MATH 335 lecture 17

Chris Camano: ccamano@sfsu.edu

October 20, 2022

Recap of main ideas relating to cyclic groups

1. If G=$< a >$ is a cyclic group then every subgroup H of G is also a cyclic group
   In fact H=$< a^d >$ where d is the smallest positive integer such that:

$$a^d \in H$$

2. If an element has finite order, this is to say: $|a| = n$ then:

$$|a^k| = \frac{|a|}{\gcd(n,k)}$$

   This is to say: If G is a cylic group generated by a where : $|a| = n$ then $|G| = n$. Then the order of H=$< a^k >$ is $\frac{|a|}{\gcd(n,k)}$

Proposition 1. Let G=$< a >$ be a cyclic group of order n. Then for every positive divisor d of n there exists a subgroup of order $\frac{n}{d}$
Let $H =< a^d >$ then

$$|H| = |a^d| = \frac{n}{\gcd d, n} = \frac{n}{d}$$

Theorem

Let G be a cyclic group of order n
Then for every positive divisor d of n there is a unique subgroup of order $\frac{n}{d}$

Proof. Let $d|n$ then $H < a^d >$ is a subgroup of order $\frac{n}{d}$ We now need to show that H is the only unique subgroup of $\frac{n}{d}$
Suppose there exists another subgroup $K =< a^b >$ with equivilant order: $\frac{n}{d}$

$$|K| = \frac{n}{\gcd(b,n)} = \frac{n}{d}$$

Thus we conclude that the $gcd(b,n) = d$
This implies that $d|b$ so:
Claim: $K =< a^b > \subset H =< a^d >$

$$a^b = (a^d)^k, k \in \mathbb{Z} \in H$$

This implies that K is a subgroup of G and that $K <= H <= G$ since $|H| = |K| = \frac{n}{d} \rightarrow H = K$ □

Prime decomposition can be read off of a divisibility lattice by taking the proudct over the subgroups connected to the identity element and taking exponents associated with the number of connections within the lattice at each prime ordered subgroup.

new idea?

The divisibility lattice can be formed by reverse engineering the prime decomposition

Definition

Left cosets of a subgroup
Let G be a group. and let H be a subgroup of G. Then the left Coset with representative $g \in G$ is a set $gH = \{gh : h \in H\}$