Homomorphisms and quotient groups

rctcwyvrn

August 2020

1 Homomorphisms and quotient groups

1.1 Generators and group presentations

We can imagine the subgroup generated by x as x being thrown in a box with itself and shook around. So what if we throw in more elements to be shook together?

Definition: Subsets as group generators

The subgroup generated by a subset S of G, $\langle S\rangle$, is the set of finite productive between elements of S and their inverses.

- $S = [a, b]$, then $\langle S\rangle$ is stuff like $abababa$, $a^5b^3ab^2$, $a^{-1}bab^{-100}$
- If $\langle S\rangle = G$, then S is a **set of generators** for G
- Notation: $\mathbb{Z} = \langle 1\rangle$
- What if we know that x has a special condition? Notation $\mathbb{Z}/100\mathbb{Z} = \langle x|x^{100} = 1\rangle$
- Basically that the group can be generated by any element that has the given property

Example: $\mathbb{Z}$

$\langle 1\rangle = \mathbb{Z}$, because each integer can be written as a bunch of 1's or a bunch of -1's

Definition: Group presentation

We can define a group by a set of generators and **relations** between them. The **group presentation** is that expression

- We can then say that two elements of a group are equal iff you can get from one to the other with the relations.

Example: Dihedral group

The group presentation is

$$D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle .$$

- This defines what the group is by defining the relationships between the generators

Example: Free group

The **free group on n elements** is the group with n generators and no relations.

$$F_n = \langle x_1, x_2, x_3 \ldots \rangle .$$

- Can basically be thought of as arbitrary units being thrown together
- $F_2 = \langle a, b \rangle$ is a bunch of a, b, a^{-1}, b^{-1} thrown together.
- $F_1 = \mathbb{Z}$. Why? Because $\mathbb{Z}$ is just the group made up by adding 1 and -1 to itself a bunch of times

Remark: The same group can have very different presentations, because a generator values can encompass two or more values of another generator set

1.2 Homomorphisms

How can we define relationships between groups that aren't just isomorphisms?

Definition: Homomorphism

For groups $(G, \star)$ and $(H, *)$, A **group homomorphism** is a map $\phi : G \to H$ where $\forall g_1, g_2 \in G$ we have

$$\phi(g_1 \star g_2) = \phi(g_1) * \phi(g_2).$$

- Like a linear map, but over groups instead of vector spaces
- Note the lack of bijection condition, we only need that the group action is respected

Remark: The right way to think about an isomorphism is as a "bijective homomorphism"

Example: Homomorphisms

- All isomorphisms are homomorphisms
- The identity map is a homomorphism
- The **trivial homomorphism** sends everything to 1_H
- From $\mathbb{Z}$ to $\mathbb{Z}/100\mathbb{Z}$ where you just mod everything by 100
- From $\mathbb{Z}$ to itself where you just multiply everything by 10
  - This map is injective, but not surjective
- From permutations S_n to S_{n+1} where you just keep the $n+1$th position constant.
  - Again, injective, but not surjective

Remark: Specifying a homomorphism from $\mathbb{Z} \to G$ is the same as just specifying what the image of 1 is. Because

$$\phi(n) = \phi(1) * \phi(1) \ldots = \phi(1)^n.$$

Remark: The last example shows something important.

To specify a homomorphism $G \to H$, we only have to specify where each generator of G goes. Making sure that the relations are still satisfied (?)

Lemma:

- $G \cong H$ iff there exists homomorphisms st $\phi \circ \psi = id_H$ and $\psi \circ \phi = id_G$
  - Proof: to do later
- Let ϕ be a homomorphism, then $\phi(1_G) = 1_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$
  - Proof for the first one:

$$\phi(g \star 1_G) = \phi(g) * \phi(1_G) \tag{1}$$
$$\phi(g) = \phi(g) * \phi(1_G) \tag{2}$$
$$1_H = \phi(1_G) \tag{3}$$

Definition: Kernel

The **kernel** of a homomorphism is the subset of G that sends values to 1_H

- It also happens to be a (not necessarily proper) subgroup of G, because 1_G is always in the kernel and it is closed
- Notation: kerϕ

Proposition: Kernel determines injectivity

$$\phi \text{ is injective if and only if } \ker\phi = \{1_G\}$$

Example: Kernels

- The kernel of an isomorphism is just 1_G
- The kernel of the trivial homomorphism (sending everything to 1_H is all of G (duh)
- The kernel of the map from Z to the cyclic group of size 100 is $100\mathbb{Z}$, namely all the integer multiples of 100. (Because the mod 100 of the map sends all of them to 0, the identity for the cyclic group
- $\phi : \mathbb{Z} \to G$ by $n \mapsto g^n$. The kernel then depends on g
  - If ord$g = \infty$, then the kernel is just 1
  - If ord$g = a$, then the kernel is $a\mathbb{Z} = \dots a^{-2}, a^{-1}, 1, a, a^2 \dots$

Remark: The image of a homomorphism forms a subgroup as well

1.3 Cosets and modding out