MAT301H5Y

Week 3 Lecture 1: Cyclic group theorems proved and subgroup latices

Thursday May 25th, 2023

4-5pm instructed by Marcu-Antone Orsoni

Overview

We went over theorem 3.10 in class and the instructor proved them throughout the lecture and we briefly touched.

Proofs for fundamental theorem of cyclic groups

Theorem 3.10: Fundamental theorem of cyclic groups

1. Every subgroup of a cyclic subgroup is cyclic
2. if $|\langle a \rangle| = n$ and $H \preceq \langle a \rangle$ then $|H| \Big| n$
3. Suppose $|a| = n$. For every $k \in \mathbb{N}$ where $k|n$, tthe group $\langle a \rangle$ has exactly one subgroup of order k namely $\left\langle a^{\frac{n}{k}} \right\rangle$

(1) *Proof*:

Assume group G is cyclic i.e. $G = \langle g \rangle$ for some $g \in G$. If H is the trivial subgroup it is trivial to see it is cyclic. Suppose H is a non-trivial subgroup of G. This means there exists $a \in H \neq e$. Since we know that G is cyclic, there exists $k \in \mathbb{N}$ such that $a = g^k$.

The next step is not very intuitive, define the set $M = \{m \in \mathbb{N} : g^m \in H\}$. This is basically the set of all $m \in \mathbb{N}$ such that g^m is contained within H. Since M is a non-empty subset of the natural numbers(positive integers). This set admits a minimum element which we can call $n \in M$(i.e. $\forall m \in M, n \leq m$).

Furthermore, we realize that $n \in M \implies g^n \in H$ by definition of M and moreover we conclude that $\langle g^n \rangle \subseteq H$(since for some element $x \in H$, $\langle x \rangle$ is the smallest possible subgroup[hence subset] containing x).

Moving forward, choose another element $x \in H \preceq G \implies \exists s \in \mathbb{Z}, x = g^s$ since G is cyclic. Applying euclidian division from s onto n we get $s \div n$ as below for some $q \in \mathbb{Z}$ and $0 \leq r < n \in \mathbb{Z}$:

$$s = nq + r$$

Applying these to our elements we get the following equation.

$$\begin{aligned} x = & g^s = g^{nq+r} \\ \implies & g^s = g^{nq} g^r \\ \implies & g^s g^{-nq} = g^r \end{aligned}$$

Realize that since H is a subgroup, $g^s, g^{nq} \in H \implies g^s g^{-nq} = g^r \in H$ by proposition 2.21($g^{nq} \in H$ due to our definition of n earlier). However, if $r < n$

as per our division algorithm earlier and $g^r \in H$, this means that $r \in M$ and contradicts the minimality of n(because $r < n$). This must mean that $r = 0$. By this observation we see that $x = g^s = g^{nq}$ which means that $x \in \langle g^n \rangle$. To summarize we've demonstrated that $x \in H \implies x \in \langle g^n \rangle \iff H \subseteq \langle g^n \rangle$. Since the other direction is trivial, we conclude that $H = \langle g^n \rangle$ and therefore conclude that H is cyclic.

■

(2) *Proof*:

Assume that $|\langle a \rangle| = n$. Since $\langle a \rangle$ is cyclic, applying theorem 3.10 part (1) we know that any subgroup is cyclic of $\langle a \rangle$. Suppose that $H \preceq \langle a \rangle$, we know H is cyclic and finite. This means there exist $h \in H$ where $\langle h \rangle = H$. We can then apply corollary 3.8 which states that any element of a cyclic subgroup has an order which divides the order of the group. This means that $|H| = |\langle h \rangle| = |h| \Big| \langle a \rangle$. This is just equivalent to $|H| \Big| \langle a \rangle$.

■

(3) *Proof*:

Assume that $|a| = n, k|n \iff k = mn$ for some integer m. We observe that $a^{\frac{n}{k}} = a^m \in \langle a \rangle \implies \langle a^m \rangle \subseteq \langle a \rangle$. From this, we can apply proposition 3.7 which states that if $|a| = n$ then for any $s \in \mathbb{Z}$, it follows that $\langle a^s \rangle = \left\langle a^{\gcd(s,n)} \right\rangle$ and $|a^s| = \frac{n}{\gcd(n,s)}$.

Using this proposition, we notice that $k = mn \implies k|n$ and $m|n$. Since, $m|n$ it is trivial that $\gcd(m, n) = m$. Applying the proposition we see that. $|\langle a^m \rangle| = |a^m| = \frac{n}{\gcd(n,m)} = \frac{n}{m} = k$. We have demonstrated that the order of $\left\langle a^{\frac{n}{k}} \right\rangle$ is k.
We now need to prove uniqueness of such a subgroup. Assume that $H \preceq \langle a \rangle$ and $|H| = k$ such that $k|n$. Realize by theorem 3.10 part 1 that H must be cyclic. This means that there exists s such that $\langle a^s \rangle = H$. Re-applying proposition 3.7 and as per our assumptions we see that:

$$H = \langle a^s \rangle = \left\langle a^{\gcd(s,n)} \right\rangle \implies k = |H| = \frac{n}{\gcd(s, n)}$$

From this we conclude that $\gcd(s, n) = \frac{n}{k}$. Therefore we see that $H = \langle a^s \rangle = \left\langle a^{\gcd(s,n)} \right\rangle = \left\langle a^{\frac{n}{k}} \right\rangle$. We have thus also shown uniqueness.

■

Subgroup lattices

Since for the moment it is challenging to construct drawings in latex, it is recommended to check the first few examples of chapter 3.3 as the same example was covered but for $\mathbb{Z}_{15}$. It is a lattice that shows all possible groups and subgroups of a cyclic group.