A *cycle* in S_n is a permutation that can be described as $i_i \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$ (and all other elements of $\{1, \ldots, n\}$ stay where they are). We write this cycle as $(i_1\ i_2\ \cdots\ i_{k-1}\ i_k)$. For instance, the cycle $(1\ 2\ 4)$ in S_6 sends 1 to 2, 2 to 4, and 4 to 1, while sending 3, 5, and 6 to themselves.

Every element of S_n is a product of disjoint cycles (disjoint means that each element of $\{1, \ldots, n\}$ appears in at most one cycle). For instance, in S_6 the element

$$(1\ 2\ 4)(3\ 5)$$

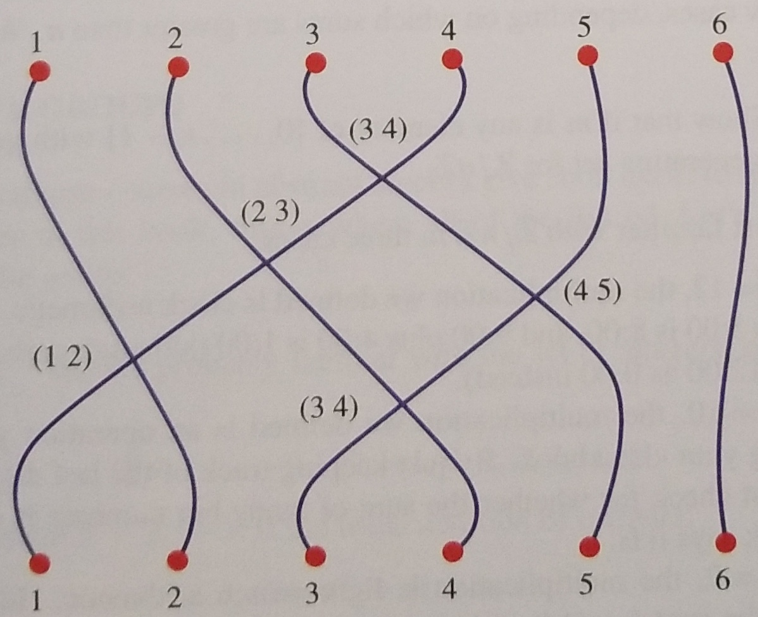
is the product of the disjoint cycles $(1\ 2\ 4)$ and $(3\ 5)$. This is the permutation that sends 1 to 2, 2 to 4, and 4 to 1, and also 3 to 5 and 5 to 3, and finally 6 to itself.

As we said, the multiplication is function composition. Say, for example, we want to multiply $(1\ 2\ 4)(3\ 5)$ by $(2\ 6)$:

$$(2\ 6) \cdot (1\ 2\ 4)(3\ 5).$$

Where does this product send 1? Well, the first permutation (on the right) sends 1 to 2, and the second permutation sends 2 to 6, so the product (= composition) sends 1 to 6. You can use the same procedure to determine where this product sends 2, 3, 4, 5, and 6. You will find that $(2\ 6) \cdot (1\ 2\ 4)(3\ 5) = (1\ 6\ 2\ 4)(3\ 5)$.

A *transposition* is a cycle of length 2, for instance, $(3\ 5)$. It is an important fact that S_n is generated by transpositions of the form $(i\ \ i+1)$, where $1 \leq i \leq n-1$ (we actually used this fact implicitly in our discussion of the cube at the beginning). Let us check that we can write $(1\ 2\ 4)(3\ 5)$ as a product of such elements in S_6. We can draw a diagram of this permutation as follows:



Each crossing in the diagram corresponds to an element of S_6 of the form $(i \;\; i+1)$. Reading top to bottom (and writing right to left), we find:

$$(1\,2\,4)(3\,5) = (3\,4)(1\,2)(4\,5)(2\,3)(3\,4).$$

The point is that multiplication in S_n can be realized by stacking diagrams. And the diagram for $(1\,2\,4)(3\,5)$ can be obtained by stacking the diagrams for the five permutations on the right-hand side of the equation. Since we can always make a diagram where the crossings occur at different heights, this argument can be used to show that every element of S_n is equal to a product of transpositions $(i \;\; i+1)$.

Exercise 1. Use the idea of stacking diagrams to prove that S_n is generated by $\{(i \;\; i+1) \mid 1 \le i \le n-1\}$.

The picture we drew of the permutation $(1\,2\,4)(3\,5)$ can be called a braid diagram. See Aaron Abrams' Office Hour 18 on braid groups for more on this idea.

Exercise 2. We showed that S_4 is the collection of symmetries of a three-dimensional cube. Can any of the other symmetric groups be thought of as the symmetries of higher-dimensional cubes? Or other shapes?

The integers modulo n. Let n be an integer greater than 1. The *integers modulo n* is the set

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

with the multiplication

$$(a, b) \mapsto \begin{cases} a+b & a+b \le n-1 \\ a+b-n & a+b \ge n. \end{cases}$$

The identity for $\mathbb{Z}/n\mathbb{Z}$ is 0. The inverse of 0 is 0, and the inverse of any other m is $n-m$. Associativity is a little trickier: to check that $(a+b)+c = a+(b+c)$, there are a few cases, depending on which sums are greater than n. We'll leave this as an exercise.

Exercise 3. Show that if m is any element of $\{0, \ldots, n-1\}$ with $\gcd(m, n) = 1$, then $\{m\}$ is a generating set for $\mathbb{Z}/n\mathbb{Z}$.

You are most familiar with $\mathbb{Z}/n\mathbb{Z}$ in three cases:

- When $n = 12$, the multiplication we defined is clock arithmetic. For example, 3:00 plus 5:00 is 8:00, and 9:00 plus 4:00 is 1:00 (although perhaps we should think of 12:00 as 0:00 instead).
- When $n = 10$, the multiplication we defined is an operation you use when balancing your checkbook. By just keeping track of the last digit, you have a quick first check for whether the sum of many big numbers is equal to what your bank says it is.
- When $n = 2$, the multiplication is light switch arithmetic. Identify 1 with flipping the switch and 0 with do nothing. Then flip plus flip is the same as doing nothing, flip plus do nothing is the same as flip, etc.