Lecture 3.1: Subgroups

Matthew Macauley

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

Math 4120, Modern Algebra

Overview

In this chapter we will introduce the concept of a subgroup and begin exploring some of the rich mathematical territory that this concept opens up for us.

A subgroup is some smaller group living inside a larger group.

Before we embark on this leg of our journey, we must return to an important property of Cayley diagrams that we've mentioned, but haven't analyzed in depth.

This feature, called *regularity*, will help us visualize the new concepts that we will introduce.

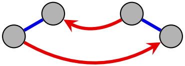
Let's begin with an example.

Regularity

Consider the group D_3. It is easy to verify that $frf = r^{-1}$.

Thus, starting at *any* node in the Cayley diagram, the path frf will *always* lead to the same node as the path r^{-1}.

That is, the following fragment permeates throughout the diagram.



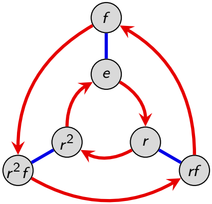
Observe that equivalently, this is the same as saying that the path $frfr$ will always bring you back to where you started. (Because $frfr = e$).

Key observation

The algebraic relations of a group, like $frf = r^{-1}$, give Cayley diagrams a uniform symmetry – every part of the diagram is structured like every other.

Regularity

Let's look at the Cayley diagram for D_3:



Check that indeed, $frf = r^{-1}$ holds by following the corresponding paths starting at any of the six nodes.

There are other patterns that permeate this diagram, as well. Do you see any?

Here are a couple: $f^2 = e$, $r^3 = e$.

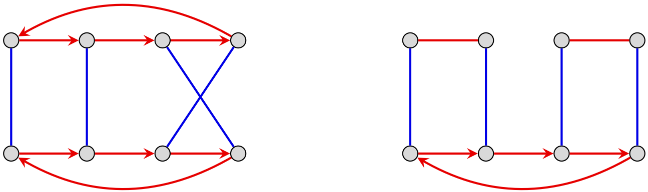
Definition

A diagram is called regular if it repeats every one of its interval patterns throughout the whole diagram, in the sense described above.

Regularity

Every Cayley diagram is regular. In particular, diagrams lacking regularity do *not* represent groups (and so they are not called Cayley diagrams).

Here are two diagrams that *cannot* be the Cayley diagram for a group because they are not regular.



Recall that our original definition of a group was informal and "unofficial."

One reason for this is that technically, regularity needs to be incorporated in the rules. Otherwise, the previous diagram would describe a group of actions.

We've indirectly discussed the regularity property of Cayley diagrams, and it was implied, but we haven't spelled out the details until now.

Subgroups

Definition

When one group is contained in another, the smaller group is called a subgroup of the larger group. If H is a subgroup of G, we write $H < G$ or $H \leq G$.

All of the orbits that we saw in Chapter 5 are subgroups. Moreover, they are *cyclic* subgroups. (Why?)

For example, the orbit of r in D_3 is a subgroup of order 3 living inside D_3. We can write

$$\langle r \rangle = \{e, r, r^2\} < D_3.$$

In fact, since $\langle r \rangle$ is really just a copy of C_3, we may be less formal and write

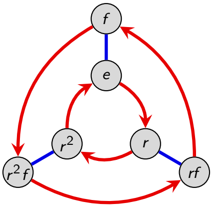
$$C_3 < D_3.$$

An example: D_3

Recall that the orbits of D_3 are

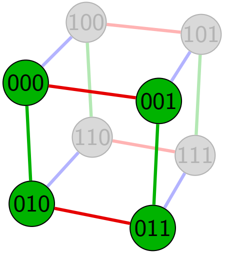
$$\langle e\rangle=\{e\},\qquad \langle r\rangle=\langle r^2\rangle=\{e,r,r^2\},\qquad \langle f\rangle=\{e,f\}$$
$$\langle rf\rangle=\{e,rf\},\qquad \langle r^2f\rangle=\{e,r^2f\}\,.$$

The orbits corresponding to the generators are staring at us in the Cayley diagram. The others are more hidden.



It turns out that all of the subgroups of D_3 are just (cyclic) orbits, but there are many groups that have subgroups that are not cyclic.

Another example: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$



Here is the Cayley diagram for the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (the "three-light switch group").

A copy of the subgroup V_4 is highlighted.

The group V_4 requires at least two generators and hence is *not* a cyclic subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. In this case, we can write

$$\langle 001, 010 \rangle = \{000, 001, 010, 011\} < \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Every (nontrivial) group G has *at least* two subgroups:

1. the trivial subgroup: $\{e\}$
2. the non-proper subgroup: G. (Every group is a subgroup of itself.)

Question

Which groups have *only* these two subgroups?

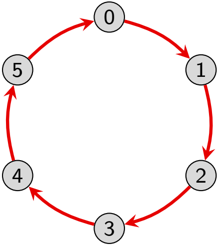
Yet one more example: $\mathbb{Z}_6$

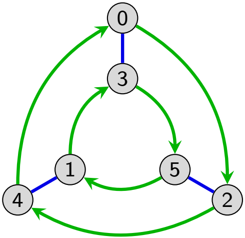
It is not difficult to see that the subgroups of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ are

$$\{0\}, \qquad \langle 2 \rangle = \{0, 2, 4\}, \qquad \langle 3 \rangle = \{0, 3\}, \qquad \langle 1 \rangle = \mathbb{Z}_6.$$

Depending our choice of generators and layout of the Cayley diagram, not all of these subgroups may be "visually obvious."

Here are two Cayley diagrams for $\mathbb{Z}_6$, one generated by $\langle 1 \rangle$ and the other by $\langle 2, 3 \rangle$:





One last example: D_4

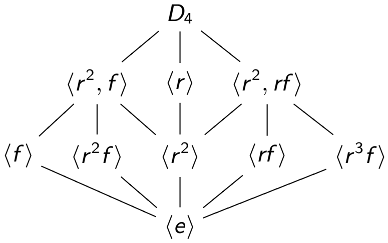
The dihedral group D_4 has 10 subgroups, though some of these are isomorphic to each other:

$$\{e\}, \underbrace{\langle r^2\rangle, \langle f\rangle, \langle rf\rangle, \langle r^2 f\rangle, \langle r^3 f\rangle}_{\text{order 2}}, \underbrace{\langle r\rangle, \langle r^2, f\rangle, \langle r^2, rf\rangle}_{\text{order 4}}, D_4.$$

Remark

We can arrange the subgroups in a diagram called a subgroup lattice that shows which subgroups contain other subgroups. This is best seen by an example.

The subgroup lattice of D_4:



A (terrible) way to find all subgroups

Here is a brute-force method for finding all subgroups of a given group G of order n.

Though this algorithm is horribly inefficient, it makes a good thought exercise.

0. we always have $\{e\}$ and G as subgroups
1. find all subgroups generated by a single element ("cyclic subgroups")
2. find all subgroups generated by 2 elements

$$\vdots$$

n-1. find all subgroups generated by $n-1$ elements

Along the way, we will certainly duplicate subgroups; one reason why this is so inefficient and impractible.

This algorithm works because every group (and subgroup) has a set of generators.

Soon, we will see how a result known as Lagrange's theorem greatly narrows down the possibilities for subgroups.