MAT301H5Y

Week 1 Lecture 2: Introduction to binary operators and groups

Thursday May 11th, 2023

4-5pm instructed by Marcu-Antone Orsoni

Overview

The 2 main topics covered in this lecture were binary operations, groups and abelian groups along with examples for each. Below are some reminders on what were covered in the previous class about equivalence classes on the modulo equivalence relation.

Reminders

Consider the congruence modulo relation $\sim$ on $\mathbb{Z}$ where $a \sim b \iff a \equiv b \pmod{n}$. This is indeed an equivalence relation, all the equivalence classes induced by $\sim$ are given as below:

$$\mathbb{Z}_k = \{[0], [1], [2], \ldots, [k-1]\}$$

Remark: keep in mind that an element in $\mathbb{Z}_k$ is a set itself. Therefore, $\mathbb{Z}_k$ is a set of sets.

An alternative notation to denote the set of all equivalence classes of an equivalence relation $\sim$ on a set A is given by the set $A/\sim$(note that $\sim$ could be any arbitrary equivalence relation on A and not necessarily the one defined above on congruence modulo). We therefore realize from the above congruence modulo relation that $\mathbb{Z}_k = \mathbb{Z}/\sim$. Below we begin to get into the definition of a binary operation on a set.

Binary operator

Definition: binary operation

Given a non-empty set G, a binary operation for G is a map $G \times G \to G$. If the symbol to denote the binary operation is $\cdot$ then we write the set G equipped with binary operation $\cdot$ as $(G, \cdot)$. Applying this binary operation on two elements $a, b \in G$ can be denoted by $a \cdot b$ in this case.

Remark: As one might notice, binary operations over a set need not commute(for example, $(\mathbb{Z}, -)$ equipped with the standard subtraction binary operator). If we define a binary operator on G such as $(G, \cdot)$ within a context, we sometimes write $a \cdot b$ as ab for concision. Although this is not advised when dealing with multiple operations.

There's also the notion of an operation to be *well defined*. When we are dealing with binary operators, they must be well-defined. This means that the operator must be closed. In other words, if $a, b \in (G, \cdot)$ then $a \cdot b \in G$. This may seem obvious from the definition of a binary operators codomain(which is G) but it's a fact to be careful about. Some examples concerning well defined binary operators are below.

Examples: well defined-ness of binary operators

Some examples of well defined operators:

- Addition($+$) for sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, for example $(\mathbb{N}, +)$ is well defined because sum of two natural numbers is still a natural number
- Multiplication($\times$) for sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, for example $(\mathbb{Q}, \times)$ is well defined because the product of two rational numbers is still rational.

Some examples of non-well defined operators:

- $(\mathbb{N}, -)$ for standard subtraction is not well defined because $1 - 2 \notin \mathbb{N}$(however, $(\mathbb{Z}, -)$ is well defined).
- $(\mathbb{Q}, \div)$ for standard division is not well defined as $1 \div 0$ is not defined(however, $(\mathbb{Q}\backslash\{0\}, \div)$ is indeed well defined).

We now move on to groups.

Groups

The definition of a group is as below(note that the use of $+$ and $\times$ as binary operators in these notes denote standard addition and multiplication respectively unless specified otherwise):

Definition: group

A non empty set G equipped with a binary operation $\cdot$ written as $(G, \cdot)$ is a group if it has all of the following properties:

1. **Associativity**: $(ab)c = a(bc)\ \forall a, b, c \in G$
2. **Identity**: There exists an identity element $e \in G$ such that $ae = ea = a\ \forall a \in G$
3. **Inverse**: For every element in $a \in G$ there exists an element $b \in G$ such that $ab = ba = e$

Remark: Although it is not explicitly stated, when proving a set is indeed a group over a binary operation, one must verify that the operation is well defined as one of steps in the proof. Below is a notational remark talked about in lecture:

Remark: shorthand notation

Some shorthand notations for sets are as follows:

- A^* is the set A without 0, in other words: $A^* = A\backslash\{0\}$ ($(Q^*, \times)$ for example is a well defined binary operation)
- $A^\times$ is the set A without any non invertible elements.

A few examples of groups and non-groups are below:

Examples: groups

Below are some examples of groups:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$

Below are some examples of non-groups and the reason why:

- $(\mathbb{Q}, \times)$ is not a group as the element 0 does not have an inverse, however $(Q^*, \times)$ is indeed a group
- $(\mathbb{N}, +)$ is not a group as it doesn't have an identity not does every element have an inverse.

We then moved on to abelian groups. A group is said to be **Abelian** if it's binary operator commutes. That is $(G, \cdot)$ is said to be an abelian group if $a \cdot b = b \cdot a$ for all $a, b \in G$. Examples of non abelian groups are covered in the course notes. However, it was left as an exercise to show the following group is indeed abelian:

Exercise: abelian group

Consider the set $\mathbb{Z}_n$ defined with the following binary operation $(+)$ as below:

$$[a] + [b] = [a + b] \ \forall a, b \in \mathbb{Z}$$

Show that $(\mathbb{Z}_n, +)$ is an abelian group.

Remark: When it comes to proving equivalence classes being groups or abelian groups, we must ensure that the representation of an element does not affect the result of the binary operation. For example, in $\mathbb{Z}_{10}$, $[1] = [11]$ but $1 \neq 11$, we must therefore ensure that this change in representation does not affect the binary operation.

To formalize this idea, we must ensure for a relation $\sim$ on A that for any $[a] = [a'], [b] = [b']$ in $A/\sim$ defined for an operator $(+)$, the following equality holds for $(A/\sim, +)$:

$$[a'] + [b'] = [a] + [b]$$