Group Theory: Part II

September 6, 2023

Note: This is the second of a two-part lecture series on Group Theory, which will discuss more about homomorphisms and introduce the concepts of subgroups, cosets, and quotient groups.

.Section 0: Review of Definitions

In order to discuss groups, we're going to first need to remember what a group is. A group is a nonempty set G together with a binary operation * under which G is closed, satisfying three key properties. Write these properties here:

1)

2)

3)

So to be a group, a set and operation must satisfy all of these properties. For instance, let's define $\oplus$ to be an operation where $a \oplus b = a+b+1$ and define $\otimes$ to be an operation where $a \otimes b = (a+1)*(b+1)$.

Then ($\mathbb{Q}^+$, $\otimes$) is not a group. Which rule does it fail to satisfy?

What about ($\mathbb{Z}$, $\oplus$)? Is that a group?

Also, recall that in any group, $a*b=c*b$ implies that $a=c$ and $b*a=b*c$ implies that $a=c$ as well. We proved this last week, and it will be important again here.

.Section 1: Homomorphisms

Recall that a *homomorphism* f : G⟶H is a function from G to H such that f(a*b)=f(a)*f(b) for all a,b∈G. Last week, we showed that homomorphisms preserve the identity element and inverses. An example of a homomorphism from (ℤ/10ℤ) to (ℤ/5ℤ) would be one that simply takes an element of (ℤ/10ℤ) to its value modulo 5.

How would we show that this is a homomorphism? Well, we can just apply the definitions. Let a,b∈(ℤ/10ℤ). Since 5 divides 10, a and b both have a well-defined remainder when divided by 5 (what would happen if we chose a different modulus, like 4?). Now, f(a+b) is the remainder of a+b when divided by 5, but since addition is well-defined in modular arithmetic, this is the same as the remainder of a when divided by 5 plus the remainder of b when divided by 5, so f(a+b)=f(a)+f(b) and we are done.

Another important thing to note about homomorphisms is the interpretation of the operation *. When we say f(a*b)=f(a)*f(b), we mean the operation a*b as interpreted in G and the operation f(a)*f(b) as interpreted in H. For instance, let's take a homomorphism from (ℤ, +) to ($\mathbb{R}^*$, *) where f(x)=2^x. This is a homomorphism because f(a+b)=2^{a+b}=2^a*2^b=f(a)*f(b). Note that we aren't multiplying the integers in the inside of the homomorphism nor adding the reals on the outside, because we don't have multiplication in the group structure (ℤ, +) nor addition in ($\mathbb{R}^*$, *).

Now, onto some more definitions. An *isomorphism* is a bijective (one-to-one and onto, or, equivalently, invertible) homomorphism, and an *automorphism* is an isomorphism[1] from a group to itself. For instance, we could set up an automorphism on (ℤ, +) where f(x)=-x. Two groups are *isomorphic* if there exists an isomorphism from one to the other. Two isomorphic groups are essentially the same group but relabeled.

1) 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 (ℤ/20ℤ) to (ℤ/4ℤ).
2) Find and describe a nontrivial homomorphism from $(\mathbb{Z}/7\mathbb{Z})^\times$ to (ℤ/2ℤ).
3) Find and describe an isomorphism from (ℤ, +) to (ℤ, ⊕)
4) Find and describe an isomorphism from (ℤ/8ℤ) to the group of symmetries on an octagon, excluding reflections.

Section 2: Subgroups and the Subgroup Test

[1] There was an error in the previous handout stating that an automorphism could be any homomorphism from a group to itself. That is not enough; the automorphism must be an isomorphism as well.

Let (G, *) be a group. Then, let H be a subset of G. We say (H, *) is a *subgroup* of G if (H, *) still satisfies the group axioms. For instance, the set of even integers (2ℤ, +) would form a subgroup of the group of integers with respect to addition.

1) Show that the elements of (ℤ/9ℤ) that are divisible by 3 form a subgroup of (ℤ/9ℤ).

Now, we could just check all the axioms every time we want to prove that something is a subgroup. However, that would be tedious and there is actually a faster way.

We still need to check that the subgroup is nonempty and closed under the operation. However, the subgroup inherits associativity from the main group (since the operation is the same), so we don't need to check that. Now, it seems that we would still need to check that there is an identity element in the subgroup and that the subgroup contains inverses.

2) Show that if H is a subgroup of G and e_g and e_h are the identity elements of G and H respectively, then e_g=e_h.
3) Show that if H is a subgroup of G and h is an element of H, then the inverse of h in H is the same as the inverse of h in G.

Using both of these results, we can find that the identity and inverses are preserved in the subgroup, so we can safely refer to them without needing to specify whether they are interpreted in the group or subgroup. Now, we can write our simplified criteria for being a subgroup H of a group G as follows:

a) There exists an element in H (H is non-empty).
b) If a,b∈H, then a*b∈H (H is closed under the operation).
c) e∈H (existence of identity).
d) If a∈H, then a^{-1}∈H (inverses).

It would be very convenient if these could all be summarized in just two properties. Fortunately, it can!

4) Show that if a*b^{-1}∈H for all a,b∈H, and H⊆G is non-empty where (G, *) is a group, then H is a subgroup of G.

This is known as the Subgroup Test and can be very useful in shortening the calculations for proving that things are subgroups.

.Section 3: Normal Subgroups and Cosets

We begin with a definition.

Let G be a group, and H be a subgroup of G. Then H is a *normal subgroup* if and only if for all h$\in$H and g$\in$G, $ghg^{-1}\in$H.

1) Verify that if G is abelian, then all subgroups of G are normal. Then, find an example of a non-normal subgroup of D_8.

Next, another definition.

Let G be a group, and H be a subgroup of G. We define the *left coset* of H containing an element g$\in$G as gH={g*h, h$\in$H}. Can you guess what a *right coset* is?

2) Let G be ($\mathbb{Z}$, +) and H be the subgroup consisting of only the even integers. Describe gH, where g=3.
3) Let G be ($\mathbb{Z}/12\mathbb{Z}$) and H be the subgroup consisting of the elements {0,6}. Describe gH, where g=2.
4) Let G be D_8 and H be the subgroup consisting of only the rotational symmetries of the square. Describe, gH, where g is the reflection over the vertical axis.
5) Let G be a group and H be a normal subgroup of G. If g$\in$G, show that the left coset gH is the same as the right coset Hg.
6) Let G be a group, H be a normal subgroup of G, and h$\in$H. If g$\in$G, show that gH=(gh)H.

Next, we will show that the left cosets of a subgroup H of a group G form a partition of G. What this means is that every element of G is in exactly one distinct left coset of H. We will prove this in the following two steps:

7) Let G be a group and H be a subgroup of G. Show that every element of G is in at least one left coset of H.
8) Let G be a group and H be a subgroup of G. Show that if two left cosets aH and bH share an element, then aH=bH.

Thus, every element is in at least one left coset of H, and in no more than one distinct left coset of H, and we are done. A similar proof holds for the right cosets.

9) Show that if G is a finite group with n elements, any subgroup of G has a number of elements that divides into n.

Section 4: Quotient Groups

Let G be a group, and H be a normal subgroup of G. Then we can define G/H as the set of cosets of H (since H is normal, we don't care about which side the cosets are), and we can define an operation on the elements of G/H where, for any a,b$\in$G, aH*bH=(a*b)H.

First, we need to figure out if what we're talking about makes sense. Remember that there could be multiple elements of G which give rise to the same coset, so we might run into problems where multiplying (using the operation on) the same two cosets might lead to a different result.

To deal with this issue, let a,b,x,y$\in$G such that aH=xH and bH=yH. We need to show that aH*bH=xH*yH.

This is equivalent to showing that (a*b)H=(x*y)H. Recall that H must include the identity element of G. Therefore, xH contains x*e=x (by definition of coset). Since aH=xH and xH contains x, so must aH. Since H is normal, aH=Ha by problem 5) of the last section. Therefore, Ha must also contain x, so by definition of coset we have that there exists some $h_a \in$H where h_a*a=x. Meanwhile, a we know that bH contains b and yH=bH, so there must exist $h_y \in$H where y*h_y=b. Now, we know that (x*y)H contains (x*y)*(h_y) by definition of coset. By associativity, (x*y)*(h_y)=x*(y*h_y)=x*b. So x*b$\in$(x*y)H. On the other hand, (a*b)H=H(a*b) by normality of H, and H(a*b) contains h_a*(a*b). But then, h_a*(a*b)=(h_a*a)*b=x*b, so (a*b)H also contains x*b. But then (a*b)H and (x*y)H share an element, so by 8) of the last section (a*b)H=(x*y)H and we are done.

We now claim that G/H is a group. To do this, we need to check our axioms.

G/H contains at least eH, so it is nonempty. G/H is also closed because if aH,bH$\in$G/H, then a,b$\in$G, so by closure a*b$\in$G and then aH*bH=(a*b)H$\in$G/H. In a similar way, associativity is inherited from G. Then, eH=H is the identity element of G/H, and the inverse of gH is g^{-1}H, so G/H is indeed a group.

That was a lot of symbolic manipulation. Let's do some practice problems!

1) Write out the elements of G/H, where G is ($\mathbb{Z}$/12$\mathbb{Z}$) and H is the subgroup consisting of the elements {0,4,8}.
2) Find an isomorphism from G/H in the previous problem to ($\mathbb{Z}$/4$\mathbb{Z}$).
3) How many elements are in the group G/H, where all we know is that G has size 30 and H has size 5?
4) Let |G| denote the number of elements in a group G. If G is a finite group and H is a subgroup of G, show that |G/H|*|H|=|G|.

Section 5: Homomorphisms and Quotient Groups

We have two more definitions to go over. Let G and H be groups, and let f:G->H be a homomorphism. We define the *kernel* of f, ker(f), as the set of elements of G that f sends to the identity of H. We then define the *image* of f, im(f), as the set of elements h∈H such that there exists some g∈G such that f(g)=h.

1) Let f be the homomorphism from (ℤ/10ℤ) to (ℤ/5ℤ) described in section 1. Find im(f) and ker(f).
2) Let f be the homomorphism f(x)=3^x from (ℤ, +) to ($ℝ^*$, *). Find im(f) and ker(f).
3) Let f be the homomorphism from (ℤ/15ℤ) to (ℤ/10ℤ) where if x∈(ℤ/15ℤ), f(x) is two times the remainder of x when divided by 5. Find im(f) and ker(f).

We now prove a statement of the fundamental theorem on homomorphisms. This statement is that if G and H are groups, and f:G->H is a homomorphism, then ker(f) is a normal subgroup of G, and im(f) is isomorphic to G/ker(f).

4) Use the definitions of a group and a homomorphism to check that ker(f) is a normal subgroup of G.
5) Show that im(f) is a group.
6) Find and prove an isomorphism from G/ker(f) to im(f).

This theorem is fundamental to a lot of group theory. While we do not have time to go over many of its implications, here are at least a few:

7) Show that if G and H are two groups and f:G->H is a surjective (onto) homomorphism, then |H| divides |G|.
8) Show that if G and H are two groups and f:G->H is a homomorphism, then |im(f)| divides both |G| and |H|. Conclude that there are no nontrivial homomorphisms between (ℤ/15ℤ) and (ℤ/91ℤ) .