MTH 417 Notes

Cliff Sun

September 29, 2025

Lecture 11: 9/17

Recall: the **SUBGROUP LATTICE** is the set of subgroups of G ordered by $\leq$.

Cyclic Groups

Let G be a group, then the cyclic subgroup of G generated by a is

$$\langle a \rangle = \{a^k \ \mid \ k \in \mathbb{Z}\} \tag{1}$$

If a can generate all of G, then G is *cyclic*. Note, that a^k denotes concatenation.

Example

If $G = \mathbb{Z}_n$, then

$$\langle [1]_n \rangle = \{[0], \pm[1], \dots\} \tag{2}$$

Definition 0.1. *The order of G is defined as $o(a) = |\langle a \rangle|$. This is just saying that the size of the set generated by a is its order.*

Proposition 0.2.

1. *If $o(a) = \infty$, then $\langle a \rangle$ is isomorphic to $\mathbb{Z}$.*
2. *if $o(a) = n$, then $\langle a \rangle$ is isomorphic to $\mathbb{Z}_n$.*

When defining functions for isomorphisms, first need to make sure that it is well defined, then check if it is a homorphism. Note, that $\mathbb{Z}^\times$ just means all elements that have multiplicative inverses, this is just the group defined under the multiplication operation, which means that every element must have an inverse.

Let

$$S^1 = \{z \in \mathbb{Z} \mid |z| = 1\} \tag{3}$$

Lecture 12: 9/19

Recall, the circle group is such that

$$S^1 = \{z \in \mathbb{Z} \,||z| = 1\} \tag{4}$$

A product in S' is a composition of rotations since $z \sim e^{i\theta}$. We can then define a function

$$f(\theta) = \exp(i\theta) \tag{5}$$

This function is clearly on-to, but is not injective.

Proposition 0.3. *Suppose θ is an angle, then we study*

$$\langle e^{i\theta} \rangle \leq S^1 \tag{6}$$

This is a finite cyclic group when θ is a rational multiple of 2π, and is infinite if not.

If $\theta = 2\pi \cdot (a/b)$, then $\langle \exp(i\theta) \rangle$ is ismorphic to $\mathbb{Z}_b$.

Definition 0.4. *D_n is the group of symmetries of a regular n-gon. We claim that*

$$D_6 = \{e, \rho, \rho^2, \ldots, \tau\rho, \ldots\} \tag{7}$$

Such that $\rho^6 = e$, $\tau^2 = e$, and $\tau\rho^k = \rho^{-k}$.

Proposition 0.5. *Let $H \leq \mathbb{Z}$, then let $H = \langle d \rangle = \{dk | k \in \mathbb{Z}\} = d\mathbb{Z}$.*

Lecture 13: 9/22

Recall:

Proposition 0.6. *Let $H \leq \mathbb{Z}$, then let $H = \langle d \rangle = \{dk | k \in \mathbb{Z}\} = d\mathbb{Z}$.*

Proposition 0.7. *Let $H \leq \mathbb{Z}_n$, then either $H = \{[0]\}$ or $\exists d \in \mathbb{N}$ such that $H = \langle [d] \rangle$. Note, H is isomorphic to $\mathbb{Z}_{n/d}$*

Lemma 0.8. *Let $n \in \mathbb{N}$, and let $b \in \mathbb{Z}/\{0\}$, $d = \gcd(n, b)$, then in $\mathbb{Z}_n$, we have*

1. $\langle [b] \rangle = \langle [d] \rangle \leq \mathbb{Z}_n$
2. $o([b]) = n/d$

We prove this lemma

Proof. Can find $s, t \in Z$ such that $d = sb + tn$, then

$$[d] = [sb] = s[b] \in \langle [b] \rangle \tag{8}$$

This means that $\langle [d] \rangle \leq \langle [b] \rangle$. But also d divides b, which means that $b = dm$, this means that $\langle [b] \rangle \leq \langle [d] \rangle$. □

Definition 0.9. *A function $f : G \to H$ is a homomorphism if*

$$f(g_1 g_2) = f(g_1) f(g_2) \tag{9}$$

If $G \leq H$, then $f : G \to$ is a homomorphism.

Lecture 14: 9/26

If $G \to H$ is a homomorphism, then

$$f(g_1 g_2) = f(g_1)f(g_2)$$

If f and g are group homomorphisms, then

$$f \circ g$$

is also a homomorphism. Let $f : G \to H$, let $A \subseteq G$ and $B \subseteq H$ be subsets. Then

$$f(A) = \{f(a) | a \in A\} \subseteq H$$

be the image of A under f. Similarly

$$f^{-1}(B) = \{g \in G | f(g) \in B\} \subseteq G$$

be the preimage of B. Let $f : G \to H$, and A, B defined similarly. Then if $A \leq G$ (subgroup) then $f(A) \leq H$. Similarly, if $B \leq H$, then $f^{-1}(B) \leq G$.

We define the kernel of f to be

$$f^{-1}(e) \leq G$$

This means that which elements of G map to e. Note, this kernel is trivial if f is injective. However, such non-trivial kernels can happen, for example:

$$f^{-1}([0]_n) = nk \;\; k \in \mathbb{Z} \tag{10}$$

Definition 0.10. *A subgroup $N \leq G$ is a normal subgroup if for all $g \in G$*

$$gNg^{-1} = N$$

In other words, gng^{-1} is also called the conjugate of n by g.

Proposition 0.11. *If $f : G \to H$ is a homomorphism. Then $\ker(f)$ is a normal subgroup of G.*

Proof. Let $g \in G$, then let

$$y = gxg^{-1}$$

Then apply

$$f(y) = f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = e$$

Therefore, $y \in G$ is in $\ker(f)$. □

Proposition 0.12. *Let f is injective. Then*

$$\iff \ker(f) = \{e\}$$

Proof. $\implies$, f is injective, then let $x \in \ker(f)$. Then if $f(e) = f(x) \implies x = e$. We next prove the opposite direction. Let $\ker(f) = \{e\}$. Suppose $f(x) = f(y)$. Then compute

$$f(x^{-1}y) = f(x)^{-1}f(y) = e$$

Then $x^{-1}y \in \ker(f) \implies x = y$. □