MATH 335 lecture 15

Chris Camano: ccamano@sfsu.edu

October 18, 2022

Definition 1. Let G be a group and pick any element$a \in G$ then:

$$< a >= \{a^k, k \in \mathbb{Z}\}$$

Where negative exponents correlate with composition over the group operator with the inverse. This sub group is called the cyclic subgroup generated by a. A cyclic subgroup always has at least two generators since $< a >=< a^{-1} >$

It could be the case as well that there exists a generator that generates the entire group to begin with:
If

$$G =< a >$$

Then we say G is a cyclic group.

Proposition 1. $\mathbb{Z}$ is a cyclic group since $\mathbb{Z} =< 1 >$. In general for the group $\mathbb{Z}$ $a^k = ka$ since addition consectuive times is the same as multiplication over n times. This cyclic group is infinite. When a cyclic group is inifinite it is always $\mathbb{Z}$

For each positive integer n $\mathbb{Z}_n$ is also a cyclic group since we have the property that under a modular operator we observe cyclic behavior as the equivilance classes loop back to the identity at every multiple of n. this is to say:

$$\mathbb{Z}_n =< [1] >$$

Not every group is cyclic, for eexample all symmetry groups are not cyclic.

Theorem 1. Every cyclic group is abelian
Let G be a cyclic group, this is to say that G is generated by one element in G , g:
let $a, b \in G$ these two elements are some powers of the generator g meaning:

$$a = g^k \quad b = g^l$$

$$ab = g^l g^l = g^{k+l} = g^l g^k = ba$$

Theorem 2. Every subgroup of a cyclic group is cyclic

Proof. Let G be a cyclic group so $G =< g >$ let $H \leq G$ If H={e then H is cyclic because H=$< e >$
Let $H \neq \{e$Then for some positive integer k, $g^k \in H$ since all elements of G are of the form g^kSuppose $g^l \in H, but l < 0$. but l< 0 so $g^{-l} \in H$
Let d be the smallest postive integer so that $g^d \in H$ by the well ordering property.

Claim:$H =< g^d >$
We first show that $< g^d > \subset H$:

$$< g^d >= \{g^{dk}, k \in \mathbb{Z}\}$$

g^d is in H and H is a subgroup which means that compositions over g^d composed with itself is an element of H by the closure of the group operator.
We now show that $H \subset < g^d >$
let $a \in H$ so we know that $a = g^n, n \in Z$ We then need to show that d divides n which is akin to proving that there is no remainder when we divide n by d. by division algorithm show:

$$n = qd + r \quad 0 \leq r < d$$

if r =0 we are done, so lets suppose r¡0, then: suppose $g^n \in H$ then with our realtion we have:

$$g^n = g^{qn+r} = g^{d^q} g^r$$

$$g^{d^q} \in H$$

by definition of H since we have $g^r \in H$ and $g^{d^q} \in H$ we know that $g^{d^q} g^r \in H$ since we are composing two elements that are both in H. r is assumed to be positive but is less than d, but d is the smallest integer meaning this cannot be the case. □

Definition 2. All subgroups of $\mathbb{Z}$ is of the form:

$$< n >= n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$$

Definition 3. Let G be a group and $a \in G$ then the smalles positive integer n such that: $a^n = e$ is called the order of a denoted as $|a|$

Proposition 2. Let G be a group, $a \in G$ such taht $|a| = n$:
Then

$$< a >= \{e, a, a^2, ..., a^{n-1}\}$$

Proof. The first direction of the proof is the following:

$$a^m = e, t = ms, s \in \mathbb{Z}$$

and we want to show that:

$$a^t = e$$

this is equivilant tos aying :

$$a^t a^{mk} = (a^m)^s = (e)^s$$

□