Applied Category Theory

Caleb Hill

Fall 2025

Contents

9/3/2025

Why?

Why should you care about studying the coming content and applying it to your field?
Physicists:

- The particles in the standard model *are* irreducible representations. So rep theory is crucial to you.
- Monoidal categories give a good framework for understanding QM.

Computer scientists:

- It gives a framework for the Curry-Howard correspondence (proofs are programs).

Me:

- Began as a study of "analogies" and turned into a study of nifty algebraic gadgets.
- It's written in a *wild* language, and learning languages is fun.

As a great motivation, see `https://arxiv.org/abs/0903.0340`

Plan

The **first goal** is to define monoidal categories with some context. The **second goal** is to describe a "skeletal" category defined by diagrammatics. To accomplish the first goal, we will study things including:

- Algebraic objects (groups, vector spaces, ...) and maps between them
- Subobjects, images, combining objects ($\times$, $\otimes$, $\oplus$, ...)
- Categories (Grp, Set, $PoSet$, $\mathbb{N}$, Vec, ...)

I'd like to have as little fat on this as necessary. That is, not get sidetracked studying, for instance, too much of the internal structure of these objects. I want to give many examples and try to build intuition. For the second goal we'll study things including:

- Representations and maps ($T(gv) = gT(v)$)
- Rep(D_3) in detail

Up to this point I have a strong vision of where we're going. After this we can go where the interest steers us.
This plan is incomplete and non-exhaustive.

Groups

This is the best onramp to categories I know of, so bear with me through some basics.

Definition 1. *A* **group** *is a triple*

$$(G, \mu, e)$$

where G is a set, $\mu : G \times G \to G$ is a function, and $e \in G$, such that

$$\forall a, b, c \in G, \quad \mu(\mu(a, b), c) = \mu(a, \mu(b, c)) \tag{Associativity}$$

$$\forall a \in G, \quad \mu(a, e) = \mu(e, a) = a \tag{Identity}$$

$$\forall a \in G, \exists b \in G, \quad \text{such that} \quad \mu(a, b) = \mu(b, a) = e \tag{Inverse}$$

We often call the element b from 1 by a^{-1}. We also often use the following shorthands:

- $\mu(a, b) = a \cdot b = a \star b = ab$

- $\underbrace{a \cdot a \cdots a}_{n \text{ copies}} = a^n$

Exercise 1. *Translate the three axioms above into the ab notation.*

Exercise 2. *Prove the identity element in a group is unique. That is, if e and e' both satisfy Axiom 1, show that $e' = e$.*

Now some examples. As an excercise, prove that each of the following is a group. The notation $:=$ reads as "is defined to be."

Example 1 (General linear group)**.** (G, μ, e)*, where*

- $G = \mathrm{GL}_2(\mathbb{C}) := \{$*invertible* 2×2 *matrices with entries in* $\mathbb{C}\}$
- $\mu(A, B) := AB$
- $e = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Example 2 (General linear group)**.** (G, μ, e)*, where*

- $G = \mathrm{GL}_n(\mathbb{C}) := \{$*invertible* $n \times n$ *matrices with entries in* $\mathbb{C}\}$
- $\mu(A, B) := AB$
- $e = I_n$ *(the $n \times n$ identity matrix)*

Example 3 (Integers)**.** (G, μ, e)*, where*

- $G = \mathbb{Z}$
- $\mu(a, b) := a + b$
- $e = 0$

Example 4 (Not a group! Why?)**.** (G, μ, e)*, where*

- $G = \mathbb{Z}$
- $\mu(a, b) := a \times b$
- $e = 1$

Example 5 (Braid group)**.** $B_n := (G, \mu, e)$*, where*

- $G =$ *n-strand braid diagrams (up to isotopy/wiggling)*
- $\mu =$ *vertical concatenation*
- $e = n$ *unbraided strands*

Steve pointed out that when $n = 2$, B_n is isomorphic to $\mathbb{Z}$. We'll get to that in the next lecture I hope.

Things that came up

- Generators and relations presentations
- Free group/group of words
- Symmetric group/permutation groups
- The natural numbers game:
  `https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/index2.html`
- Peano arithmetic:
  `https://en.wikipedia.org/wiki/Peano_axioms`

9/10/2025

More groups

Recall that, loosely, a group is a set endowed with a binary operation (multiplication), with some associativity, identity, and inversion constraints. Henceforth we will refer to a group (G, μ, e) almost exclusively as G. Usually, μ and e will be understood from context. For some of the following examples we might also write μ_G to refer specifically to multiplication in G.

Example 6 (Nonzero field elements). *The set $\mathbb{C}^\times = \mathbb{C} - \{0\}$ is a group under multiplication. Associativity is known. Its identity element is $1 \in \mathbb{C}$. This is true for any field, i.e. $\mathbb{R}^\times$, $\mathbb{Q}^\times$, and $\mathcal{F}_{p^n}^\times$ are all groups.*

Example 7 (Symmetric groups). *Let X be a set. Then (G, μ, e) is a group, where*

- $G = \{\sigma : X \to X \mid \sigma \text{ is bijective }\}$
- $\mu(\sigma_1, \sigma_2) \coloneqq \sigma_1 \circ \sigma_2$
- $e = id_X$*, defined by* $\forall x \in X$, $id_X(x) = x$

Example 8. *If $X = \{1, \ldots, n\}$, then we denote the group S_X by S_n. If $\sigma \in S_n$ then we often denote σ as*

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Example 9 (Dihedral group). *Let G consist of the following six matrices:*

These matrices permute the points

$$\left\{(1,0), (-\frac{1}{2}, \frac{\sqrt{3}}{2}), (-\frac{1}{2}, -\frac{\sqrt{3}}{2})\right\}$$

So we can see that it's "the same as" a certain permutation group. There are really 3 things at play in this last example:

- Dihedral groups: 3 wasn't special. We could divide by any positive n and get a group of $2n$ matrices.
- Generators and relations: We could equally express this group as

  $$\langle r, s \mid r^3 = e, s^2 = e, rs = sr^2 \rangle.$$

  In fact, that's usually how dihedral groups are presented.
- Isomorphism: That group of matrices "is" a permutation group.

Homomorphisms

We'll start by definine how two groups can be similar, or the same.

Definition 2. *Let G and H be two groups. Let $f : G \to H$ be a function.*

- *We call f a* **homomorphism** *if*

  $$\forall a, b \in G, f(ab) = f(a)f(b)$$

- *We call f an* **isomorphism** *if it is a bijective homomorphism*
- *If f is a homomorphism, the* **kernel** *of f is the set*

  $$\ker(f) \coloneqq \{x \in G \mid f(x) = e_H\}$$

- *If f is a homomorphism, the* **image** *of f is the set*

  $$f(G) \coloneqq \{f(X) \mid x \in G\} \subseteq H$$

Here are many examples. It would be useful to prove those you don't see immediately. Well, it would probably be good to prove all of them...

Example 10 (Modular arithmetic)**.** *$f : \mathbb{Z} \to \mathbb{Z}_n$, given by $f(x) \coloneqq x \pmod n$*

Example 11 (Multiplication)**.** *$f : \mathbb{Z} \to \mathbb{Z}$, given by $f(x) \coloneqq 4x$. What is special about 4 here? Anything?*

Example 12 (Trivial)**.** *Let G and H be any two groups. Define $f : G \to H$ by $f(x) = e$.*

Example 13 (Identity)**.** *Let G be any group. Define $f : G \to G$ by $f(x) \coloneqq x$.*

Example 14 (Symmetric group inclusion)**.** *Define $f : S_n \to S_{n+1}$ by declaring*

$$f(\sigma) \coloneqq \begin{pmatrix} 1 & 2 & \cdots & n & n+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) & n+1 \end{pmatrix}$$

In particular, since this homomorphism is injective, this means we can think of S_n as "sitting inside of" S_{n+1}. This actually holds more generally. If a homomorphism $f : G \to H$ is injective, then there is an isomorphic copy of G inside of H, in the form of the image $f(G)$. We'll define this more precisely in the next subsection.

Example 15 (Linear maps)**.** *Let V and W be vector spaces over $\mathbb{C}$. The definition of vector spaces says that $(V, +)$ and $(W, +)$ are, in particular, abelian groups. Let $T : V \to W$ be a linear map. The condition*

$$T(x + y) = T(x) + T(y)$$

implies that T is a homomorphism of (abelian) groups.

Example 16 (All linear maps)**.** *$f : \mathbb{Z} \to \mathbb{Z}_n$, given by $f(x) \coloneqq x \pmod n$*

Here's a fact that we'll have uses for.

Exercise 3. *Let $f : G \to H$ be a homomorphim of groups. For every $a \in G$, the inverse of $f(a)$ is $f(a^{-1})$. In equation form, that's*

$$[f(a)]^{-1} = f(a^{-1}).$$

Subgroups

As we saw above, S_n "sits inside of" S_{n+1}. Here's how we say that precisely.

Definition 3. *Let G be a group. A nonempty subset $A \subseteq G$ is called a subgroup of G if*

$$\forall a, b \in A, \quad ab \in A \tag{Closure}$$

$$\forall a \in A, \quad a^{-1} \in A \tag{Inversion}$$

The first consequence of this definition is that if A is a subgroup of G, then $e \in A$. Why? Well, take any element $a \in A$. Its inverse, a^{-1} also is in A by definition. Their product also must be in A. But their product is e.

Here's a fact that will be of use.

Proposition 1. *Let $f : G \to H$ be a homomorphism. Then*

1. *The kernel $\ker(f)$ is a subgroup of G.*
2. *The image $f(G)$ is a subgroup of H.*

Let's see some examples of subgroups in action.

Example 17 (Dihedral groups)**.** *Let $n \geq 1$ be a positive integer. The set of $2n$ matrices of the forms*

$$\begin{bmatrix} \cos 2\pi\frac{k}{3} & -\sin 2\pi\frac{k}{3} \\ \sin 2\pi\frac{k}{3} & \cos 2\pi\frac{k}{3} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \cos 2\pi\frac{k}{3} & \sin 2\pi\frac{k}{3} \\ \sin 2\pi\frac{k}{3} & -\cos 2\pi\frac{k}{3} \end{bmatrix}$$

for $k = 0, 1, \ldots, n-1$ is a subgroup of $\mathrm{GL}_2(\mathbb{C})$.

Example 18 (Special linear group)**.** *The set $SL_N(\mathbb{C}) \coloneqq \{M \in \mathrm{GL}_N(\mathbb{C}) \mid \det(M) = 1\}$ is a subgroup of the general linear gorup $\mathrm{GL}_N(\mathbb{C})$.*

9/17/2025

UNSTABLE

I'd like to define a representaiton today, since we have all the prerequisite knowledge. The crux of the problem is this: group multiplication is hard. It's generally undecidable whether a given group element is even the identity. But if we can translate a group's multiplication into something more concrete (like matrices!), then we can learn a lot more about the group.

We'll begin by recalling that a homomorphism between groups G and H is a function $f : G \to H$ satisfying

$$f(\underbrace{ab}_{\in G}) = \underbrace{f(a)f(b)}_{\in H}.$$

It's important to remember which group the multiplication is happening in.

There's a cool way to visualize this property that I'll draw on the board. I won't include it here becasue it's time-consuming to create…

Representations

Groups are meant to *act* on things, that is, to encode structure-preserving permutations. We've seen examples of this already:

- Permutation groups: all permutations of an abstract set X. The structure being preserved here is cardinality.
- Matrix groups: an invertible (bijective!) matrix is a permutation of $\mathbb{C}^n$.

A representation of a group is a sort of middle ground between these two. That is, it translates some (maybe not all) of the structure of a group into a matrix group, which permutes a vector space.

Definition 4. *Let G be a group. A (linear)* **representation** *of G is a homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{C})$.*

Remark 1. *Soemtimes we will write $\rho(g)$ as ρ_g and $[\rho(g)](v)$ as any one of $\rho_g v$, $g.v$, or even just gv.*

Every group has at least one representation.

Example 19. *Let G be any group. Define $\rho : G \to \mathrm{GL}_1(\mathbb{C})$ by $\rho(g) := [1]$ for every $g \in G$. Then ρ defines a representation, since it's a homomorphism:*

$$\begin{aligned} \rho(gh) &= [1] \\ &= [1][1] \\ &\rho(g)\rho(h) \end{aligned}$$

A similar construction gives a representation of G on $\mathrm{GL}_n(\mathbb{C})$ by sending $g \mapsto I_n$.

Here's an example that translates modular arithmetic into matrix multiplication.

Example 20. *Let $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition modulo 4 as the operation. Define $\rho : G \to \mathrm{GL}_1(\mathbb{C})$ by $\rho(k) := [e^{2\pi i \frac{k}{4}}]$. Then ρ defines a representation, since it's a homomorphism:*

$$\begin{aligned} \rho(j+k) &= [e^{2\pi i \frac{j+k}{4}}] \\ &= [e^{2\pi i \frac{j}{4}} e^{2\pi i \frac{k}{4}}] \\ &= [e^{2\pi i \frac{j}{4}}][e^{2\pi i \frac{k}{4}}] \\ &\rho(j)\rho(k) \end{aligned}$$

Geometric example

These examples are both one-dimensional, so they don't really show the true flavor of representation theory. Here's an example that is more complicated, which we'll linger on for a while. It's similar to the matrix group example, up to a change of basis.

Let D_3 be the group with the following six elements:

$$\{e, r, r^2, s, sr, sr^2\}$$

where we can freely multiply any elements using the reduction rules

$$r^3 = e, \quad s^2 = e, \quad rs = sr^2.$$

We could alternatively phrase this by saying $D_3 = \langle r, s \mid r^3 = e, s^2 = e, rs = sr^2 \rangle$. We'll define a representation $\rho : D_3 \to \mathrm{GL}_2(\mathbb{C})$ by declaring

$$\rho(s) := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \rho(r) := \begin{bmatrix} e^{2\pi i/3} & 0 \\ 0 & e^{-2\pi i/3} \end{bmatrix}$$

and claiming that with these assignments, the images of the rest of the elements of D_3 are fully determined. To understand this claim, we should do an example or two. We'll be as loose as you're comfortable with, and try to argue convincingly, albeit informally, that ρ translates the multiplication of D_3 into the multiplication in $\mathrm{GL}_2(\mathbb{C})$.

First consider the properties $s^2 = e$ and $r^3 = e$ separately in D_3. The image of s under ρ shares a corresponding property:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

as does the image of r under ρ:

$$\begin{bmatrix} e^{2\pi i/3} & 0 \\ 0 & e^{-2\pi i/3} \end{bmatrix} \begin{bmatrix} e^{2\pi i/3} & 0 \\ 0 & e^{-2\pi i/3} \end{bmatrix} \begin{bmatrix} e^{2\pi i/3} & 0 \\ 0 & e^{-2\pi i/3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$