GROUP COHOMOLOGY AND TOPOLOGY: USING SLINKIES TO UNDERSTAND ADDITION

ERIC PETERSON

Abstract. Much of undergraduate education in mathematics is spent revisiting and expanding ideas presented more superficially earlier in life. One piece of math frequently left out of this process and taken for granted is the standard addition algorithm taught in primary school. The incarnations of this algorithm in modern mathematics live in the intersection of abstract algebra, the field concerned with number-like systems, and topology, the field concerned with shapes and their smooth deformations. I will sketch this connection in some generality and explain how add-and-carry arises from this framework.

1. Group definitions

To start investigating why adding works the way we say it does, we have to introduce a formal notion of what "adding" could possibly mean in excessive generality. Toward these ends, we make the following definition:

An (abelian) group is a set X equipped with a binary operation $+$ which satisfies the following axioms:

(1) For any three elements $x, y, z \in X$, the associative law holds: $x + (y + z) = (x + y) + z$ (so we may write $x + y + z$ without ambiguity).
(2) There exists an element $0 \in X$ such that $0 + x = x + 0 = x$ for all $x \in X$. This element is called the identity element of the group.
(3) For each element $x \in X$ there's a corresponding element $-x \in X$ such that $x + (-x) = -x + x = 0$. The element $-x$ is called the inverse of x.
(4) For each pair of elements x, $y \in X$, we have $x + y = y + x$.

Lots of familiar things fit into these axioms, including the following examples, which will be our bread and butter for the rest of the hour:

- the integers with addition, 0, and negative numbers,
- rotation groups R_n of a regular n-gon with composition, no rotation, and reversed orientation, and
- product groups with component-wise operations, component-wise identities, and component-wise inverses.

It turns out that abelian groups are very similar to vector spaces, and so a lot of what comes next will smell like linear algebra. For instance, the first question we should ask is: how do we compare or relate groups? With sets, we have functions that map one set to another. With groups, this is not enough: for instance, R_4 and $R_2 \times R_2$ both have four elements (and so their underlying sets admit a bijection), but these groups are different. To illustrate why, the element "rotate once" in R_4 must be applied four times to a regular square to cause rotation, whereas all elements in $R_2 \times R_2$ only have to be applied twice — hence, a difference in the two group structures.

The solution to this problem is to require that our function preserve multiplication; we define a "map of groups" to be a function $f : G \to H$ satisfying the relation $f(x + y) = f(x) + f(y)$. (This looks a lot like the definition of a linear transformation!) Let's look at some examples of group maps. If we pick n, m naturals with $n \mid m$, we can select n evenly spaced points out of the m. One rotation of these n points corresponds to m/n rotations of the m points, and so we have a map $\varphi : R_n \to R_m$ given by $\varphi(r_n) = \frac{m}{n} \cdot r_m$, where r_n and r_m correspond to a single rotation in R_n and R_m respectively.

Things get more interesting when we look at noninjective maps. Here's a noninjective example: write an integer z as $z = ns + t$ for $0 \leq t < n$ using the Euclidean algorithm, then build a map of builds $f : \mathbb{Z} \to R_n$ by the formula $f(ns + t) = t \cdot r_n$ (the reader familiar with elementary number theory will recognize that this identifies R_n with "the integers modulo n"). This is a map of groups and is not injective, and so we must be losing some information along the way. So, a new reasonable question is: what does the preimage of $x \in R_n$ by f look like? To answer this: let $\phi : G \to H$ be a group map and let $\ker \phi$ (pronounced "the kernel of ϕ") denote the set $\ker \phi = \{g \in G \mid \phi(g) = 0\}$. One can show that if $\phi(g) = h$, then $\phi^{-1}(h) = \{g + k \mid k \in \ker \phi\}$, which is to say that the loss of information is "uniform," and at each point in the group we see a translated copy of the kernel. For our $f : \mathbb{Z} \to R_n$, $\ker f$ is given by all the multiples of n in $\mathbb{Z}$.

2. Extension problem

The next reasonable question: suppose someone else has a map of groups $f : G \to H$. If he gives us $\ker f$ (the information lost) and H (the information kept), is it possible to reconstruct G (the information he started with)? Somewhat surprisingly, the answer is no!—this is the first hint of how groups differ from vector spaces. For instance, consider the maps

$$R_4 \to R_2,$$

$$R_2 \times R_2 \to R_2,$$

the first of which is given by doubling (rotating twice whenever we used to rotate once) and the second of which is given by forgetting one of the copies of R_2. Both maps have kernel R_2, and so $R_2 \times R_2$ and R_4 are both possible answers to the above question, and we know from earlier that they're distinct. But this is interesting in its own right! We might now ask a smarter question: given some group N and some group H, can we construct a group G containing N and a map $f : G \to H$ so that $N = \ker f$ (called an extension of H by N)? How many? What do they look like?

3. Fibrations and slinkies

Let's break for a moment to try to answer this question. I think about algebraic topology, which means that I think of groups and spaces (or, loosely, shapes) in very similar ways. I saw earlier that we were collapsing big things (G) into smaller things (H) and the collapse was uniform (kernel N). In topology, there is a similar situation, called a covering map.

Completely eschewing details and even correctness, a "continuous map" between two shapes I'll draw on the board is the same thing as a way of laying down the source shape onto the target shape without any tearing (but stretching and bending are allowed). A continuous map is said to be a "covering map" when, if I preimage a small piece of the target shape, I get a collection of pieces in the source space that all look identical to the piece they're landing on.

Let me show you what I mean: let's take a slinky and stretch it out some, so that it's dangling down. If we shine a spotlight straight down from above, the picture we see on the floor is a circle. Moving a point on the slinky to its point in the shadow is an example of a covering map; if we take a small arc on the shadow and look at what lies above it, we see a bunch of small arcs on the slinky. Another example is a big vertical stack of loops, also with a spotlight shining straight down.

Now, an important structural remark about covering maps: trace a path in the shadow, and pick a point in the fiber (fancy name for the preimage of a point) of our starting location. I assert that there's a unique corresponding path we can trace on the slinky (or stack of loops), such that the shadow cast by our hand above would exactly mimic the original motion of our hand on the shadow circle. By checking the endpoint of our lifting path, we produce from our path an invertible map from the fiber of the starting point to the fiber of the finishing point. (We can produce an inverse map by tracing the path backward.) These maps often contain nontrivial information—for instance, if we form a complete loop in the shadow, the map on the fiber will shift points up or down the slinky.

Now, for the really amazing fact: it turns out that this assignment

$$\{\text{paths } \gamma \text{ in the shadow}\} \to \{\text{maps from the fiber over the start of } \gamma \text{ to the fiber over the end of } \gamma\}$$

is actually all you need to reconstruct the covering map!

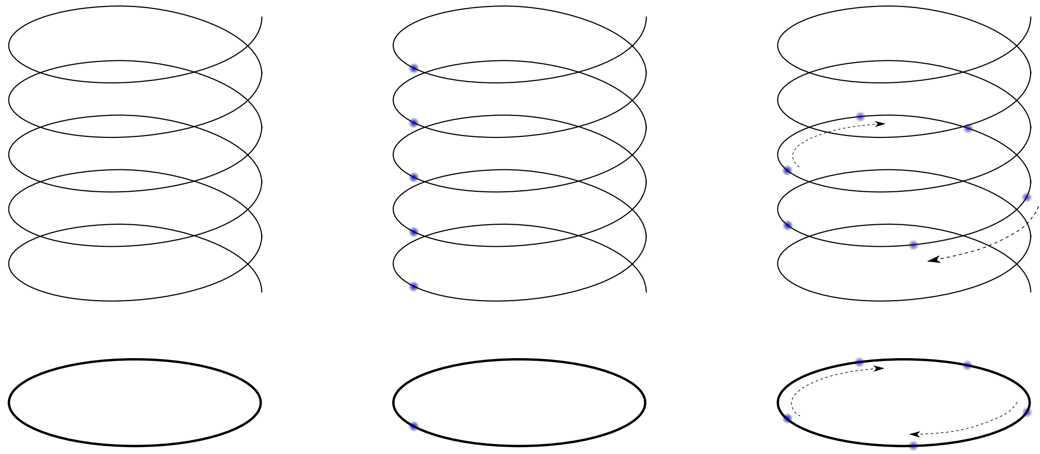

FIGURE 1. Turning paths into maps between fibers

4. Translating to algebra

Now, since covering maps can characterized by an assignment from paths in the base space to maps between the fibers, we could try to understand extensions of groups in the same way. First, we have to translate all the topological vocabulary into ideas that make sense for groups — after all, in the algebraic setting we don't have literal "paths." We'll use the following dictionary to make sense of the situation:

topology	algebra
covering maps	extensions
space structure	group structure
fiber jumps	translations in N
base paths	translations in H.

The rough idea is that where in a topological space we could move around using paths, in a group we can instead move around using the group operation. A generic point in a covering space could be identified as a pair points, one in the fiber and one in the base, and so we should try to find a group operation on the **set** $N \times H$ that reflects these ideas.

To start, we should be able to take a generic point (n, x) and translate around in the fiber by applying the group element $(m, 0)$. We arrive at the following guess for our group law: $(n, x) + (m, 0) = (n + m, x)$. We can also translate around in the base from a generic point (n, x) by applying the group element $(0, y)$. We've already seen in the slinky example that our position on the fiber can change as we move around in the base, and so we prepare for that by introducing a function $g : H \times H \to N$ so that $g(x, y)$ corresponds to the movement in the fiber when translating from x to $x + y$. This results in the following second guess for our group law: $(n, x) + (0, y) = (g(x, y) + n, x + y)$.

Putting these two together, we get

$$(n, x) + (m, y) = (n, 0) + (0, x) + (m, y) = (g(x, y) + n + m, x + y),$$

which I claim is a group provided g satisfies two "cocycle conditions":

$$g(0, 0) = 0,$$
$$g(x, y + z) + g(y, z) = g(x + y, z) + g(x, y).$$

The first axiom requires that we don't do any fiber translating if we don't move in the base. Geometrically, the second axiom asserts that there's no difference between translating in the base from one point, to a second point, then to a third point versus translating from the first point to the third point directly — that is, the following two associations are equivalent:

$$(n, x) + ((0, y) + (0, z)) = ((n, x) + (0, y)) + (0, z).$$

5. Producing g from an extension

Now we need to figure out what good this framework is by asking: how many extensions can we represent with these ideas? The answer is: all of them! To understand why, let's see how we can produce a g given an extension $N \subseteq G \xrightarrow{\pi} H$. Since π is surjective we can always find a **function** $s : H \to G$ such that $(\pi \circ s)(x) = x$ for all $x \in H$ and $s(0) = 0$ (s is called a pointed section of π). Now, we aren't requiring s to be a map of groups — and in fact there exist H and N such that s cannot be a map of groups! This is interesting to us, because the failure of s to be a map of groups is representative of how twisted up the extension G is, which is supposed to be analogous to the nontrivial connectedness of a covering space.

So, let's measure that! Define $g(x, y)$ as

$$g(x, y) = s(x) + s(y) - s(x + y).$$

We can then immediately check the two axioms required above:

$$\begin{aligned} g(0, 0) &= s(0) + s(0) - s(0) \\ &= 0 + 0 - 0 \\ &= 0, \end{aligned}$$

and

$$\begin{aligned} g(x, y + z) + g(y, z) &= s(x) + s(y + z) - s(x + y + z) + s(y) + s(z) - s(y + z) \\ &= s(x) + s(y) + s(z) - s(x + y + z) \\ &= s(x + y) + s(z) - s(x + y + z) + s(x) + s(y) - s(x + y) \\ &= g(x + y, z) + g(x, y). \end{aligned}$$

So, for any extension, we can produce a cocycle g. Then g induces a group operation on the set $N \times H$, and one can check that the map $\phi : G \to N \times H$ defined by

$$\phi(g) = (g - (s \circ \pi)(g), \pi(g))$$

is an invertible map of groups.

6. The digit filtration

Let's select $N = H = R_2$ as above. Then we saw that there are two choices for g: we can either pick the constant function $g(h, h') = 0$ (corresponding to a section of $R_2 \times R_2$), or we can pick a nontrivial g given by $g(0, 0) = g(1, 0) = g(0, 1) = 0$, $g(1, 1) = 1$ (corresponding to a section of R_4). This second g actually has an interesting interpretation — to see what it is, let's write out the multiplication table it gives us on the set $R_2 \times R_2$, using the number n for the group element corresponding to n rotations:

+	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(1, 0)	(1, 1)	(0, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(0, 0)	(0, 1)	(1, 0),

compared to the addition table for R_4:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2.

The bright observer will notice that the former looks identical to the binary representation of the second! This is where our explanation for g comes in: g plays the role of the carrying operation that we call learned in the grade school addition algorithm. If g is identically zero, then when we add $(0, 1)$ to $(0, 1)$, the carry that should result from adding the two 1s in base 2 is forgotten, but if we use the twisted g from above, g remembers our carry and moves it over into this new digit. This exact same stuff works in base 10, except there our g looks like

$$g(x, y) = \begin{cases} 0, & x + y \leq 9, \\ 1, & x + y > 9. \end{cases}$$

One quickly checks that g is a cocycle corresponding to the extension R_{100} of R_{10} by R_{10}. Iterating this construction gives R_{1000} as an extension of R_{100} by R_{10}, and so on. This corresponds to the filtration

$$\mathbb{Z} \xrightarrow{10} \mathbb{Z} \xrightarrow{10} \mathbb{Z} \xrightarrow{10} \cdots,$$

which is where our kindergarten mathematics come from.