Section I.7. Generating Sets and Cayley Digraphs

Note. In this section, we generalize the idea of a *single* generator of a group to a whole *set* of generators of a group. Remember, a cyclic group has a single generator and is isomorphic to either $\mathbb{Z}$ (if it is of infinite order) or $\mathbb{Z}_n$ (if it is of finite order), by Theorem 6.10. However, there are more groups than just the ones which are cyclic.

Example 7.1. Recall the Klein 4-group, V:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Then the set $\{a, b\}$ is said to generate V since every element of V can be written in terms of a and b: $e = a^2$, $a = a^1$, $b = b^1$, and $c = ab$. We can also show that V is generated by $\{a, c\}$ and $\{b, c\}$. In addition, $\{a, b, c\}$ is a generating set (though we could view one of the elements in this generating set as unnecessary).

Exercise 7.2. Find the subgroup of $\mathbb{Z}_{12}$ generated by $\{4, 6\}$.

Solution. We get all multiples of 4 and 6, so the subgroup contains 0, 4, 8, and 6. We get sums of 4 and 6: $4 + 6 = 10$. Also, $2 \equiv 10 + 4 \pmod{12} = 4 + 4 + 6$. So the subgroup is $\{0, 2, 4, 6, 8, 10\}$. Of course, we cannot generate any odd elements of $\mathbb{Z}_{12}$.

Note. The following result goes in a little bit of a different direction in terms of subgroups.

Theorem 7.4. The intersection of some subgroups H_i of a group G for $i \in I$ is again a subgroup of G.
(**Note.** Set I is called an *index set* for the intersection. In general, the index set may not be finite—it may not even be countable. Now for the proof.)

Note. For any set $\{a_i \mid i \in I\}$ with $a_i \in G$, there is at least one subgroup of G containing all a_i (namely, the improper subgroup G). So if the intersection of all subgroups of G containing $\{a_i \mid i \in I\}$ is taken, a subgroup of G containing $\{a_i \mid i \in I\}$ results (called the "smallest subgroup of G containing $\{a_i \mid i \in I\}$"). This justifies the following definition.

Definition 7.5. 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 the set* $\{a_i \mid i \in I\}$. This subgroup is defined as the intersection of all subgroups of G containing $\{a_i \mid i \in I\}$: $H = \cap_{i \in J} H_j$ where the set of all subgroups of G containing $\{a_i \mid i \in I\}$ is $\{H_j \mid j \in J\}$. If this subgroup is all of G, then the *set* $\{a_i \in i \in I\}$ *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. The following result shows how the elements of a group are related to the generating set.

Theorem 7.6. If G is a group and $a_i \in G$ for $i \in I$, 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 the powers of a fixed a_i may occur several times in the product.

Note. We now associate directed graphs ("digraphs") with groups based on a generating set. Such digraphs are called *Cayley digraphs* or *Cayley diagrams*.

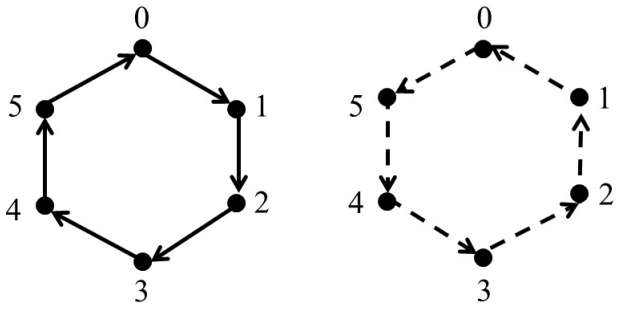
Definition (not explicit in the text). For a group G with generating set $\{a_1, a_2, \ldots, a_n\}$, define a *digraph* with *vertex set* V with the same elements as the elements of G. For each pair of vertices v_1 and v_2 define an *arc* (v_1, v_2) *of color* a_i if $v_1 a_i = v_2$. The totality of all arcs form the *arc set* A of the digraph. The vertex set V and arc set A together form a *Cayley digraph* for group G with respect to generating set $\{a_1, a_2, \ldots, a_n\}$.

Note. We will only deal with small generating sets and instead of colors, we'll code the arcs with different types of arcs: $\longrightarrow$ or $\dashrightarrow$.

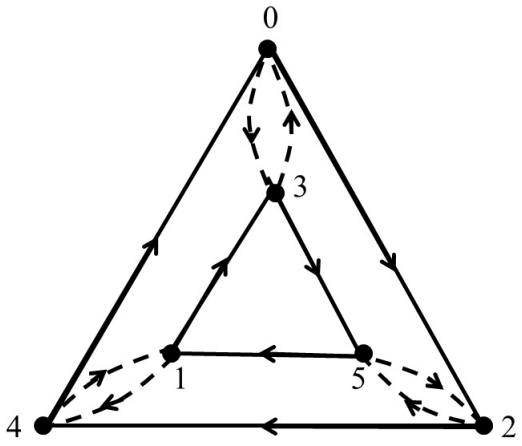
Note. The text uses the convention that if a generator g is its own inverse (i.e., $g^2 = e$) then for any arc (v_1, v_2) (for which we have $v_1 g = v_2$) we also have arc (v_2, v_1) (since $(v_1 g)g = v_2 g$ or $v_1 e = v_2 g$ or $v_1 = v_2 g$), and these two arcs are replaced with a single undirected *edge*. Strictly speaking, this does not yield a digraph, but a *mixed graph* (which has both edges and arcs).

Note. Our text doesn't really use Cayley digraphs except in this section. Additional details on Cayley digraphs can be found in *Groups and Their Graphs* by Israel Grossman and Wilhelm Magnus, New York: Yale University Press, 1964.

Example 7.7. Consider $\mathbb{Z}_6$ with generating set $\{1\}$ where right addition by 1 is represented by an arc of the form $\longrightarrow$. If the generating set of $\mathbb{Z}_6$ is $\{5\}$ and right addition by 5 is represented by an arc of the form $\dashrightarrow$, then we get the following:



Example 7.10. With group $\mathbb{Z}_6$ and generating set $\{2, 3\}$, with right addition by 2 represented by $\longrightarrow$ and right addition by 3 represented by $\dashrightarrow$ then we get:



Note. The Cayley digraph for a graph must satisfy:

1. The digraph is connected. That is, we can get from any vertex g to any vertex h by traveling along arcs, starting at g and ending at h. The reason this is true is that the Cayley digraph is based on a generating set and that every equation $gx = h$ has a solution x (and x can be expressed in terms of the generating set).

2. At most one arc goes from a vertex g to a vertex h. This is because $gx = h$ has a unique solution. If x is in the generating set, then the arc from g to h is present. If x is not in the generating set, then the arc from g to h is not present.

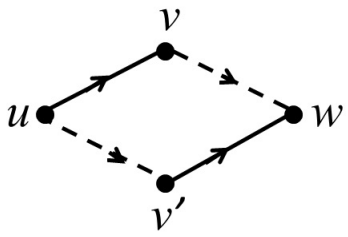
3. Each vertex g has exactly one arc of each color starting at g, and one arc of each color ending at g. This is because the arc of color a_i going out of g goes to vertex ga_i. The arc of color a_i coming into g is the arc coming from (ga_i^{-1}).

4. If two different sequences of arcs start at g and end at h, then if we follow these same two sequences by starting at any vertex u, both will end at the same vertex. This is because the two sequences represent some product of group generators. The two sequences produce the same element of the group because the equation $gx = h$ has a unique solution.

Note. The text states that any digraph which satisfies these 4 properties is a Cayley digraph for some group (though no proof or reference is given). The text also claims that some finite groups were first discovered by finding the corresponding Cayley digraphs (again, without a reference—see page 71).

Exercise 7.11. How can we tell from a Cayley digraph whether or not the corresponding group is commutative?

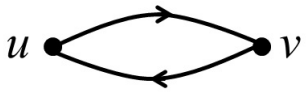
Solution. A group is commutative if and only if its generators commute (since each element is a product of the generators). The generators commute if and only if for each vertex u of the Cayley digraph, we follow an arc of color a_i to a new vertex v and then follow an arc of color a_j to vertex w, AND ALSO we can take the arc of color a_j from vertex u to some vertex v' and then take the arc of color a_i from v' and end at vertex w again:



where a_i is represented by $\longrightarrow$ and a_j is represented by $\dashrightarrow$.

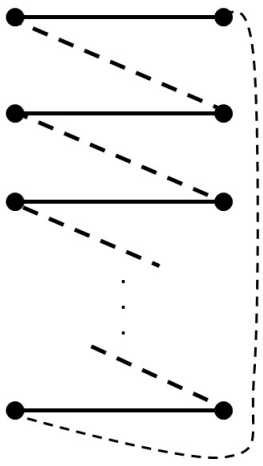
Exercise 7.19. For $n \geq 3$, there exists a nonabelian group with $2n$ elements that is generated by two elements of order 2.

Proof. We have a generator g of order 2 if $g^2 = e$ and so if g is represented as $\longrightarrow$ then between any two vertices u and v we have the Cayley digraph of the form



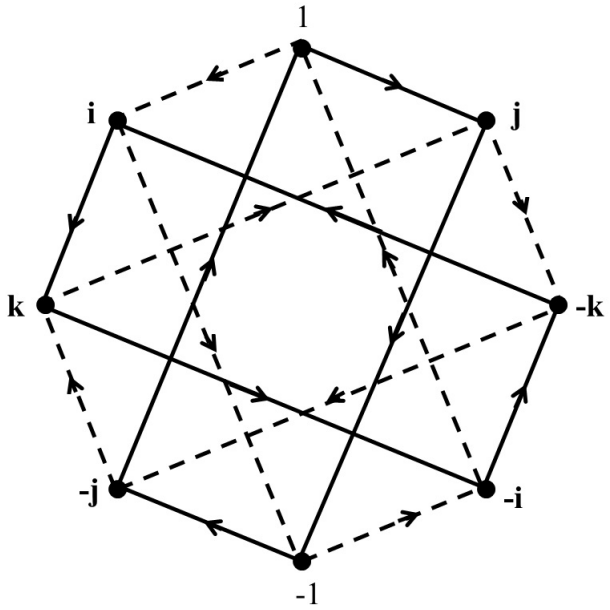
which the text (and also the *Groups and Their Graphs* book) represents as

So we can show the existence of such a group by giving the Cayley digraph and violating the property of a Cayley digraph for an abelian group as given in Exercise 7.11. This is accomplished as follows:



(Notice this does not work for $n = 2$ since it yields an abelian group in that case—in fact, it gives the Cayley digraph of the Klein 4-group V.)

Example. Consider the Cayley digraph given below. This is the Cayley digraph for the *quaternions*, denoted Q_8, which will be encountered again in Section IV.24. The dotted arrow represents multiplication on the right by $\mathbf{i}$ and the solid arrow represents multiplication on the right by $\mathbf{j}$. Create a multiplication table for the quaternions.



Solution. For multiplication on the right by $\mathbf{i}$ we have: $1 \cdot \mathbf{i} = \mathbf{i}$, $\mathbf{i} \cdot \mathbf{i} = -1$, $-1 \cdot \mathbf{i} = -\mathbf{i}$, $-\mathbf{i} \cdot \mathbf{i} = 1$, $\mathbf{j} \cdot \mathbf{i} = -\mathbf{k}$, $-\mathbf{k} \cdot \mathbf{i} = -\mathbf{j}$, $-\mathbf{j} \cdot \mathbf{i} = \mathbf{k}$, and $\mathbf{k} \cdot \mathbf{i} = \mathbf{j}$. For multiplication on the right by $\mathbf{j}$ we have: $1 \cdot \mathbf{j} = \mathbf{j}$, $\mathbf{j} \cdot \mathbf{j} = -1$, $-1 \cdot \mathbf{j} = -\mathbf{j}$, $-\mathbf{j} \cdot \mathbf{j} = 1$, $\mathbf{i} \cdot \mathbf{j} = \mathbf{k}$, $\mathbf{k} \cdot \mathbf{j} = -\mathbf{i}$, $-\mathbf{i} \cdot \mathbf{j} = -\mathbf{k}$, and $-\mathbf{k} \cdot \mathbf{j} = \mathbf{i}$. This gives us 16 of the entries in the multiplication table for Q_8. Since 1 is the identity, we get another 15 entries. All entries can be found from this information. For example, $\mathbf{k} \cdot \mathbf{k} = \mathbf{k} \cdot (\mathbf{i} \cdot \mathbf{j}) = (\mathbf{k} \cdot \mathbf{i}) \cdot \mathbf{j} = (\mathbf{j}) \cdot \mathbf{j} = -1$. The multiplication table is:

$\cdot$	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	-1	$-\mathbf{i}$	$-\mathbf{j}$	$-\mathbf{k}$
1	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	-1	$-\mathbf{i}$	$-\mathbf{j}$	$-\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	-1	$\mathbf{k}$	$-\mathbf{j}$	$-\mathbf{i}$	1	$-\mathbf{k}$	$\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	-1	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{k}$	1	$-\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	-1	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{i}$	1
-1	-1	$-\mathbf{i}$	$-\mathbf{j}$	$-\mathbf{k}$	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$-\mathbf{i}$	$-\mathbf{i}$	1	$-\mathbf{k}$	$\mathbf{j}$	$\mathbf{i}$	-1	$\mathbf{k}$	$-\mathbf{j}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	1	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{k}$	-1	$\mathbf{i}$
$-\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{i}$	1	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	-1

Notice that each of $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ are square roots of -1. So the quaternions are, in a sense, a generalization of the complex numbers $\mathbb{C}$.

Revised: 7/6/2023