Theorem 1. *Let g be an element of a group G and write*

$$\langle g \rangle = \left\{ g^k : k \in \mathbb{Z} \right\}.$$

Then $\langle g \rangle$ is a subgroup of G.

Proof. Since $e = g^0$, $e \in \langle g \rangle$. Suppose $a, b \in \langle g \rangle$. Then $a = g^k$, $b = g^m$ and $ab = g^k g^m = g^{k+m}$. Hence $ab \in \langle g \rangle$ (note that $k + m \in \mathbb{Z}$). Moreover, $a^{-1} = (g^k)^{-1} = g^{-k}$ and $-k \in \mathbb{Z}$, so that $a^{-1} \in \langle g \rangle$. Thus, we have checked the three conditions necessary for $\langle g \rangle$ to be a subgroup of G. □

Definition 2. If $g \in G$, then the subgroup $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ is called the **cyclic subgroup of G generated by g**, If $G = \langle g \rangle$, then we say that G is a **cyclic group** and that g is a **generator** of G.

Examples 3.

1. If G is any group then $\{e\} = \langle e \rangle$ is a cyclic subgroup of G.

2. The group $G = \{1, -1, i, -i\} \subseteq \mathbb{C}^*$ (the group operation is multiplication of complex numbers) is cyclic with generator i. In fact $\langle i \rangle = \{i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i\} = G$. Note that $-i$ is also a generator for G since $\langle -i \rangle = \{(-i)^0 = 1, (-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i\} = G$. Thus a cyclic group may have more than one generator. However, not all elements of G need be generators. For example $\langle -1 \rangle = \{1, -1\} \neq G$ so -1 is not a generator of G.

3. The group $G = U(7) =$ the group of units in $\mathbb{Z}_7$ is a cyclic group with generator 3. Indeed,
$$\langle 3 \rangle = \{1 = 3^0, 3 = 3^1, 2 = 3^2, 6 = 3^3, 4 = 3^4, 5 = 3^5\} = G.$$
Note that 5 is also a generator of G, but that $\langle 2 \rangle = \{1, 2, 4\} \neq G$ so that 2 is not a generator of G.

4. $G = \langle \pi \rangle = \{\pi^k : k \in \mathbb{Z}\}$ is a cyclic subgroup of $\mathbb{R}^*$.

5. The group $G = U(8)$ is not cyclic. Indeed, since $U(8) = \{1, 3, 5, 7\}$ and $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1, 3\}$, $\langle 5 \rangle = \{1, 5\}$, $\langle 7 \rangle = \{1, 7\}$, it follows that $U(8) \neq \langle a \rangle$ for any $a \in U(8)$.

If a group G is written additively, then the identity element is denoted 0, the inverse of $a \in G$ is denoted $-a$, and the powers of a become na in additive notation. Thus, with this notation, the cyclic subgroup of G generated by a is $\langle a \rangle = \{na : n \in \mathbb{Z}\}$, consisting of all the multiples of a. Among groups that are normally written additively, the following are two examples of cyclic groups.

6. The integers $\mathbb{Z}$ are a cyclic group. Indeed, $\mathbb{Z} = \langle 1 \rangle$ since each integer $k = k \cdot 1$ is a multiple of 1, so $k \in \langle 1 \rangle$ and $\langle 1 \rangle = \mathbb{Z}$. Also, $\mathbb{Z} = \langle -1 \rangle$ because $k = (-k) \cdot (-1)$ for each $k \in \mathbb{Z}$.

7. $\mathbb{Z}_n$ is a cyclic group under addition with generator 1.

Theorem 4. *Let g be an element of a group $\mathbf{G} = \langle G, \cdot, ^{-1}, e \rangle$. Then there are two possibilities for the cyclic subgroup $\langle g \rangle$.*

Case 1: *The cyclic subgroup* $\langle g\rangle$ *is finite. In this case, there exists a smallest positive integer* n *such that* $g^n = e$ *and we have*

(a) $g^k = e$ *if and only if* $n \mid k$.

(b) $g^k = g^m$ *if and only if* $k \equiv m \pmod{n}$.

(c) $\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ *and the elements* $e, g, g^2, \ldots, g^{n-1}$ *are distinct.*

Case 2: *The cyclic subgroup* $\langle g\rangle$ *is infinite. Then*

(d) $g^k = e$ *if and only if* $k = 0$.

(e) $g^k = g^m$ *if and only if* $k = m$.

(f) $\langle g\rangle = \{\ldots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\}$ *and all of these powers of* g *are distinct.*

Proof. **Case 1.** Since $\langle g\rangle$ is finite, the powers $g, g^2, g^3, \ldots$ are not all distinct, so let $g^k = g^m$ with $k < m$. Then $g^{m-k} = e$ where $m - k > 0$. Hence there is a positive integer l with $g^l = e$. Hence there is a smallest such positive integer. We let n be this smallest positive integer, i.e., n is the smallest positive integer such that $g^n = e$.

(a) If $n \mid k$ then $k = qn$ for some $q \in n$. Then $g^k = g^{qn} = (g^n)^q = e^q = e$. Conversely, if $g^k = e$, use the division algorithm to write $k = qn+r$ with $0 \le r < n$. Then $g^r = g^k(g^n)^{-q} = ee^{-q} = e$. Since $r < n$, this contradicts the minimality of n unless $r = 0$. Hence $r = 0$ and $k = qn$ so that $n \mid k$.

(b) $g^k = g^m$ if and only if $g^{k-m} = e$. Now apply Part (a).

(c) Clearly, $\{e, g, g^2, \ldots, g^{n-1}\} \subseteq \langle g\rangle$. To prove the other inclusion, let $a \in \langle g\rangle$. Then $a = g^k$ for some $k \in \mathbb{Z}$. As in Part (a), use the division algorithm to write $k = qn + r$, where $0 \le r \le n - 1$. Then

$$a = g^k = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r \in \{e, g, g^2, \ldots, g^{n-1}\}$$

which shows that $\langle g\rangle \subseteq \{e, g, g^2, \ldots, g^{n-1}\}$, and hence that

$$\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}.$$

Finally, suppose that $g^k = g^m$ where $0 \le k \le m \le n-1$. Then $g^{m-k} = e$ and $0 \le m-k < n$. This implies that $m - k = 0$ because n is the smallest positive power of g which equals e. Hence all of the elements $e, g, g^2, \ldots, g^{n-1}$ are distinct.

Case 2. (d) Certainly, $g^k = e$ if $k = 0$. If $g^k = e$, $k \neq 0$, then $g^{-k} = (g^k)^{-1} = e^{-1} = e$, also. Hence $g^n = e$ for some $n > 0$, which implies that $\langle g\rangle$ is finite by the proof of Part (c), contrary to our hypothesis in Case 2. Thus $g^k = e$ implies that $k = 0$.

(e) $g^k = g^m$ if and only if $g^{k-m} = e$. Now apply Part (d).

(f) $\langle g\rangle = \{g^k : k \in \mathbb{Z}\}$ by definition of $\langle g\rangle$, so all that remains is to check that these powers are distinct. But this is the content of Part (e). □

Recall that if g is an element of a group G, then the **order** of g is the smallest positive integer n such that $g^n = e$, and it is denoted $|g| = n$. If there is no such positive integer, then we say that g has **infinite order**, denoted $|g| = \infty$. By Theorem 4, the concept of order of an element g and order of the cyclic subgroup generated by g are the same.

Corollary 5. *If g is an element of a group G, then $|g| = |\langle g \rangle|$.*

Proof. This is immediate from Theorem 4, Part (c). $\square$

If G is a cyclic group of order n, then it is easy to compute the order of all elements of G. This is the content of the following result.

Theorem 6. *Let $G = \langle g \rangle$ be a cyclic group of order n, and let $0 \le k \le n-1$. If $m = \gcd(k, n)$, then $|g^k| = \dfrac{n}{m}$.*

Proof. Let $k = ms$ and $n = mt$. Then $(g^k)^{n/m} = g^{kn/m} = g^{msn/m} = (g^n)^s = e^s = e$. Hence n/m divides $|g^k|$ by Theorem 4 Part (a). Now suppose that $(g^k)^r = e$. Then $g^{kr} = e$, so by Theorem 4 Part (a), $n \mid kr$. Hence

$$\frac{n}{m} \,\Big|\, \frac{k}{m} r$$

and since n/m and k/m are relatively prime, it follows that n/m divides r. Hence n/m is the smallest power of g^k which equals e, so $|g^k| = n/m$. $\square$

Theorem 7. *Let $G = \langle g \rangle$ be a cyclic group where $|g| = n$. Then $G = \langle g^k \rangle$ if and only if $\gcd(k, n) = 1$.*

Proof. By Theorem 6, if $m = \gcd(k, n)$, then $|g^k| = n/m$. But $G = \langle g^k \rangle$ if and only if $|g^k| = |G| = n$ and this happens if and only if $m = 1$, i.e., if and only if $\gcd(k, n) = 1$. $\square$

Example 8. If $G = \langle g \rangle$ is a cyclic group of order 12, then the generators of G are the powers g^k where $\gcd(k, 12) = 1$, that is g, g^5, g^7, and g^{11}. In the particular case of the additive cyclic group $\mathbb{Z}_{12}$, the generators are the integers 1, 5, 7, 11 $\pmod{12}$.

Now we ask what the subgroups of a cyclic group look like. The question is completely answered by Theorem 10. Theorem 9 is a preliminary, but important, result (it is called Theorem 4.3 in our textbook).

Theorem 9. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose that $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ is a cyclic group and let H be a subgroup of G. If $H = \{e\}$, then H is cyclic, so we assume that $H \ne \{e\}$, and let $g^k \in H$ with $g^k \ne e$. Then, since H is a subgroup, $g^{-k} = (g^k)^{-1} \in H$. Therefore, since k or $-k$ is positive, H contains a positive power of g, not equal to e. So let m be the smallest positive integer such that $g^m \in H$. Then, certainly all powers of g^m are also in H, so we have $\langle g^m \rangle \subseteq H$. We claim that this inclusion is an equality. To see this, let g^k be any element of H (recall that all elements of G, and hence H, are powers of g since G is cyclic). By the division algorithm, we may write $k = qm + r$ where $0 \le r < m$. But $g^k = g^{qm+r} = g^{qm} g^r = (g^m)^q g^r$ so that

$$g^r = (g^m)^{-q} g^k \in H.$$

Since m is the smallest positive integer with $g^m \in H$ and $0 \le r < m$, it follows that we must have $r = 0$. Then $g^k = (g^m)^q \in \langle g^m \rangle$. Hence we have shown that $H \subseteq \langle g^m \rangle$ and hence $H = \langle g^m \rangle$. That is H is cyclic with generator g^m where m is the smallest positive integer for which $g^m \in H$. $\square$

Theorem 10 (Fundamental Theorem of Finite Cyclic Groups)**.** *Let $G = \langle g \rangle$ be a cyclic group of order n.*

1. *If H is any subgroup of G, then $H = \langle g^d \rangle$ for some $d \mid n$.*

2. *If H is any subgroup of G with $|H| = k$, then $k \mid n$.*

3. *If $k \mid n$, then $\langle g^{n/k} \rangle$ is the unique subgroup of G of order k.*

Proof.
1. By Theorem 9, H is a cyclic group and since $|G| = n < \infty$, it follows that $H = \langle g^m \rangle$ where $m > 0$. Let $d = \gcd(m, n)$. Since $d \mid n$ it is sufficient to show that $H = \langle g^d \rangle$. But $d \mid m$ also, so $m = qd$. Then $g^m = (g^d)^q$ so $g^m \in \langle g^d \rangle$. Hence $H = \langle g^m \rangle \subseteq \langle g^d \rangle$. But $d = rm + sn$, where r, $s \in \mathbb{Z}$, so

$$g^d = g^{rm+sn} = g^{rm} g^{sn} = (g^m)^r (g^n)^s = (g^m)^r (e)^s = (g^m)^r \in \langle g^m \rangle = H.$$

   This shows that $\langle g^d \rangle \subseteq H$ and hence $\langle g^d \rangle = H$.

2. By Part (a), $H = \langle g^d \rangle$ where $d \mid n$. Then $k = |H| = n/d$ so $k \mid n$.

3. Suppose that K is any subgroup of G of order k. By Part (a), let $K = \langle g^m \rangle$ where $m \mid n$. Then Theorem 6 gives $k = |K| = |g^m| = n/m$. Hence $m = n/k$, so $K = \langle g^{n/k} \rangle$. This proves (c).

□

Remark 11. Part (b) of Theorem 10 is actually true for *any* finite group G, whether or not it is cyclic. The more general result is Lagrange's Theorem (Theorem 6.5 of our textbook).

Finally, here is one more result about cyclic groups that is sometimes useful (for example, in the proof that $U(4n)$ is cyclic—see Homework 5 solutions).

Lemma 12. *A cyclic group contains at most one element of order 2.*

Put another way, an involution[1] of a cyclic group, if it exists, is unique.

Proof. Let $G = \langle a \rangle$ be a cyclic group.

If G is infinite, then there are no elements of order 2. So, assume the order of G is finite: $|G| = n < \infty$. If $n = 1$, then $G = \langle e \rangle$; if $n = 2$, then $G = \{e, a\}$ and $a^2 = e$. In both cases, there is nothing to prove.

Suppose $n > 2$, and let $x, y \in G$ be two non-identity elements of G, say, $x = a^j$ and $y = a^k$, where $1 < j, k < n$. If $x^2 = e$, then $a^{2j} = e$. Therefore n divides $2j$ (by Theorem 4 (a)). But $j < n$ implies $2j < 2n$, so the only way to have $n \mid 2j$ is $n = 2j$. If $y^2 = e$, then the same argument applied to k yields $n = 2k$. It follows that if $x^2 = e = y^2$, then $j = k$ and so $x = a^j = a^k = y$. Hence involutions of cyclic groups are unique. □

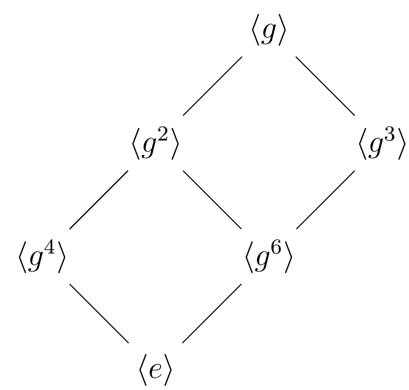
[1] Recall, an *involution* is an element of order 2.

The subgroups of a group G can be diagrammatically illustrated by listing the subgroups, and indicating inclusion relations by means of a line directed upward from H to K if H is a subgroup of K. Such a scheme is called the **Hasse diagram** of the **lattice of subgroups** of the group G.

We illustrate by determining the subgroup lattice for all the subgroups of a cyclic group $G = \langle g \rangle$ of order 12. Since the order of g is 12, Theorem 10 (c) shows that there is exactly one subgroup $\langle g^d \rangle$ for each divisor d of 12. The divisors of 12 are 1, 2, 3, 4, 6, 12. Then the unique subgroup of G of each of these orders is, respectively,

$$\{e\} = \langle g^{12} \rangle, \quad \langle g^6 \rangle, \quad \langle g^4 \rangle, \quad \langle g^3 \rangle, \quad \langle g^2 \rangle, \quad \langle g \rangle = G.$$

Note that $\langle g^m \rangle \leq \langle g^k \rangle$ if and only if $k \mid m$. Hence the lattice diagram of G is:



We can generalize this example and draw the subgroup lattice of cyclic groups of arbitrary order. Let n be the order of $G = \langle g \rangle$, and suppose the (unique) prime factorization of n is

$$n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k},$$

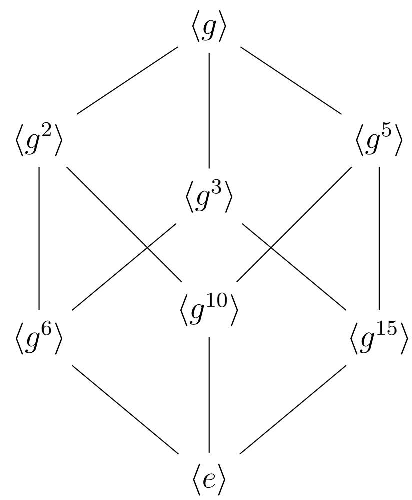
where p_i are primes and s_i are positive integers. The set of all divisors of n is then

$$\{p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} : 0 \leq t_i \leq s_i\}$$

Of course, the subgroup lattice gets complicated when the integers k and s_i are large, but for small values, the lattice is not hard to draw: For instance, if $G = \langle g \rangle$ has order $n = 30 = 2 \cdot 3 \cdot 5$, then the set of divisors is $\{2^{t_1} 3^{t_2} 5^{t_3} : 0 \leq t_i \leq 1\} = \{1, 2, 3, 5, 6, 10, 15, 30\}$, and the collection of subgroups is therefore,

$$G = \langle g \rangle, \quad \langle g^2 \rangle, \quad \langle g^3 \rangle, \quad \langle g^5 \rangle, \quad \langle g^6 \rangle, \quad \langle g^{10} \rangle, \quad \langle g^{15} \rangle, \quad \langle g^{30} \rangle = \langle e \rangle$$

Again, we have $\langle g^m \rangle \leq \langle g^k \rangle$ if and only if $k \mid m$. The lattice of subgroups of G is given by the Hasse diagram on the next page.


$\langle g \rangle$
$\langle g^2 \rangle$
$\langle g^5 \rangle$
$\langle g^3 \rangle$
$\langle g^{10} \rangle$
$\langle g^6 \rangle$
$\langle g^{15} \rangle$
$\langle e \rangle$