MAT301H5Y

Week 2 Lecture 2: Generators

Thursday May 18th, 2023

4-5pm instructed by Marcu-Antone Orsoni

Overview

In this class we revised a few topics about order and were introduced to generators which are a special kind of subgroup.

Generators

A generator is a special kind of subgroup. In fact, we proved that the generator is a subgroup in class

Definition: Generator

Suppose we have a non-empty subset $A \subseteq G$, the subgroup generated by G is given by A is given by the following set:

$$\langle A \rangle = \{a_1^{n_1} a_2^{n_2} \dots a_n^{n_m} = \prod_{i=1}^{m} a_i^{n_i} | m \in \mathbb{N}, n_i \in \mathbb{Z}, a_i \in A\}$$

We call $\langle A \rangle$ the generator of A. $\langle A \rangle$ is a subgroup and a proof of this fact is given as below.

Remark: For the product above, the elements $a_1, a_2, a_3 \dots$ need not be distinct. Also recall that $a^k = aa \dots a$ a total of $k \in \mathbb{N}$ times and $a^{-k} = (a^k)^{-1}$

Proof: Wish to show that $\langle A \rangle$ is a subgroup of G.

Assume that $A \subseteq G$ as per the definition above. We prove each property of a subgroup below:

- $\langle A \rangle \subseteq G$: this fact is trivial
- $\langle A \rangle \neq \emptyset (\langle A \rangle$ is non-empty): Choose some $x \in A$, let $a_1 = a_2 = x$, and choose $n_1 = 1, n_2 = -1$. We see from this that from the definition of $\langle A \rangle$:

  $$a_1^{n_1} a_2^{n_2} = x^1 x^{-1} = x x^{-1} = e \in \langle A \rangle$$

  Which shows that $\langle A \rangle$ is indeed non-empty.
- Closure and inverses: Let us try and use proposition 2.21 from the course notes and prove closure. Let $a \in \langle A \rangle \iff a = \prod_{i=1}^{m} a_i^{n_i}$ and $a \in \langle A \rangle \iff b = \prod_{i=1}^{m} b_i^{k_i}$. Taking the inverse of b and multiplying with a we see:

  $$ab^{-1} = \prod_{i=1}^{m} a_i^{n_i} \left(\prod_{i=1}^{m} b_i^{k_i} \right)^{-1} = \prod_{i=1}^{m} a_i^{n_i} \prod_{i=1}^{m} b_{m-i}^{-k_{m-i}}$$

  (In case confused, the product changed to $m - i$ because when you apply the inverse, you have to reverse the order of the operation on the group). We see the product above is an arbitrary product of elements in A and thus we can conclude that $ab^{-1} \in \langle A \rangle$. By proposition 2.21 we can conclude that it is closed under inverses and the operation.

From the properties above we may conclude that $\langle A \rangle$ is indeed a subgroup of G.

■

Using the definition of a subgroup, we'll see there are some interesting properties of this subgroup. These properties are summarized in the propositions below:

Proposition: properties of a generator

Let A be a non-empty subset of G. $\langle A \rangle$ has the following properties:

(1) $\langle A \rangle$ is the smallest subgroup containing A. This means that for any $A \subset H \preceq G$, $\langle A \rangle$ must be in H or $\langle A \rangle \subseteq H$

(2) $\langle A \rangle = \bigcap_{H \preceq G, A \subseteq H} H$. In other words, $\langle A \rangle$ is the intersection of all possible subgroups(H) of G such that A is in that subgroup($A \subseteq H$).

Proof for (1):

Suppose that $H \preceq G$, let $A = \{a_1, a_2 \dots a_m\} \subset H$. Realize that if you choose $x \in \langle A \rangle$ we have $x = \prod_{i=1}^{m} a_i^{n_i}$ which is closed under H because it is a subgroup. In other words, x is an arbitrary combination of the elements of A under the operation of G which is guaranteed to be closed under H due to it being a subgroup. Therefore $x \in \langle A \rangle \implies x \in H \iff \langle A \rangle \subseteq H$.

■

Proof for (2):

Since this is an equality of sets, we need to show both directions under inclusion(i.e double inclusion). So, we need to show that $\langle A \rangle \subseteq \bigcap_{H \preceq G, A \subseteq H} H$ and $\langle A \rangle \supseteq \bigcap_{H \preceq G, A \subseteq H} H$

- ($\subseteq$): This direction follows directly from the previous proof of $\langle A \rangle$ being the smallest subgroup containing A. Since $\langle A \rangle \subseteq H$ for *all* $H \preceq G$ containing A, we see that $\langle A \rangle \subseteq \bigcap_{H \preceq G, A \subseteq H} H$
- ($\supseteq$): Similar to the previous proof, if we take all the possible subgroups containing A and take their intersection, we see that we have all possible combinations of elements(under the operation) of A in H(because H is a subgroup). However, this means that by definition, these combinations mean that an element in $\bigcap_{H \preceq G, A \subseteq H} H$ must be in $\langle A \rangle$ therefore we conclude that $\bigcap_{H \preceq G, A \subseteq H} H \subseteq \langle A \rangle$.

We therefore see by double inclusion that $\langle A \rangle = \bigcap_{H \preceq G, A \subseteq H} H$.

■

We also have covered some examples of singleton generators their definition is as below:

Example: singleton generators

Suppose we fix some $a \in G$ we can take the generator of this single element as $\langle \{a\} \rangle$ which we can denote with $\langle a \rangle$. Using the definition of a generator we see that:

$$\langle a \rangle = \{a^i | i \in \mathbb{Z}\} = \{\dots a^{-2}, a^{-1}, e, a, a^2, a^3 \dots\}$$

It was also left as an exercise to the reader to verify that if $A \preceq G$ then $\langle A \rangle = A$.
We ended the class by connecting singleton generators to the order of the elements. We started by going over a theorem regarding order of an element and distinct elements:

Theorem: order and distinct elements

Let $a \in G$

- $|a| = \infty \implies a^i = a^j \iff i = j$
- $|a| = n < \infty \implies a^i = a^j \iff i \equiv j \mod n$

If we have the second case above the following generator has distinct elements:

$$\langle a \rangle = \{e, a, a^2 \dots a^{n-1}\}$$

The proofs for the above theorem were not covered in class, however they are in the textbook. It is encouraged however to try and prove this theorem. A useful hint for the reader is to realize that if $|a| = n$ and $a^k = e$ then $n|k$ for some integers $n \leq k$.