Motivating Groups

Duncan

3 September 2022

If it's 1882 and your name is Walter Dyck or Heinrich Weber, you might look through the great mathematical works and notice a lot of symmetry. The concept is sprinkled throughout many of the foremost results of the previous century. Gauss's 1827 *Theorema Egrigium* establishes the invariance of a certain property of curved surfaces under certain symmetries of Euclidean space. Galois demonstrated in 1832 the earthshaking fact that for all $n \geq 5$ there is no solution by radicals to polynomials of degree n, through arguments centering on the symmetry of polynomials when their roots are permuted. Number theory and geometry have for millennia had central symmetric properties—the preservation of even numbers under internal addition and the explicit symmetry of regular polygons and polyhedra go back to Pythagoras and Plato.

You might then consider it prudent to make rigorous the vague idea of symmetry from each of these particular contexts, to focus on it *in vacuo*.

Pondering these examples, it's clear that "symmetry" is very intimately connected to "transformation." In each case, one is taking an instance of *thing* and changing it to another instance of *thing*, e.g. mapping one hexagon to another, rotated hexagon. This also suggests some "invariance:" a transformation of a hexagon that adds a side certainly *isn't* a symmetry. Further, if given two symmetries, performing one transformation and then the other transformation ought to be a symmetry in itself (e.g. rotating twice). Additionally, given a symmetry, the transformation that reverses it should also be a symmetry (e.g. rotating back). In summary,

1. Symmetries are transformations.

2. Symmetries preserve the essential character of the mathematical objects on which they act.

3. Symmetries are composable.

4. Symmetries are invertible.

One might then pose, since functions are composable, can be invertible, transform things, and can be restricted in domain and range,

Working Definition. *A "symmetry" of a particular type of mathematical structure is an invertible function $A \to A$ where A is the set of all structures of the given type.*

The first thing you might want to consider in investigating these symmetries is collections of symmetries over a particular structure. In particular, you might ask which collections of symmetries over a structure satisfy all of the informal properties enumerated above themselves. Rotations of a hexagon satisfy all of them, but so do reflections, and so do the union of reflections and rotations.

Working Definition. *A "set of symmetries" G over a set (of structures) A is a subset of the set of invertible maps (bijections) $f : A \to A$ satisfying:*

1. *if $f, g \in G$, then $f \circ g$ is also a symmetry in G (symmetries are composable).*

2. *if f is a symmetry, the map f^{-1} is also a symmetry in G (symmetries are invertible).*

What properties does this necessarily have? Well, the identity function is in every nonempty set of symmetries: there is some $f \in G$, so by (2) $f^{-1} \in G$, and by (1) $f \circ f^{-1} = id_A \in G$. Further, the set of symmetries is associative, since function composition is. This may seem irrelevant for now.

You can chug along with these definitions, but you may notice that most of the very interesting things you prove are about the way symmetries interact, and the proofs use only the properties of the set of symmetries, and rarely the properties of the set A on which the symmetries are functions.

So, you try to suppress A from the definition, and find some mathematical structure that encodes only the formal properties of the set of symmetries. That structure is the group:

Definition. *A group $(G, \circ)$ is a set G together with a function $\circ : G \times G \to G$ such that:*

1. *$(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$,*

2. *There is an element $e \in G$ with the property $e \circ a = a \circ e = a$ for all $a \in G$,*

3. *For each $a \in G$, there is an element $a^{-1} \in G$, called the inverse of a, such that $a \circ a^{-1} = a^{-1} \circ a = e$.*

Elements of G are precisely the functions in the previous working definition. To show this, we demonstrate that we can recover those functions whenever we need an underlying set via the concept of a group action:

Definition. *The action of a group $(G, \circ)$ on a set A, written $G \circlearrowright A$, is a function from $G \times A \to A$ (written $g \cdot a$) such that*

1. *$g_1 \cdot (g_2 \cdot a) = (g_1 \circ g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$,*

2. *$e \cdot a = a$ for all $a \in A$.*

Given any set of symmetries, its definition and the two properties proven immediately after show that the set of symmetries is a group under $\circ$.

We can prove a bunch of abstract theorems about groups; we can use those to get results about the group structure of the set of symmetries.

When we need to introduce the specific context again, we can always get from "group world" back to "set of symmetries" world: given a group action, one can construct a set of symmetries by the set of projection functions $f_g : A \to A$ defined by $a \mapsto g \cdot a$. Each projection has functional inverse $f_{g^{-1}}$ ($gg^{-1} \cdot a = g^{-1}g \cdot a = e \cdot a = a$ for all a), and since g^{-1} is in the group, it is also in the set of projection functions, i.e. each projection is a bijection on A and its inverse is in the set of projection functions. Similarly, given two projection functions f_g and f_h, the projection function f_{gh} is also a projection function since $gh \in G$. It's evident that this inverts the symmetries-to-groups procedure.

The big picture:

> Groups let us study symmetries by themselves.