QUOTIENT GROUPS

JACKSON VAN DYKE

I was unhappy with the way I treated quotient groups today, so I am writing this to hopefully correct it.

Let G be a group with subgroup $H < G$. For $g \in G$ define:

$$g \cdot H = \{g \cdot h \,|\, g \in H\} \ .$$

Notice that if $h \in H$, then $h \cdot H = H$. Also notice that $g \cdot H$ is a subgroup for all $g \in G$.

Now consider the following set:

$$G/H = \{g \cdot H \,|\, g \in G\} \ .$$

When we are given a set, we might try to turn it into a group by defining a binary operation on it. Consider the following operation:

$$(g_1 H) \cdot (g_2 H) = (g_1 \cdot g_2) \, H \ .$$

Question 1. When does this binary operation define a group structure? I.e. what are the conditions on H which make G/H into a group?

Example 1. Let $G = \mathbb{Z}$ and

$$H = 2\mathbb{Z} = \{2, 2+2, 2+2+2, \ldots\} = \{2n \,|\, n \in \mathbb{Z}\} \ .$$

Then

$$\mathbb{Z}/2\mathbb{Z} = \{N + (2\mathbb{Z}) \,|\, N \in \mathbb{Z}\}$$

since the binary relation $\cdot$ is $+$ here. Let's given an example of an object of this set. Well we get one for every N, so let's try $N = 0$. This gives us:

$$0 + (2\mathbb{Z}) = \{0 + m \,|\, m \in 2\mathbb{Z}\} = \{0 + 2n \,|\, n \in \mathbb{Z}\} = \{2n \,|\, n \in \mathbb{Z}\} = 2\mathbb{Z} \ .$$

Now let's try $N = 1$. This gives us

$$\begin{aligned} 1 + 2\mathbb{Z} &= \{1 + m \,|\, m \in 2\mathbb{Z}\} = \{1 + 2n \,|\, n \in \mathbb{Z}\} = \{\ldots, -3, -1, 1, 3, 5, \ldots\} \\ &= \{\text{odd integers}\} \ . \end{aligned}$$

So this is a distinct subset of $\mathbb{Z}$. I.e. we have two elements of $\mathbb{Z}/2\mathbb{Z}$ so far. Now let's try $N = 2$. This gives us

$$2 + 2\mathbb{Z} = \{2 + m \,|\, m \in 2\mathbb{Z}\} = \{2 + 2n \,|\, n \in \mathbb{Z}\} = \{2n \,|\, n \in \mathbb{Z}\} = 2\mathbb{Z} \ .$$

So we did not get a new subgroup. This is exactly equal to what we got for $N = 0$.

Exercise 1. Do this for $N = 3$.

Date: February 12, 2020.

You will find that $N = 3$ defines the same subgroup as $N = 1$. So we discovered that as a set

$$\mathbb{Z}/2\mathbb{Z} = \left\{ \underbrace{2\mathbb{Z}}_{=0+2\mathbb{Z}}, 1 + 2\mathbb{Z} \right\} \cong \{0, 1\} \ .$$

Now we can check that the binary operation holds and satisfies the group axioms. For example:

$$(2\mathbb{Z}) \cdot (1 + 2\mathbb{Z}) = (0 + 1) + 2\mathbb{Z} = 1 + 2\mathbb{Z} \ .$$