Graph Theory: an Introduction

August 30 & September 6, 2023

Note: This is the first of a two-part lecture series on Graph Theory--this half will give some basic examples and properties of groups while the second half delves deeper into concepts such as homomorphisms and cosets.

Section 1: The Integers

You've probably worked with the integers for many years now. If so, you also probably know a few properties of addition. For instance, addition is commutative, meaning that for any integers a and b, a+b=b+a. What other properties of addition can you think of?

It turns out that the integers form a group under the operation addition. This is because it satisfies the three essential properties, or "axioms," of a group. First, the integers are associative under addition, meaning that for any three integers a, b, and c, (a+b)+c=a+(b+c). Second, the integers contain an identity element, 0, which can be added to any integer to result in the same integer. Finally, for every integer, there is an additive inverse that is also an integer; that is, given an integer a, there exists an integer -a such that a+(-a)=-a+a=0.

There are also two other properties that are assumed about any group, which is that the group is non-empty and its elements are closed under its operation. Non-empty just means that there has to be something in your group, and a group being closed under its operation means that when you use its operation on two elements of the group, the result is also in the group. For instance, the set of integers with absolute value less than 5 is not a group--even though it is associative, has an identity element, and contains inverses, it is not closed because, for instance, 4 is in the group but 4+4=8 is not. If these notions seem a bit vague, we'll get to writing them for concretely later.

What about the integers under multiplication? Well, it contains an element, so it is non-empty, and any two integers multiply to another integer, so it is closed. It is also associative, since multiplication is associative, and contains an identity element, 1. However, it does not contain inverses, so the integers under multiplication.

For these next problems, I will present a set and an operation, and you should determine whether they form a group or not. Here as in elsewhere, $\mathbb{Z}$ will denote the integers, $\mathbb{Q}$ the rationals, and $\mathbb{R}$ the real numbers, while a superscript of * indicates that we are excluding the number 0 and a superscript of $^+$ indicates that we are only considering positive values.

1) $(\mathbb{Z}^+, +)$
2) $(\mathbb{Q}, *)$
3) $(\mathbb{Q}, +)$
4) $(\mathbb{Q}^+, *)$
5) $(\mathbb{R}, -)$
6) $(\mathbb{R}^*, *)$

Section 2: Symmetry Groups

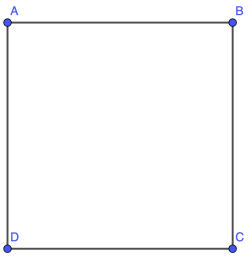
Let's recap the definition of a group a bit more formally:

A group is a nonempty set S together with a binary operation * on that set under which the set is closed, satisfying the three following properties:

a) The operation is associative; that is, for any elements a, b, and c of S, (a*b)*c=a*(b*c)
b) S contains an identity element e where for any element a of S, a*e=e*a=a.
c) For any element a of S, there exists another element a^{-1} of S such that $a*a^{-1}=a^{-1}*a=e$.

This definition actually allows a wide variety of groups to exist, and one important such type of group is the symmetry group of a regular polygon.

Consider a square, with vertices labeled A, B, C, and D.



We can list the symmetries of the square as follows:

-The symmetry where you do nothing and the square stays the same
-The symmetries where you rotate the square 90, 180, or 270 degrees counterclockwise
-The symmetry where you reflect the square over a vertical axis
-The symmetries where you reflect the square over a vertical axis and then rotate the square 90, 180, or 270 degrees counterclockwise (equivalent to reflecting over various axes)

We can denote the “do nothing” operation e, write the rotations as r, r^2, and r^3 respectively for 90, 180, and 270 degrees counterclockwise, denote the reflection over the vertical axis s, and the reflection followed by a 90, 180, and 270-degree counterclockwise rotation as rs, r^2s, and r^3s respectively.

If we define an operation between two symmetries as the act of doing the symmetry on the right followed by the one on the left, this is a group.

1) Verify that the symmetries of the square indeed form a group by checking all the axioms of a group. For instance, the symmetries are associative because they can be thought of as “functions” on the square, and functions are associative.`
2) Verify that the group of symmetries on a square does not satisfy the commutative property

We call such non-commutative groups *non-abelian*, and commutative groups are known as *abelian*.

3) Write out the elements of the group of symmetries on a hexagon.
4) Consider only the rotational symmetries of a square. Show that these still form a group under the operation of composition, and furthermore that this group is actually abelian.
5) Consider only the reflective symmetries of a square. Show that these do not form a group under the operation of composition.

Section 3: Modular Arithmetic

Another common and important type of group is found in modular arithmetic. In modular arithmetic, a positive integer greater than one is picked as a modulus, and then other integers are considered based on their remainder when divided by that integer. For instance, we would write that $2 \equiv 5 \pmod 3$, indicating that 2 and 5 leave the same remainder on division by 3.

This is a bit informal, so if you want a more formal definition, modular arithmetic divides the integers into congruence classes where two integers *a* and *b* are in the same congruence class if and only if *a*-*b* is divisible by a certain integer *n*, known as the modulus.

The point of modular arithmetic is that we can take the integers, which have an infinite number of elements, and transform them into a finite number of equivalence classes, which can be much easier to deal with. For instance, it might seem daunting to prove that the integer 4,003 cannot be written as the sum of two square numbers, but modular arithmetic makes this task very simple. (We will prove this together during the lecture).

To unlock the full potential of modular arithmetic, it is important to understand its structure as a group. However, to do that, we must first decide on an operation for the group.

1) Show that the integers modulo 5 form a group under addition. We can write this group as ($\mathbb{Z}/5\mathbb{Z}$). Can you show that ($\mathbb{Z}/n\mathbb{Z}$) is a group for any integer n>1?
2) Show that the integers modulo 5 do not form a group under multiplication. But what if we exclude the 0 element in this case?
3) Show that the integers modulo 6 do not form a group under multiplication. But what if we exclude the 0 element in this case?
4) For which *n* do the integers modulo *n* form a group under multiplication when we exclude the 0 element? For these *n*, we can denote the group as $(\mathbb{Z}/n\mathbb{Z})^X$. (warning: this one might be tricky)

Figuring out that modular arithmetic can be thought of in terms of groups is cool, but essentially useless unless we also know some properties of groups.

Part 4: The Basics of Groups

Let's go back to the group axioms. As a reminder, a group is a nonempty set S together with a binary operation * on that set under which the set is closed, satisfying the three following properties:

a) The operation is associative; that is, for any elements a, b, and c of S, (a*b)*c=a*(b*c)
b) S contains an identity element e where for any element a of S, a*e=e*a=a.
c) For any element a of S, there exists another element a^{-1} of S such that $a*a^{-1}=a^{-1}*a=e$.

In particular, remember that the operation * is just some sort of operation that we define based on the group we're looking at--it does not necessarily mean multiplication!

Now, one immediate result of these axioms is that the identity element is unique; that is, if e and f are both identity elements of some group G, then e=f. This can be proven by noting that e=e*f and e*f=f, both by property b).

1) Show that for any element of a group, its inverse is unique.
2) Using your previous result, show that if a*b=c*b in a group, then a=c.

These results already have some limited applications. For instance, let's suppose we were trying to show that if we have some integers w, x, y, and z for which wx-yz and z-x are divisible by the prime number 89, then y-w is divisible by 89 as well. Of course, we could do this directly, but we could also note first that none of the variables can be divisible by 89, so all of them are in the group $(\mathbb{Z}/89\mathbb{Z})^X$. Next, the conditions

effectively state that $wx \equiv yz \pmod{89}$ and $x \equiv z \pmod{89}$, so $wx \equiv yx \pmod{89}$ and then $w \equiv y \pmod{89}$ by our previous result, and we are done.

The study of groups would be somewhat limited if we were confined to just looking at one group at a time. Therefore, we also study the ways in which we can move between groups, through functions called group homomorphisms.

Part 5: Group Homomorphisms

Let's say we have a group G and a group H. We can define a homomorphism $f : G \to H$ as a function from G to H such that $f(a*b)=f(a)*f(b)$ for all $a,b \in G$. For instance, we could set a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}/5\mathbb{Z})$ that sends each integer to its value modulo 5, and this would work because addition is preserved when taking a modulus. Here are some basic results about homomorphisms you should prove:

1) If we have a group G, a group H, and a homomorphism $f : G \to H$, then $f(e_g)=e_h$ where e_g and e_h are the identity elements of G and H respectively.
2) If we have a group G, a group H, and a homomorphism $f : G \to H$, then $f(a^{-1})=f(a)^{-1}$ for any $a \in G$.

A homomorphism from a group to itself is called an automorphism, and a bijective (i.e. invertible) homomorphism is an isomorphism. A good way to think about isomorphisms is that they are "renaming" the elements of a group but preserving their structure. We will discuss homomorphisms more theoretically tomorrow, but for now it is probably best just to get some experience with them in practice.

3) The trivial homomorphism is the homomorphism that just sends all elements to the identity element of the "target" group. Find and describe a nontrivial homomorphism from $(\mathbb{Z}/10\mathbb{Z})$ to $(\mathbb{Z}/5\mathbb{Z})$.
4) Find and describe a nontrivial homomorphism from $(\mathbb{Z}/7\mathbb{Z})^{\times}$ to $(\mathbb{Z}/2\mathbb{Z})$.
5) Find and describe an isomorphism from $(\mathbb{Z}/7\mathbb{Z})^{\times}$ to $(\mathbb{Z}/2\mathbb{Z})$.
6) Find and describe a nontrivial homomorphism from $(\mathbb{Z}/8\mathbb{Z})$ to the group of symmetries on a square (sometimes, this group is written D_8 and sometimes it is written as D_4, which is very annoying. I will write it as D_8, representing the fact that it has 8 elements.)
7) Find and describe an nontrivial isomorphism from $(\mathbb{Z}/8\mathbb{Z})$ to the group of symmetries on an octagon, excluding reflections.
8) Find a nontrivial homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Q}^{+}, *)$

As you can probably tell from these examples, a lot of groups we might encounter have homomorphisms and isomorphisms between them, which makes group theory a nice way to unify concepts in different

parts of mathematics. The structure of groups is very fundamental to the structure of many mathematical objects, and we will look at this more in the next lesson.