Groups and their Representations

Karen E. Smith

1. Preface

There are many people to acknowledge who helped make these notes much better. The students of my course in Finland first and foremost, especially Joonas Ilmavirta, and my assistant for that course, Lauri Kahanpää. Next, my math 296 and Math 512 students at the University of Michigan found lots of errors, including David Bruce, Alex Cope, James Dunseth Matt Tanzer, and especially Elliot Wells. Also my good friend Kelli Talaska made many suggestions for improvement.

I wrote these notes out of frustration with our mathematical education curriculum. Representation theory is one of most fundamental areas of contemporary mathematics—used daily by mathematicians and physicists for many different purposes and with different goals—yet it is hardly mentioned at the undergraduate or even beginning graduate level. Why not? It is concrete, full of beautifully elegant theorems and rich examples, and most significantly, belongs to the modern canon of general knowledge for the working mathematician in *every* branch of mathematics—more so than many of the topics filling our beginning graduate algebra courses.

There are beautifully elegant introductions to representation theory–such as Serre's—which cover in much less space the same theorems we slowly develop example by example. These notes are quite different—starting from little, I wanted to teach students through examples what to expect from group actions on vector spaces before proving anything. I wanted to review and re-emphasize algebraic ways of thinking, re-explaining ideas that (I have noticed over the years) are rife with student misconceptions and confusions. I wanted to teach students how to think algebraically more broadly through a beautifully rich topic, a fundamental topic they really need to know.

The notes grew out of an advanced undergraduate graduate-school-bound math and physics course at the University of Jyväskylä, and to some extent the choice of topics, examples, and emphasis was driven by their questions, background and interests. These notes represent the first half of that course; the second half dealt with Lie Groups.

The audience for these notes are strong math and physics undergraduates. The prerequisites are

(1) A serious linear algebra course is a prerequisite, at least over the real and complex numbers. It is assumed students are familiar with the definition of real and complex vector spaces (and not just $\mathbb{R}^n$ and $\mathbb{C}^n$), bases, linear maps and their representation as matrices, and —for the sections containing the fundamental theorem on the classification of representations—also the tensor product and the notion of a non-degenerate(Hermitian) bilinear form.
(2) Mathematical sophistication appropriate to a strong undergraduate nearing the end of their undergraduate studies
(3) Some familiarity with basic algebra, though much of the needed group theory is reviewed.

CHAPTER 1

Introduction

Representation theory is the study of the concrete ways in which abstract groups can be realized as groups of rigid transformations of $\mathbb{R}^n$ (or $\mathbb{C}^n$).

First, let us recall the idea of a **group**. The quintessential example might be the symmetry group of a square. A *symmetry* of the square is any rigid motion of Euclidean space which preserves the square. For example, we can rotate the square counterclockwise by a quarter turn (90 degrees); this is one symmetry of the square. Another is flipping the square over its horizontal axis. Of course, "doing nothing" is the *identity symmetry* of the square.

Of course, any two symmetries can be composed to produce a third. For example, rotation though a quarter-turn followed by reflection over the horizontal axis has the same effect on the square as reflection over one of the diagonals. Also, every symmetry has an "opposite" or *inverse* symmetry. For example, rotation counterclockwise by ninety degrees can be undone by rotation clockwise by ninety degrees so that these two rotations are inverse to each other. Each reflection is its own inverse.

The full set of symmetries of the square forms a group: a set with natural notion of *composition* of any pair of elements, such that every element has an inverse. This group is represented as a set of rigid transformations of the vector space $\mathbb{R}^2$. We will soon give a formal definition for a group, but the idea of a group is well captured by the fundamental example of symmetries of a square, and we will return to it throughout these lectures to understand many different features of groups and their representations.

Groups arise everywhere in nature, science and mathematics, usually as collections of transformations of some set which preserve some interesting structure. Simple examples include the rigid motions of three-space that preserve a particular molecule, the transformations of space-time which preserve the axioms of gravitation theory, or the linear transformations of a vector space which preserve a fixed bilinear form.

Only in the late nineteenth century was the *abstract* definition of a group formulated by Cayley, freeing the notion of a group from any particular *representation* as a group of transformations. An analogous abstractification was happening throughout mathematics: for example, the notion of an (abstract) manifold was defined, freeing manifolds from the particular choice of embedding in $\mathbb{R}^n$. Of course this abstraction is tremendously powerful. But abstraction can have the effect of making the true spirit of a group (or a manifold, or whatever mathematical object you chose) obscure to the outsider. Group theory—both historically and as practiced by modern mathematicians today—is at its heart a very concrete subject grounded in actual transformations of a set.

It turns out that, despite the abstract definition, *every group* can be thought of concretely a group of symmetries of some set, usually in many different ways. The goal of representation theory is to understand the different ways in which abstract groups can be realized as *transformation groups.* In practice, we are mainly interested in understanding how groups can be represented as *groups of linear transformations* of euclidean space.

CHAPTER 2

Review of Elementary Group Theory

1. Abstract Groups.

Definition 1.1. A group is a set G, together with a binary operation $\star$ satisfying:

(1) Associativity: $g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3$ for all $g_1, g_2, g_3 \in G$.
(2) Existence of identity: there exists $e \in G$ such that $g \star e = e \star g = g$ for all $g \in G$.
(3) Existence of inverses: for all $g \in G$, there exists $g^{-1} \in G$ such that $g \star g^{-1} = g^{-1} \star g = e$.

A group G is *abelian* if the operation $\star$ is commutative, that is if $g \star h = h \star g$ for all g and h in G.

The *order* of a group $(G, \star)$ is the cardinality of the set G, whether finite or infinite. The order of G is denoted $|G|$.

The quintessential example of a group is the set of symmetries of the square under composition, already mentioned in the introduction. This group is called a dihedral group and denoted D_4. What is the order of D_4? That is, how many different symmetries has a square?

Well, there are four rotations: counterclockwise through $90, 180$, or 270 degrees, plus the trivial rotation through 0 degrees. We denote these by r_1, r_2, r_3, and I, respectively. Of course, we could also rotate clockwise, say by 90 degrees, but the effect on the square is the same as counterclockwise rotation through 270, so we have already counted and named this symmetry r_3.

In addition to the four rotations, there are four distinct reflections: over the horizontal axis, the vertical axis, or either of the two diagonals. We denote these by H, V, D and A, respectively[1]. Putting together the four rotations and the four reflections, we get *all* the symmetries of the square, as you should check. Thus D_4 has order eight.

By definition, a group $(G, \star)$ is *closed under* $\star$. For the dihedral group this means that composing any two of these eight symmetries, we obtain another symmetry on this list of eight. For example, if we rotate 90^0, then rotate 180^0 (both counterclockwise), we have in

[1]Fixing the square so it is centered at the origin of the cartesian plane, these are reflections over the x-axis, y-axis, the diagonal $y = x$ and the antidiagonal $y = -x$, respectively.

effect rotated 270^0. In other words $r_2 \circ r_1 = r_3$. [**Note our convention!** We write $r_2 \circ r_1$ for the transformation "r_1 followed by r_2".]

The group structure of D_4 can be expressed in a Cayley table, showing how to compose any two elements of the group. The 64 compositions of the 8 symmetry transformations are displayed as follows:

$\circ$	I	r_1	r_2	r_3	H	A	V	D
I	I	r_1	r_2	r_3	H	A	V	D
r_1	r_1	r_2	r_3	I	D	H	A	V
r_2	r_2	r_3	I	r_1	V	D	H	A
r_3	r_3	I	r_1	r_2	A	V	D	H
H	H	A	V	D	I	r_1	r_2	r_3
A	A	V	D	H	r_3	I	r_1	r_2
V	V	D	H	A	r_2	r_3	I	r_1
D	D	H	A	V	r_1	r_2	r_3	I

Another convention: We write $a \circ b$ in *row* a and *column* b. So we can read from the table: $A \circ V = r_1$.

From the Cayley table, much of the group structure is clearly visible. We see that D_4 is not abelian; the Cayley table of an abelian group would be symmetric over the main diagonal. We easily find the inverse of any element by looking for I in each column. Try picking out those g which are inverses of themselves.

Higher order dihedral groups. The collection of symmetries of a regular n-gon (for any $n \geq 3$) forms the dihedral group D_n under composition. It is easy to check that this group has exactly $2n$ elements: n rotations and n reflections. Like D_4, D_n is non-abelian.

The **quintessential example of an infinite group** is the group $GL_n(\mathbb{R})$ of invertible $n \times n$ matrices with real coefficients, under ordinary matrix multiplication. There is nothing sacred about the real numbers here: $GL_n(\mathbb{Q})$ and $GL_n(\mathbb{C})$ are also groups under multiplication, as is $GL_n(F)$, where the entries are taken from any field F. The notation $GL_n(\mathbb{R})$ *implies* the group structure to be given by ordinary matrix multiplication.

Additive groups. The integers form a group under addition, denoted $(\mathbb{Z}, +)$. Zero is identity element, and the inverse of 17, for example, is -17. Because this group (and many others) already come with standard notation, we of course won't write such foolery as $2 \star 3 = 5$ or $(17)^{-1}$ when we mean the inverse of 17 in the group $(\mathbb{Z}, +)$.

Similarly, the real numbers and the rational numbers form the additive groups $(\mathbb{R}, +)$ and $(\mathbb{Q}, +)$, respectively.

None of the groups $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ or $(\mathbb{Q}, +)$ are very good examples of groups. Most mathematicians are not interested in these objects *as groups.* They each carry a great deal more structure which obscures their "group-ness". The integers are more naturally considered as a ring—there are two operations, addition and multiplication. The rational numbers are a good example of a *field*— we can also divide by non-zero elements. The real numbers have many analytic and topological features, in addition to their algebraic properties— they are a complete ordered field, for example. Moreover, the topological and algebraic properties of $\mathbb{R}$ can even be combined giving us the simplest example of a *Lie Group*—that is a manifold which admits a compatible group structure. The group $GL_n(\mathbb{R})$ is another example of a more interesting manifold. We will discuss Lie groups in depth later.

The Multiplicative group of a field or ring. The integers *do not* form a group under multiplication, since most elements do not have multiplicative inverses. However, both $(\mathbb{Q}^*, \cdot)$ and $(\mathbb{R}^*, \cdot)$, the non-zero rational and the non-zero real numbers, respectively, do form groups under multiplication. Indeed, the non-zero elements F^* of any field F form a group under multiplication. Even more generally, the set of (multiplicatively) invertible elements R^* in any ring R, forms a group under multiplication. For example $\mathbb{Z}^*$ is the two-element group $\{1, -1\}$ under multiplication.

Some groups obtained from the complex numbers. The complex numbers give rise to groups $(\mathbb{C}, +)$ and $(\mathbb{C}^*, \cdot)$. The collection of complex numbers of absolute value 1 also forms a group under multiplication, denoted $U(1)$. The group $U(1)$ is sometimes called the *circle* group. It is the simplest example of a compact Lie group–a compact manifold which carries a compatible group structure.

REMARK 1.2. It is common to use multiplicative language and notation for groups, when this isn't likely to lead to confusion or when there isn't another already standard notation, as in $(\mathbb{Z}, +)$. For example, we rarely bother writing $\star$ for the operation, instead writing gh for $g \star h$. This justifies also the use of g^{-1} for the inverse of g under $\star$. **HOWEVER, it is important to realize that the *composition* language and notation is closer to the spirit of groups.** This is because, philosophically and literally speaking, *all groups are transformation groups,* with composition as the operation. We will see why next week.

1.1. Subgroups.

DEFINITION 1.3. A subset $H \subset G$ of a group $(G, \star)$ is a *subgroup* if H also forms a group under $\star$.

Put differently, a subgroup is a non-empty subset closed under the operation $\star$ and under taking inverses. For example, $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$, since the sum of two rational numbers is rational and the additive inverse of any rational number is rational. However $\mathbb{R}^*$ is NOT a subgroup of $(\mathbb{R}, +)$, even though it is a group in its own right, because the group operations are not the same.

On the other hand, the set of *positive* real numbers $\mathbb{R}_+$ forms a subgroup of the group $\mathbb{R}^*$ of non-zero real numbers under multiplication. Similarly, $\mathbb{Q}_+$ is a subgroup of $\mathbb{Q}^*$.

Special Linear Groups. The set $SL_n(\mathbb{R})$ consisting of real matrices of determinant one forms a *subgroup* of the matrix group $GL_n(\mathbb{R})$. Likewise, the matrices of determinant one form the subgroups $SL_n(\mathbb{Q})$ and $SL_n(\mathbb{C})$ of $GL_n(\mathbb{Q})$ and $GL_n(\mathbb{C})$, respectively.

The **rotation subgroup** R_4 of D_4 is made up of the four rotations of the square (including the trivial rotation). Likewise, the rotations of an n-gon form an order n subgroup R_n of D_n. The reflections of the square *do not* form a subgroup of D_4: the composition of two reflections is not a reflection. Looking back at the Cayley table for D_4 on page two, we can see the Cayley table for R_4 embedded as the upper left 4×4 section.

The **even-odd group** is the set consisting of the two words "even" and "odd," under the usual "rules for addition:" even plus even is even, even plus odd is odd, etc. This is *not* a subgroup of $\mathbb{Z}$: its elements are *sets* of integers, not integers in some subset of $\mathbb{Z}$. However, it is a *quotient* group of $\mathbb{Z}$, or a *modular group.*

1.2. Modular Groups. The modular group $(\mathbb{Z}_n, +)$ consists of the n congruence classes modulo n, under addition. We will write $\bar{i}$ for the congruence class of the integer i. So $\overline{-1}$ and $\overline{n-1}$ are just two different ways to represent the same element of $\mathbb{Z}_n$, just as $\frac{1}{2}$ and $\frac{2}{4}$ are two different ways to represent the same rational number. Of course, in the group $(\mathbb{Z}_n, +)$, the class $\overline{0}$ is the identity element, and the class $\overline{-i}$ is the inverse of $\bar{i}$.

The elements of $\mathbb{Z}_2$, for example, are $\overline{0}$ and $\overline{1}$, consisting of the sets of even and odd numbers respectively.

1.3. Isomorphism. The even-odd group is the "same as" the modular group $\mathbb{Z}_2$ in a certain sense–essentially we've only named the elements differently. Likewise, the group R_4 of rotations of the square seems to have the same structure as $\mathbb{Z}_4$. This "sameness" can be formalized as follows.

Definition 1.4. Two groups are *isomorphic* if there is a bijection between them *respecting the group structure.* That is, an isomorphism is a bijection $\phi : G \to H$ satisfying $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

Put more informally, two groups are isomorphic if we can rename the elements of one to be the elements of the other while preserving the Cayley table.

The rotation subgroup R_4 is isomorphic to $(\mathbb{Z}_4, +)$. Indeed, the map $r_i \mapsto \bar{i}$ respects the group operation and is thus an isomorphism.

1.4. Generators. Because they are isomorphic groups, all properties of R_4 and $\mathbb{Z}_4$ having to do with the group structure must be the same in each. For example, the rotations can all be obtained from the quarter rotation r_1 by successive compositions, just as the elements of $\mathbb{Z}_4$ can be obtained by successive additions of $\overline{1}$. In both groups, we cycle back to the identity after four iterates. We say that R_4 is *generated* by the quarter turn, and that $\mathbb{Z}_4$ is *generated* by $\overline{1}$. Formally, Definition 1.5. A subset S of a group $(G, \star)$ *generates* G if each element g in G can be written as a *word* $s_1 \star s_2 \cdots s_{t-1} \star s_t$, where each s_i or its inverse is in S.

The groups $(\mathbb{Z}_4, +)$ and R_4 of rotations of the square are examples of *cyclic groups*—groups that can be generated by one element. An example of a non-cyclic group is the D_4 of all symmetries of the square. It is generated by r_1 and H, but not by any single element. Indeed, every cyclic group is *abelian,* but D_4 is not.

Groups can (and usually do) have many different subsets which generate it. For example D_4 is also generated r_3 and A. Likewise, $(\mathbb{Z}, +)$ is a cyclic generated by 1, or by -1. Also the two-element set $\{17, 4\}$ generates $\mathbb{Z}$ as an additive group, as does, say the subset of all positive integers.

More generally, we can consider the subgroup of G generated by some subset S. This is the *smallest subgroup* of G containing S. For example, R_4 is the subgroup of D_4 generated by the rotation r_1.

The subgroup of the group $(\mathbb{Z}, +)$, generated by some fixed integer N is the subgroup of multiples of N. We denote this group $N\mathbb{Z}$. It is not hard to show that *every* subgroup of $(\mathbb{Z}, +)$ is of this form.

The Klein four-group. Consider the subgroup G of D_4 generated by D and A. It is easy to check that G consists of the four elements e, D and A, and the half rotation r_2. Indeed, $AD = DA = r_2$ in D_4. One could write longer "words" in A and D, but after canceling unnecessary factors (such as $A \circ A$, which is e), all words in D and A reduce to one of the four elements $\{e, A, D, r_2\}$.

This subgroup G can not be isomorphic to $(\mathbb{Z}_4, +)$, even though they both have four elements. Indeed, G has the interesting property that every element is its own inverse! If we could rename the elements of G to be congruence classes in $\mathbb{Z}_4$ while preserving the group structure, it would follow that every element of $(\mathbb{Z}_4, +)$ would be its own inverse as well. But this is not the case! The class $\overline{1}$ has $\overline{3}$ as its additive inverse in $\mathbb{Z}_4$, but $\overline{1} \neq \overline{3}$ in $\mathbb{Z}_4$.

1.5. Generators of $GL_n(\mathbb{R})$. The group $GL_n(\mathbb{R})$ is huge: not only is it uncountable, but it is easy to see that it can't even be generated by countably many elements. None-the-less, it does admit a reasonable set of generators.

Recall that every (invertible) linear transformation is a composition of *elementary* transformations. After fixing a basis, we can describe the elementary transformations as one of three types:

(1) interchanging two basis elements;
(2) sending e_i to some $e_i + \lambda e_j$, where λ is some scalar.
(3) scaling e_i by some non-zero scalar λ.

If we identity $\mathbb{R}^n$ as column vectors, thereby identifying linear transformations on $\mathbb{R}^n$ with left multiplication by some $n \times n$ matrix, these linear transformations are represented by the corresponding elementary matrices obtained from the identity matrix by the same transformations on columns:

(1) C_{ij} = the identity matrix with columns i and j switched;
(2) E_{ij} = the identity matrix with λ put into the ij-th spot;
(3) S_i = the identity matrix with i-th column scaled by λ.

Thus these three types of matrices together generate the group of all invertible $n \times n$ matrices under multiplication.

Exercise 1.6 (**The Center of a group**). The *center* of a group G is the set Z of elements which commute with all elements of G : $Z = \{z \in G \mid gz = zg \text{ for all } g \in G\}$.

(1) Prove that the center is a subgroup.
(2) Find the center of $\mathbb{Z}_n$.
(3) Find the center of D_4.
(4) Find the center of S_n.

2. Transformation Groups

Let X be any set, finite or infinite. A *transformation* of X is a bijective self-map $f : X \to X$. A bijective self-map of a set X is sometimes also called a *permutation* (especially when X is finite) or automorphism of X. Indeed, to use fancy language, a bijective self-map is an *automorphism* in the category of sets, so this is reasonable terminology.

Two transformations can be composed to produce a third, and every transformation has an inverse transformation (this is essentially the meaning of "bijection"). In other words, the collection of *all* transformations of X forms a group under composition[2], whose identity element is the identity transformation e fixing every element. We denote this group by

$$\text{Aut } X = \{f : X \to X \mid f \text{ is bijective}\}$$

with the group operation understood to be composition.

Definition 2.1. A transformation group is any subgroup of Aut X for some set X.

The dihedral group D_4 is a transformation group: its elements can be interpreted as transformations of $\mathbb{R}^2$ which preserve the square. Indeed, these are not arbitrary transformations of $\mathbb{R}^2$, but transformations which *respect the vector space structure structure of* $\mathbb{R}^2$—that is, they are all *linear transformations* of $\mathbb{R}^2$.

This brings up an important point. Often X carries some extra structure, and we are mainly interested in automorphisms that respect this structure. The main case of interest is

[2]composition is obviously associative

when X is a vector space,[3] where we are interested in the bijective self maps $X \to X$ preserving the vector space structure (that is, *linear transformations*). Because the composition of two linear maps is linear and the inverse of a linear map is linear, the set of all (invertible) linear transformations of X forms a subgroup of Aut X, which we denote by $GL(X)$. Of course, a linear transformation is a very special kind of bjiective self-map, so $GL(X)$ is a proper (and relatively quite small) subgroup of Aut(X) in general.[4]

2.1. All groups are transformation groups. Historically, all groups were transformation groups: Galois's groups were permutation groups of roots of polynomials, Klein's Erlangen program involved groups of linear transformations preserving some geometry. Still today, transformation groups of all kinds arise naturally in nature and mathematics. The idea of an abstract group, due to Cayley, came much later.

Most of the groups we have already discussed are transformation groups by definition: D_n, R_n, SL_n, GL_n. Most of more abstract examples, such as the quotient groups $\mathbb{Z}_n$, are easily seen to be isomorphic to transformation groups (as $\mathbb{Z}_n$ is isomorphic to the group of rotations of the regular n-gon). It turns out that *every group is (isomorphic to) a transformation group* of some kind. We will prove this fundamental fact, due to Cayley, in the next lecture.

2.2. Groups of linear transformation and matrices. The group $GL(\mathbb{R}^n)$ and its close cousin $GL(\mathbb{C}^n)$ are among the most important groups in mathematics and physics. We fix some notation and conventions for dealing with them. If we think of $\mathbb{R}^n$ as being the $\mathbb{R}$-vector space of *column vectors,* then the *standard basis* will be

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \cdots \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix}, \quad \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \\ 1 \end{pmatrix}.$$

A linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ is determined by where it sends each of these basis elements, say

$$T(e_i) = \begin{pmatrix} a_{i1} \\ a_{i2} \\ \cdots \\ a_{in} \end{pmatrix}.$$

[3] over some as-yet unnamed field— in this course usually $\mathbb{R}$ or $\mathbb{C}$

[4] Imagine all the crazy bijections we could cook up of $\mathbb{R}^2$—-there are all sorts of non-linear homomorphisms and even more arbitrary bijections that may not even be continuous at any point!

It is then straightforward to check that the linear map T is given by ordinary matrix multiplication of column vectors by the $n \times n$ matrix

$$\begin{pmatrix} a_{11} & \dots & a_{n1} \\ a_{12} & \dots & a_{n2} \\ \vdots & \dots & \vdots \\ a_{1n} & \dots & a_{nn} \end{pmatrix},$$

whose $i-th$ *column* is the column vector which is the image of e_i. This identification gives us an isomorphism

$$GL(\mathbb{R}^n) \to GL_n(\mathbb{R})$$

with the group of invertible real $n \times n$ matrices. Of course, the story is exactly the same over the complex numbers.

Convention: In dealing with $\mathbb{R}^n$, we will often identify $GL(\mathbb{R}^n)$ with $GL_n(\mathbb{R})$. However, if is important to realize that this isomorphism **depends on the choice of a basis** for $\mathbb{R}^n$; in this case, our choice was the standard basis of unit column vectors described above. Vector spaces—even finite dimensional real ones— usually **do not come with a god-given choice of basis.** Yes, every n-dimensional real vector space is *isomorphic to* $\mathbb{R}^n$, but there is no canonical way to define this isomorphism—there is no "standard basis" for example for a skew plane in $\mathbb{R}^3$. The notation $\mathbb{R}^n$ denotes an abstract vector space *together with a choice of basis.* Once a basis is chosen for a vector space V, we essentially have fixed an isomorphism with $\mathbb{R}^n$, and we therefore also we fix an isomorphism of the group $GL(V)$ with the group of invertible $n \times n$ matrices.

2.3. The Symmetric Groups. Probably the most basic example of a transformation group is the group Aut X where X is a finite set of cardinality n. Of course, the different ways in which a set of n objects can be permuted is the same regardless of whether those objects are fruits, students in a class, points in some space, or the numerals $\{1, 2, 3, \dots, n\}$. For convenience, therefore, we will usually label the objects $\{1, 2, 3, \dots, n\}$.

Definition 2.2. The group Aut $\{1, 2, 3, \dots, n\}$ is called the *symmetric* or *permutation* group on n letters, and is denoted S_n.

For example, there are six elements of S_3, which we list out as follows:

e: the identity permutation, fixing each element,
three transpositions: namely
τ_1**:** fixing 1 and switching 2 and 3,
τ_2**:** fixing 2 and switching 1 and 3,
τ_3**:** fixing 3 and switching 1 and 2,
and two 3-cycles: specifically
σ**:** sending $1 \mapsto 2$, $2 \mapsto 3$ and $3 \mapsto 1$
σ^{-1}**:** sending $1 \mapsto 3$, $2 \mapsto 1$ and $3 \mapsto 2$.

Note that each element of S_n is a bijection, so can be described by giving a list of pairs essentially describing the image of each of the n objects. However, a more compact and convenient notation is *cycle notation.* In cycle notation, the transposition τ_1 is denoted by (23), meaning it sends 2 to 3 and 3 to 2. Likewise, τ_2 is written (13) and τ_3 (12). Similarly, σ is denoted (123) since it sends 1 to 2, 2 to 3, and 3 to 1. That is, the image of each numeral is the numeral immediately following it, unless a parenthesis follows it in which case we cycle back to the first numeral in that parentheses. So σ^{-1} is (132).

For example, in S_9 the permutation

$$\sigma(1)=2 \quad \sigma(2)=4 \quad \sigma(3)=5 \quad \sigma(4)=1 \quad \sigma(5)=6 \quad \sigma(6)=7 \quad \sigma(7)=9 \quad \sigma(8)=8 \quad \sigma(9)=3$$

is denoted

$$\sigma = (124)(35679)(8),$$

which can be simplifying by omitting the fixed objects

$$\sigma = (124)(35679).$$

Note that the 3-cycle (124) is the *same* permutation as (241) and (412); there is no difference in the permuations these expressions represent. Also the disjoint cycles (124) and (35679) commute: we can just as well represent the permutation σ by (35679)(124).

An element of S_n which cyclicly permutes k of the objects is called a k-cycle. For example (12345) is a 5-cycle but (12)(345) is not any kind of cycle (though it is the composition of a two-cycle and a three-cycle). It is not always immediately obvious what permutations are cycles. For example, the composition (12)(23), which according to our convention means the permutation (23) **followed by** (12) is the 3-cycle (123). A transposition is another word for 2-cycle.

Some basic facts about S_n that you should prove to familiarize yourself with this important group include:

(1) There are $n!$ permuations in S_n.
(2) Disjoint cycles in S_n commute.
(3) Every permutation in S_n can be written as a composition of *disjoint* cycles—uniquely, up to reordering the disjoint cycles.
(4) Every permutation in S_n is a composition of transpositions. That is, S_n is generated by transpositions.

3. Products of Groups

Two groups can be put together in a simple way to form a third group, their *product.* Formally:

Definition 3.1. Let $(G, \star)$ and $(H, *)$ be groups. Their *product* is the Cartesian product set $G \times H$ with the group operation defined as follows: $(g, h) \cdot (g', h') = (g \star g', h * h')$.

It is straightforward to verify that $G \times H$ is a group with identity element (e_G, e_H).

Example 3.2. The group $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ has six elements: $(\overline{1}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{2}), (\overline{0}, \overline{0})$. The addition is defined "coordinate-wise, " so for example $(\overline{1}, \overline{1}) + (\overline{1}, \overline{1}) = (\overline{0}, \overline{2})$. Note that this group is isomorphic to $\mathbb{Z}_6$. Indeed, if we identify the element $(\overline{1}, \overline{1})$ with the element $\overline{1}$ in $\mathbb{Z}_6$, then be repeatedly adding this to itself, we list out the elements of $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ given above in the way they should be renamed to produce the elements $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{0}$ of $\mathbb{Z}_6$.

Exercise 3.3. Caution! It is not always true that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$. As an easy exercise, show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$. Find a subgroup of D_4 to which it is isomorphic. Find a necessary and sufficient condition on n and m such that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$.

Exercise 3.4. Prove that for $n \leq 3$, there is only one group of order n, up to isomorphism. Prove that there are exactly two groups of order four, up to isomorphism.

4. Homomorphism

Let G and H be groups. A group homomorphism is a map $\phi : G \to H$ which preserves the multiplication: $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

An isomorphism is the simplest example of a homomorphism. Indeed, an isomorphism can be defined as a *bijective homomorphism.*

The inclusion of a subgroup H in a group G is an example of an *injective* homomorphism.

The *projection* of a product group $G \times H$ onto either factor is an example of a surjective homomorphism. That is, $\pi : G \times H \to G$ sending (g, h) to g is a homomorphism.

A homomorphism is any set map which *respects the group structure.* For example, a homomorphism must send the identity element to the identity element (check this!). Also, if g and g' are inverse elements of some group, then their images under any homomorphism are also inverse to each other.

Example 4.1. (1) The map $\mathbb{Z} \to \{\mathrm{E}ven, Odd\}$ sending an integer n to "even" if n is even and to "odd" if n is odd defines a group homomorphism from the corresponding additive groups.

(2) The map $x \mapsto e^x$ defines a group homomorphism from $(\mathbb{Q}, +)$ to $(\mathbb{R}^*, \cdot)$. It is injective, but not an isomorphism since not every real number is in the image. However, exponential map from $(\mathbb{R}, +)$ to the positive real numbers $(\mathbb{R}_+, \cdot)$ is an isomorphism of groups.

(3) The map $\mathbb{Z} \to \mathbb{Z}_n$ sending each integer to its equivalence class modulo n is a surjective homorphism of the corresponding additive groups.

5. Quotient Groups

Before discussing quotient groups in general, we first review the construction of $\mathbb{Z}_n$.

Definition 5.1. Integers a and b are *congruent modulo* n if their difference is a multiple of n. We write $a \equiv b \bmod n$.

Note that

(1) $a \equiv a \bmod n$;
(2) $a \equiv b \bmod n$ if and only if $b \equiv a \bmod n$;
(3) $a \equiv b \bmod n$ and $b \equiv c \bmod n$ implies that $a \equiv c \bmod n$.

In other words, the relation "congruence modulo n" is reflexive, symmetric, and transitive on $\mathbb{Z}$; that is, it defines an *equivalence relation* on $\mathbb{Z}$. Like any equivalence relation, it partitions $\mathbb{Z}$ up into disjoint *equivalence classes.* These are called the congruence classes modulo n.

Definition 5.2. The congruence class of $a \in \mathbb{Z}$ modulo n is the set of integers congruent to a modulo n. We denote[5] this class by $\overline{a}$. In other words:

$$\overline{a} = \{a + nk \mid k \in \mathbb{Z}\}.$$

There are exactly n distinct congruence classes modulo n. Usually, we will write them $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. We emphasize that $\overline{a}$ is a *set* of integers, though of course, we can represent this set in many ways by choosing some *representative.* For example $\overline{-1} = \overline{n-1}$. Both representatives are equally valid, and depending on the situation, one may be more convenient than another. This is exactly analogous to the way in which both $\frac{1}{2}$ and $\frac{2}{4}$ are equally valid representations for the same rational number, and depending on the circumstances, it may be more convenient to write the fraction one way or the other.

One simple but very important observation is that if $a \equiv a'$ and $b \equiv b' \bmod n$, then also

$$a + b \equiv a' + b' \mod n.$$

In other words, it makes sense to add congruence classes by simply choosing any representative and adding those:

$$\overline{a} + \overline{b} = \overline{a + b};$$

the resulting sum is independent of the chosen representatives for each class. This means that there is a well-defined addition on the set of congruence classes: simply add any two representatives, and take the class of their sum!

Definition 5.3. The group $(\mathbb{Z}_n, +)$ is the set of congruence classes of $\mathbb{Z}$ modulo n, with the operation defined as $\overline{a} + \overline{b} = \overline{a + b}$.

Of course, you should verify that $(\mathbb{Z}_n, +)$ satisfies the axioms of a group. Associativity follows from the associativity for $\mathbb{Z}$. The identity element is $\overline{0}$ (which, we remind, is the *set* of multiples of n). The inverse of $\overline{a}$ is $\overline{-a}$, which we can also write $\overline{n - a}$.

[5] Some caution is in order when using this notation since the dependence on n is suppressed from the notation.

5.1. Cosets. Now try to carry out a similar procedure for any group. First observe that $a \equiv b \bmod n$ can be expressed by $a - b \in n\mathbb{Z}$, where $n\mathbb{Z}$ is the subgroup of $\mathbb{Z}$ consisting of multiples of n. Rewriting this in multiplicative notation we are led to the following definition.

DEFINITION 5.4. Let K be a subgroup of a fixed group G. We say that g is (right) congruent to h modulo K if

$$g \star h^{-1} \in K.$$

Taking $K \subset G$ to be the inclusion $n\mathbb{Z} \subset Z$, we recover the notion of congruence of two integers modulo n. Note g is congruent to h modulo K if and only if there exists some $k \in K$ such that

$$g = kh,$$

or equivalently if and only if

$$g \in Kh := \{kh \mid k \in K\}.$$

Using the same notation as in the integers, we could also write $g \equiv h \bmod K$.[6]

This notion of congruence modulo K defines an equivalence relation on G. Indeed, it is reflexive ($g \equiv g \bmod K$) because the subgroup K contains the identity element; it is symmetric ($g \equiv h \bmod K$ if $h \equiv g \bmod K$) because K is closed under taking inverses; and it is transitive ($g \equiv h \bmod K$ and $h \equiv s \bmod K$ implies that $g \equiv s \bmod K$) because of the associative law in G.

Again, like any equivalence relation, the group G gets partitioned up into equivalence classes, called the *right cosets* of G with respect to K. Precisely,

DEFINITION 5.5. The right coset of $g \in G$ with respect to the subgroup K is the set

$$Kg = \{kg \mid k \in K\}$$

of elements of G congruent to g modulo K.

5.2. Left Cosets. Similarly, we can define g and h to be left congruent if $g^{-1} \star h \in K$. The equivalence classes of this equivalence relation are the left cosets $gK := \{gk \mid k \in K\}$. Though which convention we chose to work with (left or right) is not important, we **caution** the reader that gK and Kg may be **different** subsets of G. That is, left and right congruence define different equivalence relations on G, and therefore result in different partitions of G into equivalence classes. Of course, if G is abelian, this issue does not arise. For example, the coset of an integer a with respect to the subgroup $n\mathbb{Z}$ is always just the congruence class of a modulo n, whether we consider left or right cosets.

EXAMPLE 5.6. Let us compute the left cosets of the rotation group R_4 inside D_4. Since R_4 is closed under multiplication,

$$I \circ R_4 = r_1 \circ R_4 = r_2 \circ R_4 = r_3 \circ R_4$$

is one coset, consisting of the rotations of the square. There is only one other coset, as you can check:

$$H \circ R_4 = A \circ R_4 = V \circ R_4 = D \circ R_4,$$

[6] although usually we prefer not to, since when G is not abelian, this may lead to confusion.

consisting of the reflections. Note that in this example, the right cosets yield the same partition of G into rotations and reflections.

For any subgroup K of a group G, the subgroup K itself is always a coset—indeed, it is both the left and right coset of the identity element e. Of course, no other coset is a subgroup, since none of these non-overlapping sets will contain e.

Can we define a group structure on the set of (say, left) cosets of a group G with respect to some subgroup K? After all, this was easy to do for $\mathbb{Z}_n$.

The answer is **NO** in general. Indeed, suppose we have two left cosets aK and bK. Why not just define their product to be abK? The reason is that this may depend on the choice of representative for the cosets! Indeed, if a' and b' had been different representatives, which is to say that $a = a'k_1$ and $b = b'k_2$ for some elements k_1 and k_2 in K, then in order for this operation to be well defined, we would need

$$ab(a'b')^{-1} \in K$$

But $ab = a'k_1b'k_2$, and there is no guarantee that we can swap k_1b' to $b'k_1$. All we really would need is that $k_1b' = b'k''$, for some $k'' \in K$, but this is not guaranteed! In general, **The set of (left) cosets of K in G does not have an induced group structure in a natural way.** Our calculation shows that in order to induce a well-defined multiplication on the (left) cosets, the precise condition we need is that for all $b \in G$ and all $k \in K$

$$b^{-1}kb \in K.$$

In other words, K must be a *normal subgroup* of G.

DEFINITION 5.7. A subgroup K of G is *normal* if $g^{-1}Kg \subset K$ for all $g \in G$.

Equivalently (prove it!) a subgroup K of G is normal if and only if $gK = Kg$ for all $g \in G$—that is, left and right congruence modulo K partitions G up into equivalence classes in the same way: the left and right cosets are the same.

If K is a normal subgroup, we will denote by G/K the set of cosets[7] of G with respect to G. Our discussion above shows that the set G/K has an naturally induced "multiplication":

$$gK \star hK = g \star hK$$

which is independent of the choices of g and h here to represent the cosets.

DEFINITION 5.8. For a normal subgroup K of a group $(G, \star)$, the *quotient group* of G with respect to K, denoted G/K, is the set of cosets of G with respect to K, together with the induced operation $gK \star hK = g \star hK$.

You should verify that G/K really satisfies the axioms of a group. Again, we emphasize that the elements of G/K are *subsets* of G. In particular, the identity element is the coset

[7] left or right, as we mentioned above, they are the same

eK of the identity element, the subset K. Of course, if K is the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, we recover the usual modular group $\mathbb{Z}_n$. That is, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

DEFINITION 5.9. If K is a normal subgroup of a group G, then the natural map

$$G \to G/K$$

sending each element of G to its coset with respect to K is a surjective homormorphism. This natural map is often called the *canonical surjection* or the *quotient map.*

EXERCISE 5.10. The *kernel* of a group homomorphism $\phi : G \to H$ is the set of elements in G which are sent to the identity under ϕ. Show that a subgroup K of G is normal if and only if it is the kernel of some group homomorphism.

5.3. Lagrange's Theorem. Even when K is not normal, the set of (left, say) cosets can be an interesting object of study, even though it doesn't have a natural group structure. For example, although most cosets *are not subgroups of* G*,* there is certainly a bijection:

$$K \leftrightarrow gK$$

$$k \leftrightarrow gk.$$

So we can think of the cosets as partitioning G up into disjoint sets of "equal size" in some natural way. Indeed, an immediate corollary is the following fundamental fact:

THEOREM 5.11 (Lagrange's Theorem). *If* G *is a finite group, the order of any subgroup of* G *divides the order of* G*.*

The number of cosets of G in K is called the *index* of K in G, and denoted $[G : K]$. By definition, if K is normal, the index is equivalently described as the order of the quotient group G/K.

Put differently, the equivalence relation "congruence modulo K" partitions a finite set G up into $[G : K]$ disjoint sets, all of cardinality $|K|$. Thus, $|G| = [G : K]|K|$ for any subgroup K of a finite group G.

Of course, infinite groups can have finite index subgroups; for example, $n\mathbb{Z}$ has index n in $\mathbb{Z}$.

EXERCISE 5.12. Let $L \subset \mathbb{R}^2$ be a one-dimensional vector subspace. Thinking of this inclusion as an inclusion of (additive) groups, compute the cosets with respect to L.

6. Group Actions

Let $(G, \star)$ be a group, and X any set (finite or infinite).

DEFINITION 6.1. An *action* of G on X is a map

$$G \times X \to X$$

$$(g, x) \mapsto g \cdot x$$

which satisfies

(1) $g_1 \cdot (g_2 \cdot x) = (g_1 \star g_2) \cdot x$ for all $g_1, g_2 \in G$ and all $x \in X$.
(2) $e_g \cdot x = x$ for all $x \in X$.

Intuitively, an action of G on X is a way to assign to each g in G some transformation of X, compatibly with the group structure of G. Formally, the action of a group G on a set X is *equivalent to* a homomorphism of groups

$$\rho : G \to \text{Aut } X,$$

defined by sending each g in G to the set map

$$\rho_g : X \to X$$
$$x \mapsto g \cdot x.$$

The map ρ_g is a bijection (that is, an element of Aut X) with inverse $\rho_{g^{-1}}$. The fact that ρ is a group homomorphism is essentially a restatement of condition (1): unraveling the meaning of $\rho(g_1 \cdot g_2) = \rho(g_1) \circ \rho(g_2)$ we arrive at $g_1 \cdot (g_2 \cdot x) = (g_1 \star g_2) \cdot x$ for all $x \in X$. Sometimes this group homomorphism is called the *associated representation* of the action or the *permutation representation* of the action. Despite the fancy name, it is really just a different packaging of the same idea: the action of a group G on a set X is *tautologically equivalent to* a homomorphism $G \to$ Aut X.

The easiest example of a group action is the group $G =$ Aut X acting on X. By definition, G acts on X via $(\phi, x) \mapsto \phi(x)$. The homorphism ρ is the identity map. For example, if X is the set $\{1, 2, \ldots, n\}$, then S_n acts tautologically on X by permutations.

Another easy example is the group $G = GL_n(\mathbb{R})$ of invertible $n \times n$ matrices acting on the space $\mathbb{R}^n$ of column matrices by left multiplication. This is equivalent to giving a group homomorphism

$$G \to \text{ Aut}(\mathbb{R}^n).$$

Of course, the image of this representation is the group $\mathrm{GL}(\mathbb{R}^n)$ of all *(invertible) linear transformations* of $\mathbb{R}^n$, and the map is the isomorphism identifying linear transformations with matrices via the choice of the standard basis of unit column vectors in $\mathbb{R}^n$.

In nature, groups act naturally on sets which often have some additional structure—for example, a vector space structure or a manifold structure. Often, we are mostly interested in actions that respect this additional structure. For example, in the example above, the group $G = GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ in way that preserves the vector space structure of $\mathbb{R}^n$. That is, each element of G gives rise to a bijective *linear* transformation of $\mathbb{R}^n$, which is of course a very special kind of bijective self-map. We say that $GL_n(\mathbb{R})$ acts *linearly* $\mathbb{R}^n$.

Definition 6.2. A *linear representation* of a group G on a vector space V is an action of G on the underlying set V which respects the vector space structure. More precisely, the corresponding group homomorphism

$$G \to \quad \text{Aut } V$$

has image in the subgroup $GL(V)$ of *linear transformations* of V.

More succiently put, a linear representation of a group G on a vector space V is a homomorphism $G \to GL(V)$. When the field is not implicitly understood, we qualify by its name: For example, a complex representation of a group G is a group homomorphism $G \to GL(V)$ where V is a *complex* vector space.

EXAMPLE 6.3. Let us consider some different actions of the dihedral group D_4 of the square. Perhaps the simplest is the action of D_4 on the set of vertices of the square. If we label the vertices $\{1, 2, 3, 4\}$, say, in clockwise order from the top right, this gives an action of D_4 on the set $\{1, 2, 3, 4\}$. The corresponding homomorphism to Aut $\{1, 2, 3, 4\}$ gives a map

$$\rho : D_4 \to S_4$$

sending for example r_1 to the 4-cycle (1234) and the reflection H to the permutation (12)(34). The group homomorphism ρ is *injective*—a non-trivial symmetry of the square cannot fix all vertices. This is an example of a *faithful action:*

DEFINITION 6.4. A action of a group G on a set X is *faithful* if each non-identity element of G gives rise to a non-trivial transformation of X. Equivalently, an action is faithful if the corresponding group homomorphism $G \to \text{Aut } X$ is injective. Put differently, **a faithful action of a group G on a set X is a way to identify G with a group of transformations of X.**

6.1. The tautological representation of a dihedral group. The **tautological action** of D_4 on the Euclidean plane is given by the very definition of D_4 as the rigid motions of the plane which preserve the square. This action is also faithful. These two different action give two different ways of viewing D_4 as a transformation group—the first identifies D_4 with a subgroup of S_4, and the second identifies D_4 with a subgroup of Aut $(\mathbb{R}^2)$.

Let us consider the tautological representation

$$\rho : D_4 \to \text{ Aut } (\mathbb{R}^2)$$

in detail. Fix coordinates so that the square is centered at the origin. Then ρ sends the rotation r_1 to the corresponding rotation of $\mathbb{R}^2$, and so on. Because both rotations and reflections are *linear transformations* of $\mathbb{R}^2$, the image of ρ actually lies in $GL(\mathbb{R}^2)$. Identifying elements of $\mathbb{R}^2$ with column vectors so that linear transformations are given by left multiplication by 2×2 matrices, the elements r_1, r_2, r_3 respectively are sent to the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

respectively, whereas the reflections H, V, D and A are sent to

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

respectively. Put differently, we can identify the symmetry group of the square with the matrix group consisting of these seven 2×2 matrices and the identity matrix.

6.2. The action of F^* on a vector space. Let V be a vector space over a field F. The multiplicative group F^* of the field acts on the set V by scalar multiplication. In fact, it is not hard to show that a set V is an F-vector space if and only if V is an abelian group with an F^* action.

6.3. The action of a group on itself by left multiplication. Let $(G, \star)$ be any group, and write X for a second copy of the underlying set of G. We have an action

$$G \times X \to X$$

$$(g, x) \mapsto g \star x$$

of G on itself (that is, $X = G$) by left multiplication.

The action of G on itself is *faithful.* Indeed, if $g \in G$ acts trivially on *every* $x \in X$, then $gx = x$ for all $x \in X = G$. But this implies that $g = e_G$, so the corresponding group homomorphism

$$\rho : G \to \mathrm{Aut}G$$

$$g \mapsto [G \to G;\ x \mapsto gx]$$

is injective.

Thus, *any group G is isomorphic to its image under this representation ρ.* That is, we have proved

Theorem 6.5 (Cayley's Theorem). *Every group $(G, \star)$ is a transformation group. Specifically, G is isomorphic to a subgroup of Aut G.*

As a corollary, this says that every group of (finite) order n is isomorphic to a subgroup of S_n. Thus abstract groups always have concrete realizations as permutation groups.

6.4. The action of group on itself by conjugation. Let G be any group, and let X denote the underlying set of G. We have an action of G on itself:

$$G \times X \to X$$

$$(g, x) \mapsto g \star x \star g^{-1}.$$

This is quite different from the previous action of G on itself. For example, it is not usually faithful! Indeed, an element $g \in G$ fixes all $x \in X$ if and only if $g \star x \star g^{-1} = x$ for all $x \in X$. Equivalently, g acts trivially on X if and only if g commutes with all $x \in G$, that is, if and only if g is in the *center* of G.

Exercise 6.6. Show that the kernel of the conjugation representation

$$\rho : G \to \mathrm{Aut}G$$

$$g \mapsto \left[G \to G;\ x \mapsto gxg^{-1}\right]$$

is the center of G. Compute the kernel of the conjugation representations of D_4 and S_3.

6.5. Groups acting on sets with interesting structure. In these examples, the set X on which G acts has more structure than a mere set: it is of course a group! Do these actions preserve the group structure of X? That is, the induced map $\rho(g) : G \to G$ actually a map of *groups*, ie, a group homomorphism?

For the action of G on itself by left multiplication, the group structure is *not* preserved. Indeed, the identity element is not even sent to the identity element. However, the conjugation action *does* preserve the group structure:

$$G \to G$$
$$x \mapsto gxg^{-1}$$

is easily checked to be a *group homomorphism.* Thus this is a special type of representation of G. The image of the corresponding map

$$\rho : G \to \mathrm{Aut}G$$

actually lands in the subgroup of *group automorphisms,* or self-isomorphisms of G, denoted $\mathrm{Aut}_{Grp}G$. For this reason, we can expect this representation to play an especially important role in the theory of groups.

Exercise 6.7. Suppose a group G acts on a set X. The stabilizer of a point $x \in X$ is the set $\mathrm{Stab}(x) = \{g \in G | g \cdot x = x\}$.

(1) Show that $\mathrm{Stab}(x)$ is a subgroup of G.
(2) Compute the stabilizer in D_4 of a vertex of the square, under the tautological action.
(3) Characterize a faithful action in terms of stabilizers.

Exercise 6.8. Suppose a group G acts on a set X. The orbit of a point $x \in X$ is the set $\mathrm{O}(x) = \{y \in G \mid \text{there exists } g \in G \text{ such that } y = g \cdot x\}$.

(1) Compute the orbit of a vertex of the square under the tautological action of D_4.
(2) Compute the orbit of a point $x \in G$ under the action of G on itself by left multiplication.
(3) Compute the orbit of a point $z \in \mathbb{C}$ under the action of the circle group $U(1)$ by multiplication.

CHAPTER 3

Group Representations

1. Linear Representations

We repeat the fundamental concept: a linear representation of a group G on a vector space V is an action of G on V by *linear transformations*—that is, is a way of assigning some *linear* transformation of V to each element of G, compatible with the group structure of G. More formally,

DEFINITION 1.1. A *linear representation of a group* G *on a vector space* V is a group homomorphism

$$G \to GL(V).$$

We will usually omit the word "linear" and just speak of a *representation* of a group on a vector space, unless there is a chance of confusion. There are many ways to refer to this fundamental idea—we sometimes also say V is a "G-representation" or V is a "G-module." This an abuse of terminology since there can be many different actions of G on a given vector space—we need to know which action is intended!

A representation has *dimension* d if the vector space dimension of V is d. (Some books use the term *degree* of V).

For example, **the tautological representation of** D_n on $\mathbb{R}^2$ induced by the action of D_n on the plane by linear transformations is a two-dimensional representation of D_n. We explicitly described the map $D_n \to GL(\mathbb{R}^2)$ in the previous lecture for $n = 4$. The tautological representation is *faithful* since every non-identity element of D_4 is some non-trivial transformation of the plane.

Every group admits a **trivial representation** on every vector space. The trivial representation of G on V is the group homomorphism $G \to GL(V)$ sending every element of G to the identity transformation. That is, the elements of G all act on V trivially—by doing nothing.

1.1. Permutation Representations. Suppose a group G acts on a set X. There is an associated (linear) **permutation representation** defined over any field. Consider the F-vector space on basis elements e_x indexed by the elements x of X. Then G acts by permuting the basis elements via its action on X. That is $g \cdot e_x = e_{g \cdot x}$. For example, S_3 has a three-dimensional representation defined by

$$S_3 \to GL(\mathbb{R}^3)$$

sending, for example,

$$(12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \ (13) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}; \ (123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

More generally, there is an analogous permutation representation of S_n on $\mathbb{R}^n$, or indeed on F^n for any field F, induced by the action of S_n on a basis. This is called the **Permutation Representation** of S_n.

The **Vertex Permutation** representation of D_4 on $\mathbb{R}^4$ is induced by the action of D_4 on the vertices of a square which index a basis for $\mathbb{R}^4$. Similarly, D_n has a vertex permutation representation on $\mathbb{R}^n$, or even on $\mathbb{F}^n$ for an arbitrary field F, for any $n \geq 3$.

1.2. The **Regular Representation** is perhaps the most important type of permutation representation. The regular representation of a group G is the permutation representation induced by the action of G on itself by left multiplication. In particular, the dimension of the regular representation is $|G|$. The regular representation over the field $\mathbb{F}$, for example, is given by the group homomorphism

$$G \to GL(\mathbb{F}^{|G|})$$

$$g \mapsto \left[g : \mathbb{F}^{|G|} \to \mathbb{F}^{|G|};\ e_h \mapsto e_{gh} \right].$$

For example, we have a representation of D_4 on $\mathbb{R}^8$ induced this way. The regular representation is defined even when G is infinite, but we usually consider it only for finite groups. The regular representation is faithful, since *every* non-identity element of G moves each basis element to some other basis element: $g \cdot e_h = e_{gh}$ for all g and h in G. In particular, the orbit of any basis vector is the full set of basis vectors $\{e_g\}_{g \in G}$. That is, G acts transitively on our chosen basis.

1.3. The alternating representation of S_n. Let σ be any permutation of n objects. Write σ as a composition of transpositions $\sigma = \tau_1 \circ \dots \tau_t$, where each τ_i just interchanges two elements, fixing the others. Of course, there may be many ways to do this (for example, the identity is $(12)(12)$) but you can check that the parity of t is well-defined. We say the *sign* of σ is 1 or -1 depending on whether σ is a product of an even or an odd number of transpositions. That is, there is a well-defined map

$$sign : S_n \to \{\pm 1\}$$

$$\sigma = \tau_1 \circ \dots \circ \tau_t \mapsto (-1)^t$$

where the τ_i are transpositions. Note that the set $\{\pm 1\}$ forms a group under multiplication, isomorphic to $\mathbb{Z}_2$, and that this map is a group homomorphism.

The **alternating representation** of S_n is the one-dimensional representation (defined over any field $\mathbb{F}$) in which each σ acts by multiplication by its sign. The corresponding group homomorphism is the composition

$$S_n \xrightarrow{sign} \{\pm 1\} \subset \mathbb{F}^* = GL(\mathbb{F}).$$

2. A digression on some uses of representation theory in real math, expressed in fancy language

Suppose that a group acts on a set X, and that the set X has some interesting structure we want to preserve. We have already considered at length the case where X is a vector space, and G acts by linear transformations on X. But it may also arise quite naturally that X is a topological space, say, and that G acts by *homeomorphisms* on X.

Put differently, if X belongs to some interesting *category* of mathematical objects, we often look at automorphisms of X in that category instead of merely the automorphisms of X as a set. The term category can be taken here in its precise technical meaning or more informally, depending on the reader's background and inclination. However, because the language of category theory is so ubiquitous in algebra, it is probably a good idea for the student to start hearing it, at least informally.

In the category of vector spaces, an automorphism is simply an invertible linear map, so the set $\mathrm{Aut}_{vec}(X)$ of automorphisms in the category of vector spaces (which is a group under composition) is just the subgroup $GL(X)$ of Aut X preserving the vector space structure of X. In the category of topological spaces, an automorphism is simply a self-homeomorphism. Of course, the composition of homeomorphisms is a homeomorphism, and the inverse of any homeomorphism is a homeomorphism, which means that the collection $\mathrm{Aut}_{top}(X)$ of all self-homeomorphisms of X is a *subgroup* of $\mathrm{Aut}(X)$, the group of *all* bijective self-maps of X as a set. A similar story holds if X has even more structure—for example, a smooth manifold structure, in which case, we'd like to consider the group of all self-diffeomorphisms of X.

In nature, topological spaces (especially manifolds) are quite common—probably much more common than their simpler cousin $\mathbb{R}^n$— and often come with natural group actions on them. For example, space-time is a manifold, on which a group of coordinate changes acts. So we get natural representations of groups on topological spaces or manifolds which require study. This is much harder than studying linear representations on vector spaces—linear algebra is easier than geometry—but fortunately, it often happens that there is a natural way to transform an action of a group on a topological space or manifold into some corresponding action on an associated vector space. Indeed, this sort of thing is ubiquitous throughout mathematics—precisely because linear algebra is much easier to deal with.

For example, given a topological space X, its homology and cohomology groups form natural vector spaces associated to X. If a group acts on X (by homeomorphisms of course), there will be an induced action on its homology and cohomology groups (by linear transformations). This reduces the study of a group action on a topological space to study of a linear representation of the same group—-the subject of this course! Similarly, we can often reduce the study of a group action on a manifold (by diffeomorphisms) to a corresponding study of the same group acting on the tangent space to X at a point (by linear transformations). The advantage is that representation theory provides powerful tools for dealing with the linear algebra.

2.1. Categories and Functors. Roughly speaking, a **category** is a collection of mathematical objects with some common structure, together with a notion of mappings between them respecting that structure ("morphisms"). For example, we have the category of groups (with group homomorphisms), the category of vector spaces over a fixed field (with linear mappings), the category of topological spaces (with continuous mappings), the category of smooth manifolds (with smooth mappings), and the category of sets (with set mappings), to name just a few familiar categories. A few axioms are needed to work at this level of abstraction—for example, there should be a notion of composition of morphisms—- but in practice, these axioms are so obvious so as to be hardly worth mentioning.

In any category (whether groups, topological spaces, etc), there is a notion of "sameness" for our objects: groups are "the same" if they are isomorphic, topological spaces are "the same" if they are homeomorphic, and so on. In general, the notion of isomorphism is defined in any category by the existence of morphisms (in that category!) $X \to Y$ and $Y \to X$ which are mutually inverse. The *automorphisms,* or self-isomorphisms, of a fixed object X in any category form a group under composition. For example, the set of all automorphisms of a set X is simply the group Aut X already discussed, and the set of automorphisms of a vector space V is the group $\mathrm{GL}(V)$ of linear transformations of V. Likewise, if X is a topological space, the group $\mathrm{Aut}_{top}(X)$ of self-homeomorphisms of X is a group, which may be very large in general.

A **functor** is a mapping from one category to another, which of course, preserves the structures. For example, a functor Γ from the category of topological spaces to the category of groups is a gadget which assigns to each topological space X, some group $\Gamma(X)$, *and to each continuous mapping of topological spaces* $X \to Y$ some corresponding group homomorphism $\Gamma(X) \to \Gamma(Y)$. For example, the assignment of the fundamental group to each topological space is a functor from the category $\{\mathbf{Top}\}$ to $\{\mathbf{Gp}\}$. Naturally, the assignment must satisfy some basic properties in order to be a functor: it should send the identity map in one category to the identity map in the other for example, and it is should preserve compositions. The reader can look up the precise definition of a functor in any book on category theory (or most graduate level texts on algebra).

Representation theory is so useful in physics and mathematics because group actions— symmetries— are everywhere, on all sorts of structures from individual molecules to space-time. We have invented nice functors to transform these actions into actions on vector spaces—that is, into linear representations of groups. And finally, linear algebra is something we have plenty of tools for—even computers can be easily programmed to do linear algebra. So although linear representations of groups on vector spaces may seem quite abstract and algebraic, it is an excellent way of understanding symmetry at the micro-and-macroscopic levels throughout the universe.

3. Sub-representations.

Unless otherwise explicitly stated, we now consider only finite dimensional *linear representations.*

A sub-representation is a subvector space which is also a G-representation under the *same* action of G. More precisely

DEFINITION 3.1. Let V be a linear representation of a group G. A subspace W of V is a sub-representation if W is invariant under G—that is, if $g \cdot w \in W$ for all $g \in G$ and all $w \in W$.

In terms of the group homomorphism

$$\rho : G \to GL(V),$$

W is a sub-representation if and only if ρ factors through the subgroup

$$G_W = \{\phi \in GL(V) \mid \phi(W) \subset W\}$$

of linear transformations stabilizing W.

For example, every subspace is a sub-representation of the trivial representation on any vector space, since the trivial G action obviously takes every subspace back to itself. At the other extreme, the tautological representation of D_4 on $\mathbb{R}^2$ has no proper non-zero sub-representations: there is no line taken back to itself under *every* symmetry of the square, that is, there is no line left invariant by D_4.

The vertex permutation representation of D_4 on $\mathbb{R}^4$ induced by the action of D_4 on a set of four basis elements $\{e_1, e_2, e_3, e_4\}$ indexed by the vertices of a square *does have* a proper non-trivial sub-representation. For example, the one dimensional subspace spanned by $e_1 + e_2 + e_3 + e_4$ is fixed by D_4— when D_4 acts, it simply permutes the e_i so their sum remains unchanged. Thus for all $g \in G$, we have $g \cdot (\lambda, \lambda, \lambda, \lambda) = (\lambda, \lambda, \lambda, \lambda)$ for all vectors in this one-dimensional subspace of $\mathbb{R}^4$. That is, D_4 acts trivially on this one-dimensional sub-representation.

Another sub-representation of the vertex permutation representation of D_4 on $\mathbb{R}^4$ is the subspace $W \subset \mathbb{R}^4$ of vectors whose coordinates sum to 0. Clearly, when D_4 acts by permuting the coordinates, it leaves their sum unchanged. For example H sends $(1, 2, 3, -6)$ to $(-6, 3, 2, 1)$ if the vertices are labelled counterclockwise from the upper right. The space W is a three dimensional sub-representation of the permutation representation of D_4 on $\mathbb{R}^4$. Note that W is a *non-trivial* sub-representation since the elements of G *do* move around the vectors in the space W.

3.1. The Standard Representation of S_n. One important representation is the standard representation of S_n, which is defined as a sub-representation of the permutation representation of S_n. Let S_n act on a vector space of dimension n, say $\mathbb{C}^n$, by permuting the n vectors of a fixed basis (say, the standard basis of unit column vectors in $\mathbb{C}^n$). Note that the subspace spanned by the sum of the basis elements is fixed by the action of S_n—that is, it is a sub-representation on which S_n acts trivially. But more interesting, the $n-1$-dimensional subspace

$$W = \{ \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad | \quad \sum x_i = 0 \} \subset \mathbb{C}^n$$

is also invariant under the permutation action. This is called the **standard representation** of S_n.

4. Direct Sums of Representations.

Suppose a group G acts on the vector spaces V and W (over the same field, $\mathbb{F}$). We can define an action of G "coordinate-wise" on their direct sum as follows:

$$g \cdot (v, w) = (g \cdot v, g \cdot w) \in V \oplus W.$$

Note that if V has basis $v_1, \dots, v_n$ and W has basis $w_1, \dots w_m$, then the direct sum has basis $v_1, \dots, v_n, w_1, \dots w_m$ (where v_i is interpreted to mean $(v_i, 0)$, etc). With this choice of basis for the direct sum, the matrix of every g acting on $V \oplus W$ will be the block diagonal matrix

$$\begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}$$

obtained from the $n \times n$ matrix $\rho_1(g)$ describing the action of g on V in given basis, and the $m \times m$ matrix $\rho_2(g)$ describing the action of g on W in its given basis.

For example, we have a three-dimensional real representation of D_4 defined as follows:

$$g \cdot (x, y, z) = (g \cdot (x, y), z),$$

where $\dot{g}(x, y)$ denotes the image of (x, y) under the tautological action of D_4 on $\mathbb{R}^2$. In the standard basis, for example, the element $r_1 \in D_4$ acts by the matrix

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This representation is the *direct sum* of the tautological and the one-dimensional trivial representations of D_4.

Of course, we also have a representation of D_4 on $\mathbb{R}^3$ where D_4 acts trivially in the x-direction and by the tautological action in the yz plane direction: $g \cdot (x, y, z) = (x, g \cdot (y, z))$. This is also a direct sum of the trivial and tautological representation. In fact, just thinking about these actions there is a very strong sense in which they are "the same." We are led to the following definition:

Definition 4.1. Two linear representations V and W of G (over the same field) are *isomorphic* if there is a vector space isomorphism between them that preserves the G-action—that is, if there exists an isomorphism $\phi : V \to W$ such that $g \cdot \phi(v) = \phi(g \cdot v)$ for all $v \in V$ and all $g \in G$.

The idea that ϕ preserves the G action is also expressed by the following commutative diagram, which must hold for all $g \in G$:

$$\begin{array}{ccc} V & \xrightarrow{g} & V \\ \phi \downarrow & & \phi \downarrow \\ W & \xrightarrow{g} & W \end{array}.$$

For example, the two representations of D_4 discussed above are isomorphic under the isomorphism which switches the x and z coordinates.

We are especially interested in decomposing representations in direct sums of sub-representations. For example, the permutation representation of S_n on $\mathbb{C}^n$ is easily seen to be isomorphic to the direct sum of the trivial and standard sub-representations discussed in 3.1 above:

$$\mathbb{C}^n \cong \mathbb{C} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \bigoplus W,$$

where W is the subspace of vectors whose coordinates sum to zero.

5. Mappings of Representations.

Given two representations of a fixed group G over the same field, we define a mapping between them as follows:

Definition 5.1. A *homomorphism* of (linear) G-representations is a map $\phi : V \to W$ which preserves both the vector space structure and the G-action. That is, it is a linear map ϕ of vector spaces (over the same field) satisfying $g \cdot \phi(v) = \phi(g \cdot v)$ for all $v \in V$ and all $g \in G$.

There are many different words for the notion of a homomorphism of representations, probably because representation theory is used in so many different places in mathematics and science. The terms "G-linear mapping", "G-module mapping," or even just "a map of representations of G" are common. The adjective "linear" is often suppressed: if the representations are linear, so also are the homorphisms between them assumed to be *linear* homomorphisms. But, depending on the context, it may also be interesting to study group actions on, say, a topological space, in which case the corresponding representations should be *continuous,* and the maps between them as well should be continuous.

An isomorphism of G-representations is simply a bijective homomorphism. On the other hand, it might be better to think of an isomorphism as a homomorphism $\phi : V \to W$ which has an inverse homomorphism, because this way of thinking is valid more broadly throughout mathematics.[1] But for representations, you can check that if $\phi : V \to W$ is a bijective linear transformation, then the inverse map $\phi^{-1} : W \to V$ is also a linear map, and that if ϕ preserves the group action, so does ϕ^{-1}. To wit: $g \cdot \phi(v) = \phi(g \cdot v)$ for all $v \in V$ if and only if $g^{-1} \cdot \phi^{-1}(w) = \phi^{-1}(g^{-1} \cdot w)$ for all $w \in W$.

The **inclusion** of any sub-representation W of a representation V of a group G provides an example of an injective homomorphism of representations. Indeed, $\phi : W \hookrightarrow V$ obviously satisfies $g\phi(w) = \phi(gw)$ because, by definition of sub-representation, the action of G is the same on elements of W whether we think of them in W or V.

The **projection** $\pi : V \oplus W \to V$ from a direct sum of G-representations onto either factor is an example of a surjective homomorphism. Again, that this map is G-linear is easy to verify directly from the definitions (do it!).

Although it is far from obvious, these examples—isomorphism, inclusion, and projection—are virtually the *only* homomorphisms between representations, at least for finite dimensional representations of finite groups G. Perhaps this is not surprising: a similar fact is true for vector spaces. If $\phi : V \to W$ is a linear map of vector spaces, then because $V \cong im\,\phi \oplus ker\,\phi$, every mapping of vector spaces essentially factors as projection onto the image followed by inclusion of the image into the target. On the other hand, nothing like this is remotely true for most sorts of maps between mathematical objects: there are all sorts of group homomorphisms, such as $\mathbb{Z} \to \mathbb{Z}_n$, which are not of this sort.

6. Homomorphisms of Representations are rare.

Let us consider two representations of D_4: the tautalogical representation T (which is the vector space $\mathbb{R}^2$, with the tautological D_4 action) and the vertex permutation representation V (namely, the vector space $\mathbb{R}^4$ with basis elements indexed by the vertices of a square, with the action of D_4 given by permuting the vertices according to the action of D_4 on the vertices.) Of course, there are many linear mappings from $\mathbb{R}^2$ to $\mathbb{R}^4$. Do any of these preserve the group action? That is, are any of them homomorphisms of the D_4-representations $T \to V$. Of course, stupidly, we could take the zero-map $T \to V$ mapping every element of $\mathbb{R}^2$ to $\mathbb{R}^4$. This preserves the group action, but it is not interesting. Can we find any injective maps?

Let us consider whether the inclusion

$$i : \mathbb{R}^2 \to \mathbb{R}^4$$

sending

$$(x, y) \mapsto (x, y, 0, 0)$$

[1] Indeed, this is how the notion of "same-ness" or isomorphism can be defined in any category. For example, an isomorphism in the category of topological spaces—or homeomorphism— is a continuous map which has a continuous inverse; it is not enough to have a bijective continuous map.

is D_4-linear. For example, does this preserve the action of the element r_1 in D_4. We have that $r_1 \cdot (x, y) = (-y, x)$ for the representation T, which yields $(-y, x, 0, 0)$ under the inclusion map i, where as $r_1 \cdot (x, y, 0, 0) = (0, x, y, 0)$ for the representation V. This means that i *does not* respect the group structure— the linear map i is *not* a map of representations of D_4.

6.1. Searching for sub-representations. Can there be *any* injective map of representations $T \to V$? If so, then the image of T would be a two-dimensional subspace of the four-dimensional space V where the the vertex permutation representation restricts to the tautological representation. Is this possible? Essentially, we are asking whether there is any two-dimensional square in four space on which the vertex permutation action of D_4 (given by permuting the coordinates as D_4 permutes the vertices of a square) agrees with the usual symmetries of that square. Clearly, this can happen only if there is a set of four points in $\mathbb{R}^4$ spanning a two-dimensional subspace invariant under this action.

To understand the permutation action of D_4 on $\mathbb{R}^4$ it is helpful to identify D_4 with the subgroup of S_4 generated by the 4-cycle (1234) (the rotation r_1) and the transposition (13) (the reflection A). Formally, we are embedding D_4 in S_4 by sending each symmetry to the corresponding permutation of the vertices. The 4-cycle acts by cycling the coordinates (one spot to the right, say), and the transposition acts by switching the first and third coordinates. Since D_4 is generated by these two elements, a subspace is invariant under D_4 if and only if it is invariant under these two elements (Prove it!).

To see whether the permutation representation has any sub-representation isomorphic to T, then, we are looking for four points in $\mathbb{R}^4$ spanning a two-dimensional subspace, and invariant under these two transformations, which can serve as the vertices of a square. Can one of these points be, say $(1, 0, 0, 0)$? Note that when r_1 acts on this vector in V, it moves it to $(0, 1, 0, 0)$. When it acts again—in other words when r_2 acts on $(1, 0, 0, 0)$— we get $(0, 0, 1, 0)$. Again, and we get $(0, 0, 0, 1)$, and then we cycle back to $(1, 0, 0, 0)$. Thus, any vector subspace of V containing $(1, 0, 0, 0)$ and invariant under D_4 must contain each of the four standard basis elements—that is, it must be V, since these span V. Indeed, it is easy to check that this sort of thing happens for "most vectors:" typically, the orbit of a randomly chosen vector in V will consisting of (eight) vectors which span V.

To find interesting sub-representations of V, we can look for non-zero vectors whose orbits span proper subspaces of V. One way is to find vectors with small orbits. For example, the vector $(1, 1, 1, 1)$ is fixed by D_4. It spans a one dimensional sub-representation of V where D_4 acts trivially, as we have already noted.

Another vector with a small orbit is $w = (-1, 1, -1, 1)$. Note that r_1 acts on w to produce $(1, -1, 1, -1)$, which is $-w$. Also, the reflection A acts by permuting the first and third coordinates, which means it fixes w. Since *every* element in D_4 is an iterated composition of the generators r_1 and A, we see that the D_4-orbit of w is the two element set $\{w, -w\}$. Thus the one-dimensional subspace spanned by w is a sub-representation of V. This is *not* a trivial representation—some element acts by multiplication by -1.

How does this help us find two dimensional sub-representations of V isomorphic to T, or show none exist? Well, clearly if any such two-dimensional sub-representation exists, it can not contain $(1,1,1,1)$, since T fixes *no* subspace. Nor could it contain $(1,-1,1,-1)$ since r_1 acts there by multiplication by -1 but r_1 is *never* scalar multiplication on T. Thus, we need to look for a vector in V whose orbit does not contain either of these two special vectors (nor anything in their span).

Consider the vector $(1,1,-1,-1)$. Its orbit produces the four points

$$(1,1,-1,-1),\ \ (-1,1,1,-1),\ \ (-1,-1,1,1),\ \ (1,-1,-1,1),$$

and so it *does* generate a two-dimensional sub-representation T' of V (which has basis, for example, $(1,1,-1,-1),(-1,1,1,-1)$.) It is easy to check that the vertex permutation action of D_4 on T' *does restrict* to the tautological representation of D_4 on this two-plane. Indeed, the four points described above serve nicely as the vertices of a square on which D_4 acts by the usual symmetry actions. So V *does contain* a sub-representation isomorphic to T, embedded in a rather special way as a skew plane.

Finally, since these three sub-representations span V, there is a direct sum decomposition of representations:

$$V \cong T' \bigoplus \mathbb{R}(1,1,1,1) \bigoplus \mathbb{R}(1,-1,1,-1),$$

where the first summand has basis $\{(1,1,-1,-1),(-1,1,1,-1)\}$ and is isomorphic to the tautological representation of D_4 and the second summand is a trivial representation of D_4, but the third is not isomorphic to either of these. Furthermore, none of these three sub-representations can be further decomposed. Although it is not obvious, we will soon prove that *every representation* of a finite group on a real or complex vector space *decomposes as a direct sum of irreducible representations.*

We isolate for future reference a simple idea used in the previous example:

LEMMA 6.1. *Let V be a linear representation of a group G. Let W be a sub-vector space of V, spanned by the elements $w_1,\dots,w_t$. Then W is a sub-representation if and only if $g\cdot w_i \in W$ for all $i=1,\dots,t$ and each g in one fixed generating set for G.*

PROOF. We leave this as an easy exercise. One slightly subtle point that is needed: If an element g leaves W invariant, then also g^{-1} does. Indeed, the linear transformation $g: V \to V$ is invertible, which means that restricted to W, it is also invertible. So g^{-1} defines its inverse, also on W. $\square$

6.2. The kernel, image and cokernel of a map of representations. The category[2] of G-representations and their maps is very nice from an algebraic point of view: we can form kernel representations, image representations, quotient representations and cokernel representations.

[2]The reader can take the word *category* in an informal sense, or in its full mathematically technical sense here.

Proposition 6.2. *Let $\phi : V \to W$ be a homomorphism of linear representations of a group G. Then the kernel is a sub-representation of V and the image is a sub-representation of W.*

Proof. Since the kernel and image of ϕ are subvector spaces, we only have to check that each is invariant under the G-action. Suppose that $v \in V$ is in the kernel of V, and $g \in G$. We need to check that $g \cdot v$ is in the kernel of ϕ. But $\phi(g \cdot v) = g\phi(v)$ because ϕ is G-linear, and $g\phi(v) = g \cdot 0 = 0$ since v is in the kernel of ϕ and g acts by linear transformations (so preserves the zero).

The proof for the image is also straightforward: $g \cdot \phi(v) = \phi(g \cdot v)$ is in the image of ϕ. $\square$

Whenever there is an inclusion of linear G-representations $W \subset V$, the **quotient representation** V/W can be defined. Indeed, we define V/W as the quotient vector space with the G-action defined by

$$g \cdot \overline{v} = \overline{g \cdot v}$$

where v is any representative of the class. This does not depend on the choice of representative, since if $\overline{v} = \overline{v}'$, then $v - v' \in W$, and whence $g \cdot v - g \cdot v' \in g \cdot W \subset W$, which of course means $g \cdot v$ and $g \cdot v'$ represent the same class of V/W.

In particular, the **cokernel** $W/\mathrm{im}\phi$ of any homomorphism $\phi : V \to W$ of representations of G is also a representation of G.

7. Irreducible Representations

Definition 7.1. A representation of a group on a vector space is *irreducible* if it has no proper non-trivial sub-representations.

For example, the tautological representation T of D_4 is irreducible: if there were some proper non-zero sub-representation, it would have to be one dimensional, but clearly no line in the plane is left invariant under the symmetry group of the square. Indeed, the plane $\mathbb{R}^2$ is irreducible even under the action of the subgroup R_4 of rotations.

On the other hand, the vertex permutation representation is *not* irreducible. For example, the line spanned by the vector $(1, 1, 1, 1)$ or either of the two other subspaces described above in Example 6.1 are non-zero proper sub-representations.

Another example of an irreducible representation is the tautological representation of $GL(V)$ on a vector space V. Indeed, given any non-zero vector $v \in V$, we can always find a linear transformation taking v to any other non-zero vector. In other words, $GL(V)$ acts transitively on the set of non-zero vectors, so there can be no *proper* subset of V left invariant under this action, other than the single element set $\{0\}$.

On the other hand, the action of $GL_n(\mathbb{R})$ on the space of $n \times m$ real matrices by left multiplication (in other words, by row operations) is *not irreducible.* For example, the subspace of $n \times m$ matrices whose last column is zero is certainly invariant under row operations.

To check whether or not a representation is irreducible, it is helpful to think about *sub-representations generated by certain elements:*

DEFINITION 7.2. Let V be any representation of a group G, and S be any sub*set*[3] of V. The *sub-representation* generated by S is the smallest sub-representation of V containing the set S, that is

$$\bigcap_{W \text{ sub-rep of } V \text{containing } S} W.$$

Put differently, the sub-representation of a G-representation V generated by a subset S is the vector space spanned by the vectors in the G-orbits of all the elements in S. For example, the sub-representation of the vertex permutation representation V of D_4 generated by $(1, 0, 0, 0)$ is the whole of V, since r_1 takes $(1, 0, 0, 0)$ to $(0, 1, 0, 0)$, r_2 takes $(1, 0, 0, 0)$ to $(0, 0, 1, 0)$ and r_3 takes $(1, 0, 0, 0)$ to $(0, 0, 0, 1)$.

The following easy fact is more or less obvious:

PROPOSITION 7.3. *A representation is irreducible if and only if it is generated (as a representation) by* **any one** *non-zero vector.*

EXAMPLE 7.4. Consider the additive group $G = (\mathbb{R}, +)$. This has a representation on $\mathbb{R}^2$ given by the group homomorphism

$$(\mathbb{R}, +) \to GL_2(\mathbb{R})$$
$$\lambda \mapsto \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}.$$

Explicitly, the element λ in G acts by sending a column vector $\begin{bmatrix} x \\ y \end{bmatrix}$ to $\begin{bmatrix} x + \lambda y \\ y \end{bmatrix}$. Clearly, the x-axis is a G-invariant subspace—indeed G acts trivially on the one-dimensional subspace of vectors of the form $\begin{bmatrix} a \\ 0 \end{bmatrix}$. In particular, this two dimensional representation of $(\mathbb{R}, +)$ is *not* irreducible.

Are there any other interesting sub-representations? Let us take any vector not on the x-axis, say $\begin{bmatrix} a \\ b \end{bmatrix}$ where $b \neq 0$. When some non-trivial element λ in G acts on $\mathbb{R}^2$, it sends this element to $\begin{bmatrix} a + \lambda b \\ b \end{bmatrix}$, which is obviously *not* a scalar multiple of $\begin{bmatrix} a \\ b \end{bmatrix}$ since $\lambda \neq 0$. Thus, these two vectors span the whole of $\mathbb{R}^2$. This shows that no vector off the x-axis can generate a proper sub-representation— the x-axis is the *only* proper non-zero sub-representation of

[3] emphasis: S need be a sub*set* only, not necessarily a sub-representation or even a subspace

V. Thus, this two-dimensional representation of the additive group $(\mathbb{R}, +)$ has exactly one irreducible non-zero proper sub-representation. In particular, it can not be decomposed into a direct sum of irreducible representations!

EXAMPLE 7.5. Caution! Whether or not a representation is irreducible may depend on the *field* over which it is defined. For example, we have already observed that the tautological representation of the rotation group R_4 on $\mathbb{R}^2$ is irreducible. Explicitly, this is the representation

$$R_4 \to GL_2(\mathbb{R})$$
$$r_1 \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \quad r_2 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \quad r_3 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad e \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Of course, we can also think of this as a representation of the group $\mathbb{Z}_4$, in which case, we will call it the **rotation representation** of $\mathbb{Z}_4$. Of course, the elements $1, -1$ and 0 make sense in any field $\mathbb{F}$, so we can consider the "same" action of R_4 on $\mathbb{F}^2$, for any field! For example, the group map above can be taken to have target say, $GL_2(\mathbb{C})$, instead of $GL_2(\mathbb{R})$.

Let us consider whether the complex rotation representation has any interesting sub-representations. If so, there must be some complex vector $\begin{bmatrix} a \\ b \end{bmatrix}$ which generates a one-dimensional sub-representation of $\mathbb{C}^2$. In particular, we must have

$$r_t \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \lambda_t \begin{bmatrix} a \\ b \end{bmatrix}$$

for each $r_t \in R_4$ and some complex scalar λ_t, depending on r_t. Since R_4 is generated by r_1, we see that it is enough to check this condition just for r_1: the condition for r_t will follow with λ_t taken to be λ_1^t (of course, the condition for the identity element e holds in any case, with the corresponding λ taken to be 1).

That is, the one-dimensional subspace of $\mathbb{C}^2$ spanned by $\begin{bmatrix} a \\ b \end{bmatrix}$ is invariant under R_4 if and only if $\begin{bmatrix} a \\ b \end{bmatrix}$ is an *eigenvector* of the linear transformation r_1. In this case, λ_1 is the corresponding eigenvalue.

Over $\mathbb{C}$, of course, every linear transformation has eigenvectors! Indeed, we can find them by computing the zeros of the characteristic polynomial. For the transformation given by r_1, which is represented by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, the characteristic polynomial is

$$\chi(T) = \det \begin{pmatrix} T & 1 \\ -1 & T \end{pmatrix} = T^2 + 1.$$

Its roots are the complex numbers i and $-i$, and we easily compute the corresponding eigenvectors to be

$$\begin{bmatrix} i \\ 1 \end{bmatrix} \text{ and } \begin{bmatrix} -i \\ 1 \end{bmatrix}.$$

Thus, the two dimensional complex rotation representation of R_4 decomposes into the two one-dimensional representations

$$\mathbb{C}\begin{bmatrix} i \\ 1 \end{bmatrix} \oplus \mathbb{C}\begin{bmatrix} -i \\ 1 \end{bmatrix}.$$

The idea of a *irreducible object* comes up in other algebraic categories as well.[4] For example, we can ask what *groups* have the property that they contain no (normal, say) proper non-trivial subgroups: these are called the *simple* groups. Mathematicians have spent the better part of the last century classifying all the finite simple groups. In other settings, this task is much easier: for example, a vector space has no proper non-trivial subspaces if and only if it has dimension one.

Of course, once one understands all the simple groups (or the "simplest objects" in any category), the next step is to understand how *every group* can be built up from these simple ones. Again, for vector spaces, this is quite easy to understand: every (finite dimensional) vector space is a direct sum of "simple"—meaning one-dimensional—vector spaces. For groups, the story is more complicated. For example, the group $\mathbb{Z}_4$ is *not* simple, as the element $\{\overline{0}, \overline{2}\}$ forms a proper subgroup. However, nor can $\mathbb{Z}_4$ be isomorphic to the direct sum of two smaller groups in a non-trivial way (prove it!). There is a whole theory of *extensions* for groups which treats the question of how arbitrary groups can be built up from simple ones. This is a beautiful story, but not one we digress to discuss here.

Returning to our main interest: what happens for representations? Can every representation of a group be built up out of irreducible ones in some easy to understand way? The answer is as nice as possible, at least for finite groups over familiar fields:

8. Complete Reducibility

THEOREM 8.1. *Every finite dimensional representation of a finite group over the real or complex numbers decomposes into a direct sum of irreducible sub-representations.*

We explictly found such a decomposition for the vertex permutation representation V for D_4. (Example 6.1). The key to proving Theorem 8.1 is the following fact, valid even for infinite dimensional representations:

THEOREM 8.2. *Every sub-representation of a real or complex representation of a finite group has a representation complement. That is, if W is a sub-representation of V, then there exists another sub-representation W' of V such that $V \cong W \oplus W'$ as representations of G.*

REMARK 8.3. The restriction to $\mathbb{R}$ or $\mathbb{C}$ is not really necessary. Indeed, our proof is valid for any field of characteristic zero—for example, the rational numbers $\mathbb{Q}$ or the field of Laurent polynomials $\mathbb{C}((t))$—or more generally over any field in which $|G|$ is non-zero.

[4]The language of category theory is so ubiquitous in algebra that, even though we do not need it, it is probably a good idea for the student to start hearing it, at least informally.

However, if for example, G is a group of order p (prime), our proof fails (as does the theorem). Representation theory over fields of prime characteristic is tremendously interesting and important, especially in number theory, but in this course our ground field will be usually assumed to be $\mathbb{R}$ or $\mathbb{C}$, the cases of primary interest in geometry and physics.

The proof we give is not valid for infinite groups. However, we will later show that for many of the most interesting infinite groups, a similar statement holds.

Proof. Fix any *vector space complement* U for W inside V, and decompose V as a direct sum of vector spaces $V \cong W \oplus U$. Of course, if U happens to be G-invariant, we are done. But most likely it is not, so there is work to be done.

This vector space decomposition allows us to define a projection $\pi : V \to W$ onto the first factor. The map π is a surjective linear map which restricts to the identity map on W. Although π is *not* necessarily a homomorphism of G-representations, we will "average it over G" to construct a G-linear projection. To this end, define

$$\phi : V \to W$$
$$v \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot v).$$

Although it looks complicated, this is really just a simple projection of V onto W. Indeed, we are simply summing a finite collection of linear maps $V \to W$, since the composition $g \circ \pi \circ g^{-1}$ breaks down as a linear map of V, followed by the projection onto W, followed again by the linear map g of W. Also, since π is the *identity* map on W, it is easy to check that $g \circ \pi \circ g^{-1}$ is the identity map of W for each g: summing over all the elements of G and then dividing by the order, of course, it follows that ϕ is the identity map on the subspace W.

The projection ϕ is much better than the arbitrary π we began with: it is a homomorphism of G-representations! To check this, we just compute, for any $h \in G$,

$$h \cdot \phi(v) = \frac{1}{|G|} \sum_{g \in G} h \cdot (g \cdot \pi(g^{-1} \cdot v))$$

whereas

$$\phi(h \cdot v) = \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot (h \cdot v)).$$

Unravelling the meaning of these expressions, we see that they are the same: we are simply summing up the expressions of the form $g \cdot (\pi(g^{-1} \star h) \cdot v)$ over the elements g of G in two different orders. In other words, for any $h \in G$, we have $h \cdot \phi(v) = \phi(h \cdot v)$, so that the linear map ϕ is a homomorphism of representations of G.

Now, the advantage of a G-representation map is that its kernel is a G-representation. Let W' be the kernel of ϕ. Then G acts on W' and the vector space decomposition

$$V \cong W \oplus W'$$

is a decomposition of G-representations. Indeed, $g \in G$ acts on $v = w + w'$ by $g \cdot v = g \cdot w + g \cdot w'$. Since both $g \cdot w$ and $g \cdot w'$ belong to the respective subspaces W and W', the G-action is "coordinatewise" as needed. $\square$

Let us try to understand this proof in some examples we have already studied. Let V be the vertex permutation representation of D_4 and consider the sub-representation L spanned by $(-1, 1, -1, 1)$. How can we construct a D_4-representation complement?

First, take any vector space complement U—say U consists of the vectors in $\mathbb{R}$ whose last coordinate is zero. The induced projection $\pi : V \to L$ maps

$$\pi : \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \mapsto \begin{bmatrix} -x_4 \\ x_4 \\ -x_4 \\ x_4 \end{bmatrix}.$$

Now averaging over the eight elements of D_4 we have

$$\phi : \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \mapsto \frac{1}{8} \sum_{g \in D_4} g \cdot \pi(g^{-1} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}).$$

Thinking about the action of D_4 on the sub-representation L of V, we see that the elements r_1, r_3, H and V all act by multiplication by -1, where as the others act by the identity. On the other hand, on the four-dimensional representation V, the rotations act by cyclicly permuting the coordinates and the reflections by interchanging the respective coordinates, as discussed in Subsection 6.1. Thus this expression (with the elements ordered as in the table on page 3) simplifies as $\frac{1}{8}$ of

$$\pi \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} - \pi \begin{bmatrix} x_2 \\ x_3 \\ x_4 \\ x_1 \end{bmatrix} + \pi \begin{bmatrix} x_3 \\ x_4 \\ x_1 \\ x_2 \end{bmatrix} - \pi \begin{bmatrix} x_4 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} - \pi \begin{bmatrix} x_2 \\ x_1 \\ x_4 \\ x_3 \end{bmatrix} + \pi \begin{bmatrix} x_3 \\ x_2 \\ x_1 \\ x_4 \end{bmatrix} - \pi \begin{bmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \end{bmatrix} + \pi \begin{bmatrix} x_1 \\ x_4 \\ x_3 \\ x_2 \end{bmatrix}.$$

Now applying the map π and simplifying further, we see that

$$\phi : V \to L$$

sending

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \mapsto \frac{1}{4}(x_2 + x_4 - x_1 - x_3) \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix}$$

is a D_4 linear map. [Of course, we have proven this in general in our proof of Theorem 8.1, but you should verify explicitly for yourself that ϕ respects the action of D_4.]

Now, the kernel of ϕ, like any homomorphisms of G-representations, will be a G-representation. Indeed, it is the three-dimensional representation $W = \{(x_1, x_2, x_3, x_4) \mid x_1 + x_3 = x_2 + x_4\} \subset \mathbb{R}^4$. Thus $V \cong L \oplus W$ *as representations* of G. Now, since W has an invariant subspace, namely the space L spanned by $(1,1,1,1)$, we can repeat this process to construct a G-representation complement to L in W. You should do it, and verify that this produces the sub-representation T' we found above, spanned by $(1,1,-1,-1)$ and $(1,-1,-1,1)$.

Again, we have decomposed the four-dimensional G-representation V as the direct sum $T' \oplus L \oplus \mathbb{R}(1,1,1,1)$. The procedure we used is essentially an algorithm for decomposing any finite dimensional representation: we keep choosing invariant subspaces and constructing their G-invariant complements until none of the sub-representations we construct this way has any invariant subspaces. Thus we have proved:

THEOREM 8.4. *Any finite dimensional real or complex representation of a finite group can be decomposed into a direct sum of irreducible sub-representations.*

Such a representation is said to be *completely reducible* or *semi-simple.*

The theorem does not say anything about *what* irreducible representations appear in the decomposition of a given one, or whether there might be more than one such decomposition. Indeed, we made several choices along the way: a choice of an original invariant subspace, then the choice of a vector space complement. Might these result in different decompositions? Or, might all choices lead ultimately to the same decomposition—might there be a unique way to decompose into irreducibles? At least the vertex permutation representation of D_4 appears to decompose in *only one way* into irreducibles.

Unfortunately, it is too optimistic to hope for a unique decomposition. Indeed, consider the trivial representation of any group G on a two-dimensional vector space V. Now *any* decomposition of V as a vector space will also be a decomposition of V as a G-representation, and clearly, there are many ways to decompose V into two one-dimensional subspaces. On the other hand, these one-dimensional sub-representations are all isomorphic to each other, so it is true that the isomorphism-types of G-representations and the number of times each appears is the same for any decomposition. As we will soon prove, this degree of "uniqueness of the decomposition" *does* hold quite generally.

9. Uniqueness of Decomposition into Irreducibles.

Every finite dimensional real or complex representation of a finite group can be decomposed into irreducible representations (Theorem 8.1). Is this decomposition unique? In Example 6.1, we saw explicitly that *there is only one way* to decompose the vertex permutation representation into its three non-zero proper sub-representations. Might it be true in general that the decomposition of a representation into irreducible sub-representations is unique?

Naively posed, the answer is "NO." For example, *every* decomposition of a two-dimensional vector space into two one-dimensional subspaces will be a decomposition of the trivial representation of a group G. Of course, there are many different choices of vector-space decompositions! On the other hand, in this example, the isomorphism types of the indecomposable sub-representations, and the number of them appearing, is the same in every decomposition. A similar fact holds in general:

THEOREM 9.1. *Let V be a finite dimensional real or complex representation of a finite group G. Then V has a unique decomposition into sub-representations*

$$V = V_1 \oplus \cdots \oplus V_t$$

where each V_i is isomorphic to a direct sum of some number of copies of some fixed irreducible representations W_i, with $W_i \ncong W_j$ unless $i = j$. That is, given two different decompositions of V into non-isomorphic irreducible sub-representations

$$W_1^{a_1} \oplus \cdots \oplus W_t^{a_t} = U_1^{b_1} \oplus \cdots \oplus U_r^{b_r},$$

where the W_i (respectively U_i) are all irreducible and non-isomorphic, then after relabling, $t = r$, $a_i = b_i$, the sub-representations $W_i^{a_i}$ equal the $U_i^{b_i}$ for all i, and corresponding W_i are isomorphic to U_i for all i.

In other words, the irreducible sub-representations that appear as summands *are uniquely determined up to isomorphism,* as is their *multiplicity* (or number of them appearing) in V. Furthermore, the summands V_i consisting of the span of all the vectors in the subrepresentations W_i are *uniquely determined* sub-representations of V, although the decomposition of V_i into the components isomorphic to W_i may not be.

The vertex permutation representation of D_4 discussed in Example 6.1 admits a completely unique decomposition because the three irreducible sub-representations we identified are all non-isomorphic and the multiplicity of each is one. According to Theorem 9.1, this is therefore the only decomposition.

To prove Theorem 9.1, we first need the following, quite general, lemma.

LEMMA 9.2. *A homomorphism of irreducible representations is either zero or an isomorphism.*

PROOF. Consider a homomorphism $V \to W$ of irreducible representations. Since the kernel is a sub-representation of V, we see that the kernel is either 0 or all of V. Likewise, since the image is a subrepresentation of W, it is either zero or all of W. Thus, a non-zero homomorphism between irreducible representations must be both injective and surjective. The lemma follows. □

PROOF OF THEOREM. Suppose that $V = W_1^{a_1} \oplus \cdots \oplus W_t^{a_t} = U_1^{b_1} \oplus \cdots \oplus U_r^{b_r}$ are two different decompositions of V into irreducible representations of G. The composition of the inclusion of W_1 in V followed by projection onto U_i

$$W_1 \hookrightarrow V \to U_i$$

is a G-linear map of irreducible representations, so must be either zero or an isomorphism. It can not be the zero map for all i, so some U_i—after relabling say U_1— is isomorphic to W_1. Repeating this argument for W_2 we see that $W_2 \cong U_2$ and so on until each W_j is paired with some U_i. Reversing the roles of the U_j and W_i we see that the isomorphism types appearing in both decompositions are precisely the same.

Now it remains only to show that $W_i^{a_i}$ and $U_i^{b_i}$ are precisely the *same* sub-representations of V (not just isomorphic—but literally the same subspaces). For this, we again consider the composition of inclusion with projection:

$$W_1^{a_1} \hookrightarrow V \to U_2^{b_2} \oplus \cdots \oplus U_t^{b_t},$$

where the second map is projection onto all the summands complementary to $U_1^{b_1}$. It is easy to see that this must be the zero map. (If not, then by restricting and projecting onto selected factors, we'd have a non-zero map $W_1 \to U_i$, for $i \neq 1$.) This means that $W_1^{a_1}$ is contained in the kernel of the projection, in other words,

$$W_1^{a_1} \subset U_1^{b_1}.$$

Reversing the roles of U and W, we get the reverse inclusion. It follows that $W_1^{a_1} = U_1^{b_1}$, and since U_1 and W_1 have the same dimension, also $a_1 = b_1$. Clearly, we can apply this argument for each index $i = 2, \ldots, n$, and so the theorem is proved. $\square$

CHAPTER 4

Classification of Irreducible Representations of Finite Groups

1. Irreducible representations over the complex numbers.

We have seen that irreducible representations are quite rigid. This is even more true for representations over the complex numbers.

LEMMA 1.1 (Schur's Lemma). *The only self-isomomorphisms of a finite dimensional irreducible representation of a group G over the complex numbers are given by scalar multiplication.*

PROOF. Fix an isomorphism $\phi : V \to V$ of complex representations of G. The linear map ϕ must have an eigenvalue λ over $\mathbb{C}$, and so also some non-zero eigenvector v. But then the G-linear map

$$V \to V$$

$$x \mapsto [\phi(x) - \lambda x]$$

has the vector v in its kernel, which is again a representation of G. Since V is irreducible, the kernel must be all of V. In other words, we have $\phi(x) = \lambda(x)$ for all $x \in V$, which is to say, ϕ is multiplication by λ. $\square$

Schur's Lemma is false over $\mathbb{R}$. For example, rotation through 90^0 (or indeed any angle) is obviously an automorphism of the irreducible representation of the rotation subgroup R_4 acting tautologically (by rototations) on the real plane. The eigenvalues of this rotation map are non-real complex numbers, so we can not argue as above over the reals. Indeed, consider the "same" representation over $\mathbb{C}$, that is, by composing

$$R_4 \subset GL_2(\mathbb{R}) \hookrightarrow GL_2(\mathbb{C})$$

to get a representation of R_4 on $\mathbb{C}^2$. Over $\mathbb{C}$, this representation is not irreducible. Indeed, it decomposes into the two representations spanned by $\begin{bmatrix} i \\ 1 \end{bmatrix}$ and $\begin{bmatrix} i \\ -1 \end{bmatrix}$ where the generator r_1 acts by multiplication by i and $-i$ respectively. See Example 7.5.

Schur's Lemma gives another—more quantitative—perspective on the rarity of homomorphisms between representations. Let V and W be representations of G. The G-linear homomorphisms form a subspace $\mathrm{Hom}_G(V, W)$ of the space of all linear maps $\mathrm{Hom}_{\mathbb{C}}(V, W)$ from V to W. Schur's Lemma can be restated as follows:

Lemma 1.2. *If V and W are irreducible finite dimensional complex representations of a group G, then the dimension of the space*

$$Hom_G(V,W)$$

of all G-representation homomorphisms is either one or zero, depending on whether $W \cong V$ or not.

In particular, if V is irreducible of dimension n, then

$$\mathrm{Hom}_G(V,V) \subset \mathrm{Hom}_{\mathbb{C}}(V,V)$$

is a one dimensional subspace of the n^2 dimensional space of all linear self maps of V.

Exercise 1.3. Consider only finite dimensional complex representations of a group G. Show that if one of W or V is irreducible, then the dimension of $\mathrm{Hom}_G(V,W)$ is equal to the multiplicity of (the isomorphism class of) the irreducible one in the other.

1.1. Representations of Abelian groups. Schur's Lemma has some striking consequences for the classification of representations of finite groups over the complex numbers.

Let V be any representation of a group G. Each element $g \in G$ induces a linear map

$$V \to V$$

$$v \to g \cdot v.$$

Is this a homomorphism of representations? Not usually! It is a homomorphism of G-representations if and only if it commutes with the action of each $h \in G$, that is, if and only if

$$h \cdot g \cdot v = g \cdot h \cdot v$$

for all h in G and all $v \in V$. Of course, this rarely happens: imagine that G is $GL_n(\mathbb{R})$, and g and h are non-commuting matrices.

However, if G is abelian, or more generally if g is in its center, then the action of g on V is G-linear. Indeed, then

$$h \cdot (g \cdot v) = (h \star g) \cdot v = (g \star h) \cdot v = g \cdot (h \cdot v)$$

for all $h \in G$ and all $v \in V$.

This observation, together with Schur's lemma, leads to the following striking result:

Proposition 1.4. *Every finite dimensional irreducible complex representation of an abelian group is one-dimensional.*

Proof. Suppose that V is a finite dimensional irreducible representation of an abelian group G. Then the action of G on V is G-linear, so by Schur's lemma, the action of g on V is simply multiplication by some scalar, $\lambda(g)$, which of course, can depend on the element g. In any case, every subspace is invariant under scalar multiplication, so every subspace is a sub-representation. So since V is irreducible, it must have dimension one. $\square$

This does not mean that the representation theory of abelian groups over $\mathbb{C}$ is completely trivial, however. An irreducible representation of an abelian group is a group homomorphism

$$G \to GL_1(\mathbb{C}) = (\mathbb{C}^*, \cdot),$$

and there can be many different such homomorphisms (or elements of the "dual group"). Furthermore, it may not be obvious, given a representation of an abelian group, how to decompose it into one-dimensional sub-representations. Schur's Lemma guarantees that there is a choice of basis for V so that the action of an abelian group G is given by multiplication by

$$\begin{pmatrix} \lambda_1(g) & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2(g) & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & \lambda_n(g) \end{pmatrix}$$

where the diagonal entries $\lambda_i : G \to \mathbb{C}^*$ are group homomorphisms. But it doesn't tell us how to find this basis or the functions λ_i.

1.2. Irreducible representations of S_3. Let us now try the first non-abelian case: can we identify all the irreducible representations of S_3 over $\mathbb{C}$, up to isomorphism?

Suppose V is complex representation of S_3. The group S_3 is generated by $\sigma = (123)$ and $\tau = (12)$, so to find sub-representations, it is enough to find subspaces of V invariant under the action of both σ and τ.

First consider the action of σ on V. Let v be an eigenvector for this action, with eigenvalue θ. Let $\tau v = w$. Because we know that $\tau\sigma\tau = \sigma^2$ in S_3, is easy to check that w is also an eigenvector for σ with eigenvalue θ^2. Indeed:

$$\sigma \cdot w = \sigma\tau \cdot v = \tau\sigma^2 \cdot v = \tau \cdot \theta^2 v = \theta^2 \tau \cdot v = \theta^2 w.$$

It follows that the subspace generated by v and w is invariant under both σ and τ, hence under all of S_3. In particular, an irreducible representation of S_3 over the complex numbers can have dimension no higher than two.

Can we actually identify all the irreducible representations of S_3 over $\mathbb{C}$? Suppose V is irreducible, and again let v be an eigenvector for the action of σ on V, with eigenvalue θ. Since σ^3 is the identity element of S_3, this eigenvalue must satisfy $\theta^3 = 1$. There are essentially two cases to consider: either the eigenvalue is one, or it is a primitive third root of unity.

First we consider the case where the eigenvalue $\theta \neq 1$. In this case, $\theta \neq \theta^2$, so the vectors v and $w = \tau v$ have distinct eigenvalues θ and θ^2, hence are independent. This means that v and w span V, which necessarily has dimension two. In this case, the map

$$V \to W = \{(x_1, x_2, x_3) \mid \sum x_i = 0\} \subset \mathbb{C}^3$$

$$v \mapsto (1, \theta, \theta^2); \;\; w \mapsto (\theta, 1, \theta^2),$$

defines an isomorphism from V to the **standard representation** of S_3 (prove it!).

It remains to consider the case where $\theta = 1$. Now $w = \sigma v = v$, so that the irreducible representation V is one dimensional. We already know that σ acts trivially, so the only issue is how τ might act. But since $\tau^2 = 1$, the only possibilities for the actions of τ are either trivially, or by multiplication by -1. If τ acts trivially, the irreducible representation V is the trivial representation. If τ acts acts by -1, then V is the **alternating representation.** Thus, up to isomorphism, there are precisely three irreducible representations of S_3 over the complex numbers: the trivial, the alternating and the standard representations.

2. Characters

We now understand, in a sense, *all* complex representations of any finite abelian group, as well as the simplest non-abelian group: they are all direct sums of irreducible representations, and we have explicitly identified the finite list of these. On the other hand, this doesn't help us to find a decomposition of a given representation, or even to recognize when two given representations (say, of an abelian group or S_3) are isomorphic.

Fortunately, there is a very effective technique for decomposing any given finite dimensional representation into its irreducible components. For example, we can tell at a glance—or at least easily program a computer to—whether two very large dimensional representations of a finite group are isomorphic or not. The secret is *character theory.*

In our analysis of the representations of S_3, the key was to study the eigenvalues of the actions of individual elements of S_3. This is the starting point of character theory. Finding individual eigenvalues, however, is difficult. Luckily, it is sufficient to consider their sum, the *trace,* which is much easier to compute.

Definition 2.1. Let $\phi : V \to V$ be a linear transformation of a finite dimensional vector space. The *trace* of ϕ is the sum of the diagonal entries $a_{11} + a_{22} + \cdots + a_{nn}$ of a matrix representing ϕ in any fixed basis for V. This is independent of the choice of basis, and can also be defined as sum of the roots of its characteristic polynomial, counting multiplicity[1].

Definition 2.2. Fix a finite dimensional representation V of a group G, say, over $\mathbb{C}$. The *character* of the representation is the complex valued function

$$\begin{aligned} \chi_V : G &\to \mathbb{C} \\ g &\mapsto \text{ trace of } g \text{ acting on } V. \end{aligned}$$

Of course if V is defined over $\mathbb{R}$ or some other field, then the character takes values in $\mathbb{R}$ or whatever ground field.

The character of a representation is easy to compute. If G acts on an n-dimensional space V, we write each element g as an $n \times n$ matrix according to its action expressed in some convenient basis, then sum up the diagonal elements of the matrix for g to get $\chi_V(g)$. For example, the trace of the identity map of an n-dimensional vector space is the trace of the $n \times n$ identity matrix, or n. Thus, for any group, the character of the trivial representation

[1]If you are not already familiar with the trace from a linear algebra course, you should prove this!

of dimension n is the constant function sending each element of G to n. More generally, $\chi_V(e) = \dim V$ for any finite dimensional representation V of any group.

We often write the values of the character χ_V as a "vector" whose coordinates are indexed by the elements of G.

$$\chi_V := (tr(g_1), tr(g_2), \ldots, tr(g_r)),$$

where $r = |G|$. For example, the character of the n-dimensional trivial representation of G can be written $(n, n, \ldots, n)$ (where the length of the vector here is the order of G). Similarly, the character of the tautological representation of D_4 is

$$(2, 0, -2, 0, 0, 0, 0, 0).$$

This is simply the list of the traces of the transformations $\{e, r_1, r_2, r_3, H, A, V, D\}$ of symmetries of the square acting on $\mathbb{R}^2$ (Cf. the list of matrices representing these symmetries in Example 6.1.)

2.1. The fixed point theorem. The character of any permutation representation (see 1.1) is easy to compute. Suppose a group G acts on a finite set X, and let V_X be the associated permutation representation. So V_X is a vector space with basis indexed by the elements of X and G acts by permuting the basis vectors according to its action on the indices. In this case, the character is

$$\chi_{V_X}(g) = \text{ the number of elements of } X \text{ fixed by } g.$$

Indeed, if we imagine the basis $\{e_x\}_{x \in X}$ written as column vectors indexed by $x \in X$, the action of g is simply permuting them in some way, and the corresponding matrix is the corresponding (inverse) permutation of the columns of the identity matrix. In particular, each diagonal entry is either 0 or 1. It is 1 if and only if $e_{gx} = e_x$— that is, if and only if g fixes x—and zero otherwise. Thus the trace of the action of g on V_X is the number of elements of x fixed by g.

2.2. The character of the regular representation. Let R be the regular representation of a finite group G—which is to say, the permutation representation of G induced by the action of G on itself by left multiplication. The character χ_R can be computed using the fixed point theorem. Indeed, since left multiplication by a non-identity element fixes *no element* of G, the trace of every $g \neq e$ is zero. On the other hand, of course e acts by the identity on this vector space of dimension G. Thus

$$\chi_R = (|G|, 0, 0, \ldots, 0).$$

2.3. Characters of S_3. Let us compute the characters of the three irreducible representations of S_3 identified in the last lecture.

The trivial representation of S_3 is one dimensional and takes the value 1 for each of the six elements of S_3. Its character is therefore

$$\chi_E : G \to \mathbb{C}; \;\; g \mapsto 1; \quad \text{or } (1, 1, 1, 1, 1, 1).$$

The alternating representation is also one dimensional, but takes the value 1 on the even permutations ($e, (123)$ and 132), and -1 on the odd permutations (the transpositions $(12), (23)$ and (13)). Thus

$$\chi_A : (1, -1, -1, -1, 1, 1).$$

The character of the standard representation could be found by writing out the matrix for the action of each of the six elements of S_3, with respect to some basis, perhaps the one already identified in 1.2. However, we prefer to make use of the following helpful fact:

PROPOSITION 2.3. *Let V and W be finite dimensional representations of a group G. Then*

$$\chi_{V \oplus W} = \chi_V + \chi_W$$

as functions on G.

Now, because the permutation representation of S_3 decomposes as a sum of the trivial and the standard representations, we can compute the character of the standard representation using Proposition 2.3. This has the advantage of being easy: the matrices for the permutation action are simply the permutation matrices, so we see immediately that the identity element has trace 3, each of the transpositions has trace 1, and each of the 3-cycles has trace 0. Subtracting the character of the trivial representation, we conclude that the standard representation has character

$$\chi_W = (2, 0, 0, 0, -1, -1).$$

This information can be displayed in a character table

	e	(12)	(13)	(23)	(123)	(132)
trivial	1	1	1	1	1	1
alternating	1	-1	-1	-1	1	1
standard	2	0	0	0	-1	-1

whose rows are the characters of the prescribed representations. The character of any complex representation V of S_3 can be obtained from these three, by decomposing V into irreducibles $V = E^a \oplus A^b \oplus W^c$, and then using Proposition 2.3 to conclude that

$$\chi_V = a\chi_E + b\chi_A + c\chi_W.$$

There are several other useful formulas for relating characters of related representations:

EXERCISE 2.4. For any finite dimensional representations V and W of a finite group G, show

(1) $\chi_{V \otimes W} = \chi_V \cdot \chi_W$
(2) $\chi_{V^*} = \frac{1}{\chi_V}$. In particular, over $\mathbb{C}$, $\chi_{V^*} = \overline{\chi_V}$, the complex conjugate.
(3) $\chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)} = \overline{\chi_V}\chi_W$.

3. Statements of the main theorems of character theory

Obviously, isomorphic representations have the same character, but remarkably, the character *completely determines the representation* up to isomorphism, at least over $\mathbb{C}$:

THEOREM 3.1. *Two finite dimensional complex representations of a finite group G are isomorphic if and only if they have the same character.*

Indeed, much more is true. Take a close look at the character table for S_3. Its rows are *orthogonal* with respect to the standard (Hermitian) inner product. Also, each has length $\sqrt{|S_3|}$. In other words, the characters of the irreducible representations are *orthonormal* with respect to the inner product on the space of $\mathbb{C}$-valued functions of G:

$$(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}. \tag{1}$$

Amazingly, this is a general feature of the characters of any finite group!

THEOREM 3.2. *For any finite group G, the characters for the irreducible complex representations are orthonormal under the inner product (1) on the space of all $\mathbb{C}$-valued functions of G.*

Put differently, if χ_V and χ_W are characters of irreducible representations, then (χ_V, χ_W) is either 1 or 0, depending on whether $V \cong W$ or not.

Theorem 3.2 already implies that there are finitely many isomorphism classes of irreducible representations. Orthonormal vectors are independent, so clearly there are at most $|G|$ irreducible representations for G.

In fact, there is a better bound on the number of irreducible representations a finite group. Note another interesting feature of the character table of S_3: each character takes the same value on all transpositions, and also takes the same value on each of the three-cycle. This, too, is a general feature of the character of any finite group.

PROPOSITION 3.3. *The character of a representation is constant on conjugacy classes of G. That is, for any finite dimensional representation V of a group G,*

$$\chi_V(hgh^{-1}) = \chi_V(g)$$

for all $g, h \in G$.

PROOF. This is more or less obvious, since the action of h can be considered a change of basis for V. Since the trace does not depend on the basis—that is, conjugate (similar) matrices have the same trace— the character must be constant on conjugacy classes of G. ☐

For example, S_3 has three conjugacy classes—the identity, the transpositions, and the three-cycles—and we have seen that the character of any representation is constant on each of these.

To avoid redundancy, we usually think of the character of a representation as a function the set of *conjugacy classes* of G. For example, the character table of S_3 could be compactified to

	e	(12)	(123)
trivial	1	1	1
alternating	1	-1	1
standard	2	0	-1

Here the elements $e, (12)$ and (123) are representatives for their respective conjugacy classes. Some authors include another row above the first row to indicate the number of elements in each conjugacy class; this is helpful in computing the inner product, since that sum is still taken over all the elements of G.

We postpone the proof of Theorem 3.2 in order to summarize some of its amazing consequences.

COROLLARY 3.4. *For finite dimensional complex representations of a finite group G we have:*

(1) *There are at most t irreducible representations of G, where t is the number of conjugacy classes of G.*
(2) *The multiplicity of an irreducible representation W in a representation V is (χ_W, χ_V).*
(3) *Each representation is determined (up to isomorphism) by its character.*
(4) *A representation V is irreducible if and only if $(\chi_V, \chi_V) = 1$.*

REMARK 3.5. In fact, the characters of the irreducible representations actually span the t-dimensional vector space of all functions on G constant on conjugacy classes, so there are *exactly* t distinct isomorphism classes of irreducible representations of G. We will outline the proof of this in the exercises.

PROOF OF COROLLARY. (1). The characters of the different representations of G live in the t-dimensional space of functions on G which are constant on conjugacy classes (for example, by listing the values at each conjugacy class, we get a "vector" of t complex numbers). Since the characters of the irreducible representations are orthonormal, they are independent, and hence there can be at most t of them. This means there are at most t isomorphism classes of irreducible representations.

(2). Now, suppose $V \cong W_1^{a_1} \oplus \cdots \oplus W_t^{a_t}$ is a decomposition of V into irreducibles. Using Proposition 2.3, $\chi_V = a_1\chi_{W_1} + \cdots + a_t\chi_{W_t}$. So using the bilinearity of the inner product and the orthonormality of the χ_{W_i}, we conclude that

$$(\chi_V, \chi_{W_i}) = a_i.$$

(3). Suppose V and U are two representations with the same character. Decomposing each,

$$V \cong W_1^{a_1} \oplus \cdots \oplus W_t^{a_t}, \quad U \cong W_1^{b_1} \oplus \cdots \oplus W_t^{b_t}$$

so that if $\chi_V = \chi_U$, then

$$a_1\chi_{W_1} + \cdots + a_t\chi_{W_t} = b_1\chi_{W_1} + \cdots + b_t\chi_{W_t}.$$

But now because the χ_{W_i} are independent, we see that $a_i = b_i$ for each i, and so $V \cong U$.

(4). Decompose V into irreducibles $W_1^{a_1} \oplus \cdots \oplus W_t^{a_t}$, so that $\chi_V = a_1\chi_{W_1} + \cdots + a_t\chi_{W_t}$. Then using the orthonormality of the χ_{W_i}, we see that

$$(\chi_V, \chi_V) = a_1^2 + a_2^2 + \cdots + a_t^2.$$

Since the a_i are all non-negative integers, we see that $(\chi_V, \chi_V) = 1$ if and only if exactly one of the a_i is 1, and the others are zero, that is, if and only V is irreducible. $\square$

4. Using Character theory to decompose representations.

We now have a very powerful tool[2] for analyzing complex representations of a finite group. For example, let us decompose the regular representation R of S_3 into its irreducible components. (Recall that the regular representation of S_3 is the six-dimensional representation with a basis indexed by the elements of S_3, where S_3 acts by left multiplication on these indices.) We have proved that the only irreducible representations of S_3 are the trivial E, the alternating A and the standard W. Thus we have a decomposition

$$R \cong E^a \oplus A^b \oplus W^c$$

for some non-negative integers a, b and c. This produces the following relation on the characters:

$$\chi_R = a\chi_E + b\chi_A + c\chi_W.$$

The character of the regular representation is $(6, 0, 0)$, as we saw in 2.2. Thus we have a system of linear equations in three unkowns,

$$(6, 0, 0) = a(1, 1, 1) + b(1, -1, 1) + c(2, 0, -1)$$

which is easy to solve: $(a, b, c) = (1, 1, 2)$. So the regular representation decomposes as

$$R \cong E \oplus A \oplus W^2.$$

4.1. The decomposition of the regular representation. A similarly beautiful picture emerges for the regular representation of any finite group:

Corollary 4.1. *The regular representation R of any finite group G decomposes (over $\mathbb{C}$) as*

$$R \cong W_1^{\dim W_1} \oplus W_2^{\dim W_2} \oplus \cdots \oplus W_t^{\dim W_t}$$

with every irreducible representation W_i appearing exactly $\dim W_i$ *times.*

In particular,

Corollary 4.2. *For any finite group G*

$$|G| = \sum_{W_i} (\dim W_i)^2, \tag{2}$$

[2] though we haven't proven it yet

where the sum is taken over the (isomorphism classes of) irreducible complex representations of G.

PROOF. We know that

$$R \cong W_1^{a_1} \oplus W_2^{a_2} \oplus \cdots \oplus W_t^{a_t}$$

where the W_i range through all the irreducible representations of G, and the a_i are some non-negative integers. We have already computed that $\chi_R = (|G|, 0, 0, \ldots, 0)$ (see Example 2.2), so by Corollary 3.4 (2), we have

$$a_i = (\chi_{W_i}, \chi_R) = \frac{1}{|G|} \sum_{g \in G} \chi_{W_i}(g) \overline{\chi_R(g)} = \frac{1}{|G|} \chi_{W_i}(e)|G| = \dim W_i.$$

□

Formula (2) can be very helpful in unraveling the mysteries of the representations of a particular group.

EXERCISE 4.3. Describe all the irreducible complex representations of D_4.

5. The Proof of orthonormality

5.1. Another nice property of the character. Looking again at the character table of S_3 we observe another interesting feature: the rows (except the trivial character) have values summing to zero! This, too, is a general property of any non-trivial irreducible representation.

PROPOSITION 5.1. *For finite dimensional complex representations of a finite group,*

(1) *The values of the character of a non-trivial irreducible representation sum to zero.*
(2) *More generally, the multiplicity of the trivial representation in a decomposition into irreducibles is*

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

PROOF. Let V be any finite dimensional (real or complex) representation of a finite group G. The trivial part of V—that is, the sub-representation V^G where G acts trivially—can be split off from V using the projection

$$\begin{aligned} \pi : \ & V \to V \\ & v \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot v. \end{aligned}$$

The linear map π is easily seen to be a homomorphism of G-representations with image V^G. Because π is the identity on V^G and zero on its complement, the trace of π is simply the dimension of V^G. We conclude that

$$\dim V^G = \text{trace } \pi = \frac{1}{|G|}\sum_{g\in G} \text{trace of } g \text{ acting on } V = \frac{1}{|G|}\sum_{g\in G}\chi_V(g).$$

This proves the second statement. The first statement follows as well, since if V is irreducible but not trivial, we have $V^G = 0$. $\square$

Proof of Theorem 3.2. Let W and V be irreducible complex representations of a finite group G. We want to show that

$$(\chi_W, \chi_V) = \quad 1 \quad \text{or} \quad 0,$$

depending on whether $V \cong W$ or not. Writing out the meaning of this, we want to show that

$$\frac{1}{|G|}\sum_{g\in G}\chi_W(g)\overline{\chi_V(g)} = \quad 1 \quad \text{or} \quad 0,$$

depending on whether $V \cong W$ or not. Taking a clue from Exercise 2.4, we consider

$$\chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)} = \chi_{V^*} \otimes \chi_W,$$

and observe that

$$(\chi_W, \chi_V) := \frac{1}{|G|}\sum_{g\in G}\chi_W(g)\overline{\chi_V(g)} = \frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)}(g),$$

which, according to Proposition 5.1 should be equal to the multiplicity of the trivial representation in $\mathrm{Hom}_{\mathbb{C}}(V,W)$. How can we compute this multiplicity?

5.2. The representation $\mathrm{Hom}_{\mathbb{C}}(V,W)$. Let V and W be representations of G. The vector space $\mathrm{Hom}_{\mathbb{C}}(V,W)$ has a natural structure of a representation of G under the action:

$$g\cdot\phi : V \to W$$
$$v \mapsto g\cdot\phi(g^{-1}\cdot v).$$

The G-linear homomorphisms are precisely those linear maps in $\mathrm{Hom}_{\mathbb{C}}(V,W)$ on which g acts trivially. (Prove it!) In particular, the *trivial part* of $\mathrm{Hom}_{\mathbb{C}}(V,W)$—that is, the subrepresentation of $\mathrm{Hom}_{\mathbb{C}}(V,W)$ on which G acts trivially–is precisely the space $\mathrm{Hom}_G(V,W)$ of G-representation homormorphisms.

Now, Schur's lemma tells us that for (*complex*) irreducible representations W and V,

$$\dim \mathrm{Hom}_G(V,W) = 1 \;\text{ if }\; V \cong W; \quad 0 \text{ if } \; V \not\cong W,$$

so that multiplicity of the trivial representation in $\mathrm{Hom}_{\mathbb{C}}(V,W)$ is equal to one or zero, depending on whether $V \cong W$ or not. The proof of Theorem 3.2 is complete. $\square$

Remark 5.2. It is not much harder to show that the characters of the irreducible representations span the space of functions constant on conjugacy classes, which is to say, they form an orthonormal basis. However, since the main conclusions follow already from the orthonormality, we leave the proof of this fact as an exercise.

Exercise 5.3. Fix a finite group G. Consider the vector space $\mathcal{F}_G$ of all $\mathbb{C}$-valued functions on G, and the subspace $\mathcal{C}$ of those that are constant on conjugacy classes. We wish to show that the characters of irreducible representations of G span $\mathcal{C}$.

(1) Show that $\alpha \in \mathcal{F}_G$ is constant of conjugacy classes if and only if the map

$$\phi_{\alpha,V} : V \to V; \;\; v \mapsto \sum_{g \in G} \alpha(g) g \cdot v$$

is G-linear for all complex representations V.

(2) Show that the trace of $\phi_{\alpha,V}$ is (α, χ_{V^*}) for all $\alpha \in \mathcal{F}$.

(3) Show if $(\alpha, \chi_{V^*}) = 0$ for some irreducible representation V and $\alpha \in \mathcal{C}$, then $\phi_{\alpha,V}$ is the zero map.

(4) Show that if $\alpha \in \mathcal{C}$ is non-zero, then $\phi_{\alpha,R}$ is not zero, where R is the regular representation.

(5) Conclude that the characters of irreducible representations span $\mathcal{C}$.

6. Representations of S_n

There is a beautiful theory of representations of S_n: an explicit construction of each of the irreducible representations (over $\mathbb{C}$) via the so-called Young symmetrizers and Frobenius's formula for their characters. To describe it all carefully takes us into the realm of combinatorics, and perhaps beyond what our priorities allow us to prove here. Still, it may be worth stating the results and discussing the main ideas involved in the representation theory of S_n, as they come up again in the representation theory of GL_n. We hope this discussion will encourage students to look up the details in serious book on representation theory, such as Fulton and Harris.

First, we know that the number of irreducible representations (up to isomorphism) of S_n is equal to the number of conjugacy classes in S_n. It turns out that there is a nice way to enumerate the conjugacy classes of S_n—in terms of *Young tableaux*—and that the Young tableaux also give us a nice way to construct explicit irreducible representations.

In particular, for S_n, we have an explicit construction of an irreducible representation for each conjugacy class. Amazingly, even though it has been known for over 100 years that the set of conjugacy classes of a finite group and the set of its irreducible representations have the same cardinality, no one knows how to explicitly construct a representation corresponding to a given conjugacy class in an arbitrary group.

6.1. Conjugacy in S_n and Young diagrams. Recall that every permutation in S_n can be written, uniquely up to order, as a composition of disjoint cycles $\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t$, where here we even list the 1-cycles (though we ealier agreed that sometimes we drop them from the notation). Say that σ_i is a k_i-cycle, and that we have listed the cycles so that $k_1 \geq k_2 \geq \cdots \geq k_t$. Note that the cycles (including the 1-cycles) give a perfect partition of the set of n elements into t disjoint sets whose cardinalities are k_i.

Definition 6.1. The *cycle type* of σ is the partition

$$[k_1 k_2 \dots k_t] := \{k_1 \geq k_2 \geq \cdots \geq k_t \geq 1 \mid \sum k_i = n\}$$

of n, where the k_i are a (weakly) decreasing list of positive natural numbers summing to n.

For example the cycle type of the permutation $(1457)(368)$ in S_8 is $[4,3,1]$ because this permutation decomposes as the composition of the cycles $(1457), (368)$ and (2), of lengths $4, 3$, and 1, respectively. The permutation $(1234)(567)$ has the same cycle type.

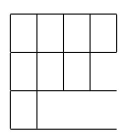
Exercise 6.2. Two permutations in S_n are conjugate if and only if they have the same cycle type.

The exercise is quite easy if one notes that conjugation can be thought of as a "change of labeling" for the transformations of the set of n-objects. For example, conjugating by the transposition (16) will interchange the roles of 1 and 6 in the permutation of $\{1, 2, \dots, n\}$. For example, the permutations $(123)(456)$ and $(623)(451)$ are conjugate to each other via conjugation by (16):

$$(16)(123)(456)(16) = (623)(451).$$

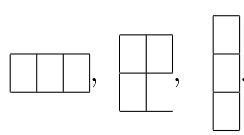
This makes it easy to list the conjugacy classes of S_n: there is exactly one for each distinct way of partitioning a set of n objects—that is, they are indexed by the *partitions of* n.

Partitions of n (and so the conjugacy classes of S_n) can be easily enumerated pictorially using Young diagrams. For example, the Young diagram of the partition $[4,3,1]$ (of eight) has rows of 4, 3, and 1 box respectively:



More generally, the Young diagram for the partition $[k_1 k_2 \dots k_t]$ of n consists of n-equal sized boxes arranged in t left-justified rows consisting of $k_1, k_2, \dots, k_t$ boxes respectively.

For example, there are exactly three conjugacy classes S_3, corresponding to the partitions $[3]$, $[2,1]$ and $[1,1,1]$. These are the classes of 3-cycles $\{(123), (132)\}$, of transpositions $\{(12), (13), (23)\}$, and the identity, respectively. These are visualized with the three Young diagrams



Likewise, there are five conjugacy classes in S_4, corresponding to the partitions $[4], [3,1], [2,2], [2,1,1]$, and $[1,1,1,1]$. These correspond to the 4-cycles, the 3-cycles, the pairs of transpositions, the transpositions, and the identity elements, respectively.

6.2. The Representation Ring.

6.3. The irreducible representations of constructed from Young tableaux.

Part 2: Lie Groups and their representations

CHAPTER 5

Lie Groups

1. Examples

1.1. $GL_n(\mathbb{R})$**.**

1.2. $SL_n(\mathbb{R})$**.**

1.3. $SO_n(\mathbb{R})$**.**

1.4. $U_n(\mathbb{C})$**.**