

# MAT301H5Y

## Week 6 Lecture 2: Cosets

Thursday Jun 15th, 2023

4-5pm instructed by Marcu-Antone Orsoni

### Overview

We went over an example regarding inner automorphisms in class. However, most of the lecture was related to the topic of cosets. To avoid confusion, let  $\text{Id} : G \rightarrow G$  be the identity automorphism and  $\epsilon \in G$  be the identity element of group  $G$  unless specified otherwise.

### Example where $\text{Inn}(D_n)$ not equal to $\text{Aut}(D_n)$

We covered an example in the previous class regarding the cases where  $\text{Inn}(G) \prec \text{Aut}(G)$  and this is the continuation of that example. We want to show the following.

**Example: Showing  $\text{Inn}(D_n)$  not equal to  $\text{Aut}(D_n)$**

Consider  $D_n$  for odd  $n$  and  $n > 3$ . Show that  $\text{Inn}(D_n) \prec \text{Aut}(D_n)$ . You may use without proof that  $|\text{Aut}(D_n)| = n\phi(n)$  [where  $\phi$  is the euler totient function].

*Solution:*

Consider the special homomorphism discussed in the previous lecture defined as  $\Phi : G \rightarrow \text{Aut}(G)$  where  $g \rightarrow \phi_g$  (where  $\phi_g(x) = gxg^{-1}$ ). We'll take this homomorphism for  $\Phi : D_n \rightarrow \text{Aut}(D_n)$ . We learned as a proposition last class that  $Z(G) = \ker(\Phi)$ , observe that  $Z(D_n) = \{\epsilon\} = \ker(\Phi)$  as  $n$  is odd (basically there is only one center element, this result is an exercise in the course notes).

Since the kernel is trivial, we may conclude that  $\Phi$  is injective. Knowing that the image is inner automorphisms of  $D_n$  ( $\text{Im}(\Phi) = \text{Inn}(D_n)$ ). We conclude that it is *bijective* to  $\text{Im}(\Phi)$  and thus an isomorphism between  $D_n$  and  $\text{Inn}(D_n) \iff D_n \cong \text{Inn}(D_n)$ .

We learned in class that  $|D_n| = 2n$ , since it is isomorphic to  $\text{Inn}(D_n)$ , we conclude that  $|\text{Inn}(D_n)| = |D_n| = 2n$ . Knowing that  $|\text{Aut}(D_n)| = n\phi(n)$  and that  $n > 3$ , the following inequality holds

$$\begin{aligned} |\text{Aut}(D_n)| &= n\phi(n) > 2n = |\text{Inn}(D_n)| \\ \iff |\text{Aut}(D_n)| &> |\text{Inn}(D_n)| \\ \implies \text{Aut}(D_n) &\succ \text{Inn}(D_n) \end{aligned}$$

Realize that the inequality  $n\phi(n) > 2n$  arises from the fact that  $\phi(n) > 2$  for  $n > 2$  as per the nature of the euler totient function.

After this we moved on to cosets which should be chapter 6 in the course notes.

### Cosets

### Definition: Coset

Suppose  $G$  is a group and  $H \preceq G$ . The types of cosets are as below:

- **Left cosets:** all the left cosets are defined as  $aH = \{ah : \forall h \in H\}$  for all  $a \in G$
- **Right cosets:** all the right cosets are defined as  $Ha = \{ha : \forall h \in H\}$  for all  $a \in G$ .
- **Conjugation:** all conjugation sets are defined as  $gHg^{-1} = \{ghg^{-1} : \forall h \in H\}$  for all  $g \in G$

*Remark:* Note that above we describe *all* possible cosets. While if you just take a single element  $a$ , a possible left coset of some  $H \preceq G$  is  $aH = \{ah : \forall h \in H\}$ .

### Additional remarks

- We sometimes use the addition symbol for cosets for subgroups have operation is standard addition. In other words, if the operation for a subgroup  $H$  is addition and  $g \in G$ , then we write  $gH = g + H = \{g + h : \forall h \in H\}$ .
- Observe that if  $G$  is abelian then  $aH = Ha$  for all cosets.
- The notation  $n\mathbb{Z}$  is *not* a coset notation
- $aH$  is a subgroup if and only if  $a \in H$

### Proposition: Equivalence relation of cosets

Define the relations  $\overset{r}{\sim}, \overset{l}{\sim}$  as right and left coset relations respectively on  $G$  for some subgroup  $H \preceq G$  as below:

$$\begin{aligned}x \overset{r}{\sim} y &\iff y \in xH \iff x^{-1}y \in H \\x \overset{l}{\sim} y &\iff y \in Hx \iff xy^{-1} \in H\end{aligned}$$

From the properties of equivalence relations, we define the notations for the given equivalence relations as below:

- $G / \overset{l}{\sim} = H \backslash G$  is defined as all the possible equivalence classes induced by the left coset relation. This tells us that  $xH$  forms a partition on  $G$  for all  $x \in G$ . In other words,  $[a]_l \in G / \overset{l}{\sim}$  where  $[a]_l = aH$
- $G / \overset{r}{\sim} = G / H$  is defined as all the possible equivalence classes induced by the right coset relation. This tells us that  $Hx$  forms a partition on  $G$  for all  $x \in G$ . In other words,  $[a]_r \in G / \overset{r}{\sim}$  where  $[a]_r = Ha$

*Remark:* The reader is encourage to see other properties of cosets in proposition 6.3 in the course notes. However, the instructor remarked that a lot of the properties listed followed from the fact that the cosets induce an *equivalence* relation and those have nice properties.

### Additional remarks

- In general  $aH \neq Ha$
- If  $aH \neq bH$ , then  $aH \cap bH = \emptyset$  (because of partitions). However, it is not necessary that as a result,  $aH \cap Hb = \emptyset$

We then covered an example in class regarding cosets considering the subgroups of  $\mathbb{Z}$ .

### Example: coset relation on $\mathbb{Z}$ with $n\mathbb{Z}$ subgroups

Observe how congruence modulo relation relates to cosets of  $\mathbb{Z}$  with the subgroup  $n\mathbb{Z}$

#### *Solution*

Taking our group  $G = \mathbb{Z}$  and  $n\mathbb{Z} \leq \mathbb{Z}$  for non-negative  $n$ . Knowing that  $\mathbb{Z}$  is abelian, we see that  $a + n\mathbb{Z} = n\mathbb{Z} + a$  for all  $a \in \mathbb{Z}$ . Therefore, consider our relation on  $\mathbb{Z}$  we see that for any  $x, y \in \mathbb{Z}$  that  $x \overset{r}{\sim} y \iff x \overset{l}{\sim} y \iff xy^{-1} \in n\mathbb{Z} \iff x - y \in n\mathbb{Z}$ . By definition of  $n\mathbb{Z}$ , we see that  $x - y \in n\mathbb{Z} \iff n|x - y$ . Using our modulo relation, this means that  $x \equiv y \pmod{n}$ .

*Remark:* it is now in the course where we finally realize that  $\mathbb{Z}/\overset{r}{\sim} = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ . All we are doing is partitioning  $\mathbb{Z}$  into it's equivalence classes on congruence modulo  $n$  when constructing  $\mathbb{Z}_n$ .