

Cyclic Groups

Cyclic subgroups are the **simplest** subgroups. They are the basic building blocks in the world of groups.

Definition. The **cyclic subgroup** generated by an element $a \in G$ is $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

It is easy to show that

Proposition. $\langle a \rangle$ is a subgroup of G .

Cyclic subgroups have a universal property. They are the smallest subgroup containing the generator.

Proposition. If $a \in G$ generates subgroup $\langle a \rangle < G$ then every $H < G$ with $a \in H$ has $\langle a \rangle < H$ as well.

One special case of this is **very useful** for comparing cyclic subgroups.

Corollary. If $a \in \langle b \rangle$ then $\langle a \rangle < \langle b \rangle$. In particular, if $a \in \langle b \rangle$ and $b \in \langle a \rangle$, then $\langle a \rangle = \langle b \rangle$.

Definition. A group G is **cyclic** if there is $a \in G$ such that $G = \langle a \rangle$.

Cyclic subgroups are very nice. In particular we get the following.

Proposition. $\langle a \rangle$ is commutative.

Example. Experimenting in $(\mathbb{Z}_n, +)$, we compute the following.

- In $\mathbb{Z}_3 = \{0, 1, 2\}$, both 1 and 2 generate the entire group since $2 + 2 = 1$.
So $\mathbb{Z}_3 = \langle 1 \rangle = \langle 2 \rangle$.
- In $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, both 1 and 3 generate the entire group but 2 doesn't since $3 + 3 = 1$, but $2 + 2 = 0$.
So $\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle$. On the other hand $\langle 2 \rangle = \{0, 2\}$.
- In $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, each of 1, 2, 3, 4 generate the entire group since $1 = 2 + 2 + 2 = 3 + 3 = 4 + 4 + 4 + 4$.
So $\mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle$.
- In $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ we see the following cyclic subgroups.
 - $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$
 - $\langle 3 \rangle = \{0, 3\}$
 - $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$

We use cyclic subgroups to define orders of elements. First recall the following.

Definition. The **order of a group** is the number of elements it contains (as a set), $|G| = \#G$.

If there are infinitely many elements, we say that the order is infinite.

Definition. The **order of an element** $a \in G$ is the order of the subgroup it generates, $|a| = |\langle a \rangle|$.

There is an alternate description of the **order of an element**.

Proposition. An element has **infinite order** if and only if $a^n \neq e$ for any power n .

An element has **order** $|a| = n$ if and only if n is the smallest non-negative integer so that $a^n = e$.

This has a number of immediate consequences.

Corollary. If $|a| = n$ is finite, then $a^{-1} = a^{n-1}$.

Corollary. If $|a| = n$ is finite, then $a^i = a^j$ if and only if $i \equiv j \pmod{n}$.

Corollary. If $|a|$ is infinite, then $a^i = a^j$ if and only if $i = j$.

Corollary. If $|a| = n$ is finite, then $|a^k| = \frac{n}{\gcd(k, n)}$.

We looked back at recent work and rephrased some of our understanding of S_3 in this language.

Recall. We can express $S_3 = \{e, x, x^2, y, xy, x^2y\}$ with relations $x^3 = e$, $y^2 = e$, and $yx = x^2y$.

S_3 has the following four cyclic subgroups, one of order 3 and three of order 2.

- $\langle x \rangle = \{x, x^2, x^3 = e\}$ “increment once, increment again, return to original position”
- $\langle y \rangle = \{y, y^2 = e\}$ “swap 1 \leftrightarrow 2 and swap back”
- $\langle xy \rangle = \{xy, (xy)^2 = e\}$ “swap 1 \leftrightarrow 3 and swap back”
- $\langle x^2y \rangle = \{x^2y, (x^2y)^2 = e\}$ “swap 2 \leftrightarrow 3 and swap back”

I'll sketch a proof which we didn't include in class, though I stated the proposition.

Proposition. *These are the only subgroups of S_3 .*

Proof sketch. Recall that if a subgroup contains a generator of a cyclic subgroup then it contains the entire cyclic subgroup. Note that x and x^2 both generate $\langle x \rangle$.

If a subgroup contains x or x^2 and any one of y , xy , x^2y , then it must contain all others, and thus must equal S_3 . Similarly if a subgroup contains any two of y , xy , x^2y then it contains x and so must equal S_3 . \square

Returning to the general situation, we finally showed that

Proposition. *All subgroups of cyclic groups are themselves cyclic.*

Corollary. *The only subgroups of \mathbb{Z} are $n\mathbb{Z} = \langle n \rangle$.*

Next came student presentations!

Proposition. *Elements and their inverse generate the same subgroup, $\langle a^{-1} \rangle = \langle a \rangle$.*

Proposition. *If all elements of a group have order 2, then the group is abelian.*

Proposition. *If $a, b \in G$ each have order 2 and commute, then ab also has order 2.*

Proposition. $|a| = |a^2|$ if and only if a has **odd** order.

Note that the middle two propositions above combine to yield the following.

Proposition. *If a and b both have order 2, then ab has order 2 if and only if a and b commute.*

We've seen one interesting example of this already! Recall the “Klein 4 group” – the smallest **non-cyclic** group. It can be written either as $\mathbb{Z}_2 \times \mathbb{Z}_2$ or as $\{e, a, b, ab\}$ where $a^2 = e$, $b^2 = e$, and $ab = ba$. These two expressions are connected by setting $a = (1, 0)$, $b = (0, 1)$, and $ab = (1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Note that even if a and b have order 2, unless there is some extra relation involving ab , the product could easily have infinite order. For example, the set $G = \{\text{strings of alternating } a \text{ and } b\}$ forms a group with the relation $a^2 = e, b^2 = e$. In this group $(ab)^n \neq e$ for any n . [Homework!]

The following statements finish off our investigation of subgroups of cyclic groups.

Proposition. *If G is cyclic and $H < G$, then $|G| = m|H|$ for some m .*¹

Theorem. *If G is cyclic of order n , then G has **exactly one** subgroup of order k for each divisor k of n .*

Corollary. *If $g \in G$ has order n , then $\langle g^k \rangle = \langle g^d \rangle$ where d is the greatest common divisor, $d = \gcd(k, n)$.*

Corollary. *If $g \in G$ has order n , then $\langle g^k \rangle = \langle g \rangle$ if and only if k and n are relatively prime.*

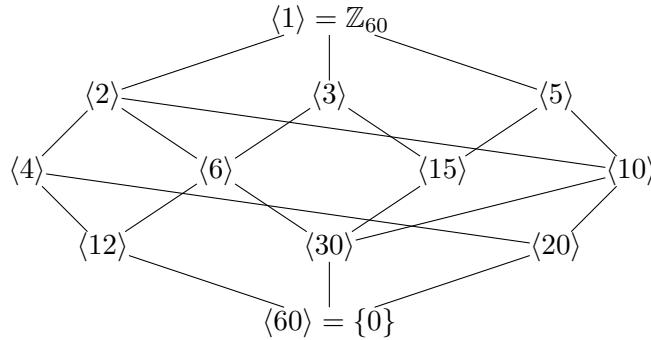
Corollary. $\langle k \rangle = \mathbb{Z}_n$ if and only if k and n are relatively prime.

¹We will eventually show this for subgroups of any group (not just cyclic).

An interesting consequence of the theorem above is that cyclic subgroups form a **lattice** (by divisors).

Example. The cyclic group of order 60, \mathbb{Z}_{60} has subgroup lattice shown below.

(“Hasse edges” connecting downwards indicate subgroups.)



Notice that the order of the subgroup $\langle k \rangle$ is $\frac{60}{k}$. For example

- $\langle 5 \rangle < \mathbb{Z}_{60}$ is $\langle 5 \rangle = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\}$ (order $\frac{60}{5} = 12$)
- $\langle 6 \rangle < \mathbb{Z}_{60}$ is $\langle 6 \rangle = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54\}$ (order $\frac{60}{6} = 10$)
- $\langle 12 \rangle < \mathbb{Z}_{60}$ is $\langle 12 \rangle = \{0, 12, 24, 36, 48\}$ (order $\frac{60}{12} = 5$)
- $\langle 15 \rangle < \mathbb{Z}_{60}$ is $\langle 15 \rangle = \{0, 15, 30, 45\}$ (order $\frac{60}{15} = 4$)

Proof of Theorem. Suppose that $G = \langle g \rangle$ is cyclic of order n . By previous work, we know that $\langle g^{n/k} \rangle$ is a subgroup of order k for each divisor k of n . We also know that no subgroups exist with other order since orders of subgroups divide the order of the group. It remains only to show that such subgroups are unique!

Suppose that $H < G = \langle g \rangle$ with $|H| = k$ (where k divides n). Since subgroups of cyclic groups are cyclic $H = \langle g^m \rangle$ for some m . We will show that $\langle g^m \rangle = \langle g^{n/k} \rangle$. Previously we noted that the order is $|g^m| = \frac{n}{\gcd(m,n)}$. Thus $k = \frac{n}{\gcd(m,n)}$. In other words, $\gcd(m,n) = \frac{n}{k}$; so in particular m is a multiple of $\frac{n}{k}$. Then $g^m \in \langle g^{n/k} \rangle$, which implies containment of the entire subgroup $\langle g^m \rangle < \langle g^{n/k} \rangle$.

However, these subsets both have k elements, so they must be equal. □