Groups are very general things, and thus we don't have much control over them. However, there are some groups which are much easier to understand and gain control over. These are the cyclic groups. Cyclic groups are very nice because any element in the cyclic group must be of a certain form. We thus open with the motivating example of the integers.

Example 0.1 (The integers)**.** Let $G = \mathbb{Z}$. Consider any integer $n \in \mathbb{Z}$. Since $n = 1 + \cdots + 1$, n times, we can write $n = n \cdot 1$. Every integer is of this form, a multiple of 1. Thus, $\mathbb{Z} = \{ n \cdot 1 : n \in \mathbb{Z} \}$. Alternatively, we could say that $n = -n \cdot -1$, and so $\mathbb{Z} = \{ n \cdot -1 : n \in \mathbb{Z} \}$. //

It seems that 1 and -1 *generate* the entire group of integers (under addition), and indeed this is true.

Definition 0.2 (Cyclic group)**.** Let G be a group. Then G is **cyclic** if there is a $g \in G$ such that $G = \{ g^n : n \in \mathbb{Z} \}$. Such an element g is called a **generator** of G.

If G is cyclic and g is a generator of G, we denote this situation with $G = \langle g \rangle$.

Example 0.3 (Cyclic subgroups)**.** Let G be a group and $g \in G$. Then, $\langle g \rangle$ is a subgroup of G. //

Exercise 0.4. Prove that $\langle g \rangle$ is a subgroup of G.

Example 0.5 (Integers modulo n)**.** Let $G = \mathbb{Z}_n$. Notice that this is again a cyclic group under addition modulo n. Of course, 1 remains a generator for G. However, unlike $\mathbb{Z}$, which only has 2 generators, $\mathbb{Z}_n$ could have more than one. We will see this in the next example. //

Example 0.6. Let $G = \mathbb{Z}_6$. Then $G = \langle 1 \rangle = \langle 5 \rangle$. However, 2 is not a generator of G as $\langle 2 \rangle = \{ 0, 2, 4 \}$ which is not all of $\mathbb{Z}_6$. //

Example 0.7 (Non-example of a cyclic group)**.** Let $G = U(8)$. Then, G is not cyclic, as $\langle 1 \rangle = \{ 1 \}$, $\langle 3 \rangle = \{ 1, 3 \}$, $\langle 5 \rangle = \{ 1, 5 \}$ and $\langle 7 \rangle = \{ 1, 7 \}$. //

Taking $G = \mathbb{Z}_6$, we notice that $4 \cdot 2 = 1 \cdot 2$. In general, we would like to be able to tell when a^i and a^j are the same element (and when they are not). The next theorem gives necessary and sufficient conditions to be able to determine this.

Theorem 0.8. Let G be a group and $a \in G$. If a has infinite order then $a^i = a^j$ if and only if $i = j$. If a has order n then $\langle a \rangle = \{ e, a, a^2, \ldots, a^{n-1} \}$ and $a^i = a^j$ if and only if n divides $i - j$.

Before starting the proof, a remark about what the statement $\langle a \rangle = \{ e, a, a^2, \ldots, a^{n-1} \}$ means. We are essentially saying that if a has order n, then the cyclic group generated by a has n distinct elements in it and it is *precisely* the set as written.

Proof. Suppose a has infinite order. Then $a^n = e$ if and only if $n = 0$. Since $a^i = a^j$ if and only if $a^{i-j} = e$, $i - j = 0$. Suppose a has order n. It is clear that $\{ e, a, a^2, \ldots, a^{n-1} \} \subseteq \langle a \rangle$. Now let $a^k \in \langle a \rangle$. Then using the division algorithm on k and n, $a^k = a^{qn+r} = a^{qn} a^r = a^r$. Keeping in mind that $0 \leq r < n$, $a^k \in \{ e, a, a^2, \ldots, a^{n-1} \}$. Now suppose $a^i = a^j$, so $a^{i-j} = e$. Apply the division algorithm on $i - j$ to see that $e = a^{i-j} = a^{qn+r} = a^r$. Since n is the least positive integer for which $a^n = e$ and $r < n$, $r = 0$. The converse direction is trivial. □

In **??**, we used the absolute value operation to refer to both the order of an element and the order of a group. We promised that we will justify that abuse of notation here. Let us now make good on our promise. Notice that as a consequence of this theorem we have $|a| = |\langle a \rangle|$. Thus, the order of an element a is precisely the order of the cyclic (sub)group that it generates.

Another consequence of this theorem is the following corollary.

Corollary 0.9. $a^k = e$ if and only if $|a|$ divides k.

Corollary 0.10. If G is a finite group and $a, b \in G$ where $ab = ba$, then $|ab|$ divides $|a||b|$.

In general, however, there is no relationship between $|ab|$ and $|a|, |b|$. The next exercise shows this.

Exercise 0.11. Let $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ be from $\mathbb{SL}_2(\mathbb{R})$. Compute $|A|, |B|$ and $|AB|$.

Given cyclic subgroups $\langle a^i \rangle$ and $\langle a^j \rangle$, how do we determine whether they are the same? Given an element a and its order, can we determine $\left|a^k\right|$ for any k? The answers to all these questions is yes, and the following theorem illustrates this.

Theorem 0.12. Let $a \in G$ and $|a| = n$. Let $k > 0$. Let $d = \gcd(n, k)$. Then, we have

- $\langle a^k \rangle = \langle a^d \rangle$,
- $\left|a^k\right| = n/d$.

Proof. Let $k = dr$, so $a^k = a^{dr}$ which shows $\langle a^k \rangle \subseteq \langle a^d \rangle$. Now write $d = ns + kt$ (c.f. **??**), then

$$a^d = a^{ns} a^{kt} = a^{kt}.$$

So $a^d \in \langle a^k \rangle$. Let's prove the second part. Firstly, $(a^d)^{n/d} = e$ so $\left|a^d\right| \leq n/d$. If $i < n/d$, then $(a^d)^i \neq e$ so this establishes $\left|a^d\right| = n/d$. The desired conclusion follows from the first part. □

The next corollary of this theorem tells us that in a finite cyclic group, the order of an element divides the order of the group.

Corollary 0.13 (Order of an element divides order of the group)**.** If G is a finite cyclic group and $a \in G$, then $|a|$ divides $|G|$.

It thus follows that the order of a cyclic subgroup of a finite cyclic group divides the order of the group. In a later chapter, we shall soon this is true in general for any finite group.

This corollary gives us a criterion for the equivalence of cyclic subgroups.

Corollary 0.14 (Criterion for equivalence of cyclic subgroups)**.** Suppose $a \in G$ has order n. Then, $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$.

Exercise 0.15. Prove this corollary.

We now have the tools to find all the generators of a finite cyclic group.

Corollary 0.16 (Criteria for being a generator)**.** Let $G = \langle a \rangle$ be a cyclic group of order n. Let b be an element of order m. Then, b generates G if and only if $\gcd(m, n) = 1$.

Since $\mathbb{Z}_n$ is always cyclic, we can always easily determine the generators of $\mathbb{Z}_n$.

A burning question in the reader's mind is on the kind and number of subgroups a group may contain. For example, we may be wondering if every subgroup of a cyclic group is cyclic. Intuitively, this should feel true.

Theorem 0.17. Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ and $H \subseteq G$ be a subgroup. Suppose H is not the trivial subgroup, for else it is trivially cyclic. Then there is some $t > 0$ such that $a^t \in H$. We now attempt to find a generator for H. Let m be the least positive integer such that $a^m \in H$. Obviously $\langle a^m \rangle \subseteq H$. Now let $a^k \in H$. Then write $a^k = a^{qm+r}$. Since m is the least, $r = 0$. Thus $a^k \in \langle a^m \rangle$ and so $\langle a^m \rangle \supseteq H$. □

We remark that we make use of the well ordering principle here, so make sure you have spotted it!

This theorem tells us exactly what the subgroups of a cyclic group are, and how to find them. We will invoke Theorem 0.12 many times in the proof, so keep that in mind. Additionally, if d divides n, we note that $\gcd(d, n) = d$.

Theorem 0.18 (Fundamental Theorem of Cyclic Groups). Let $G = \langle a \rangle$ be a finite cyclic group of order n. Then, if d divides n, there is *exactly one* subgroup of order d. Moreover, these are the *only* subgroups of G.

Proof. Suppose d divides n. It is clear that $\langle a^{n/d} \rangle$ is a subgroup of order d. Let $H = \langle a^k \rangle$ be a subgroup of order d, we shall show $H = \langle a^{n/d} \rangle$. Since $\langle a^k \rangle = \langle a^j \rangle$ where $j = \gcd(n, k)$ and $\langle a^j \rangle$ has order $n/j = d$ it follows that $n/d = j$ so $\langle a^k \rangle = \langle a^{n/d} \rangle$. The final claim follows from Theorem 0.17 and Corollary 0.13. □

With this theorem, it is now very easy to find all the subgroups of $\mathbb{Z}_n$.
Exercise 0.19. Formulate a corollary that classifies the subgroups of $\mathbb{Z}_n$.

Since cyclic groups are so nice, they should behave nicely under homomorphisms and isomorphisms as well.
Proposition 0.20 (Properties of cyclic groups under homomorphisms)**.** *Let $\phi : G \to H$ be a group homomorphism, and G be a cyclic group. Then, the following are true.*

1. *If $G = \langle g \rangle$, then $\phi[G] = \langle \phi(g) \rangle$. In other words, ϕ takes generators to generators.*

Proof. If $\phi(x) \in \phi[G]$, then there is some integer n such that $x = g^n$. Thus, we have $\phi(x) = \phi(g^n) = \phi(g)^n$. □

Proposition 0.21 (Properties of cyclic groups under isomorphisms)**.** *Let $\phi : G \to H$ be a group isomorphism, and let G be a cyclic group. Then, the following are true.*

1. *H is cyclic.*

Proof. (1) follows from Proposition 0.20(1) □

Thus, if G is a cyclic group of order n, it is isomorphic to $\mathbb{Z}_n$.
Exercise 0.22. Show that any cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

We can thus say that there is only one cyclic group of order n up to isomorphism, which means precisely that any cyclic group of order n is isomorphic to any other cyclic group of order n. This means that any question about finite cyclic groups can be answered by studying $\mathbb{Z}_n$ instead.

0.0.1 Problems

Exercise 0.23 (Criterion for element to be identity)**.** Prove that if $a^k = e$, then k divides $|a|$.
Exercise 0.24. Show that if G has order 3, then it must be cyclic.
Exercise 0.25. Show that if $a \in G$, then $\langle a \rangle$ is a subgroup of $C(a)$.
Exercise 0.26. Let G be a group and $a \in G$. Show that $\langle a \rangle = \langle a^{-1} \rangle$.
Exercise 0.27. Let $G = \mathbb{Z}$ and let $m, n \in \mathbb{Z}$. Consider $\langle m \rangle$ and $\langle n \rangle$ as subgroups of G. Find a generator of $\langle m \rangle \cap \langle n \rangle$.
Exercise 0.28. Show that $\mathbb{Q}$ under multiplication is not cyclic.
Exercise 0.29. Let G be a cyclic group of order 15 and let $x \in G$. Suppose that *exactly two* of x^3, x^5 and x^9 are equal. Determine $|x^{13}|$.
Exercise 0.30. Prove that an infinite group has infinitely many subgroups. *Warning: Do not assume that an infinite group must have an element of infinite order.*
Exercise 0.31. Let n be an natural number. Find a group that has exactly n subgroups.
Problem 0.1. Let G be a group with more than one element, and suppose that G has no proper nontrivial subgroups. Show that G is a finite group and $|G|$ is prime.
Problem 0.2. Let G be a finite group. Prove that G is the union of proper subgroups if and only if G is not cyclic.

Given a cyclic group, a question is to determine how many generators it has. We already have Corollary 0.16, which gives us necessary and sufficient conditions for an element to be a generator. At this point, the reader should recall the definition of $U(n)$. It appears that every element of $U(n)$ is a generator of $\mathbb{Z}_n$, and these are the only generators. Is this true?
Proposition 0.32 (Number of generators)**.** *Let G be a cyclic group of order n. Then, G has exactly $|U(n)|$ generators.*

Proof. Let $g \in G$ and $m = |g|$. Notice that g generates G if and only if $\gcd(m, n) = 1$, which is true if and only if $m \in U(n)$. □

0.1 Euler totient function

We have spent a large amount of time working with $\mathbb{Z}_n$. This feels very number theoretic, and the reader may very well be wondering[1] about the connection between group theory and number theory. We shall scratch the surface of this connection by using group theory to prove some facts about a common function used in number theory, the Euler totient function.

Warning. *Do not think about skipping this section. There are important theorems in here.*

Definition 0.33 (Euler totient function)**.** We define the Euler totient function $\varphi(n)$ to be the number of natural numbers less than or equal to n that are coprime to n.

It is immediate, by definition, that $\varphi(n) = |U(n)|$.

Those who have had number theory may be familiar with the following proposition. You might also recall how much of a pain these are to prove with number theory. Are we going to subject you to the same pain as you have previously experienced? No. We are going to show how we can use group theory to deal with these facts.

Proposition 0.34. *Let φ denote the Euler totient function. Then,*

1. *If a is coprime to b, $\varphi(ab) = \varphi(a)\varphi(b)$*
2. *Let p be a prime. Then, $\varphi(p^n) = p^n - p^{n-1}$.*

Proof. (1) will follow from the more general statement that $U(ab) \cong U(a) \times U(b)$. (2) will follow from the more general statement that $U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}}$ for an odd prime, and $U(2^n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ when $p = 2$. Thus we shall prove the more general statements instead. □

A common theme in algebra is trying to break down larger structures into smaller, more understandable structures. We began with number theory, by factorizing numbers into primes and studying the primes to gain control over all numbers. In group theory, we can try to understand a group in terms of its subgroups. We shall now prove a theorem that lets us "factorize" $U(n)$.

Theorem 0.35 (Structure of $U(n)$)**.** Let a, b be coprime. Then, $U(ab) \cong U(a) \times U(b)$.

Proof. Notice that the mapping $n \mapsto (n \bmod a, n \bmod b)$ is an isomorphism from $U(ab)$ to $U(a) \times U(b)$. □

The reader should find that the choice of the isomorphism very natural. This choice is natural in part because we didn't really have any other good options to choose.

Exercise 0.36. Check that the mapping which is claimed to be isomorphisms are indeed isomorphisms.

[1] If you're not wondering about it, you might try to skip this section. Heed the warning, and do not skip it.