MATH 335 lecture 14

Chris Camano: ccamano@sfsu.edu

October 11, 2022

1 Refresher on subgroups:

Definition 1. Subgroup
Let G be a group. A subset H of G is called a subgroup if H itself is a group, when we restrict the group operation to H.
This is akin to saying:

1. $e \in H$
2. $\forall g_1, g_2 \in H$, then $g_1 \circ g_2 \in H$
   "Closed under the group operation of G"
3. $\forall g \in H, g^{-1} \in H$
   Closed under taking inverses

Proposition 1. A nonempty subset H of a group G is a subgroup if and only if $\forall g_1, g_2 \in H, g_1 g_2^{-1} \in H$ This satisfies the aforementined three critera needed to determine if something is a subgroup or not.

Proof. Prove the identity element is in H. Since H is not the empty set take any element in H. We also take: $g_1 = g, g_2 = g$ then :

$$g_1 g_2^{-1} = gg^{-1} = e \in H$$

Let g and take $g_1 = e$, take $g_2 = g$ then:

$$g_1 g_2^{-1} = eg^{-1} = g^{-1} \in H$$

Prove of property 2. :
Let $g, h \in H$

$$g_1 = g, g_2 = h^{-1}$$

Thus

$$g_1 g_2^{-1} = g(h^{-1})^{-1} = gh \in H$$

For the other direction of the biconditional we need to show that if all three properties are true then $g_1 g_2^{-1} \in H$. However by the second proof we have that $g_2^{-1} \in H$ finally by the last proof we have $g_1 g_2^{-1} \in H$ $\square$

Definition 2. Cyclic subgroups
Let G be a group, pick $g \in G$ now form the following set:

$$H = \{g^k, k \in Z\}$$

Here note that negative powers equate the powers over g inverse. H is a subgroup of G called the cyclic subgroup generated by g. Written conventionally as:

$$H =< g >$$

the selected element g can be thought of as the seed or the generator of this set.
Comparable to a vector subspace given a basis.

Proof. We show that if $g_1, g_2 \in< g >$ then $g_1 g_2^{-1} \in< g >$
let $g = g^i$ let $g_2 = g^j$

$$g_1 g_2^{-1} = g^i g^{-j} = g^i - j \in< g >$$

□

Given G=$\mathbb{Z}$:

$$H < 2 >= \{2k : k \in \mathbb{Z}\}$$

$$H < 3 >= \{3k : k \in \mathbb{Z}\}$$

$$\mathbb{Z} =< 1 >$$

It is always true that

$$H < g >= H < g^{-1} >$$
