7 Generating Sets and Cayley Digraphs

7.1 Generating Sets

Recall that the smallest subgroup of G that contains $a \in G$ is $\langle a \rangle$. What would be the smallest subgroup of G that contains $a, b \in G$?

By a theorem, every subgroup $H \leq G$ such that $a, b \in H$, must also have $a^m, b^n \in H$ for all $m, n \in \mathbb{Z}$. Therefore, H must also contain all products of such powers of a and b. For example, $a^2b^4a^{-3}b^2a^5 \in H$. Note that G may not be abelian, so we may not simplify this expression as a power of a multiplied by a power of b. However, products of such expressions are again expressions of the same type. Furthermore, $e = a^0$ and the inverse of such an expression is again of the same type. For example, the inverse of $a^2b^4a^{-3}b^2a^5$ is $a^{-5}b^{-2}a^3b^{-4}a^{-2}$.

Since H is closed under the binary operation, $e \in H$, and $\forall a \in H, a^{-1} \in H$, by a theorem, $H \leq G$. Such a subgroup is the smallest subgroup of G that contains both a and b. We say a, b are **generators** of this subgroup. If $H = G$, we say that $\{a, b\}$ **generates** G. Similar argument applies to three, four, and other number of elements of G, as long as we take finite products of their integral powers.

Remark. *If a subset $S \subseteq G$ generates a group G, then every subset of G that contains S also generates G.*

Definition. *Let $\{S_i \mid i \in I\}$ be a collection of sets where I is a set of indices. The* ***intersection*** *of the sets S_i, denoted by $\bigcap_{i \in I} S_i$, is the set of all elements that are in all the sets S_i. That is,*

$$\bigcap_{i \in I} S_i = \{x \mid x \in S_i, \forall i \in I\}$$

If $I = \{1, 2, \ldots, n\}$, then

$$\bigcap_{i \in I} S_i = S_1 \cap S_2 \cap \cdots \cap S_n.$$

Theorem. *If $H_i \leq G$ for a group G and $i \in I$, then $\left(\bigcap_{i \in I} H_i\right) \leq G$.*

Proof. For the proof, we show that

- $\forall a, b \in \bigcap_{i \in I} H_i \implies ab \in \bigcap_{i \in I} H_i$ (That is, $\bigcap_{i \in I} H_i$ is closed under the binary operation of G)
- $e \in \bigcap_{i \in I} H_i$ (That is, $\bigcap_{i \in I} H_i$ has the identity element of G)
- $\forall a \in \bigcap_{i \in I} H_i \implies a^{-1} \in \bigcap_{i \in I} H_i$ (That is, $\bigcap_{i \in I} H_i$ contains the inverse of each of its elements)

□

Consider $\{a_1, a_2, \ldots, a_n\} \subseteq G$, where G is a group. The previous theorem guarantees that the intersection of all subgroups of G that contains all a_i is the smallest subgroup of G that contains all $a_i, i = 1, \ldots, n$.

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****.*

Remark. *If we say an element b generates G, either $G = \langle b \rangle$ or b is a member of a subset of G that generates G. The context should make it clear which meaning is intended.*

Theorem. *If G is a group and $a_i \in G$ for $i \in I$, then the subgroup $H \leq G$ 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.*

Example 1. *List the elements of the subgroup generated by the subset $\{12, 30\}$ of $\mathbb{Z}_{36}$.*

7.2 Cayley Digraphs

A Cayley digraph represents a group G with a generating set S. The word *digraph* means "directed graph." A **digraph** has a finite number of points called vertices and directed arcs that join vertices. We use a different arc for each generator a_i. For example, $x \to y$ may mean $xa_3 = y$, which is equivalent to $x = ya_3^{-1}$. By convention, if a generator is its own inverse, we omit the arrow. For example, if $b^2 = e$, then we may draw $x - - - y$ to indicate $xb = y$ or $x = yb$.

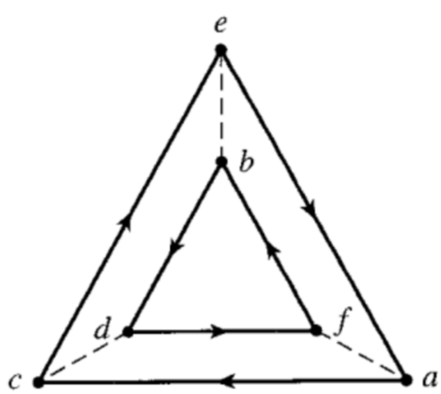
Each Cayley digraph has the following properties.

Property	Reason
digraph is connected	$ax = b$ has a solution
at most one arc goes from a vertex to another	the solution to $ax = b$ is unique
each vertex x has exactly one arc of each type starting, and one arc of each type ending, at that vertex	for each generator b, we can compute xb and $(xb^{-1})b = x \in G$
if two different sequences of arc types starting from vertex x lead to the same vertex c, then those same sequences of arc types starting from every vertex w will lead to the same vertex d	If $xa = c = xb$, then $d = wa = w(x^{-1}c) = wb$

and every digraph with the above properties is a Cayley digraph for some group.

Because of symmetry of Cayley digraphs, we may name any vertex the identity element e and obtain the other vertices by product of arc labels and their inverses as we travel from our vertex e to reach the other vertex.

Example 2. *Give the table for the group having the digraph below. Take e as identity element. List the identity e first in your table, and list the remaining elements alphabetically.*



Example 3. *Draw digraphs of the two possible structurally different groups of order 4, taking as small a generating set as possible in each case. You need not label vertices.*