Math 3230 Abstract Algebra I
Sec 2.1: Cyclic and abelian groups, orbits

Slides created by M. Macauley, Clemson (Modified by E. Gunawan, UConn)

http://egunawan.github.io/algebra

Abstract Algebra I

Overview

In Section 2, we will discuss 5 famous families of groups

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

as well as new concepts and visualization techniques.

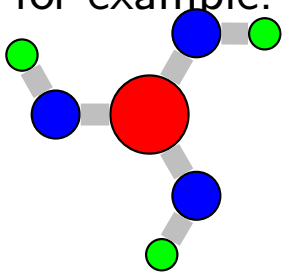
Motivation: Cayley's theorem says that every finite group is isomorphic to a collection of permutations (i.e., a subgroup of a symmetric group).

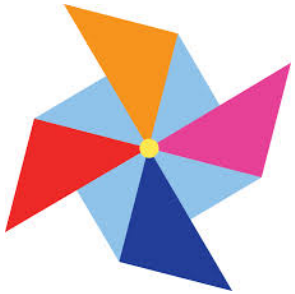
Cyclic groups

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, for example:





A possible generator is *counterclockwise rotation by* $2\pi/n$, where n is the number of "arms." This leads to the group presentation $C_n = \langle r \mid r^n = e \rangle$.

Remark

The rotation by $2\pi/n$ is not the only choice of generator.
(1) Can you think of another choice of generator?

(2) Would this change the group presentation? It depends. For example, $C_{10} = \langle a, b | a^2 = e, b^5 = 2, ab = ba \rangle$ if we let $a = r^5$ and $b = r^2$.

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 $\mathbb{Z}_n$).

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 $\mathbb{Z}_6$: $3 + 5 \equiv 2 \mod 6$. "3 clicks plus 5 clicks are equal to 2 clicks". (If the context is clear, we may write $[3] + [5] = [2]$ or $3 + 5 = 2$.)

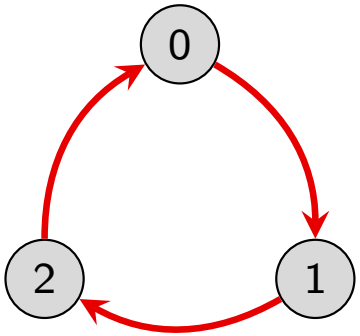
Cyclic groups, as additive groups

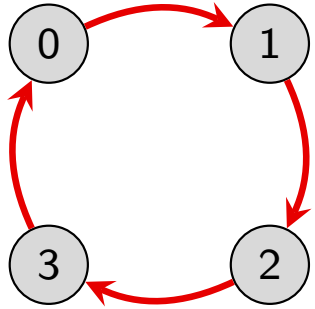
A common way to write elements in a cyclic group is with the integers $0, 1, 2, \ldots, n-1$, where

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

Note: 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, as multiplicative groups

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

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

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

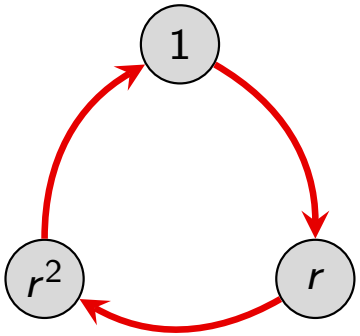
Cyclic groups, as multiplicative groups

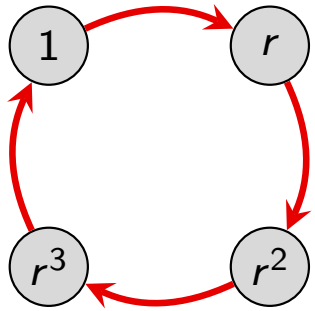
Here's another natural choice of *notation* for cyclic groups. If r is a generator (e.g., a rotation by $2\pi/n$), then we can denote the n elements by

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

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. Do you notice modular addition 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 $(\mathbb{Z}, +)$, only 1 or -1 can be a generator if we insist on only one generators. There are many possible minimal generators if we allow multiple generators.

Proposition

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

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

$$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle, \quad \mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle, \quad \mathbb{Z}_9 = \langle 1 \rangle = \langle \ \rangle = \langle \ \rangle = \langle \ \rangle = \langle \ \rangle = \langle \ \rangle$$

Recall 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

Observation

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

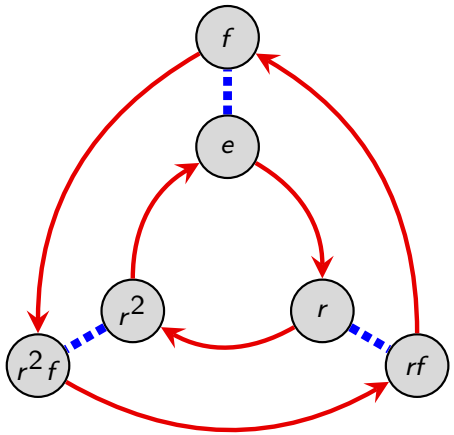
Do you see *why* this happens?

Orbits

Cyclic groups play a fundamental role in more complicated groups.

Observe how cyclic groups "fit" into other groups.

Consider the Cayley diagram for D_3:



Notice copies of the Cayley diagram for C_3 in this picture:

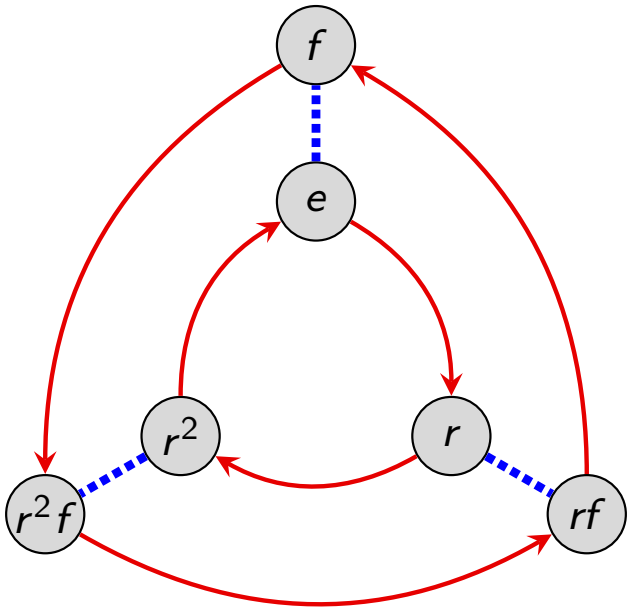
Starting at e, the red arrows lead in a length-3 cycle around the inside of the diagram. We refer to this cycle as the orbit of the element r.

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

Orbits are usually written with braces to emphasize that they are *sets*. 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.



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

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

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

Remarks:

- In any group, the orbit of e will simply be $\{e\}$.
- An orbit may be a finite or infinite set.
- We allow negative exponents, though this only matters in infinite groups.
- Think: 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 see later.

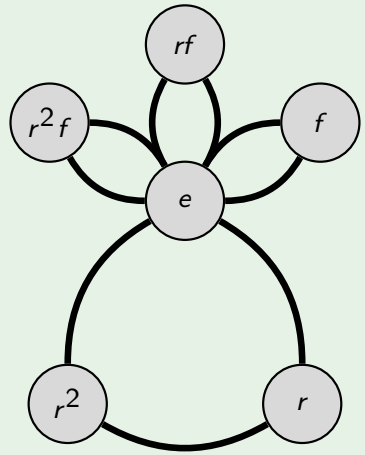
Definition

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 $|G|$.)

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	$\{e, r^2f\}$



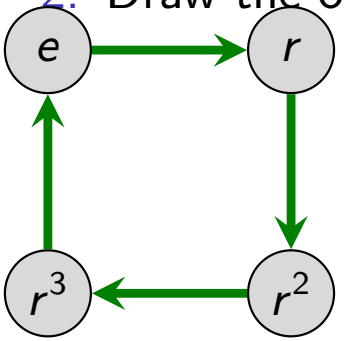
Comments

- 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.
- 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.

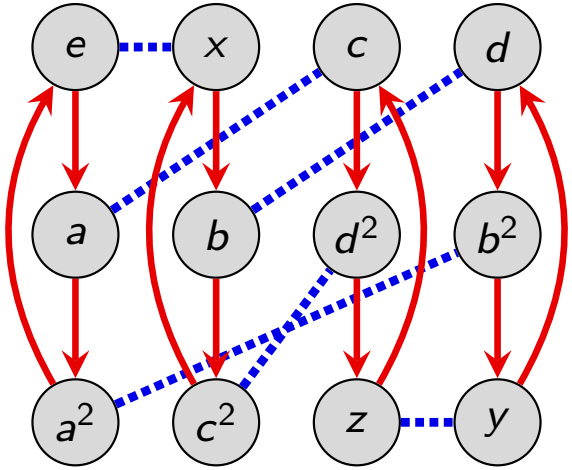
Taken from HW3 (Part I)

Carry out the same steps for the groups whose Cayley graphs are below.

1. Find the orbit of each element.
2. Draw the orbit graph of the group.



element	orbit
e	$\{e\}$
r	
r^2	
r^3	

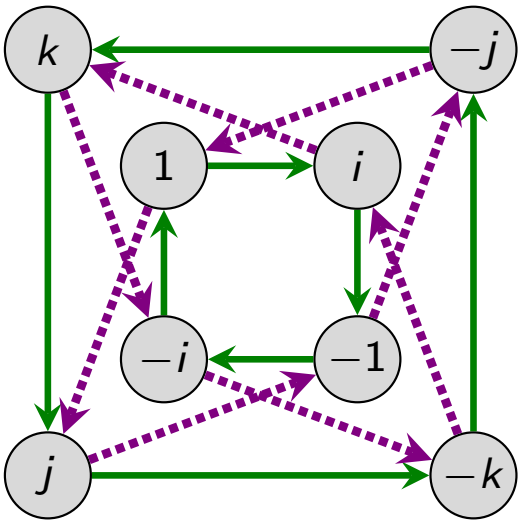


element	orbit
e	$\{e\}$
a	$\{e, a, a^2\}$
a^2	$\{\quad\quad\}$
x	$\{\quad\quad\}$
b	
c^2	

Taken from HW3 (Part II)

Carry out the same steps for the group whose Cayley graphs are below.

1. Find the orbit of each element.
2. Draw the orbit graph of the group.



element	orbit
e	$\{e\}$
i	$\{e, i, -1, -i\}$
-1	$\{$ $\}$
$-i$	
k	
j	

Abelian groups

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

Definition

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

Abelian groups are sometimes referred to as commutative.

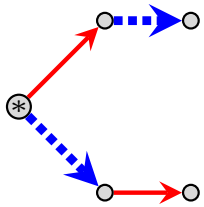
Remark

To check that a group G is abelian, 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.



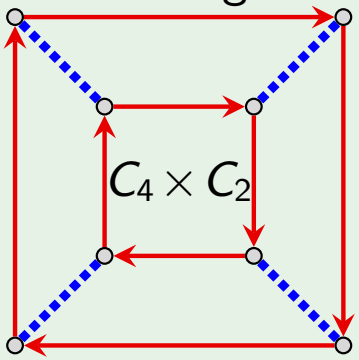
Reason 1: The configuration cannot occur (since there is only 1 generator).

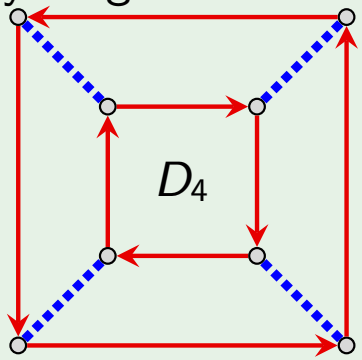
Reason 2: In the cyclic group $\langle r \rangle$, every element can be written as r^k for some k. Clearly, $r^k r^m = r^m r^k$ for all k and m.

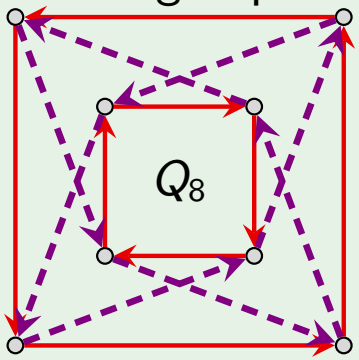
The converse is not true: if a group is abelian, it may not be cyclic (e.g, V_4.)

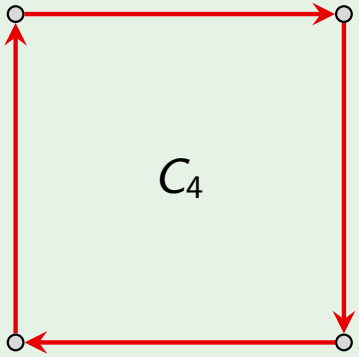
Example

The following are Cayley diagrams for four different groups.







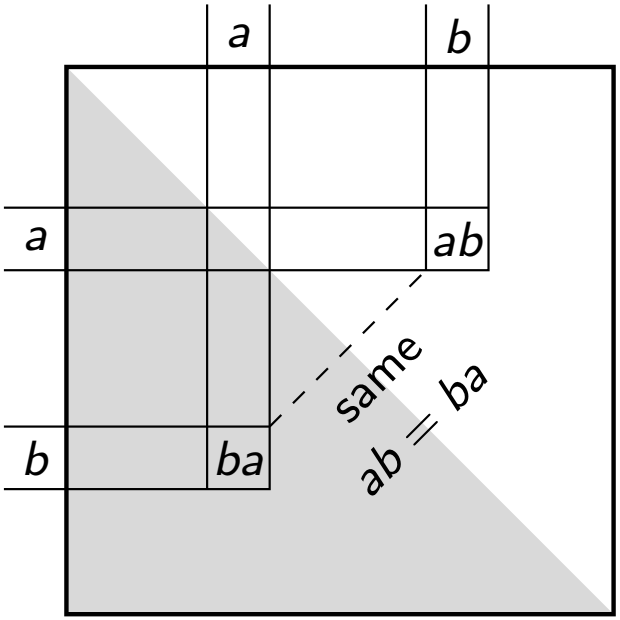


Which of these groups are abelian?

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