1. Cyclic groups and subgroups

Definition 1.1. A group H is cyclic if H can be generated by a single element, i.e., there exists $a \in H$ such that

$$H = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \text{ where } a^n \in H.$$

Remark 1.1.1.

1. In additive notation $H = \{2m \mid m \in \mathbb{Z}\}$. *(In additive notation $(\mathbb{Z}/n\mathbb{Z})$ is cyclic and $\mathbb{Z}/2\mathbb{Z} = \langle 1 \rangle$)*
2. If H is cyclic then there exists some $x \in H$ such that $H = \langle x \rangle$.
3. If $|H| = \langle x \rangle$ then x is not unique (and more).
4. $x^n \neq x^m$ if and only if $n \neq m$.
5. If $G = D_n$ and $H = \langle r \rangle$, then $H = \langle r^m \rangle$ and $k = m$ if and only if $k \equiv m \mod n$.
6. Every cyclic subgroup H is abelian. For example, if $H = \langle r \rangle$ in $G = D_n$, then H is abelian, but D_n is not cyclic.
7. By convention, $x^0 = 1$ for any element x

Proposition 1.2. *If $H = \langle x \rangle$ then $|H| = |x|$. More specifically:*

1. *If $|H| = n < \infty$, then $x^n = 1$ and $1, x, \ldots, x^{n-1}$ are all distinct elements of H.*
2. *If $|H| = \infty$, then $x^n \neq 1$ for $n \neq 0$ and $x^a \neq x^b$ for $a \neq b$ in $\mathbb{Z}$.*

Proposition 1.3. *Let G be a group, $x \in G$, and $m, n \in \mathbb{Z} \backslash \{0\}$.*

- *If $x^m = 1$ and $x^n = 1$, then $x^d = 1$ where $d = \gcd(m, n)$.*
- *In particular, if $x^m = 1$, then $x^{|m|} = 1$.*

Proof. By the Euclidean Algorithm, there exist $r, s \in \mathbb{Z}$ such that $d = mr + ns$ where $d = \gcd(m, n)$. Therefore, $x^d = (x^m)^r \cdot (x^n)^s = 1^r \cdot 1^s = 1$.

On the other hand, if $x^m = 1$ and $n = |x|$, then if $m = 0$ (implying $n \mid m$), then by 1), $x^d = 1$ where $d = \gcd(m, n)$,

therefore $d = n$ by minimality. Then (since $d \mid n$ and $n \mid m$), $d = m$. □

Proof. □

Theorem 1.4. *Any two cyclic groups of the same order are isomorphic.*

Proof. (1) **Finite case:** Let $H_1 = \langle x \rangle$ and $H_2 = \langle y \rangle$ where $|x| = |y| = n$. Define $\varphi : \langle x \rangle \to \langle y \rangle$ by $\varphi(x^k) = y^k$. Then φ is a well-defined isomorphism.

- **Well-defined:** If $x^k = x^l$ then $\varphi(x^k) = \varphi(x^l)$ since $y^k = y^l$. Since $x^k = x^l$ implies $k \equiv l \mod n$, $y^k = y^l$ by the same logic.
- **Homomorphism:** $\varphi(x^k \cdot x^l) = \varphi(x^{k+l}) = y^{k+l} = y^k \cdot y^l = \varphi(x^k) \cdot \varphi(x^l)$.
- **Injective:** If $\varphi(x^k) = y^k = 1$, then $x^k = 1$ since $n \mid k$.
- **Surjective:** Let $y^k \in \langle y \rangle$ then $\varphi(x^k) = y^k$.

(2) **Infinite case:** If $H = \langle x \rangle$ with $|H| = \infty$, then define $\varphi : \mathbb{Z} \to \langle x \rangle$ by $\varphi(k) = x^k$. φ is an isomorphism:

- φ is a function from $\mathbb{Z}$ to $\langle x \rangle$ that maps each integer k to x^k, preserving the structure of $\mathbb{Z}$ under addition, mirroring the group operation of $\langle x \rangle$ under multiplication.

□

Remark 1.4.1. Up to isomorphism, there exists a unique cyclic group of finite order n, namely $\mathbb{Z}/n\mathbb{Z} = \langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\}$ (multiplicative), and a unique cyclic group of infinite order, $\mathbb{Z} = \langle x \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\}$ (additive).

Proposition 1.5. *Let G be a group, let $x \in G$, and let $a \in \mathbb{Z} \setminus \{0\}$.*

(i) If $|x| = \infty$, then $|x^a| = \infty$.

(ii) If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$.

(iii) If $|x| = n < \infty$ and also $a \equiv 0 \mod n$, then $|x^a| = \frac{n}{a}$.

Proof. 1. Assume that $|x| = \infty$. Just assume $|x^a| = m < \infty$. Then $(x^a)^m = x^{am} = 1$. Show that there exist $r, s \in \mathbb{Z}$ such that $n = amr + s$ where $x^n = x^s$. This shows $|x| < \infty$, which is a contradiction.

2. Define $y = x^a$ and $d = \gcd(n, a)$, then $n = db$ and $a = dc$ for some $b, c \in \mathbb{Z}$ with $\gcd(b, c) = 1$. We need to prove that $|y| = b$. First note that $y^b = (x^a)^b = x^{ab} = x^{dcb} = (x^n)^c = 1^c = 1$. Thus $|y| \leq b$.

   Let $k = |y|$, then $y^k = x^{ak} = 1$. If $ak = nd$, since $\gcd(b, c) = 1$, then $b \mid k$. Thus $k = b$ and hence $|y| = b$.

3. This is a special case of 2.

□

Theorem 1.6. *Let H be a cyclic group. Assume $H = \langle x \rangle$.*

1. *Every subgroup $K \leq H$ is cyclic and $K = \langle x^d \rangle$ where $d = \min\{k \in \mathbb{N} \mid x^k \in K\}$.*
2. *If $|H| = \infty$, then $\langle x^s \rangle \neq \langle x^t \rangle$ for all $s \neq t$ in $\mathbb{Z}$, and $\langle x^n \rangle = \langle x \rangle$ implies $\mathbb{Z}$. Thus, there exists an injective correspondence between $\mathbb{N}$ and the subgroups of H.*

3. *If $|H| = n < \infty$, then for all $a \in \mathbb{Z}^*$ such that $a \mid n$ and $a \neq n$, $\langle x^d \rangle \leq H$ implies that $|K| = a$ where $d \cdot m = n/a$.*

   (a) $\langle x^s \rangle = \langle x^{(n/m)} \rangle$ *where* $\gcd(m, n) = 1$.

4. *The subgroups of H correspond bijectively with the positive divisors of $|H|$.*

Remark 1.6.1. In $\mathbb{Z}/n\mathbb{Z}$:

1. $\mathbb{Z}/n\mathbb{Z} = \langle t \rangle = \langle m \rangle$ if and only if $\gcd(m, n) = 1$ for $m \in \mathbb{Z}$.
2. $\langle s \rangle \leq \langle \gcd(s, m) \rangle$.
3. $\langle a \rangle \leq \langle b \rangle$ if and only if $\gcd(b, n) \mid \gcd(a, n)$ where $1 \leq a, b \leq n$.

Example 1. In $\mathbb{Z}/48\mathbb{Z}$, compute $\langle 6 \rangle$, find the order of a and relation between $\langle 6 \rangle$ and Molien subgroups.

- $\phi(48) = \phi(2^4 \cdot 3) = \phi(2^4) \cdot \phi(3) = 2^3 \cdot (3-1) = 16$.

  The subgroup relations for $\mathbb{Z}/48\mathbb{Z}$ are represented as follows:

$$
\begin{aligned}
\langle 1 \rangle &= \langle 47 \rangle = \langle 49 \rangle = \cdots = \langle 1 \rangle, \\
\langle 2 \rangle &= \langle 46 \rangle = \langle 50 \rangle = \cdots = \langle 2 \rangle, \\
\langle 3 \rangle &= \langle 45 \rangle = \langle 51 \rangle = \cdots = \langle 3 \rangle, \\
\langle 4 \rangle &= \langle 44 \rangle = \langle 52 \rangle = \cdots = \langle 4 \rangle, \\
\langle 6 \rangle &= \langle 42 \rangle = \langle 54 \rangle = \cdots = \langle 6 \rangle, \\
\langle 8 \rangle &= \langle 40 \rangle = \langle 56 \rangle = \cdots = \langle 8 \rangle, \\
\langle 12 \rangle &= \langle 36 \rangle = \langle 60 \rangle = \cdots = \langle 12 \rangle, \\
\langle 16 \rangle &= \langle 32 \rangle = \langle 64 \rangle = \cdots = \langle 16 \rangle, \\
\langle 24 \rangle &= \langle 24 \rangle = \langle 72 \rangle = \cdots = \langle 24 \rangle.
\end{aligned}
$$

  Subgroups of $\mathbb{Z}/48\mathbb{Z}$ are related as follows:

$$
\begin{aligned}
&\langle 24 \rangle \subset \langle 12 \rangle \subset \langle 6 \rangle \subset \langle 3 \rangle \subset \langle 1 \rangle, \\
&\langle 16 \rangle \subset \langle 8 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle \subset \langle 1 \rangle, \\
&\langle 18 \rangle \subset \langle 9 \rangle \subset \langle 3 \rangle \subset \langle 1 \rangle, \\
&\langle 20 \rangle \subset \langle 10 \rangle \subset \langle 5 \rangle \subset \langle 1 \rangle.
\end{aligned}
$$