Lecture 2.1: Cyclic and abelian groups

Matthew Macauley

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

Math 4120, Modern Algebra

Overview

In this series of lectures, we will introduce 5 families of groups:

1. cyclic groups
2. abelian groups
3. dihedral groups
4. symmetric groups
5. alternating groups

Along the way, a variety of new concepts will arise, as well as some new visualization techniques.

We will study permutations, how to write them concisely in cycle notation. Cayley's theorem tells us that every finite group is isomorphic to a collection of permutations.

This lecture is focused on the first two of these families: cyclic groups and abelian groups.

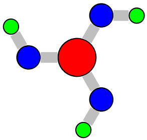
Informally, a group is cyclic if it is generated by a single element. It is abelian if multiplication commutes.

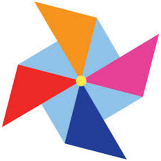
Cyclic groups

Definition

A group is cyclic if it can be generated by a single element.

Finite cyclic groups describe the symmetry of objects that have *only* rotational symmetry. Here are some examples of such objects.





An obvious choice of generator would be: *counterclockwise rotation by* $2\pi/n$ (called a "click"), where n is the number of "arms." This leads to the following presentation:

$$C_n = \langle r \mid r^n = e \rangle .$$

Remark

This is not the only choice of generator; but it's a natural one. Can you think of another choice of generator? Would this change the group presentation?

Cyclic groups

Definition

The order of a group G is the number of distinct elements in G, denoted by $|G|$.

The cyclic group of order n (i.e., n rotations) is denoted C_n (or sometimes by $\mathbb{Z}_n$).

For example, the group of symmetries for the objects on the previous slide are C_3 (boric acid), C_4 (pinwheel), and C_{10} (chilies).

Comment

The alternative notation $\mathbb{Z}_n$ comes from the fact that the binary operation for C_n is just modular addition. To add two numbers in $\mathbb{Z}_n$, add them as integers, divide by n, and take the remainder.

For example, in $\mathbb{Z}_6$: $\quad 3+5 \equiv_6 2$. "3 clicks + 5 clicks = 2 clicks". (If the context is clear, we may even write $3+5=2$.)

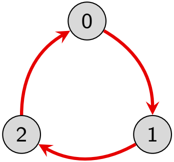
Cyclic groups, additively

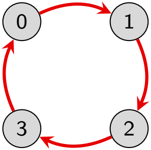
A common way to write elements in a cyclic group is with the integers $0, 1, 2, \ldots, n-1$, where

- 0 is the identity
- 1 is the single counterclockwise "click".

Observe that the set $\{0, 1, \ldots, n-1\}$ is closed under addition modulo n. That is, if we add (mod n) any two numbers in this set, the result is another member of the set.

Here are some Cayley diagrams of cyclic groups, using the canonical generator of 1.





Summary

In this setting, the cyclic group consists of the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under the binary operation of $+$ (modulo n). The (additive) identity is 0.

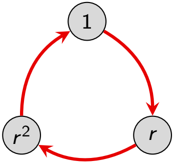
Cyclic groups, multiplicatively

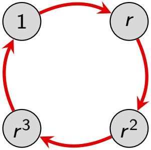
Here's another natural choice of *notation* for cyclic groups. If r is a generator (e.g., a rotation by $2\pi/n$), then we can denote the n elements by

$$1, r, r^2, \dots, r^{n-1}.$$

Think of r as the complex number $e^{2\pi i/n}$, with the group operation being *multiplication!*

Note that $r^n = 1$, $r^{n+1} = r$, $r^{n+2} = r^2$, etc. Can you see modular addition rearing its head again? Here are some Cayley diagrams, using the canonical generator of r.





Summary

In this setting, the cyclic group can be thought of as the set $C_n = \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\}$ under the binary operation of $\times$. The (multiplicative) identity is 1.

More on cyclic groups

One of our notations for cyclic groups is "additive" and the other is "multiplicative." This doesn't change the actual group; only our choice of notation.

Remark

The (unique) infinite cyclic group (additively) is $(\mathbb{Z}, +)$, the integers under addition. Using multiplicative notation, the infinite cyclic group is

$$G = \langle r \mid \quad \rangle = \{r^k : k \in \mathbb{Z}\}.$$

For the infinite cyclic group $(\mathbb{Z}, +)$, only 1 or -1 can be generators. (Unless we use multiple generators, which is usually pointless.)

Proposition

Any number from $\{0, 1, \dots, n-1\}$ that is relatively prime to n will generate $\mathbb{Z}_n$.

For example, 1 and 5 generate $\mathbb{Z}_6$, while $1, 2, 3$, and 4 all generate $\mathbb{Z}_5$. i.e.,

$$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle\,, \qquad\qquad \mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle\,.$$

Note that the above notation isn't a presentation, it just means "generated by."

More on cyclic groups

Modular addition has a nice visual appearance in the multiplication tables of cyclic groups.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

There are many things worth commenting on, but one of the most important properties of the multiplication tables for cyclic groups is the following:

Observation

If the headings on the multiplication table are arranged in the "natural" order $(0, 1, 2, \dots n-1)$ or $(e, r, r^2, \dots r^{n-1})$, then each row is a cyclic shift to the left of the row above it.

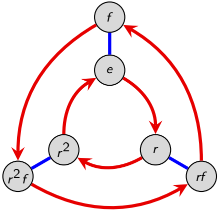
Do you see *why* this happens?

Orbits

We started our discussion with cyclic groups because of their simplicity, but also because they play a fundamental role in more complicated groups.

Before continuing our exploration into the 5 families, let's observe how cyclic groups "fit" into other groups.

Consider the Cayley diagram for D_3:



Do you see any copies of the Cayley diagram for any cyclic groups in this picture?

Starting at e, the red arrows lead in a length-3 cycle around the inside of the diagram. We refer to this cycle as the orbit of the element r.

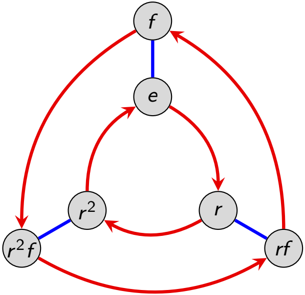
The blue arrows lead in a length-2 cycle – the orbit of f.

Orbits are usually written with braces. In this case, the orbit of r is $\{e, r, r^2\}$, and the orbit of f is $\{e, f\}$.

Orbits

Every element in a group traces out an orbit. Some of these may not be obvious from the Cayley diagram, but they are there nonetheless.

Let's work out the orbits for the remaining elements of D_3.



element	orbit
e	$\{e\}$
r	$\{e, r, r^2\}$
r^2	$\{e, r^2, r\}$
f	$\{e, f\}$
rf	$\{e, rf\}$
r^2f	$\{e, r^2f\}$

Note that there are 5 *distinct* orbits. The elements r and r^2 have the same orbit.

Orbits

Definition

The order of an element $g \in G$, denoted $|g|$, is the size of its orbit. That is, $|g| := |\langle g \rangle|$. (Recall that the order of G is defined to be $|G|$.)

Note that in any group, the orbit of e will simply be $\{e\}$.

In general, the orbit of an element g is the set

$$\langle g \rangle := \{g^k : k \in \mathbb{Z}\}.$$

This set is not necessarily infinite, as we've seen with the finite cyclic groups.

We allow negative exponents, though this only matters in infinite groups.

One way of thinking about this is that the orbit of an element g is the collection of elements that you can get to by doing g or its inverse any number of times.

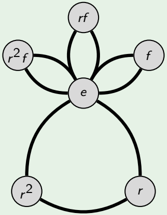
Remark

In *any* group G, the orbit of an element $g \in G$ is a cyclic group that "sits inside" G. This is an example of a subgroup, which we will study in more detail later.

Visualizing the orbits of a groups using "cycle graphs"

Example: Cycle graph of D_3

element	orbit
e	$\{e\}$
r	$\{e, r, r^2\}$
r^2	$\{e, r^2, r\}$
f	$\{e, f\}$
rf	$\{e, rf\}$
r^2f	$\{e, r^2f\}$



Comments

- In a cycle graph (also called an orbit graph), each cycle represents an orbit.
- The convention is that orbits that are subsets of larger orbits are only shown within the larger orbit.
- We don't color or put arrows on the edges of the cycles, because one orbit could have multiple generators.
- Intersections of cycles show what elements they have in common.
- What do the cycle graphs of cyclic groups look like? (*Answer*: a single cycle.)

Abelian groups

Recall that a group is abelian (named after Neils Abel) if the order of actions is irrelevant (i.e., the actions *commute*). Here is the formal mathematical definition.

Definition

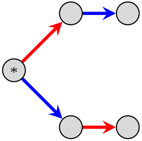
A group G is abelian if $ab = ba$ for all $a, b \in G$.

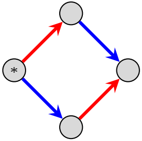
Abelian groups are sometimes referred to as commutative.

Remark

To check that a group G is abeliean, it suffices to only check that $ab = ba$ for all pairs of generators of G. (*Why?*)

The pattern on the left *never* appears in the Cayley graph for an abelian group, whereas the pattern on the right illustrates the relation $ab = ba$:





Examples

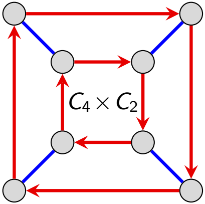
Cyclic groups are abelian.

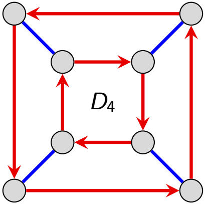
Reason 1: The left configuration on the previous slide can never occur (since there is only one generator).

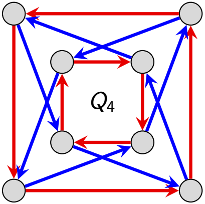
Reason 2: In the cyclic group $\langle r \rangle$, every element can be written as r^k for some k. Clearly, $r^k r^m = r^m r^k$ for all k and m.

Note that the converse fails: if a group is abelian, it need not be cyclic. (Take V_4 as an example.)

Let's explore a little further. The following are Cayley diagrams for three groups of order 8.





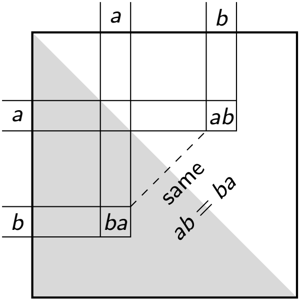


Are any of these groups abelian?

Multiplication tables of abelian groups

Abelian groups are easy to spot if you look at their multiplication tables.

The property "$ab = ba$ for all a and b" means that the table must be symmetric across the main diagonal.



	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3