GROUPS AND THEIR REPRESENTATIONS

KAREN E. SMITH

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 reflection clockwise by ninety degrees so that these two rotations are inverse to eachother. 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. Intuitively, the elements of a group can *always* be considered transformations of some set with the usual notion of composition. 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.

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.

2. Abstract Groups.

Definition 2.1. 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. 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 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".]

[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.

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	I	r_3	r_2

Another convention: We write $a \circ b$ in *column* a and *row* b, not vice versa. 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 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** could be 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. Mover, 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.

Definition 2.2. 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 fr 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 $\mathbb{Z}$. We will discuss quotient groups in detail in the next lecture.

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 $\bar{0}$ is the identity element, and the class $\overline{-i}$ is the inverse of $\bar{i}$.

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 2.3. Two groups are *isomorphic* if there is a bijection between them that *respects the group operations* of each. Equivalently, 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 thus an isomorphism.

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 rotations r_1 by successive compositions, just as the elements of $\mathbb{Z}_4$ can be obtained by successive additions of $\bar{1}$. In both groups, we cycle back at the identity after four iterates. We say that R_4 is *generated* by the quarter turn, and that $\mathbb{Z}_4$ is *generated* by $\bar{1}$. Formally,

Definition 2.4. 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 sugroup of D_4 generated by the rotation r_1.

The subgroup of the group $(\mathbb{Z}, +)$, generated by some fixed integer N is the sugroup 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 r_2.[2] 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 $\{e, A, D, r_2\}$.

The group 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 $\mathbb{Z}_4$.

Remark 2.5. 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.

2.1. **Generators of $GL_n(\mathbb{R})$.**

The group $GL_n(\mathbb{R})$ is huge: not only is it uncountable, but it 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 2.6 (The Center of a group). The *center* of a group G is the set Z of elements which commute with all elements of G : $Z = \{z \in G \mid gz = zg \text{ for all } g \in G\}$.

[2] Note $AD = DA = r_2$ in D_4.

(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.

3. 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[3], 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 3.1. 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. Put differently, if X belongs to some interesting category of mathematical objects, we often look at automorphisms of X in that category[4] instead of merely the automorphisms of X as a set.The main case of interest is when X is a vector space,[5] where we are interested in the bijection self maps $X \to$ preserving the vector space structure (that is, *linear transformations*). Because the composition of two linear maps 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.*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!* In the category of vector spaces, an automorphism is simply an invertible linear map. We could say $GL(\mathbb{R}^n) = \text{Aut}_{vect.sp}(\mathbb{R}^n)$.

[3] composition is obviously associative

[4] The term category can be taken here in its precise technical meaning or in a more informal decription way, depending on the reader's background and inclination.

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

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.

3.1. **Groups of linear transformation and matrices.** The group $\mathbb{G}L(\mathbb{R}^n)$ and its close cousin $GL(\mathbb{C}^n)$ is one of the most important group in mathematics and physics. We fix some notation and conventions for dealing with it. 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

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

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.

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 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.

3.2. **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 $\{1, 2, 3, \ldots, n\}$. For convenience, therefore, we will usually label the objects $\{1, 2, 3, \ldots, n\}$.

Definition 3.2. The group Aut $\{1, 2, 3, \ldots, n\}$ 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 object. 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.

4. Products of Groups

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

Definition 4.1. 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 4.2. The group $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ has six elements: $(\overline{1}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{2}), (\overline{0}, \overline{2}), (\overline{0}, \overline{0})$. 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 4.3. 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 4.4. 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.

5. 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 5.1. (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 an surjective homorphism of the corresponding additive groups.

6. Quotient Groups

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

Definition 6.1. Integers a and b are *congruent modulo* n if their difference is a multiple of n. We write $a \equiv b \mod n$.

Note that

(1) $a \equiv a \mod n$;

(2) $a \equiv b \mod n$ if and only if $b \equiv a \mod n$;

(3) $a \equiv b \mod n$ and $b \equiv c \mod n$ implies that $b \equiv c \mod n$.

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 6.2. The congruence class of $a \in \mathbb{Z}$ modulo n is the set of integers congruent to a modulo n. We denote[6] 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

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

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 $b \equiv b'$ mod 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 6.3. The group $(\mathbb{Z}_n, +)$ is the set of congruence classes of $\mathbb{Z}$ modulo n, with the operation defined as $\overline{a} + \overline{b} = \overline{a+b}$.

One 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 $\overline{n-a}$.

6.1. **Cosets.** Now let try to carry out a similar procedure for any group. First observe that $a \equiv b$ mod 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.

Consider any subgroup K of a fixed group G.

Definition 6.4. 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 $g \equiv h$ mod K.[7]

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

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

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 6.5. 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.

6.2. **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 6.6. 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:

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

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 6.7. 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[8] 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 6.8. 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 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 6.9. 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 6.10. The *kernel* of a group homomorphism $\phi : G \to H$ is the set of elements in G which are sent the 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.

6.3. **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 immediately corollary is the following fundamental fact:

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

Theorem 6.11 (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 6.12. 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.