Permutations and Cayley's Theorem

Definition. A **permutation** of a nonempty set X is a bijection $\sigma : X \xrightarrow{\cong} X$.

The **permutation group** on X is $S_X = \left\{\sigma : X \xrightarrow{\cong} X\right\}$ using composition as the group operation.

The letter "S" is for "**S**ymmetries of the set X". It is easy to show that

Proposition. *Permutations form a group.*

We previously defined the symmetric groups.

Definition. The n^{th} symmetric group is $S_n = S_{\{1,2,\ldots n\}}$.

Other names for this are "the symmetric group on n elements" or else "the symmetric group on n letters". Since the group operation is given by function composition, symmetric group elements combine right-to-left.

Example. We previously discussed operations x, y and xy in S_3.

$$x : \begin{cases} 1 \xmapsto{x} 2 \\ 2 \xmapsto{x} 3 \\ 3 \xmapsto{x} 1 \end{cases} \qquad y : \begin{cases} 1 \xmapsto{y} 2 \\ 2 \xmapsto{y} 1 \\ 3 \xmapsto{y} 3 \end{cases} \qquad xy : \begin{cases} 1 \xmapsto{y} 2 \xmapsto{x} 3 \\ 2 \xmapsto{y} 1 \xmapsto{x} 2 \\ 3 \xmapsto{y} 3 \xmapsto{x} 1 \end{cases}$$

In the early 1800's Cauchy developed a beautiful notation for working with symmetric groups. His notation centers around decomposing permutations as collections of cycles, and is called "cyclic notation".

Definition. A **cycle**, written as an **ordered list** of **distinct** set elements, corresponds to the permutation which maps each element to the next element in the list, cycling the last element back to the first. Elements which are not included in the list are not changed.

Example. Identifying cycles as permutations in S_3.

$$(1\,2\,3) : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases} \qquad (1\,3\,2) : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases} \qquad (1\,2) : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \qquad (1\,3) : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases} \qquad (1) : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases}$$

Note that we can write cycles in multiple ways, for example $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$. The standard choice is to pick the representation which has the smallest number written first.

Two cycles are called "disjoint" if their underlying sets are disjoint. For example, $(1\ 3\ 5)$ and $(2\ 4)$ are disjoint. However $(1\ 2\ 5)$ and $(2\ 4)$ are not disjoint. It is easy to show that

Proposition. *Disjoint cycles commute.*

We can write permutations as products of disjoint cycles by applying the permutation iteratively and tracing the path of an element until it "closes off" back at the initial value. This gives the cyclic path "generated by" each element. Usually we begin by writing the cycle generated by 1 then consider the next lowest element which wasn't contained in this cycle, etc. Trivial cycles, like (1) or (4), are usually dropped from notation.

Example. Converting from function to cyclic notation in S_6.

$$\begin{cases} 1 \mapsto 4 \\ 2 \mapsto 2 \\ 3 \mapsto 6 \\ 4 \mapsto 1 \\ 5 \mapsto 3 \\ 6 \mapsto 5 \end{cases} \longleftrightarrow \begin{array}{l} (1\,4)\,(2)\,(3\,6\,5) \\ = \quad (1\,4)\,(3\,6\,5) \end{array} \qquad \text{and} \qquad \begin{cases} 1 \mapsto 5 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \\ 4 \mapsto 6 \\ 5 \mapsto 1 \\ 6 \mapsto 4 \end{cases} \longleftrightarrow (1\,5)\,(2\,3)\,(4\,6)$$

Proposition. *This method writes permutations as products of disjoint cycles.*

Furthermore, such an expression is unique (up to commuting disjoint cycles).

We can simplify products of **non-disjoint** cycles by tracing the path of elements, applying **right-to-left**.

Example. Consider the product $(2\ 4\ 3)\,(1\ 4\ 3)$ in S_4.

- Begin with 1. The right cycle sends $1 \mapsto 4$ which the left cycle continues $4 \mapsto 3$.
  So the product will begin $(1\ 3\cdots$
- Continuing with 3, the right cycle sends $3 \mapsto 1$ which is not moved by the left cycle. This returns to the starting position, closing off the cycle.
  So the first cycle is complete: $(1\ 3)$
- We haven't seen 2 yet, so we start the next cycle with it. 2 is not moved by the right cycle $2 \mapsto 2$ but is sent $2 \mapsto 4$ by the left cycle.
  So the product is $(1\ 3)\,(2\ 4\cdots$
- Continuing from 4, the right cycle sends $4 \mapsto 3$ which the left cycle sends $3 \mapsto 2$. This returns to the starting position, closing off the cycle.
  We've used all of the numbers, so the product is $(1\ 3)\,(2\ 4)$

Example. Consider the product $(2\ 3)\,(1\ 3)$ in S_3.

- Begin with 1. The right cycle sends $1 \mapsto 3$, which the left cycle sends $3 \mapsto 2$
  So the cycle begins $(1\ 2\cdots$
- Now continue with 2. The right cycle sends $2 \mapsto 2$ which the left cycle sends $2 \mapsto 3$.
  So the cycle continues $(1\ 2\ 3\cdots$
- Now continue with 3. The right cycle sends $3 \mapsto 1$ which the left cycle sends $1 \mapsto 1$. This returns to the start of the cycle we've been writing, and uses all of the numbers!
  So the full cycle is $(1\ 2\ 3)$

Remark. An excellent practice problem is to write all of this using **permutation matrices!** That takes a lot more space, though. Recall that a permutation matrix is an $n \times n$ square matrix which is all 0 except for at n positions, one in each row and column, where it has 1. Multiplying by a permutation matrix reorders the vector $[x_1, ..., x_n]$. The matrix which moves x_i to position j will have 1 at position (j, i) – column i and row j – with the remainder of that row and column $= 0$. **This part of group theory has a tight connection to linear algebra!**

The most basic cycles are the **length 2 cycles**, usually called either "**transpositions**", or "**swaps**". It isn't hard to show that if you can swap any two elements, then you can build any permutation you want!

Proposition. *All permutations can be written as products of length 2 cycles (swaps).*

Proof. It is enough to write general cycles in such form. Note that $(a_1\ a_2\ \cdots\ a_n) = (a_1\ a_n)\ \cdots\ (a_1\ a_3)\,(a_1\ a_2)$ □

This allows us to split the group of permutations in half based on the number of swaps which are required to build them!

Proposition. *For any given permutation, any decomposition into product of swaps must either always require an even number of swaps or always require an odd number of swaps.*

The most beautiful proof of this involves converting permutations to matrices, noticing that swaps are matrices with determinant -1, and finally recalling that determinant of matrices is multiplicative: $\det(AB) = \det(A)\det(B)$. Permutations which can be written with an even number of swaps have determinant 1. An odd number of swaps corresponds to determinant -1. (Recall that swapping rows or columns in a matrix changes the sign of the determinant.)

Definition. A permutation is **even** if it decomposes as a product of an even number of swaps.
A permutation is **odd** if it decomposes as a product of an odd number of swaps.

Remark. Somewhat confusingly, a cycle is even if it has odd length (and vice versa).
For example $(1\ 2\ 3) = (1\ 3)\,(1\ 2)$ (following the method outlined in the decomposition proof earlier).

Definition. The **alternating group**, $A_n < S_n$ is the subgroup of **even** permutations.

These correspond to the permutation matrices with determinant $\det(P) = 1$. Exactly half of the permutations will be even, so $|A_n| = \frac{n!}{2}$. Alternating groups show up in a lot of places. For example, possible arrangements of the "15 puzzle" correspond to alternating group elements. They also appear as orientation preserving symmetries of certain objects.
Note that the odd permutations don't form a subgroup since (1) the identity is even and (2) products of odd permutations are even.

Permutation groups are important because all finite groups can be viewed as subgroups of a permutation group! This is called **Cayley's Theorem**. We need to be a little clear about what we mean by "*viewed as* a subgroup", though.

Definition. Two groups are **isomorphic** if there is a set bijection between them which preserves all group structure.

Isomorphism is our notion of equality for groups. We've already seen a few examples of this.

Example. $S_{\{1,2,3\}} \cong S_{\{a,b,c\}} \cong S_{\{X,Y,Z\}} \cong S_{\{\text{"Will"},\text{"Treston"},\text{"Darielly"}\}}$.

Example. The Klein 4 group of matrices $\left\{\begin{pmatrix}\pm 1 & 0\\ 0 & \pm 1\end{pmatrix}\right\}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ which is isomorphic to $\{e, x, y, xy\}$ with the relations $x^2 = e$, $y^2 = e$, $xy = yx$. (This is the smallest non-cyclic group.)

Example. The fourth roots of unity $\langle i \rangle < \mathbb{C}$ is isomorphic to $\mathbb{Z}_4$.

Example. Exponentiation gives an isomorphism between the additive and multiplicative real numbers, since $e^{x+y} = e^x \cdot e^y$.

Every finite group is isomorphic to a subgroup of a permutation group using an amazing trick called the "**regular representation**". This is a shadow of the Yoneda Lemma in category theory, so similar things show up in a number of other areas of mathematics!

Theorem [Cayley's Theorem]. *Every finite group is isomorphic to a group of permutations.*

Proof Sketch. Use the **underlying set** of G as the set to be permuted, $X = G$.
Note that for each element $g \in G$ multiplication by that element gives a map $\lambda_g : X \to X$. (Usually we choose left multiplication $\lambda_g(a) = ga$.) To show λ_g is a permutation, we show injective ($ga = gb \iff a = b$) and surjective ($g(g^{-1}a) = a$).
To show that $\{\lambda_g\}$ form a subgroup, note that $\lambda_g \circ \lambda_h = \lambda_{gh}$, so λ_e is the identity and $(\lambda_g)^{-1} = \lambda_{g^{-1}}$. □

We've seen this before. Back when we were first looking at groups we made multiplication tables. In a group, each row of a multiplication table should be a rearrangement of the elements. Multiplication tables are called **Cayley tables**.

products in $\mathbb{Z}_5$

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

products in $\mathbb{Z}_6$

×	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	2	3	2	1