Cyclic groups

Examples:
• \( \mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle \) under +.
• \( \mathbb{Z}_n = \langle 1 \rangle = \langle -1 \rangle \) under + mod \( n \); in fact, there may be other generators of \( \mathbb{Z}_n \) besides \( \pm 1 \).
• \( U(n) \) is sometimes cyclic, e.g., \( n = 2, 3, 4, 6, 7, 9, \ldots \).

Theorem If \( a \in G \) has infinite order, then \( a^i = a^j \)
\( \iff i = j. \) If \( a \in G \) has finite order \( n \), then
\( \langle a \rangle = \{a, a^2, a^3, \ldots, a^n\} \) and \( a^i = a^j \iff n \) divides \( i - j \).

Proof \( a^i = a^j \iff a^{i-j} = e. \) So if \( a \) has infinite order, then, because no positive power of \( a \) equals \( e \), and further, no negative power of \( a \) can equal \( e \) (as if \( a^{-n} = e \) then multiplication by \( a^n \) implies that \( e = a^n \) which is impossible), we must have that
\( a^i = a^j \iff i = j. \)

If \( a \) has finite order \( n \), then the sequence
\( e = a^0, a, a^2, a^3, \ldots, a^{n-1} \) of powers of \( a \) forms a list of distinct group elements (else \( a^i = a^j \) with
\( 0 \leq j < i \leq n - 1 \), which implies \( a^{i-j} = e \) with
\( 0 < i - j < n \), contradicting that \( n \) is the order of \( a \).

If \( k \) is any integer, and dividing \( k \) by \( n \) yields
quotient \( q \) and remainder \( r \) (that is, \( k = qn + r \), with
\( 0 \leq r < n \)), then
\( a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r \), so
\( \langle a \rangle = \{a, a^2, a^3, \ldots, a^n\} \). Further, as above,
\( a^i = a^j \iff a^{i-j} = e. \) Dividing \( i - j \) by \( n \) to find a
quotient $q$ and remainder $r$, we have $i - j = qn + r$ with $0 \leq r < n$ and as before, $e = a^{i-j} = a^{qn+r} = a^r$ which forces $r = 0$, meaning that $n$ divides $i - j$.

Conversely, if $n$ divides $i - j$, then $r = 0$ and so $a^{i-j} = a^{qn+r} = a^r = e$. Thus $a^i = a^j$. //

**Corollary**  $|a| = |\langle a \rangle|$. //

**Corollary** If $a \in G$ has finite order $n$ and $a^k = e$ then $n$ divides $k$.

**Proof** Take $i = k$ and $j = 0$ above. //

Notice that any cyclic group $\langle a \rangle$ appears to have a structure identical to either $\mathbb{Z}$ (if $a$ has infinite order), or $\mathbb{Z}_n$ (if $a$ has finite order).

**Theorem** If $a \in G$ has finite order $n$, then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

**Proof** Put $d = \gcd(n,k)$; then there are integers $r,s$ and $t$ so that $k = dr$ and $d = ns + kt$ (see p. 5). So $a^k = (a^d)^r$, which implies that $\langle a^k \rangle \subseteq \langle a^d \rangle$, and $a^d = a^{ns+kt} = (a^n)^s (a^k)^t = e^s (a^k)^t = (a^k)^t$, which implies that $\langle a^d \rangle \subseteq \langle a^k \rangle$. So $\langle a^k \rangle = \langle a^d \rangle$. //
Next, \( n = du \) for some integer \( u \), whence \((a^d)^u = a^n = e \Rightarrow |a^d| \leq u \). But if \( i < u \), then \( di < du = n \), so \((a^d)^i \neq e \Rightarrow |a^d| \neq u \). Therefore, \(|a^d| = u \).

But \( d = \gcd(n,k) \) and \( u = n/\gcd(n,k) \), so the theorem is proved. //

**Corollary** If \( a \in G \) has finite order \( n \), then \( \langle a^i \rangle = \langle a^j \rangle \iff \gcd(n,i) = \gcd(n,j) \).

**Proof** By virtue of the theorem, \( \langle a^i \rangle = \langle a^j \rangle \iff \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle \). Certainly, \( \gcd(n,i) = \gcd(n,j) \)

\[ \Rightarrow \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle. \]

But \( \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle \Rightarrow |a^{\gcd(n,i)}| = |a^{\gcd(n,j)}| \Rightarrow n/\gcd(n,i) = n/\gcd(n,j) \) by the theorem \( \Rightarrow \gcd(n,i) = \gcd(n,j) \). //

**Corollary** Suppose \( G = \langle a \rangle \) is a cyclic group of order \( n \). Then \( G = \langle a^k \rangle \iff \gcd(n,k) = 1 \). //

**Corollary** The integer \( k \in \mathbb{Z}_n \) generates \( \mathbb{Z}_n \) if and only if \( \gcd(n,k) = 1 \). //
We can now describe the complete structure of a cyclic group.

**The Fundamental Theorem of Cyclic Groups**

Every subgroup of a cyclic group \( G = \langle a \rangle \) is cyclic. Moreover, if \( |\langle a \rangle| = n \), then the only subgroups of \( \langle a \rangle \) have order \( k \), one for each divisor \( k \) of \( n \), namely the subgroup \( \langle a^{n/k} \rangle \).

**Proof**  The case of the trivial subgroup of \( G \) is, well, trivial: it is certainly cyclic. Let \( H \) then be a nontrivial subgroup of \( G \). So \( H \) contains some nonidentity element \( a^m \) of \( G \), that is, \( m \neq 0 \). Since the inverse \( a^{-m} \) of \( a^m \) is also in \( H \), we may assume that \( m \) is positive. Indeed, for convenience we can also assume that \( m \) is the exponent of the smallest positive power of \( a \) that lies in \( H \).

If \( a^k \) is any other element of \( H \), we write \( k = qm + r \), with \( 0 \leq r < m \) (dividing \( k \) by \( m \)), so that \( r = k - qm \); then \( a^r = a^k a^{-qm} = a^k (a^m)^{-q} \in H \). But \( m \) is the exponent of the smallest positive power of \( a \) that lies in \( H \), so \( r \) must be 0. That is, \( m \) divides \( k \). This shows that \( H = \langle a^m \rangle \) and that every subgroup of \( G \) must be cyclic.

If in addition, \( G \) has order \( n \), then taking \( k = n \) in the paragraph above, we see that \( m \), the order of \( H \), must divide \( n \).
Finally, by the last theorem, if $k$ is a divisor of $n$, we know that the subgroup $H = \langle a^{n/k} \rangle$ has order

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

And conversely, if $H$ has order $k$, then from above, we know that $H = \langle a^m \rangle$ where $m$ is a divisor of $n$. Also $k = |a^m| = n/\gcd(n,m) = n/m$, so $m = n/k$ and $H = \langle a^{n/k} \rangle$.

**Corollary**  For each positive divisor $k$ of $n$, $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order $k$. Moreover, these are the only subgroups of $\mathbb{Z}_n$.

By combining the last two theorems, we can determine the count of the elements of a given order in a cyclic group.

**Theorem**  If $d$ is a divisor of $n$, then the number of elements of order $d$ in a cyclic group of order $n$ is

$$\phi(d) = \# \text{(positive integers less than } d \text{ and prime to } d)$$

(This defines the **Euler phi function**).

**Proof**  There is just one (cyclic) subgroup $\langle b \rangle$ of order $d$ in a cyclic group $\langle a \rangle$ of order $n$, so all
elements of order $d$ in $\langle a \rangle$ generate this same subgroup $\langle b \rangle$. These elements are all powers of $b$, but we also know that $\langle b^k \rangle = \langle b \rangle \iff \gcd(d,k) = 1$. So there are exactly $\phi(d)$ such generators. //

**Corollary** In any finite group, the number of elements of order $d$ is divisible by $\phi(d)$.

**Proof** If there are no elements of order $d$, then the statement is true as $\phi(d)$ divides 0. So suppose there is an element $a$ of order $d$. By the theorem, $\langle a \rangle$ has $\phi(d)$ elements of order $d$, so if all the elements of order $d$ in the full group lie in $\langle a \rangle$, the proof is complete. If not, then there is another element $b$ of order $d$ not in $\langle a \rangle$. But then $\langle b \rangle$ contains $\phi(d)$ elements of order $d$ by the same argument, and none of these can be common to both $\langle a \rangle$ and $\langle b \rangle$, for if $c$ were one such element, then we would have $\langle a \rangle = \langle c \rangle = \langle b \rangle$, forcing $b \in \langle a \rangle$, a contradiction. Continuing this way, we see that the number of elements of order $d$ is a multiple of $\phi(d)$. //

We can show the structure of the subgroups of a group is via a **subgroup lattice**, a diagram that depicts all the subgroups connected to each other with segments so that smaller subgroups appear below the subgroups that contain them.