Math 31: S_3 Worksheet

Wednesday, September 26

Given any set X, recall that

$$A(X) = \{f : X \to X \mid f \text{ is a bijection}\}.$$

You know $A(X)$ is more than just a set of functions, $A(X)$ is also equipped with a binary operation $\circ$. Given two bijections $f, g \in A(X)$, we obtain a third, $g \circ f$, by $(g \circ f)(x) = g(f(x))$. With respect to this binary operation, you know $A(X)$ forms a group. The group identity is the *identity function* id on X, defined by

$$\mathrm{id} : X \to X, \qquad \text{where } \mathrm{id}(x) = x \text{ for every } x \in X.$$

Given a bijection f, we obtain its inverse f^{-1} by "undoing" f.

So far, this is all very abstract. In fact, by Cayley's theorem, every group can be viewed as a subgroup of $A(X)$ for some set X. In this sense, the study of $A(X)$ subsumes all of group theory.

Let's consider the case when X is a finite set. For example, suppose S has three elements. Does it matter what we call the elements of X? Well not really. For example, suppose

$$X = \{1, 2, 3\} \qquad \text{and} \qquad Y = \{\triangle, \square, \star\}.$$

The groups $A(X)$ and $A(Y)$ are *secretly the same*: after relabelling X and Y, any bijection on X gives rise to a bijection on Y, and vice versa. Though $A(X)$ and $A(Y)$ are superficially different, the algebraic content of these two groups is the same. This is a common theme in algebra: We really care about the underlying structure of a group, not the superficial labels we use to name things.

Given a positive integer n, let $X_n = \{1, 2, 3, \ldots, n\}$. We define the *symmetric group on n letters* to be the group

$$S_n = A(X_n).$$

The elements of S_n are called *permutations on* $\{1, 2, 3, \ldots, n\}$. What is the order of S_n? To specify a permutation f, we need to determine where f sends $1, 2, 3, \ldots, n$. There are n choices for $f(1)$, $n-1$ choices of $f(2)$, $n-2$ choices for $f(3)$, and so on. When we get to $f(n)$, there is only 1 choice. This shows that there are $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$ permutations, and so S_n has order $n!$.

We need a convenient notation for writing a permutation in S_n. One way is to use *two-line notation*:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ f(1) & f(2) & f(3) & f(4) & f(5) \end{pmatrix}$$

denotes a permutation $f \in S_5$. For example,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$

denotes the permutation $f \in S_5$ with $f(1) = 4$, $f(2) = 1$, $f(3) = 3$, $f(4) = 5$, and $f(5) = 2$.

Investigate the group S_3 (with your neighbors) by answering the following questions.

1.) If $f, g \in S_3$ are given by

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \text{and} \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

compute $f \circ g$ and $g \circ f$. Is S_3 abelian?

2.) Find the cyclic subgroups of S_3. Is S_3 itself cyclic?

3.) Is S_3 similar to another group you've studied? Perhaps recently? Maybe on your problem set? Last night?? Why might S_3 and D_3 be *secretly the same*? Think about a natural way to relabel the triangle symmetries in D_3 so to obtain permutations in S_3.

4.) Is it possible to apply your thoughts from the previous question to the groups D_4 and S_4? Try to relabel symmetries of the square to obtain permutations of $\{1, 2, 3, 4\}$. Is D_4 *secretly the same* as S_4? Explain.