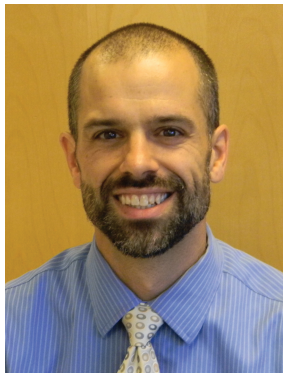
PART 1

Groups and Spaces

Office Hour One

Groups

Matt Clay and Dan Margalit



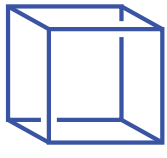
Symmetry, as wide or as narrow as you define its meaning, is one idea by which man through the ages has tried to comprehend and create order, beauty and perfection.

Hermann Weyl

An important problem in mathematics is to determine the symmetries of objects. The objects we are interested in might be concrete things such as planar shapes, higher-dimensional solids, or the universe. Or they might be more abstract, such as groups, spaces of functions, or electric fields.

We'll begin in this office hour with a general discussion of groups; the focus will be on interpreting every group as a group of symmetries of some object. In the second office hour we will make precise what it means for a group to be a group of symmetries of an object. These ideas are at the very heart of geometric group theory, the study of groups, spaces, and the interactions between them.

Symmetry. By understanding the symmetries of an object we come closer to fully understanding the object itself. For instance, consider a cube in Euclidean 3–space:



A symmetry of the cube is a rigid transformation of the cube (for now, no reflections allowed). In other words, a symmetry of the cube is what you get if you pick the cube up, rotate it with your hands, and then put in back in the same spot where it started. One way to obtain a symmetry is to skewer the cube through the centers of two opposite faces and rotate by any multiple of $\pi/2$. We could also skewer the cube through the midpoints of two opposite edges, or through two opposite corners.

Here is a question:

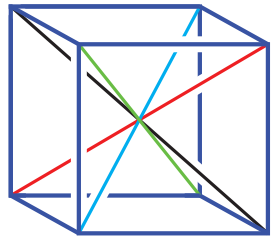
What are all of the symmetries of the cube?

If we don't know the answer to this question, then we don't know the cube!

There is a fairly straightforward analysis which tells us that there are exactly 24 symmetries of the cube: there are eight places to send any given corner, and once a corner is fixed, there are three choices for how to turn the cube at that corner.

This is a start, but leaves a lot to be desired: What is a good way to list the 24 symmetries? If we do one symmetry followed by another symmetry, we get a third symmetry; where is this third symmetry on our list?

Here is a simple idea that completely illuminates the problem. Draw the four long diagonals of the cube:



We can check the following two facts:

- Any symmetry of the cube gives a permutation of the four long diagonals.
- Any permutation of the four long diagonals gives a unique symmetry of the cube.

The validity of the first statement is not too hard to see. The second one takes a little thought. First notice that if we take the permutation that swaps two long diagonals, then we obtain a symmetry of the cube, namely, a symmetry obtained by skewering the cube through the midpoints of the two edges that connect the endpoints of the two long diagonals in question. But an arbitrary permutation of the four long diagonals can be obtained by swapping two long diagonals at a time, so we are done.

It follows that the set of symmetries of the cube is in bijection with the set of permutations of its four long diagonals. There are $4! = 24$ permutations of the four long diagonals, agreeing with our calculation that there are 24 symmetries of the cube. Moreover, since a permutation is just a bijective function from a set to itself, we know what happens when we do one permutation, then another—we get the composition of the two functions. We'll say more about permutations in a few minutes, when we talk about symmetric groups.

That was satisfying—we certainly understand the cube better now than we did at the start. In geometric group theory we aim to understand symmetries of much more complicated (and beautiful!) objects.

Here is the plan for this first office hour. We'll start by revisiting the basic examples of groups from any undergraduate course in abstract algebra. But we will look at these groups from the point of view that *every* group should be the collection of symmetries of some geometric object, just as the symmetric group on four letters is the collection of symmetries of a three-dimensional cube. To some extent, a lot of the material in this first office hour is a review of some of the important ideas from a first course in abstract algebra; you may want to skim through it if you are comfortable with those concepts.

In the next office hour, we will make sense of and prove the following theorem (Theorem 2.2 below):

> *Every group is naturally identified with the collection of symmetries of some geometric object, namely, the Cayley graph of the group.*

The goal of this book is to convince you that this theorem—along with the many other theorems in this book—is the beginning of a beautiful and fruitful dictionary relating the algebraic and geometric structures arising in the wild and fascinating world of infinite groups.

1.1 GROUPS

Let's recall the definition of a group. Then we'll explain why you should think of a group in terms of symmetries.

First, a *multiplication* on a set G is a function

$$G \times G \to G.$$

The image of (g, h) is usually written gh. In other words, a multiplication is a way of combining two elements of G in order to get a third one.

Then, a *group* is a set G together with a multiplication that satisfies the following three properties:

- *Identity.* There is an element 1 of G such that $1g = g1 = g$ for all $g \in G$. The element 1 is called the *identity element* of G.
- *Inverses.* For each $g \in G$, there is an element $h \in G$ such that $gh = hg = 1$. The element h is often denoted by g^{-1} and is called the *inverse* of g.
- *Associativity.* The multiplication on G is associative, that is:

  $$(fg)h = f(gh)$$

  for all $f, g, h \in G$.

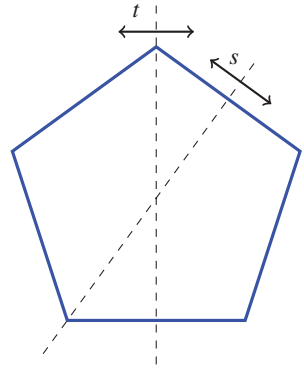
What does this abstract, formal definition have to do with symmetries? Let's first think about this in the case of the cube. We defined a symmetry of the cube as a rigid transformation of the cube. The way we multiply two symmetries g and h is:

"do h, then do g." This is just like composing functions: in the composition $g \circ h$ we apply h first.

We now see that the set of symmetries of the cube satisfies the definition of a group. The identity symmetry 1 is the rigid transformation of the cube that leaves it alone. Indeed, doing one rigid transformation g and then doing 1 is the same as doing g. The inverse of a symmetry g is the symmetry that undoes g. Associativity follows from the associativity of composition of functions: doing h, then g and f is the same as doing h and g, then f.

As we already said, we'd like to eventually convince you that every group—that is, every set with a multiplication as above—is the set of symmetries of some object. First, let's look at a few examples of groups and explain how they each can be thought of as a set of symmetries.

The dihedral group. The dihedral group D_n is the set of symmetries (rigid transformations) of a regular n–gon in the plane. The multiplication is the same as in the example of the cube. Two symmetries of the regular pentagon are the reflections s and t shown here:



For general n we can take s to be the reflection through any line that passes through the center of the n–gon and a vertex of the n–gon, and t to be the reflection about the line that differs from the first line by a π/n rotation. The elements s and t *generate* the group D_n, by which we mean that every symmetry of D_n is obtained by multiplying, s, t, s^{-1}, and t^{-1} (actually, in this example $s = s^{-1}$ and $t = t^{-1}$). For example, the clockwise rotation by m "clicks" is $(st)^m$.

Adam Piggott's Office Hour 13 on Coxeter groups discusses examples of groups that are all based on the idea of the dihedral groups.

The symmetric group. The symmetric group S_n is the set of permutations of the set $\{1, \ldots, n\}$, with multiplication given by composition of functions. This makes sense since a permutation of $\{1, \ldots, n\}$ is really just a bijective function $\{1, \ldots, n\} \to \{1, \ldots, n\}$. If we want to think of S_n as the set of symmetries of some object, we can think of it as the symmetries of a set of n points.

A *cycle* in S_n is a permutation that can be described as $i_i \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$ (and all other elements of $\{1, \ldots, n\}$ stay where they are). We write this cycle as $(i_1\ i_2\ \cdots\ i_{k-1}\ i_k)$. For instance, the cycle (1 2 4) in S_6 sends 1 to 2, 2 to 4, and 4 to 1, while sending 3, 5, and 6 to themselves.

Every element of S_n is a product of disjoint cycles (disjoint means that each element of $\{1, \ldots, n\}$ appears in at most one cycle). For instance, in S_6 the element

$$(1\ 2\ 4)(3\ 5)$$

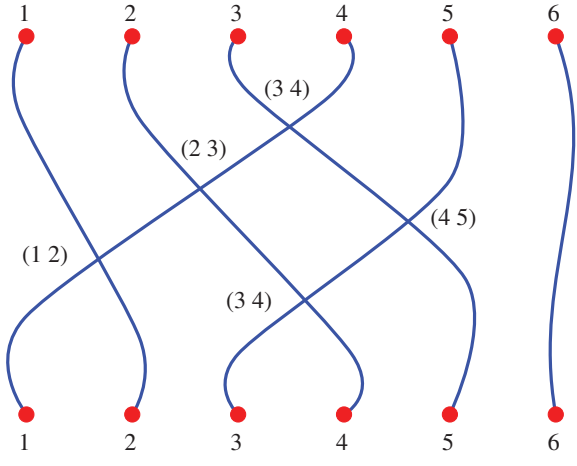
is the product of the disjoint cycles (1 2 4) and (3 5). This is the permutation that sends 1 to 2, 2 to 4, and 4 to 1, and also 3 to 5 and 5 to 3, and finally 6 to itself.

As we said, the multiplication is function composition. Say, for example, we want to multiply (1 2 4)(3 5) by (2 6):

$$(2\ 6) \cdot (1\ 2\ 4)(3\ 5).$$

Where does this product send 1? Well, the first permutation (on the right) sends 1 to 2, and the second permutation sends 2 to 6, so the product (= composition) sends 1 to 6. You can use the same procedure to determine where this product sends 2, 3, 4, 5, and 6. You will find that $(2\ 6) \cdot (1\ 2\ 4)(3\ 5) = (1\ 6\ 2\ 4)(3\ 5)$.

A *transposition* is a cycle of length 2, for instance, (3 5). It is an important fact that S_n is generated by transpositions of the form $(i\ \ i+1)$, where $1 \leq i \leq n-1$ (we actually used this fact implicitly in our discussion of the cube at the beginning). Let us check that we can write (1 2 4)(3 5) as a product of such elements in S_6. We can draw a diagram of this permutation as follows:



Each crossing in the diagram corresponds to an element of S_6 of the form $(i \;\; i+1)$. Reading top to bottom (and writing right to left), we find:

$$(1\ 2\ 4)(3\ 5) = (3\ 4)(1\ 2)(4\ 5)(2\ 3)(3\ 4).$$

The point is that multiplication in S_n can be realized by stacking diagrams. And the diagram for $(1\ 2\ 4)(3\ 5)$ can be obtained by stacking the diagrams for the five permutations on the right-hand side of the equation. Since we can always make a diagram where the crossings occur at different heights, this argument can be used to show that every element of S_n is equal to a product of transpositions $(i \;\; i+1)$.

Exercise 1. Use the idea of stacking diagrams to prove that S_n is generated by $\{(i \;\; i+1) \mid 1 \leq i \leq n-1\}$.

The picture we drew of the permutation $(1\ 2\ 4)(3\ 5)$ can be called a braid diagram. See Aaron Abrams' Office Hour 18 on braid groups for more on this idea.

Exercise 2. We showed that S_4 is the collection of symmetries of a three-dimensional cube. Can any of the other symmetric groups be thought of as the symmetries of higher-dimensional cubes? Or other shapes?

The integers modulo *n*. Let n be an integer greater than 1. The *integers modulo* n is the set

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

with the multiplication

$$(a, b) \mapsto \begin{cases} a+b & a+b \leq n-1 \\ a+b-n & a+b \geq n. \end{cases}$$

The identity for $\mathbb{Z}/n\mathbb{Z}$ is 0. The inverse of 0 is 0, and the inverse of any other m is $n-m$. Associativity is a little trickier: to check that $(a+b)+c = a+(b+c)$, there are a few cases, depending on which sums are greater than n. We'll leave this as an exercise.

Exercise 3. Show that if m is any element of $\{0, \ldots, n-1\}$ with $\gcd(m, n) = 1$, then $\{m\}$ is a generating set for $\mathbb{Z}/n\mathbb{Z}$.

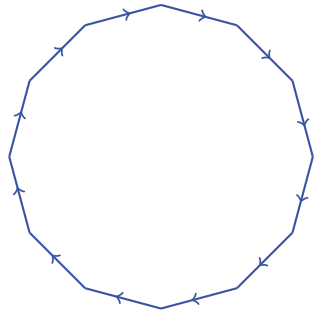
You are most familiar with $\mathbb{Z}/n\mathbb{Z}$ in three cases:

- When $n = 12$, the multiplication we defined is clock arithmetic. For example, 3:00 plus 5:00 is 8:00, and 9:00 plus 4:00 is 1:00 (although perhaps we should think of 12:00 as 0:00 instead).
- When $n = 10$, the multiplication we defined is an operation you use when balancing your checkbook. By just keeping track of the last digit, you have a quick first check for whether the sum of many big numbers is equal to what your bank says it is.
- When $n = 2$, the multiplication is light switch arithmetic. Identify 1 with flipping the switch and 0 with do nothing. Then flip plus flip is the same as doing nothing, flip plus do nothing is the same as flip, etc.

The idea of light switch arithmetic inspires a whole class of groups called lamplighter groups; see Jen Taback's Office Hour 15.

For what object is $\mathbb{Z}/n\mathbb{Z}$ the group of symmetries? Using the idea of the clock we might try to use a regular n–gon. We can certainly see $\mathbb{Z}/n\mathbb{Z}$ as a set of symmetries of the n–gon, namely, the rotational symmetries. Thus, $\mathbb{Z}/n\mathbb{Z}$ can be regarded as a *subgroup* of the full symmetry group, D_n. This means that we have realized $\mathbb{Z}/n\mathbb{Z}$ as a subset of D_n in such a way that the multiplication in $\mathbb{Z}/n\mathbb{Z}$ agrees with the multiplication in D_n. We can see that $\mathbb{Z}/n\mathbb{Z}$ is a proper subgroup of D_n (i.e., it is not the whole thing), since D_n also has reflectional symmetries.

That's pretty good. But we can modify the n–gon so that $\mathbb{Z}/n\mathbb{Z}$ is exactly the group of symmetries. One way to do this is to draw a little arrow in the middle of each edge:



We think of the arrow as defining a preferred direction on each edge. Then we define a symmetry of this modified n–gon to be a rigid transformation that preserves the directions of the arrows. This is still a perfectly fine notion of symmetry! The group $\mathbb{Z}/n\mathbb{Z}$ is the full group of symmetries of the n–gon in this modified sense.

1.2 INFINITE GROUPS

Many undergraduate courses in abstract algebra give short shrift to infinite groups. As we will see in this book, this is where all of the fun is! Let's start with the simplest infinite group.

The integers. You are probably familiar with the set of *integers*, or whole numbers:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

The multiplication $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is the usual addition of integers:

$$(m, n) \mapsto m + n.$$

The group $\mathbb{Z}$ is generated by $\{1\}$. But it is also generated by $\{2, 3\}$, for example.

Of what object is $\mathbb{Z}$ the set of symmetries? A first guess is that $\mathbb{Z}$ is the symmetries of the number line L, by which we mean the real line $\mathbb{R}$ with a distinguished point at each integer:

Here, by a symmetry of L, we just mean a rigid transformation of L that preserves the set of distinguished points. Examples of symmetries of L are: translate L to the left or right by n units, where n is a positive integer; reflect it about an integer point; and reflect it about a half-integer point.

The group $\mathbb{Z}$ gives a set of symmetries of L as follows: the integer n is the symmetry that translates L by n units to the right if $n \geq 0$ and translates L by $-n$ units to the left if $n < 0$. If we think of L as an ∞–gon, this is analogous to what we did for $\mathbb{Z}/n\mathbb{Z}$. As in the case of $\mathbb{Z}/n\mathbb{Z}$, this identifies $\mathbb{Z}$ as a proper subgroup of the set of symmetries of L, since we don't get any of the reflections.

We can use the same trick as in the $\mathbb{Z}/n\mathbb{Z}$ case to modify L in such a way that $\mathbb{Z}$ is the full symmetry group: on each edge we draw a little arrow that points to the right:

The integers squared. Our next group is

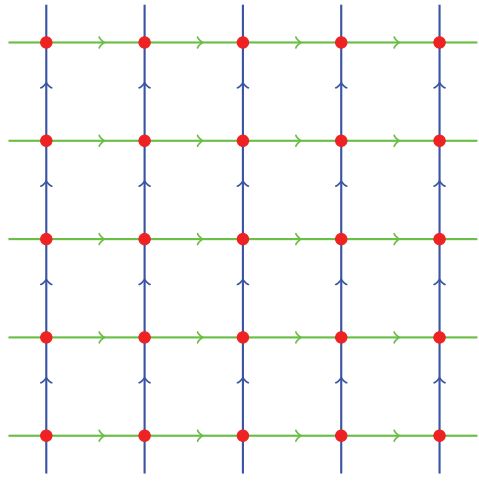
$$\mathbb{Z}^2 = \{(m, n) : m, n \in \mathbb{Z}\}$$

with the multiplication

$$((m, n), (m', n')) \mapsto (m + m', n + n').$$

If we think of $\mathbb{Z}^2$ as the set of vectors in $\mathbb{R}^2$ with integer coordinates, then this is simply vector addition. One generating set for $\mathbb{Z}^2$ is $\{(1, 0), (0, 1)\}$.

We can use the same idea as above to build an object whose symmetries are exactly described by $\mathbb{Z}^2$:



In order for this to work, we need to again refine what we mean by symmetry: this time we insist that colors are preserved as well as the red points and the arrows. The symmetry corresponding to $(m, n) \in \mathbb{Z}^2$ is the translation by m units to the right and n units up. (If m or n are negative, then translate left and down accordingly.)

Multiplicative groups of numbers. We would be remiss to not mention two important groups, $\mathbb{R}^\star$ and $\mathbb{C}^\star$. These are the groups of nonzero real numbers and nonzero complex numbers. The group multiplication in each group is the usual multiplication in $\mathbb{R}$ and $\mathbb{C}$. In both cases the identity is 1. An important distinction between these groups and our previous examples is that $\mathbb{R}^\star$ and $\mathbb{C}^\star$ are not finitely generated, that is, there does not exist a finite generating set.

If you've already seen these groups, you might want to learn about the quaternions, a generalization of the complex numbers which is very important in physics. Instead of just i, the quaternions have i, j, and k! There is a corresponding multiplicative group, consisting again of the nonzero elements.

Matrix groups. There is another set of examples of groups that you learned about in linear algebra (although in such a class you might not have used the word "group"). Denote by $\mathrm{GL}(n, \mathbb{R})$ the set of real $n \times n$ matrices with nonzero determinant. Why is this a group? Well, given two matrices, we already know how to multiply them. Note that this multiplication is closed (that is, the product of two matrices with nonzero determinant is another matrix with nonzero determinant). Indeed, this follows immediately from the following basic fact you learned in linear algebra:

$$\det(MN) = \det(M)\det(N).$$

Two other things you learned in linear algebra is that every square matrix with nonzero determinant is invertible and that multiplication is associative. The identity matrix has determinant 1, which is not zero, so we have checked that $\mathrm{GL}(n, \mathbb{R})$ is indeed a group. It is called the *general linear group*. There are really lots of general linear groups, since n can be any nonnegative integer and $\mathbb{R}$ can be replaced with any ring (see below), but when the context is clear we still call it *the* general linear group.

There are many variations. The group $\mathrm{SL}(n, \mathbb{R})$ is the subgroup of $\mathrm{GL}(n, \mathbb{R})$ consisting of matrices with determinant 1 (this is the *special linear group*). The group $\mathrm{GL}(n, \mathbb{Z})$ is the subgroup of $\mathrm{GL}(n, \mathbb{R})$ consisting of all invertible integral matrices (note: these are exactly the integral matrices with determinant ± 1). Then $\mathrm{SL}(n, \mathbb{Z})$ is the subgroup of $\mathrm{GL}(n, \mathbb{Z})$ consisting of integral matrices with determinant 1. There is also $\mathrm{GL}(n, \mathbb{C})$, the group of complex $n \times n$ matrices with nonzero determinant, and $\mathrm{SL}(n, \mathbb{C})$, the subgroup of $\mathrm{GL}(n, \mathbb{C})$ consisting of $n \times n$ matrices with determinant 1. All of the above examples are subgroups of $\mathrm{GL}(n, \mathbb{C})$, and there are many other examples of interesting subgroups of $\mathrm{GL}(n, \mathbb{C})$ (subgroups of $\mathrm{GL}(n, \mathbb{C})$ are called *linear groups*).

We will study $\mathrm{SL}(2, \mathbb{Z})$ in detail in Office Hour 3, giving a finite presentation for this group as well as many of its relatives.

Exercise 4. Construct a matrix group whose entries lie in a finite field.

The free group of rank 2. Our next example is the most complicated (and interesting!) one yet. And it is most probably not a group that you saw in your undergraduate algebra course.

First we define a *word* in the letters a and b to be an arbitrary finite string made up of the symbols a, b, a^{-1}, and b^{-1}. Some examples are:

$$abababa, aaaaaaa, aba^{-1}b^{-1}, \text{ and } aa^{-1}.$$

We allow the empty word as well; this is the string containing no letters. We can multiply two words by concatenating them:

$$(ab, b^{-1}a) \mapsto abb^{-1}a.$$

Next, we define a *reduced word* to be a word with the property that we never see an a followed by an a^{-1} (or vice versa) or a b followed by a b^{-1} (or vice versa). If we have a word that is not reduced, we can make it shorter by deleting an offending pair of symbols:

$$aa^{-1}abb^{-1}a \rightsquigarrow abb^{-1}a.$$

Performing this procedure inductively will eventually lead to a reduced word. You should check that this reduction procedure always results in the same reduced word. In the above example, there are three places where we could start reducing. In this case, though, no matter what we do we will end up with the reduced word aa.

Exercise 5. Show that every word in a, b, a^{-1}, and b^{-1} can be reduced to a unique reduced word.

We are finally ready to define the *free group of rank 2*. It is the set

$$F_2 = \{\text{reduced words in } a \text{ and } b\}$$

with the multiplication:

$$\text{concatenate, then reduce.}$$

Let's check that this is a group. The identity is the empty word. The inverse of a word is obtained by reversing the word, and then replacing each a by a^{-1}, a^{-1} by a, b by b^{-1}, and b^{-1} by b. For example, the inverse of

$$aba^{-1}b$$

is

$$b^{-1}ab^{-1}a^{-1}$$

Indeed, if we concatenate these two (in either order!) and reduce, we obtain the empty word. Associativity follows immediately from the fact that the reduction procedure always results in the same reduced word (but this fact needs to be proved!). By the very definition of F_2, we see that this group is generated by $\{a, b\}$.

Exercise 6. Check the details of the construction of the free group of rank 2, in particular the assertion that the multiplication is associative. *Hint: Show by induction on the length of (unreduced) words that if there are two choices for a reduction, then either choice leads to the same reduced word. There are two cases, according to whether the two reductions are adjacent or not.*

Free groups are important examples of groups in geometric group theory. Office Hours 3, 4, 5, and 6 explore these groups in more detail.

How can we construct an object whose symmetry group is F_2? This is not so easy! In Office Hour 2 we will explain a way to do this for an arbitrary group.

Other free groups. Given a set S, we can define a free group $F(S)$ as follows. First, we artificially create inverses for each element of S. For $s \in S$, we can write this inverse as s^{-1} (let's not allow s and s^{-1} to both be elements of S). Then the elements of $F(S)$ are reduced words in the elements of S, and the multiplication is defined in the same way as for F_2. As such, when S is a finite set with n elements, we can denote $F(S)$ by F_n (different choices of S with $|S| = n$ technically give different groups, but they are all isomorphic in the sense defined below). Convince yourself that $F(S)$ still is a well-defined group when S is infinite, or even uncountable. In general, the cardinality of S is the *rank* of the corresponding free group.

As we will explain in more detail in the next section, free groups are important because every group is the quotient of a free group.

And many more. One aspect of geometric group theory is to explore the zoo of infinite groups that are out there. Some examples of interesting classes of groups in this book are the Coxeter groups already mentioned (Adam Piggott's Office Hour 13), the right-angled Artin groups (Bob Bell and Matt Clay's Office Hour 14), the lamplighter groups (Jen Taback's Office Hour 15), Thompson's groups (Sean Cleary's Office Hour 16), the mapping class groups (Tara Brendle and Leah Childers' Office Hour 17), and the braid groups (Aaron Abrams' Office Hour 18).

1.3 HOMOMORPHISMS AND NORMAL SUBGROUPS

We'll now take a few minutes to give a quick overview of the most basic and important ideas from a first course in group theory. If you already know all about the first isomorphism theorem and about group presentations, then you might want to skip ahead to the next office hour.

Homomorphisms. We have talked about groups and we now have some examples. Next we would like to discuss how groups relate to each other. A *homomorphism* from a group G to a group H is a function

$$f\colon G \to H$$

so that

$$f(ab) = f(a)\,f(b)$$

for all $a, b \in G$. We can say this succinctly as: f is a function that preserves the multiplication in G. A homomorphism is an *isomorphism* if it is bijective, and two groups are *isomorphic* if there is an isomorphism from one to the other. Convince yourself that isomorphic groups are essentially the same group.

To illustrate the idea of an isomorphism, let's look at a pair of groups. Consider the group $\mathbb{Z}$ on one hand, and the free group F_1 on one generator a on the other hand. Elements of F_1 are finite, freely reduced strings in a and a^{-1}, and the multiplication is given as usual by concatenation and free reduction. What is an isomorphism $\mathbb{Z} \to F_1$? (There is more than one!)

Besides isomorphisms, we might also be interested in injective homomorphisms and surjective homomorphisms. A homomorphism is injective if and only if the preimage of the identity in H is the identity in G. (Why?)

Note that any homomorphism $f\colon G \to H$ can be turned into a surjective homomorphism by replacing H with $f(G)$. For that reason, the surjectivity of a homomorphism is not nearly as crucial as the injectivity. As such we will focus on injective and non-injective homomorphisms.

Injective homomorphisms. If we have an injective homomorphism $f\colon G \to H$, then we can think of f as realizing G as a subgroup of H. Here are a few examples:

1. There is an injective homomorphism $\mathbb{Z}/n\mathbb{Z} \to D_n$ where m maps to rotation by $2\pi m/n$.
2. There is an injective homomorphism $\mathbb{Z}/2\mathbb{Z} \to D_n$ where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ maps to any reflection.
3. There is an injective homomorphism $\mathbb{Z}/2\mathbb{Z} \to S_n$ where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ maps to any product of disjoint transpositions.
4. For any integer $m \neq 0$, there is an injective homomorphism $\mathbb{Z} \to \mathbb{Z}$ given by multiplication by m.
5. For any choice of $(a, b) \neq (0, 0)$, there is an injective homomorphism $\mathbb{Z} \to \mathbb{Z}^2$, where n maps to (na, nb).
6. For any choice of nontrivial element $w \in F_2$, there is an injective homomorphism $\mathbb{Z} \to F_2$ given by $n \mapsto w^n$.

Exercise 7. How many other injective homomorphisms can you find between the groups we have already discussed?

Non-injective homomorphisms. Non-injective homomorphisms can be just as interesting and just as useful. Since we have multiple elements of G mapping to the same element of H, we are definitely losing some information. But the fact that a homomorphism preserves the multiplication of G means we are still remembering some important data. Often we can set up a non-injective homomorphism to

remember exactly the data we care about and throw away everything else. Here are some examples:

1. The most basic example is the homomorphism $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ where 1 maps to 1. A light switch is a great example of this: it does not remember how many times it has been flipped, just whether it has been flipped an even or an odd number of times.
2. There is a homomorphism $\mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^\star$ given by the determinant. So if you want to know the determinant of a product of matrices, you do not need to remember the actual matrices, just their determinants.
3. There is a homomorphism $\mathbb{R}^\star \to \mathbb{Z}/2\mathbb{Z}$ where positive numbers map to 0 and negative numbers map to 1. The fact that this is a homomorphism can be rephrased as: in order to tell if a product of nonzero numbers is positive or negative, you do not need to remember what the numbers are, just whether they are positive or negative.
4. The composition $\mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^\star \to \mathbb{Z}/2\mathbb{Z}$ is a homomorphism that remembers whether an element of $\mathrm{GL}(n, \mathbb{R})$ has positive or negative determinant.
5. There is a homomorphism $S_n \to \mathbb{Z}/2\mathbb{Z}$ that records whether the diagram for a permutation (as above) has an even or an odd number of crossings. In other words, this homomorphism records the parity of the number of transpositions needed to write a given element of S_n.
6. There is a homomorphism $D_n \to \mathbb{Z}/2\mathbb{Z}$ where rotations map to 0 and reflections map to 1. This homomorphism remembers whether the polygon has been flipped over or not.
7. There is a homomorphism $F_2 \to \mathbb{Z}^2$ where the generators a and b for F_2 map to $(1, 0)$ and $(0, 1)$, respectively. This homomorphism remembers the sum of the exponents on a and b in any element of F_2.
8. Any linear map $\mathbb{R}^n \to \mathbb{R}^m$ is a homomorphism. For example, the map $\mathbb{R}^2 \to \mathbb{R}$ that projects to the x–axis is a homomorphism that remembers just the first coordinate. This is a fancy way to state the obvious fact that in order to know the first coordinate of a sum of vectors, you need to know just the first coordinate of each vector.

Exercise 8. How many other non-injective homomorphisms can you find between the groups we have already discussed?

Normal subgroups. Next we will present a definition that will seem unrelated to homomorphisms; and then we will make a deep connection. A *normal subgroup* of a group G is a group N where N is a subset of G and where gng^{-1} lies in N for all $n \in N$ and all $g \in G$.

Why are normal subgroups important? Well, one way to make a normal subgroup of G is to find a group homomorphism f from G to another group H. The *kernel* of f is the set of $g \in G$ so that $f(g)$ is the identity (we use the same terminology in linear algebra). We have the following basic fact: the kernel of a homomorphism $f : G \to H$ is a normal subgroup of G.

Here is why: if n is in the kernel of f, then

$$\begin{aligned} f(gng^{-1}) &= f(g)f(n)f(g^{-1}) = f(g)\,1\,f(g^{-1}) \\ &= f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1, \end{aligned}$$

and so gng^{-1} is also in the kernel of f. Thus the kernel of f is normal.

The above examples of non-injective homomorphisms have kernels as follows:

1. The kernel of our $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is $2\mathbb{Z}$.
2. The kernel of our $\mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^\star$ is $\mathrm{SL}(n, \mathbb{R})$.
3. The kernel of our $\mathbb{R}^\star \to \mathbb{Z}/2\mathbb{Z}$ is $\mathbb{R}_+$.
4. The kernel of our $\mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^\star \to \mathbb{Z}/2\mathbb{Z}$ is the subgroup $\mathrm{GL}^+(n, \mathbb{R})$ consisting of matrices with positive determinant.
5. The kernel of our $S_n \to \mathbb{Z}/2\mathbb{Z}$ is the *alternating group* A_n; this consists of the elements that can be written as the product of an even number of transpositions.
6. The kernel of our $D_n \to \mathbb{Z}/2\mathbb{Z}$ is the subgroup consisting of rotations; this subgroup is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.
7. The kernel of our $F_2 \to \mathbb{Z}^2$ is the set of elements whose a–exponents and b–exponents both add to zero, e.g., $a^7b^{-5}a^{-10}b^5a^3$. This group is also known as the commutator subgroup of F_2 and is denoted by $[F_2, F_2]$.
8. The kernel of the projection $\mathbb{R}^2 \to \mathbb{R}$ is the same as the kernel from linear algebra; in this case it is isomorphic to $\mathbb{R}$.

So non-injective homomorphisms give us nontrivial normal subgroups. Can we go the other way? That is, if N is a normal subgroup of G, is there a homomorphism $G \to H$ so that N is the kernel? The answer is yes! Let's explain this. The first step is to define the *quotient group* G/N. Informally, this is the group obtained from G by declaring every element of N to be trivial.

Let us make this more precise. Declare two elements g_1, g_2 of G to be equivalent if $g_1g_2^{-1} \in N$, and write $[g]$ for the equivalence class of g. Then the elements of G/N are the equivalence classes of the elements of G (notice that the equivalence class of the identity is precisely N). Now we need to say how to multiply two equivalence classes. We declare that the product of the equivalence class $[g_1]$ with the equivalence class $[g_2]$ is the equivalence class $[g_1g_2]$. This is precisely the place where the definition of a normal subgroup comes from—it is exactly what is needed so that this multiplication is well defined.

Exercise 9. Check that the multiplication in G/N is well defined if and only if N is normal.

There is an obvious homomorphism $G \to G/N$, where $g \in G$ maps to $[g] \in G/N$. It is not hard to see that the kernel of this homomorphism is precisely N. So we have completed the loop: normal subgroups and surjective homomorphisms are the same thing!

The first isomorphism theorem. The so-called first isomorphism theorem succinctly summarizes the relationship between homomorphisms and normal subgroups that we have just described.

THEOREM 1.1 (First isomorphism theorem). *If $G \to H$ is a surjective homomorphism with kernel K, then H is isomorphic to G/K.*

Again using our above examples, we have the following isomorphisms:

1. $(\mathbb{Z})/(2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ (this explains the notation $\mathbb{Z}/2\mathbb{Z}$)
2. $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \cong \mathbb{R}^\star$
3. $\mathbb{R}^\star/\mathbb{R}_+ \cong \mathbb{Z}/2\mathbb{Z}$
4. $\mathrm{GL}(n, \mathbb{R})/\mathrm{GL}^+(n, \mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$
5. $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$
6. $D_n/(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$
7. $F_2/[F_2, F_2] \cong \mathbb{Z}^2$
8. $\mathbb{R}^2/\mathbb{R} \cong \mathbb{R}$

Exercise 10. Use the first isomorphism theorem to come up with your own isomorphisms.

1.4 GROUP PRESENTATIONS

You may not have covered group presentations in your first course in abstract algebra, but they are closely tied to the other topics in this section and will loom large in this book.

One naive way to completely describe a group is to list all of the elements and write down the multiplication table (that is, explicitly give the product of any two elements). For a very small finite group, this is a reasonable way of understanding the group. But once you start considering larger—or even infinite—groups this approach becomes unwieldy.

We already have a more economical way of listing the elements of a group: we can list a set of generators. Often the infinite groups we care about have finite sets of generators. This is good, but it certainly doesn't tell us enough about a group: the free group F_2 and the free abelian group $\mathbb{Z}^2$ both have generating sets with two elements and we know that these are different groups since one is abelian and the other is not. We need a way of describing the multiplication table. But obviously we don't want to just list all of the entries.

The key observation is that some entries in the multiplication table imply other entries. In other words, equations between group elements imply other equations. For instance, if $gh = k$ and $h = pq$, then (substituting pq for h in the first equation) we know that $gpq = k$. So what we can hope for is that we don't need to write down the entire multiplication table, but rather a small set of equalities that imply all the others. So now we have exactly hit upon the idea of what a group presentation is: it is firstly a list of generators and secondly a list of defining equalities so that all equalities follow from the listed ones.

Here is a first example, the group $\mathbb{Z}/n\mathbb{Z}$. Let's denote the elements of $\mathbb{Z}/n\mathbb{Z}$ by $a^0, \ldots, a^{n-1}$ instead of $0, \ldots, n-1$. Naturally, the multiplication is $a^j a^k = a^{j+k}$, where the exponents are all taken modulo n. With this notation, $\mathbb{Z}/n\mathbb{Z}$ has the

presentation

$$\mathbb{Z}/n\mathbb{Z} \cong \langle a \mid a^n = 1 \rangle.$$

So the generating set is a and the only defining equality is $a^n = 1$. Every entry in the multiplication table for $\mathbb{Z}/n\mathbb{Z}$ follows from this one equality. For instance, one entry in the multiplication table is $a^{n-3}a^4 = a$. But we can easily derive this using the defining equality $a^n = 1$ as follows:

$$a^{n-3}a^4 = a^{n+1} = a^n a^1 = 1 \cdot a = a.$$

A second important example of a group presentation is the following:

$$\mathbb{Z}^2 = \langle x, y \mid xy = yx \rangle.$$

Can you see why this is a presentation of $\mathbb{Z}^2$? We'll come back to this in a little bit.

Exercise 11. Convince yourself that $\mathbb{Z}^2$ indeed has the purported presentation.

Hopefully these examples give you an idea of what a group presentation is. The way we make things formal—and the way we really think about group presentations—is through the use of free groups. At first our definition of a presentation won't look exactly like the examples we just gave, but we'll eventually explain why it is really the same thing.

A *group presentation* is a pair (S, R), where S is a set and R is a set of words in S. If we freely reduce the elements of R, then we can regard them as elements of the free group $F(S)$, and indeed it will be important to take this point of view. The presentation is finite when both sets S and R are finite.

We say that a group G has the presentation $\langle S \mid R \rangle$ if G is isomorphic to the quotient of $F(S)$ by the normal closure of R, the smallest normal subgroup of $F(S)$ containing R (equivalently, the subgroup of $F(S)$ generated by all conjugates of all elements of R). We write:

$$G \cong \langle S \mid R \rangle.$$

Here is how we think of this: the group G consists of reduced words in $S \cup S^{-1}$ but with the added caveat that words in R are the same as the empty word (this is where the normal closure comes in: if some element of R is supposed to represent the identity, then any conjugate of that element in $F(S)$ should also represent the identity, and any products of conjugates of such elements ...). The elements of S are called *generators* for G and the elements of the normal closure of R are called *relators* for G, and the elements of R are called defining relators. If we have a presentation (as in our above discussion) with a relation like $ab = ba$ or $aba = bab$, then we turn this into a relator by moving everything to one side: $aba^{-1}b^{-1}$ or $abab^{-1}a^{-1}a^{-1}$.

How does this formal definition match up with what we said before? Let's look more closely at $\mathbb{Z}^2$. This group has the presentation

$$\mathbb{Z}^2 \cong \langle a, b \mid aba^{-1}b^{-1} \rangle.$$

(Notice that this is different from the presentation we gave a few minutes ago, but bear with us!) What are the elements of the group $\langle a, b \mid aba^{-1}b^{-1} \rangle$? Well, we

start with the free group on a and b, which consists of all freely reduced words in a and b. Then we need to take the quotient by the normal closure of $aba^{-1}b^{-1}$. What is the quotient as a set? Well, in the quotient we can change a word w into an equivalent word by inserting $aba^{-1}b^{-1}$ anywhere in w, or removing it from anywhere in w.

Why is that the same as our first presentation of $\mathbb{Z}^2$ as $\langle x, y \mid xy = yx \rangle$? Well, we claim that two elements of the free group on $\{a, b\}$ are equivalent in the quotient (by the normal quotient by $aba^{-1}b^{-1}$) if and only if they differ by a sequence of swaps, where we swap ab for ba or vice versa. Let's convince ourselves of this. Start with a word $wbaw'$, where w and w' are both words in a and b. We said we can insert $aba^{-1}b^{-1}$ anywhere we want; so in the quotient,

$$wbaw' = w(aba^{-1}b^{-1})baw' = wab(a^{-1}b^{-1}ba)w' = wabw'.$$

By applying swaps like this we see that every element of the quotient is equivalent to $a^m b^n$ for some m and n. But this gives us an obvious isomorphism between our quotient and $\mathbb{Z}^2$; the isomorphism is given by $a^m b^n \leftrightarrow (m, n)$.

We can also see from the above discussion how our new presentation of $\mathbb{Z}^2$ (with generators a and b) matches up with our old one (with generators x and y). Both presentations are really saying the same thing. So which one you use just depends on your preference. When we have an equality between generators like $xy = yx$, then the equality is called a *relation*. And when we have an equality like $aba^{-1}b^{-1} = 1$ we say that $aba^{-1}b^{-1}$ is a *relator*, as in our formal definition. We can always change a relation to a relator by moving all of the generators to one side (as in our $\mathbb{Z}^2$ example), and the net effect is the same. In this book we will tend to use relators more than relations, but both will come up.

Every group can be given by a group presentation. In particular:

Every group is a quotient of a free group.

This is one reason why free groups are so important. In many ways, geometric group theory grew out of the study of combinatorial group theory, a subject largely concerned with studying groups via their presentations.

Exercise 12. Show that every group has a presentation. *Hint: Your presentation does not have to be efficient.*

Exercise 13. Find (nice) group presentations for F_n, D_n, and S_n.

Armed with the notion of a group presentation, you can start to list lots of different groups. Which presentations represent isomorphic groups? It turns out that this is an unsolvable problem in general; there is no algorithm that will take two presentations and decide in finite time if they present the same group. It is good to keep this in mind: group presentations are very helpful, but they do have limitations.

That's it for the first office hour—we introduced a number of examples of groups that will play key roles in the rest of the book. We want to understand these groups from as many points of view as possible. At first glance you might wonder what there is to learn about a free abelian group or a free group. The answer: more than you might imagine!

Hopefully we have convinced you that the concept of a group is deeply intertwined with the idea of symmetries: groups lead to symmetries and symmetries lead to groups. In order to study infinite groups, we will want to take advantage of this and think of groups geometrically. A key step on this path is to show that every group really is the group of symmetries of some geometric object. That's the goal of the next office hour—see you there!