CCS Discrete Math I | Professor: Padraic Bartlett

Lecture 4: Finite Groups

Week 4 | *UCSB 2014*

Over the first three weeks of this course, we've considered combinatorial questions about **sets**: that is, collections of static objects, which we've focused on enumerating in various ways. However, these are not the only sorts of objects combinatorialists study! Instead, we can study what happens when we equip sets with **operations**: that is, various ways to act on and manipulate elements of our set! When we do this in certain ways, this gives us access to questions that demand stronger techniques than we've developed so far: we can enumerate elements of sets, but what happens when we add functions into the mix? How do we study sets that can change?

This, in a sense, is going to be the focus of the rest of the course. Over the next seven weeks, we're going to examine three specific ways to add structure to sets: **groups**, **fields** and **vector spaces**. In particular, we're going to study **finite** examples of all of these objects, and look at how combinatorialists use all of these objects to solve problems in the field!

The first such concept we study here is the idea of a **group**:

1 Groups

1.1 Basic definitions / examples.

Definition. A **group** is a set G along with some operation $\cdot$ that takes in two elements and outputs another element of our group, such that we satisfy the following properties:

- **Identity**: there is a unique identity element $e \in G$ such that for any other $g \in G$, we have $e \cdot g = g \cdot e = g$.

  In other words, combining any group element g with the identity via our group operation does not change g! You know many objects like this: if we work with the real numbers $\mathbb{R}$ and think of addition as our group operation, then 0 is our identity, as $0 + x = x$ for any x. Similarly, if we consider the real numbers again but take our operation to be multiplication, then 1 is our identity, as $1 \cdot x = x$ for any x.

- **Inverses**: for any $g \in G$, there is a unique g^{-1} such that $g \cdot g^{-1} = g^{-1} g = e$.

  In other words, if we start at any group element g, we can always find something to combine with g using our group operation to get back to the identity! Again, you know several objects like this: with $\mathbb{R}$ and addition, the inverse of any number x is just its negative $-x$, while if we consider the set of nonzero real numbers and multiplication, the inverse for any x is just $1/x$.

- **Associativity**: for any three $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

  In other words, the order in which we group combinations together doesn't matter, as long as the sequence that we have those objects grouped together in does not change!

I.e. we can combine a with $b \cdot c$, or first find $a \cdot b$ and then combine that with c. Again, most of the natural operations you're familiar with (addition, multiplication) are associative: it is perhaps more interesting to point out some things that are nonassociative. For example, exponentiation is a nonassociative operation: $2^{(3^4)} = 2^{81} \approx 2.41 \cdot 10^{24}$, while $(2^3)^4 = 8^4 = 4096$.

It bears noting that this does not say that $a \cdot b = b \cdot a$: that is a different property, called **commutativity**, and is not a property that groups need to have (as we will show in the examples!) Groups that are commutative are called **abelian groups**, after the mathematician Niels Henrik Abel.

We list a number of examples of groups, as well as some nonexamples. Here, we don't give formal proofs that any of these objects are groups; instead, we list them rapid-fire to give you a list of examples to think about in your head! (If you're interested, you can prove that any of these objects satisfy the claimed properties, though! For some it will be harder than others, but if you're in the Introduction to Higher Mathematics class they are all proofs you could come up with given sufficient time.)

Example. As noted above, the real numbers with respect to addition, which we denote as $\langle \mathbb{R}, + \rangle$, is a group: it has the identity 0, any element x has an inverse $-x$, and it satisfies associativity.

Nonexample. The real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}, \cdot \rangle$, is **not** a group: the element $0 \in \mathbb{R}$ has no inverse, as there is nothing we can multiply 0 by to get to 1!

Example. The nonzero real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}^\times, \cdot \rangle$, is a group! The identity in this group is 1, every element x has an inverse $1/x$ such that $x \cdot (1/x) = 1$, and this group satisfies associativity.

Example. The integers with respect to addition, $\langle \mathbb{Z}, + \rangle$ form a group!

Nonexample. The integers with respect to multiplication, $\langle \mathbb{Z}, \cdot \rangle$ do not form a group: for example, there is no integer we can multiply 2 by to get to 1.

Nonexample. The natural numbers $\mathbb{N}$ are not a group with respect to either addition or multiplication. For example: in addition, there is no element $-1 \in \mathbb{N}$ that we can add to 1 to get to 0, and in multiplication there is no natural number we can multiply 2 by to get to 1.

Example. $GL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices, is a group under the operation of matrix multiplication. Notice that this group is an example of a **nonabelian** group, as there are many matrices for which $AB \neq BA$: consider $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ versus $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Example. $SL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices with determinant 1, is also a group under the operation of matrix multiplication; this is because the property of being determinant 1 is preserved under taking inverses and multiplication for matrices.

These examples are all great, but they're not really what I'm interested in for this class. Instead, I want to focus on examples of **finite** groups! In the next section, we study examples of these groups in more depth than above, and explain more about why they form a group.

1.2 Finite groups.

Definition. The object $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$ is defined as follows:

- Your set is the numbers $\{0, 1, 2, \ldots n-1\}$.
- Your addition operation is the operation "addition mod n," defined as follows: we say that $a + b \equiv c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

  For example, suppose that $n = 3$. Then $1 + 1 \equiv 2 \mod 3$, and $2 + 2 \equiv 1 \mod 3$.
- Similarly, our multiplication operation is the operation "multiplication mod n," written $a \cdot b \equiv c \mod n$, and holds whenever $a + b$ and c differ by a multiple of n.

  For example, if $n = 7$, then $2 \cdot 3 \equiv 6 \mod 7$, $4 \cdot 4 \equiv 2 \mod 7$, and $6 \cdot 4 \equiv 3 \mod 7$.

Example. $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots n-1\}$ is a commutative group with respect to the operation of addition mod n! This is not hard to check:

1. **Identity**: 0 is the identity of this group. This is easy to check: take any $x \in \{0, 1, \ldots n-1\}$. We know that $0 + x = x$ in the integers; therefore, because the difference of any two equal numbers is 0, and 0 is a multiple of n for any n, we have by definition that $0 + x \equiv x \mod n$.
2. **Associativity** and **commutativity** are inherited from the integers in a similar fashion! Notice that

$$\begin{aligned} &\forall x, y, z \in \mathbb{Z}/n\mathbb{Z}, x + (y + z) = (x + y) + z \text{ and } x + y = y + x \\ \Rightarrow &\forall x, y, z \in \{1, \ldots n-1\}, x + (y + z) = (x + y) + z \text{ and } x + y = y + x \\ \Rightarrow &\forall x, y, z \in \{1, \ldots n-1\}, x + (y + z) \equiv (x + y) + z \mod n \text{ and } x + y \equiv y + x \mod n, \end{aligned}$$

   by exactly the same logic as above (equality implies equivalence mod n for any n.)
3. **Inverses**: Given any $k \neq 0 \in \{0, 1, \ldots n-1\}$, notice that $n - k$ is also in this set, and that $k + n - k = n \equiv 0 \mod n$. Therefore every element has an inverse, as claimed!

This is not the only way in which modular arithmetic can make a group:

Example. $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \dots p-1\}$ is a commutative group with respect to the operation of multiplication mod p, if and only if p is a prime.

Seeing this is not too difficult. If you repeat the logic from our earlier proof, we can see that $(\mathbb{Z}/p\mathbb{Z})^\times$ satisfies **associativity**, **identity** and **commutativity**, simply because these properties are "inherited" from the integers $\mathbb{Z}$.

Therefore, the only property we need to check is inverses. We first deal with the case where p is not prime. Write $p = mn$ for two positive integers $m, n \neq 1$; notice that because both of these values must be smaller than p if their product is p, both m and n live in the set $\{1, \dots p-1\}$.

Consider the element n. In particular, notice that for any k, we have

$$\begin{aligned} & kn \equiv x \mod p \\ \Rightarrow & kn - x \text{ is a multiple of } p \\ \Rightarrow & kn - x \text{ is a multiple of } mn \\ \Rightarrow & kn - x \text{ is a multiple of } n \\ \Rightarrow & x \text{ is a multiple of } n. \end{aligned}$$

(If none of the above deductions make sense, reason them out in your head!) Because of this, we can see that n has no inverse in $(\mathbb{Z}/p\mathbb{Z})^\times$, as kn is only congruent to multiples of n, and 1 is not a multiple of n.

The converse — showing that if p is prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ has inverses — is a little trickier. We do this as follows: first, we prove the following claim.

Claim. For any $a, b \in \{0, \dots p-1\}$, if $a \cdot b \equiv 0 \mod p$, then at least one of a, b are equal to 0.

Proof. Take any a, b in $\{0, \dots p-1\}$. If one of a, b are equal to 0, then we know that $a \cdot b = 0$ in the normal "multiplying integers" world that we've lived in our whole lives. In particular, this means that $a \cdot b \equiv 0 \mod p$ as well.

Now, suppose that neither a nor b are equal to 0. Take both a and b. Recall, from grade school, the concept of **factorization**:

Observation. Take any nonzero natural number n. We can write n as a product of prime numbers $n_1 \cdot \ldots \cdot n_k$; we think of these prime numbers $n_1, \dots n_k$ as the "factors" of n. Furthermore, these factors are **unique**, up to the order we write them in: i.e. there is only one way to write n as a product of prime numbers, up to the order in which we write those primes. (For example: while you could say that 60 can be factored as both $2 \cdot 2 \cdot 3 \cdot 5$ and as $3 \cdot 2 \cdot 5 \cdot 2$, those two factorizations are the same if we don't care about the order we write our numbers in.)

In the special case where $n = 1$, we think of this as already factored into the "trivial" product of no prime numbers.

Take a, and write it as a product of prime numbers $a_1 \cdot \ldots \cdot a_k$. Do the same for b, and write it as a product of primes $b_1 \cdot \ldots \cdot b_m$. Notice that because a and b are both numbers that are strictly between 0 and $n-1$, n cannot be one of these prime numbers (because positive multiples of n must be greater than n!)

In particular, this tells us that the number $a \cdot b$ on one hand can be written as the product of primes $a_1 \cdot \ldots \cdot a_k \cdot b_1 \cdot \ldots \cdot b_m$, and on the other hand (because factorizations into primes are unique, up to ordering!) that there is no n in the prime factorization of $a \cdot b$.

Conversely, for any natural number k, the number $k \cdot n$ **must** have a factor of n in its prime factorization. This is because if we factor k into prime numbers $k_1 \cdot \ldots \cdot k_j$, we have $k \cdot n = k_1 \cdot \ldots \cdot k_j \cdot n$, which is a factorization into prime numbers and therefore (up to the order we write our primes) is unique!

In particular, this tells us that for any k, the quantities $a \cdot b$ and $k \cdot p$ are distinct; one of them has a factor of p, and the other does not. Therefore, we have shown that if both a and b are nonzero, then $a \cdot b$ cannot be equal to a multiple of p — in other words, $a \cdot b$ is not congruent to 0 modulo p! Therefore, the only way to pick two $a, b \in \{0, \ldots p-1\}$ such that $a \cdot b$ is congruent to 0 modulo p is if at least one of them is equal to 0, as claimed. $\square$

From here, the proof that our group has inverses is pretty straightforward. Take any $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, and suppose for contradiction that it did not have any inverses. Look at the multiplication table for x in $(\mathbb{Z}/p\mathbb{Z})^\times$:

	1	2	3	...	$p-1$
x	?	?	?	...	?

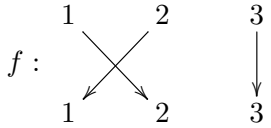
If x doesn't have an inverse, then 1 does not show up in the above table! The above table has p slots, and if we're trying to fill it without using 1, we only have $p-1$ values to put in this table; therefore some value is repeated! In other words, there must be two distinct values $k < l$ with $xl \equiv xk \mod p$.

Consequently, we have $x(l-k) \equiv 0 \mod p$, which by our above observation means that one of $x, (l-k)$ are equal to 0. But x is nonzero, as it's actually in $(\mathbb{Z}/p\mathbb{Z})^\times$: therefore, $l-k$ is equal to 0, i.e. $l = k$. But we said that k, l are distinct; so we have a contradiction! Therefore, every element x has an inverse, as claimed.

There are other finite groups beyond those made out of modular arithmetic! In particular, there are several notable examples of **noncommutative** groups: we describe some of those here.

Example. The **symmetric group** S_n is the collection of all of the permutations on the set $\{1, \ldots n\}$, where our group operation is composition. In case you haven't seen this before:

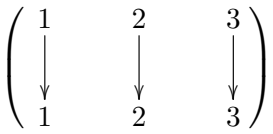
- A **permutation** of a set is just a bijective function on that set. For example, one bijection on the set $\{1, 2, 3\}$ could be the map f that sends 1 to 2, 2 to 1, and 3 to 3.
- One way that people often denote functions and bijections is via "arrow" notation: i.e. to describe the map f that we gave above, we could write

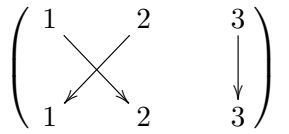


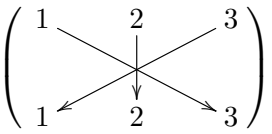
- This, however, is not the most space-friendly way to write out a permutation. A much more condensed way to write down a permutation is using something called **cycle notation**. In particular: suppose that we want to denote the permutation that sends $a_1 \to a_2$, $a_2 \to a_3$, $\ldots a_{n-1} \to a_n$, $a_n \to a_1$, and does not change any of the other elements (i.e. keeps them all the same.) In this case, we would denote this permutation using cycle notation as the permutation

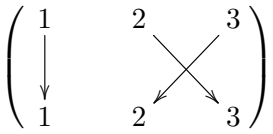
$$(a_1 a_2 a_3 \ldots a_n).$$

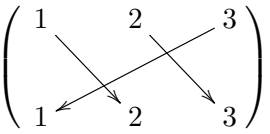
To illustrate this notation, we describe all of the six possible permutations on $\{1, 2, 3\}$ using both the arrow and the cycle notations:

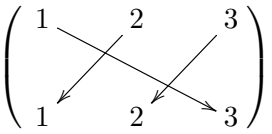
id : 

(12) : 

(13) : 

(23) : 

(123) : 

(132) : 

It's worth noting that some permutations need to be represented with multiple cycles. For example,

$$(143)(25) = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ & & & & \\ 1 & 2 & 3 & 4 & 5 \end{array} \right),$$

because 1 maps to 4, 4 maps to 3, and 3 maps to 1, giving us (143), and 2 maps to 5 maps to 2, giving us (25).

Because the composition of any two bijections is still a bijection, we have in particular that the composition of any two permutations is another permutation: so our group operation does indeed combine group elements into new group elements.

Composing any map f with the identity map $id(x) = x$ does not change the map f, so $id(x)$ is an identity element.

Associativity is tedious but doable to check: take any three bijections $f : C \to D, g : B \to C, h : A \to B$. We want to check that $(f \circ g) \circ h : A \to D$ is the same map as $f \circ (g \circ h) : A \to D$. To do this, it suffices to show that they send the same elements to the same places, as this is exactly what it means for two functions to be equal. Take any $a \in A$, and notice that

$$((f \circ g) \circ h)(a) = (f \circ g)(h(a)) = f(g(h(a)))$$
$$(f \circ (g \circ h))(a) = (f(g(h(a)))) = f(g(h(a))).$$

So we satisfy associativity!

Finally, to see that we have inverses, notice that any bijection $f : X \to Y$ has an inverse function $f^{-1}Y \to X$ defined by

$$f^{-1}(y) = \text{ the unique } x \text{ such that } f(x) = y.$$

Notice that $f^{-1} \circ f(x) = x$ for any x: in other words, their composition is the identity! Therefore, any bijection has an inverse, and thus S_n is a group.

While the above work certainly shows that S_n is a group, it may not do a great job of giving us a feel for how to combine its elements. To do this, let's demonstrate a small yet useful property about S_n:

Definition. A permutation $\sigma \in S_n$ is called a **transposition** if we can write $\sigma = (ab)$, for two distinct values $a, b \in \{1, \dots n\}$.

Claim. We can write any $\sigma \in S_n$ as a product of transpositions.

Proof. To illustrate what our claim is, let's work it out for all of the elements of S_3. We first note that $(12), (13)$ and (23) are all trivially covered by this proposition, as they are themselves transpositions; as well, we can "trivially" write id as the product $(12)(12)$, amongst other things, as

$$id : \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix} \quad = \quad (12)(12) : \begin{pmatrix} 1 & 2 & 3 \\ \searrow\swarrow & & \downarrow \\ 1 & 2 & 3 \\ \searrow\swarrow & & \downarrow \\ 1 & 2 & 3 \end{pmatrix},$$

because both maps send 1 to 1, 2 to 2, and 3 to 3 (just follow the arrows!)

To work this out for (123) and (132) takes not much more work. Simply notice that to do the permutation (123), we could start with the swap 1 and 2, to get 1 to map to the right thing; from there, we currently have $2 \to 1$ and $3 \to 3$, when we want $2 \to 3$ and $3 \to 1$. Swapping 1 and 3 fixes these issues, and gives us the swap we want! Because function compositions are read right-to-left (because in $f(g(x))$, you apply g to x before applying f!), we would write this as (13)(12): and indeed, we can check that

$$(123) = \begin{pmatrix} 1 & 2 & 3 \\ & \searrow\swarrow\searrow & \\ 1 & 2 & 3 \end{pmatrix} = (13)(12) = \begin{pmatrix} 1 & 2 & 3 \\ \searrow\swarrow & & \downarrow \\ 1 & 2 & 3 \\ \swarrow\downarrow\searrow & & \\ 1 & 2 & 3 \end{pmatrix}.$$

Using similar logic, we can see that (132) can be written as (12)(13):

$$(132): \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 1 & 2 & 3 \end{pmatrix} = (12)(13) = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 1 & 2 & 3 \\ & & \\ 1 & 2 & 3 \end{pmatrix}.$$

This hopefully gives us a bit more of a feel for what we're doing here! Just to illustrate a tricker case, however, let's try a longer permutation: what about $\sigma = (12345) \in S_5$? Well: let's use similar logic to our earlier cases. We know that σ sends $1 \to 2$; so we can start with (12) as our first transposition. Now 1's going to the right place! If we consider 2, it's currently going to 1, when it should be going to 3. Therefore, if we follow up our first switch with (13), it will send 2 to 3, while not changing where 1 maps to (as we didn't touch its target from the first step, 2!)

This process continues: 3 is mapping to 1 now, and it should map to 4; so we should apply (14). Then, 4 is mapping to 1, and it should map to 5; so we apply (15). Now we have 5 mapping to 1, which is correct; in other words, all of our elements are mapping to the right place! This is easily verified with a quick diagram:

$$(12345) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$(15)(14)(13)(12) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \\ 1 & 2 & 3 & 4 & 5 \\ & & & & \\ 1 & 2 & 3 & 4 & 5 \\ & & & & \\ 1 & 2 & 3 & 4 & 5 \\ & & & & \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

In general, suppose we have any cycle $(a_1 a_2 \dots a_n)$. I claim that we can write this cycle as the product

$$(a_1 a_2 \dots a_n) = (a_1 a_n) \dots (a_1 a_4)(a_1 a_3)(a_1 a_2);$$

we prove this by induction. Our base case, when $n = 2$, is trivially true: so we move to our inductive step. Assume that our case holds for length-n cycles, and consider a cycle $(a_1 a_2 \dots a_n a_{n+1})$ of length $n + 1$.

So: consider the product $(a_1a_{n+1})(a_1a_n)\dots(a_1a_4)(a_1a_3)(a_1a_2)$. We want to show that this permutation is precisely the cycle $(a_1a_2\dots a_na_{n+1})$.

By induction, we know our product of transpositions is equal to $(a_1a_{n+1})(a_1a_2\dots a_n)$. Consider where this permutation sends elements:

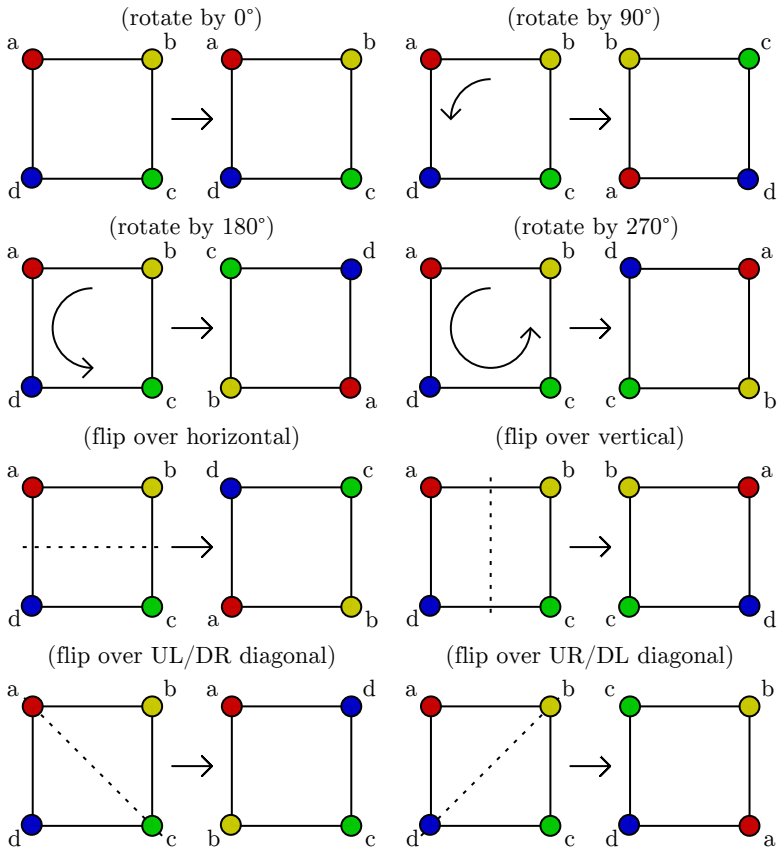
- If we look at any of the elements $a_k \in \{a_1, \dots a_{n-1}\}$, each a_k gets sent to a_{k+1} by the cycle $(a_1a_2\dots a_n)$; because none of the elements $a_2, \dots a_n$ are in the transposition (a_1a_{n+1}), it does not interact further with any of these elements.
- If we look at a_n, it is sent to a_1 by the cycle $(a_1a_2\dots a_n)$; because a_1 is then sent to a_{n+1} by the transposition (a_1a_{n+1}), in total we have that a_n is sent to a_{n+1}.
- Finally, a_{n+1} is not touched by the cycle $(a_1a_2\dots a_n)$, and is then sent to a_1 by the transposition (a_1a_{n+1}).

In total, we have that each a_k is sent to a_{k+1}, with the exception of a_{n+1}, which is sent to a_1. In other words, our product of transpositions is precisely $(a_1a_2\dots a_na_{n+1})$, as claimed.

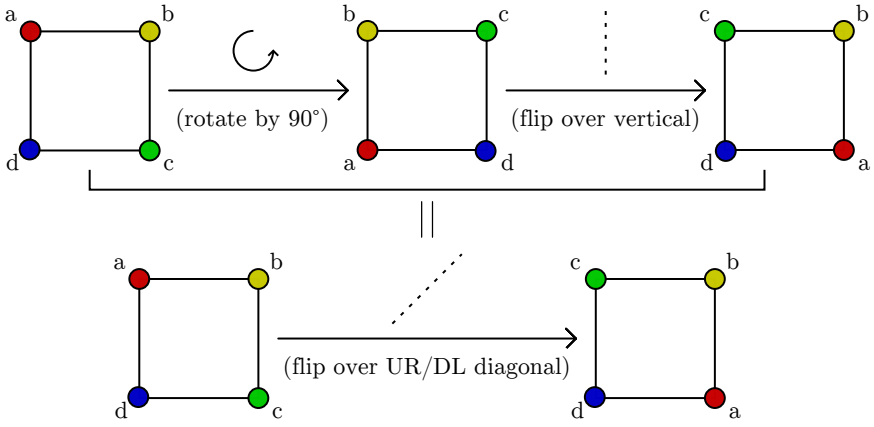
Via cycle notation, we can write any permutation as some product of cycles: applying this result to each cycle in turn lets us write each permutation as a product of cycles, as claimed. □

Not all finite groups are as algebraic as S_n! Our last example, for instance, is beautifully geometric in nature:

Example. Consider a regular n-gon. There are a number of geometric transformations, or **similarities**, that we can apply that send this n-gon to "itself" without stretching or tearing the shape: i.e. there are several rotations and reflections that when applied to a n-gon do not change the n-gon. For example, given a square, we can rotate the plane by $0°, 90°, 180°$, or $270°$, or flip over one of the horizontal, vertical, top-left/bottom-right, or the top-right/bottom-left axes:



Given two such transformations f, g, we can compose them to get a new transformation $f \circ g$. Notice that because these two transformations each individually send the n-gon to itself, their composition also sends the n-gon to itself! Therefore composition is a well-defined operation that we can use to combine two transformations.



Notice that the trivial rotation by 0°, when composed with any other map, does not change that map: so, under the operation of composition, rotation by 0° is an **identity**! Similarly, notice that performing the same flip twice in a row returns us back to the identity, so every flip has an **inverse** given by itself! (I.e. if f is a flip, $f \circ f = id$: i.e. $f = f^{-1}$.)

As well, if we rotate by k degrees, rotating by $360 - k$ degrees results in a total rotation by 360: i.e. rotation by $0°$. So all rotations have inverses as well!

Finally, notice that because function composition is associative (as shown above!), this operation is **associative** as well. Consequently, the collection of all symmetries of a regular n-gon forms a group under the operation of function composition!

We call this last group D_{2n}, because it is the group of **order**[1] $2n$. Algebraists will usually use this terminology; geometers, however, will often write the same group as D_n, as they care about they object whose symmetries we are studying (a n-gon) more than the number of symmetries themselves ($2n$).

1.3 Enumerating groups.

This is a discrete mathematics course! Consequently, the first question we should have, upon encountering a new concept, is (roughly) the following: **how many of these things exist**? To be a bit more precise:

Question. Given any natural number n, how many groups are there of order n?

At first glance, you might suspect that the answer is infinite! For example, the following four groups all give us groups of order 1:

- $\langle \{1\}, \cdot \rangle$, the group with one element 1, and the operation of multiplication.
- $\langle \{0\}, + \rangle$, the group with one element 0, and the operation of addition.
- $\langle \{f : \mathbb{R} \to \mathbb{R}, f(x) = x\}, \circ \rangle$, the group with one element $f(x) = x$, and the operation of composition.
- S_1, the group made of all permutations of the set $\{1\}$ with respect to composition of permutations.

We could easily keep going, and in fact make an infinite family of order-1 groups:

- For any $n \in \mathbb{N}$, let $\langle \{f : \{n\} \to \{n\}, f(n) = n\}, \circ \rangle$ denote the one-element group of all maps from $\{n\}$ to $\{n\}$ under group composition.

However, in a sense all of these groups are the **same**! They all have one element — call it x for right now — and their operations are all defined by sending (x, x) to x. So, in a sense, calling these groups "different" is kind of silly: they have different names and labels, but they're all encoding the same **size** and **structure** as each other!

We make this formal via the following definition:

Definition. Take any two groups $\langle G, \cdot \rangle, \langle H, \star \rangle$, and any map $\varphi : G \to H$. We say that φ is a **group isomorphism** if it satisfies the following two properties:

1. **Preserves size**: φ is a bijection[2].

[1] The **order** of a group is the number of elements in that group!

[2] Notice that this means that there is an inverse map $\varphi^{-1} : H \to G$, defined by $\varphi^{-1}(h) =$ the unique $g \in G$ such that $\varphi(g) = h$.

2. **Preserves structure**: φ, in a sense, sends $\cdot$ to $\star$. To describe this formally, we say the following:

$$\forall g_1, g_2 \in G, \quad \varphi(g_1 \cdot g_2) = \varphi(g_1) \star \varphi(g_2).$$

This property "preserves structure" in the following sense: suppose that we have two elements we want to multiply together in H. Because φ is a bijection, we can write these two elements as $\varphi(g_1), \varphi(g_2)$. Our property says that $\varphi(g_1 \cdot g_2) = \varphi(g_1) \star \varphi(g_2)$: in other words, if we want to multiply our two elements in H together, we can do so using either the G-operation $\cdot$ by calculating $\varphi(g_1 \cdot g_2)$, or by using the H-operation $\star$ by calculating $\varphi(g_1) \star \varphi(g_2)$.

Similarly, if we want to multiply any two elements g_1, g_2 in G together, we can see that $g_1 \cdot g_2 = \varphi^{-1}(\varphi(g_1 \cdot g_2)) = \varphi^{-1}(\varphi(g_1) \star \varphi(g_2))$. So, again, we can multiply elements using either G or H's operation! To choose which operation we use, we just need to apply φ or φ^{-1} as appropriate to get to the desired set, and perform our calculations there.

This is something that is perhaps best understood with an example. Consider the following two groups:

Example. Take a 1×2 rectangle, and the set of all geometric transformations that send this rectangle to itself without stretching or tearing. There are four such transformations: flipping across either the horizontal or vertical axes, rotating 180°, or the identity transformation:

$$id, r_{180}, f_v, f_h.$$

These transformations form a group!

To see how they interact, we can form a **group table,** which we define here:

Definition. Take any group $\langle G, \cdot \rangle$ of order n: that is, any group G consisting of n distinct elements. We can create a **group table** corresponding to G as follows:

- Take any ordering $r_1, \ldots r_n$ of the n elements of G: we use these elements to label our rows.
- Take any other ordering $c_1, \ldots c_n$ of the n elements of G: we use these elements to label our columns. (This ordering is usually the same as that for the rows, but it does not have to be.)
- Using these two orderings, we create a $n \times n$ array, called the **group table** of G, as follows: in each cell (i, j), we put the entry $r_i \cdot c_j$.

For example, one group table for the symmetries of the rectangle we were discussing earlier could be the following:

$r_i \circ c_j$	id	r_{180}	f_v	f_h
id	id	r_{180}	f_v	f_h
r_{180}	r_{180}	id	f_h	f_v
f_v	f_v	f_h	id	r_{180}
f_h	f_h	f_v	r_{180}	id

This table actually helps us verify that our collection of transformations is a group! In particular, by looking at it, we can see that id is an identity, as $id \circ$(anything) = (anything). We can also see that every element has an inverse, as there is a copy of id in every row (and therefore for any element x, there is some other element x^{-1} such that $x \cdot x^{-1} = id$.) Associativity is the only group property that is not immediate from looking at a group table; to check it for this example, however, we can just refer to our earlier proof that function composition in general was associative.

Example. Take the set $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, otherwise denoted as $(\mathbb{Z}/2\mathbb{Z})^2$. This set has four elements: $(0,0), (0,1), (1,0), (1,1)$, and is a group under the operation of "pairwise addition mod 2. To see this, we will construct this group's table as well:

$r_i + c_j \mod 2$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(0,0)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(0,1)$	$(0,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(1,0)$	$(1,1)$	$(0,0)$

As before, we can tell by looking at this table that our set has an identity $(0,0)$, and that every element has an inverse! To see associativity, we just use the fact that we know that $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ is associative from our earlier work: therefore, if we have any three elements $(a,b), (c,d), (e,f)$, we know that

$$\begin{aligned}(a,b) + ((c,d) + (e,f)) &= (a,b) + (c+e, d+f) \\ &= (a + (c+e), b + (d+f)) \\ &= ((a+c)+e, (b+d)+f) \\ &= (a+c, b+d) + (e,f) \\ &= ((a,b) + (c,d)) + (e,f).\end{aligned}$$

So this is a group!

In fact, not only is $\langle (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), + \rangle$ a group, but it's a group that is **isomorphic** to our first group of symmetries of a rectangle! To see this, simply consider the bijection $\varphi : (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \to \{id, r_{180}, f_v, f_h\}$ defined by

- $f((0,0)) = id$,
- $f((1,0)) = f_v$,
- $f((1,1)) = r_{180}$,
- $f((0,1)) = f_h$.

Take this map, and apply it to the group table for $\langle(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), +\rangle$: that is, replace each element of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ with ϕ of that element! This gives us

$r_i + c_j \mod 2$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(0,0)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(0,1)$	$(0,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(1,0)$	$(1,1)$	$(0,0)$

$\longmapsto$

$\varphi(r_i + c_j \mod 2)$	id	r_{180}	f_v	f_h
id	id	r_{180}	f_v	f_h
r_{180}	r_{180}	id	f_h	f_v
f_v	f_v	f_h	id	r_{180}
f_h	f_h	f_v	r_{180}	id

which is just our table that we calculated earlier for the symmetries of a rectangle! In other words, we've just explicitly shown that $\varphi(g_1 + g_2) = \varphi(g_1) \circ \varphi(g_2)$, for any $g_1, g_2 \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Therefore, φ is a group isomorphism, and these two groups are isomorphic!

The idea here is that on some fundamental level, these two groups are the "same:" if you're adding things in $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ or composing symmetries of a rectangle, you're really doing the **same** things, up to the labels you've assigned to objects! This is a powerful observation to have. Many times in mathematics, it can be useful to take a problem and rephrase it in a different way; i.e. some tools may be easier to apply to a problem that's talking about geometric transformations, while others might be easier when you're working with a more number-theoretic setting like $\mathbb{Z}/n\mathbb{Z}$!

Notice, also, **how** we showed that these two groups were equal: by finding a **bijection** that sent one group's table to the other! This process generalizes completely:

Theorem. Two groups $\langle G, \cdot\rangle, \langle H, \star\rangle$ are isomorphic if and only if there is a bijection $\varphi : G \to H$ such that when we apply φ to a group table of G, we get a group table of H!.

Note that our claim is not that applying φ to a group table of G gives us **any** group table of H. It is possible that when we look at H's group table, we would have written some elements in a different order; this does not mean that our group is different, or that φ would not be a isomorphism!

Using these ideas, you can verify the following claims:

- There is one group of order 1, up to isomorphism.
- There is one group of order 2, up to isomorphism.
- There is one group of order 3, up to isomorphism.
- There are two groups of order 4, up to isomorphism.

To verify these claims, use the following process:

1. To count groups of order n, take n distinct elements $id, a_1, \ldots a_{n-1}$, where we've decided that id is the identity element. (One identity must exist, so we are justified in doing this, and have lost no generality in doing so thus far!)

2. Attempt to find all of the ways to fill in the $n \times n$ group table for these elements that preserves our identity and inverse properties. Notice that this will force you to have no repeated elements in any row or column (as $rc_1 = rc_2 \Rightarrow c_1 = c_2$ by using the existence of inverses!)

3. Now that you've made all of your tables, check to see if any are isomorphic!

4. Finally, check each table for associativity. (This is the least-fun part.)

5. The total number of nonisomorphic group tables is your total number of groups.

We illustrate this method for $n = 3$:

Claim. There is one group of order 3 up to isomorphism

Proof. Take any group on three elements. Without loss of generality, let's name its elements $\{id, x, y\}$; we can do this without losing generality because we only care about groups up to isomorphism, and thus in particular don't care about the names of our elements (as a bijection can just relabel them to anything else.) Furthermore, assume that one of them is the identity; we can do this because we know some identity element exists. Again, because we don't care about what things are named, we can assume that id is the identity.

Consider any possible group table for these elements under any arbitrary group operation. We know that because id is an identity, we have the following entries filled in "for free' by using the definition of identity:

$r_i \cdot c_j$	id	x	y
id	id	x	y
x	x		
y	y		

Notice that if $x \cdot x = id$, our "no repeats in any row or column" idea would force $x \cdot y = y$, which would place a repeated value in y's column. This cannot happen; therefore $x \cdot x \neq id$. We also know from this no-repeats property that $x \cdot x \neq x$, as we already have an x in this row: therefore, we have $x \cdot x = y$.

$r_i \cdot c_j$	id	x	y
id	id	x	y
x	x	y	
y	y		

Our no-repeats property then forces us to set $x \cdot y = id, y \cdot x = id$, and $y \cdot y = x$:

$r_i \cdot c_j$	id	x	y
id	id	x	y
x	x	y	id
y	y	id	x

Therefore we have at most one group table! If you want, you could directly check that this table is associative: alternately, you can observe that this is just the table for addition mod 3, which we already know is a group!

$r_i \cdot c_j$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

So there is only one group of order 3, as claimed. □