Permutations

Peter Rowlett

1 Definition and notation

Definition. If A is a set, a *permutation* is a bijection $\sigma\colon A \to A$.

We will often consider permutations on a set $\mathbb{Z}(n) = \{x \in \mathbb{Z} \mid 1 \leq x \leq n\}$.

Example

Consider a permutation $\sigma\colon \mathbb{Z}(4) \to \mathbb{Z}(4)$ which maps the elements $\{1, 2, 3, 4\}$ onto $\{a, b, c, d\}$.

- a, b, c and d must be distinct, because σ is injective.
- $\{a, b, c, d\}$ must contain all the elements of $\mathbb{Z}(4)$, because σ is surjective.

Say σ is the permutation that maps $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 4$ and $\sigma(4) = 1$. We can represent this permutation using two-line notation as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

In this notation, the numbers are written out on the top line, with the second line showing where they are mapped to.

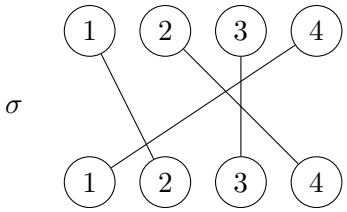
There is also a cycle notation where the permutation is written as a product of *disjoint cycles*. In this representation, we have

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

It is common to omit 1-cycles, so this could also be represented

$$\sigma = (1\,2\,4).$$

We can also draw the permutation as a diagram.



2 Composing Permutations

If $\sigma, \tau\colon \mathbb{Z}(n) \to \mathbb{Z}(n)$ are permutations, then the composite function $\sigma \circ \tau\colon \mathbb{Z}(n) \to \mathbb{Z}(n)$ is also a permutation, since the composite of bijections is also a bijection. This notation tells us that we perform τ first, followed by σ, often just written as $\sigma\tau$ instead of $\sigma \circ \tau$.

2.1 Example

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\,2\,4)$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\,2)(3\,4)$$

In the two-line notation, we can write out the first permutation to be performed as normal, and then what the second permutation does on the line below. Then we just read off the resulting permutation by ignoring the middle row.

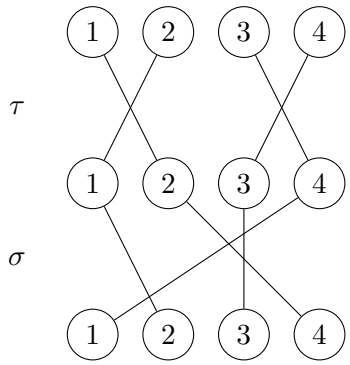
$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

In the one-line notation, we write the cycles out in order, before then following each element through the cycles from right to left.

$$\sigma\tau = (1\,2\,4)(1\,2)(3\,4) = (1\,4\,3)(2) = (1\,4\,3)$$

In this example, we can think about what happens to each of the numbers from 1 to 4. For 1, the right-most cycle $(3\,4)$ doesn't move it, the next cycle $(1\,2)$ swaps it with 2, and then the left-most cycle $(1\,2\,4)$ sends that 2 to 4. So 1 ultimately ends up at 4. Similarly, 2 is swapped with 1 by $(1\,2)$ before being sent back to 2 by the cycle $(1\,2\,4)$. The number 3 is sent to 4 by $(3\,4)$, is not affected by $(1\,2)$, but is then sent to 1 by the cycle $(1\,2\,4)$. Finally, 4 is sent to 3, then left alone, then sent to 1 by the left-most cycle.

Using diagrams, we can think of this as stacking the diagram for τ on top of the diagram for σ.



Note that for $\tau\sigma$ we have

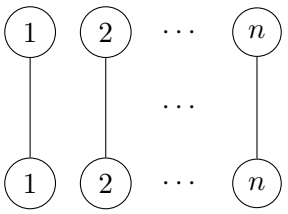
$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \neq \sigma\tau.$$

In general, composition of permutations is not commutative.

3 Identity Permutation

There is a very simple permutation which doesn't relabel anything at all. This is called the identity permutation, defined by $e_n \colon \mathbb{Z}(n) \to \mathbb{Z}(n)$ where $e_n(x) = x$. In the two-line and one-line notation, this is just

$$e_n = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix} = (1)(2)\ldots(n-1)(n).$$



If we compose an identity permutation with any other permutation σ, then this leaves σ unchanged:

$$\sigma e_n = \sigma = e_n \sigma.$$

4 Inverse Permutations

Every permutation σ has an inverse σ^{-1}, which we think of as 'un-shuffling' the numbers we started with.

Example

Using the permutation

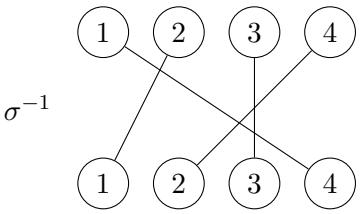
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\,2\,4)$$

then the inverse is easy to find. In two-line notation, we simply read the permutation from bottom to top, rather than top to bottom. We can write the bottom row on the top row, and vice-versa, before reordering.

$$\sigma^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

In the one-line notation, we can simply write the cycle backwards and then rearrange to have the lowest number at the front if we desire.

$$\sigma^{-1} = (4\,2\,1) = (1\,4\,2)$$



Inverse permutations have the property that

$$\sigma\sigma^{-1} = e_n = \sigma^{-1}\sigma.$$

5 Inverses of Composites

Taking inverses of composites is a little trickier, but not by much. If we take the permutations σ and τ from before, then we can show that $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\,2\,4)$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\,2)(3\,4)$$

We know that $\sigma\tau = (1\,4\,3)$, so we should find that $(\sigma\tau)^{-1} = (1\,3\,4)$.

$$\begin{aligned}\tau^{-1}\sigma^{-1} &= (3\,4)^{-1}(1\,2)^{-1}(1\,2\,4)^{-1} \\ &= (3\,4)(1\,2)(1\,4\,2) \\ &= (1\,3\,4) \\ &= (\sigma\tau)^{-1}.\end{aligned}$$

6 Symmetric Groups

Definition. The set of all permutations of $\mathbb{Z}(n)$ forms a group, under composition of permutations. This group is called the **symmetric group** of degree n. We use the notation S_n to denote this group.

Consider S_5. How many elements does it have? i.e. how many permutations are there of five elements?

There are:

- 5 choices for the first number;
- 4 remaining choices for the second number;
- 3 remaining choices for the third number;
- 2 remaining choices for the fourth number;
- 1 remaining choices for the fifth number.

Therefore there are $5 \times 4 \times 3 \times 2 \times 1 = 5! = 120$ elements in S_5.
In general, there are $n!$ permutations of $\mathbb{Z}(n)$, so $n!$ elements in S_n.