Notes on Group Theory

Blake Stacey

March 27, 2007

Chapter 1

Introduction

These notes cover the topics covered in the Science After Sunclipse seminar series on group theory and related topics, led by Ben Allen, Eric Downes and Blake Stacey in the early months of 2007. The mailing list for the seminar is `diyu@mit.edu` (as in Do-It-Yourself University).

The introductory topics covered in this chapter come from the session led by Ben Allen at Boston University, the evening of 26 March 2007.

Begin with a set, S, and consider the functions of the set to itself, $f : S \to S$. What can we say about the set of all such maps f? First, we can compose any two maps, $f \circ g$. This composition will obey an associative rule,

$$(f \circ g) \circ h = f \circ (g \circ h), \tag{1.1}$$

and we note the special importance of the *identity map,*

$$e : S \to S, \text{ such that } e(x) = x \ \forall\ x \in S. \tag{1.2}$$

The identity e obeys the rule,

$$e \circ f = f \circ e = f \ \forall\ f. \tag{1.3}$$

If we have $f : S \to S$, under what circumstances will there exist $g : S \to S$ such that $f \circ g = e$? It is not hard to deduce that if f is *one-to-one,* then g exists; we call such a g the *inverse* of f, written f^{-1}.

Definition 1.0.1. A *group* is a set G with a binary operation $(\cdot)$ satisfying the following properties:

- Associativity:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c). \tag{1.4}$$

- Identity:
$$\exists e \text{ such that } a \cdot e = e \cdot a = a. \tag{1.5}$$

- Inverses:
$$\forall\ a \in G,\ \exists a^{-1} \text{ such that } a \cdot a^{-1} = a^{-1} \cdot a = e. \tag{1.6}$$

The set $\{f\}$ of all functions from S to itself is a group if the inverse condition is satisfied, *i.e.,* if the functions are one-to-one. In situations where our set of interest satisfies some but not all of the group properties, we have different names. A set with an operation which satisfies *associativity* and the *identity condition* but not the inverse condition is called a *monoid,* while a set with an operation satisfying *only associativity* is called a *semigroup.*

Keeping these ideas in mind, we would like to generalize a bit. Given a set S, let's look at all maps $f : S \to S$ which preserve the "structure" of S. For example, consider a pentagon with vertices labeled 1 through 5. What is the "structure" of this set, and what maps preserve it?

The point of this example is that *many valid answers* to those questions exist. We can map vertices from one to another, like so:

$$\{1,2,3,4,5\} \to \{1,2,3,4,5\}, \tag{1.7}$$

changing the order as we desire,

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} \to \begin{pmatrix} 1 \\ 2 \\ 4 \\ 3 \\ 5 \end{pmatrix}. \tag{1.8}$$

These permutations have inverses, clearly enough, and it is easy to conceive the identity operation. Because the permutations are one-to-one, the set of all permutations constitutes a group. For any possible ending configuration — of which there are $5! = 120$ — we can write a one-to-one function taking the initial configuration into that ending state. Therefore, we have a group with 120 elements; we call this particular group the *symmetric group* S_5.

What happens if we mandate that the permutations must preserve the left- and right-hand neighbors of each vertex? When this is our "structure", we arrive at the *cyclic group* of order 5, the group consisting of the five possible rotations. We write this as Z_5.

It is interesting to note that Z_5 is commutative (or *abelian*) while S_5 is not. One way we can think about this is that Z_5 has only one *generator,* the action of rotating by one step in a certain direction. We can build up each member of the group by composing multiple copies of this generator, r, so that our group looks like this:

$$\{r, r^2, r^3, r^4, r^5 = e\}. \tag{1.9}$$

Whenever we have associativity, we can say that

$$r^a r^b = r^{a+b}, \tag{1.10}$$

where we here have the added proviso

$$r^5 = r^0 = e. \tag{1.11}$$

We have blundered our way into modular arithmetic!

Quick Calculation 1.0.1. Convince yourself that S_5 is not commutative.

Discuss 1.0.2. Given the set $S = \{1,2,3\}$, what are the groups of functions from S to itself? Are they abelian, cyclic, symmetric?

Let us briefly note what happens when we abandon the rigid requirement that left neighbors become left neighbors — relaxing our concern for chirality and allowing *reflections* as well as rotations. Here we're dealing with *two* generators, one for rotation (which we had before) and one for reflection. Call the former r and the latter s. Note that we can reflect a pentagon in many ways: right-to-left on a page, for example, or taking the mirror image in a verticle line. Geometric intuition tells us that these images are identical *up to a rotation.*

We now introduce a standard notation for group presentation:

$$\langle r, s | r^5 = e, s^2 = e, r^a s = s r^{5-a} \rangle. \tag{1.12}$$

This is one of the more rigorous ways of writing out a group. If we have any "word" made of r and s, we can apply the relations among r, s and e to find equivalent words.

How big is this *dihedral group*? The intuitive answer is the product of the sizes of the two groups, or ten.

Discuss 1.0.3. What is the role of the last equivalence relation in Eq. (1.12), $r^a s = s r^{5-a}$?

To wrap up for today and lay the groundwork for next time, consider what happens when $S = \mathbb{R}^2$. What are the different structures of interest which mappings $f : \mathbb{R}^2 \to \mathbb{R}^2$ can preserve? Brainstorm:

- Distances

- Angles
- Areas
- Topology (continuous transforms)
- Linear structure (linear transforms)
- Orientation and chirality