Dillan Marroquin
MATH 331.1001
Scribing Week 6
Due. 4 October 2021

Lecture 13

Classifying Cyclic Groups

Goal: To show that every cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n$ (for a particular n).

Question: Given a group G, can we determine if G is cyclic?
Answer: This is hard to answer in general.

Theorem (13.1)**.** If $|G| = p$ for p prime, then G is cyclic. In particular, $\forall a \in G - \{e\}$, $G = \langle a \rangle$.

Abstract Properties of Cyclic Groups

Idea: If G does NOT have all of these following properties, then G cannot be cyclic. (Note that the converse is M E G A false!)

Proposition (13.2)**.** Every cyclic group is abelian.

Theorem (13.3)**.** Every proper subgroup of a cyclic group is cyclic.

Remark (13.4). The converse of Theorem 13.3 is false.

Lecture 14

The converse of Theorem 13.3 from last lecture is NOT true: If every proper subgroup G is cyclic, it is not guaranteed that G is cyclic. Here are two counter-examples:

1. Consider $S_3 := \{\text{bijections from } \{1,2,3\} \to \{1,2,3\}\}$. The order of S_3 is 6, so by Lagrange's Theorem any proper subgroup of S_3 has order $1, 2$, or 3. For a subgroup $H \leq S_3$ with $|H| = 1$, then $H = \{e\} = \langle e \rangle$ and is cyclic.
   By Theorem 13.1, if $|H| = 2$ or 3, H is cyclic. Therefore every proper subgroup is cyclic, but obviously S_3 is not cyclic since it is not abelian.
2. Now consider $G = \mathbb{Z}/3 \times \mathbb{Z}/3$ with $([a_1],[b_1]) + ([a_2],[b_2]) = ([a_1 + a_2],[b_1 + b_2])$. Then $|G| = 9$. The same argument as above implies that every proper subgroup is cyclic because it must have order 1 or 3. Note G is abelian. We can check by hand that every element of G has order 1 or 3, NOT 9. Therefore G is not cyclic. For example, $3([a],[b]) = (3[a],3[b]) = ([0],[0])$.

Corollary (14.1)**.**

1. Let $H \leq \mathbb{Z} = \langle 1 \rangle$ be a subgroup. Then $\exists m > 0$ such that $H = \langle m \rangle = m\mathbb{Z}$.
2. If $H \leq \mathbb{Z}/m$ is a subgroup, then $\exists [m] \in \mathbb{Z}/n$ such that $H = \langle [m] \rangle = \{[0],[m],[2m],\ldots\}$.

Finding the Order of a Subgroup of a Cyclic Group

Theorem (14.2)**.** Let $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ be a finite cyclic group of order n. Let $a^k \in G$. Then $|a^k| = \frac{n}{\gcd(n,k)}$.

Lemma (14.3)**.** If $G = \langle a \rangle$ has order n and $l \in \mathbb{Z}$, $l > 0$ such that $a^l = e$, then $n | l$.

Lemma (14.4)**.** Given $k, n \in \mathbb{Z} \setminus \{0\}$, let m_k, m_n be unique integers such that $k = dm_k$ and $n = dm_n$, where $d = \gcd(n,k)$. Then $\gcd(m_k, m_n) = 1$.

Lecture 15

Converse to Lagrange's Theorem for Cyclic Groups

Corollary (15.1)**.** If $G = \langle a \rangle$ is a cyclic group of order n and l is a positive divisor of n, then there exists a subgroup $H \leq G$ with $|H| = l$.

Classification of Cyclic Groups

Recall: Let G, H be groups. A function $\Phi : G \to H$ is a group homomorphism iff $\forall x, y \in G$, $\Phi(xy) = \Phi(x)\Phi(y)$. Also, Φ is an isomorphism iff it is bijective and a homomorphism.

Remark. "$\cong$" gives an equivalence relation on the "set" of group implies $G \cong H$ iff $H \cong G$.

Theorem (15.2)**.** If $G = \langle a \rangle$ is a cyclic group of infinite order, then $G \cong \mathbb{Z}$.

Proof. By the above Remark, it suffices to construct a group isomorphism $\Phi : \mathbb{Z} \to G$. Observe that $G = \{a^k | k \in \mathbb{Z}\}$. Define $\Phi(k) := a^k$. To show Φ is a group homomorphism, let $k, l \in \mathbb{Z}$. Then $\Phi(k+l) = a^{k+l} = a^k a^l = \Phi(k)\Phi(l)$.
To show Φ is a bijection, we first prove surjectivity. Consider the image of Φ: $\Phi(\mathbb{Z}) = \{\Phi(k) | k \in \mathbb{Z}\} = \{a^k | k \in \mathbb{Z}\}$. But $\{a^k | k \in \mathbb{Z}\} = G$, so Φ is surjective.
To show Φ is injective, suppose $\Phi(k) = \Phi(l)$. Then $a^k = a^l$ in G which implies $a^k a^l = e$ and thus $a^{k-l} = e$. Since a has infinite order, $a^{k-l} = e$ iff $k - l = 0$. Therefore $k = l$ and Φ is injective. ∎

Theorem (15.3)**.** If $G = \langle a \rangle$ is cyclic order n, then $G \cong \mathbb{Z}/n$.

Looking Ahead: Getting Subgroups from Group Homomorphisms

Definition (15.4)**.** Let $\Phi : G \to H$ be a group homomorphism.

1. The **image** of Φ is the subset of H where $\mathrm{im}\Phi = \{\Phi(x) | x \in G\}$.
2. The **kernel** of Φ is the subset of G where $\ker\Phi = \{x \in G | \Phi(x) = e_H\}$.