MAT301H5Y

Week 3 Lecture 1: Cyclic groups

Tuesday May 23th, 2023

3-5pm instructed by Marcu-Antone Orsoni

Overview

We had recapped on generators from the previous lecture and were introduced to cyclic groups and their properties.

Recap: Generators

Recap: Generators and properties

Generators:

Suppose we have a non-empty subset $A \subseteq G$, the subgroup generated by G from 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.

Theorem 3.3

Let $a \in G$

(1) $|a| = \infty \implies a^i = a^j \iff i = j$

(2) $|a| = n < \infty \implies a^i = a^j \iff i \equiv j \mod n$

Although last class theorem 3.3 was left as an exercise, the proof was indeed covered in this class and is as below:

Proof for (1):

Assume $|a| = \infty$ this means that $a^k = e \iff k = 0$. Using this fact, let $a^i = a^j$ and after some re-arranging:

$$\begin{aligned} a^i = a^j &\iff a^i a^{-j} = a^j a^{-j} = e \\ &\iff a^{i-j} = e \iff i - j = 0 \text{ [From previous fact]} \\ &\iff i = j \end{aligned}$$

As one can see, these chain of equivalences prove the given statement.

Proof for (2)

Assume $|a| = n < \infty$, from this we realize that $a^k = e \iff n|k$. Let $a^i = a^j$ by re-arranging below we see:

$$\begin{aligned} a^i = a^j &\iff a^i a^{-j} = a^j a^{-j} = e \\ &\iff a^{i-j} = e \\ &\iff n|(i-j) \text{ [From previous fact]} \\ &\iff i \equiv j \mod n \end{aligned}$$

■

An additional consequence of finite order of a generator($|a| = n < \infty$), is the following set equality:

Corollary

Let $|a| = n < \infty$, the following holds true as a result of the previous theorem.

$$\langle a\rangle = \{a^k : k \in \mathbb{Z}, 0 \leq k < n\} = \{e, a, a^2, \dots, a^{n-1}\}$$

Proof:

Assume $|a| = n < \infty$. The reverse inclusion($\langle a\rangle \supseteq \{a^k : k \in \mathbb{Z}, 0 \leq k < n\}$) is trivial by definition of a generator. Consider the forward inclusion below.

Let $x \in \langle a\rangle$. This means that for some $l \in \mathbb{Z}$ $x = a^l$. As per the division algorithm we realize that there exists $0 \leq r < n \in \mathbb{Z}$, $q \in \mathbb{Z}$ such that $l = nq + r$. From this equality it follows that:

$$\begin{aligned} l = nq + r &\implies a^l = a^{nq+r} \\ &\implies a^l = a^{nq}a^r = a^r \text{ [Because } a^{nq} = e \text{ due to } |a| = n] \end{aligned}$$

Since we know that $0 \leq r < n$ from the division algorithm, we see that this fits the definition of our set. Therefore $x \in \langle a\rangle \implies x \in \{a^k : k \in \mathbb{Z}, 0 \leq k < n\} \iff \langle a\rangle \subseteq \{a^k : k \in \mathbb{Z}, 0 \leq k < n\}$. By double inclusion, we conclude indeed that $\langle a\rangle = \{a^k : k \in \mathbb{Z}, 0 \leq k < n\}$

■

We then moved on to cyclic groups, which are special types of groups that connect to single element generators.

Cyclic groups

Definition: Cyclic group

A group G is said to be cyclice if there exists $a \in G$ such that $\langle a\rangle = G$

Consider some examples of finite and infinite cyclic groups.

Example

- $(\mathbb{Z}, +)$ is cyclic and infinite with $\langle \pm 1\rangle = (\mathbb{Z}, +)$.
- $(\mathbb{Z}_n, +)$ is cyclic and finite with $\langle [1]\rangle = (\mathbb{Z}_n, +)$

There was more notation introduced in relation to subgroups of $(\mathbb{Z}, +)$.

nZ notation

Suppose $n \in \mathbb{Z}$, then $\langle n\rangle = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} = \{\cdots - 3n, -2n, n, e, n, 2n, 3n, \dots\}$

Remark: in case it's not clear why $\langle n\rangle$ gives the above subgroup, when it comes to the addition binary operator for $\mathbb{Z}$, then we see that $a^k = a + a + \dots a = ka$ which is why we see that $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. It was left as an execise to the reader to realize that $m\mathbb{Z} \subseteq n\mathbb{Z} \implies n|m$.

Some groups need not be cyclic under a certain binary operation.

Examples of non-cyclic groups

The following groups are examples of non-cyclic groups:

(1) $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$

(2) $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$

(3) $(\mathbb{C}, +)$, $(\mathbb{C}, \cdot)$

Proof:

For (1), choose some $x \in \mathbb{Q}^*$(we exclude $x = 0$ because clearly $\langle 0 \rangle = \{0\} \neq \mathbb{Q}$). The definition of the generator is $\langle x \rangle = \{nx : n \in \mathbb{Z}\}$. We'll see that $\frac{x}{2} \notin \langle x \rangle$ by the following argument.

Observe that by excluding $x = 0$, we see that for $\langle x \rangle, n \neq 0 \implies n = \pm 1, \pm 2, \cdots \implies |n| > \frac{1}{2}$. We use this inequality and multiply both sides by $|x|$, giving us $|n||x| = |nx| > \frac{|x|}{2}$.

This result is important because we conclude from this fact that for all $n \in \mathbb{Z}, nx \neq \frac{x}{2}$. This consequently allows us to conclude that $\frac{x}{2} \notin \langle x \rangle$. Therefore we have shown that for any arbitrary $x \in \mathbb{Q}$ we can find an element such that cannot be generated by the given group with the chosen binary operation. Therefore, we may conclude that $\mathbb{Q}$ is not cyclic under addition. Similar argument can be made for the remaining groups.

■

Remark: For groups $\mathbb{R}$ and $\mathbb{C}$ under addition and multiplication, we can make a simpler argument as to why they are non cyclic. It is not hard to see that generator subgroups are *countable*. Seeing that $\mathbb{R}$, $\mathbb{C}$ are uncountable in terms of cardinality, we can simply argue that generators are countable while $\mathbb{R}, \mathbb{C}$ are uncountable and thus differ in cardinality. A difference in cardinality guarantees that they are different sets. Therefore, we conclude that $\mathbb{R}$, $\mathbb{C}$ are non-cyclic due to this argument. This generalizes for any uncountable group.

In class we also covered some examples of finite cyclic groups and trying to determine generators for that group. We can try and use the property of order to determine these as shown below

Exercise: determining generators for a group

Show that $U(10)$ is cyclic by finding its generators.

Solution: Notice that $|U(10)| = 4$, therefore it is sufficient to find elements a such that $|a| = 4$ We recall from a previous lecture that $|[3]| = |[7]| = 4$ and therefore we may conclude that our generators for this group are $[3], [7]$.

Remark: Is $U(8)$ cyclic? We observed in class that all elements of $U(8)$ are less than $|U(8)|$ which automatically makes it non cyclic. We also covered in class the following proposition relating to the group $U(n)$ being cyclic

Proposition: $U(n)$ being cyclic or non-cyclic

Suppose $n \in \mathbb{N}$, the following conditions are equivalent to $U(n)$ being cyclic:

- $n = p^k$ for some prime p
- $n = 1, 2, 4$
- $2p^k$ for some prime p

The proof of the above proposition was not given in class and the instructor said it is possible for it to show up on an assignment.

There are connections that can be made with the order of a subgroup and it's generator as the below proposition.

Proposition 3.7

Let $a \in G$ with $|a| = n < \infty$ and $k \in Z$. The following holds true.

$$\left\langle a^k \right\rangle = \left\langle a^{\gcd(k,n)} \right\rangle \text{ and } |a^k| = \frac{n}{\gcd(k,n)}$$

Proof:

The proof covered in class in incomplete, however the complete proof can be found in the course notes with the corresponding number. The direction proved in class is $\left\langle a^{\gcd(k,n)} \right\rangle \subseteq \left\langle a^k \right\rangle$.

Assume $x \in \left\langle a^{\gcd(k,n)} \right\rangle$ such that $|a| = n < \infty$ and let $d = \gcd(k,n)$ for short. Using bezout's theorem, knowing thaat $d = \gcd(k,n)$, there exists integers p, q such that $kp + nq = d$. Using this fact below:

$$\begin{aligned} kp + nq = d &\implies a^{kp+nq} = a^d \\ &\implies a^{kp}a^{nq} = a^{kp} = a^d = x \text{ [Because } |a|n \implies a^{nq} = e] \end{aligned}$$

Since $x = a^{kp}$ for some integer p, it follows that $x \in \left\langle a^k \right\rangle$. We may thus conclude that $\left\langle a^{\gcd(k,n)} \right\rangle \subseteq \left\langle a^k \right\rangle$

When it comes to cyclic groups and subgroups, we have a theorem regarding them in general as below:

Theorem 3.10: Fundamental theorem of cyclic groups/subgroups

1. Every subgroup of a cyclic group is cyclic
2. If $|a| = n$ and $H \preceq \langle a \rangle$, then $|H|\Big|n$
3. Suppose $|a| = n$. For all $k \in \mathbb{Z}$ such that $k|n(k$ is a factor or divisor for $n)$. The group $\langle a \rangle$ has exactly one subgroup of order k which is $\left\langle a^{\frac{n}{k}} \right\rangle$.

Remark: This theorem provides a way to find out the finite cyclic subgroups of a cyclic group, namely by their divisors/factors. The proof for this theorem was not covered in lecture. However, it can be found in the course notes under the respective number(3.10). We however covered an example of finding the cyclic subgroups for a group.

Example: finding finite subgroups using theorem 3.10

Find finite cyclic subgroups of the group $\mathbb{Z}_{15}$ under modulo addition with $\langle 1 \rangle$ as the generator.

Solution

For this problem, we can use (3) of theorem 3.10 as mentioned earlier. Here we set $a = [1]$ as specified by the question. We see that $|a| = 15 = n$. We thus can find the factors of 15 and see our possible values of k to be $1, 3, 5, 15$. This gives us a total of 4 cyclic subgroups which we can find as below applying (3) from theorem (3.10):

$$\begin{aligned}
&\left\langle a^{\frac{n}{1}} \right\rangle = \left\langle [1]^{\frac{15}{1}} \right\rangle = \langle [15] \rangle \text{ [Because we see that } [1]^n = [1] + [1] + \cdots + [1] = [n]] \\
&\left\langle a^{\frac{n}{3}} \right\rangle = \left\langle [1]^{\frac{15}{3}} \right\rangle = \langle [1]^5 \rangle = \langle [5] \rangle = \{[0], [5], [10]\} \\
&\left\langle a^{\frac{n}{5}} \right\rangle = \left\langle [1]^{\frac{15}{5}} \right\rangle = \langle [1]^3 \rangle = \langle [3] \rangle = \{[0], [3], [6], [9], [12]\} \\
&\left\langle a^{\frac{n}{15}} \right\rangle = \langle [1] \rangle = \langle [1]^1 \rangle = \langle [1] \rangle = \{[0], [1], \ldots, [14]\}
\end{aligned}$$

Our instructor pointed out in lecture an interesting result connecting $\mathbb{Z}_n$ and $U(n)$. Consider the proposition below:

Proposition: connection between Z_n and $U(n)$

The set of all possible generators of $\mathbb{Z}_n$ are $U(n)$.

Proof:

We want to find all elements $a \in \mathbb{Z}_n$ such that $\langle a \rangle = \langle [1] \rangle = \mathbb{Z}_n$ Notice that since $a = [1]^k$ for some $k \in \mathbb{Z}$ by definition. We are interested in k such that $\left\langle a^k \right\rangle = \langle a \rangle$. Subtituting we get equivalently that we need all k such that $\left\langle [1]^k \right\rangle = \langle [1] \rangle$. By proposition 3.7 we realize that we want $|[1]^k| = n$ which is equal to $|[1]^k| = \frac{n}{\gcd(k,n)} = n \implies \gcd(k, n) = \frac{n}{n} = 1$. This means our k must be co-prime to n. By definition, this means our elements are just all $k \in \mathbb{Z}$ such that $[1]^k = [k]$ is co-prime to n which is the definition of $U(n)$. Therefore, all possible generators of $\mathbb{Z}_n$ are $U(n)$.

■

In addition to what was covered in class, we also have the euler totient function which was introduced towards the end of the lecture which is going to be useful later in the course. Its definition is as below:

Definition: Euler totient function and properties

The euler totient function $\Phi(n)$ defined for $n \geq 2$ computes the total number of numbers from 1 to n that are co-prime to n. Below are some properties of $\Phi(n)$:

- $\Phi(p) = p - 1$ for some prime p
- $\Phi(p) = p^{k-1}(p - 1)$ for some prime p
- $\Phi(ab) = \Phi(a)\Phi(b)$ if a and b are co-prime
- Combining the above 3 we see that if $n \in \mathbb{N}$ such that $n = \prod_{i=1}^{k} p_i^{n_i}$ where p_i are its prime factors:

$$\Phi(n) = \Phi\left(\prod_{i=1}^{k} p_i^{n_i}\right) = \prod_{i=1}^{k} \Phi(p_i^{n_i}) = \prod_{i=1}^{k} p_i^{n_i-1}(p_i - 1)$$