Cyclic Groups

**Cyclic groups** are groups in which every element is a power of some fixed element. (If the group is abelian and I’m using + as the operation, then I should say instead that every element is a *multiple* of some fixed element.) Here are the relevant definitions.

**Definition.** Let $G$ be a group, $g \in G$. The *order* of $g$ is the smallest positive integer $n$ such that $g^n = 1$. If there is no positive integer $n$ such that $g^n = 1$, then $g$ has **infinite order**.

In the case of an abelian group with + as the operation and 0 as the identity, the order of $g$ is the smallest positive integer $n$ such that $ng = 0$.

**Definition.** If $G$ is a group and $g \in G$, then the **subgroup generated by** $g$ is

$$\langle g \rangle = \{ g^n | n \in \mathbb{Z} \}.$$  

If the group is abelian and I’m using + as the operation, then

$$\langle g \rangle = \{ ng | n \in \mathbb{Z} \}.$$  

**Definition.** A group $G$ is **cyclic** if $G = \langle g \rangle$ for some $g \in G$. $g$ is a **generator** of $\langle g \rangle$.

If a generator $g$ has order $n$, $G = \langle g \rangle$ is **cyclic of order** $n$. If a generator $g$ has infinite order, $G = \langle g \rangle$ is **infinite cyclic**.

**Example.** $\mathbb{Z}$ is an infinite cyclic group. (In fact, it is the only infinite cyclic group up to isomorphism.) Notice that $\mathbb{Z}$ is generated by 1 and by $-1$ — a cyclic group can have more than one generator.

If $n$ is a positive integer, $\mathbb{Z}_n$ is a cyclic group of order $n$ generated by 1.

For example,

$$\mathbb{Z}_7 = \{ 0, 1, 2, 3, 4, 5, 6 \}$$

is cyclic of order 7. 1 generates $\mathbb{Z}_7$, since

\[
\begin{align*}
1 + 1 &= 2 \\
1 + 1 + 1 &= 3 \\
1 + 1 + 1 + 1 &= 4 \\
1 + 1 + 1 + 1 + 1 &= 5 \\
1 + 1 + 1 + 1 + 1 + 1 &= 6 \\
1 + 1 + 1 + 1 + 1 + 1 + 1 &= 0
\end{align*}
\]

In other words, if you add 1 to itself repeatedly, you eventually cycle back to 0.

\[\text{a cyclic group of order 7}\]
Notice that 3 also generates $\mathbb{Z}_7$:

\[
\begin{align*}
3 + 3 &= 6 \\
3 + 3 + 3 &= 2 \\
3 + 3 + 3 + 3 &= 5 \\
3 + 3 + 3 + 3 + 3 &= 1 \\
3 + 3 + 3 + 3 + 3 + 3 &= 4 \\
3 + 3 + 3 + 3 + 3 + 3 + 3 &= 0
\end{align*}
\]

The “same” group can be written using multiplicative notation this way:

$$\mathbb{Z}_7 = \{1, a, a^2, a^3, a^4, a^5, a^6\}.$$

In this form, $a$ is a generator of $\mathbb{Z}_7$.

It turns out that in $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, every nonzero element generates the group.

On the other hand, in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 generate. \(\square\)

**Lemma.** Let $G = \langle g \rangle$ be a finite cyclic group, where $g$ has order $n$. Then the powers \{1, $g$, $g^2$, \ldots, $g^{n-1}$\} are distinct.

**Proof.** Since $g$ has order $n$, $g$, $g^2$, \ldots, $g^{n-1}$ are all different from 1.

Now I’ll show that the powers \{1, $g$, $g^2$, \ldots, $g^{n-1}$\} are distinct. Suppose $g^i = g^j$ where $0 \leq j < i < n$. Then $0 < i - j < n$ and $g^{i-j} = 1$, contrary to the preceding observation.

Therefore, the powers \{1, $g$, $g^2$, \ldots, $g^{n-1}$\} are distinct. \(\square\)

**Lemma.** Let $G = \langle g \rangle$ be infinite cyclic. If $m$ and $n$ are integers and $m \neq n$, then $g^m \neq g^n$.

**Proof.** One of $m$, $n$ is larger — suppose without loss of generality that $m > n$. I want to show that $g^m \neq g^n$; suppose this is false, so $g^m = g^n$. Then $g^{m-n} = 1$, so $g$ has finite order. This contradicts the fact that a generator of an infinite cyclic group has infinite order. Therefore, $g^m \neq g^n$. \(\square\)

The next result characterizes subgroups of cyclic groups. The proof uses the Division Algorithm for integers in an important way.

**Theorem.** Subgroups of cyclic groups are cyclic.

**Proof.** Let $G = \langle g \rangle$ be a cyclic group, where $g \in G$. Let $H < G$. If $H = \{1\}$, then $H$ is cyclic with generator $1$. So assume $H \neq \{1\}$.

To show $H$ is cyclic, I must produce a generator for $H$. What is a generator? It is an element whose powers make up the group. A thing should be smaller than things which are “built from” it — for example, a brick is smaller than a brick building. Since elements of the subgroup are “built from” the generator, the generator should be the “smallest” thing in the subgroup.

What should I mean by “smallest”? Well, $G$ is cyclic, so everything in $G$ is a power of $g$. With this discussion as motivation, let $m$ be the smallest positive integer such that $g^m \in H$.

Why is there such an integer $m$? Well, $H$ contains something other than $1 = g^0$, since $H \neq \{1\}$. That “something other” is either a positive or negative power of $g$. If $H$ contains a positive power of $g$, it must contain a smallest positive power, by well ordering.

On the other hand, if $H$ contains a negative power of $g$ — say $g^{-k}$, where $k > 0$ — then $g^k \in H$, since $H$ is closed under inverses. Hence, $H$ again contains positive powers of $g$, so it contains a smallest positive power, by Well Ordering.

So I have $g^m$, the smallest positive power of $g$ in $H$. I claim that $g^m$ generates $H$. I must show that every $h \in H$ is a power of $g^k$. Well, $h \in H < G$, so at least I can write $h = g^n$ for some $n$. But by the Division Algorithm, there are unique integers $q$ and $r$ such that

$$n = mq + r, \quad \text{where} \quad 0 \leq r < m.$$
It follows that
\[ g^r = g^{mq+r} = (g^m)^q \cdot g^r, \quad \text{so} \quad h = (g^m)^q \cdot g^r, \quad \text{or} \quad g^r = (g^m)^{-q} \cdot h. \]

Now \( g^m \in H \), so \((g^m)^{-q} \cdot h \in H\). Hence, \((g^m)^{-q} \cdot h \in H\). However, \( g^m \) was the smallest positive power of \( g \) lying in \( H \). Since \( g^r \in H \) and \( r < m \), the only way out is if \( r = 0 \). Therefore, \( n = qm \), and \( h = g^m = (g^m)^q \cdot (g^m) \).

This proves that \( g^m \) generates \( H \), so \( H \) is cyclic. \( \square \)

---

**Example.** In case \( G = \mathbb{Z} \), the proof of the theorem shows that every subgroup has the form \( n\mathbb{Z} \) for \( n \in \mathbb{Z} \).

For example, \[ 13\mathbb{Z} = \langle 13 \rangle = \{ \ldots, -26, -13, 0, 13, 26, \ldots \} \]
is a subgroup of \( \mathbb{Z} \). \( \square \)

---

**Lemma.** Let \( G \) be a group, and let \( g \in G \) have order \( m \). Then \( g^n = 1 \) if and only if \( m \) divides \( n \).

**Proof.** If \( m \) divides \( n \), then \( n = mq \) for some \( q \), so \( g^n = (g^m)^q = 1 \).

Conversely, suppose that \( g^n = 1 \). By the Division Algorithm,
\[ n = mq + r \quad \text{where} \quad 0 \leq r < m. \]

Hence,
\[ g^n = g^{mq+r} = (g^m)^q \cdot g^r \quad \text{so} \quad 1 = g^r. \]

Since \( m \) is the smallest positive power of \( g \) which equals \( 1 \), and since \( r < m \), this is only possible if \( r = 0 \). Therefore, \( n = qm \), which means that \( m \) divides \( n \). \( \square \)

---

**Example.** If I tell you that an element \( g \) in a group \( G \) satisfies \( g^{45} = 1 \), then the order of \( g \) must be a divisor of \( 45 \). Thus, the order could be
\[ 1, \quad 3, \quad 5, \quad 9, \quad 15, \quad \text{or} \quad 45. \]

And the order is certainly not (say) \( 7 \), since \( 7 \) doesn’t divide \( 45 \). \( \square \)

---

Thus, the order of an element is the smallest power which gives the identity the element in two ways. It is smallest in the sense of being numerically smallest, but it is also smallest in the sense that it divides any power which gives the identity.

Next, I’ll find a formula for the order of an element in a cyclic group.

**Proposition.** Let \( G = \langle g \rangle \) be a cyclic group of order \( n \), and let \( m < n \). Then \( \langle g^m \rangle \) has order \( \frac{n}{(m,n)} \).

**Proof.** Since \( (m,n) \) divides \( m \), it follows that \( \frac{m}{(m,n)} \) is an integer. Therefore, \( n \) divides \( \frac{mn}{(m,n)} \), and \( (g^m)^{\frac{n}{(m,n)}} = 1 \)

by the last lemma. Thus, \( \frac{n}{(m,n)} \) is a power which kills \( g^m \).

Now suppose that \((g^m)^k = 1 \). By the preceding lemma, \( n \) divides \( mk \), so
\[ \frac{n}{(m,n)} \quad \text{divides} \quad k \cdot \frac{m}{(m,n)}. \]

---
However, \( \left( \frac{n}{(m,n)} \right) = 1 \), so \( \frac{n}{(m,n)} \) divides \( k \). Thus, \( \frac{n}{(m,n)} \) divides any power of \( g^m \) which is 1, so it is the order of \( g^m \). □

In terms of \( \mathbb{Z}_n \), this result says that \( m \in \mathbb{Z}_n \) has order \( \frac{n}{(m,n)} \).

**Example.** Find the order of the element \( a^6 \) in the cyclic group \( G = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7\} \).

In the notation of the Proposition, \( n = 8 \) and \( m = 6 \). Since \( (n, m) = 6,8 = 2 \), \( a^6 \) has order \( n/2 = 4 \). Check:

\[
(a^6)^1 = a^6, \quad (a^6)^2 = a^{12} = a^4, \quad (a^6)^3 = a^{18} = a^2, \quad (a^6)^4 = a^{24} = 1. \]

**Example.** Find the order of the element \( 18 \in \mathbb{Z}_{30} \).

In this case, I'm using *additive* notation instead of multiplicative notation. The group is cyclic with order \( n = 30 \), and the element \( 18 \in \mathbb{Z}_{30} \) corresponds to \( a^{18} \) in the Proposition — so \( m = 18 \).

\( 18,30 \) = 6, so the order of 18 is \( \frac{30}{6} = 5 \). Check:

\[
2 \cdot 18 = 6, \quad 3 \cdot 18 = 24, \quad 4 \cdot 18 = 12, \quad 5 \cdot 18 = 0. \]

Next, I’ll give two important Corollaries of the proposition.

**Corollary.** The generators of \( \mathbb{Z}_n = \{0,1,2,\ldots, n-1\} \) are the elements of \( \{0,1,2,\ldots, n-1\} \) which are relatively prime to \( n \).

**Proof.** If \( m \in \{0,1,2,\ldots, n-1\} \) is a generator, its order is \( n \). The Proposition says its order is \( \frac{n}{(m,n)} \). Therefore, \( n = \frac{n}{(m,n)} \), so \( (m,n) = 1 \).

Conversely, if \( (m,n) = 1 \), then the order of \( m \) is

\[
\frac{n}{(m,n)} = \frac{n}{1} = n.
\]

Therefore, \( m \) is a generator of \( \mathbb{Z}_n \). □

**Example.** The generators of \( \mathbb{Z}_{12} \) are 1, 5, 7, and 11. These are the elements of \( \{0,1,2,\ldots, 11\} \) which are relatively prime to 12.

The generators of \( \mathbb{Z}_5 \) are 1, 2, 3, and 4.

In fact, if \( p \) is prime, the generators of \( \mathbb{Z}_p \) are 1, 2, \ldots, \( p-1 \). □

**Corollary.** A finite cyclic group of order \( n \) contains a subgroup of order \( m \) for each positive integer \( m \) which divides \( n \).

**Proof.** Suppose \( G \) is a finite cyclic group of order \( n \) with generator \( g \), and suppose \( m \mid n \). Thus, \( mp = n \) for some \( p \).
I claim that $g^p$ generates a subgroup of order $m$. The preceding proposition says that the order of $g^p$ is $\frac{n}{(p,n)}$. However, $p \mid n$, so $(p,n) = p$. Therefore, $g^p$ has order $\frac{n}{p} = m$. 

In other words, $g^p$ generates a subgroup of order $m$. $\blacksquare$

In fact, it’s possible to prove that there is a unique subgroup of order $m$ for each $m$ dividing $n$.

Note that for an arbitrary finite group $G$, it isn’t true that if $n \mid |G|$, then $G$ contains a cyclic subgroup of order $n$.

**Example.** $\mathbb{Z}_{15}$ contains subgroups of order 1, 3, 5, and 15, since these are the divisors of 15. The subgroup of order 1 is the identity, and the subgroup of order 15 is the entire group.

The last result says:

- If $n$ divides 15, then there is a subgroup of order $n$ — in fact, a unique subgroup of order $n$.

Since $\mathbb{Z}_{15}$ is cyclic, these subgroups must be cyclic. They are generated by 0 and the nonzero elements in $\mathbb{Z}_{15}$ which divide 15: 1, 3, and 5.

**Lagrange’s theorem** (which I’ll discuss later) says that in any finite group, the order of a subgroup must divide the order of the group. In this context, Lagrange’s theorem says:

- If $H$ is a subgroup of order $n$, then $n$ divides 15.

Putting these results together, this means that:

- You can find all the subgroups of $\mathbb{Z}_{15}$ by taking $\{0\}$ (the trivial subgroup), together with the cyclic subgroups generated by the nonzero elements in $\mathbb{Z}_{15}$ which divide 15: 1, 3, and 5.

For example, 5 generates a subgroup of order 3:

$$\langle 5 \rangle = \{0, 5, 10\}.$$

Likewise, 3 generates a subgroup of order 5:

$$\langle 3 \rangle = \{0, 3, 6, 9, 12\}.$$

Similarly, here are all the subgroups of $\mathbb{Z}_{24}$:

$$\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle, \langle 8 \rangle, \langle 12 \rangle.$$

The subgroup generated by 3 has order 8:

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}. \quad \blacksquare$$

**Example.** Consider the group

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(m,n) \mid m \in \mathbb{Z}_2, n \in \mathbb{Z}_3\}.$$

The operation is componentwise addition:

$$(m, n) + (m', n') = (m + m', n + n').$$

It is routine to verify that this is a group, the **direct product** of $\mathbb{Z}_2$ and $\mathbb{Z}_3$. 

5
The element \((1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3\) has order 6:

\[
\begin{align*}
(1,1) + (1,1) &= (0,2), \\
(1,1) + (0,2) &= (1,0), \\
(1,1) + (1,0) &= (0,1), \\
(1,1) + (0,1) &= (1,2), \\
(1,1) + (1,2) &= (0,0).
\end{align*}
\]

Hence, \(\mathbb{Z}_2 \times \mathbb{Z}_3\) is cyclic of order 6. More generally, if \((m,n) = 1\), then \(\mathbb{Z}_m \times \mathbb{Z}_n\) is cyclic of order \(mn\). Be careful! \(\mathbb{Z}_2 \times \mathbb{Z}_2\) is not the same as \(\mathbb{Z}_4\). \(\square\)