Algebraic GT | Instructor: Padraic Bartlett

Lecture 1: Cayley Graphs

Week 5 | *Mathcamp 2014*

Today and tomorrow's classes are focused nthe interplay of **graph theory** and **algebra**. Specifically, we are going to develop **Cayley graphs** and **Schreier diagrams**, use them to study various kinds of groups, and from there prove some very deep and surprising theorems from abstract algebra!

In specific: this course kind-of has a natural split into two parts, (a) exploring the concepts that link groups and graphs, and (b) using those concepts to prove results! This talk falls into the (a) camp; we're going to mostly study a large stack of definitions and examples here.

For the most part, I'm assuming everyone here has seen groups before. However, there are some specific group concepts that I want people to know for this class: **free groups**, **generating sets**, **presented groups**, and **cosets**.

Definition. The **free group** on n generators $a_1, \dots a_n$, denoted

$$\langle a_1, \dots a_n \rangle,$$

is the following group:

- The elements of the group are all of the strings of the form

  $$a_{i_1}^{k_1} a_{i_2}^{k_2} \dots a_{i_l}^{k_l},$$

  where the indices $i_1, \dots i_l$ are all valid indices for the $a_1, \dots a_n$ and the $k_1, \dots k_l$ are all integers.

- We also throw in an identity element e, which corresponds to the "empty string" that contains no elements.

- Given two strings s_1, s_2, we can **concatenate** these two strings into the word $s_1 s_2$ by simply writing the string that consists of the string s_1 followed by the string s_2.

- Whenever we have a^k in a string, we think of this as being $\overbrace{a \cdot a \cdot \dots a}^{k \text{ copies}}$, i.e. k copies of a. If we have multiple consecutive strings of a's, we can combine them together into one such a^k: for example, the word $a^3 a a^2$ is the same thing as the word a^6.

- Finally, if we ever have an aa^{-1} or an $a^{-1}a$ occurring next to each other in a string, we can simply replace this pairing with the empty string e.

For example, the free group on two generators $\langle a, b \rangle$ contains strings like

$$a^6 b^4 a^{-2} b^3 a^1, b^{12}, a^{-1} b^{-2} a^4 b, \dots$$

As described earlier, we concatenate strings by simply placing one after the other: i.e.

$$a^2b^{-2}a^3ba^3 \cdot a^{-3}b^{-1}a^1b^3 = a^2b^{-2}a^3ba^3a^{-3}b^{-1}a^1b^3.$$

As described above, we typically simplify this right-hand string by canceling out terms and their inverses, and grouping together common powers of our generators:

$$a^2b^{-2}a^3ba^3 \cdot a^{-3}b^{-1}a^1b^3 = a^2b^{-2}a^3\cancel{ba^3}\cancel{a^{-3}}\cancel{b^{-1}}a^1b^3 = a^2b^{-2}a^4b^3$$

This is a group! In particular, concatenation is associative, the empty string e is clearly an identity, and we can "invert" any word $a_{i_1}^{k_1}a_{i_2}^{k_2}\dots a_{i_l}^{k_l}$ by simply reversing it and switching the signs on the k_i's: i.e.

$$\cancel{a_{i_1}^{k_1}}\cancel{a_{i_2}^{k_2}}\dots\cancel{a_{i_l}^{k_l}} \cdot \cancel{a_{i_l}^{-k_l}}\dots\cancel{a_{i_2}^{-k_2}}\cancel{a_{i_1}^{-k_1}} = e$$

Definition. Given a group G, we say that it is **generated** by some collection of elements $a_1, \dots a_n \in G$ if we can create any element in G via some combination of the elements $a_1, \dots a_n$ and their inverses. Note that some groups have multiple different sets of generators: i.e. $\langle \mathbb{Z}, + \rangle$ is generated both by the single element 1 and also by the pair of elements $\{2, 3\}$

Definition. In our above discussion, we have primarily defined groups by giving a set and an operation on that set. There are other ways of defining a group, though! A **group presentation** is a collection of n generators $a_1, \dots a_n$ and m words $R_1, \dots R_m$ from the free group $\langle a_1, \dots a_n \rangle$, which we write as

$$\langle a_1, \dots a_n \mid R_1, \dots R_m \rangle.$$

We associate this presentation with the group defined as follows:

- Start off with the free group $\langle a_1, \dots a_n \rangle$.
- Now, declare that within this free group, the words $R_1, \dots R_m$ are all equal to the empty string: i.e. if we have any words that contain some R_i as a substring, we can simply "delete" this R_i from the word.

You have actually seen some groups defined via a presentation before:

Examples. Consider the group with presentation

$$\langle a \mid a^n \rangle.$$

This is the collection of all words written with one symbol a, where we regard $a^n = e$: i.e. it's just

$$e, a, a^2, a^3, \dots a^{n-1}.$$

This is because given any string $a^k \in \langle a \rangle$, we have $a^k = a^l$ for any $k \equiv l \mod n$. This is because we can simply concatenate copies of the strings a^n, a^{-n} as many times as we want without changing a string, as $a^n = e$!

You have seen this group before: this is just $\mathbb{Z}/n\mathbb{Z}$ with respect to addition, if you replace a with 1 and think of $\overbrace{11\dots1}^{k \text{ times}}$ as k.

Often, we will give a group with a presentation in the form

$$\langle a_1, \ldots a_n \mid R_1 = R_2, R_3 = R_4, \ldots, \ldots R_{m-1} = R_m \rangle,$$

because it is easier sometimes to think of saying that certain kinds of words are equal rather than other kinds of words are the identity; this is equivalent to the group presentation

$$\langle a_1, \ldots a_n \mid R_1(R_2)^{-1}, R_3(R_4)^{-1}, \ldots, \ldots R_{m-1}(R_m)^{-1} \rangle.$$

Definition. Suppose that G is a group, $s \in G$ is some element of G, and H is a subgroup of G. We define the **right coset** of H corresponding to s as the set

$$Hs = \{hs \mid h \in H\}.$$

We will often omit the "right" part of this definition and simply call these objects cosets.

Examples. Consider the group $G = \langle \mathbb{Z}, + \rangle$. One subgroup of this group is the collection of all multiples of 5: i.e.

$$H = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\}$$

This subgroup has several cosets:

- $s = 0$: this forms the coset

  $$H + 0 = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\},$$

  which is just H itself.
- $s = 1$: this forms the coset

  $$H + 1 = \{\ldots -14, -9, -4, 1, 6, 11, 16 \ldots\}.$$

- $s = 2$: this forms the coset

  $$H + 2 = \{\ldots -13, -8, -3, 2, 7, 12, 17 \ldots\}.$$

- $s = 3$: this forms the coset

  $$H + 3 = \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}.$$

- $s = 4$: this forms the coset

  $$H + 4 = \{\ldots -11, -6, -1, 4, 9, 14, 19 \ldots\}.$$

Notice that this collection of cosets above is indeed the collection of **all** of the possible cosets of H within G: if we take any other element in $\mathbb{Z}$, like say 13, we'll get one of the five cosets above: i.e.

$$H + 13 = \{\ldots -2, 3, 8, 13, 18 \ldots\} = H + 3.$$

In general, $H + x = H + y$ for any $x \equiv y \mod 5$.

Examples. Consider the group $G = \langle (\mathbb{Z}/7\mathbb{Z})^\times, \cdot \rangle$, i.e. the nonzero integers mod 7 with respect to the multiplication operation. This has the set

$$H = \{1, 6\}$$

as a subgroup (check this if you don't see why!)

This group has the following cosets:

- $s = 1$, which creates the cosets $H \cdot 1 = H$,
- $s = 2$, which creates the coset

$$H \cdot 2 = \{2, 5\}.$$

- $s = 3$, which creates the coset

$$H \cdot 3 = \{3, 4\}.$$

- $s = 4$, which creates the coset

$$H \cdot 4 = \{4, 3\}.$$

  Notice that this coset is the same as $H \cdot 3$.

- $s = 5$, which creates the coset

$$H \cdot 5 = \{5, 2\}.$$

  Notice that this coset is the same as $H \cdot 2$.

- $s = 6$, which creates the coset

$$H \cdot 6 = \{6, 1\}.$$

  Notice that this coset is the same as H.

Examples. Consider the group S_3. This group has the subgroup

$$H = \{id, (123), (132)\}$$

as a subgroup. This subgroup has two possible distinct cosets:

- $H \cdot id = H \cdot (123) = H \cdot (132)$ are all the same coset, which is just H.
- $H \cdot (12) = H \cdot (13) = H \cdot (23) = \{(12), (13), (23)\}$.

With these definitions set down, we can actually start to do some graph theory:

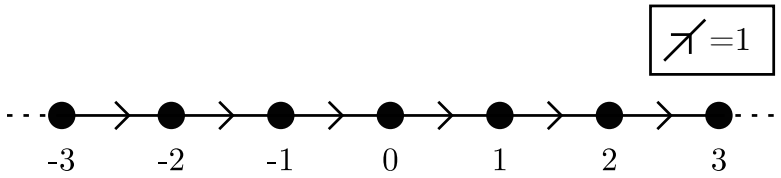
1 Cayley Graphs and Groups

Definition. Take any group A along with a generating set S. We define the **Cayley graph** $G_{A,S}$ associated to A as the following directed graph:

- Vertices: the vertices of G_A are precisely the elements of A.
- Edges: for two vertices x, y, create the oriented edge (x, y) if and only if there is some generator $s \in S$ such that $x \cdot s = y$. If this happens, we decorate the edge (x, y) with this generator s, so that we can keep track of how we have formed our connections.

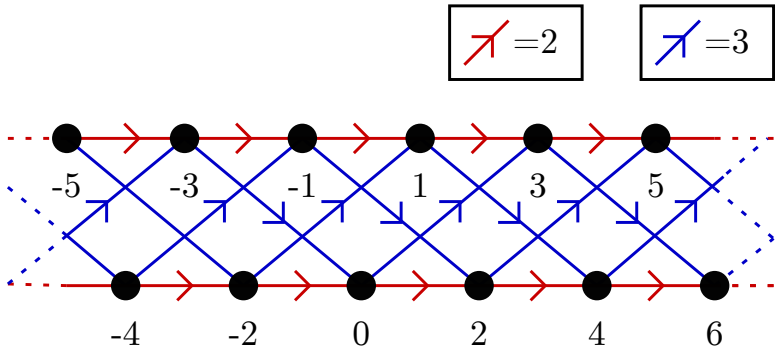
We consider a few examples here:

Examples. The integers $\mathbb{Z}$ with the generator 1 have the following very simple Cayley graph:



This is not hard to see: we have one vertex for every element in our group (i.e. every integer,) and an edge (x, y) for each pair x, y such that $x = y + 1$, by definition. Because this is a Cayley graph, we label each of these edges with the generator that created that edge: for this graph, because there's only one generator this is pretty simple (we just label every edge with a 1.)

Examples. The integers $\mathbb{Z}$ with the generating set $\{2, 3\}$ have the following Cayley graph:

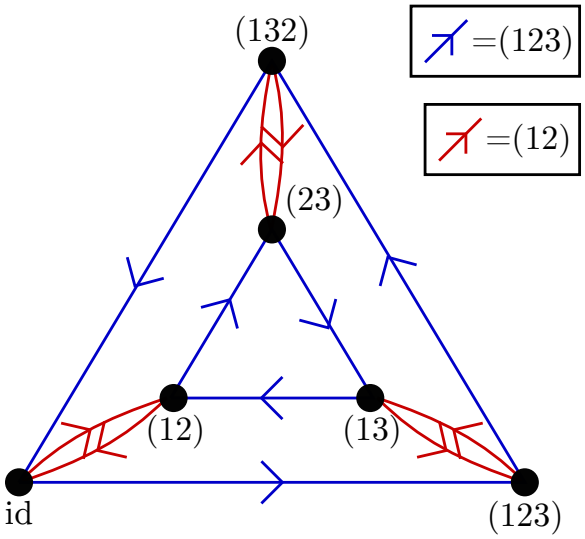


Again, our vertices are just the integers. However, this time we have two generators: the generator 2 connects any two integers that differ by 2, while the generator 3 connects any two integers that differ by 3. Notice that this graph is not the same as the graph above: in general, a group can have many markedly different Cayley graphs depending on the generators that you pick for it.

Examples. Consider the symmetric group S_3 with generators $(12), (123)$. First, we calculate how these generators interact with our group elements when composed together:

group elt. $\circ$ generator	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(123)	(132)	(13)	(23)
(123)	(123)	(23)	(12)	(13)	(132)	(123)

We can use this table to create the Cayley graph for this group and generating set:



Examples. Consider the group given by the presentation

$$\langle a, b \mid a^3 = b^2 = (ab)^2 = id \rangle.$$

Because we do not know all of the elements in this group ahead of time, it is not necessarily obvious how to create this group's Cayley graph; unlike in our earlier examples, we cannot simply write down all of the vertices and then draw edges corresponding to our generators.

Instead, to find the Cayley graph corresponding to this group, we can use the following procedure:

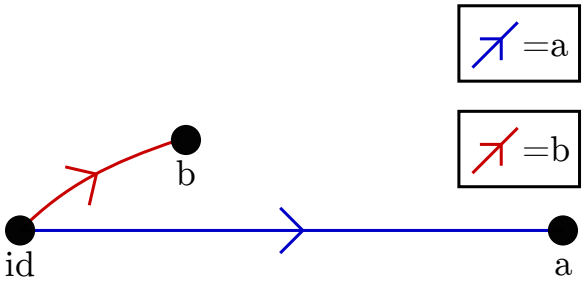
0. Start by placing one vertex that corresponds to the identity.

1. Take any vertex corresponding to a group element g that we currently have in our graph. Because our graph is a Cayley graph, it must have one edge leaving that vertex for each generator in our generating set. Add edges and vertices to our graph so that this property holds.

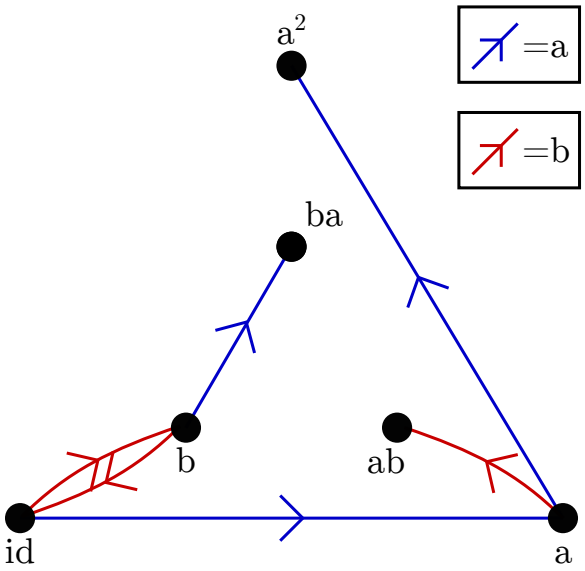
2. If some word R_i is a word that is equal to the identity in our group, then in our graph the path corresponding to that word must be a **cycle**: this is because if this word is the identity, then multiplying any element in our group by that word (i.e. taking the walk on our graph corresponding to that word) should not change that element (i.e. our walk should not take us somewhere new, and therefore should return to where it started!)

Identify vertices only where absolutely necessary to insure that this property holds at every vertex. (This is the computationally "difficult" part of this algorithm. In general, finding the Cayley graph, or even more simply determining whether two arbitrary words in a presented graph are equal, is an **undecidable** problem: it is provable that no algorithm exists that will always solve this problem. Look up things like the halting problem if you want more examples of such things.)

So: if we do this here, we would start by drawing the following graph.



We add edge/vertex pairs to both of these added vertices a, b, that correspond to our generators. Notice that the relation $b^2 = id$ tells us that our b-edge leaving b must return to id, and that none of our other relations apply at this current stage (as they correspond to walks of length at least 3.)

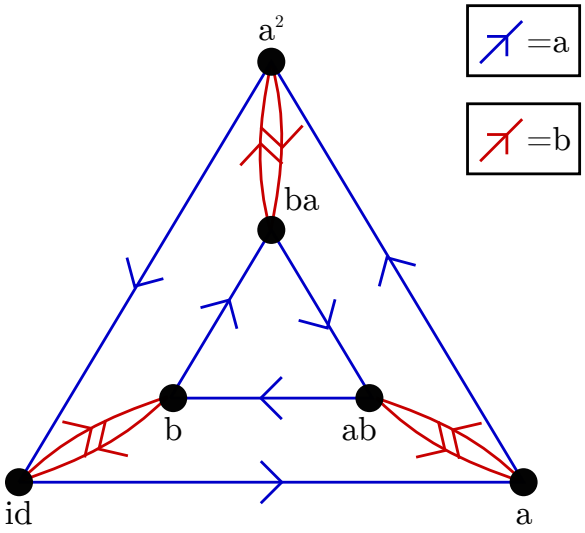


Now, we draw new edge from the vertices ab, ba, a^2. Notice that the relation $a^3 = id$ tells us that the a-edge leaving a^2 returns to the identity, and that the relation $b^2 = id$ tells us that the b edge leaving ab returns to a. Furtheromre, the relation $abab = id$, along with the observations that $b^2 = id \Rightarrow b = b^{-1}, a^3 = id \Rightarrow a^2 = a^{-1}$ gives us a number of new relations:

- $abab = id \Rightarrow bab = a^{-1} = a^2$, and therefore the b-edge leaving ba goes to a^2. Furthermore, this also tells us that the b-edge leaving a^2 goes to ba, because the walk corresponding to b^2 starting from ba must return to ba.

- $abab = id \Rightarrow aba = b^{-1} = b$, and therefore that the a-edge leaving ab goes to b. Furthermore, this also tells us that the a-edge leaving ba goes to ab, because the walk corresponding to a^3 starting at ab must return to ab.

This gives us the following graph:



At this stage, we have satisfied our second property (that there is an edge leaving each vertex for each generator,) and we have only identified vertices when absolutely forced to do so by our relations. From visual inspection, it is clear that we satisfy the three relations $a^3 = b^2 = abab = id$ at every vertex; so this is the Cayley graph corresponding to our group!