MAT301H5Y

Week 2 Lecture 1: Subgroups and order

Tuesday May 16th, 2023

3-5pm instructed by Marcu-Antone Orsoni

Overview

This 2 hour lecture recapped a few groups covered in the previous class but also introduced subgroups, ways to prove a subset is a subgroup, center/centralizer/normalizer and also the definition of order. There were plenty of examples of groups and subgroups covered in today's lecture.

Recap/reminders

Last time we covered Abelian groups, we also were introduced to the following special Abelian group denoted by $U(n)$.

Special Abelian group: $U(n)$

The abelian group $U(n)$ is defined below under modulo product($[a][b] = [ab] \quad a, b \in \mathbb{Z}\_n$):

$$\begin{aligned} U(n) &= \{[a] \in \mathbb{Z}_n : \exists x \in \mathbb{Z} \text{ where } [a][x] \equiv [1] \mod n\} \\ &= \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\} \end{aligned}$$

Note that usually seeing why the second definition using gcd is the same as the previous definition is not easy. Therefore, I've chosen to provide a proof of this fact is given as below:

Proof:

Assume that $\gcd(a, n) = 1$ for $a \leq n$. Using Bezout's lemma we know there exists integers k, m such that the following holds true:

$$ak + mn = \gcd(a, n) = 1$$

Re-arranging we get:

$$\begin{aligned} ak + mn = 1 &\implies mn = 1 - ak \implies n|(1 - ak) \\ &\iff ak \equiv 1 \mod n \text{ (By definition of congruence modulo)} \end{aligned}$$

Which is equivalent to the previous definition of $U(n)$.

■

There was an exercise provided in class regarding on determining whether a set under a binary operation is a group. The exercise with the solution is given as below:

Exercise: Group or not a group

Consider the following set:

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}) : ad = 0 \right\}$$

Is $(G, +)$ under usual matrix addition a group?

Solution:

$(G, +)$ is not a group. The reason for this is that G is not closed under its operation. Consider the following matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in G$$

However, we see that their sum is not in G

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin G$$

That is because in this case $ad = 1 \cdot 1 = 1 \neq 0$ and thus not in G. Therefore, G is not a group.

We also covered an example of a group which is commonly seen in mathematics called $GL(n, \mathbb{R})$.

Example: GL matrix group

The following set is a group under standard matrix multiplication.

$$GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$$

Which can be summarized as the gruop of matrices that are invertible with real entries/coefficients.

Subgroups

We now move on to subgroups. The basic definition of a subgroup H is a subset $H \subseteq G$ which is also a group under the operation of G. This is denoted by $H \preceq G$. The complete definition is as below

Definition: Subgroup

A non empty subset $H \subseteq G$ is a subgroup of G if it satisfies the following:

- **Closure under binary operation**: Its elements must be closed under the same binary operation. $a, b \in H \implies ab \in H$ for any a, b.
- **Closure under inverses**: Its inverse under G must also be in H. $b \in H \implies b^{-1} \in H$ for any $b \in H$.

Remark: A consequence of H being a subgroup of G is that they both will share the same identity element. The proof of this is given as below. Let e_H be the identity element of H and e_G be the identity element of G, also note that $(e_H)^{-1G}$ is the inverse of e_H in G(since $H \preceq G$). We want to show that $e_H = e_G$. *Proof:*

We know trivially the following is true:

$$e_H e_H = e_G$$

After doing some manipulation we get

$$\begin{aligned} & e_H e_H (e_H)^{-1G} = e_H (e_H)^{-1G} \\ \implies & e_H e_G = e_G \\ \implies & e_H = e_G \end{aligned}$$

Which is what we needed to show, thus subgroups share the same identity of the larger group.

■

There is a shorter way to prove that a subset is indeed a subgroup. This is written in the course notes as proposition 2.21. It is as follows:

Proposition 2.21(course notes)

A non-empty subset $H \subseteq G$ is a subgroup of G if the following holds for any $a, b \in H$:

$$a, b \in H \implies ab^{-1} \in H$$

The proof of this proposition is not covered in class but can easily found in the course notes as proposition 2.21 for anyone curious.

There are some examples of other subgroups in class which are seen in mathematics. These are subgroups of $GL(n, \mathbb{R})$ as earlier:

Examples: subgroups of

The following sets are subgroups of $GL(n, \mathbb{R})$:

- $O(n, \mathbb{R})$ = set of orthogonal matrices = $\{A \in M_n(\mathbb{R}) : A^{-1} = A^T\}$.
- $SL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}$
- $SLO(n, \mathbb{R}) = O(n, \mathbb{R}) \cap SL(n, \mathbb{R})$

Consider below some properties of subgroups which was left as an exercise to the reader in class.

Properties of subgroups

Suppose $H, K \preceq G$ for some group G, below are some properties covered in class to prove:

- $H \cap K \preceq G$
- if $HK = \{hk : h \in H, k \in K\}$ is abelian then $HK \preceq G$

Center,centralizer and normalizer

Later in the lecture we covered these special subsets of G.

Definitions: center/centralizer

- **Center**: The center of G given by $Z(G)$ is as follows:

$$Z(G) = \{g \in G : gx = xg, \forall x \in g\}$$

  Which can be summarized as the subset of all elements in G that commute with every other element of G.

- **Centralizer:** given some element $a \in G$, the centralizer on a denoted by $C_G(a)$ is given as below:

$$C_G(a) = \{g \in G : ag = ga\}$$

- **Subgroup centralizer**: Given a subgroup $H \preceq G$, we have a subgroup centralizer denoted by $C_G(H)$ as below:

$$C_G(H) = \{g \in G : hg = gh, \forall h \in H\}$$

  Which can be summarized as all the elements in G that commute with all elements of H.

Remarks: All the above subsets are indeed subgroups of G. The proof of center $Z(G)$ being a subgroup of $C_G(H)$ was done in class. Another subgroup known as the normalizer will be covered later in the course as mentioned by the instructor. However, its definition can be found above Theorem 2.27 in the course notes for a normalizer. The proof for $Z(G) \preceq C_G(H)$ is given as below.

Proof:

First let's show that $Z(G) \subseteq C_G(H)$ is a non-empty subset. We see that $e \in Z(G)$ and therefore is non-empty(because e commutes with all elements in G). The subset proof is as below:

$$\begin{aligned} g \in Z(G) &\implies \forall x \in G, gx = xg \\ &\implies \forall h \in H, gh = gh \text{(Using the definition from above)} \\ &\implies g \in C_G(H) \\ &\iff Z(G) \subseteq C_G(H) \end{aligned}$$

Moving on to the properties of a subgroup:

- **Closure under operation**: Let $a, b \in Z(G)$ observe that for any $x \in G$ that $abx = axb = xab$(due to commutativity) thus $ab \in Z(G)$.

- **Closure under inverses**: Let $a \in Z(G)$, we see that for any $x \in G$ that $ax = xa \implies x = a^{-1}xa \implies xa^{-1} = a^{-1}x \implies a^{-1} \in Z(G)$

Therefore, by definition, we observe that $Z(G) \preceq C_G(H)$.

■

Order

We briefly touched upon the definition of order with an example worked out in class.

Definition: Order

Order is classified into two kinds, order of a group and order of an element in a group given as below:

- **Order of a group**, the order of a group G denoted by $|G|$ is the number of elements in G. If it is infinite(countable or not), the order is simply infinite and denoted by $|G| = \infty$.
- **Order of an element** let $a \in G$ for some group G. The order of a denoted by $|a|$ is the smallest positive integer k such that $a^k = e$. where a^k is the operation applied on a a total of k times or $aaa \cdot a$ k times. If no such k exists we say that the order $|a|$ is infinite or $|a| = \infty$

Remark: One must remember that the order of $a \in G$ is the *smallest* integer k and thus we see that if $|a| = k$ is finite then $a^{nk} = e$. If we know that $a^m = e$ but are not sure if m is the smallest positive integer then we can claim safely that $|a| \leq m$. It is left as an exercise to realize that $|a| \Big| m$ in this case. If $|G| = 1$ for some group G, it is called the trivial group containing only the identity $G = \{e\}$.

We did an example in class for order computation. The exercise is as below with the solution following it.

Exercise: order computation

Find $|U(10)|$ and the order of all of its elements.

Remark: there is a fairly useful and well known function in mathematics called the euler totient function $\Phi(n)$ which counts the number of positive integers that are coprime to n. It is left as an exercise to the reader to realize why $|U(n)| = \Phi(n)$. There is a piazza post(as of writing these notes) which has the solution in case stuck.

Solution:

Let us first find $U(10)$, this is the same as the set of equivalence classes which are coprime to 10. We see that $U(10)$ is the following:

$$U(10) = \{[1], [3], [7], [9]\}$$

and thus $|U(10)| = 4$ from counting. We now need to find the orders of all of its elements, 2 elements are shown in the solution while the others follow from the same method. Note that the identity element is [1] in our set $U(10)$. Finding $|[1]|$ we see that $1 \equiv 1 \mod 10$ by default thus we don't need to raise it to the power of anything, we thus see that $|[1]| = 1$.

Computing $|[3]|$: we need to find the smallest k such that $[3]^k = [1]$, doing it below:

$$\begin{aligned} & 3 \equiv 3 \mod 10 \\ \implies & 3^2 \equiv 9 \equiv -1 \mod 10 \\ \implies & 3^4 \equiv (-1)^2 \equiv 1 \mod 10 \end{aligned}$$

We can stop there seeing that $[3]^4 = [1]$ therefore $|[3]| = 4$. Similarly doing the procedure we get $|[7]| = 4, |[9]| = 2$.

Remark: Realize that the orders of elements in $U(n)$ divide the overall order of $U(n)$. For example $|[7]| = 4 \Big| |U(n)| = 4$ and so on for the other elements. This is a property we will study deeper in later lectures.