group of a two-dimensional surface with two handles and three (green) holes.

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:

[8] For more detail see Chapter 2 below.

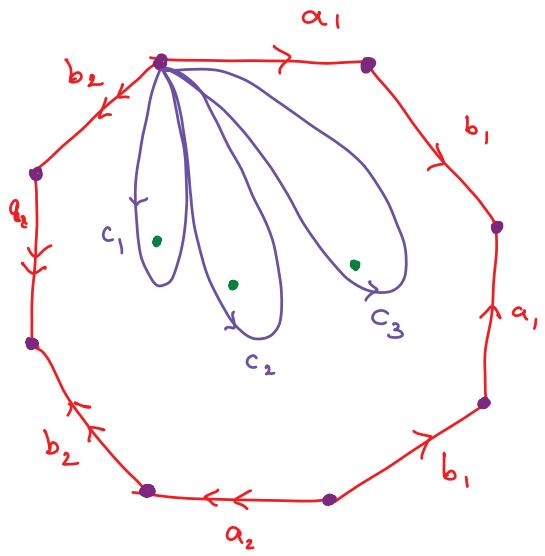


Figure 6: When the directed edges are identified according to their labels the above surface reproduces the genus two surface with three punctures. Since the disk is simply connected we derive one relation on the curves shown here.

From these kinds of constructions one can prove [9] that the fundamental group of an orientable surface with g handles and p punctures will be

$$\pi_1(S, x_0) = \langle a_i, b_i, c_s | \prod_{i=1}^{g} [a_i, b_i] \prod_{s=1}^{p} c_s = 1 \rangle \tag{5.11}$$

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 (5.11) are sometimes called *surface groups*.

Exercise *Fundamental group of the Klein bottle*

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

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

$$\langle a, b | a^2 = b^2 \rangle \tag{5.12}$$

and the other is

$$\langle g_1, g_2 | g_1 g_2 g_1 g_2^{-1} = 1 \rangle \tag{5.13}$$

Show that these two presentations are equivalent.

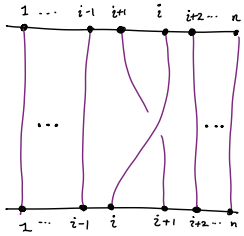


Figure 7: Pictorial illustration of the generator σ_i of the braid group B_n.

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

$$\tilde{\sigma}_i \tilde{\sigma}_j = \tilde{\sigma}_j \tilde{\sigma}_i \qquad\qquad |i-j| \geq 2 \tag{5.14}$$

and

$$\tilde{\sigma}_i \tilde{\sigma}_{i+1} \tilde{\sigma}_i = \tilde{\sigma}_{i+1} \tilde{\sigma}_i \tilde{\sigma}_{i+1} \tag{5.15}$$

where the relation (5.15) 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 (5.14)(5.15):

$$\mathcal{B}_n := \langle \tilde{\sigma}_1, \ldots, \tilde{\sigma}_{n-1} | \tilde{\sigma}_i \tilde{\sigma}_j \tilde{\sigma}_i^{-1} \tilde{\sigma}_j^{-1} = 1, |i-j| \geq 2; \tilde{\sigma}_i \tilde{\sigma}_{i+1} \tilde{\sigma}_i = \tilde{\sigma}_{i+1} \tilde{\sigma}_i \tilde{\sigma}_{i+1} \rangle \tag{5.16}$$

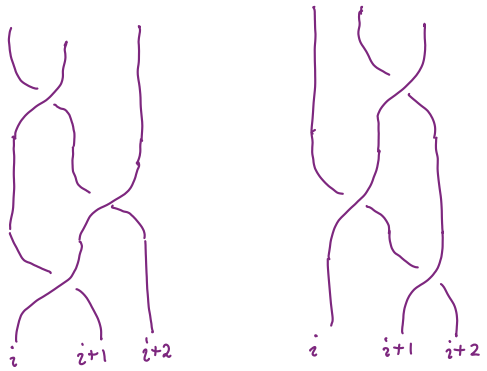


Figure 8: Pictorial illustration of the Yang-Baxter relation.

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.

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 $\phi : \mathcal{B}_n \to S_n$.

Remarks

1. In the theory of integrable systems the relation (5.15) 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. 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. For a recent review see: [10]

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.

[10] A. Stern, "Anyons and the quantum Hall effectA pedagogical review". Annals of Physics 323: 204; arXiv:0711.4697v1.

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: $G = S_3$, $H = S_2 = \{1, (12)\}$. 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. [11]

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.

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

Definition 6.2.2: If G is any group and H any subgroup then the he *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: If $G = S_3, H = S_2$, then $G/H = \{H, (13) \cdot H, (23) \cdot H\}$, and $[G : H] = 3$.

Remark: What about the converse to Lagrange's theorem? Suppose $n||G|$, does there then exist a subgroup of G of order n? Not necessarily!

Exercise
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. [12] [13]

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

Theorem 6.2.2: (Sylow's 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.

For a proof, see Herstein's book, sec. 2.12.

As a final application, an element $g \in G$ is said to have *order* n if n is the smallest natural number such that $g^n = 1$. If G is a finite group then by considering the subgroup generated by g, i.e. $\{1, g, g^2, \dots\}$ we see that the order g must divide $|G|$, and in particular $g^{|G|} = 1$. (It is very easy to give examples of elements with infinite order in infinite groups.)

Exercise *Subgroups of A_4*
Write down all the 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 $\exists g \in G \qquad h' = ghg^{-1}$.

[12] *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 $|G|$.

[13] 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.

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

$$C(h) := \{ghg^{-1} : g \in G\} \tag{6.6}$$

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

$$K = gHg^{-1} \equiv \{ghg^{-1} : h \in H\} \tag{6.7}$$

Exercise
a.) Show that conjugacy is an equivalence relation
b.) Prove that gHg^{-1} is also a subgroup.

Example 6.3.1 : Let $G = GL(n,k)$ 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

$$gNg^{-1} = N \qquad \forall g \in G \tag{6.8}$$

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, is *not* a group. But, if H is normal something special happens:

Theorem 6.3.1. If $N \subset G$ is a normal subgroup then the set of left cosets $G/N = \{gN | g \in G\}$ is *itself* a group with group multiplication:

$$(g_1 N) \cdot (g_2 N) := (g_1 \cdot g_2) N \tag{6.9}$$

Proof- left as an exercise:

The main thing to check is that this is is even well defined. If $g_1 N = g_1' N$ do you get the same answer from (6.9) ? Show this carefully.

Once we see that (6.9) 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. ♠

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 (6.8) 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?

Example 6.3.3 . 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.

Example 6.3.4 .

$$A_3 \equiv \{1, (123), (132)\} \subset S_3 \tag{6.10}$$

is normal. What group is S_3/A_3?

Exercise *Even permutations*

Example 6.3.4 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.

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

e.) 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.

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. Note the following two points:

1. *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 $g(i_1 i_2 \cdots i_k)g^{-1} = (j_1 j_2 \cdots j_k)$.

2. *Therefore, any two cycles of length k are conjugate.*

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

$$(12)(123)(12)^{-1} = (213) = (132) \tag{6.11}$$

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 how many distinct cycles of length j we have in a cycle decomposition of a typical element σ of $C(\sigma)$.*

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

$$(12)(34), \qquad (13)(24), \qquad (14)(23) \tag{6.12}$$

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

Given a cycle decomposition call the number of disjoint cycles of length j, ℓ_j. Clearly since we must account for all n letters being permuted:

$$n = \ell_1 + 2\ell_2 + \cdots n\ell_n = \sum_{j=1}^{n} j\ell_j \tag{6.13}$$

such a decomposition of n into a sum of nonnegative integers is called a *partition of n*. We denote the conjugacy class by

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

The conjugacy classes of S_n 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 $p(n)$.

Example Conjugacy classes of S_4 and S_5:

Partition	Cycle decomposition	Typical g	$\lvert C(g)\rvert$	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

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

Remarks:

1. 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:

$$[a_j, a_k] = 0 \qquad [a_j^\dagger, a_k^\dagger] = 0 \qquad [a_j, a_k^\dagger] = \delta_{j,k} \qquad j,k = 1,\ldots \tag{6.15}$$

Suppose they have frequencies which are all a multiple of a basic harmonic ω, so the frequencies are $\omega, 2\omega, 3\omega, \ldots$. The Hamiltonian is, formally,

$$H^{\text{formal}} = \sum_{j=1}^{\infty} j\omega(a_j^\dagger a_j + \frac{1}{2}) \tag{6.16}$$

This is formal, because on the usual lowest weight module defined by $a_j|vac\rangle = 0$ 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

$$\sum_{j=1}^{\infty} \frac{j}{2}\omega = \frac{\omega}{2}\sum_{j=1}^{\infty}\frac{1}{j^{-1}} \to \frac{\omega}{2}\zeta(-1) = -\frac{\omega}{24} \tag{6.17}$$

This can be justified much more rigorously and indeed it gives the correct Casimir energy for a massless scalar field on a circle. In any case, things work out very nicely if we take the Hamiltonian to be:

$$H = \sum_{j=1}^{\infty} j\omega a_j^\dagger a_j - \frac{\omega}{24} \tag{6.18}$$

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:

$$(a_1^\dagger)^{\ell_1}(a_2^\dagger)^{\ell_2}\cdots(a_n^\dagger)^{\ell_n}|0\rangle \tag{6.19}$$

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.

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

$$\frac{1}{\prod_{n=1}^{\infty}(1-q^n)} = 1 + \sum_{n=1}^{\infty} p(n)q^n \tag{6.20}$$

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

$$Z(\beta) = \mathrm{Tr}e^{-\beta H} = \frac{1}{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)}, \tag{6.21}$$

where we trace over the Hilbert space of states of our collection of oscillators. Here we identify $q = e^{-\beta\omega}$. Expanding out (6.20) gives the first few values of $p(n)$:

$$\begin{aligned} &1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + 11q^6 + 15q^7 + 22q^8 + 30q^9 + \\ &+ 42q^{10} + 56q^{11} + 77q^{12} + 101q^{13} + 135q^{14} + \cdots \end{aligned} \tag{6.22}$$

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

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

$$\beta^{1/4}Z(\beta) = \tilde{\beta}^{1/4}Z(\tilde{\beta}) \tag{6.23}$$

$$\beta\tilde{\beta} = \left(\frac{2\pi}{\omega}\right)^2 \tag{6.24}$$

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:

$$p(n) \sim \frac{1}{\sqrt{2}}(\frac{1}{24})^{3/4} n^{-1} \exp\left(2\pi\sqrt{\frac{n}{6}}\right) \tag{6.25}$$

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!

4. Analogs of equation (6.25) 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 *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 $|C(g)|$. [14]

Exercise *Deriving the Hardy-Ramanujan formula*

Write

$$p(n) = \int_0^{2\pi i/\omega} d\beta e^{-n\beta\omega} Z(\beta) \tag{6.26}$$

and use the above transformation formula, together with the stationary phase method to derive (6.25).

---

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

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:

$$Z(g) := \{h \in G | hg = gh\} \tag{6.27}$$

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

$$|C(g)| = \frac{|G|}{|Z(g)|} \tag{6.28}$$

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

$$\psi : g_i Z(g) \to g_i g g_i^{-1} \tag{6.29}$$

1. First, check that this is well-defined.
2. Then note that ψ is 1-1 and onto $C(g)$.

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

$$|G| = \sum_{classes} \frac{|G|}{|Z(g)|} \tag{6.30}$$

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 $C(g)$.

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
$$Z(S^1) = \frac{1}{|G|} \sum_{g \in G} 1 \tag{6.31}$$
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:

$$Z(S^1) = \frac{1}{|G|} \sum_{cc} |C(g)| = \sum_{cc} \frac{1}{|Z(g)|} \tag{6.32}$$

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!

Here is a nice application of this counting principle:

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:

$$|G| = |Z(G)| + \sum_{classes}{}' \frac{|G|}{|Z(a)|} \tag{6.33}$$

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 (6.33) is divisible by p and hence $p||Z(G)|$. ♠

A similar useful fact is:

Theorem(Cauchy's theorem): If p divides $|G|$ then there is an element $g \in G$, $g \neq 1$ with order p.

Proof: See Herstein's book. The idea is to use induction on the order $|G|$ together with the class equation ♠

Exercise

If $|G| = p^2$ where p is a prime then G is abelian. Show that $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.

Exercise

Show that if p^k divides $|G|$ with $k > 1$ then it does *not* follow that there exists an element of order p^k. [15]

[15] *Answer*: One counterexample is to consider $(\mathbb{Z}_2)^k$. It has order 2^k, but all elements are order two.

Exercise
Find the centralizer of $(12\dots n)$ in S_n.

Exercise
Prove that if $|G| = 15$ then $G = \mathbb{Z}/15\mathbb{Z}$.

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

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

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?

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

$$G_1 \stackrel{f_1}{\to} G_2 \stackrel{f_2}{\to} G_3 \tag{7.4}$$

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

This generalizes to sequences of several groups and homomorphisms

$$\dots \stackrel{f_{i-1}}{\to} G_i \stackrel{f_i}{\to} G_{i+1} \stackrel{f_{i+1}}{\to} \dots \tag{7.5}$$

In particular, a *short exact sequence* is a sequence of the form

$$1 \to G_1 \stackrel{f_1}{\to} G_2 \stackrel{f_2}{\to} G_3 \to 1 \tag{7.6}$$

where 1 refers to the trivial group with one element is exact at G_1, G_2, G_3. Thus, the meaning of (7.6) is that

1. f_1 is an injection of G_1 into G_2. There is no nontrivial kernel.
2. $\mathrm{im} f_1 = \ker f_2$.
3. f_2 is a surjection onto G_3.

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: $k_1, k_2 \in K \Rightarrow$

$$\begin{aligned} \mu(k_1 k_2) &= \mu(k_1)\mu(k_2) = 1_{G'} \\ \mu(k^{-1}) &= \mu(k)^{-1} = 1_{G'} \end{aligned} \tag{7.7}$$

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

$$\mu(g) = \mu(g') \qquad \leftrightarrow \qquad gK = g'K \tag{7.8}$$

Thus we have

Theorem 7.2:

$$\boxed{\mu(G) \cong G/K} \tag{7.9}$$

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

$$\psi : gK \mapsto \mu(g) \tag{7.10}$$

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

1. ψ is a well defined map:

$$gK = g'K \Rightarrow \exists k \in K, g' = gk \Rightarrow \mu(g') = \mu(gk) = \mu(g)\mu(k) = \mu(g) \tag{7.11}$$

2. ψ is 1 to 1, i.e.

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

Remark: If we have a short exact sequence

$$1 \to N \to G \to Q \to 1 \tag{7.13}$$

Then N is isomorphic to a normal subgroup of G and Q, the *quotient group*, is isomorphic to G/N. A frequently used terminology is that *"G is an extension of Q by N. "* but some authors 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. Group extensions play an important role in quantum mechanics so we will discuss them rather thoroughly in §11 below. For the moment we quote two important examples:

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

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{7.14}$$

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

Example 2: In chapter 10 we will discuss the beautiful relation between two-by-two matrix groups and groups of rotations and boosts. One example of this leads to the exact sequence

$$1 \to \mathbb{Z}_2 \to SU(2) \to SO(3) \to 1 \tag{7.15}$$

Example 3: 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

$$P_{i,j} = \delta_{j=i+1 \bmod N} \tag{7.16}$$

$$Q_{i,j} = \delta_{i,j}\omega^j \tag{7.17}$$

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

$$PQ = \omega QP \tag{7.18}$$

For $N = 4$ the matrices look like

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad Q = \begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 \\ 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{7.19}$$

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

$$1 \to \mathbb{Z}_N \to \text{Heis}_N \xrightarrow{\pi} \mathbb{Z}_N \times \mathbb{Z}_N \to 1 \tag{7.20}$$

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

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

$$1 \to \mu^{-1}(H_2)/H_1 \to G_1/H_1 \to G_2/H_2 \tag{7.21}$$

Exercise

Let n be a natural number and let

$$\psi : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^d \tag{7.22}$$

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

Using the matrices of (7.16) and (7.17) show that the word

$$P^{n_1}Q^{m_1}P^{n_2}Q^{m_2}\cdots P^{n_k}Q^{m_k} \tag{7.23}$$

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.

Exercise

Compute the kernel of the natural homomorphism $\phi : \mathcal{B}_n \to S_n$ and show that there is an exact sequence

$$1 \to \mathbb{Z}^{n-1} \to \mathcal{B}_n \to S_n \to 1 \tag{7.24}$$

Exercise *Centrally symmetric shuffles*

Let us consider again the permutation group of the set $\{0, 1, \ldots, 2n-1\}$. Recall we let WB_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

$$1 \to \mathbb{Z}_2^n \to WB_n \to S_n \to 1 \tag{7.25}$$

and therefore $|WB_n| = 2^n n!$.

---

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

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

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:

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

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:

$$(m_1, m_2) = (m_1, m_2 - xm_1) \tag{8.3}$$

for any integer x and hence we are reducing by

$$(A, B) = (B, r_1) = (r_1, r_2) = \cdots = (r_{j-1}, r_j) = (r_j, 0) = r_j. \tag{8.4}$$

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

$$Ax + By = g \tag{8.5}$$

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

$$m_1 x + m_2 y = 1. \tag{8.6}$$

Of course x, y are not unique. Equation (8.6) 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 (8.5), find all the others.

Exercise *Continued fractions and the Euclidean algorithm*

a.) Show that the quotients q_i in the Euclidean algorithm define a continued fraction expansion for A/B:

$$\frac{A}{B} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_j}}} := [q_1, q_2, q_3, \cdots, q_j] \tag{8.7}$$

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 (8.38) $r_{j-1}, \ldots, r_1$ (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: [16]

$$AD_{j-1} - BN_{j-1} = (-1)^{j-1}(A, B) \tag{8.8}$$

---

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

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:

$$(h_1, g_1) \cdot (h_2, h_2) = (h_1 \cdot h_2, g_1 \cdot g_2) \tag{8.9}$$

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 $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ is generally used.

Let us begin with the question: Is it true that

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \stackrel{?}{\cong} \mathbb{Z}_{m_1 m_2}. \tag{8.10}$$

In general (8.10) 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

$$0 \to \mathbb{Z}_g \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \to \mathbb{Z}_\ell \to 0 \tag{8.11}$$

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

Recall that if we write the prime factors of m_1, m_2 as

$$m_a = \prod_i p_i^{e_{i,a}}, \qquad a = 1, 2 \tag{8.12}$$

then

$$\begin{aligned} g = \gcd(m_1, m_2) &= \prod_i p_i^{\min[e_{i,1}, e_{i,2}]} \\ \ell = \mathrm{lcm}(m_1, m_2) &= \prod_i p_i^{\max[e_{i,1}, e_{i,2}]} \end{aligned} \tag{8.13}$$

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

$$\mu_1 \nu_1 + \mu_2 \nu_2 = 1 \tag{8.14}$$

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

To prove (8.11) 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:

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

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

$$\Lambda = m_1\mathbb{Z} \oplus m_2\mathbb{Z} = \{ \begin{pmatrix} m_1\alpha \\ m_2\beta \end{pmatrix} | \alpha, \beta \in \mathbb{Z}\} \tag{8.15}$$

Then

$$\mathbb{Z}^2/\Lambda = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \tag{8.16}$$

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

$$\begin{pmatrix} \mu_2 & \mu_1 \\ -\nu_1 & \nu_2 \end{pmatrix} \in SL(2, \mathbb{Z}) \tag{8.17}$$

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

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \mu_2 & \mu_1 \\ -\nu_1 & \nu_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{8.18}$$

that is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \nu_2 & -\mu_1 \\ \nu_1 & \mu_2 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \tag{8.19}$$

which we prefer to write as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = x' \begin{pmatrix} \nu_2 \\ \nu_1 \end{pmatrix} + y' \begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \tag{8.20}$$

Thus, we are using the basis vectors

$$v_1 = \begin{pmatrix} \nu_2 \\ \nu_1 \end{pmatrix} \qquad v_2 = \begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \tag{8.21}$$

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 (8.18) 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 (7.21) ψ descends to a map

$$\bar{\psi} : \mathbb{Z}^2/\Lambda \to \mathbb{Z}/\ell\mathbb{Z} \tag{8.22}$$

Now note from (8.20) that

$$\begin{pmatrix} -\mu_1 \\ \mu_2 \end{pmatrix} \mathrm{mod}\Lambda \tag{8.23}$$

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

$$0 \to \mathbb{Z}_g \to \mathbb{Z}^2/\Lambda \to \mathbb{Z}_\ell \to 0 \tag{8.24}$$

This concludes our second proof. ♠

Now, a corollary of (8.11) is that if m_1, m_2 are relatively prime then indeed we have

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \cong \mathbb{Z}_{m_1 m_2}. \tag{8.25}$$

In fact, there is an important generalization of this statement known as the *Chinese remainder theorem*:

Theorem Suppose $m_1, \ldots, m_r$ are pairwise relatively prime positive integers, (i.e. $(m_i, m_j) = 1$ for all $i \neq j$) then

$$(\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \cong \mathbb{Z}/M\mathbb{Z} \tag{8.26}$$

where $M = m_1 m_2 \cdots m_r$.

Proof: We construct a homomorphism

$$\psi : \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \tag{8.27}$$

by

$$\psi(x) = (x \mathrm{mod} m_1, x \mathrm{mod} m_2, \ldots, x \mathrm{mod} m_r) \tag{8.28}$$

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

$$\begin{aligned} x &= a_1 \mathrm{mod} m_1 \\ x &= a_2 \mathrm{mod} m_2 \\ \vdots \quad &\quad \vdots \\ x &= a_r \mathrm{mod} m_r \end{aligned} \tag{8.29}$$

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

$$x_i m_i + y_i \hat{m}_i = 1 \tag{8.30}$$

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

$$g_i = \delta_{i,j} \mathrm{mod} m_j \qquad \forall 1 \leq i,j \leq r \tag{8.31}$$

Therefore if we set

$$x = \sum_{i=1}^{r} a_i g_i \tag{8.32}$$

then x is a desired solution to (8.29) and hence is a preimage under ψ.

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

$$0 \to M\mathbb{Z} \to \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}) \to 0 \tag{8.33}$$

and hence the desired isomorphism follows. ♠

Remarks

1. (8.25) is used implicitly all the time in physics, whenever we have two degrees of freedom with different but commensurable frequencies. 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 (8.25).

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 [17] 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.

[17] 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? [18]

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

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \& \qquad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{8.34}$$

Here is an algorithm for decomposing an arbitrary element

$$h = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL(2,\mathbb{Z}) \tag{8.35}$$

as a word in S and T.

First, note the following simple

Lemma Suppose $h \in SL(2,\mathbb{Z})$ as in (8.35). Suppose moreover that $g \in SL(2,\mathbb{Z})$ satisfies:

$$g \cdot \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8.36}$$

Then

$$gh = T^n \tag{8.37}$$

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

$$\begin{aligned} A &= q_1 C + r_1 \qquad 0 < r_1 < C \\ C &= q_2 r_1 + r_2 \qquad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \qquad 0 < r_3 < r_2 \\ &\vdots \quad \vdots \\ r_{N-2} &= q_N r_{N-1} + r_N \qquad 0 < r_N < r_{N-1} \\ r_{N-1} &= q_{N+1} r_N \end{aligned} \tag{8.38}$$

[18] Apply the Chinese remainder theorem with $m_1 = 5, m_2 = 11, m_3 = 13$. Then $M = 715$, $\hat{m}_1 = 143$, $\hat{m}_2 = 65$ and $\hat{m}_3 = 55$. Using the Euclidean algorithm you find convenient lifts to the integers $g_1 = 286$, $g_2 = -65$ and $g_3 = -220$. Then the number of troops is $3 \times 286 - 2 \times 65 - 1 \times 220 = 508 \text{mod} 715$. Therefore there are 508 soldiers.

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:

$$\begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} r_1 \\ C \end{pmatrix} \tag{8.39}$$

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:

$$\sigma^1 \begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} C \\ r_1 \end{pmatrix} \tag{8.40}$$

Now the Euclidean algorithm implies the matrix identity:

$$\tilde{g} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8.41}$$

$$\tilde{g} = (\sigma^1 T^{-q_{N+1}}) \cdots (\sigma^1 T^{-q_1}) \tag{8.42}$$

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

$$\det \tilde{g} = (-1)^{N+1} \tag{8.43}$$

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

$$\begin{aligned} (\sigma^1 T^{-q_{2\ell}})(\sigma^1 T^{-q_{2\ell-1}}) &= (\sigma^1 \sigma^3)(\sigma^3 T^{-q_{2\ell}} \sigma^3)(\sigma^3 \sigma^1) T^{-q_{2\ell-1}} \\ &= -S T^{q_{2\ell}} S T^{-q_{2\ell-1}} \end{aligned} \tag{8.44}$$

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

$$\tilde{g} = g = (-1)^s \prod_{\ell=1}^{s} (S T^{q_{2\ell}} S T^{-q_{2\ell-1}}) \tag{8.45}$$

2. Now suppose that $N + 1 = 2s + 1$ is odd. Then we rewrite the identity (8.41) as:

$$\sigma^1 \tilde{g} \begin{pmatrix} A \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8.46}$$

   so now we simply take

$$g = \sigma^1 \tilde{g} = (-1)^{s+1} (S T^{-q_{2s+1}}) \prod_{\ell=1}^{s} (S T^{q_{2\ell}} S T^{-q_{2\ell-1}}) \tag{8.47}$$

Thus we can summarize both cases by saying that

$$g = (-1)^{\lfloor \frac{N+1}{2} \rfloor} \prod_{\ell=1}^{N+1} (ST^{(-1)^\ell q_\ell}) \tag{8.48}$$

Then we can finally write

$$h = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = g^{-1} T^n \tag{8.49}$$

as a word in S and T for a suitable integer n. (Note that $S^2 = -1$.)

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

$$\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ C + mA & D + mB \end{pmatrix} \tag{8.50}$$

while

$$\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} = ST^m S \tag{8.51}$$

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

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

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

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

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

Remarks

1. In practice people often say that an element $\varphi \in \mathrm{Aut}(G)$ is an "outer automorphism" if 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)

2. Note that the group of automorphisms of any abelian group G consists entirely of outer automorphisms.

Example 9.1: 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 $Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$. Similarly, $Aut(\mathbb{Z}_3) \cong \mathbb{Z}_2$.

Example 9.2: 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

$$\phi_2^2 = \phi_4 \qquad \phi_2^3 = \phi_3 \qquad \phi_2^4 = \phi_1 = 1 \tag{9.6}$$

So $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$.

Example 9.3: Consider $Aut(\mathbb{Z}_N)$. A generator ω must go to ω^r for some r. On the other hand, ω^r must be a generator. Hence r is relatively prime to N. This is true iff there is an s with

$$rs = 1 \mathrm{mod} N \tag{9.7}$$

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 9.4: $Aut(S_n)$. There are no outer automorphisms of S_n so

$$Aut(S_n) \cong Inn(S_n) \cong S_n, \qquad n \neq 2, 6 \tag{9.8}$$

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

$$\phi((ab))=(xy) \qquad \phi((ac))=(zw) \tag{9.9}$$

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

$$\phi((ab))=(xy) \qquad \phi((ac))=(xz) \tag{9.10}$$

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

$$\binom{n}{2}=\frac{n!}{(n-2)!2!} \tag{9.11}$$

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

$$\frac{n!}{(n-2\ell)!\ell!2^\ell} \tag{9.12}$$

Setting these equal results in the identity

$$\frac{(n-2)!}{(n-2\ell)!}=\ell!2^{\ell-1} \qquad n\geq 2\ell \tag{9.13}$$

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 $n=2\ell$:

$$(2\ell-2)!=\ell!2^{\ell-1} \tag{9.14}$$

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 9.5: Alternating groups. For the group $A_n\subset S_n$ there is an obvious outer automorphism: 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 $Out(G)$. Again for $n=6$ there is an exceptional outer automorphism.

Example 9.6: 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

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

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

$$\phi(x_1, x_2) = (a_1 x_1 + a_2 x_2, a_3 x_3 + a_4 x_4) \tag{9.15}$$

where we are writing the group additively, and

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in GL(2, \mathbb{Z}_2) \tag{9.16}$$

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

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

$$\bar{n}_1 + \bar{n}_2 = \overline{n_1 + n_2}, \tag{9.17}$$

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

However, note that since

$$(n_1 + N\ell_1)(n_2 + N\ell_2) = n_1 n_2 + N\ell'' \tag{9.18}$$

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

$$\bar{n}_1 \cdot \bar{n}_2 := \overline{n_1 \cdot n_2}. \tag{9.19}$$

In general, even if we omit $\bar{0}$, $\mathbb{Z}/N\mathbb{Z}$ is *not* a group with respect to the multiplication law (find a counterexample). Nevertheless, $\mathbb{Z}/N\mathbb{Z}$ with $+, \times$ is an interesting object which is an example of something called a *ring*. See the next chapter for a general definition of a ring.

On the other hand, let us define *the group of units in the ring* $\mathbb{Z}/N\mathbb{Z}$:

$$(\mathbb{Z}/N\mathbb{Z})^* := \{\bar{m} : 1 \leq m \leq N-1, \gcd(m, N) = 1\} \tag{9.20}$$

where (m, N) is the *greatest common divisor* of m and N.

Then, $(\mathbb{Z}/N\mathbb{Z})^*$ *is* a group with the law (9.19) ! Clearly the multiplication is closed and $\bar{1}$ is the unit. The existence of multiplicative inverses follows from (8.6).

Moreover, as we have seen above, we can identify

$$\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^* \tag{9.21}$$

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

$$\phi_a : n \mathrm{mod} N \to an \mathrm{mod} N \tag{9.22}$$

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

$$\phi_a : \omega \to \omega^a \tag{9.23}$$

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

$$\begin{aligned} \phi(2) &= 1 \\ \phi(3) &= 2 \\ \phi(4) &= 2 \end{aligned} \tag{9.24}$$

Now, we have seen that if (n, m) are relatively prime then

$$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m \tag{9.25}$$

Therefore, the group of automorphisms should be the same and hence

$$\mathbb{Z}^*_{nm} \cong \mathbb{Z}^*_n \times \mathbb{Z}^*_m \tag{9.26}$$

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

$$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \cdots (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^* \tag{9.27}$$

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

$$\phi(N) = \prod_i (p_i^{e_i} - p_i^{e_i - 1}) = N \prod_{p|N} (1 - \frac{1}{p}) \tag{9.28}$$

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. 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 a is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$.

On the other hand, if $p = 2$

$$(\mathbb{Z}/4\mathbb{Z})^* \cong \{\pm 1\} \tag{9.29}$$

is cyclic but

$$(\mathbb{Z}/2^e\mathbb{Z})^* = \{(-1)^a 5^b | a = 0, 1, 0 \leq b < 2^{e-2}\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{e-2}\mathbb{Z}) \tag{9.30}$$

when $e \geq 3$.

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:

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1 \qquad \text{mod}7 \tag{9.31}$$

$$5^1 = 5, \quad 5^2 = 4, \quad 5^3 = 6, \quad 5^4 = 2, \quad 5^5 = 3, \quad 5^6 = 1 \qquad \text{mod}7 \tag{9.32}$$

   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 $2, 3, 4$.

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

Exercise *Euler's theorem and Fermat's little theorem*

a.) Let G be a finite group of order n. Show that if $g \in G$ then $g^n = e$ where e is the identity element.

b.) Prove *Euler's theorem*: For all integers a relatively prime to N, $g.c.d(a, N) = 1$,

$$a^{\phi(N)} = 1\text{mod}N \tag{9.33}$$

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

$$a^p = a\text{mod}p \tag{9.34}$$

Remark: This theorem has important practical applications in *prime testing*. If we want to test whether an 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.

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:

$$a \leftrightarrow 0, b \leftrightarrow 1, c \leftrightarrow 2, \ldots \tag{9.35}$$

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:

$$ZOLPPQEBORYFZLK! \tag{9.36}$$

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. 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.

Now $\phi(n_A) = (p_A - 1)(q_A - 1)$. Next, she chooses a random thousand-digit number d_A such that $gcd(d_A, \phi(n_A)) = 1$ and computes an inverse $d_A e_A = 1\text{mod}\phi(n_A)$. This is relatively easy, because Euclid's algorithm is very fast. Thus there is some integer f so that

$$d_A e_A - f\phi(n_A) = 1 \tag{9.37}$$

That is, she solves the congruence $x = 1\text{mod}\phi(n_A)$ and $x = 0\text{mod}d_A$, 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 $a \leftrightarrow 01$, $b \leftrightarrow 02$, $\ldots$, $z \leftrightarrow 26$. (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.

Bob computes the ciphertext:

$$c := m^{e_A} \mathrm{mod} n_A \tag{9.38}$$

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

Then Alice can decode the message by computing

$$\begin{aligned} c^{d_A} \mathrm{mod} n_A &= m^{e_A d_A} \mathrm{mod} n_A \\ &= m^{1+f\phi(n_A)} \mathrm{mod} n_A \\ &= m \mathrm{mod} n_A \end{aligned} \tag{9.39}$$

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. Thus, the security of the method hinges on the inability of Eve to factor n_A into primes.

Note that the decoding will *fail* if m and n_A have a common factor. However, $n_A = p_A q_A$ and p_A, q_A are primes with thousands of digits. The probability that Bob's message is one of these is around 1 in 10^{1000}.

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

$$(n = 661643, e = 325993) \tag{9.40}$$

Bob sends her the ciphertext in four batches:

$$c_1 = 541907 \quad c_2 = 153890 \quad c_3 = 59747 \quad c_4 = 640956 \tag{9.41}$$

What is Bob's message? [19]

---

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

[19] Factor the integer $n = 541 * 1223$. Then you know p, q and hence $\phi(n) = 659880$. Now take e and compute d by using the Chinese Remainder theorem to compute $x = 1 \mathrm{mod} \phi$ and $x = 0 \mathrm{mod} e$. This gives $x = 735766201 = de$ and hence $d = 2257$. Now you can compute the message from the ciphertext $m = c^d \mathrm{mod} n$.

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

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

For an element $g \in G$ we will denote the corresponding automorphism by α_g. The value of α_g on an element $h \in H$ is denoted $\alpha_g(h)$. Thus $\alpha_g(h_1 h_2) = \alpha_g(h_1)\alpha_g(h_2)$ because α_g is a homomorphism of H to itself while we also have $\alpha_{g_1 g_2}(h) = \alpha_{g_1}(\alpha_{g_2}(h))$ because α is a homomorphism of G into the group of automorphisms $Aut(H)$.

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."

Exercise

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

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

$$(h, g)^{-1} = \left(\alpha_{g^{-1}}(h^{-1}), g^{-1}\right) \tag{10.3}$$

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. [20] This explains the funny fish product $\rtimes$: it is a combination of $\times$ with the normal subgroup symbol $\lhd$.

c.) Show that we have a short exact sequence:

$$1 \to N \to H \rtimes G \to Q \to 1 \tag{10.5}$$

[20] 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

$$(h_1, g_1)(1, g)(h_1, g_1)^{-1} = (h_1 \alpha_{g_1 g g_1^{-1}}(h_1^{-1}), g_1 g g_1^{-1}). \tag{10.4}$$

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

e.) Conversely, show that if $G = NQ$ where N is a normal subgroup of G and Q is a subgroup of G, (that is, every element of G can be written in the form $g = nq$ with $n \in N$ and $q \in Q$ and $N \cap Q = \{1\}$) then 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.

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:

$$\begin{aligned}(x_1, e)(x_2, e) &= (x_1 + x_2, e)\\ (x_1, e)(x_2, \sigma) &= (x_1 + x_2, \sigma)\\ (x_2, \sigma)(x_1, e) &= (x_2 - x_1, \sigma)\\ (x_1, \sigma)(x_2, \sigma) &= (x_1 - x_2, e)\end{aligned} \tag{10.6}$$

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:

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

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

$$\mathbb{Z} \rtimes \mathbb{Z}_2 \cong \langle x, y | x^2 = 1 \qquad y^2 = 1 \rangle \tag{10.8}$$

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 but with $H = \mathbb{Z}/N\mathbb{Z}$. This defines the *finite dihedral group* D_N, which we will meet again as the group of symmetries of the regular N-gon in the plane. Note that the presentation is now

$$(\mathbb{Z}/N\mathbb{Z}) \rtimes \mathbb{Z}_2 \cong \langle r, s | s^2 = 1, \qquad r^N = 1, \qquad srs = r^{-1} \rangle \tag{10.9}$$

Indeed, note that $\mathcal{N} = \{(x, e) | x = 0 \mathrm{mod} N\} \subset \mathbb{Z} \rtimes \mathbb{Z}_2$ is a normal subgroup and

$$(\mathbb{Z}/N\mathbb{Z}) \rtimes \mathbb{Z}_2 \cong (\mathbb{Z} \rtimes \mathbb{Z}_2)/\mathcal{N}. \tag{10.10}$$

Example 10.3: We will study below group actions on spaces. In particular we will look at the Euclidean group Euc(d) of isometries of the affine space $\mathbb{E}^d$ modeled on $\mathbb{R}^d$ with Euclidean metric. For now, we choose an origin and identify $\mathbb{E}^d \cong \mathbb{R}^d$ and then to a pair $R \in O(d)$ and $v \in \mathbb{R}^d$ we can associate the isometry: [21]

$$\{R|v\} : x \mapsto Rx + v \tag{10.11}$$

[21] Logically, since we operate with R first and then translate by v the notation should have been $\{v|R\}$, but unfortunately the notation used here, known as the Seitz notation, is the standard one.

In this notation the group multiplication law is

$$\{R_1|v_1\}\{R_2|v_2\} = \{R_1R_2|v_1 + R_1v_2\} \tag{10.12}$$

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 $O(d)$:

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

and $\pi : \{R|v\} \to R$ is a surjective homomorphism $\mathrm{Euc}(d) \to O(d)$. Similarly the Poincaré group is the semidirect product of the translation and Lorentz group.

Example 10.4: *Kaluza-Klein theory.* In Kaluza-Klein theory we study general relativity on a product manifold 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. 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 $\psi_f : (x, y) \to (f(x), y)$ with $f \in Diff(X)$. 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 point we make here we might as well take $\mathcal{G} = Map(X, Diff(Y))$, so an element g is a family of diffeomorphisms: $x \to g_x : y \to g(y; x)$. That is, for fixed x, the map $y \mapsto g(y; x)$ is a diffeomorphism of Y. Then we take $\mathcal{G}$ to be the subgroup of diffeomorphisms of $Diff(X \times Y)$ of the form $(x, y) \to (x, g(y; x))$. Note that within $Diff(X \times Y)$ we can write the subgroup

$$\mathcal{G}\mathcal{D} \tag{10.14}$$

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

$$\begin{aligned} \psi_f\psi_g\psi_f^{-1} : (x, y) &\to (f^{-1}(x), y) \\ &\to (f^{-1}(x), g(y; f^{-1}(x))) \\ &\to (x, g(y; f^{-1}(x))) \end{aligned} \tag{10.15}$$

so this subgroup is a semidirect product. This is a model for the group of gauge transformations in Kaluza-Klein theory, where $\mathcal{D}$ is the diffeomorphism group of the large spacetime. Typically, Y is endowed with a fixed metric ds^2_Y and the diffeomorphism symmetry of Y is (spontaneously) broken down to the group of isometries of Y, $Isom(Y, ds^2_Y)$. Then $\mathcal{G}$ is taken to be the unbroken subgroup $Map(X, Isom(Y, ds^2_Y))$ and is interpreted as a group of gauge transformations of a gauge theory on X coupled to general relativity on X.

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

$$Z(g) \cong \prod_{i=1}^{n} \left(\mathbb{Z}_i^{\ell_i} \rtimes S_{\ell_i} \right) \tag{10.16}$$

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 [22]

$$\Psi : H \rtimes_\alpha G \to H \times G \tag{10.17}$$

Exercise

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. [23]

---

11. Group Extensions and Group Cohomology

11.1 Group Extensions

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

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

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

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

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

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

[23] *Answer:* Note that $n_1 q_1 n_2 q_2 = n_1 n_2 (n_2^{-1} q_1 n_2 q_1^{-1}) q_1 q_2$. However, if both N and Q are normal subgroups then $(n_2^{-1} q_1 n_2 q_1^{-1}) \in N \cap Q = \{1\}$. Therefore $n_1 q_1 n_2 q_2 = n_1 n_2 q_1 q_2$ is the direct product structure.

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota_1} & G_1 & \xrightarrow{\pi_1} & Q & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota_2} & G_2 & \xrightarrow{\pi_2} & Q & \longrightarrow & 1 \end{array} \tag{11.4}$$

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.

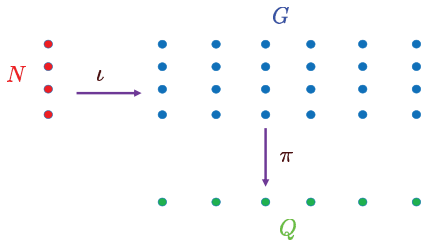


Figure 9: Illustration of a group extension $1 \to N \to G \to Q \to 1$ as an N-bundle over Q.

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 9. 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.[24] Note that in general $s(\pi(g)) \neq g$. This is obvious from Figure 9: 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 9 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:

$$g(s(\pi(g)))^{-1} \tag{11.5}$$

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

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

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

$$g = \iota(n)s(q) \tag{11.7}$$

[24] By the axiom of choice. For continuous groups such as Lie groups there might or might not be continuous sections.

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

$$\iota(n_1)s(q_1) = \iota(n_2)s(q_2) \tag{11.8}$$

Then we rewrite this as

$$\iota(n_2^{-1}n_1) = s(q_2)s(q_1)^{-1} \tag{11.9}$$

Now, applying π we learn that $1 = q_2\pi(s(q_1)^{-1}) = q_2(\pi(s(q_1))^{-1}) = q_2q_1^{-1}$, so $q_1 = q_2$. But that implies $n_1 = n_2$. Therefore, *as a set* G can be identified with $N \times Q$.

Now, given an extension and a choice of section s we define a map

$$\omega : Q \to \mathrm{Aut}(N) \tag{11.10}$$

denoted by

$$q \mapsto \omega_q \tag{11.11}$$

where the definition of ω_q is given by

$$\iota(\omega_q(n)) = s(q)\iota(n)s(q)^{-1} \tag{11.12}$$

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 $\omega_q(n_1n_2) = \omega_q(n_1)\omega_q(n_2)$, therefore we really have a homomorphism (11.10).

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. 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. Let us see how close ω comes to being a group homomorphism:

$$\begin{aligned} \iota\left(\omega_{q_1} \circ \omega_{q_2}(n)\right) &= s(q_1)\iota(\omega_{q_2}(n))s(q_1)^{-1} \\ &= s(q_1)s(q_2)\iota(n)(s(q_1)s(q_2))^{-1} \end{aligned} \tag{11.13}$$

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 (11.13) we know that

$$\omega_{q_1} \circ \omega_{q_2} = \omega_{q_1 q_2} \tag{11.14}$$

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 (11.7) 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 (11.7). Write

$$\iota(n)s(q)\iota(n')s(q') = \iota(n)\left(s(q)\iota(n')s(q)^{-1}\right)s(qq') \tag{11.15}$$

Note that

$$s(q)\iota(n')s(q)^{-1} = \iota(\omega_q(n')) \tag{11.16}$$

so

$$\iota(n_1)s(q_1)\iota(n_2)s(q_2) = \iota\left(n_1\omega_{q_1}(n_2)\right)s(q_1q_2) \tag{11.17}$$

But this just means that

$$\Psi(n,q) = \iota(n)s(q) \tag{11.18}$$

is in fact an isomorphism $\Psi : N \rtimes_\omega Q \to G$. Indeed equation (11.17) just says that:

$$\Psi(n_1,q_1)\Psi(n_2,q_2) = \Psi((n_1,q_1)\cdot_\omega (n_2,q_2)) \tag{11.19}$$

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 §11.4 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.

Exercise

If $s : Q \to G$ is any section of π show that for all $q \in Q$,

$$s(q^{-1}) = s(q)^{-1}n = n's(q)^{-1} \tag{11.20}$$

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

$$1 \longrightarrow H' \xrightarrow{\iota} H \xrightarrow{\pi} H'' \longrightarrow 1 \tag{11.21}$$

and a homomorphism

$$\rho : G'' \to H'' \tag{11.22}$$

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

$$G := \{(h, g'') | \pi(h) = \rho(g'')\} \subset H \times G'' \tag{11.23}$$

and is an extension of the form

$$1 \longrightarrow H' \xrightarrow{\iota} G \xrightarrow{\tilde{\pi}} G'' \longrightarrow 1 \tag{11.24}$$

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H' & \longrightarrow & G & \xrightarrow{\tilde{\pi}} & G'' & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \tilde{\rho}} & & \downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & H' & \longrightarrow & H & \xrightarrow{\pi} & H'' & \longrightarrow & 1 \end{array} \tag{11.25}$$

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

Exercise *Choice of splitting and the Euclidean group* $\mathrm{Euc}(d)$

As we noted, the Euclidean group $\mathrm{Euc}(d)$ 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.

Show that a change of origin corresponds to a change of 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, [25] is a group $\tilde{G}$ such that

$$1 \to A \quad \stackrel{\iota}{\to} \quad \tilde{G} \quad \stackrel{\pi}{\to} \quad G \to 1 \tag{11.26}$$

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

[25] Some authors say an extension of A by 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:

$$1 \to \mathbb{Z}_2 \to SU(2) \to SO(3) \to 1 \tag{11.27}$$

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. A simple example is the spin representation of the rotation group. We will explain this relation in more detail later, but for the moment the reader might find it useful to think about G as 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. 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. 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.

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

$$\pi(s(g)) = g \qquad \forall g \in G \tag{11.28}$$

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

$$\iota(a)s(g) \to (a, g) \tag{11.29}$$

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 (11.26) 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:

$$s(g_1)s(g_2)\left(s(g_1g_2)\right)^{-1}. \tag{11.30}$$

Now the quantity (11.30) 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

$$\iota(f_s(g_1, g_2)) := s(g_1)s(g_2)\left(s(g_1g_2)\right)^{-1}. \tag{11.31}$$

That is, we can write:

$$s(g_1)s(g_2) = \iota(f_s(g_1, g_2))s(g_1g_2) \tag{11.32}$$

The function f_s satisfies the important *cocycle identity*

$$\boxed{f(g_1, g_2g_3)f(g_2, g_3) = f(g_1, g_2)f(g_1g_2, g_3)} \tag{11.33}$$

Exercise

Verify (11.33) by using (11.31) to compute $s(g_1g_2g_3)$ in two different ways.

(Note that simply substituting (11.31) into (11.33) 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

$$f(g, 1) = f(1, g) = f(1, 1) \qquad \forall g \in G \tag{11.34}$$

b.) Show that

$$f(g, g^{-1}) = f(g^{-1}, g). \tag{11.35}$$

Now we introduce some fancy terminology:

Definition: In general

1. A *2-cochain on G with values in A*, $C^2(G,A)$ is a function
$$f : G \times G \to A \tag{11.36}$$
2. A *2-cocycle* $f \in Z^2(G,A)$ is a 2-cochain $f : G \times G \to A$ satisfying (11.33).

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 §11.5 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 (11.31).

Now, if we choose a different section $\hat{s}$ then
$$\hat{s}(g) = s(g)\iota(t(g)) \tag{11.37}$$
for some function $t : G \to A$. It is easy to check that
$$f_{\hat{s}}(g_1,g_2) = f_s(g_1,g_2)t(g_1)t(g_2)t(g_1g_2)^{-1} \tag{11.38}$$
where we have used that $\iota(A)$ is central in $\tilde{G}$.

Definition: In general two 2-cochains f and $\hat{f}$ are said to *differ by a coboundary* if they satisfy
$$\hat{f}(g_1,g_2) = f(g_1,g_2)t(g_1)t(g_2)t(g_1g_2)^{-1} \tag{11.39}$$
for some function $t : G \to A$.

One can readily check 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. Moreover, this set carries a natural structure of an abelian group.

As mentioned above, the group multiplication making $H^2(G,A)$ into an abelian group is simply defined by
$$(f_1 \cdot f_2)(g,g') = f_1(g,g') \cdot f_2(g,g') \tag{11.40}$$
where we are writing the product in A multiplicatively. This descends to a well-defined muiltiplication on cohomology classes: $[f_1] \cdot [f_2] := [f_1 \cdot f_2]$.

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 $H^2(G,A)$. Moreover, considering $H^2(G,A)$ itself as an abelian group, the identity element corresponds to the split extension $A \times G$.

Proof: From (11.31)(11.33)(11.38) 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

$$\begin{aligned} s'(g_1)s'(g_2) &= \psi(s(g_1))\psi(s(g_2)) \\ &= \psi(s(g_1)s(g_2)) \\ &= \psi(\iota(f_s(g_1,g_2))s(g_1g_2)) \\ &= \psi(\iota(f_s(g_1,g_2)))\psi(s(g_1g_2)) \\ &= \iota'(f_s(g_1,g_2))s'(g_1g_2) \end{aligned} \tag{11.41}$$

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:

$$(a_1,g_1)(a_2,g_2) := (a_1a_2f(g_1,g_2), g_1g_2) \tag{11.42}$$

Now suppose that we use two 2-cocycles f and f' which are related by a coboundary as in (11.39) above. Then we claim that the map $\psi : \tilde{G} \to \tilde{G}'$ defined by

$$\psi : (a,g) \to (at(g)^{-1}, g) \tag{11.43}$$

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 $\tilde{G}'$. ♠

Remark: Using a coboundary one can usefully simplify cocycles. For example, by setting $t(1) = f(1,1)^{-1}$ we may assume $f(1,1) = 1$. Then, by (11.34) we have $f(g,1) = f(1,g) = 1$ for all g. Similarly, if $g \neq g^{-1}$ we may put $f(g,g^{-1}) = f(g^{-1},g) = 1$. If $g = g^{-1}$ then we might not be able to set $f(g,g) = 1$. We can "preserve this gauge" with further coboundary transformations that satisfy $t(1) = 1$ and $t(g^{-1}) = t(g)^{-1}$.

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. 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

$$(1, \sigma_2) \cdot (1, \sigma_2) = (f(\sigma_2, \sigma_2), 1) = (\sigma_1, 1) \tag{11.44}$$

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,

$$\begin{aligned} \Psi &: (\sigma_1, 1) \to \omega^2 = -1 \\ \Psi &: (1, \sigma_2) \to \omega \end{aligned} \tag{11.45}$$

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:

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{11.46}$$

Recall that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 2. The generalization of the previous example to an odd prime p is extremely instructive. So, let us study in detail the extensions

$$1 \to \mathbb{Z}_p \to G \to \mathbb{Z}_p \to 1 \tag{11.47}$$

where we will write our groups multiplicatively. Now, using methods of topology one can show that [26]

$$H^2(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p. \tag{11.48}$$

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 (11.48)? The answer is that there can be nonisomorphic extensions (11.26) involving the same group $\tilde{G}$. To see this, let us examine in detail the standard extension:

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 1 \tag{11.49}$$

We write the first, second and third groups in this sequence as

$$\begin{aligned} \mathbb{Z}_p &= \langle \sigma_1 | \sigma_1^p = 1 \rangle \\ \mathbb{Z}_{p^2} &= \langle \alpha | \alpha^{p^2} = 1 \rangle \\ \mathbb{Z}_p &= \langle \sigma_2 | \sigma_2^p = 1 \rangle \end{aligned} \tag{11.50}$$

respectively. Then the first injection must take

$$\iota(\sigma_1) = \alpha^p \tag{11.51}$$

[26] You can also show it by examining the cocycle equation directly.

since it must be an injection and it must take an element of order p to an element of order p. The standard sequence then takes the second arrow to be reduction modulo p, so

$$\pi(\alpha) = \sigma_2 \tag{11.52}$$

While there is no choice in ι we are making a choice in defining π. We will return to this shortly.

Now, with the choice (11.52), we try to choose a section of π. Let us try to make it a homomorphism. Therefore we must take $s(1) = 1$. What about $s(\sigma_2)$? Since $\pi(s(\sigma_2)) = \sigma_2$ we have a choice: $s(\sigma_2)$ could be any of

$$\alpha, \alpha^{p+1}, \alpha^{2p+1}, \ldots, \alpha^{(p-1)p+1} \tag{11.53}$$

Here we will make the simplest choice $s(\sigma_2) = \alpha$. 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 $s(\sigma_2) = \alpha$, if s were a homomorphism then we would be forced to take:

$$\begin{aligned} s(1) &= 1 \\ s(\sigma_2) &= \alpha \\ s(\sigma_2^2) &= \alpha^2 \\ \vdots \qquad &\quad \vdots \\ s(\sigma_2^{p-1}) &= \alpha^{p-1} \end{aligned} \tag{11.54}$$

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 $s(\sigma_2^p) = \alpha^p$. But because $\sigma_2^p = 1$ and $\alpha^p \neq 1$ these requirements are incompatible. Therefore, with this choice of section we find a nontrivial cocycle as follows:

$$s(\sigma_2^k)s(\sigma_2^\ell)s(\sigma_2^{k+\ell})^{-1} = \begin{cases} 1 & k+\ell < p \\ \alpha^p & p \leq k+\ell \end{cases} \tag{11.55}$$

and therefore,

$$f(\sigma_2^k, \sigma_2^\ell) = \begin{cases} 1 & k+\ell < p \\ \sigma_1 & p \leq k+\ell \end{cases} \tag{11.56}$$

In these equations we assume $1 \leq k, \ell \leq p-1$. We know the cocycle is nontrivial because $\mathbb{Z}_p \times \mathbb{Z}_p$ is not isomorphic to $\mathbb{Z}_{p^2}$.

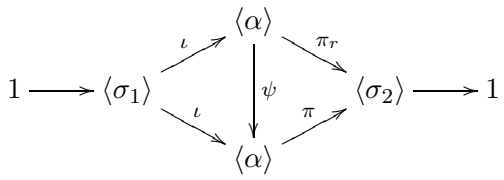
But now let us use the group structure on the group cohomology. $[f]^r$ is the cohomology class represented by

$$f^r(\sigma_2^k, \sigma_2^\ell) = \begin{cases} 1 & k+\ell < p \\ \sigma_1^r & p \leq k+\ell \end{cases} \tag{11.57}$$

This corresponds to replacing (11.52) by

$$\pi_r(\alpha) = (\sigma_2)^r \tag{11.58}$$

and the sequence will still be exact, i.e. $\ker(\pi_r) = \mathrm{im}(\iota)$, if $(r,p) = 1$, that is, if we compose the standard projection with an automorphism of $\mathbb{Z}_p$. Thus π_r also defines an extension of the form (11.49). But we claim that it is not isomorphic to the standard extension! To see this let us try to construct ψ so that



(11.59)

In order for the triangle on the right to commute we must have $\psi(\alpha) = \alpha^r$, but then the triangle on the left will not commute. Thus the extensions $\pi_1, \ldots, \pi_{p-1}$, all related by outer automorphisms of the quotient group $\mathbb{Z}_p = \langle\sigma_2\rangle$, define inequivalent extensions with the same group $\mathbb{Z}_{p^2}$ in the middle.

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

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \to 1 \tag{11.60}$$

and then there is an orbit of $(p-1)$ nontrivial extensions of the form

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 1 \tag{11.61}$$

acted on by $\mathrm{Aut}(\mathbb{Z}_p)$.

Example 3: Let us analyze in detail the extension

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_8 \to \mathbb{Z}_4 \to 1 \tag{11.62}$$

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

$$\begin{aligned} s(\omega) &= \alpha \\ s(\omega^2) &= \alpha^2 \\ s(\omega^3) &= \alpha^3 \end{aligned} \tag{11.63}$$

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

$$f(\omega,\omega^3)=f(\omega^2,\omega^2)=f(\omega^2,\omega^3)=f(\omega^3,\omega^3)=\alpha^4=\sigma. \tag{11.64}$$

Example 4.. Nonabelian groups can also have central extensions. For example the symmetric group S_n has one nontrivial central extension by $\mathbb{Z}_2$. To define it we let $\sigma_i=(i,i+1)$, $1\leq i\leq n-1$ be the transpositions generating S_n. Then $\hat{S}_n$ is generated by $\hat{\sigma}_i$ and a central element z satisfying the relations:

$$\begin{aligned} z^2&=1\\ \hat{\sigma}_i^2&=z\\ \hat{\sigma}_i\hat{\sigma}_{i+1}\hat{\sigma}_i&=\hat{\sigma}_{i+1}\hat{\sigma}_i\hat{\sigma}_{i+1}\\ \hat{\sigma}_i\hat{\sigma}_j&=z\hat{\sigma}_j\hat{\sigma}_i \qquad\qquad j>i+1 \end{aligned} \tag{11.65}$$

There is an elegant realization of this group using Clifford algebras.

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.

Exercise

Choosing the natural section $s:\sigma_i\to\hat{\sigma}_i$ in example 2 find the corresponding cocycle f_s.

Exercise

Show that the associative law for the twisted product (11.42) is equivalent to the cocycle condition on the 2-cochain f.

Exercise

a.) Compute the group commutator:

$$[(a_1, g_1), (a_2, g_2)] = \left(\frac{f(g_1 g_2, g_1^{-1} g_2^{-1})}{f(g_2 g_1, g_1^{-1} g_2^{-1})} \frac{f(g_1, g_2)}{f(g_2, g_1)}, g_1 g_2 g_1^{-1} g_2^{-1} \right) \tag{11.66}$$

b.) Suppose G is abelian. Show that $\tilde{G}$ is abelian iff $f(g_1, g_2)$ is symmetric.

Exercise

Using methods of topology one can prove that

$$H^2(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \tag{11.67}$$

There are 4 isomorphisms classes of groups which fit in the central extensions of $\mathbb{Z}_2 \times \mathbb{Z}_2$ by $\mathbb{Z}_2$, two of which are nonabelian groups of order 8. They are:

$$\begin{aligned} &1 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\ &1 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\ &1 \to \mathbb{Z}_2 \to Q \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \\ &1 \to \mathbb{Z}_2 \to D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1 \end{aligned} \tag{11.68}$$

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

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \& \qquad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \tag{11.69}$$

(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

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \& \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{11.70}$$

Question: 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 (11.68) while (11.67) is order 8.

11.3 Heisenberg extensions

In all the examples above (except for Q and D_4 in (11.68)) 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:

$$[\hat{q}, \hat{p}] = i\hbar \tag{11.71}$$

One realization of these operator relations is in terms of wavefunctions $\psi(q)$ where we write:

$$\begin{aligned} (\hat{q} \cdot \psi)(q) &= q\psi(q) \\ (\hat{p} \cdot \psi)(q) &= -i\hbar \frac{d}{dq}\psi(q) \end{aligned} \tag{11.72}$$

Now, let us consider the unitary operators

$$\begin{aligned} U(\alpha) &:= \exp[i\alpha\hat{p}] \\ V(\alpha) &:= \exp[i\beta\hat{q}] \end{aligned} \tag{11.73}$$

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:

$$U(\alpha)V(\beta) = e^{i\hbar\alpha\beta}V(\beta)U(\alpha) \tag{11.74}$$

Therefore, the group generated by the operators $U(\alpha)$ and $V(\alpha)$ for $\alpha \in \mathbb{R}$, which we'll denote $\mathrm{Heis}(\mathbb{R} \times \mathbb{R})$ fits in a central extension:

$$1 \to U(1) \to \mathrm{Heis}(\mathbb{R} \times \mathbb{R}) \to \mathbb{R} \times \mathbb{R} \to 1 \tag{11.75}$$

Let us now step back and think more generally about central extensions of G by A where G is *also abelian*. From the exercise (11.66) we know that for G abelian the commutator is

$$[(a_1, g_1), (a_2, g_2)] = \left(\frac{f(g_1, g_2)}{f(g_2, g_1)}, 1 \right) \tag{11.76}$$

(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

$$\kappa(g_1, g_2) = \frac{f(g_1, g_2)}{f(g_2, g_1)} \tag{11.77}$$

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*:
$$\kappa(g_1, g_2) = \kappa(g_2, g_1)^{-1} \tag{11.78}$$

4. κ is *alternating*:
$$\kappa(g, g) = 1 \tag{11.79}$$

5. κ is *bimultiplicative*:
$$\kappa(g_1 g_2, g_3) = \kappa(g_1, g_3)\kappa(g_2, g_3) \tag{11.80}$$
$$\kappa(g_1, g_2 g_3) = \kappa(g_1, g_2)\kappa(g_1, g_3) \tag{11.81}$$

All of these properties except perhaps the last are obvious. To prove the bimultiplicative properties (it suffices to prove just one) we rewrite (11.80) as

$$f(g_1 g_2, g_3) f(g_3, g_2) f(g_3, g_1) = f(g_2, g_3) f(g_1, g_3) f(g_3, g_1 g_2) \tag{11.82}$$

Now multiply the equation by $f(g_1, g_2)$ and use the fact that A is abelian to write

$$(f(g_1, g_2) f(g_1 g_2, g_3)) f(g_3, g_2) f(g_3, g_1) = f(g_2, g_3) f(g_1, g_3)(f(g_1, g_2) f(g_3, g_1 g_2)) \tag{11.83}$$

We apply the cocycle identity on both the LHS and the RHS (and also use the fact that G is abelian) to get

$$f(g_2, g_3) f(g_1, g_2 g_3) f(g_3, g_2) f(g_3, g_1) = f(g_2, g_3) f(g_1, g_3) f(g_3, g_1) f(g_3 g_1, g_2) \tag{11.84}$$

Now canceling some factors and using that A is abelian we have

$$f(g_1, g_2 g_3) f(g_3, g_2) = f(g_1, g_3) f(g_3 g_1, g_2) \tag{11.85}$$

Now use the fact that G is abelian to write this as

$$f(g_1, g_3 g_2) f(g_3, g_2) = f(g_1, g_3) f(g_1 g_3, g_2) \tag{11.86}$$

which is the cocycle identity. This proves the bimultiplicative property (11.80). ♠

For a large class of abelian groups G, namely those which are (noncanonically!) products of finitely generated discrete abelian groups, tori, and vector spaces, 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

$$\kappa : G \times G \to U(1) \tag{11.87}$$

which are alternating (and hence skew).

For a proof of the theorem see[27]

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.

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

$$M(a,b,c) := \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \tag{11.88}$$

The multiplication law is easily worked out to be

$$M(a,b,c)M(a',b',c') = M(a+a', b+b', c+c'+ab') \tag{11.89}$$

[27] D. Freed, G. Moore, G. Segal, "The uncertainty of fluxes," Commun.Math.Phys. 271 (2007) 247-274, arXiv:hep-th/0605198, Proposition A.1.

Therefore, as abelian groups we have an extension

$$0 \to R \to \mathrm{Heis}(R \times R) \to R \times R \to 0 \tag{11.90}$$

with cocycle $f((a,b),(a',b')) = ab'$ and commutator

$$\kappa((a,b),(a',b')) = ab' - a'b \tag{11.91}$$

We now relate this notion of Heisenberg group to the Heisenberg extensions above. First, let us generalize the Heisenberg groups 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

$$0 \to \mathcal{Z} \to \tilde{G} \to R \times R \to 0 \tag{11.92}$$

by the law

$$(z_1,(a,b)) \cdot (z_2,(a',b')) = (z_1 + z_2 + c(a,b'),(a+a',b+b')) \tag{11.93}$$

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 nondegenerate.

Example: *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

$$U = \begin{pmatrix} \bar{1} & \bar{1} & 0 \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad V = \begin{pmatrix} \bar{1} & 0 & 0 \\ 0 & \bar{1} & \bar{1} \\ 0 & 0 & \bar{1} \end{pmatrix} \qquad q = \begin{pmatrix} \bar{1} & 0 & \bar{1} \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix} \tag{11.94}$$

We easily check that for $a \in \mathbb{Z}$,

$$U^a = \begin{pmatrix} 1 & \bar{a} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad V^a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \bar{a} \\ 0 & 0 & 1 \end{pmatrix} \qquad q^a = \begin{pmatrix} 1 & 0 & \bar{a} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{11.95}$$

And moreover,

$$UV = qVU \qquad qU = Uq \qquad qV = Vq \tag{11.96}$$

Thus we obtain a presentation:

$$\mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n) = \langle U, V, q | U^n = V^n = q^n = 1, \quad UV = qVU, \quad Uq = qU, \quad Vq = qV \rangle \tag{11.97}$$

It is interesting to look at the Heisenberg extension

$$1 \to \mathbb{Z}_n \to \mathrm{Heis}(\mathbb{Z}_n \times \mathbb{Z}_n) \to \mathbb{Z}_n \times \mathbb{Z}_n \to 1 \tag{11.98}$$

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

$$f\left((\omega_1^s, \omega_2^t),(\omega_1^{s'}, \omega_2^{t'})\right) := \omega_3^{st'} \tag{11.99}$$

The corresponding commutator function is

$$\kappa\left((\omega_1^s,\omega_2^t),(\omega_1^{s'},\omega_2^{t'})\right) := \omega_3^{st'-ts'} \tag{11.100}$$

To connect with our general theory of extensions let $U := (1,(\omega_1,1))$, $V := (1,(1,\omega_2))$ and compute

$$\begin{aligned} UV &= (f((\omega_1,1),(1,\omega_2)),(\omega_1,\omega_2)) \\ &= (\omega_3,(\omega_1,\omega_2)) \\ VU &= (f((1,\omega_2),(\omega_1,1)),(\omega_1,\omega_2)) \\ &= (1,(\omega_1,\omega_2)) \end{aligned} \tag{11.101}$$

or in other words, since the center is generated by $q = (\omega_3,(1,1))$ we can write:

$$UV = qVU \tag{11.102}$$

Remarks

1. Let us compare a general Heisenberg extension

$$1 \to \mathcal{Z} \to \tilde{G} \to G \to 0 \tag{11.103}$$

with (11.92)(11.93). The difference is that G has been split into $R \times R$. For a general Heisenberg extension with commutator function κ we can define a *Lagrangian subgroup* to be a maximal subgroup $L \subset G$ such that $\kappa(g_1,g_2) = 1$ for all pairs $(g_1,g_2) \in L$. Since κ is nondegenerate there will be a complementary Lagrangian subgroup L' so that $G = L \times L'$. However, the maximal subgroup is in general *not* unique and so this decomposition of G is noncanonical.

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 and its dual $V^\vee$ 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.

Exercise

a.) Prove (11.74) by using the action on wavefunctions (11.72).

b.) Show that the choice of section

$$s(\alpha,\beta) = U(\alpha)V(\beta) \tag{11.104}$$

leads to the cocycle

$$f((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{i\hbar(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_1\beta_2)} \tag{11.105}$$

c.) Show that the choice of section

$$s(\alpha,\beta) = \exp[i\hbar(\alpha\hat{p}+\beta\hat{q})] \tag{11.106}$$

leads to the cocycle

$$f((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{\frac{i}{2}\hbar(\alpha_1\beta_2-\alpha_2\beta_1)} \tag{11.107}$$

d.) Show that in both cases the commutator function is

$$\kappa((\alpha_1,\beta_1),(\alpha_2,\beta_2) = e^{i\hbar(\alpha_1\beta_2-\alpha_2\beta_1)} \tag{11.108}$$

Exercise *Alternating implies skew*

Show that a map $\kappa : G \times G \to A$ which satisfies the bimultiplicative identity (11.80) and the alternating identity (11.79) is also skew, that is, satisfies (11.78).

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. [28]

While these are not - strictly speaking - Heisenberg extensions people will often refer to them as Heisenberg extensions. We might call them "degenerate Heisenberg extensions."

11.4 General Extensions

Let us briefly return to the general extension (11.1). We might ask what happens if we try to apply the reasoning of the previous section to this general case. Thus, we are now not assuming that N or Q is abelian.

What we showed is that for *any* group extension a choice of a section automatically gives us two maps:

1. $\omega_s : Q \to \mathrm{Aut}(N)$
2. $f_s : Q \times Q \to N$

[28] The center is generated by q, U^m, V^m and is $\mathbb{Z}_n \times \mathbb{Z}_k \times \mathbb{Z}_k$.

defined by

$$\iota(\omega_{s,q}(n)) = s(q)\iota(n)s(q)^{-1} \tag{11.109}$$

and

$$s(q_1)s(q_2) = \iota(f_s(q_1,q_2))s(q_1,q_2) \tag{11.110}$$

respectively.

Now (11.109) 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. Rather, using (11.109) and (11.110) we can derive a twisted version of the homomorphism rule:

$$\omega_{s,q_1} \circ \omega_{s,q_2} = I(f_s(q_1,q_2)) \circ \omega_{s,q_1q_2} \tag{11.111}$$

Recall that $I(a)$ denotes the inner automorphism given by conjugation by a.

Moreover, using (11.110) 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:

$$\omega_{s,q_1}(f_s(q_2,q_3))f_s(q_1,q_2q_3) = f_s(q_1,q_2)f_s(q_1q_2,q_3) \tag{11.112}$$

Note the difference from (11.33) is in the action of ω on the first term. Also, the order of the terms is very important since we no longer assume that N is abelian.

Conversely, given the data of two maps:

1. A map $f : Q \times Q \to N$
2. A map $\omega : Q \to \mathrm{Aut}(N)$

satisfying (11.111) and (11.112) we can construct an extension (11.1) with the multiplication law:

$$(n_1,q_1) \cdot_{f,\omega} (n_2,q_2) := (n_1\omega_{q_1}(n_2)f(q_1,q_2), q_1q_2) \tag{11.113}$$

With a few lines of algebra, using the identities (11.111) and (11.112) one can check the associativity law. Note that this formula simultaneously generalizes the twisted product of a semidirect product (10.2) and the twisted product of a central extension (11.42).

If we change the choice of section by a function $t : Q \to N$ then we have

$$\tilde{s}(q) = \iota(t(q))s(q) \tag{11.114}$$

and one easily computes that we now have

$$\omega_{\tilde{s},q} = I(t(q)) \circ \omega_{s,q} \tag{11.115}$$

$$f_{\tilde{s}}(q_1,q_2) = t(q_1)\omega_{s,q_1}(t(q_2))f_s(q_1,q_2)t(q_1q_2)^{-1} \tag{11.116}$$

Equation (11.116) generalizes the coboundary relation (11.39) of central extension theory.

The relations (11.115) and (11.116) define an equivalence relation on the pairs (ω, f) satisfying (11.111) and (11.112) and the theorem generalizing the main theorem of Section **** on central extensions states that isomorphism classes of extensions are in 1-1 correspondence with the equivalence classes $[(\omega, f)]$.

Exercise *Checking the group laws*

Show that (11.113) really defines a group structure.

a.) Check the associativity relation.

b.) What is the identity element? [29]

c.) Check that every element has an inverse.

Exercise

Show that for an arbitrary extension $q \mapsto [\omega_q]$ defines a homomorphism $Q \to Out(N)$, to the outer automorphisms of N.

11.4.1 Non-central extensions when N is abelian

An important special case is where $N = A$ is abelian, but $\iota(A)$ is not necessarily central in G.

Noncentral extensions of this type are useful in studying symmetries involving time-reversal and/or "charge-conjugation" (in the sense of condensed matter physics).

In this case, the inner automorphisms on N are trivial so (11.111) simplifies to a *homomorphism* $\omega : Q \to \mathrm{Aut}(N)$. Moreover, from (11.115) we see that ω is independent of the choice of section. In this case, with the action of G on A understood through ω the solutions of (11.112) modulo (11.116) define again a cohomology group $H^{2+\omega}(G, A)$, where the superscript ω reminds us that G acts on A through ω. This is a simple example of what is known as *twisted cohomology*.

The analog of Theorem *** above is:

Theorem: Let $\alpha : G \to \mathrm{Aut}(A)$ be a fixed homomorphism. Then the set of isomorphism classes of extensions of the form

$$1 \to A \to \tilde{G} \to Q \to 1 \tag{11.117}$$

which induce the automorphism α, denoted $\mathrm{Ext}^{\alpha}(G, A)$, is in 1-1 correspondence with the twisted cohomology $H^{2+\alpha}(Q, A)$.

[29] *Answer*: $(f(1,1)^{-1}, 1_Q)$.

11.5 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. Condensed matter/topological phases of matter (Kitaev; Wen; ...)
4. Three-dimensional Chern-Simons theory and three dimensional supersymmetric gauge theory.

So here we'll just give a few definitions.

11.5.1 Definition

Suppose we are given any group G and an abelian group A (written additively in this section) and a homomorphism

$$\alpha : G \to \mathrm{Aut}(A) \tag{11.118}$$

Definition: An n-cochain is a function $\phi : G^{\times n} \to A$. The space of n-cochains is denoted $C^n(G, A)$.

Note that $C^n(G, A)$ 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: $d : C^n(G, A) \to C^{n+1}(G, A)$

$$\begin{aligned}(d\phi)(g_1, \dots, g_{n+1}) := {} & \alpha_{g_1}\left(\phi(g_2, \dots, g_{n+1})\right) \\ & - \phi(g_1 g_2, g_3, \dots, g_{n+1}) + \phi(g_1, g_2 g_3, \dots, g_{n+1}) \pm \cdots + (-1)^n \phi(g_1, \dots, g_{n-1}, g_n g_{n+1}) \\ & + (-1)^{n+1} \phi(g_1, \dots, g_n)\end{aligned} \tag{11.119}$$

We interpret a 0-cochain ϕ_0 to be some element $\phi_0 = a \in A$. Then we have, for $n = 0$:

$$(d\phi_0)(g) = \alpha_g(a) - a \tag{11.120}$$

For $n = 1$ $\phi_1 : G \to A$ and the differential acts as:

$$(d\phi_1)(g_1, g_2) = \alpha_{g_1}\left(\phi_1(g_2)\right) - \phi_1(g_1 g_2) + \phi_1(g_1) \tag{11.121}$$

$$(d\phi_2)(g_1, g_2, g_3) = \alpha_{g_1}\left(\phi_2(g_2, g_3)\right) - \phi_2(g_1 g_2, g_3) + \phi_2(g_1, g_2 g_3) - \phi_2(g_2, g_3) \tag{11.122}$$

$$(d\phi_3)(g_1, g_2, g_3, g_4) = \alpha_{g_1}\left(\phi_3(g_2, g_3, g_4)\right) - \phi_3(g_1 g_2, g_3, g_4) + \phi_3(g_1, g_2 g_3, g_4) - \phi_3(g_1, g_2, g_3 g_4) + \phi_3(g_1, g_2, g_3) \tag{11.123}$$

The set of n-cocycles is defined to be the subgroup $Z^n(G,A) \subset C^n(G,A)$ that satisfy $d\phi_n = 0$.

Next, one can check that for any ϕ, $d(d\phi) = 0$. (We give a simple proof below.) Therefore, we can define a subgroup $B^n(G,A) \subset Z^n(G,A)$ by

$$B^n(G,A) := \{\phi_n | \exists \phi_{n-1} \qquad s.t. \qquad d\phi_{n-1} = \phi_n\} \tag{11.124}$$

Then the group cohomology is defined to be the quotient

$$H^n(G,A) = Z^n(G,A)/B^n(G,A) \tag{11.125}$$

Remarks:

1. 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 **** above.

2. *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

$$\varphi(hg_0, hg_1, \ldots, hg_n) = \alpha_h\left(\varphi(g_0, g_1, \ldots, g_n)\right) \tag{11.126}$$

Let $\mathcal{C}^n(G,A)$ denote the abelian group of such homogeneous group cochains. Define

$$\delta : \mathcal{C}^n(G,A) \to \mathcal{C}^{n+1}(G,A) \tag{11.127}$$

by

$$\delta\phi(g_0, \ldots, g_{n+1}) := \sum_{i=0}^{n+1} (-1)^i \varphi(g_0, \ldots, \widehat{g_i}, \ldots, g_{n+1}) \tag{11.128}$$

where $\widehat{g_i}$ means the argument is omitted. It is then very straightforward to prove that $\delta^2 = 0$. Indeed, if $\varphi \in \mathcal{C}^{n-1}(G,A)$ we compute:

$$\begin{aligned}
\delta^2\varphi(g_0, \ldots, g_{n+1}) &= \sum_{i=0}^{n+1} (-1)^i \Big(\sum_{j=0}^{i-1} (-1)^j \varphi(g_0, \ldots, \widehat{g_j}, \ldots, \widehat{g_i}, \ldots, g_{n+1}) \\
&\qquad - \sum_{j=i+1}^{n+1} (-1)^j \varphi(g_0, \ldots, \widehat{g_i}, \ldots, \widehat{g_j}, \ldots, g_{n+1}) \Big) \\
&= \sum_{0 \le j < i \le n+1} (-1)^{i+j} \varphi(g_0, \ldots, \widehat{g_j}, \ldots, \widehat{g_i}, \ldots, g_{n+1}) \\
&\qquad - \sum_{0 \le i < j \le n+1} (-1)^{i+j} \varphi(g_0, \ldots, \widehat{g_i}, \ldots, \widehat{g_j}, \ldots, g_{n+1}) \\
&= 0
\end{aligned} \tag{11.129}$$

Now, we can define an isomorphism $\psi : \mathcal{C}^n(G,A) \to C^n(G,A)$ by defining

$$\phi_n(g_1, \ldots, g_n) := \varphi_n(1, g_1, g_1g_2, \ldots, g_1 \cdots g_n) \tag{11.130}$$

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 (11.128) becomes the more complicated formula (11.119). Put more formally: there is a unique d so that $d\psi = \psi\delta$.

3. 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.

11.5.2 Interpreting the meaning of H^0

These are just fixed points of the α_g action.

11.5.3 Interpreting the meaning of H^1

Let us interpret the cohomology group $H^1(G,A)$. For simplicity let us take α to be trivial, so that $\alpha_g(a) = a$ for all $a \in A$ and $g \in G$. Then $d\phi_0 = 0$ for any 0-cochain and for a 1-cochain

$$(d\phi)(g_1,g_2) = \phi(g_2) - \phi(g_1g_2) + \phi(g_1) \tag{11.131}$$

so the equation $d\phi = 0$ is equivalent to saying that $\phi : G \to A$ is just a homomorphism.

Now, suppose we know that a 2-cocycle ϕ_2 induces the zero cohomology class, $[\phi_2] = 0$. Then we say that *a trivialization of* ϕ_2 is a choice of ϕ_1 so that $\phi_2 = d\phi_1$. Note that two different trivializations differ by a 1-cocycle and hence:

There is a 1-1 correspondence between the trivializations of trivializable 2-cocycles and elements of $H^1(G,A)$.

This is an example of a general pattern in cohomology theory: If a cocycle is trivializable, the isomorphism classes of trivializations can be identified with the cohomology of one degree lower.

Remark: Now suppose $\alpha \neq 1$. It turns out there is still a nice interpretation of $H^{1+\alpha}(G,A)$. We can study the automorphisms of extensions in Ext^α. Conjugation by elements of A are trivially such automorphisms and one can show that $H^{1+\alpha}(G,A)$ acts on $Aut(Ext^\alpha)/A$.

11.5.4 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 §11.4.

It follows from (11.111) and (11.115) that a general extension (11.1) has a canonically associated homomorphism

$$\bar\omega : Q \to \mathrm{Out}(N) \tag{11.132}$$

where $\mathrm{Out}(N)$ is the group of outer automorphisms of N.

The natural question arises: *Given a homomorphism* $\bar\omega$ *as in* (11.132) *is there a corresponding extension of* Q *by* N *inducing* $\bar\omega$*?*

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 $\mathrm{Out}(N)$. We know that for all $q_1, q_2 \in Q$

$$\xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_1q_2}^{-1} \in \mathrm{Inn}(N) \tag{11.133}$$

Therefore, for every q_1, q_2 we may *choose* an element $f(q_1,q_2) \in N$ so that

$$\xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_1q_2}^{-1} = I(f(q_1,q_2)) \tag{11.134}$$

i.e.

$$\xi_{q_1} \circ \xi_{q_2} = I(f(q_1, q_2)) \circ \xi_{q_1 q_2} \tag{11.135}$$

Of course, the choice of $f(q_1, q_2)$ is ambiguous by an element of $Z(N)$!

Equation (11.135) is of course just (11.111) written in slightly different notation. Therefore, as we saw in §11.4, if $f(q_1, q_2)$ were to satisfy the the twisted cocycle condition (11.112) then we could use (11.113) 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. Looking at the RHS of (11.112) we compute:

$$\begin{aligned} I(f(q_1, q_2) f(q_1 q_2, q_3)) &= I(f(q_1, q_2)) I(f(q_1 q_2, q_3)) \\ &= \left(\xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_1 q_2}^{-1}\right) \circ \left(\xi_{q_1 q_2} \circ \xi_{q_3} \circ \xi_{q_1 q_2 q_3}^{-1}\right) \\ &= \xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_3} \circ \xi_{q_1 q_2 q_3}^{-1} \end{aligned} \tag{11.136}$$

On the other hand, looking at the LHS of (11.112) we compute:

$$\begin{aligned} I(\xi_{q_1}(f(q_2, q_3)) f(q_1, q_2 q_3)) &= I(\xi_{q_1}(f(q_2, q_3))) I(f(q_1, q_2 q_3)) \\ &= \xi_{q_1} \circ I((f(q_2, q_3))) \circ \xi_{q_1}^{-1} \circ I(f(q_1, q_2 q_3) \\ &= \xi_{q_1} \circ \left(\xi_{q_2} \circ \xi_{q_3} \circ \xi_{q_2 q_3}^{-1}\right) \circ \xi_{q_1}^{-1} \circ \left(\xi_{q_1} \circ \xi_{q_2 q_3} \circ \xi_{q_1 q_2 q_3}^{-1}\right) \\ &= \xi_{q_1} \circ \xi_{q_2} \circ \xi_{q_3} \circ \xi_{q_1 q_2 q_3}^{-1} \end{aligned} \tag{11.137}$$

Therefore, comparing (11.136) and (11.137) we conclude that

$$I(\xi_{q_1}(f(q_2, q_3)) f(q_1, q_2 q_3)) = I(f(q_1, q_2) f(q_1 q_2, q_3)) \tag{11.138}$$

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

$$f(q_1, q_2) f(q_1 q_2, q_3) = z(q_1, q_2, q_3) \xi_{q_1}(f(q_2, q_3)) f(q_1, q_2 q_3) \tag{11.139}$$

Now, one can check (with a lot of algebra) that

1. z is a cocycle in $Z^3(Q, Z(N))$.
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 11.5.4.1 : 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

Theorem 11.5.4.2 : If $[z] = 0$ then the isomorphism classes of 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.

Note that Theorem 11.5.4.2 gives an interpretation $H^2(Q, Z(N))$ quite analogous to the interpretation of H^1 discussed in §11.5.3.

****

Next time: Do interpretations of H^0, H^1, H^2, H^3 more systematically. Consult: S. MacLane, Retiring Presidential Address, Bull. Amer. Math. Soc. 82 (1976), 1-4.

****

11.6 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 11.5.4, 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

Textbooks:

1. K. Brown, Group Cohomology
2. Karpilovsky, The Schur Multiplier

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

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 compact semisimple Lie groups, have a very beautiful classification.

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

$$1 \to \mathbb{Z}_4 \to G \to \mathbb{Z}_2 \to 1 \tag{12.3}$$

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:

$$1 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1 \tag{12.4}$$

$$1 \to \mathbb{Z}_4 \to \mathbb{Z}_8 \to \mathbb{Z}_2 \to 1 \tag{12.5}$$

$$1 \to \mathbb{Z}_4 \to D_4 \to \mathbb{Z}_2 \to 1 \tag{12.6}$$

$$1 \to \mathbb{Z}_4 \to \widetilde{D}_2 \to \mathbb{Z}_2 \to 1 \tag{12.7}$$

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:

$$\mathbb{Z}_{12}, \quad , \mathbb{Z}_2 \times \mathbb{Z}_6, \quad , D_6, \quad , \tilde{D}_3 \tag{12.9}$$

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. [30]

[30] 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.)

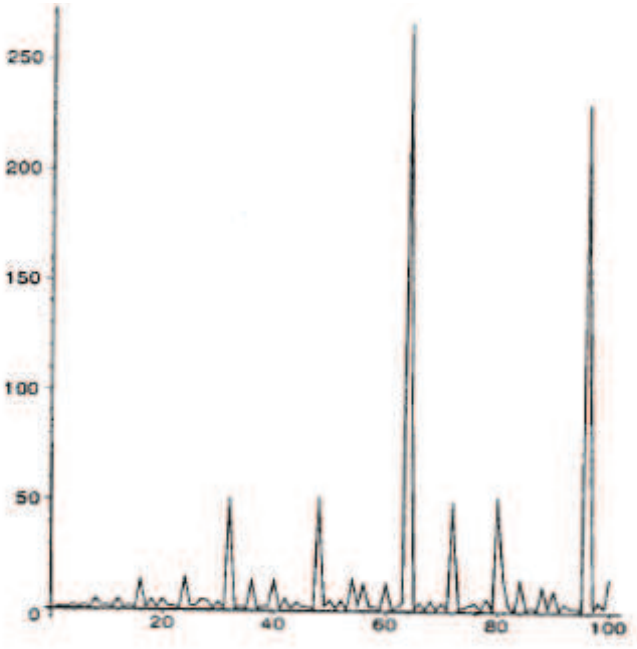


Figure 10: A plot of the number of nonisomorphic groups of order n. This plot was taken from the book by D. Joyner, *Adventures in Group Theory*.

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 10 from Joyner's book shows a plot of the number of isomorphism classes vs. order up to order 100. Figure 11 shows a log plot of the number of groups up to order 2000.

Exercise *Relating the binary dihedral and dihedral groups*

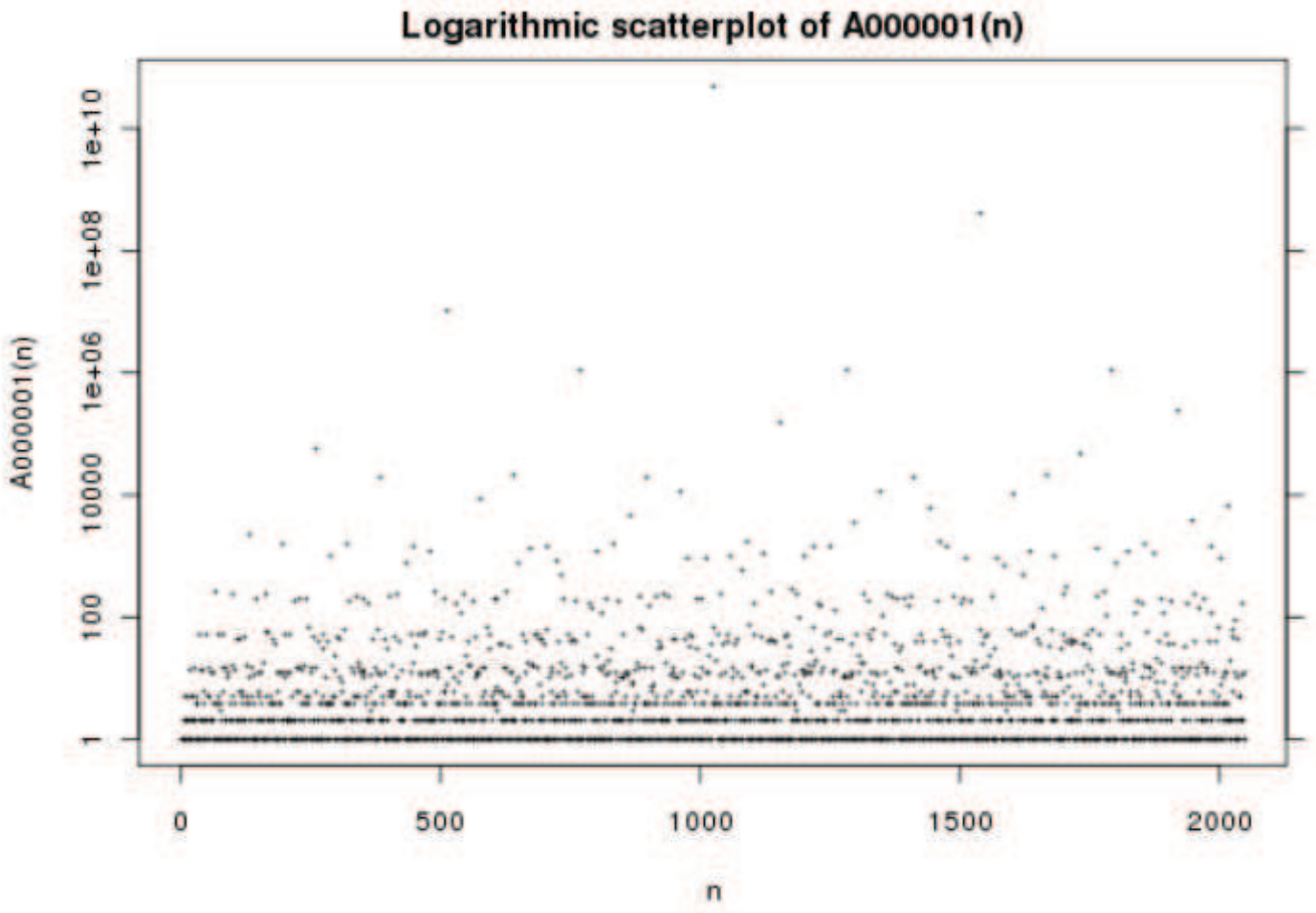


Figure 11: A logarithmic plot of the number of nonisomorphic groups of order n out to $n \leq 2000$. This plot was taken from online encyclopedia of integer sequences, OEIS.

Show that $\widetilde{D}_n$ is a double-cover of D_n which fits into the exact sequence:

$$\begin{array}{ccccccccc} & & \mathbb{Z}_2 & = & \mathbb{Z}_2 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & \mathbb{Z}_{2n} & \longrightarrow & \widetilde{D}_n & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 1 & \longrightarrow & \mathbb{Z}_n & \longrightarrow & D_n & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 1 \end{array} \tag{12.10}$$

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

$$0 \to \mathbb{Z}/gcd(p,q)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/lcm(p,q)\mathbb{Z} \to 0 \tag{12.11}$$

and in particular, if p, q are relatively prime then

$$\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}. \tag{12.12}$$

It thus follows that if n has prime decomposition

$$n = \prod_i p_i^{e_i} \tag{12.13}$$

then

$$\mathbb{Z}/n\mathbb{Z} \cong \oplus_i \mathbb{Z}/p_i^{e_i}\mathbb{Z} \tag{12.14}$$

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:

$$\begin{aligned} G &= G_2 \oplus G_3 \oplus G_5 \oplus G_7 \oplus \cdots \\ &= \oplus_{p \text{ prime}} G_p \end{aligned} \tag{12.15}$$

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:

$$G_p = \oplus_i \mathbb{Z}/(p^{n_i}\mathbb{Z}) \tag{12.16}$$

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

$$s_1 m_1 + s_2 m_2 = 1 \tag{12.17}$$

Therefore any element g can be written as

$$g = s_1(m_1 g) + s_2(m_2 g) \tag{12.18}$$

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 (12.18) implies $a = 0$. Thus,

$$G = m_1 G \oplus m_2 G \tag{12.19}$$

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 (12.18) we see that $g = s_1 m_1 g = m_1(s_1 g) \in m_1 G$.

Thus, we can decompose

$$G = \oplus G_p \tag{12.20}$$

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 (12.16). 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. One proves Cauchy's theorem for abelian groups by induction on the order. If p divides $|G|$ and G is not $\mathbb{Z}/p\mathbb{Z}$ then G has a nontrivial proper subgroup H. Then p divides H or G/H. In either case there is an element of order p. In the second case one needs to argue a little further to produce an element in G of order p.

Now, note that any p-group G has an order which is a power p^n for some n. If not, then $|G| = p^n q$ where q 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 q.

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:

$$H = \{g | pg = 0\} \tag{12.21}$$

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 is not. 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.

Exercise

Show that an alternative of the structure theorem is the statement than any finite abelian group is isomorphic to

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k} \tag{12.22}$$

where

$$n_1 | n_2 \quad \& \quad n_2 | n_3 \quad \& \quad \cdots \quad \& \quad n_{k-1} | n_k \tag{12.23}$$

Write the n_i in terms of the prime powers in (12.16).

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*:

$$\mathrm{Tors}(G) := \{g \in G | \exists n \in \mathbb{Z} \qquad ng = 0\} \tag{12.24}$$

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

$$0 \to \mathrm{Tors}(G) \to A \to \mathbb{Z}^r \to 0 \tag{12.25}$$

where Tors(G) is a *finite abelian group.*

For a proof, see, e.g., S. Lang, *Algebra* .

Moreover (12.25) is a split extension, that is, it is isomorphic to [31]

$$\mathbb{Z}^r \oplus \mathrm{Tors}(G) \tag{12.26}$$

The integer r, called the *rank of the group*, and the finite abelian group 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.

Remarks

1. The groups $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ under addition are abelian but not finitely generated. To see that $\mathbb{Q}$ is not finitely generated consider any finite set of fractions $\{\frac{p_1}{q_1}, \ldots, \frac{p_s}{q_s}\}$. This set will will only generate fractions with 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.

Exercise

Find a splitting of the sequence (12.25).

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.

[31] albeit, not canonically isomorphic

A key concept in abstract group theory is provided by the notion of a *composition series*. This is a sequence of subgroups

$$1 = G_{s+1} \triangleleft G_s \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 = G \tag{12.27}$$

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.)

It follows that in a composition series the subgroups 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 between the subgroups $N \subset H \subset G$ and subgroups of G/N, and under this correspondence normal subgroups of G/N correspond to normal subgroups $H \subset G$. 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}. ♠

A composition series is a nonabelian generalization of the Kronecker decomposition. It is not unique (see exercise below) but the the following theorem, known as the Jordan-Hölder theorem states that there are some invariant aspects of the decomposition:

Theorem: Suppose there are two different composition series for G:

$$1 = G_{s+1} \triangleleft G_s \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 = G \tag{12.28}$$

$$1 = G'_{s'+1} \triangleleft G'_s \triangleleft \cdots \triangleleft G'_2 \triangleleft G'_1 = G \tag{12.29}$$

Then $s = s'$ and there is a permutation $i \to i'$ so that $G_i/G_{i+1} \cong G'_{i'}/G'_{i'+1}$. That is: The length and the unordered set of quotients are both invariants of the group and do not depend on the particular composition series.

For a proof see Jacobsen, Section 4.6.

The classification of all finite groups is reduced to solving the extension problem in general, and then classifying finite simple groups. The idea is that if we know $G_i/G_{i+1} = S_i$ is a finite simple group then we construct G_i from G_{i+1} and the extension:

$$1 \to G_{i+1} \to G_i \to S_i \to 1 \tag{12.30}$$

We have discussed the extension problem thoroughly above. One of the great achievements of 20th century mathematics is the complete classification of finite simple groups, so let us look at the finite simple groups:

First consider the abelian ones. These cannot have nontrivial subgroups and hence must be of the form $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

So, now we search for the nonabelian finite simple groups. A natural source of nonabelian groups are the symmetric groups S_n. Of course, these are not simple because $A_n \subset S_n$ are normal subgroups. Could the A_n be simple? The first nonabelian example

is A_4 and it is not a simple group! Indeed, consider the cycle structures $(2)^2$. There are three nontrivial elements: (12)(34), (13)(24), and (14)(23), they are all involutions, and

$$((12)(34)) \cdot ((13)(24)) = ((13)(24)) \cdot ((12)(34)) = (14)(23) \tag{12.31}$$

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

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix} \tag{12.32}$$

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 $i \in \{1, \ldots, n\}$ 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 $\sigma = (12 \ldots r)\pi$ with π fixing $\{1, \ldots, r\}$. If $r \geq 3$ then consider the conjugate:

$$\sigma' = (345)\sigma(345)^{-1} = (345)(123\cdots)\pi(354) \tag{12.33}$$

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 $F = \mathbb{C}[a_0, \ldots, a_{n-1}]$ for an n^{th} order polynomial

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{12.34}$$

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: [32]

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,

[32] See the *Atlas of Finite Simple Groups*, by Conway and Norton

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.

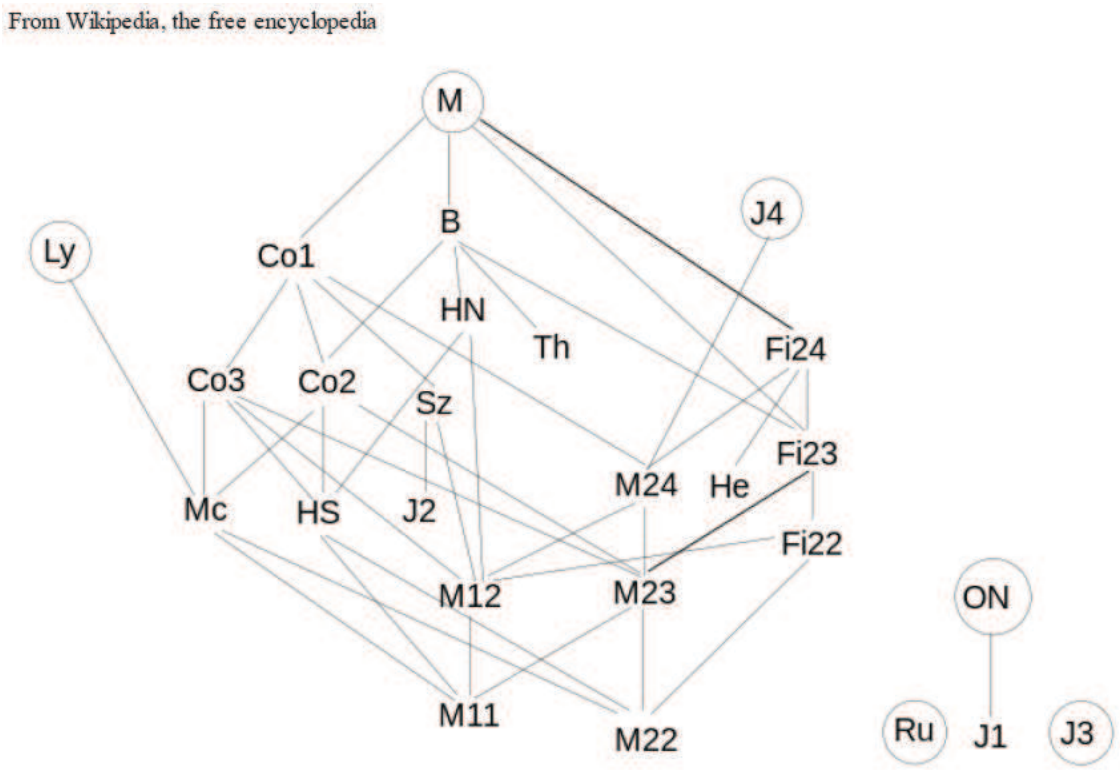


Figure 12: A table of the sporadic groups including subgroup relations. Source: Wikipedia.

It turns out that there are exactly 26 oddballs, known as the "sporadic groups." Some relationships between them are illustrated in Figure 12. The sporadic groups first showed up in the 19^{th} century via the Mathieu groups

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}. \tag{12.35}$$

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 1963, roughly 100 years after the discovery of the Mathieu groups. The list of sporadic groups is now thought to be complete. The largest sporadic group is called the Monster group and its order is:

$$\begin{aligned} |Monster| &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &= 808017424794512875886459904961710757005754368000000000 \\ &\cong 8.08 \times 10^{53} \end{aligned} \tag{12.36}$$

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: [33]

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 (1966) 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:

[33] Our source here is the Wikipedia article on the classification of finite simple groups.

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]

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):

$$[(abe), (ab)(cd)] = (aeb) \tag{12.37}$$

$$[(abc), (abcde)] = (abd) \tag{12.38}$$

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 $p(p^2-1)$. [34]

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.

---

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. However, it seems to be of increasing utility in the further formal development of string theory and supersymmetric gauge theory.

We briefly illustrate some of that language here.

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:

$$X \quad \stackrel{\phi}{\to} \quad Y \tag{13.1}$$

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.

2. $\forall X \in Ob(\mathcal{C})\ \exists\ 1_X : X\to X$, uniquely determined by:

$$1_X\circ\phi = \phi \qquad \psi\circ 1_X = \psi \tag{13.4}$$

for morphisms ϕ,ψ, when the composition is defined.

3. Composition of morphisms is associative:

$$(\psi_1\circ\psi_2)\circ\psi_3 = \psi_1\circ(\psi_2\circ\psi_3) \tag{13.5}$$

[34] 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 $bc=-1$.

An alternative definition one sometimes finds is that a category is defined by two sets X_0 (the objects) and X_1 (the morphisms) with two maps $p_0 : X_1 \to X_0$ and $p_1 : X_1 \to X_0$. The map $p_0(f) = x_1$ is the *range* map and $p_1(f) = x_0$ is the *domain* map. In this alternative definition a category is then defined by a composition law on the set of *composable morphisms*

$$X_2 = \{(f, g) \in X_1 \times X_1 | p_0(f) = p_1(g)\} \tag{13.6}$$

which is sometimes denoted $X_{1p_1} \times_{p_0} X_1$ and called the *fiber product*. The composition law takes $X_2 \to X_1$ 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 $g1_x = g$ 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.

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 then 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 more 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.

One use of categories is that they provide a language for describing precisely notions of "similar structures" in different mathematical contexts. For example:

1. **SET**: The category of sets and maps of sets

2 **DIFF**: The category of manifolds and smooth maps.

3. **GROUP**: the category of groups and homomorphisms of groups.

4. **AB**: The (sub) category of abelian groups.

When discussed in this way it is important to introduce the notion of functors and natural transformations (morphisms between functors) 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 if f_1, f_2 are composable morphisms then

$$F_{\rm mor}(f_1 \circ f_2) = F_{\rm mor}(f_1) \circ F_{\rm mor}(f_2) \tag{13.9}$$

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.

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**.

Example 3: Since **AB** is a subcategory of **GROUP** there is an obvious functor $\mathcal{F} : \mathbf{AB} \to \mathbf{GROUP}$.

Example 4: In an exercise below you are asked to show that the abelianization of a group defines a functor $\mathcal{G} : \mathbf{AB} \to \mathbf{GROUP}$.

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 $f \in \hom(X,Y)$,

$$\tau_Y \circ F_1(f) = F_2(f) \circ \tau_X \tag{13.10}$$

Or, in terms of diagrams.

$$\begin{array}{ccc} F_1(X) & \xrightarrow{F_1(f)} & F_1(Y) \\ \Big\downarrow{\scriptstyle \tau_X} & & \Big\downarrow{\scriptstyle \tau_Y} \\ F_2(X) & \xrightarrow{F_2(f)} & F_2(Y) \end{array} \tag{13.11}$$

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.)

Many important theorems in mathematics can be given an elegant and concise formulation by saying that two seemingly different categories are in fact equivalent. In physics, the very statement of the important phenomenon of "mirror symmetry" is a statement of the equivalence of two (A_∞)-) 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 $\mathrm{FUNCT}(\mathcal{C}_1, \mathcal{C}_2)$ 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_{mor} is a bijection on all the hom-sets. That is, for all $X, Y \in Obj(\mathcal{C}_1)$ the map

$$F_{\mathrm{mor}} : \hom(X, Y) \to \hom(F_{\mathrm{obj}}(X), F_{\mathrm{obj}}(Y)) \tag{13.12}$$

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** $\to$ **GROUP** just given by inclusion.

a.) Show that the abelianization map $G \to G/[G, G]$ defines a functor **GROUP** $\to$ **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 13.

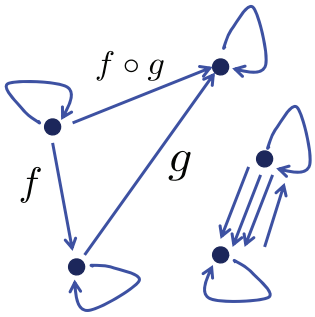


Figure 13: Pictorial illustration of a category. The objects are the black dots. The arrows are shown, and one must give a rule for composing each arrow and identifying with one of the other arrows. For example, given the arrows denoted f and g it follows that there must be an arrow of the type denoted $f \circ g$. 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. A morphism is an equivalence relation $a \sim b$. Composition of morphisms $a \sim b$ with $b \sim c$ is $a \sim c$. 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.

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.

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

$$g_1 \xrightarrow{h} g_2 \tag{13.13}$$

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 simplicial space whose simplices are:

0. 0-simplices = objects
1. 1-simplices = $\Delta_1(f)$ associated to each morphism $f : x_0 \to x_1 \in X_1$.
2. 2-simplices: $\Delta(f_1, f_2)$ associated composable morphisms $(f_1, f_2) \in X_2$.

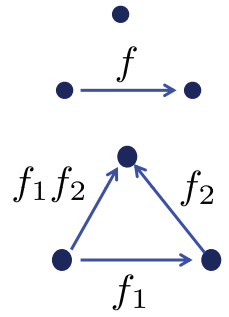


Figure 14: Elementary $0, 1, 2$ simplices in the simplicial space $|\mathcal{C}|$ of a category

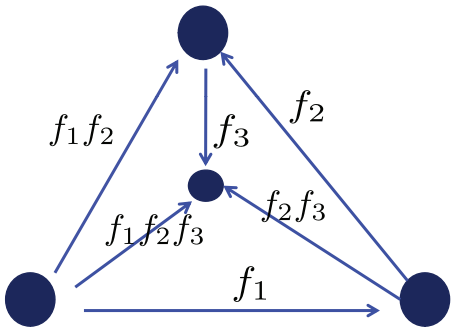


Figure 15: An elementary 3-simplex in the simplicial space $|\mathcal{C}|$ of a category

3. 3-simplices: $\Delta(f_1, f_2, f_3)$ associated to 3 composable morphisms, i.e. elements of:

$$X_3 = \{(f_1, f_2, f_3) \in X_1 \times X_1 \times X_1 | p_0(f_i) = p_1(f_{i+1})\} \tag{13.14}$$

And so on. See Figures 14 and 15. The figures make clear how these simplices are glued together:

$$\partial\Delta_1(f) = x_1 - x_0 \tag{13.15}$$

$$\partial\Delta_2(f_1, f_2) = \Delta_1(f_1) - \Delta_1(f_1 f_2) + \Delta_1(f_2) \tag{13.16}$$

and for Figure 15 view this as looking down on a tetrahedron. Give the 2-simplices of Figure 14 the counterclockwise orientation and the boundary of the simplex the induced orientation from the outwards normal. Then we have

$$\partial\Delta(f_1, f_2, f_3) = \Delta(f_2, f_3) - \Delta(f_1 f_2, f_3) + \Delta(f_1, f_2 f_3) - \Delta(f_1, f_2) \tag{13.17}$$

Note that on the three upper faces of Figure 15 the induced orientation is the ccw orientation for $\Delta(f_1, f_2 f_3)$ and $\Delta(f_2, f_3)$, but with the cw orientation for $\Delta(f_1 f_2, f_3)$. On the bottom fact the inward orientation is ccw and hence the outward orientation is $-\Delta(f_1, f_2)$.

Clearly, we can keep composing morphisms so the space $|\mathcal{C}|$ has simplices of arbitrarily high dimension, that is, it is an infinite-dimensional space.

Let look more closely at this space for the case of a group, regarded as a category with one object. Then in the above pictures we identify all the vertices with a single vertex.

For each group element g we have a one-simplex $\Delta_1(g)$ beginning and ending at this vertex.

For each ordered pair (g_1, g_2) we have an oriented 2-simplex $\Delta(g_1, g_2)$, etc. We simply replace $f_i \to g_i$ in the above formulae, with g_i now interpreted as elements of G:

$$\partial\Delta(g) = 0 \tag{13.18}$$

$$\partial\Delta(g_1, g_2) = \Delta_1(g_1) + \Delta_1(g_2) - \Delta_1(g_1 g_2) \tag{13.19}$$

$$\partial\Delta(g_1, g_2, g_3) = \Delta(g_2, g_3) - \Delta(g_1 g_2, g_3) + \Delta(g_1, g_2 g_3) - \Delta(g_1, g_2) \tag{13.20}$$

See Figure 15.

And so on.

To put this more formally: We have $n+1$ maps from $G^n \to G^{n-1}$ for $n \geq 1$ given by

$$\begin{aligned} d^0(g_1, \ldots, g_n) &= (g_2, \ldots, g_n) \\ d^1(g_1, \ldots, g_n) &= (g_1 g_2, g_3, \ldots, g_n) \\ d^2(g_1, \ldots, g_n) &= (g_1, g_2 g_3, g_4, \ldots, g_n) \\ &\cdots\cdots \\ &\cdots\cdots \\ d^{n-1}(g_1, \ldots, g_n) &= (g_1, \ldots, g_{n-1} g_n) \\ d^n(g_1, \ldots, g_n) &= (g_1, \ldots, g_{n-1}) \end{aligned} \tag{13.21}$$

On the other hand, we can view an n-simplex Δ_n as

$$\Delta_n := \{(t_0, t_1, \ldots, t_n) | t_i \geq 0 \qquad \& \qquad \sum_{i=0}^{n} t_i = 1\} \tag{13.22}$$

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:

$$\begin{aligned} d_0(t_0, \ldots, t_{n-1}) &= (0, t_0, \ldots, t_{n-1}) \\ d_1(t_0, \ldots, t_{n-1}) &= (t_0, 0, t_1, \ldots, t_{n-1}) \\ &\cdots\cdots \\ &\cdots\cdots \\ d_n(t_0, \ldots, t_{n-1}) &= (t_0, \ldots, t_{n-1}, 0) \end{aligned} \tag{13.23}$$

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

$$(\amalg_{n=0}^{\infty} \Delta_n \times G^n) \,/\, \sim$$

via

$$(d_i(\vec{t}), \vec{g}) \sim (\vec{t}, d^i(\vec{g})). \tag{13.24}$$

The space we have constructed this way has a homotopy type denoted BG. 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

$$\langle d\phi_n, \Delta \rangle = \langle \phi_n, \partial\Delta \rangle \tag{13.25}$$

and from the above formulae we recover, rather beautifully, the formula for the coboundary in group cohomology.

Remark: 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 $G//G \to pt//G$.