2.3 Cyclic Groups (Definitions) [54]

Tuesday, October 10, 2023 11:00

Defn: a group H is cyclic if it is generated by one element $x \in H$

$$H = \{x^n \mid n \in \mathbb{Z}\}$$

$$H = \langle x \rangle$$

H is generated by x or x is a generator of H

In certain example where "+" is typically the notation of group operation denoted as: $\{nx \mid n \in \mathbb{Z}\}$

---

① $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$
with the operation of addition

② $\mathbb{Z}/6\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle$

③ $(\mathbb{Z}/6\mathbb{Z})^{\times} = \langle \bar{5} \rangle$

④ $(\mathbb{Z}/8\mathbb{Z})^{\times} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

not cyclic b/c ...

not cyclic b/c $\langle \bar{1} \rangle = \{\bar{1}\}$

$\langle \bar{3} \rangle = \{\bar{3}, \bar{1}\}$

$\langle \bar{5} \rangle = \{\bar{5}, \bar{1}\}$

$\langle \bar{7} \rangle = \{\bar{7}, \bar{1}\}$

⑧ $D_{2n} = \{1, r, r^2, \ldots r^{n-1}, s, sr \ldots sr^{n-1}\}$

$\langle r^i \rangle \leq \{1, r, \ldots r^{n-1}\} \subsetneq D_{2n}$

$\langle sr^j \rangle = \{1, sr^j\} \subsetneq D_{2n}$

⑥ S_n not cyclic b/c S_n is not abelian

$S_2 = \{1, (1\ 2)\}$
$= \langle (1\ 2) \rangle$

Consider $x^a x^b = x^{a+b} = x^b x^a$

If G is cyclic then G is abelian

Q2 If $H = \langle x \rangle$, how does $|H|$ compare with $|x|$

Q1 How does the cardinality (the order)

of H compare with the order of the element x

Answer $|H| = |x|$, $|\langle x \rangle| = |x|$

What does $|\langle x \rangle| = |x|$ say and what do we need to do to prove it?

(1) if $|x| = n \in \mathbb{Z}^+$ then $|H| = n$

(2) if $|x| = \infty$ then $|H| = \infty$

(a) if $|H| = n \in \mathbb{Z}^+$ then $|x| = n$

(b) if $|H| = \infty$ then $|x| = \infty$

It suffices to prove (1) and (2) then we showed $|x| = |H|$ and

$0 \leq a < b \leq n-1$

then (a) and (b) come for free.

(1) if $|x| = n$, a positive integer then $\{x^n \mid n \in \mathbb{Z}\} = H = \{1, x, x^2 \ldots x^{n-1}\}$ is a set of n distinct elements

② If $|x| = \infty$

then $x^n \neq 1$ for any $n \in \mathbb{Z}^+$

then $H = \{x^n \mid n \in \mathbb{Z}\}$

An infinit set

show for $a, b \in \mathbb{Z}$ $a \neq b$

then $x^a \neq x^b$

$$\begin{cases} \mathbb{Z} \longrightarrow H \\ a \longmapsto x^a \end{cases}$$

is a bijection

---

if $H = \langle x \rangle$ what are the generators of H:

for which $a \in \mathbb{Z}$ is $H = \langle x^a \rangle$

$\Rightarrow$ Proposition 6

Suppose $H = \langle x \rangle$

① Assume $|x| = \infty$ then $H = \langle x^a \rangle$ iff $a = \pm 1$

② assume $|x| = n \in \mathbb{Z}^+$ then
$H = \langle x^a \rangle$ iff $(a,n) = 1$

---

proof ideas

for any $a \in \mathbb{Z}$
$\langle x^a \rangle \subseteq \langle x \rangle$

1.) ($\Leftarrow$) assume

show $\langle x^{-1} \rangle = \langle x \rangle$

check $\supseteq$ $x^a \in \langle x^{-1} \rangle$

($\Rightarrow$) show $\langle x^a \rangle \neq \langle x \rangle$

find an element in $\langle x \rangle$ that is not in $\langle x^a \rangle$

$x \in \langle x^a \rangle \Rightarrow x = x^{na}$ $\exists n \in \mathbb{Z}$

$na = 1$ $\boxed{\text{Contradiction}}$

2.) Since we have $\forall a \in \mathbb{Z}$

$\langle x^a \rangle \subseteq \langle x \rangle = H$

and $|H| = |x| = n$

then $H = \langle x^a \rangle$ iff $|\langle x^a \rangle| = n$

which happens if and only if

$|x^a| = n$

When is $|x^a| = |x|$?

What is $|x^a|$?

Proposition 5

Let G be a group and $x \in G$

$a \in \mathbb{Z} - \{0\}$

1. if $|x| = \infty$ then $|x^a| = \infty$

2. if $|x| = n \in \mathbb{Z}$ then $|x^a| = \frac{n}{(n,a)}$

1. assume $|x^a| \neq \infty$

then $(x^a)^n = 1 \quad \exists\, n \in \mathbb{Z}^+$

$\longrightarrow x^{an} = 1$

$\longrightarrow$ $\boxed{\text{contradicts}}$ $|x| = \infty$

2. We need the following proposition

Let G be a group $x \in G$

1.) if $x^m = 1$ and $x^n = 1$

for some $m, n \in \mathbb{Z}$

Let $d = (m, n)$ then $x^d = 1$

2.) if $x^m = 1$ $\exists m \in \mathbb{Z}$ then

$|x|$ divides m

for $d = mx + ny$, $x, y \in \mathbb{Z}$

try the euclidian algorithm