LECTURE 8 SEP 16

Cosets

Author
Tom Jeong

September 16, 2024

Contents

1 Order of Element

ex. What are the possible orders of an element $[n] \in \mathbb{Z}/5\mathbb{Z}$ $5 = |\mathbb{Z}/5\mathbb{Z}|$
is prime so by Proposition 2.6.3, every element is either order 1 or order 5.
<u>note:</u> Any order 5 element generates $\mathbb{Z}/5\mathbb{Z}$

example: what are the possible homomorphism from $\mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/6\mathbb{Z}$?
Recall if $f : G \to K$ is a homormorphism then $ker f \leq G$ and $im f \leq K$
<u>note:</u> if ord(g) = n then $e_k = f(e_G) = f(g^n) = f(g)^n$
so $f(g)$ is of order divides n. by proposition 2.6.3 (3) – check notes from previous lecture

$$\begin{aligned}
&\mathbb{Z}/3\mathbb{Z} \\
&ord([0]) = 1 \\
&ord([1]) = ord([2]) = 3 \\
&\mathbb{Z}/6\mathbb{Z} \\
&ord([0]) = 1 \\
&ord([1]) = ord([5]) = 6 \\
&ord([2]) = ord([4]) = 3 \\
&ord([3]) = 2
\end{aligned}$$

What homomorphisms are possible ??

$$\begin{aligned}
&f([0]) = [0] \\
&f([1]) = [0] \text{ or } [2] \text{ or } [4] \\
&f([2]) = f([1] + [1]) = f([1]) + f([1])
\end{aligned}$$

so there is 3. homo morphisms

Definition 1.1 (2.7.1)**.**
A cyclic group is a group G containnig an element g such that $G =< g >$ The element g is called the generator of G and we say that G is the generated by g

example: $\mathbb{Z}/n\mathbb{Z}$ is generated by $[1]$ or $[n-1]$

Can there be an infinite cycle group? yes; the $\mathbb{Z}$ (under addition) is cyclic that is generated by 1 or -1.

Proposition 1.1. Any cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$
<u>Note:</u> $0\mathbb{Z} = \{0\}$, $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$, $\mathbb{Z}/1\mathbb{Z} = \{0\}$

Proof.

Consider $G =< g >$ thus

$$f_g : \mathbb{Z} \to G$$
$$f_g(n) = g^n$$

is a surjective homomorphism then $Ker(f_g)$ is a subgroup of $\mathbb{Z}$ and in Proiposition 2.2.3, we proved every subgroup of $\mathbb{Z}$ is of the form of $n\mathbb{Z}$ for some $n \in \mathbb{N}$
so $Ker(f_g) = n_g\mathbb{Z}$ for some $n_g \in \mathbb{N}$ and by the first isomorphism theorem, $\mathbb{Z}/n_g\mathbb{Z} \cong G \cong \mathbb{Z}/Ker(f_g)$

□

recall from HW the n^{th} roots of unity are:

$$z_k = e^{2\pi ik/n} \text{ for } k = 0, 1, 2, \dots, n-1$$

1.1 exercise

the nth roots of unity are a cyclic group generated by $z_1 = e^{2\pi i/n}$ and is isomorphic to Z/nZ
concrete example and its proof; taking a look at 4-th roots of unity. draw it:

$$\{1, i, -1, -i\} \cong (Z/4Z, +)$$

$$\begin{aligned} 1 &\to [0] : \text{ identity} \\ i &\to [1] \\ -1 &\to i^2 = [1] + [1] = [2] \\ -i &\to [3] \end{aligned}$$

Proposition 1.2 (2.7.2)**.**
A gfroup G of prime order $|G| = p$ is cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$

Proof.
Let $g \in G$ such that $g \neq e$ and let $H =< g >$. Since $H \leq G$ and by LaGrange Theorem, $|H|$ divides $|G| = p$ so $|H| = 1$ or p but $g \neq e$ so $|H| = p$ and $H = G$ so $G =< g >$ and G is cyclic.

□

Cyclic groups of composite order

Q: What about cyclic groups with orders not prime?
Lets look at $Z/12Z$

$$ord[0] = 1$$
$$ord[1] = ord[5] = 12$$
$$ord[2] = ord[10] = 6$$
$$ord[3] = ord[9] = 4$$
$$ord[4] = ord[8] = 3$$
$$ord[6] = ord[6] = 2$$
$$ord[7] = ord[11] = 12$$

we can see a pattern here. $[1], [5], [7], [11]$ are the generators of $Z/12Z$ and $Z/12Z$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$

Definition 1.2. Let $n \in \mathbb{Z}$ the Euler ϕ function is defined as $\phi(n) = |\{k \in \mathbb{Z}|1 \leq k \leq n \text{ and } gcd(k, n) = 1\}|$

Lemma 1.3 (Cor 1.5.10)**.**
Let $a, b, c \in \mathbb{Z}$ If gcd (a,b) $= 1$ and $a|bc$ then $a|c$

see textbook for proof

Proposition 1.4 (2.7.4)**.**
let G be a cyclic group

1. every subgroup of G is cyclic
2. Suppose G is finite and is a divisor of $|G|$ Then G contains a unique subgroup H of order d
3. There are $\phi(d)$ elementz of order d in G They are exactly the generators of the subgroup in part 2.

Proof.
1. if $|G| = \infty$ then $G \cong \mathbb{Z}$ and by Proposition 2.6.3, every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ so every subgroup of G is cyclic.

□