Group theory introduction

Mendel Keller

November 15, 2017

1 Defining things

A group G is a set, equipped with an operation $*$ (for any g and h in G, we have an element $g * h$ of G), and a special element, which we denote 1 satisfying the following properties. For any $g, h, k \in G$:

1. $g * (h * k) = (g * h) * k = g * h * k$
2. $g * 1 = 1 * g = g$
3. $\forall g \in G\ \exists g^{-1} \in G : g * g^{-1} = g^{-1} * g = 1$ (read "for all g in G there exists an element g^{-1} in G such that...")

I will from here on sometimes omit the $*$ and write $g * h$ as gh, as this is more natural. I only used it in the above to be clear about how things are being defined.

We call g^{-1} the *inverse* of g, and 1 is called the *identity* element.

2 Some examples and properties

A few examples of groups are $\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2\ldots\}$ the set of integers, $\mathbb{Q}$ the set of fractions, $\mathbb{R}$ the set of real numbers (where we include things like π,$\sqrt{2}$ and $\sqrt[5]{7}$), and $\mathbb{C}$ the set of complex numbers. In all of these, 1 is equal to 0 and $*$ is addition.

If we want $*$ to be multiplication, in which case 1 would actually be the number 1, we could so this for all the above examples, besides for the integers $\mathbb{Z}$. Because there's no whole number you can multiply 2 by to get to 1, in order to do that we would need fractions, in fact, this is why we have fractions in the first place.

3 Subgroups

An subgroup H of a group G is a subset of G, satisfying the following conditions:

1. $g, h \in H \Rightarrow g * h \in H$
2. $h \in H \Rightarrow h^{-1} \in H$

Or, in English, multiplying elements of a subgroup stays in the subgroup, and inverses stay in the subgroup. One simple thing that we get from this is that $1 \in H$, since we have h^{-1} for every h and $hh^{-1} = 1$. This gives us that H is actually a group, this is why we call it a subgroup, because it's a group in a group.

A special type of subgroup is a *normal subgroup*, this is a subgroup where $gHg^{-1} = H$ i.e. for any group element $g \in G$ and element $h \in H$ the group element ghg^{-1} is also in H.

4 Homomorphism

A group homomorphism is a function $f : G \to H$ from one group to another, satisfying the property that $f(gh) = f(g)f(h)$. This immediately gives us that $f(1) = 1$, a homomorphism takes the identity to the identity. Similarly $f(g^{-1}) = f(g)^{-1}$, a homomorphism takes inverses to inverses.

The *image* of a homomorphism $Im(f)$ is the set of elements in H such that there's an element $g \in G$ with $f(g) = h$. This is a subgroup of H. The set $Ker(f)$ of elements in G mapping to 1 in H is called the kernel of of f.

Theorem 1. *For any homomorphism, $Ker(f)$ is normal subgroup.*

Proof. We first show that it is a subgroup. Firstly, $f(1) = 1$ because we have that $f(g) = f(1g) = f(1)f(g)$ so that multiplying on the left by $f(g)^{-1}$ we get that $f(1) = 1$ so this gives that $1 \in Ker(f)$. We also have that if $g \in Ker(f)$ then $1 = f(1) = f(gg^{-1}) = f(g)f(g^{-1}) = 1f(g^{-1}) = f(g^{-1})$ so that $g^{-1} \in Ker(f)$ as well. Lastly, if $g, h \in Ker(f)$ then $f(gh) = f(g)f(h) = 1 * 1 = 1$ so that $gh \in Ker(f)$.

We now show that it is in fact normal, given $h \in Ker(f)$ and $g \in G$ we have that $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)1f(g^{-1}) = f(g)f(g)^{-1} = 1$ so $ghg^{-1} \in Ker(f)$. ■

5 Quotient group

Given a group G, and a normal subgroup of it H, we can define a quotient subgroup G/H. But first we need to define a *coset*. Given a subgroup H, and an element $g \in G$ the coset gH is the set of group elements expressible as products gh for any element $h \in H$, we write this in set notation as $gH = \{gh : h \in H\}$. If a subgroup is normal, we have that $gH = Hg$ for every element $g \in G$, where Hg is defined analogously, with the order of the products reversed.

We can now, for a normal subgroup H, define the quotient group G/H, defined as the set of cosets of H. Given two such cosets gH and $g'H$, we have that $gHg'H = gg'HH = gg'H$ ($HH = H$ because $1 \in H$ so every h in H can be expressed as a product of 1 and h, we also have that every product of things in H remains in H). This allows the group structure on G/H to be compatible with the group structure of G, in fact, there exists a homomorphism $f : G \to G/H$, given by $f(g) = gH$, this homomorphism has kernel H.