§3 - Cyclic Groups

We say a group G is cyclic if

$$\boxed{G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}}$$

for some $a \in G$ (called a generator of G)

Ex 1. In §2 we saw that for all $n \in \mathbb{Z}$,

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

Thus, $n\mathbb{Z}$ is a cyclic group generated by n. It is also generated by $-n$.

In particular, with $n = 1$ we have that

$\mathbb{Z} = 1\mathbb{Z} = \langle 1 \rangle$ is cyclic.

Ex 2: In §2 we also saw that

$\mathbb{Z}_{10}^* = \{1,3,7,9\}$ is cyclic. We have

$\mathbb{Z}_{10}^* = \langle 3 \rangle = \langle 7 \rangle$. These are the only

generators.

Ex 3: For any $n \in \mathbb{N}$, the group $\mathbb{Z}_n$ is cyclic. Indeed, $\mathbb{Z}_n = \langle 1 \rangle$. This is not the only generator, however.

e.g. in $\mathbb{Z}_8 = \langle 1 \rangle$, we have

$$\langle 5 \rangle = \{5, 2, 7, 4, 1, 6, 3, 0\} = \mathbb{Z}_8.$$

Thus, 5 is also a generator. Are there any others?

Ex 4: Fix $n \in \mathbb{N}$ and define

$$G = \{ z \in \mathbb{C} \mid z^n = 1 \} \subseteq \mathbb{C}^*.$$

From Math 135 we know that

$$G = \{ e^{2k\pi i/n} : k \in \mathbb{Z} \}.$$

Thus, we have that $G = \langle e^{2\pi i/n} \rangle$, and hence G is a cyclic subgroup of $\mathbb{C}^*$. This is the group of n^{th} roots of unity.

(We've worked with these groups already!

$$n = 2 \Rightarrow G = \{1, -1\} = \langle -1 \rangle$$

$$n = 4 \Rightarrow G = \{1, i, -1, -i\} = \langle i \rangle \quad)$$

Notice that all of these groups are Abelian.

This is no coincidence.

Proposition: Every cyclic group is Abelian.

Proof: An easy exercise. ■

Cyclic groups are, in some sense, the nicest groups that exist. Not only are they Abelian, but they are generated by just one element.

This has major implications for the structure of such a group. Indeed, suppose that $G = \langle a \rangle$. If $|a| = \infty$, then

$$G = \{ \ldots, a^{-2}, a^{-1}, a^{0}, a^{1}, a^{2}, \ldots \}$$

and the group operation $a^m a^n = a^{m+n}$ is sort of like addition in $\mathbb{Z}$.

If $|a| = n < \infty$, then $G = \{a^0, a^1, \ldots, a^{n-1}\}$, and the group operation is like addition in $\mathbb{Z}_n$.

These observations will be extremely important later when we determine every cyclic group up to isomorphism!

For now, our goals are to describe the subgroup structure of a cyclic group, and determine which of its elements are generators.

Theorem 1: Every subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle a \rangle$ be a cyclic group and $H \leq G$. If $H = \{e\}$, then clearly H is cyclic. So suppose that H contains an element $a^t \neq e$ (in particular, $t \neq 0$). Note that since H also contains $(a^t)^{-1} = a^{-t}$, it follows that H contains a positive power of a.

Let m be the smallest positive integer such that $a^m \in H$. We claim that $H = \langle a^m \rangle$.

Proof of claim: Since H is a group and $a^m \in H$, it follows that $\langle a^m \rangle \subseteq H$.

We must now prove $\supseteq$. If $b \in H$, then $b = a^k$ for some $k \in \mathbb{Z}$. By the division algorithm, write

$$K = mq + r \text{ for some } r \in \{0, 1, \dots, m-1\}.$$

Using this equation, we have that

$$a^r = a^{k-mq} = \underbrace{a^k}_{\in H} \underbrace{(a^m)^{-q}}_{\in H} \in H.$$

Recall that m is the smallest positive integer such that $a^m \in H$. Since $a^r \in H$

and $r < m$, it must be that $r = 0$.

Consequently, $b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle$.

We conclude that $H = \langle a^m \rangle$, as claimed. ■

The above theorem demonstrates that every subgroup of a cyclic group $G = \langle a \rangle$ is given by $H = \langle a^k \rangle$ for some $k \in \mathbb{Z}$.

In particular, we have seen that $\mathbb{Z} = \langle 1 \rangle$ is cyclic. Thus, every subgroup of $\mathbb{Z}$ is of the form $\langle 1^n \rangle = \langle n \rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Next, we determine when two subgroups $\langle a^i \rangle$ and $\langle a^j \rangle$ of a cyclic group are equal.

Theorem 2: Let a be a group element of order $n < \infty$, and let $k \in \mathbb{N}$.

(i) $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(ii) $|a^k| = |a^{n/\gcd(n,k)}|$.

Proof: (i) Let $d = \gcd(n,k)$, and write $k = dr$ for some $r \in \mathbb{Z}$. We have that

$a^k = (a^d)^r \in \langle a^d \rangle$, and hence $\langle a^k \rangle \subseteq \langle a^d \rangle$.

To see that $\langle a^k \rangle \supseteq \langle a^d \rangle$, write $d = ns + kt$ for some $s, t \in \mathbb{Z}$. We have

$$a^d = a^{ns+kt} = (a^n)^s (a^k)^t = e^s (a^k)^t = (a^k)^t.$$

Consequently, $a^d \in \langle a^k \rangle$, so $\langle a^k \rangle \supseteq \langle a^d \rangle$.

This proves (i).

For (ii), we show that if d is any divisor of n, then $|a^d| = n/d$. Indeed, it is clear that $(a^d)^{n/d} = a^n = e$, so $|a^d| \leq n/d$. But if $j < n/d$, then $dj < d(n/d) = n$, so $a^j \neq e$ by definition of $|a|$. Thus $|a^d| = n/d$.

Finally, if $d = \gcd(n,k)$ as in (i), then

$$|a^k| = |\langle a^k \rangle| = |\langle a^{\gcd(n,k)} \rangle| \quad \text{(by (i))}$$
$$= |a^{\gcd(n,k)}| = n/\gcd(n,k)$$

■

Corollary 1: Let a be a group element of order $n < \infty$. Then for any $i, j \in \mathbb{Z}$, $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n,i) = \gcd(n,j)$.

Proof: ($\Rightarrow$) If $\langle a^i \rangle = \langle a^j \rangle$, then

$|\langle a^i \rangle| = |\langle a^j \rangle|$, and hence $|a^i| = |a^j|$.

By Theorem 2, we have

$$\frac{n}{\gcd(n,i)} = \frac{n}{\gcd(n,j)},$$ so $\gcd(n,i) = \gcd(n,j)$.

($\Leftarrow$) If $\gcd(n,i) = \gcd(n,j)$, then

$$\langle a^i \rangle \underset{\text{Theorem 2}}{=} \langle a^{\gcd(n,i)} \rangle \underset{\text{Hypothesis}}{=} \langle a^{\gcd(n,j)} \rangle \underset{\text{Theorem 2}}{=} \langle a^j \rangle$$

$\blacksquare$

Corollary 2: Let a be a group element of order $n < \infty$. Then for $k \in \mathbb{Z}$,
$\langle a \rangle = \langle a^k \rangle$ iff $\gcd(n,k) = 1$.

Proof: Immediate from Corollary 1. $\blacksquare$

Ex: For each n, $\mathbb{Z}_n = \langle 1 \rangle$. By Corollary 2, every generator of $\mathbb{Z}_n$ is given by $1^k = k$ where $\gcd(n,k) = 1$.

e.g. The generators of $\mathbb{Z}_8$ are all $k \in \mathbb{Z}_8$ such that $\gcd(8,k) = 1$ (i.e., $1, 3, 5, 7$).

Ex: We saw above that $\mathbb{Z}_{10}^{\times} = \langle 3 \rangle$ is cyclic.

Since $|3| = 4$, all generators are given by 3^k where $\gcd(4, k) = 1$. (ie., $3^1 = 3$, $3^3 = 7$)

Exercise: The group $\mathbb{Z}_{14}^*$ is cyclic with generator 5. Find all other generators.

Exercise: For any $n \in \mathbb{N}$, the subgroup $\langle e^{2\pi i/n} \rangle$ of $\mathbb{C}^*$ consisting of n^{th} roots of unity is cyclic. Find all generators of this subgroup.

Let's take a closer look at $\mathbb{Z}_8$. By Theorem 1, we know that every subgroup of $\mathbb{Z}_8$ is cyclic, and hence is of the form $\langle n \rangle$ for some $n \in \mathbb{Z}_8$. If $n = 1, 3, 5, 7$, then

$\langle n \rangle = \mathbb{Z}_8$. What are the other subgroups?

$$\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8$$

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

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

$$\langle 0 \rangle = \{0\}.$$

Notice anything interesting?

The order of every subgroup is a divisor of 8. Moreover, every positive divisor of 8 occurs as the order of exactly one subgroup of $\mathbb{Z}_8$!

Theorem 3. Let $G = \langle a \rangle$ be a cyclic group of order $n < \infty$.

(i) The order of any subgroup of G is a divisor of n.

(ii) If k is a positive divisor of n, then there is a unique subgroup of G of order k, namely $\langle a^{n/k} \rangle$.

Proof: By Theorem 1, every subgroup of G is of the form $\langle a^k \rangle$ for some $k \in \mathbb{N}$. By Theorem 2, $|\langle a^k \rangle| = |a^k| = n/\gcd(n,k)$, which is a divisor of n. This proves (i)

For (ii), let $k \in \mathbb{N}$ be a divisor of n.

By Theorem 2,

$$|\langle a^{n/k}\rangle| = |a^{n/k}| = n/\gcd(n,\tfrac{n}{k}) = n/(n/k) = k.$$

Thus, $\langle a^{n/k}\rangle$ is indeed a subgroup of G of order k. To see that this is the unique such subgroup, let H be a subgroup of G of order k. By Theorem 1, H is cyclic, hence $H = \langle a^m\rangle$ for some $m \in \mathbb{N}$. By Theorem 2,

$$\underline{n/\gcd(n,m) = |\langle a^m\rangle| = k},$$

hence $\gcd(n,m) = n/k$. Thus,

$$H = \langle a^m\rangle \underset{\text{Theorem 2}}{=} \langle a^{\gcd(n,m)}\rangle = \langle a^{n/k}\rangle.$$

This completes the proof. $\blacksquare$

Ex: Consider the cyclic group $G = \mathbb{Z}_{20} = \langle 1 \rangle$ of order 20. The group G has exactly one subgroup of order K for each divisor K of 20 $(K = 1, 2, 4, 5, 10, 20)$. This subgroup is given by $\langle 1^{20/K} \rangle$.

$K = 1$: $\langle 1^{20/1} \rangle = \{0\}$

$K = 2$: $\langle 1^{20/2} \rangle = \langle 10 \rangle = \{0, 10\}$

$K = 4$: $\langle 1^{20/4} \rangle = \langle 5 \rangle = \{0, 5, 10, 15\}$

$K = 5$: $\langle 1^{20/5} \rangle = \langle 4 \rangle = \{0, 4, 8, 12, 16\}$

$K = 10$: $\langle 1^{20/10} \rangle = \langle 2 \rangle = \{0, 2, 4, 6, \ldots, 16, 18\}$

$K = 20$: $\langle 1^{20/20} \rangle = \langle 1 \rangle = \{0, 1, 2, 3, \ldots, 19\} = \mathbb{Z}_{20}$.

Ex: Let $G = \langle a \rangle$ be a cyclic group of order 100.

The subgroups $H \leq G$ are in 1-1 correspondence with the positive divisors k of 100.

$k \mid 100$	1	2	4	5	10	20	25	50	100
$\lvert H \rvert = k$	$\langle a^{100} \rangle = \{e\}$	$\langle a^{50} \rangle$	$\langle a^{25} \rangle$	$\langle a^{20} \rangle$	$\langle a^{10} \rangle$	$\langle a^{5} \rangle$	$\langle a^{4} \rangle$	$\langle a^{2} \rangle$	$\langle a \rangle$

Exercise: Write down all subgroups of the cyclic group $\mathbb{Z}_{14}^{*} = \langle 5 \rangle$.

Exercise: Let G be a cyclic group of order 90. How many elements of G have order 15?

Subgroup Lattices

We can represent the subgroups of a group G visually using a subgroup lattice. This is a diagram that includes all subgroups of a group G. A subgroup K at some level of the lattice is connected to a subgroup H at a higher level if and only if K is properly contained in H.

Ex: If $G = \langle a \rangle$ is a cyclic group of order 10, then G has subgroup lattice

$$\begin{tikzcd}[column sep=small]
 & \langle a \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle a^2 \rangle \arrow[dr, dash] & & \langle a^5 \rangle \arrow[dl, dash] \\
 & \langle a^{10} \rangle &
\end{tikzcd}$$

Ex: If $G = \langle a \rangle$ is a cyclic group of order 20, then G has subgroup lattice

$$\begin{tikzcd}[column sep=small]
 & \langle a \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle a^2 \rangle \arrow[d, dash] \arrow[drr, dash] & & \langle a^5 \rangle \arrow[d, dash] \\
\langle a^4 \rangle \arrow[dr, dash] & & \langle a^{10} \rangle \arrow[dl, dash] \\
 & \langle a^{20} \rangle &
\end{tikzcd}$$

Exercise: Draw the subgroup lattice for a cyclic group $G = \langle a \rangle$ of order 100.