Subgroups Generated by Subsets

A cyclic subgroup of a group $G$ is a subgroup of the form $H = \langle g \rangle = \{g^k | g \in \mathbb{Z} \}$, where $g$ is an element of $G$. Recall that such a group can be described as the smallest subgroup of $G$ containing $g$. That is,

$$\langle g \rangle = \bigcap_{g \in K} K_{K \subseteq G}$$

In today’s lab we wish to generalize these ideas. In particular, we will be interested in answering the following questions:

**What is the smallest subgroup of a group $G$ containing elements $g_1, g_2, \ldots, g_n \in G$? How can you describe an arbitrary element in this subgroup?**

Or, more generally, **What is the smallest subgroup of a group $G$ containing a subset $S \subseteq G$ and how can you describe an arbitrary element in this subgroup?**

**Definition.** Let $S$ be a subset of a group $G$. Then the **subgroup of $G$ generated by $S$**, denoted by $\langle S \rangle$, is defined to be the intersection

$$\langle S \rangle = \bigcap_{S \subseteq K} K_{K \subseteq G}$$

Note: If the set $S$ in the definition above happens to be a finite set, say $S = \{g_1, g_2, \ldots, g_n\}$, then we normally write $\langle g_1, g_2, \ldots, g_n \rangle$ instead of $\langle \{g_1, g_2, \ldots, g_n\} \rangle$ when speaking about this subgroup.

**Question 1.** Explain why the definition above ensures that $\langle S \rangle$ is the smallest subgroup of $G$ containing $S$.

**Question 2.** The subgroup generated by $S$ could have been defined a second way, as the set of all possible products of elements in $S$. Indeed, if $g_1$ and $g_2$ are two elements in a subgroup of $G$ then closure implies that the products $(g_1)^2, (g_2)^2, (g_1g_2)^2, (g_1g_2)^2(g_1)^3(g_1g_2)^2(g_2)^{12}, \ldots$ must also be in the subgroup. Define the **closure of $S$** to be the set:

$$\bar{S} = \{s_1^{\alpha_1}s_2^{\alpha_2}\cdots s_n^{\alpha_n} | n \in \mathbb{Z}, n \geq 0 \text{ and } s_i \in S, \alpha_i = \pm 1 \text{ for each } 1 \leq i \leq n \}$$

and prove that $\langle S \rangle = \bar{S}$.
Describing $\langle S \rangle$ as the closure of $S$ is particularly helpful when you want to be able to describe an arbitrary element in $\langle S \rangle$. The second definition is also more easily incorporated into computer programs such as gap.

**Question 2.** Let’s look at some examples in gap. Type in the commands below to define the subgroup $S_5$ generated by the two cycle $(1, 2)$ and the three cycle $(1, 2, 3)$.

```gap
gap> G:=SymmetricGroup(5);
gap> a:=(1, 2); b:=(1, 2, 3);
gap> H1:=Subgroup(G, [a, b]);
gap> Elements(H1);
gap> Size(H1);
```

Using gap’s output, classify the group $\langle (1,2), (1,2,3) \rangle$.

**Question 3.** Use gap to classify each of the subgroups of $S_5$ listed below.

a.) $H_2 = \langle (1,2), (2,3,4) \rangle$

b.) $H_3 = \langle (1,2), (3,4,5) \rangle$

c.) $H_4 = \langle (1,2), (1,2,3,4) \rangle$

d.) $H_5 = \langle (1,2), (2,3,4,5) \rangle$

Experiment with other pairs of cycles until you are able to answer the questions that follow.

e.) Given a 2-cycle $(a, b)$ and a 3-cycle $(c, d, e)$ in $S_5$, when is $S_5 = \langle (a, b), (c, d, e) \rangle$?

f.) For which cycles, $(a, b)$ and $(c, d, e, f)$ in $S_5$, is $S_5 = \langle (a, b), (c, d, e, f) \rangle$?

g.) For which cycles, $(a, b)$ and $(c, d, e, f, g)$ in $S_5$, is $S_5 = \langle (a, b), (c, d, e, f, g) \rangle$?

**Question 4.** Classify the subgroups of $S_5$ listed below.
a.) $H_6 = \langle (1, 2, 3), (2, 3, 4) \rangle$

b.) $H_7 = \langle (1, 2, 3), (3, 4, 5) \rangle$

c.) $H_8 = \langle (1, 2, 3), (2, 3, 4), (3, 4, 5) \rangle$

e.) Can $S_5$ be generated by 3-cycles? Why or why not?

**Question 5.** Note that for any group $G$, we can certainly say that $G$ is generated by all elements in $G$. That is, $\langle G \rangle = G$. However, in practice we are interested in finding a small set of generators for a group. If $G$ is cyclic, for example, then the smallest set will contain just one element – the generator. In general, it is difficult to find a smallest set of generators for a group.

Show that the symmetric group, $S_n$, can be generated by just two generators. Then explain why any generating set of $S_n$ must contain at least two elements. (Hence a minimal generating set of $S_n$ has order 2.)