Lecture 1.6: The formal definion of a group

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Moving towards the standard definition of a group

We have been calling the members that make up a group "actions" because our definition requires a group to be a collection of actions that satisfy our 4 rules.

Since the standard definition of a group is not phrased in terms of actions, we will need more general terminology.

We will call the members of a group elements. In general, a group is a set of elements satisfying some set of properties.

We will also use standard set theory notation. For example, we will write things like

$$h \in V_4$$

to mean "h is an element of the group V_4."

Binary operations

Intuitively, an operation is a method for combining objects. For example, $+$, $-$, $\cdot$, and $\div$ are all examples of operations. In fact, these are binary operations because they combine two objects into a single object.

Definition

If $*$ is a binary operation on a set S, then $s * t \in S$ for all $s, t \in S$. In this case, we say that S is closed under the operation $*$.

Combining, or "multiplying" two group elements (i.e., doing one action followed by the other) is a binary operation. We say that it is a binary operation *on* the group.

Recall that Rule 4 says that any sequence of actions is an action. This ensures that the group is closed under the binary operation of multiplication.

Multiplication tables are nice because they depict the group's binary operation in full.

However, not every table with symbols in it is going to be the multiplication table for a group.

Associativity

Recall that an operation is associative if parentheses are permitted anywhere, but required nowhere.

For example, ordinary addition and multiplication are associative. However, subtraction of integers is *not* associative:

$$4 - (1 - 2) \neq (4 - 1) - 2.$$

Is the operation of combining actions in a group associative? YES! We will not prove this fact, but rather illustrate it with an example.

Recall D_3, the group of symmetries for the equilateral triangle, generated by r (=rotate) and f (=horizontal flip).

How do the following compare?

$$rfr, \qquad (rf)r, \qquad r(fr)$$

Even though we are associating differently, the end result is that *the actions are applied left to right*.

The moral is that we never need parentheses when working with groups, though we may use them to draw our attention to a particular chunk in a sequence.

Classical definition of a group

We are now ready to state the standard definition of a group.

Definition (official)

A set G is a group if the following criteria are satisfied:

1. There is a binary operation $*$ on G.
2. $*$ is associative.
3. There is an identity element $e \in G$. That is, $e * g = g = g * e$ for all $g \in G$.
4. Every element $g \in G$ has an inverse, g^{-1}, satisfying $g * g^{-1} = e = g^{-1} * g$.

Remarks

- Depending on context, the binary operation may be denoted by $*$, $\cdot$, $+$, or $\circ$.
- As with ordinary multiplication, we frequently omit the symbol altogether and write, e.g., xy for $x * y$.
- We generally only use the $+$ symbol if the group is abelian. Thus, $g + h = h + g$ (always), but in general, $gh \neq hg$.
- Uniqueness of the identity and inverses is *not* built into the definition of a group. However, we can without much trouble, prove these properties.

Definitions of a group: Old vs. New

Do our two competing definitions agree? That is, if our informal definition says something is a group, will our official definition agree? Or vice versa?

Since our first definition of a group was informal, it is impossible to answer this question officially and absolutely. An informal definition potentially allows some technicalities and ambiguities.

This aside, our discussion leading up to our official Definition provides an informal argument for why the answer to the first question should be yes. We will answer the second question in the next chapter.

Regardless of whether the definitions agree, we always have $e^{-1} = e$. That is, the inverse of doing nothing is doing nothing.

Even though we haven't officially shown that the two definitions agree (and in some sense, we can't), we shall begin viewing groups from these two different paradigms:

- a group as a collection of actions;
- a group as a set with a binary operation.

A few simple properties

One of the first things we can prove about groups is uniqueness of the identity and inverses.

Theorem

Every element of a group has a *unique* inverse.

Proof

Let g be an element of a group G. By definition, it has at least one inverse.

Suppose that h and k are both inverses of g. This means that $gh = hg = e$ and $gk = kg = e$. It suffices to show that $h = k$. Indeed,

$$h = he = h(gk) = (hg)k = ek = k\,,$$

and the proof is complete. □

The following proof is relegated to the homework; the technique is similar.

Theorem

Every group has a *unique* identity element.