We have given an intuitive explanation of the subgroup of a group G generated by a subset of G. What follows is a detailed exposition of the same idea approached in another way, namely via intersections of subgroups. After we get an intuitive grasp of a concept, it is nice to try to write it up as neatly as possible. We give a set-theoretic definition and generalize a theorem that was in Exercise 61 of Section 5.

7.4 Definition Let $\{S_i \mid i \in I\}$ be a collection of sets. Here I may be any set of indices. The **intersection** $\cap_{i\in I}S_i$ **of the sets** S_i is the set of all elements that are in all the sets S_i; that is,

$$\bigcap_{i\in I} S_i = \{x \mid x \in S_i \text{ for all } i \in I\}.$$

If I is finite, $I = \{1, 2, \ldots, n\}$, we may denote $\cap_{i\in I}S_i$ by

$$S_1 \cap S_2 \cap \cdots \cap S_n.$$ ■

7.5 Theorem For any group G and any nonempty collection of subgroups $\{H_i \leq G \mid i \in I\}$, the intersection of all the subgroups H_i, $\cap_{i\in I}H_i$, is also a subgroup of G.

Proof Let us show closure. Let $a \in \cap_{i\in I}H_i$ and $b \in \cap_{i\in I}H_i$, so that $a \in H_i$ for all $i \in I$ and $b \in H_i$ for all $i \in I$. Then $ab \in H_i$ for all $i \in I$, since H_i is a group. Thus $ab \in \cap_{i\in I}H_i$.

Since H_i is a subgroup for all $i \in I$, we have $e \in H_i$ for all $i \in I$, and hence $e \in \cap_{i\in I}H_i$.

Finally, for $a \in \cap_{i\in I}H_i$, we have $a \in H_i$ for all $i \in I$, so $a^{-1} \in H_i$ for all $i \in I$, which implies that $a^{-1} \in \cap_{i\in I}H_i$. ◆

Let G be a group and let $a_i \in G$ for $i \in I$. There is at least one subgroup of G containing all the elements a_i for $i \in I$, namely G is itself. Theorem 7.5 assures us that if we take the intersection of all subgroups of G containing all a_i for $i \in I$, we will obtain a subgroup H of G. This subgroup H is the smallest subgroup of G containing all the a_i for $i \in I$.

7.6 Definition Let G be a group and let $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i \mid i \in I\}$ is the **subgroup generated by** $\{a_i \mid i \in I\}$. If this subgroup is all of G, then $\{a_i \mid i \in I\}$ **generates** G and the a_i are **generators of** G. If there is a finite set $\{a_i \mid i \in I\}$ that generates G, then G is **finitely generated.** ■

Note that this definition is consistent with our previous definition of a generator for a cyclic group. Note also that the statement *a is a generator of* G may mean either that $G = \langle a \rangle$ or that a is a member of a subset of G that generates G. The context in which the statement is made should indicate which is intended. Our next theorem gives the structural insight into the subgroup of G generated by $\{a_i \mid i \in I\}$ that we discussed for two generators before Example 7.1.

7.7 Theorem If G is a group and $a_i \in G$ for $i \in I \neq \phi$, then the subgroup H of G generated by $\{a_i \mid i \in I\}$ has as elements precisely those elements of G that are finite products of integral powers of the a_i, where powers of a fixed a_i may occur several times in the product.

Proof Let K denote the set of all finite products of integral powers of the a_i. Then $K \subseteq H$. We need only observe that K is a subgroup and then, since H is the smallest subgroup containing a_i for $i \in I$, we will be done. Observe that a product of elements in K is again in K. Since $(a_i)^0 = e$, we have $e \in K$. For every element k in K, if we form from the product giving k a new product with the order of the a_i reversed and the opposite sign on all exponents, we have k^{-1}, which is thus in K. For example,

$$\left[(a_1)^3(a_2)^2(a_1)^{-7}\right]^{-1} = (a_1)^7(a_2)^{-2}(a_1)^{-3},$$

which is again in K. ◆

7.8 Example Recall that the dihedral group D_n consists of permutations of $\mathbb{Z}_n$ that map edges to edges in the regular n-gon P_n. In disjoint cycle notation, $\rho = (0, 1, 2, 3, \ldots, n-1)$ and $\mu = (1, n-1)(2, n-2)\cdots\left(\frac{n-1}{2}, \frac{n+1}{2}\right)$ if n is odd, and $\mu = (1, n-1)(2, n-2)\cdots\left(\frac{n-2}{2}, \frac{n+2}{2}\right)$ if n is even. Since $\mu^2 = \iota$ and $\rho^n = \iota$ any product of integer powers of μ and ρ can be rewritten to only have powers of 0 or 1 for μ and powers of $0, 1, 2, 3, \ldots n-1$ for ρ. Furthermore, the relation $\rho\mu = \mu\rho^{n-1}$ allows us to move all the powers of μ to the left and all the powers of ρ to the right, being careful to replace ρ with ρ^{n-1} each time we move a μ past a ρ. So in the case of $n = 6$,

$$\rho^8\mu^9 = \rho^2\mu = \rho\mu\rho^5 = \mu\rho^5\rho^5 = \mu\rho^4.$$

Thus the subgroup of $S_{\mathbb{Z}_n}$ generated by μ and ρ is the set

$$\{\iota, \rho, \rho^2, \ldots, \rho^{n-1}, \mu, \mu\rho, \mu\rho^2, \ldots, \mu\rho^{n-1}\}$$

which is the dihedral group. ▲

Cayley Digraphs

For each generating set S of a finite group G, there is a directed graph representing the group in terms of the generators in S. The term *directed graph* is usually abbreviated as *digraph*. These visual representations of groups were devised by Cayley, and are also referred to as *Cayley diagrams* in the literature.

Intuitively, a **digraph** consists of a finite number of points, called **vertices** of the digraph, and some **arcs** (each with a direction denoted by an arrowhead) joining vertices. In a digraph for a group G using a generating set S we have one vertex, represented by a dot, for each element of G. Each generator in S is denoted by one type of arc. We could use different colors for different arc types in pencil and paperwork. Since different colors are not available in our text, we use different style arcs, like solid, dashed, and dotted, to denote different generators. Thus if $S = \{a, b, c\}$ we might denote

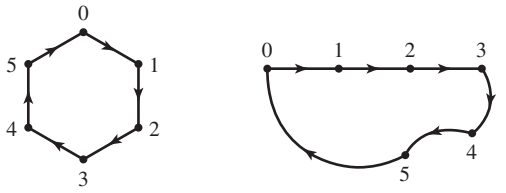
a by ——➤——, b by - - -➤- - -, and c by ·····➤·····.

With this notation, an occurrence of x •——➤—— y in a Cayley digraph means that $xa = y$. That is, traveling an arc in the direction of the arrow indicates that multiplication of the group element at the start of the arc *on the right* by the generator corresponding to that type of arc yields the group element at the end of the arc. Of course, since we are in a group, we know immediately that $ya^{-1} = x$. Thus traveling an arc in the direction opposite to the arrow corresponds to multiplication on the right by the inverse of the corresponding generator. If a generator in S is its own inverse, it is customary to denote this by omitting the arrowhead from the arc, rather than using a double arrow. For example, if $b^2 = e$, we might denote b by ————.

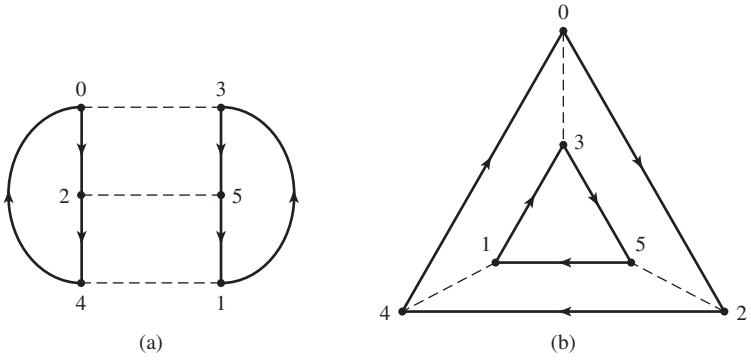
7.9 Example Both of the digraphs shown in Fig. 7.10 represent the group $\mathbb{Z}_6$ with generating set $S = \{1\}$. Neither the length and shape of an arc nor the angle between arcs has any significance. ▲

7.12 Example Both of the digraphs shown in Fig. 7.11 represent the group $\mathbb{Z}_6$ with generating set $S = \{2, 3\}$. Since 3 is its own inverse, there is no arrowhead on the dashed arcs representing 3. Notice how different these Cayley diagrams look from those in Fig. 7.10 for the same group. The difference is due to the different choice for the set of generators. ▲

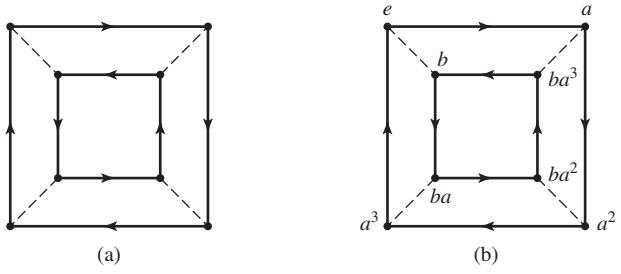
Every digraph for a group must satisfy these four properties for the reasons indicated.



7.10 Figure Two digraphs for $\mathbb{Z}_6$ with $S = \{1\}$ using $\xrightarrow[1]{}$.



7.11 Figure Two digraphs for $\mathbb{Z}_6$ with $S = \{2, 3\}$ using $\xrightarrow[2]{}$ and $\underset{3}{\_\_\_\_\_}$.



7.13 Figure

Property	***Reason***
1. The digraph is connected, that is, we can get from any vertex g to any vertex h by traveling along consecutive arcs, starting at g and ending at h.	Every equation $gx = h$ has a solution in a group.
2. At most one arc goes from a vertex g to a vertex h.	The solution of $gx = h$ is unique.
3. Each vertex g has exactly one arc of each type starting at g, and one of each type ending at g.	For $g \in G$ and each generator b we can compute gb, and $(gb^{-1})b = g$.
4. If two different sequences of arc types starting from vertex g lead to the same vertex h, then those same sequences of arc types starting from any vertex u will lead to the same vertex v.	If $gq = h$ and $gr = h$, then $uq = ug^{-1}h = ur$.