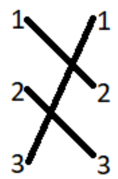
Algebra - I

Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

Hello, today we are going to talk about permutations. I will use the notation [n] to denote the first n natural numbers. A permutation of n symbols is just a bijective function from [n] to [n]: $\sigma:[n]\rightarrow[n]$.

What does bijective function mean? It is a function that is **injective** and **surjective**.

Example 1.
Take n=3. Observe that [3]={1,2,3}. Recall that a permutation of [3] is a bijective function $\sigma:[3]\rightarrow[3]$.
These are the images of each element in [3] under this permutation:
$\sigma(1)=2$
$\sigma(2)=3$
$\sigma(3)=1$.
We can denote this permutation by matching an element on the left to its image on the right as under for the permutation σ :



A permutation is thus a rearrangement of the numbers {1,...,n}. We use the notation S_n to denote the set of all permutations on n letters.

I will use what is called *one-line notation* to describe a permutation. So, if I have a permutation σ , then its one-line notation is simply $\sigma(1)\sigma(2)...\sigma(n)$ in sequence. So, if you look at the permutation we had earlier it is one line notation is just - $\sigma(1)\sigma(2)\sigma(3)$ which is 231. This is an efficient way of writing down permutations.

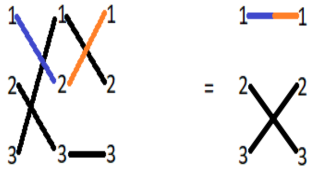
Example 2.
I am going to try to list all the permutations in S_3 . The simplest permutation takes 1 to 1, 2 to 2 and 3 to 3. Such a permutation exists for all S_n defined in the obvious way. It is called the *identity* and is denoted id. So, in one-line notation the id is **123**.
So, what else can I do? I can take 1 to 1, I can take 2 to 3 and 3 to 2 to give **132**. This exhausts the possibilities where I am taking 1 to 1.
If I am taking 1 to 2 then what can I do? I can take 2 to 1 and 3 to 3 to give **213**, or I can take 2 to 3 and then 3 to 1 to give **231.**
I can take 1 to 3 in which case I can take 2 to 1 and 3 to 2 to give **312**, or 3 to 1 and 2 to 2 to give **321**.
So, these are the 6 permutations on 3 letters.

How many permutations are there in S_n ? Firstly how many choices do I have for $\sigma(1)$? So it can go to any of the numbers 1 to n. So, sigma(1) has **n** choices. Now having made that choice, how many choices do I have for $\sigma(2)$? Well, I have already used up 1 of the n numbers for $\sigma(1)$ so I cannot use it again. So, I have **n-1** choices for $\sigma(2)$. Now having chosen $\sigma(1)$ and $\sigma(2)$ what remains are **n-2** choices for $\sigma(3)$ and so it goes. All the way in the end having chosen $\sigma(1)$, $\sigma(2)$,... $\sigma(n-1)$, there will be only one element from the set 1 to n which has not been used and that is going to be $\sigma(n)$. So, there are: $n!:=n(n-1)(n-2)...1$ permutations of the set [n]. We call n! “n factorial”. Observe that S_3 has cardinality 6=3!.

If you take a deck of cards, then the every every rearrangement of this deck of cards is a permutation. How many possible such decks can I get? If you do not have the jokers then it is 52!- pretty large!

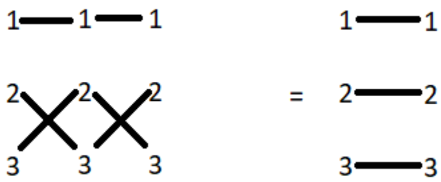
The theory of permutations becomes much more interesting once we take into account certain binary operations that we can perform on them. *Binary operations* on a set S are functions $\sigma : S \times S \rightarrow S$ - that is, they take two elements of S as input and output an element of S. The operation I am talking about is called *composition*. If I have bijections $\sigma_1 : [n] \rightarrow [n]$ and $\sigma_2 : [n] \rightarrow [n]$, then I can compose these functions to get a bijection which we denote $\sigma_2 \cdot \sigma_1 : [n] \rightarrow [n]$. This is because the composition of bijections is still a bijection. What I get is a way of creating a new permutation given 2 permutations.

Example 3.

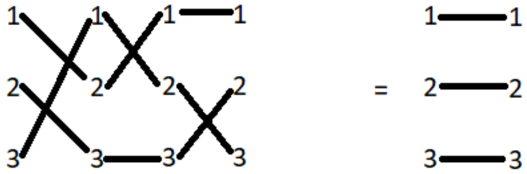


Let us take $\sigma_1 = 231$ and $\sigma_2 = 213$. How do I compute $\sigma_2 \cdot \sigma_1$ (note σ_2 is on the left in the product but on the right in the figure)? So, $\sigma_2 \cdot \sigma_1(1) = \sigma_2(\sigma_1(1))$. Now $\sigma_1(1) = 2$ and $\sigma_2(2) = 1$, so $\sigma_2 \cdot \sigma_1(1) = 1$. Similarly $\sigma_1(2) = 3$ and $\sigma_2(3) = 3$ so $\sigma_2 \cdot \sigma_1(2) = 3$ .Similarly, $\sigma_2 \cdot \sigma_1(3) = 2$. So $\sigma_2 \cdot \sigma_1 = 132$. Another way of thinking about this is: Under σ_1 , 1 goes to 2 and then 2 goes to 1 under σ_2 . So I can just follow through this arrow from left to right and that is telling me that under $\sigma_2 \cdot \sigma_1$ 1 goes to 1.
And where does 2 go? Again I will start with 2 and then I will follow the arrow. So, 2 goes to 3 under σ_1 and 3 goes to 3 under σ_2 , so 2 goes to 3. The 3 goes to 1 under σ_1 and then 1 goes to 2 under σ_2 , so 3 goes to 2. So, so you can compose permutations by simply following through the arrows.

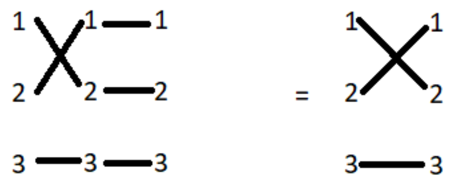
Example 4.
This time we will take a 3rd permutation $\sigma_3 = 132$. I want to compute $\sigma_3 \cdot \sigma_2 \cdot \sigma_1$. You can think about this in 2 ways, either as composing σ_1 and σ_2 - so that is what we just computed- and then we compose it with σ_3 .



So we get the identity permutation from Example 2.
Or I could have done this in another order I could have done it $(\sigma_3 \cdot \sigma_2) \cdot \sigma_1$. Note that there is no difference between $(\sigma_3 \cdot \sigma_2) \cdot \sigma_1$ and $\sigma_3 \cdot (\sigma_2 \cdot \sigma_1)$.

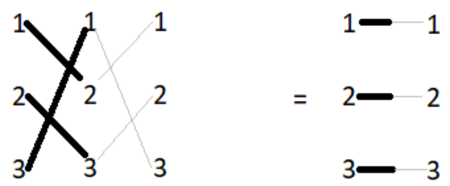


The identity permutation has the property that when you compose it with any permutation it does not change the permutation.



The third property that I want to illustrate about permutations is that it is possible to 'undo' anything that you have done.

Example 5.
Let $\sigma=231$, then I can find a permutation which undoes whatever I did. So, if I have taken 1 to 2 I want to undo it I want to take 2 back to 1. So, 2 must go back to 1. Since 2 goes to 3, I want to take 3 back to 2; and 3 goes to 1, thus I want to take 1 back to 3.



This is what we call the inverse function in set theory. So this is called the *inverse* of σ , and is denoted σ^{-1}. Observe that $\sigma\cdot\sigma^{-1}$ is also the identity.
So to summarize, for every $n\geqslant 1$, :

- The set S_n of permutations of [n] has cardinality n!.
- Each permutation may be written in one-line notation by listing in increasing order of elements of [n] the images of those elements.
- The set S_n has a binary operation called composition.
- This binary operation satisfies the following axioms:
  - Closure: Composing two permutations yields a permutation.
  - Associativity: $\sigma_3\cdot(\sigma_2\cdot\sigma_1)=(\sigma_3\cdot\sigma_2)\cdot\sigma_1$ for all $\sigma_{3,}\sigma_{2,}\sigma_1\in S_n$.
  - Existence of identity: There exists an element $id\in S_n$ such that $id\cdot\sigma=\sigma\cdot id=\sigma$ for all $\sigma\in S_n$.
  - Existence of inverse: For every $\sigma\in S_n$ there exists an element σ^{-1} such that $\sigma^{-1}\cdot\sigma=\sigma\cdot\sigma^{-1}=id$.

These these properties of permutations taken together abstractly give the definition of an abstract group, which we will talk about next time.