Of Permutations

In this series, we shall deal with problems involving various arrangements, orderings and rankings. All of these can be easily formalised using permutations.

A *permutation* π on a set A is a function $\pi : A \to A$ that is *bijective*, i.e. it is

(1) *surjective* (or *onto* A), which means that for each $y \in A$, there exists $x \in A$ such that $\pi(x) = y$,
(2) *injective*, which means that if $\pi(x) = \pi(y)$ for some $x, y \in A$, then $x = y$.

We denote the set of all permutations on the set A as S_A. Specifically, for $n \in \mathbb{N}$ and $A = \{1, 2, \ldots, n\}$, we denote this set of permutations on A as S_n. We call the "permutation" $\pi(x) = x$ that leaves every element of A in place the *identity permutation* (or just *identity*), which we denote id_A or just id.

S_n contains exactly

$$n! = n \cdot (n-1) \cdots 2 \cdot 1$$

permutations — number 1 can be mapped to any number $\pi(1)$ from among 1, 2, ..., n, number 2 can then be mapped to any such number which is not $\pi(1)$, number 3 can be mapped to any such number which is not $\pi(1)$ or $\pi(2)$ etc.

We formulated what a permutation is on an arbitrary set A, but we will mainly work with finite sets. In that case, it is easier to show that a given function acting on this finite A is a permutation, as this theorem shows:

Theorem. Let A be a finite set of size n and let $f : A \to A$ be a function on A. Then, f is injective if and only if f is surjective.

Proof. ($\Longrightarrow$) Because f is injective, every element of A is mapped to a different value, which means that there are n different values in the form $f(a)$, $a \in A$, each of them lying in the set A, which has n elements. That means that among those $f(a)$, $a \in A$, every element of A is represented. In other words, for arbitrary $y \in A$, there must exist an $x \in A$ such that $f(x) = y$.

($\Longleftarrow$) If f was not injective, there would exist distinct $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$. That would mean that there are at most $(n-1)$ different values $f(a)$, $a \in A$, contrary to the fact that f is surjective. □

A corollary of this theorem is that for a finite set A, every injective function $A \to A$ is a permutation, and similarly, every surjective function $A \to A$ is a permutation.

Because permutations are bijections, we may refer to their *inverses* — for $\pi \in S_A$, there exists a mapping π^{-1} such that π^{-1} maps $b \in A$ to the unique element $a \in A$ satisfying $\pi(a) = b$. Because π is a bijection acting on A, π^{-1} is also a bijection defined on A, i.e. it is a permutation again.

It also holds that the *composition* of permutations $\pi, \sigma \in S_A$, defined by

$$(\pi \circ \sigma)(a) = \pi(\sigma(a)), \qquad a \in A,$$

is a permutation. If we compose π with itself $k \in \mathbb{N}$ times, we write this composition as π^k.

Cycles

Suppose we have a permutation π on a finite set A and we choose an element $a_1 \in A$. Then π might map a_1 to itself, or it can map it to another element $a_2 = \pi(a_1)$. Next, a_2 can be then mapped to a_1 or some other element a_3 of A, but it cannot be mapped to a_2, because π is injective and a_1 is already being mapped to a_2.

More generally, suppose that a_1, a_2, …, a_k are all distinct elements of A and it holds that $\pi(a_i) = a_{i+1}$ for $i \in \{1, 2, \ldots, k-1\}$. Suppose also that a_k is mapped to an already visited element, say a_ℓ for some $\ell \in \{1, 2, \ldots, k\}$ — this has to eventually happen, because A is finite. Now, if $\ell \geq 2$, then we would have $\pi(a_k) = a_\ell$ and also $\pi(a_{\ell-1}) = a_\ell$. But $a_k \neq a_{\ell-1}$, so π would not be injective, and thus not a permutation. This means that $\ell = 1$ must happen and therefore π creates a *cycle*

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1.$$

It can be the case that A also contains some other elements which are not part of this cycle. With the same procedure, we can again choose some $b_1 \in A \setminus \{a_1, \ldots, a_k\}$, which will construct another cycle — let us dispense with the arrows and just write the cycle as $(b_1\ b_2\ \ldots\ b_m)$. Continuing like this, we can *decompose the permutation π into disjoint cycles* as

$$\pi = (a_1^1\ a_2^1\ \ldots\ a_{k_1}^1)(a_1^2\ a_2^2\ \ldots\ a_{k_2}^2)\ldots(a_1^m\ a_2^m\ \ldots\ a_{k_m}^m),$$

where the elements a_i^j are all distinct — this notation lists all the individual cycles, $(a_1^j\ a_2^j\ \ldots\ a_{k_j}^j)$ being the j-th cycle. Moreover, these cycles are uniquely determined for the given permutation. Usually, we omit cycles of length 1 for simplicity.

As an example, the permutation $\pi \in S_6$ which is given by $\pi(1) = 4$, $\pi(2) = 2$, $\pi(3) = 6$, $\pi(4) = 5$, $\pi(5) = 1$ and $\pi(6) = 3$ is represented by the cycles

$$\pi = (1\ 4\ 5)(2)(3\ 6) = (1\ 4\ 5)(3\ 6)$$

(we omit the cycle (2) of length one). This gives us a better idea how the permutation behaves — for example, we see that $\pi^6 = \mathrm{id}$ (more generally, it is not hard to see that the smallest positive exponent with this property is equal to the least common multiple of all the cycle lengths). We can also immediately determine the inverse of π — we just have to reverse the order of elements in individual cycles, so $\pi^{-1} = (5\ 4\ 1)(6\ 3)$.

If $\pi(a) = a$ for $a \in A$, we say that a is a *fixed point* of π. If π consists only of one cycle, it is called *cyclic*. If $\pi = (b\ a) \in S_A$, i.e. if π swaps a with b while leaving the remaining points fixed, then we say that π is a *transposition*.

Counting Permuted Values

When several numbers are summed or multiplied together, it does not matter how we order these numbers — $1 + 2 + 3$ is the same as $2 + 1 + 3$ or $3 + 1 + 2$. Thus, if we have a permutation π on a finite set of numbers A, it holds that[1]

$$\sum_{a \in A} a = \sum_{a \in A} \pi(a) \qquad \text{and} \qquad \prod_{a \in A} a = \prod_{a \in A} \pi(a).$$

This simple fact can serve as a surprisingly powerful tool, as we will now illustrate:

Theorem. (Fermat's little theorem) Let p be a prime and $a \in \{1, 2, \ldots, p-1\}$. Then $a^{p-1} \equiv 1 \pmod{p}$.

[1] $\sum$ denotes the *sum* and $\prod$ the *product*.

Proof. Let $A = \{1, 2, \ldots, p-1\}$ and $\pi : A \to A$ defined as $\pi(x) = (ax \mod p)$. We claim that π is injective — to that end, suppose that $x, y \in A$ satisfy $\pi(x) = \pi(y)$. Then $ax \equiv ay \pmod{p}$, and because a and p are coprime, it follows that $x \equiv y \pmod{p}$. However, x and y are from A which contains only numbers between 1 and $p-1$, so $x = y$. We showed that π is injective, and so it must be a permutation thanks to the finiteness of A.

Now, the product

$$\prod_{x \in A} \pi(x) = \pi(1) \cdot \pi(2) \cdots \pi(p-1)$$

must be equal to

$$\prod_{x \in A} x = 1 \cdot 2 \cdots (p-1),$$

because both run over the whole A and π is a permutation, so every element of A appears exactly once in each product, regardless of whether we multiply the values 1, 2, …, $p-1$ in ascending order or in the permuted order given by π.

Finally, we calculate

$$\prod_{x \in A} x = \prod_{x \in A} \pi(x) = \prod_{x \in A} (ax \mod p) \equiv \prod_{x \in A} ax = a^{p-1} \cdot \prod_{x \in A} x \pmod{p},$$

and so $1 \equiv a^{p-1} \pmod{p}$ thanks to the fact that individual elements of A are coprime to p, hence their product is also coprime to p. □