GROUPS AND SYMMETRY: LECTURE 21

LEO GOLDMAKHER

Recall from last lecture that we say two groups are isomorphic if they are the same up to renaming the elements. This sounds a bit silly at first – after all, any two sets with the same number of elements are the same up to renaming their elements! But a group is much more than a collection of elements; its elements are intimately connected to one another via the binary operation. Whereas a set can be summarized just by listing all of its elements, a group can be summarized by displaying its multiplication table. Thus when we say two groups to be isomorphic, we really mean their multiplication tables are the same up to relabeling the elements. Last time we concluded that, up to isomorphism, the only group of order 3 is the cyclic group. There were two different groups of order 4: the cyclic group of order 4, and the Klein V group. How many groups are there of order 5? Since 5 is prime, any group of order 5 must be cyclic. It follows that there is only one group of order 5 (up to isomorphism).

We next tried to formulate more precisely what it means for two groups Γ and H to be isomorphic. Dan pointed out that they must have the same size, i.e. there must exist a bijection $\varphi : \Gamma \to H$. You can think of this as a dictionary which translates from the language of Γ into the language of H: an element $g \in \Gamma$ corresponds to $\varphi(g)$, and the fact that φ is bijective means that you can use the dictionary to translate in either direction between the two languages. This isn't quite enough for the groups to be isomorphic, however; we need that this relabeling matches up with the multiplication table. In other words, we need to know that if we translate the multiplication table for Γ into the language of H, then we get the multiplication table for H. Hui suggested the following formulation:

$$\textit{If } c = ab \textit{ in } \Gamma\textit{, then } \varphi(c) = \varphi(a)\varphi(b) \textit{ in } H.$$

We're now ready to write down a formal definition.

Definition. *We say two groups Γ and H are* isomorphic*, written $\Gamma \simeq H$, iff there exists a bijection $\varphi : \Gamma \to H$ which satisfies*

$$\varphi(ab) = \varphi(a)\varphi(b)$$

for all $a, b \in \Gamma$. If such a map φ exists, it is called an isomorphism *from Γ to H.*

Given an function φ, we will often indicate that it's an isomorphism by simply writing

$$\varphi : \Gamma \xrightarrow{\sim} H.$$

In other words, from now on, whenever you see a function defined with a tilde above the arrow, you may assume it's an isomorphism.

We've already seen a few examples of isomorphic groups. Here are a few more.

(1) $\mathbb{Z} \simeq 2\mathbb{Z}$. What's the isomorphism? The most natural bijection between these is $\varphi(n) := 2n$, and this is easily seen to be an isomorphism:

$$\varphi(a + b) = 2(a + b) = 2a + 2b = \varphi(a) + \varphi(b).$$

Date: November 22, 2013.

This illustrates a general principle – the most natural bijection between two groups is often an isomorphism.

(2) $\mathbb{Z}/2\mathbb{Z} \simeq \{\pm 1\}$. Note that the binary operations are different – on the left it's addition, on the right it's multiplication. Nonetheless, they are isomorphic. We checked by hand that $\varphi : \mathbb{Z}/2\mathbb{Z} \to \{\pm 1\}$ defined by $\varphi([0]) := 1$, $\varphi([1]) := -1$ gives an isomorphism.

(3) $\mathbb{R}_{>0} \simeq \mathbb{R}$. Here the set on the left is a group under multiplication, while the set on the right is a group under addition. What's an isomorphism between them? Jerry suggested that $\log : \mathbb{R}_{>0} \simeq \mathbb{R}$ is an isomorphism. It's straightforward to check that it's injective and surjective. It's also an isomorphism, since

$$\log(ab) = \log a + \log b$$

for all $a, b > 0$. (Jerry further pointed out that this gives infinitely many different isomorphisms between $\mathbb{R}_{>0}$ and $\mathbb{R}$: we can take the logarithm to any base.)

Thus, even groups which appear completely different on the surface might be isomorphic. Note that there are three steps involved in proving that two groups are isomorphic:

Step 1: Guess an isomorphism φ.

Step 2: Check that φ is a bijection.

Step 3: Check that $\varphi(ab) = \varphi(a)\varphi(b)$ for all a, b.

In practice, Steps 2 and 3 are fairly straightforward, while Step 1 can be quite tricky. One general guideline is to let φ be a 'natural' bijection. But there are some other tricks which help us look for potential isomorphisms. For example, we have the following result, which Dan conjectured in lecture:

Proposition 1. *If $\varphi : \Gamma \xrightarrow{\sim} H$, then*

- $\varphi(e_\Gamma) = e_H$
- $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof. Eric suggested the following proof of the first assertion. We know $\varphi(ab) = \varphi(a)\varphi(b)$ for every $a, b \in \Gamma$. Pick $a = e_\Gamma$; then $\varphi(b) = \varphi(e_\Gamma)\varphi(b)$. This is an equation in H, a group, so we can cancel on both sides to find $\varphi(e_\Gamma) = e_H$ as claimed.

For the second assertion, observe that

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_\Gamma) = e_H.$$

It follows that $\varphi(a^{-1})$ is an inverse of $\varphi(a)$ in the group H. Since inverses are unique, we conclude. □

Jamal pointed out a curious asymmetry. The relation $\simeq$ should be an equivalence relation, and hence symmetric, but the definition relies upon a function from Γ to H. This seems to treat Γ and H differently. However, if φ is an isomorphism. This implies that φ^{-1} is a bijection from H to Γ; it is a nice exercise to show that φ^{-1} is an isomorphism. Thus, there exists an isomorphism from Γ to H if and only if there exists an isomorphism from H to Γ. The relation is symmetric after all.

The language of isomorphisms allows us to ignore the more superficial aspects of groups and focus on their underlying structure. For example, here is a theorem you will prove in this week's problem set:

Theorem 2 (Cayley's Theorem)**.** *Every group Γ is isomorphic to a subgroup of S_Γ, the symmetric group Γ.*

In particular, it follows that every group can be written in the language of permutations. Colloquially, one can view this as saying that every group is a subgroup of a group of permutations.

The statement of Cayley's theorem is surprisingly unspecific: it asserts the existence of a subgroup $H \leq S_\Gamma$ and an isomorphism $\varphi : \Gamma \xrightarrow{\sim} H$, but doesn't tell us how to find either. Can we be more specific about the map φ? The only things we can say for sure are that $\varphi : \Gamma \to S_\Gamma$, and that $\varphi(ab) = \varphi(a)\varphi(b)$ for every $a, b \in \Gamma$. The reason φ is interesting is because it translates the elements of Γ into the more familiar language of permutations. This type of function, which acts as a partial dictionary between something mysterious and something familiar, appears throughout mathematics. In group theory, it's called a homomorphism.

Definition. *A function $\varphi : \Gamma \to H$ (both groups) is called a* homomorphism *iff $\varphi(ab) = \varphi(a)\varphi(b)$ for every $a, b \in \Gamma$.*

Thus, an isomorphism is a bijective homomorphism.

We finished lecture by discussing several examples of homomorphisms.

(1) Given groups Γ and H, there always exists a homomorphism $\varphi : \Gamma \to H$; the trivial homomorphism, defined by $\varphi(x) = e_H$ for all $x \in \Gamma$. This is typically neither injective nor surjective.
(2) Given an abelian group Γ, let $\varphi : \Gamma \to \Gamma$ defined by $\varphi(x) = x^2$. This is a homomorphism, which is often nontrivial.
(3) The map $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ defined by $\varphi(n) = [n]$ is a surjective homomorphism, but is not injective.

WWW.MATH.TORONTO.EDU/LGOLDMAK/C01F13/
E-mail address: lgoldmak@math.toronto.edu