GROUP THEORY VIA ACTIONS

ANTHONY H. LEE

Abstract. This article is about group theory via their actions, from the perspective of someone who did not enjoy their prior exposure to the theory.

During my undergraduate years, I have taken two courses under the name 'algebra'; one was an introductory course for undergraduate students, and the other was a graduate course. Although my overall understanding of the subject has improved over time, I always found noncommutative groups very unintuitive. It turns out that I wasn't looking at them the right way.

1. Groups are symmetries

Here is the textbook definition of a group:

Definition 1.1. A group $(G, \cdot)$ is a set G together with a binary operation $\cdot : G \times G \to G$ such that

(1) the operation $\cdot$ is associative, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for every $a, b, c \in G$,
(2) there exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$,
(3) for each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

I believe (and hope many agree) that the definition given above does not provide much intuition on how mathematicians actually want to look at groups. The following definition should be closer to the essence of groups:

Definition 1.2. A group is a subset of $\mathrm{Isom}(C)$ for an object C in a category $\mathcal{C}$, endowed with the operation of composing morphisms.

Of course the subset must be taken so that it fits the group axioms, instead of some arbitrary subset. Informally, we can put the definition above as follows:

$$\text{Some group} \longleftrightarrow \text{Symmetries of some object}$$

Let us go through some examples to get a grasp of this perspective. To use our new categorical definition, it will be convenient to work with categories whose morphisms can be concretely understood. As such, we will look at FinSet and $\mathsf{FinDimVect}$.

Example 1.3 (Finite sets)**.** Suppose we have a finite set S of cardinality n. The entirety of $\mathrm{Isom}(S)$ is just S_n, the symmetric group on n letters. Every finite group can be realized as subsets of these groups, by Cayley's theorem.

Date: March 20, 2025.

Now this reformulation itself isn't quite illuminating, but later on we will use our intuition about $\mathsf{FinDimVect}$ on finite groups. This approach is surprisingly insightful.

Example 1.4 (Finite dimensional vector spaces)**.** For the sake of simplicity let us assume that we are working over an algebraically closed field k of characteristic zero. Suppose that V is a k-vector space of dimension n. One can consider the group $\mathrm{GL}(V) := \mathrm{Isom}(V)$, and if we fix a k-basis of V, this can be identified with the familiar matrix group $\mathrm{GL}_n(k)$.

Note, however, that the identification $\varphi_\beta : \mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(k)$ depends heavily on a choice of basis β! This means that if we choose a different basis γ of V, a single element of $\mathrm{GL}(V)$ can be mapped to different elements of $\mathrm{GL}_n(k)$, depending on whether the identification is φ_β or φ_γ. This can be treated using conjugation.

Consider some $T \in \mathrm{GL}(V)$, and a fixed basis β of V. For any other basis γ of V, one can consider the change of basis matrix $U \in \mathrm{GL}_n(k)$ such that $[T]_\gamma = U^{-1}[T]_\beta U$. Using this, we can see that the essence of the group $\mathrm{GL}(V)$ isn't the matrix group $\mathrm{GL}_n(k)$ but rather its conjugacy classes. In this sense, passing a group to the set of its conjugacy classes gets rid of the dependence on coordinates.

Remark 1.5*.* The essence of $\mathrm{GL}(V)$ is captured by the Jordan Canonical Form.

We can apply our observations to finite groups to unveil their essence:

Remark 1.6*.* Conjugacy classes of S_n correspond to possible cycle types.

You can see how this is a 'coordinate free' way of describing S_n; to be precise the essence of S_n does not depend on renaming letters. This is analogous to changing bases in our matrix group example. As such, looking at the conjugacy classes of groups is insightful. We can extend this to the more general notion of group action, where conjugation is a special case of a group acting on itself via conjugation. (In particular, it is a right group action in the sense of matrices.)

2. Group actions

Again, I will first give you the (dull) textbook definition of a group action, and then provide a more insightful definition.

Definition 2.1. A (right) G-action on a set S is a map $\cdot : S \times G \to S$ such that

(1) $s \cdot e = s$ for all $s \in S$,
(2) $(s \cdot g) \cdot h = s \cdot gh$ for all $g, h \in G$.

A left G-action is a right G^{op}-action.

As left and right group actions can be recovered from one another, the distinction between the two is not really important. I have first defined the right group action, as we have seen as an example the matrix group conjugation action $x \mapsto g^{-1}xg$ which is a right action. Moreover, we can compactify this data into the following definition, which is not only more concise but also reveals more of what's actually going on:

Definition 2.2. A G-action on a set S is a group homomorphism $G \to \mathrm{Isom}_{\mathsf{Set}}(S)$.

The motto is that to study properties of a group G, one should study its actions on some set S. In fact, we can extend this definition from Set to $\mathsf{FinDimVect}$, where these group actions are given a special name: group representations. I won't go into the details of representation theory in general, but I will showcase a beautiful application of group actions in finite group theory.

Theorem 2.3 (Sylow I)**.** *Let G be a group such that $|G| = p^n m$, for p a prime not dividing m. Then G has a subgroup of order p^n.*

Proof. We must choose our set S for G to act on carefully; in this case, we let

$$S = \{X \subset G \mid \operatorname{card}(X) = p^n\},$$

namely the set of cardinality p^n subsets of G. We let G act on S by left multiplication. It is obvious that S itself has cardinality $\binom{p^n m}{p^n}$. The idea of the proof is to first argue that the group action of G on S has an orbit whose length is not divisible by p. Well, if every orbit were a multiple of p, then surely $\operatorname{card}(S)$ itself should be a multiple of p. But this is not the case, as

$$\binom{p^n m}{p^n} \equiv m \mod p,$$

which can be seen by evaluating the coefficient of x^{p^n} of the polynomial

$$(x+1)^{p^n m} = (x^{p^n} + 1)^m \in \mathbb{F}_p[x].$$

To proceed, we need a small lemma:

Lemma 2.4 (Orbit-Stabilizer theorem)**.** *Let a group G act on a finite set X. Given $x \in X$, the cardinality of the orbit of x is equal to the index $[G : \operatorname{Stab}(x)]$ of the stabilizer subgroup of x in G.*

Here, $\operatorname{Stab}(x)$ consists of elements of G that fix x, hence the name. We won't prove this lemma as it is quite straightforward. Now back to proving our theorem, pick an orbit O of the G-action on S, and an element $X \in O$. By the Orbit-Stabilizer theorem, we have $\operatorname{card}(O) = [G : \operatorname{Stab}(X)]$. Since the LHS is not divisible by p, we must have that the cardinality of $\operatorname{Stab}(X)$ is divisible by p^n. On the other hand, for an element $x \in X$ the cosets $\operatorname{Stab}(X)$ and $\operatorname{Stab}(X)x$ have the same cardinality, where $\operatorname{Stab}(X)x \subset X$ as by definition we must have $\operatorname{Stab}(X)X = X$. Therefore, the only possible cardinality of $\operatorname{Stab}(X)$ is p^n, and it is a subgroup of G. □