3 Cyclic groups

Cyclic groups are a very basic class of groups: we have already seen some examples such as $\mathbb{Z}_n$. Cyclic groups are nice in that their complete structure can be easily described. The overall approach in this section is to define and classify all cyclic groups and to understand their subgroup structure.

3.1 Definitions and Examples

The basic idea of a cyclic group is that it can be generated by a single element. Here are two motivating examples:

1. The group of integers under addition can be generated by $1$. By this we mean that the element $1$ can be combined with itself using only the group operation and inverses to produce the entire set of integers: if $n > 0$, then
   $$n = 1 + 1 + \cdots + 1$$
   from which we can easily produce $-n$ and $0 = 1 + (-1)$. The element $-1$ could also be used to generate $\mathbb{Z}$.

2. The group $U_4 = \{1, -1, i, -i\}$ of $4^{th}$ roots of unity under multiplication and also be generated from a single element $i$:
   $$U_4 = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$$
   The same construction can be performed using $-i$.

Now we formalize this idea.

Lemma 3.1. Let $G$ be a multiplicative group and let $g \in G$. Then the set
$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\} = \{\ldots, g^{-1}, e, g, g^2, \ldots\}$$
is a subgroup of $G$.

Proof. Non-emptiness Clearly $e \in \langle g \rangle$ (similarly $g \in \langle g \rangle$).

Closure Every element of $\langle g \rangle$ has the form $g^k$ for some $k \in \mathbb{Z}$. It suffices to check that
$$g^k \cdot g^l = g^{k+l} \in \langle g \rangle$$

Inverses Since $(g^k)^{-1} = g^{-k} \in \langle g \rangle$, we are done.

Definition 3.2. The subgroup $\langle g \rangle$ defined in Lemma 3.1 is the cyclic subgroup of $G$ generated by $g$. The order of an element $g \in G$ is the order $|\langle g \rangle|$ of the subgroup generated by $g$. $G$ is a cyclic group if $\exists g \in G$ such that $G = \langle g \rangle$: we call $g$ a generator of $G$.

We now have two concepts of order.

The order of a group is the cardinality of the group viewed as a set.

The order of an element is the cardinality of the cyclic group generated by that element.

Cyclic groups are the precisely those groups containing elements having the same order as that of the group: these are the generators of the cyclic group.
Examples

Integers The integers \( \mathbb{Z} \) form a cyclic group under addition. \( \mathbb{Z} \) is generated by either 1 or \(-1\). Note that this group is written additively, so that, for example, the subgroup generated by 2 is the group of even numbers under addition:

\[
\langle 2 \rangle = \{2m : m \in \mathbb{Z}\} = 2\mathbb{Z}.
\]

Modular Addition For each \( n \in \mathbb{N} \), the group of remainders \( \mathbb{Z}_n \) under addition modulo \( n \) is a cyclic group. It is also written additively, and is generated by 1. Typically \( \mathbb{Z}_n \) is also generated by several other elements. For example, \( \mathbb{Z}_4 = \{0, 1, 2, 3\} \) is generated by both 1 and 3:

\[
\langle 1 \rangle = \{1, 2, 3, 0\} \quad \langle 3 \rangle = \{3, 2, 1, 0\}
\]

Roots of Unity For each \( n \in \mathbb{N} \), the \( n \)th roots of unity \( U_n = \{1, \zeta, \ldots, \zeta^{n-1}\} \) form a cyclic group under multiplication. This group is generated by \( \zeta \), amongst others. The generators of \( U_n \) are termed the primitive \( n \)th roots of unity.

We shall see shortly that every cyclic group is isomorphic to either the integers or the modular integers. Regardless, we will still write abstract cyclic groups multiplicatively. This, at least in part, is because the application of cyclic groups very often involves the study of cyclic subgroups of more complex groups, rather than of cyclic groups in their own right.

3.2 Classification of Cyclic Groups

Our first goal is to describe all cyclic groups.

Lemma 3.3. Every cyclic group is abelian.

Proof. Let \( G = \langle g \rangle \). Then any two elements of \( G \) can be written \( g^k, g^l \) for some \( k, l \in \mathbb{Z} \). But then

\[
g^k g^l = g^{k+l} = g^{l+k} = g^l g^k,
\]

and so \( G \) is abelian.

Note that the converse is false: the Klein 4-group \( V \) is abelian but not cyclic.

Before going any further, we need to distinguish between finite and infinite groups. To do this, suppose that \( G = \langle g \rangle \) is cyclic, and consider the following set of natural numbers\(^1\)

\[
S = \{m \in \mathbb{N} : g^m = e\}
\]

The distinction hinges on whether the set \( S \) is empty or not.

\(^1\)Recall \( \mathbb{N} = \{1, 2, 3, \ldots\} \).
Infinite Cyclic Groups

Theorem 3.4. Suppose $G = \langle g \rangle$ is cyclic and that the set $S = \{m \in \mathbb{N} : g^m = e\}$ is empty. Then $G$ is an infinite group and we have an isomorphism $G \cong \mathbb{Z}$ via

$$\mu : \mathbb{Z} \to G : x \mapsto g^x$$

Proof. We simply check the properties of $\mu$:

Injectivity WLOG assume that $x \geq y$. Then

$$\mu(x) = \mu(y) \implies g^x = g^y \implies g^{x-y} = e \implies x - y = 0 \implies x = y$$

since $S = \emptyset$. Thus $\mu$ is 1–1.

Surjectivity $\mu$ is onto by definition: every element of $G$ has the form $g^x$ for some $x \in \mathbb{Z}$.

Homomorphism $\mu(x + y) = g^{x+y} = g^x g^y = \mu(x) \mu(y)$.

Finite Cyclic Groups

Theorem 3.5. Suppose that $G = \langle g \rangle$ is cyclic and that $S = \{m \in \mathbb{N} : g^m = e\}$ is non-empty. By the well-ordering of $\mathbb{N}$, there exists a natural number $n = \min S$. Then $G \cong \mathbb{Z}_n$ via the isomorphism $^2$

$$\mu : \mathbb{Z}_n \to G : [x] \mapsto g^x$$

In particular, $n$ is the order of $G$.

The proof is almost identical to that for infinite groups with two important differences: we need to check well-definition of $\mu$ since the domain is a set of equivalence classes, and we need to apply the division algorithm to invoke the injectivity argument.

Proof. Check the properties of $\mu$.

Well-definition $[x] = [y] \implies y = x + \lambda n$ for some $\lambda \in \mathbb{Z}$. But then

$$\mu([x]) = g^x = g^y g^{\lambda n} = g^y = \mu([y])$$

since $g^n = e$.

Injectivity Suppose that $\mu([x]) = \mu([y])$. Then

$$g^x = g^y \implies g^{x-y} = e$$

Apply the division algorithm: $x - y = \lambda n + r$ for unique integers $\lambda, r$ with $0 \leq r < n$. But then

$$e = g^{x-y} = g^{\lambda n} g^r = g^r \implies r = 0$$

since $r < n$. But then $x - y = \lambda n \implies [x] = [y]$.

Surjectivity This is by definition of $\mu$.

Homomorphism As in the infinite case, $\mu([x + y]) = g^{x+y} = g^x g^y = \mu([x]) \mu([y])$.

---

2We use the equivalence class notation $[x] = \{x + \lambda n : \lambda \in \mathbb{Z}\}$ to be clear regarding the nature of the elements of $\mathbb{Z}_n$. In particular, this stresses the fact that we need to check well-definition of $\mu$. 

3
Examples

1. The group of 7th roots of unity \((U_7, \cdot)\) is isomorphic to \((\mathbb{Z}_7, +)\) via the isomorphism
\[
\phi : \mathbb{Z}_7 \to U_7 : k \mapsto \xi_7^k
\]

2. The group \(5\mathbb{Z} = \langle 5 \rangle\) is an infinite cyclic group. It is isomorphic to the integers via
\[
\phi : (\mathbb{Z}, +) \cong (5\mathbb{Z}, +) : z \mapsto 5z
\]

3. The real numbers \(\mathbb{R}\) form an infinite group under addition. This cannot be cyclic because its cardinality \(2^{\aleph_0}\) is larger than the cardinality \(\aleph_0\) of the integers.

The cyclic group of order \(n\)?

Given the Theorem, we see that all cyclic groups of order \(n\) are isomorphic. This is usually summarized by saying that there is exactly one cyclic group of order \(n\) (up to isomorphism). We label this abstract group \(C_n\).

The fact that \(C_n\) is somewhat nebulous turns out to be convenient. For example: in some texts you may find \(\mathbb{Z}_6\) referred to as the cyclic group of order 6. What, then, should we call the subgroup
\[
\langle 2 \rangle = \{2, 4, 6, 8, 10, 0\} \leq (\mathbb{Z}_{12}, +)?
\]

Certainly \(\langle 2 \rangle\) is isomorphic to \(\mathbb{Z}_6\) via \(\phi : 2z \mapsto z\). It would be erroneous however to say that \(\langle 2 \rangle\) equals \(\mathbb{Z}_6\), since \(\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}\) has different elements.
The notation \(C_6\) is neutral: it’s elements have no explicit interpretation. It is therefore a little safer to write \(\langle 2 \rangle \cong C_6\).

3.3 Subgroups of cyclic groups

We can very straightforwardly classify all the subgroups of a cyclic group.

**Theorem 3.6.** All subgroups of a cyclic group are themselves cyclic.

**Proof.** Let \(G = \langle g \rangle\) and let \(H \leq G\). If \(H = \{e\}\) is trivial, we are done. Otherwise, since all elements of \(H\) are in \(G\), there must exist a smallest natural number \(s\) such that \(g^s \in H\). We claim that \(H = \langle g^s \rangle\).

Let \(g^m \in H\) be a general element of \(H\). The division algorithm says that there exist unique integers \(q, r\) such that
\[
m = qs + r \quad \text{and} \quad 0 \leq r < s
\]

Therefore
\[
g^m = g^{qs+r} = (g^s)^q g^r \implies g^r = (g^s)^{-q} g^m \in H
\]
since \(H\) is closed under \(\cdot\) and inverses. But this forces \(r = 0\), since \(r < s\).

In summary \(g^m = (g^s)^q \in \langle g^s \rangle\) and we are done.

\[3\text{Well-ordering again…}\]
Subgroups of infinite cyclic groups

If $G$ is an infinite cyclic group, then any subgroup is itself cyclic and thus generated by some element. It is easiest to think about this for $G = \mathbb{Z}$. There are two cases:

- The trivial subgroup: $\langle 0 \rangle = \{0\} \leq \mathbb{Z}$.
- Every other subgroup: $\langle s \rangle = s\mathbb{Z} \leq \mathbb{Z}$ for $s \neq 0$. All these subgroups are isomorphic to $\mathbb{Z}$ via the isomorphism $\mu: \mathbb{Z} \to s\mathbb{Z}: x \mapsto sx$.

It should also be clear that $n\mathbb{Z} \leq m\mathbb{Z} \iff n \mid m$.

In the language of an abstract cyclic group $G = \langle g \rangle$ the non-trivial subgroups have the form

$\langle g^s \rangle \cong G$ via $\mu: G \to \langle g^s \rangle: g^x \mapsto g^{sx}$

You should be comfortable comparing notations.

Subgroups of finite cyclic groups

As above, it is easier to consider the case where $G = \mathbb{Z}_n$ first. We state the general result afterwards.

**Theorem 3.7.** Let $s \in \mathbb{Z}_n$. Then $\langle s \rangle \cong \mathbb{Z}_{\gcd(n)}$.

More precisely, let $d = \gcd(s, n)$. Then $\langle s \rangle = \langle d \rangle$ as subgroups of $\mathbb{Z}_n$. Moreover, $\langle d \rangle \cong \mathbb{Z}_{\frac{n}{d}}$.

**Proof.** Let $d = \gcd(s, n)$. Since $d \mid n$ we see that $s \in \langle d \rangle \implies \langle s \rangle \leq \langle d \rangle$.

Conversely, by Bézout’s identity, $d = \lambda s + \sigma n$ for some $\lambda, \sigma \in \mathbb{Z}$, from which $d \equiv \lambda s \pmod{n}$. But then $d \in \langle s \rangle \implies \langle d \rangle \leq \langle s \rangle$.

Since $d \mid n$, there are precisely $\frac{n}{d}$ elements in $\langle d \rangle$, indeed

$\langle d \rangle = \left\{0, d, 2d, \ldots, \left(\frac{n}{d} - 1\right)d\right\}$

**Corollary 3.8.**
1. If $d \mid n$, then $\mathbb{Z}_n$ has precisely one subgroup of order $d$.
2. If $G = \langle g \rangle$ has order $n$ and $d \mid n$, then $G$ has precisely one subgroup of order $d$. Indeed

$\langle g^s \rangle = \langle g^t \rangle \iff \gcd(s, n) = \gcd(t, n)$

and this subgroup has order $\frac{n}{\gcd(s, n)}$.

Summary

We now know everything there is to know about cyclic groups and their subgroups.

1. Is $G = \langle g \rangle$ infinite? If yes, then $G \cong \mathbb{Z}$ via $g^x \leftrightarrow x$. Every subgroup has the form $\langle g^s \rangle$: these are distinct for each $s$. A subgroup is trivial if $s = 0$ and isomorphic to $G$ otherwise.

2. Is $G$ finite? Then $G \cong \mathbb{Z}_n$ where $n = \min\{k \in \mathbb{N} : g^k = e\}$. There exists exactly one subgroup of $G$ for each divisor $d$ of $n$:

$H = \langle g^s \rangle \leq G$ has $H \cong \mathbb{Z}_{\frac{n}{\gcd(s, n)}}$

Armed with this information, it is easy to construct the complete subgroup diagrams for some cyclic groups. Indeed you will probably need to work several examples in order to learn and believe all these theorems!
Examples

1. $\mathbb{Z}_8$ is generated by 1, 3, 5 and 7, since these are precisely the elements $s \in \mathbb{Z}_8$ for which $\gcd(s, 8) = 1$. For example,

$$
\mathbb{Z}_8 = \langle 5 \rangle = \{5, 2, 7, 4, 1, 6, 3, 0\} \cong \mathbb{Z}_{\frac{8}{\gcd(5,8)}}
$$

The subgroup generated by 6 is

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

which has order $4 = \frac{8}{\gcd(6,8)}$ in accordance with the Theorem. This subgroup is also generated by 2. The complete collection of subgroups and their generators is shown in the table, and the subgroup diagram is also drawn.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\gcd(x, 8)$</th>
<th>$\frac{8}{\gcd(x, 8)}$</th>
<th>subgroup generated $\langle x \rangle$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0(8)</td>
<td>0(8)</td>
<td>1</td>
<td>$\mathbb{C}_1$</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>$\mathbb{C}_2$</td>
</tr>
<tr>
<td>2, 6</td>
<td>2</td>
<td>4</td>
<td>$\mathbb{C}_4$</td>
</tr>
<tr>
<td>1, 3, 5, 7</td>
<td>1</td>
<td>8</td>
<td>$\mathbb{Z}_8$</td>
</tr>
</tbody>
</table>

2. Here we find all the subgroups of $\mathbb{Z}_{30}$. Note that $30 = 2 \cdot 3 \cdot 5$. We list all the elements of $\mathbb{Z}_{30}$ according to their greatest common divisor with 30, and then the subgroup generated by each. According to the above results, each subgroup in the right column is generated by any of the numbers in the left column.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\gcd(x, 30)$</th>
<th>$\frac{30}{\gcd(x, 30)}$</th>
<th>subgroup generated $\langle x \rangle$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0(30)</td>
<td>0(30)</td>
<td>1</td>
<td>$\mathbb{C}_1$</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>2</td>
<td>$\mathbb{C}_2$</td>
</tr>
<tr>
<td>10, 20</td>
<td>10</td>
<td>3</td>
<td>$\mathbb{C}_3$</td>
</tr>
<tr>
<td>6, 12, 18, 24</td>
<td>6</td>
<td>5</td>
<td>$\mathbb{C}_5$</td>
</tr>
<tr>
<td>5, 25</td>
<td>5</td>
<td>6</td>
<td>$\mathbb{C}_6$</td>
</tr>
<tr>
<td>3, 9, 21, 27</td>
<td>3</td>
<td>10</td>
<td>$\mathbb{C}_{10}$</td>
</tr>
<tr>
<td>2, 4, 8, 14, 16, 22, 26, 28</td>
<td>2</td>
<td>15</td>
<td>$\mathbb{C}_{15}$</td>
</tr>
<tr>
<td>1, 7, 11, 13, 17, 19, 23, 29</td>
<td>1</td>
<td>30</td>
<td>$\mathbb{Z}_{30}$</td>
</tr>
</tbody>
</table>

Here is the subgroup diagram for $\mathbb{Z}_{30}$ with the obvious generator chosen for each subgroup.
3.4 Generating sets — non-examinable

**Definition 3.9.** If \( X \subseteq G \) is a subset of a group \( G \) then the subgroup of \( G \) generated by \( X \) is the subgroup created by making all possible combinations of elements and inverses of elements in \( X \). The subgroup generated by \( X \) will be written as \( \langle x \in X \rangle \).

\( G \) is _finitely generated_ if there exists a finite subset of \( G \) which generates \( G \).

The subgroup of \( G \) generated by \( X \) really is a subgroup: it is certainly a subset, so we need only check that it is closed under multiplication and inverses. However, the definition says that we keep throwing things into the subgroup so that it satisfies precisely these conditions!

**Examples**

1. \((\mathbb{Z}, +) = \langle 2, 3 \rangle\). The inverse of 2 = -2 must lie in \( \langle 2, 3 \rangle \). But then \( 3 + (-2) = 1 \in \langle 2, 3 \rangle \). Since 1 generates \( \mathbb{Z} \), we are done.

2. In general if \( m, n \in \mathbb{Z} \) then the subgroup \( \langle m, n \rangle = \{ \lambda m + \mu n : \lambda, \mu \in \mathbb{Z} \} \) is \( \langle d \rangle = d\mathbb{Z} \) where \( d = \text{gcd}(m, n) \).

3. The dihedral group of rotations and reflections of a regular \( n \)-gon can be seen to be generated by the 1-step rotation \( \rho_1 \) and _any_ reflection \( \mu \): that is \( D_n = \langle \rho_1, \mu \rangle \).

4. \((\mathbb{Q}, +) = \langle \frac{1}{n} : n \in \mathbb{Z}^+ \rangle\). \((\mathbb{Q}, +)\) is not finitely generated: there exists no finite subset which generates \( \mathbb{Q} \). To see this, consider the subgroup generated by some finite set \( X = \{ \frac{m_i}{n_i} \}_{i=1}^k \). Now let \( p \) be a prime which does not divide any of the denominators \( n_i \) (there are infinitely many primes and each \( n_i \) can have only finitely many divisors...). It is then impossible to create the fraction \( \frac{1}{p} \) from the set \( X \).

If this seems a little tricky, consider that if \( X = \{ \frac{1}{2}, \frac{1}{3} \} \), then

\[
\langle x \in X \rangle = \left\{ \frac{3m + 2n}{6} : m, n \in \mathbb{Z} \right\} = \left\{ \frac{k}{6} : k \in \mathbb{Z} \right\}
\]

for reasons similar to example 2. Clearly this subgroup does not contain \( \frac{1}{2} \).