A Group by Any Other Name

Anakin Dey

2024–01–01

Groups are one of the most common structures in all of mathematics. They appear in many fields even outside of algebra such as differential topology and combinatorics, and have applications in areas such as chemistry and computational complexity theory. However, what defines a group, and how much play is there in this definition? First, I'll define a group as you may have seen before.

Definition 1. *A* group *is defined as a set of elements G along with an operation $\cdot$ satisfying the following* axioms*:*

1. Associativity*: For any $x, y, z \in G$, we have that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;*
2. Identity*: There exists an element $e \in G$ which we call the identity such that for any $x \in G$, $e \cdot x = x = x \cdot e$;*
3. Inverse*: For any $x \in G$, there exists $x^{-1} \in G$ such that $x \cdot x^{-1} = e = x^{-1} \cdot x$.*

Writing the $\cdot$ is annoying so from now on I'll adopt the tradition of writing $x \cdot y$ as xy. Similarly, I will use superscripts such as $x^2 = xx$. Although the definition of a group technically only includes a single binary operation $\cdot$ taking two elements of G and producing a new element in G, we often think about inversion of an element, $x \mapsto x^{-1}$, as an operation in its own right.

A Slight Relaxation

If we take a look at the Identity axiom in a group G, we notice that it is two-sided. For any $x \in G$, we have that identity e satisfies $ex = x = xe$. What if we relaxed this to a right-sided version? Define a right-handed version of the Identity axiom where e is the element such that for any $x \in G$, we just have that $xe = x$. In fact, let's do the same for the Inverse axiom as well. It doesn't really make sense to do this for Associativity since that's about three elements being operated on.

Definition 2. *A* right-handed *group is a set R with an operation $\cdot$ such that*

1. Associativity*: Same as in Definition 1;*
2. RH-Identity*: There exists an identity element $e \in G$ such that for any $x \in G$, $xe = x$;*

3. RH-Inverse*: For any $x \in G$, there exists $x^{-1} \in G$ such that $x \cdot x^{-1} = e$.*

Theorem 3. *Every right-handed group R is also a group.*

Proof. Clearly every group is also a right-handed group. So I will not write out that portion of the proof.

Let R be a right-handed group. We need to show that the axioms Associativity, RH-Identity, and RH-Inverse in Definition 2 imply the normal two-sided Identity and Inverse axioms in Definition 1. First we show that any element $a \in R$ satisfying $a^2 = a$ must be the right-handed identity element e. Clearly the identity satisfies this with $e^2 = ee = e$. If a is such an element, then it has a right-inverse a^{-1} where $aa^{-1} = e$. Thus, we have that

$$a = ae = aaa^{-1} = a^2a^{-1} = aa^{-1} = e$$

and $a = e$.

Then, for any element $x \in R$, we know it has a right inverse x^{-1} satisfying $xx^{-1} = e$. Thus, for all $x \in R$ we have that

$$xx^{-1}xx^{-1} = \left(xx^{-1}\right)^2 = e^2 = e = xx^{-1}.$$

Now consider $x^{-1}xx^{-1}x$. We have that

$$\begin{aligned} x^{-1}xx^{-1}x &= x^{-1}\left(xx^{-1}\right)xx^{-1}x \\ &= x^{-1}xx^{-1}xx^{-1}x \\ &= x^{-1}\left(xx^{-1}xx^{-1}\right)x \\ &= x^{-1}\left(xx^{-1}\right)x = x^{-1}x. \end{aligned}$$

But now we have that $x^{-1}xx^{-1}x = x^{-1}x$. By the above, this means that $x^{-1}x = e$ and that x^{-1} is not just a right-handed inverse, but also a left-handed inverse.

Note that nowhere in the above proof did we assume that e was a left-handed identity, just that e is a right-handed identity. We now prove that e is also a left-handed identity. Let $x \in R$. We know that x has a (left and right)-inverse x^{-1} so $x^{-1}x = e = xx^{-1}$. Since $xe = x$, we have that

$$x = xe = xx^{-1}x = ex.$$

Thus, e is also a left-handed identity. Overall we have shown that R satisfies all axioms of a group given in Definition 1 meaning R is a group. □ □

Pretty much the same proof works if you define the analogous left-handed group and want to show that left-handed groups are also equivalent to groups. Thus, there is no distinction between groups and their left or right counterparts. While Definition 2 is different to Definition 1, morally it doesn't feel that different. Can we redefine groups in more interesting ways? It turns out you can! I will show you how groups can be defined in terms of equations (even a single equation), in terms of a new operation, and even in terms of literal abstract nonsense.

Axioms are Equations

One major motivation of studying group theory is studying algebraic equations. Following this motivation, we can formulate groups as satisfying certain equations. This result is not from anywhere in particular and is sort of a folklore result.

Definition 4. *An* equational group *is a set E with elements satisfying the following axioms:*

1. E-Product*: For every element $x, y \in E$ there exists a unique element $xy \in E$;*
2. E-Associativity*: For every $x, y, z \in E$, the equation $a(bc) = (ab)c$ is true;*
3. E-Solution*: For every $x, y \in E$, there exists at least one element a and one element b in E such that the equations $xa = y$ and $bx = y$ are true.*

Theorem 5. *Equational groups are equivalent to groups.*

Proof. Consider a group G. By the definition of product in a group, G satisfies the axiom E-Product. Similarly, multiplication in a group G is associative and so G satisfies the axiom E-Associativity. Finally, let $x, y \in G$. Then $a = x^{-1}y$ and $b = yx^{-1}$, both of which exist since x and y exist, shows that G satisfies the E-Solution. Thus groups are also equational groups.

Now let E be an equational group. Note that the definition of equational group does not explicitly define an operation like in the definition of group (Definition 1). We will give E an operation using axiom E-Product to define $x \cdot y = xy$ for all $x, y \in E$. This is sufficient since E-Product not only says xy exists, but is unique meaning our operation is a well-defined function. This product satisfies the axiom Associativity of a group since we have the axiom E-Associativity.

We want to show that certain elements, identities and inverses, exist. These elements satisfy certain equations as defined, so we should use the axiom E-Solution. To show that the identity element exists, let $x, y \in E$. Then by E-Solution, there exists left and right identity elements a and b such that $xa = x$ and $by = y$. Similarly, there exists elements a' and b' such that $ya' = a$ and $b'x = b$. Thus

$$b = b'x = b'xa = ba = bya' = ya'a.$$

Thus, $a = b$ is our multiplicative identity element, which we will now call e. This is the identity element for all of E since x and y were arbitrary. The intutition for this proof occurs in the middle, with ba, reflecting that $e^2 = e$. We saw this in the proof of Theorem 3.

To see that inverses exist, we immediately have by E-Solution that for $x \in E$, there exists elements a and b such that $xa = e = bx$. Thus we have that

$$b = be = bxa = ea = a.$$

Thus, left and right inverses for each element in E exist and are equivalent yielding that every element in E has an inverse $x^{-1} = a = b$. Again the intuition here is that $x^{-1}xx^{-1} = x$ by grouping with parentheses either the left two elements or the right two elements. Overall we have that groups are equivalent to equational groups. □ □

. . . is Multiplication is Division is Multiplication is Division is . . .

Typically, the definition of the binary operation $\cdot : G \times G \to G$ for a group is thought of in a multiplicative manner: combine two elements x and y to get a new one xy. But can we define groups a divisive manner: tearing y off of x and getting an element z representing whatever is leftover? Since we have notions of both multiplication and inversion in our normal definition (Definition 1) of a group, we can indeed do this. I found this definition during my research for this post from this MathOverflow post.

Definition 6. *A* Division Group *is a set D along with an operation $/$ satisfying*

1. D-Inversion*: There exists a unique element $e \in D$ such that for all $x \in D$, we have that $x/x = e$;*
2. D-Identity*: For all $x \in D$ and the element e, we have that $x/e = x$;*
3. D-Cancellation*: For any $x, y, z \in D$, We have that $(x/z)/(y/z) = x/y$.*

Theorem 7. *Division groups are equivalent to groups.*

Proof. Showing that a group is a division group is simple. Intuitively, division is just multiplication by the inverse and so we can take all of the axioms of Definition 6 and replace x/y with xy^{-1} and see that the group axioms imply the division group axioms.

Now suppose we have a division group D. We first need to translate from $/$ to the operations multiplication and inversion. Let $xy = x/(e/y)$ and $x^{-1} = e/x$ for all $x, y \in D$. Then we also claim that our multiplicative identity is $e \in D$. Then all that is left is to check that the axioms in Definition 1 are satisfied by this translation. These are all just computations of various levels of tedium and juggling of parentheses. Let $x, y, z \in D$. For associativity we have

$$\begin{aligned}
(xy)z &= (x/(e/y))/(e/z) && \text{(Translation)}\\
&= (x/(e/y))/((e/z)/e) && \text{(D-Identity)}\\
&= (x/(e/y))/(((e/z)/y)/(e/y)) && \text{(D-Cancellation)}\\
&= x/((e/z)/y) && \text{(D-Cancellation)}\\
&= x/(((e/z)/(e/z))/(y/(e/z))) && \text{(D-Cancellation)}\\
&= x/(e/(y/(e/z))) && \text{(D-Inversion)}\\
&= x(yz). && \text{(Translation)}
\end{aligned}$$

Fortunately, proving identity and existence of inversion is simpler:

$$ex = e/(e/x) = (x/x)/(e/x) = x/e = x = x/e = x/(e/e) = xe$$

$$xx^{-1} = x/(e/(e/x)) = x/((x/x)/(e/x)) = x/(x/e) = x/x = x = (e/x)/(e/x) = x^{-1}x.$$

Thus, division groups are equivalent to groups. □

An ever-so-slightly shorter proof would have been proving directly that division groups are equivalent to right-handed groups and then invoking the fact that right-handed groups are equivalent to groups.

One Law to Rule Them All

There is a way to combine ideas from the previous two notions and use a single equation to define what a group is using division. This is due to Graham Higman and B.H. Neumann in their paper *Groups as groupoids with one law*. However, I will build off of an easier to understand exposition from Neumann's paper *Another Single Law for Groups*. First a primer on *reverse Polish notation*. This notation is common in the early study of these axiomatic systems, and so I will use it here. It is a way of writing functions and their inputs without parentheses. If we wanted to notate the multiplication of two numbers x and y, rather than writing $x \cdot y$ in what is called *infix notation*, we would write $xy\cdot$ for reverse Polish notation. If you know how many arguments your functions take, then this removes the need for parentheses.

In a group, $x/y = xy^{-1}$ where the operation right division / is from Definition 6. Here we are using that division groups are equivalent to groups (Theorem 7). We will notate right division, multiplication, and inversion in reverse Polish notation with the letters ρ, μ, and ι:

$$xy\rho = x/y, \qquad xy\mu = x \cdot y, \qquad x\iota = x^{-1}.$$

Verify for yourself that the following identities hold.

$$x\iota = xx\rho x\rho, \qquad xy\mu = xyy\rho y\rho\rho.$$

It will be easier to see if you notice that $e = xx\rho$ and use some parentheses.

Now imagine a set G with the operation right division ρ, outside of all context of inversion and multiplication. Then we have the following theorem which is the main result from Graham Higman and B.H. Neumann's work:

Theorem 8. *A set G with right division ρ satisfying the following for all $x, y, z \in G$ is a group:*

$$xxx\rho y\rho z\rho xx\rho x\rho z\rho\rho\rho = y.$$

I will omit the proof because it is far far too long to repeat.

Abstract Nonsense

Category theory, also known as abstract nonsense by many, is a powerful framework for understanding various structures. A category is a collection of objects and functions, called morphisms, between these objects. Formally, little other structures exists:

Definition 9. *A category $\boldsymbol{C}$ is a collection of objects $\mathrm{ob}(\boldsymbol{C})$ and morphisms $\hom(\boldsymbol{C})$ between these objects. If we have objects $A, B \in \mathrm{ob}(\boldsymbol{C})$, a morphism f from A to B is denoted $f\colon A \to B$. Intuitively morphisms are functions, but they don't have to be! We also have an operation $\circ$ called composition where if $f\colon A \to B$ and $g\colon B \to C$ are morphisms, then we have a morphism $g \circ f\colon A \to B$ where we apply the morphism g after f. This composition is associative, meaning that if we also have a morphism $h\colon C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$. We also require that a special identity morphism id_A exists for every object $A \in \mathrm{ob}(\boldsymbol{C})$ such that $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$ for every morphism $f\colon A \to B$.*

This definition is somewhat reminiscent of a group! For example, the proof that the identity morphism in a category is unique for each object is very much the same as the proof that the identity in a group is unique. Consider a group G and an element $x \in G$. Then we have a group homomorphism called left multiplication by x:

$$\begin{aligned} L_x\colon G &\to G \\ g &\mapsto xg \end{aligned}$$

Right multiplication by x is defined in the way you expect.

This allows us to view a single group in a category-theoretic manner. Fix your favorite group G. Consider the not-yet-proven-to-be-category $\mathbf{G}$ where the only object is G, so $\mathrm{ob}(\mathbf{G}) = \{G\}$. Then let $\hom(\mathbf{G})$ be all left-multiplications and right-multiplications in G. So $\hom(\mathbf{G})$ is the set of all $L_x\colon G \to G$ and $R_x\colon G \to G$ for all $x \in G$. I claim that $\mathbf{G}$ is a category.

Composition of morphisms is just multiplication by two (or more) elements at once rather than just one element. For any elements $x, y \in G$ we have $L_x \circ L_y = L_{xy}$ and $R_x \circ R_y = R_{yx}$. Associativity of composition then follows from the fact that multiplication in a group is associative. As one may expect, we have that the identity morphism for G, id_G, is $L_e = R_e$. Indeed, composing with L_e before or after L_x for any $x \in G$ yields L_x and similarly for R_x. Thus, we have a category.

Notice, however, that we did not use the fact that every element $x \in G$ has an inverse x^{-1}. We have that $L_x \circ L_{x^{-1}} = L_e = R_x \circ R_{x^{-1}}$. Thus, every one of our morphisms in $\mathbf{G}$ is an *isomorphism*: every morphism has an inverse. Let us take the definition of a category (Definition 9) and add the requirement that inverses exist.

Definition 10. *A category $\boldsymbol{G}$ where for every morphism $f\colon A \to B$, there exists a morphism $f^{-1}\colon B \to A$ such that $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$ is called a groupoid.*

Above we have defined a group as a groupoid with one object.

In fact, we can use this to construct groups, rather than just identifying groups as groupoids. Lets construct a new groupoid $\mathbf{S}_n$. If we let our single object be $\mathrm{ob}(\mathbf{S}_n) = \{\ [n]\ \} = \{\ \{1, \ldots, n\}\ \}$ and let $\hom(\mathbf{S}_n)$ be all possible permutation of $[n]$ then we have constructed the symmetric group on n elements, S_n, as a groupoid. If you know a little algebraic topology, then you can also construct the fundamental group of a topological space X with a fixed base point $x \in X$ by considering your morphisms as the classes of loops $x \to x$. Groupoids in general are cool objects which nicely generalize properties of groups, but perhaps I'll discuss that another day.

View this as a webpage.