Lecture 2: Functions and Permutations

Summary:
We explore functions and permutations, starting with a fundamental theorem connecting inverses and bijections. We prove that for finite sets of equal size, injectivity, surjectivity, and bijectivity are equivalent properties. We introduce permutations, cycle notation, and the symmetric group. We demonstrate how to represent permutations as products of disjoint cycles and prove that this representation is unique up to reordering.

Topics Covered: cycle, disjoint cycles, permutation, situational equivalence of injectivity and surjectivity, symmetric group

Theorem:

Let $f : S \to T$ be a function. Then, f has an inverse, $\iff$ f is a bijection

Proposition: Let $f : S \to T$ be a function and assume that S and T are finite sets with $|S| = |T|$. Then, TFAE:

1. f is bijection
2. f is surjective
3. f is injective

Note that in order for a bijection $f : S \to T$ to exist, it must be the case that $|S| = |T|$.

Proof of $2 \implies 1$:

Assume that f is surjective with $|S|, |T| < \infty$ and $|S| = |T|$. We want to show that f is injective.

Suppose, for contradiction, that f is not injective. This means there exist $s, s' \in S$ such that $s \neq s'$ and $f(s) = f(s')$.

Note that

$$|\text{im}(S - \{s, s'\})| \leq |S| - 2$$

This is because $|S - \{s, s'\}| = |S| - 2$, so at most $|S| - 2$ elements are mapped to in T.

Note that since $f(s) = f(s')$, we have that

$$\text{im}(S - \{s, s'\}) = \text{im}(S - \{s\})$$

So,

$$|\text{im}(S - \{s, s'\})| = \text{im}(S - \{s\}) \leq |S| - 2$$
$$\implies |\text{im}(S)| \leq |S| - 2 + 1 = |S| - 1 = |T| - 1 < |T|$$
$$\implies |\text{im}(S)| < |T|$$
$$\implies \text{im}(S) \neq T$$

Therefore, f is not surjective, which is a contradiction. So, we conclude that f must be injective.

$$QED$$

Proof of $3 \implies 1$:

Suppose that $f : S \to T$ is injective and $|S|, |T| < \infty$ and $|S| = |T|$. We want to show that f is surjective.

We know that

$$\text{im}(f) = \{f(s) : s \in S\}$$

Since f is injective, we know that $\forall s, s' \in S.\ s \neq s' \implies f(s) \neq f(s')$

$$\implies |\text{im}(f)| = |\{f(s) : s \in S\}| = |S| = |T|$$
$$\implies |\text{im}(f)| = |T|$$

$$\implies \text{im}(f) = T$$

Therefore, f is surjective.

$$QED$$

We have shown that

- $1 \implies 2$
- $1 \implies 3$
- $2 \implies 1$
- $3 \implies 1$

Therefore, we have proven the equivalence.

$$QED$$

Definition:

Let S be a set. A function $\sigma : S \to S$ is called is called a permutation of S when σ is a bijection.

The set of all permutations of S is denoted $\text{Sym}(S)$.

Generally, we will take $S = \{1, 2, ..., n\} = [n]$, in which we use the notation

$$S_n = \text{Sym}([n])$$

Recall that the composition of bijections is a bijection.

Therefore,

1. $\tau, \sigma \in S_n \implies \tau\sigma \in S_n$
2. $\iota_S \in S_n$
   - ι_S is the identity permutation for S
3. $\sigma \in S_n \implies \sigma^{-1} \in S_n$

Later, we will see that permutations of S with composition form a group.

Here is a 2 line notation we can use to describe a permutation

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & .... & \sigma(n) \end{pmatrix}$$

Suppose that

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

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

Then, we have

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

Definition: The permutation σ is called a cycle of length k when there exist elements $a_1, ..., a_k \in [n]$ such that

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, ..., \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$$

and

$$\forall x \in [n] - \{a_1, ..., a_k\}.\ \sigma(x) = x$$

In this case, we use cycle notation as follows:

$$\sigma = (a_1, a_2, ..., a_k)$$

Note that a permutation written in cycle notation can be written in several ways. For example:

$$(2,1,4)=(1,4,2)=(4,2,1)$$

Because it's a cycle so we can start at any element, as long as the order of the elements is the same.

The identity permutation is a cycle of length 0.

Definition: If $\sigma=(a_1,\ldots.,a_k)$ and $\tau=(b_1,\ldots.,b_m)$ are cycles in S_n, then σ and τ are said to be disjoint cycles when

$$\{a_1,\ldots.,a_k\}\cap\{b_1,\ldots.,b_m\}=\emptyset$$

Note that in general, for $\sigma,\tau\in S_n$, it is not the case that $\sigma\tau=\tau\sigma$ (the permutations commute).

For example:

$$(1,2)(3)\ (1,3)(2)=(1,3,2)$$

$$(1,3)(2)\ (1,2)(3)=(1,2,3)$$

Lemma:

If $\sigma,\tau\in S_n$ are disjoint cycles, then $\sigma\tau=\tau\sigma$ (σ and τ commute).

Proof:

Let $\sigma=(a_1,\ldots.,a_k)$ let $\tau=(b_1,\ldots.,b_m)$ with $\{a_1,\ldots.,a_k\}\cap\{b_1,\ldots.,b_m\}=\emptyset$.

Then, $\sigma\tau=\tau\sigma$ holds because the permutations are disjoint, so, they do not interfere with each other.

Definition:

We define the following exponent notation for the composition of permutations:

$$\sigma^i=\underbrace{\sigma\ldots.\sigma}_{i}$$

$$\sigma^{m+n}=\sigma^m\sigma^n$$

$$(\sigma^m)^n=\sigma^{mn}$$

$$\sigma^1\sigma^{-1}=\mathrm{id}=\sigma^0$$

Example:

Note that if

$$\sigma=(a_1,\ldots.,a_n)$$

then

$$\sigma^{-1}=(a_n,\ldots.,a_1)$$

To get the inverse of a cycle, just reverse the order of the cycle.

Theorem:

Every permutation $\sigma\in S_n$ can be written as a product of disjoint cycles. Moreover, up to the rearrangement of cycles, this representation is unique.

Example:

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11\\11&7&6&5&4&8&9&1&10&2&3\end{pmatrix}$$

$$\sigma=(1,11,3,6,8)(2,7,9,10)(4,5)$$

To do this, we start with an arbitrary element and just follow it until we get back to the start. We keep doing this, starting at new elements until we finish.

Proof: We will give an algorithm to write any σ as a product of disjoint cycles.

Successively apply powers of σ to 1

$$1, \sigma(1), \sigma^2(1), \sigma^3(1), \ldots.$$

Eventually we will have $\sigma^k(1) = 1$ for some $k \in \mathbb{Z}^+$. Then, define the cycle

$$\sigma_1 = (1, \sigma(1), \ldots., \sigma^k(1))$$

Then, pick another element $x \in [n] - \{1, \sigma(1), \ldots., \sigma^k(1)\}$ and do the same thing

$$\sigma_2 = (x, \sigma(x), \ldots., \sigma^l(x))$$

And keep going until all elements are in a cycle. If $\sigma_1, \ldots., \sigma_m$ are the cycles that we've defined, then, we have

$$\sigma = \sigma_1 \ldots. \sigma_m$$

$$\text{QED}$$

Practice problem

Let $S = [n]$. Suppose that $\sigma \in S_n$ is n-cycle

$$\sigma = (a_1, \ldots., a_n)$$

Show that σ^{n-1} is the inverse of σ.

It suffices to show that $\forall x \in [n].\ \sigma^n(x) = x$.

Note that x is guaranteed to be in the cycle, since it's an n-cycle and we are working with $S = [n]$.

Suppose that $x = a_1$.

Then,

$$\sigma(a_1) = a_2$$

$$\sigma^2(a_1) = a_3$$

$$\ldots.$$

$$\sigma^n(a_k) = a_{k+1}$$

$$\implies \sigma^n(a_1) = a_1$$

$$QED$$

Another practice problem

Suppose that $\sigma \in S_n$ such that $\forall \tau \in S_n.\ \sigma\tau = \tau\sigma$. Show that $\sigma = \text{id}$.

Proof:

Suppose, for contradiction, that $\sigma \neq \text{id}$. Then, there exists $1 \in [n]$ such that

$$\sigma(1) = k \neq 1$$

Since σ is a bijection, there exists $m \neq 1$ such that $\sigma(m) = 1$.

Pick $t \neq 1, m$

$$\tau = (t, m)$$

$$\sigma\tau(m) = \sigma(t) \neq 1$$

$$\tau\sigma(m) = \tau(1) = 1$$

This is a contradiction because $\sigma\tau \neq \tau\sigma$.

We conclude that $\sigma = \text{id}$.

QED