Section 2.3 Cyclic Groups and Cyclic Subgroups

Definitions Given an element $a \in G$, the following subgroup can be formed:

$$H = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \} \leq G \quad \text{(if operation is } \cdot \text{)}$$
$$H = \langle a \rangle = \{ na \mid n \in \mathbb{Z} \} \leq G \quad \text{(if operation is } + \text{)}$$

Subgroup $\langle a \rangle$ is called the cyclic subgroup generated by a.

If $G = \langle a \rangle$ for some $a \in G$, we say G is a cyclic group with generator a.

Examples

$\langle \sqrt{2} \rangle = \{ n\sqrt{2} \mid n \in \mathbb{Z} \} = \{ \ldots -\sqrt{2}, 0\sqrt{2}, 2\sqrt{2}, \ldots \} \leq \mathbb{R}$

$\langle 3 \rangle = \{ 3^n \mid n \in \mathbb{Z} \} = \{ \ldots \tfrac{1}{3}, 1, 3, 9, 27 \ldots \} \leq \mathbb{R}^\times$

$\langle -1 \rangle = \{ -1, 1 \} \leq \mathbb{R}^\times$

Consider $\mathbb{Z}/12\mathbb{Z}$

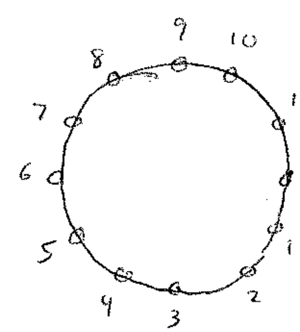
$\langle 1 \rangle = \{ n \cdot 1 \mid n \in \mathbb{Z} \} = \mathbb{Z}/n\mathbb{Z}$

$\langle 2 \rangle = \{ 0, 2, 4, 6, 8, 10 \}$

$\langle 3 \rangle = \{ 0, 3, 6, 9 \}$

$\langle 4 \rangle = \{ 0, 4, 8 \}$

$\langle 5 \rangle = \{ 0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7 \}$



Note: $\mathbb{Z}/12\mathbb{Z} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$ so it's cyclic

Notation For Cyclic Groups

$\mathbb{Z}/n\mathbb{Z} = \{ 0, 1, 2, \ldots n-1 \} = \langle 1 \mid n \cdot 1 = 0 \rangle \quad (+)$

$Z_n = \{ 1, a, a^2 \ldots a^{n-1} \} = \langle a \mid a^n = 1 \rangle \quad (\cdot)$

$\mathbb{Z} = \{ \ldots -1, 0, 1, 2, \ldots \} = \langle 1 \rangle$

Note isomorphism $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}_n = \langle a \rangle$

$$\bar{i} \longmapsto a^i$$

Note: If $G = \langle a \rangle$ is cyclic, then either $|G| = n < \infty$ or $|G| = |\mathbb{Z}| = \aleph_0$

Theorem 4 Suppose $G = \langle a \rangle$ is cyclic.

If $|G| = n < \infty$, then $G \cong \mathbb{Z}/n\mathbb{Z}$

If $|G| = \infty$, then $G \cong \mathbb{Z}$.

Consequence: Any two cyclic groups of the same order are isomorphic.

Proposition 3 Suppose G is arbitrary and $x \in G$.

1. $x^m = 1 \iff m$ is a multiple of $|x|$, i.e. $|x| \mid m$.
2. If $x^m = x^n = 1$, then $x^{\gcd(m,n)} = 1$.

Proof For 1, see lemma in Homework #1 solutions.

Proof of 2: Suppose $x^m = x^n = 1$

By part 1, $m = k|x|$, $n = \ell|x|$

Thus $\gcd(m,n) = p|x|$

Then $x^{\gcd(m,n)} = x^{p|x|} = (x^{|x|})^p = 1^p = 1$ ∎

Proposition 5 Suppose G is arbitrary, $x \in G$ and $a \in \mathbb{Z} - \{0\}$

1. If $|x| = \infty$, then $|x^a| = \infty$
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$
3. If $|x| = n$ and $a \mid n$, then $|x^a| = \frac{n}{a}$
4. If $\gcd(n,a) = 1$ then $\langle x^a \rangle = \langle x \rangle$.

[Proof hinges on Proposition 3]

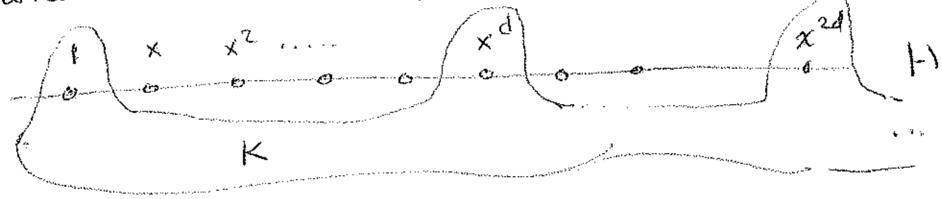
Example: Look at $\mathbb{Z}/12\mathbb{Z}$.

We saw $\langle \bar{4} \rangle = \{0, 4, 8\}$ and $|\bar{4}| = 3$

This is $\langle \bar{4} \rangle = \langle 4 \cdot \bar{1} \rangle = \frac{12}{\gcd(12,4)} = \frac{12}{4} = 3$

<u>Theorem 7</u> Suppose $H = \langle x \rangle$ is cyclic

① Every subgroup of H is cyclic.
If $K \leq H$ then $K = \{1\}$ or $K = \langle x^d \rangle$
when d is smallest pos. integer with $x^d \in K$



② If $|H| = \infty$ and $a \neq b$, $a, b \geq 0$, then $\langle x^a \rangle \neq \langle x^b \rangle$
~~Also~~ $\cancel{H \cong} \mathbb{Z}$. Subgroups of H are $\langle 1 \rangle, \langle x \rangle = H, \langle x^2 \rangle\ \langle x^3 \rangle \ldots$

③ If $|H| = n < \infty$ and $a | n$, then is a unique subgroup $K \leq H$ with $|K| = \frac{n}{a}$
In fact, $K = \langle x^{n/a} \rangle$
Cyclic subgroups of H correspond bijectively with divisors of H.

Theorem 7 is useful because it tells us exactly how to find the subgroups of a cyclic group.

<u>Ex</u> Subgroups of $\mathbb{Z}$ are exactly $\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle \ldots$

<u>Ex</u> Subgroups of $\mathbb{Z}/12\mathbb{Z}$ are $\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \ldots \langle 11 \rangle$
(although some of these are equal)

So cyclic groups have predictable subgroup structures <u>and</u> the subgroups are <u>few</u>.

The number of subgroups of cyclic group G is <u>at most</u> $|G|$.

<u>Query</u>! Is there a non-cyclic group G that has more than $|G|$ subgroups?
Answer is YES.