Lecture 14

Symmetries and groups

14.1 Goals

1. Understand why groups are defined the way they are

2. See examples of groups

3. See that “symmetry” is a notion that depends on specifying what properties of an object one wants to preserve

14.2 Symmetries

Today we’re going to leave behind the idea of rings for a bit, and focus on the idea of a *group*. Groups arise in nature when one studies symmetries. The set of all symmetries of a shape is the most common example of a group.

More abstractly, it turns out that you can abstract the notion of symmetry as any operation the preserves some structure on an object—so symmetry will no longer be just about shapes. We’ll come back to this shortly.

Finally, when you enumerate, and understand the relations between, all the symmetries of certain objects, it may magically turn out that one object has an analogous set of symmetries to a seemingly unrelated object. In other words, two very different objects may have *isomorphic* symmetry groups. So groups begin to give us a deeper insight into the world around us—some objects that seem very different may actually have things in common.[1]

[1] This is similar to the discovery that $\mathbb{Q}$ and $\mathbb{Z}$ admit a bijection between them. As sets,

So, think of a shape. Maybe a circle, a square, a regular pentagon. What do we mean by a symmetry of this shape?

Confusingly, we are taught about symmetry as just a visual property. But in this course, we will think of symmetry as follows:

Definition 14.2.1 (A vague definition of symmetry)**.** A symmetry of an object is some operation we can perform on the object (i) while maintaining an important properties of that object, and (ii) which we can undo.

More accurately, let O be an object, and $\mathbf{P}$ some collection of properties. A symmetry of O is an operation we can perform on O without changing $\mathbf{P}$, and which we can undo.

So to specify what we mean by a symmetry, we must say not only the object we are considering, but *what about* that object we want to preserve.

Example 14.2.2. Consider the isosceles triangle T in the picture above; we will treat it as a subset of $\mathbb{R}^2$ consisting only of the edges and vertices (T does not include the "interior" of the triangle). What properties about T could we care about?

(a) (T as a set.) Let's say you only care about T as a subset of $\mathbb{R}^2$—in other words, as the shape drawn on the sheet of paper. Then the natural property we may want to preserve is: Which subset of $\mathbb{R}^2$ T is. A natural notion of an operation preserving this data, then, is a function from T to T that is a surjection. For is f is a surjection, then $f(T) = T$, so we preserve the subset of $\mathbb{R}^2$ we care about. But if we further want f to be an operation we can "undo," then we'd better demand that f is a bijection (so we can "undo" f by applying its inverse).

This is a crazy large set of symmetries of T. Indeed, there are uncountably many bijections from T to itself. To visualize a crazy bijection, imagine that each point of T is a bee, and we simply allow the bees to fly around, then land again anywhere along T. Points/bees that may have started nearby may end up completely far from each other.

the two are equivalent; the other structures on these sets—such as their addition, or their multiplication—are what distinguish them meaningfully. This insight alone is a powerful way to understand how we differentiate objects in math.

(b) (T as a space.) You could further care not only about T as a subset of $\mathbb{R}^2$, but as a "shape" or as a "space." Put informally, by a symmetry of T, we can now mean an operation which requires us to *not* tear T apart. The natural notion we learn about in multivariable calculus to realize this intuition is the notion of a continuous function. So, we could now narrow down our symmetries to not only be a bijection from T to itself, but a bijection which is also continuous.[2] A typical such symmetry could be visualized as follows: Imagine that T consists of amoebas that are only allowed to travel along T, and who are not allowed to climb over each other; but they can be squished to change size. It again turns out that there are a lot of such symmetries—the set of them is uncountable. But perhaps you can see that the set of continuous bijections of T is naturally a subset of all bijections of T.

(c) (T as something with a notion of distance.) Of course, T has even more structure. If we draw T on $\mathbb{R}^2$, given any two points on T, we can say what the distance between those two points is. So what if we want symmetries of T to preserve distances between points? It turns out there are only 6 operations we can do to T that preserve distance.[3]

Example 14.2.3. Let's consider symmetries of $\mathbb{C}$. As before, if we think of $\mathbb{C}$ just as a set, there are uncountably many symmetries. Now let's think of $\mathbb{C}$ as some ring that contains $\mathbb{R}$, and let's think of symmetries that respect this structure. In other words, let's think of functions $f : \mathbb{C} \to \mathbb{C}$ that send real numbers x to themselves (so $x \in \mathbb{R} \implies f(x) = f(x)$), that happen to be ring homomorphisms (so f respects the ring structure of $\mathbb{C}$) and that are bijections (so f can be undone).

In fact, there are only two such functions: The identity function (sending

[2] For more complicated shapes, we should also demand that the bijection's inverse is continuous. It turns out there are continuous bijections whose inverses are not continuous; but this is for a course in point-set topology.

[3] Here is a proof that there are at most 6: The points farthest from each other on the triangle are the vertices, so any function $f : T \to T$ that preserves distance must send vertices to vertices. A permutation count shows there are at most 6 permutations of the vertices. And in fact, once you specify what a distance-preserving function must do to vertices, this completely determines what the function does on all points on T—this is because if x is on some edge between two vertices v and v', a distance-preserving function f must send $f(x)$ to a point on the edge between $f(v)$ and $f(v')$ with specified distance from each vertex, and there is only one such point.

z to z) and complex conjugation (sending z to $\overline{z}$).[4]

This is in contrast to thinking of $\mathbb{C}$, say, as the space $\mathbb{R}^2$ with a notion of distance. It turns out there are infinitely many bijections of $\mathbb{R}^2$ that preserve distance. For example, choose any point, and rotate any amount around that point; or, choose any vector, and translate $\mathbb{R}^2$ by that vector. Or, choose any line, and reflect about that line.[5] Complex conjugation is an example of this last operation: Reflecting about the real line.

The two take-aways: We think of a symmetry as a reversible operation on an object, and whether a reversible operation counts as a symmetry depends on what properties of the object we want to preserve.

14.3 Definition of group

As I wrote above, the notion of group arises when we try to articulate the set of all symmetries of an object. Here are some non-trivial, but sensible, properties that a set of symmetries should satisfy:

(i) If f is a symmetry of an object, and g is another symmetry, we should be able to "do one symmetry after another" to obtain a new symmetry gf (or, if one does it in the other order, fg).

In other words if, G is a set of symmetries of an object, it should have a binary operation $G \times G \to G$. We'll often call this "composition" or "multiplication." Aren't things getting pretty exciting already?

(ii) "Do nothing" should be a symmetry of any object. (If we don't do anything to an object, we certainly preserve all its properties. And "do nothing" is certainly a reversible process—as we haven't changed anything!)

So, there should be a "multiplicative unit" or an "identity element" in a set of symmetries. After all, if e is the "do nothing" symmetry, and f is any other symmetry, we should have that $fe = ef = f$ because "do nothing, then do f" and "do f, then do nothing" are the same as "just do f."

[4] You should explore why this is! Hint: If $f : \mathbb{C} \to \mathbb{C}$ is a ring homomorphism and if $z^2 = -1$, then $f(z)^2 = -1$, too.

[5] It turns out that any distance-preserving function $f : \mathbb{R}^2 \to \mathbb{R}^2$ is a finite composition of these operations.

(iii) Any symmetry should have an "inverse" symmetry (because we can undo a symmetry operation).

So, every element f in a set of symmetries should have an inverse h for which $fh = e$ and $hf = e$. (To "undo" f means to do an operation h so that the end-result of doing fh is to "do nothing."

(iv) And, of course, composing symmetries should be an associative operation.

We formalize these intuitions into the following definition:

Definition 14.3.1. A *group* is the data of a set G, together with a binary operation (that we will often call a *multiplication*, or the *group operation*) satisfying the following properties:

1. There exists an element e so that, for every $g \in G$, we have $eg = g$ and $ge = g$. We call e the "identity element" of a group.
2. For every $g \in G$, there exists an element $h \in G$ so that $gh = e$ and $hg = e$. We will often call h the *multiplicative inverse* or *inverse* to g.
3. The binary operation is associative, so $g(hk) = (gh)k$ for any triplet $g, h, k \in G$.

Notation 14.3.2. If we need to give an explicit name to the binary operation of a group, we will often use the letter m (for multiplication). So m is a function $m : G \times G \to G$, and the most explicit way to write the product gh would be to write $m(g, h)$.[6]

Notation 14.3.3. Though the data of a group is, strictly speaking, the data of the pair (G, m), we will often write things like "Let G be a group," with the multiplication implicit in the notation.

In contrast, if the operation needs to be made explicit, we will often say G is "a group under m." For example, we will later see that $\mathbb{Z}$ is a group under addition, but not under multiplication.

Remark 14.3.4. Recall that in a ring, when you posit the existence of a multiplicative identity 1, it is unique—in that any other $1'$ satisfying the defining property of a multiplicative identity must equal 1.

[6] But life is short, so we will often write gh instead.

Likewise in a ring, a multiplicative inverse is unique.

The exact same proofs apply to show that the identity element of a group G is unique, and that the inverse to an element g is unique. For this reason, we will say "the" identity element and "the" inverse to an element g.

Notation 14.3.5. Let G be a group and fix an element $g \in G$. We let g^{-1} denote the inverse to g.

More generally, let n be an integer. We let g^n denote the following:

$$\begin{cases} g \cdot \ldots \cdot g & n \text{ times, if } n > 0 \\ (g^{-1}) \cdot \ldots \cdot (g^{-1}) & -n \text{ times, if } n < 0 \\ e & \text{if } n = 0. \end{cases}$$

So for example, g^{-3} is the product of g^{-1} with itself three times.

14.3.1 Abelian groups

Nothing above says that the group operation must be commutative–gh could be unequal to hg. We have a special name for when the group operation is commutative:

Definition 14.3.6. We say that a group G is *abelian* if, for every $g, h \in G$, we have that $gh = hg$.

Remark 14.3.7. "Abelian" is a word derived from the name of Neils Henrik Abel, a Norwegian mathematician who died at the age of 26 in 1829. He studied polynomials whose roots had a symmetry group with commutative multiplication.

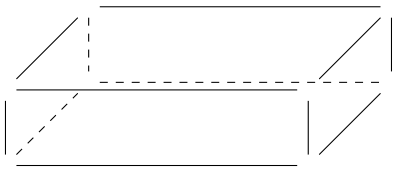
Remark 14.3.8. Often, when a group G is abelian, it is common to write "$g + h$" instead of gh. Just be ready for such notation in the future. There is not concrete rule that says when you should write $g + h$ rather than gh in an abelian group; it often has to do with the intuitions of the writer in the moment.

Example 14.3.9. Let G be a set with one element. Then of course there is a unique function $m : G \times G \to G$; this renders G a group. The identity element is the only element of G, and the identity element is its own inverse. This is called the *trivial group.* It is an abelian group.

14.4 Example: The mattress group

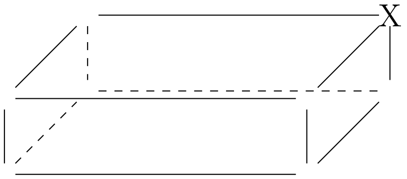
Let's begin with a silly real-life example.

Consider a twin mattress. For ease of visualization, we'll pretend that the mattress is already placed in a (twin-sized) bed frame.

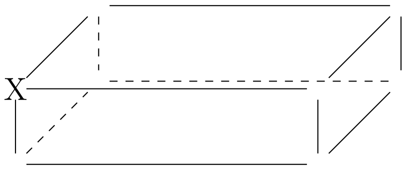


Now, how many ways are there that we can physically re-place the mattress so that it fits inside the frame snugly again?

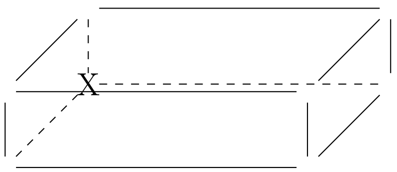
For ease of visualization, let me put a little X in one corner of the mattress that we can follow. Then (and you should try this at home!) there are four ways we can re-place the mattress. The first one is "do nothing," where the little X begins in the far right corner. The other three symmetries are rotations about one of three axes:



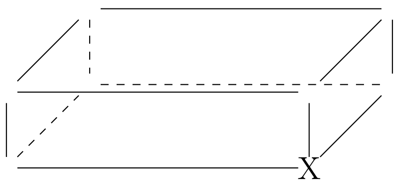
e (Do nothing)



R_z (Rotate 180° about z-axis)



R_y (Rotate 180° about y axis)



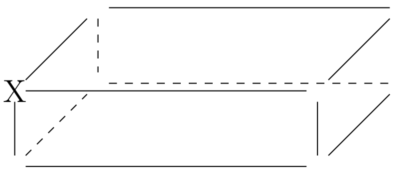
R_x (Rotate 180° about x axis)

Note that the y axis is pointing at you, out of the page. (By the way, you may have asked: Wait, rotate 180 degrees in *which* direction? You end up with the same operation regardless of whether you spin clockwise or counterclockwise, so long as you fix an axis.)

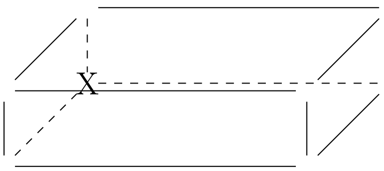
So, while you've probably never thought about this, there are a total of 4 configurations in which you can fit a mattress into a frame. In other words, there are four symmetries to a mattress. We say that "the symmetry group of the mattress has four elements."

But wait, the interesting part about groups is the composition law. In other, what happens when we do one of these symmetries after another?

Let's first apply R_z, and then apply R_y. Here's what we get:



R_z



$R_y R_z$

Look familiar? What we see is the relation $R_y R_z = R_x$! I encourage you to do this at home—if not with a mattress, then some other rectangular solid like a tissue box, or a notebook. Then the multiplication table for this group looks as follows:

	e	R_x	R_y	R_z
e	e	R_x	R_y	R_z
R_x	R_x	e	R_z	R_y
R_y	R_y	R_z	e	R_x
R_z	R_z	R_y	R_x	e

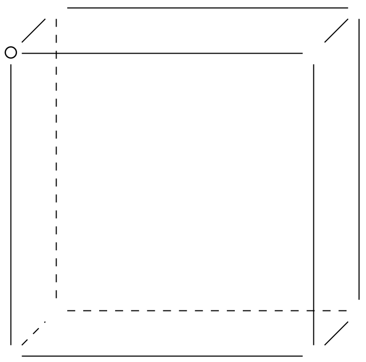
It might surprise you to see that this multiplication table is symmetrical along the diagonal—in other words, the group of symmetries of a mattress is abelian! Moreover, every element is its own inverse (this is why the diagonal consists of the identity element in each entry).

14.5 Exploratory example: A square mattress

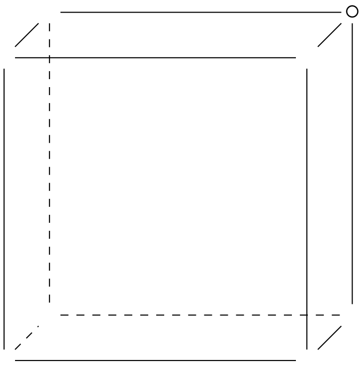
Let's call a mattress *square* if one of its faces is a square. These may not exist in real life, but it's fun to think about the following problem regardless.[7]

[7] A king size bed is very nearly square, but not quite.

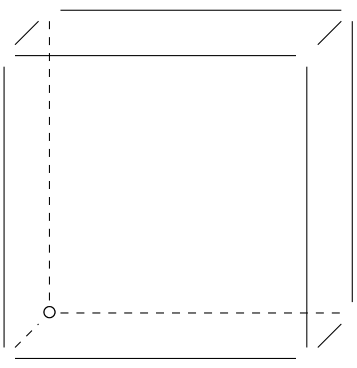
Intuitively, a “square” mattress seems more symmetric than an ordinary mattress—just as a square seems more symmetric than a rectangle. For ease of visualization, I will draw my mattress as though it is standing straight up:



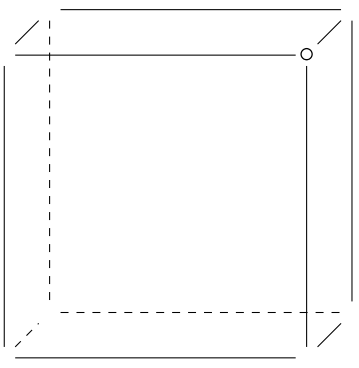
(The face closest to you is the square face.) I’ve marked one corner with a $\circ$ symbol to make the following pictures easier to interpret. We have the following basic operations we can do to the mattress:



R_z



R_y



Q_x (Rotate 90° about x axis)

Note that Q_x is a 90-degree rotation while the others are 180 degree rotations.

We’ve written four of the symmetries of a square mattress–e, R_x, R_z, and R_y. In fact, there should be eight total.

Exercise 14.5.1. Draw pictures of all 8 symmetries you can perform on a square mattress.

(a) Write the multiplication table (it is 8-by-8). This will involve you choosing letters/names for all 8 of the symmetries. Choose wisely!

(b) Is the group of symmetries of a mattress abelian?

(c) Let's write R_x for the operation Q_x^2. If you limit yourself to a well-chosen set of 4 rows and 4 columns, does your multiplication table look like the multiplication table of the symmetries of a non-square mattress?

14.6 The history that led to the idea of groups

We may have occasion to talk about this another time. But in case we don't, let me tell you where groups were first studied systematically.

A lot of mathematicians would credit Evariste Galois as among the first people to abstractly study groups. In fact, Galois combined two areas of mathematics: The area in which one studies symmetries (e.g., groups), and the area in which one studies solutions to polynomial equations. Indeed, just as we've seen that there is a ring automorphism $\mathbb{C} \to \mathbb{C}$ that fixes $\mathbb{R}$ (and exchanges i with $-i$), in general there are ways to "adjoin" new numbers to a given field to solve polynomial equations. For example, you can think of $\mathbb{Q}[\sqrt{2}]$ as the smallest ring inside $\mathbb{C}$ that contains both $\mathbb{Q}$ and $\sqrt{2}$. It turns out that such extensions have symmetries that permute the roots of polynomials. The fundamental theorem of Galois theory gives an explicit relationship between subgroups of a symmetry group and intermediate extensions of a given field.

When phrased in this way, it probably seems like an amazing leap of imagination that "symmetry" (a geometric concept) can have a profound impact on algebra. I don't know to what extent Galois would have used the word "symmetry" to describe what he was doing. I think he mainly thought of his symmetries as just exchanging roots around—nothing more than permutations. And perhaps it is a more modern way of thinking that a permutation is a symmetry of a set.

14.7 Exercises

Exercise 14.7.1. For this problem, you may assume the following fact from linear algebra: If A and B are n-by-n matrices over $\mathbb{R}$, then

$$\det(AB) = \det(A)\det(B).$$

(Here, det is the determinant.) Using the fact that the determinant of the identity matrix is 1, show that if A is an invertible matrix, then $\det A$ cannot be zero. The converse is also true, but we do not prove it here. (If you are curious, you may look up Cramer's Rule.)

(In fact, this holds in $M_n(R)$ when R is any commutative ring, not necessarily $\mathbb{R}$. In this generality, it turns out that a matrix is invertible if and only if its determinant is a unit of R.)

Exercise 14.7.2. In some textbooks, they demand that a group G be "closed" under the multiplication operation. This is a bit old-fashioned; it comes from the fact that we often define operations but make the mistake that the output of an operation might not be in the correct set. Here is an exercise illustrating this:

Let R be a ring (not necessarily commutative). Verify that if x and y are units, then xy is also a unit. (Thus, we say that "the set of units is closed under multiplication.")

Exercise 14.7.3. We say that a group G is *cyclic* if there exists some $g \in G$ so that the set $\{g^n, n \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots$ is all of G. (We say that g "generates G.")

1. Prove that $(\mathbb{Z}/4\mathbb{Z})^\times$ is a cyclic group.
2. Prove that $(\mathbb{Z}/8\mathbb{Z})^\times$ is not a cyclic group.
3. Prove that $(\mathbb{Z}/5\mathbb{Z})^\times$ is a cyclic group.

Gauss proved the following amazing result: $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if n is 2, 4, p^k, or $2p^k$ for some odd prime.

Exercise 14.7.4. Let G be a group.

1. Prove that the identity element of G is unique.
2. Let $g \in G$. Prove that the inverse of g is unique.
3. Prove that $(gh)^{-1} = h^{-1}g^{-1}$.