30 January 2023
MAT 2250

Proof of Theorem (Every permutation can be decomposed as a union of disjoint cycles in a unique way, up to the order of cycles)

Let's say the permutation is $(f(1)\ f(2) \dots f(n))$

So $1 \mapsto f(1)$.

If $f(1) = 1 \Rightarrow$ we have a cycle (1) & we can write the permutation as:

$f = [1]\ (f(2) \dots f(n))$

disjoint supports

and then we can consider 2 here & use induction on n

If $f(1) \neq 1$:

$1 \mapsto f(1) \mapsto f(f(1))$

If $f(f(1)) = 1 \Rightarrow$ we can decompose $f = [1\ f(1)]\ (\dots)$ length $n-2$ (use induction)

In general, if $\exists$ m such that

(*) $\underbrace{f \dots f}_{m \text{ times}}(1) = 1$, then we are done

$f = [1\ f(1) \dots \underbrace{f \dots f}_{m-1 \text{ times}}(1)]\ (\dots)$ ↪ length $< n$ (so can use induction)

Claim: $\exists$ always $m \geq 1$ such that $\underbrace{f \dots f}_{m}(1) = 1$.

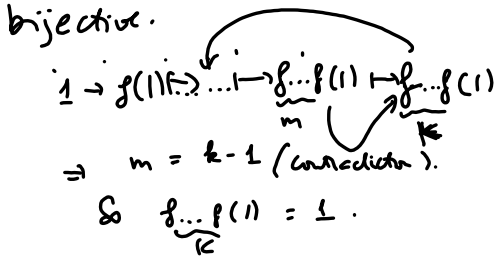
If not, we claim that

$1 \mapsto f(1) \to f(f(1)) \mapsto \dots$ contains an infinite sequence. If it is not infinite, assume that m is the largest number such that all elements $1, f(1), \dots, \underbrace{f \dots f}_{m}(1)$ are pairwise distinct.

$1 \mapsto f(1) \mapsto f(f(1)) \mapsto \dots \mapsto \underbrace{f \dots f}_{m}(1) \mapsto \underbrace{f \dots f}_{k}(1)$

$k < m$.

Claim that:
$f \cdots f(1)$ must be 1.
(k)
We will use that $f:\{1,\dots,n\} \circlearrowleft$ is bijective.



$\Rightarrow m = k-1$ (contradiction).
So $\underbrace{f \cdots f}_{k}(1) = 1$.

Now $1 \mapsto f(1) \mapsto \cdots$ must be finite because $f:\{1,\dots,n\} \circlearrowleft$ has a finite image set. $\square$

Example: $\pi = (5\ 8\ 3\ 1\ 9\ 7\ 6\ 2\ 4)$
$1 \mapsto 5 \mapsto 9 \mapsto 4 \mapsto 1 \Rightarrow$ cycle $[1\ 5\ 9\ 4]$
$2 \mapsto 8 \mapsto 2 \Rightarrow$ cycle $[2\ 8]$
$3 \mapsto 3 \rightarrow$ cycle $[3]$ (this is identity)

$6 \mapsto 7 \mapsto 6 \Rightarrow$ cycle $[6\ 7]$
$\pi = [1\ 5\ 9\ 4]\ [2\ 8]\ [3]\ [6\ 7]$

Rmk: If we have a (bijective) permutation of infinite sets, then maybe this theorem is not true.
Example: $f: \mathbb{N} \to \mathbb{N}$

Stirling numbers of the first kind:
$s_{n,k}$ = # of permutations of $\{1,\dots,n\}$ which can be decomposed into k cycles.

$\pi = (5\ 8\ 3\ 1\ 9\ 7\ 6\ 2\ 4)$
$= \underbrace{[1\ 5\ 9\ 4][2\ 8][3][6\ 7]}_{4 \text{ cycles}}$
So π is counted in $s_{9,4}$.
Set $\{1,5,9,4\} \Longrightarrow (4-1)!$ cycles

$\{1,5,9,4\}$ gives us 4! permutations.
Each cycle corresponds to 4 such permutations
$[1\ 5\ 9\ 4] = [5\ 9\ 4\ 1]$
$= [9\ 4\ 1\ 5] = [4\ 1\ 5\ 9]$
So # of cycles $= \frac{4!}{4} = 3!$
So there are some relations between $S_{n,k}$ & $s_{n,k}$. But the precise relation is through "inversion formula" which we will learn later.

§ 1.4 Recurrence relation

In general, Recurrence relation allows us to actually compute some numbers which are complicated to define. (i.e. we can use computers to compute)
Def: Induction $\Leftrightarrow$ Recurrence

Example: in Logic, you can define $\mathbb{N}$ by claiming that it has an element 0, & define by recurrence an element $S(n)$ if n is already defined ($S(n) = n+1$)

$S(n)$ satisfies:
$S(n+m) = S(n) + m + 1$ ...
$S(nm)$ ...

Example: We know $n!$. But if we want actually to compute $n!$ we need the recurrence:
$n! = (n-1)! \cdot n$.

Some important recurrences:

For binomial numbers:

$$\begin{cases} \binom{n}{k} = \binom{n}{k-1} + \binom{n-1}{k-1} \\ \binom{n}{0} = 1 \end{cases}$$

1st proof:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

$$\binom{n-1}{k-1} = \frac{(n-1)!}{(k-1)!(n-k)!}$$

$$\binom{n-1}{k} = \frac{(n-1)!}{k!(n-1-k)!}$$

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!}$$

$$= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left[\frac{1}{(n-k)} + \frac{1}{k}\right]$$

$$= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left[\frac{k+(n-k)}{k(n-k)}\right]$$

$$= \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Second proof: $\binom{n}{k}$ = # of k-subsets of $\{1,\dots,n\}$ = # of subsets of $\{1,\dots,n\}$ having k elements.

If A is a k-subset of $\{1,\dots,n\}$
$\Rightarrow$ $\exists$ 2 disjoint cases:

Case 1: $n \notin A \Rightarrow A$ is a k-subset of $\{1,\dots,n-1\} \Rightarrow$ by definition $\exists$ $\binom{n-1}{k}$ such A's.

Case 2: $n \in A \Rightarrow B = A \setminus \{n\}$ is $(k-1)$-subset of $\{1,\dots,n-1\}$
$\Rightarrow$ $\exists$ $\binom{n-1}{k-1}$ such B's

$\exists$ bijection: B $(k-1)$-subset of $\{1,\dots,n-1\}$ $\longrightarrow$ A k-subset of $\{1,\dots,n\}$ containing n

$$B \longmapsto B \cup \{n\} = A$$

$$B = A \setminus \{n\} \longleftarrow A$$

So, by the Summation Rule:
$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. □

$\binom{n}{n} = 1 = \binom{n}{0}$

# of subsets with n elements

# of subsets with $= \{\emptyset\}$ elements.

n \ k	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1
⋮						

Pascal's triangle (known long before Pascal)

For Stirling numbers of the second kind

$S_{n,k} = S_{n-1,k-1} + k S_{n-1,k}$.

$S_{n,k}$ = # of ways to decompose $\{1,\dots,n\}$ into k non-empty disjoint subsets.

Proof: Fix $a \in \{1,\dots,n\}$.

Consider a decomposition, called D:

$\{1,\dots,n\} = A_1 \sqcup \dots \sqcup A_k$.

Case 1: If $\{a\} = A_j$ for some j ($\{a\}$ is a block itself)

$\Rightarrow D = $ a $(k-1)$-decomposition of $\{1,\dots,n\} \setminus \{a\}$ $\sqcup \{a\}$

$\exists$ a $S_{n-1,k-1}$ such. (the first term on the RHS for the recurrence relation)

Case 2: a is not a block itself

i.e.: $\exists\ j$ such that $a \in A_j$ but $\{a\} \neq A_j$. $\Rightarrow A_j \setminus \{a\} \neq \emptyset$.

Then $D' = A_1 \sqcup \dots \sqcup A_{j-1} \sqcup (A_j \setminus \{a\}) \sqcup A_{j+1} \sqcup \dots \sqcup A_k$

is a k-decomposition of $\{1,\dots,n\} \setminus \{a\}$

There are $S_{n-1,k}$ such D'.

$\exists$ k-to-1 correspondence

D': k-decomposition of $\{1,\dots,n\} \setminus \{a\}$ $\longrightarrow$ D: k-decomp of $\{1,\dots,n\}$

$D' = A_1' \sqcup \dots \sqcup A_k'$ $\mapsto$ k choices:

$D_1 = (A_1' \cup \{a\}) \sqcup A_2' \sqcup \dots \sqcup A_k'$

$D_2 = A_1' \sqcup (A_2' \cup \{a\}) \sqcup A_3' \sqcup \dots \sqcup A_k'$

$\vdots$

$D_k = A_1' \sqcup A_2' \sqcup \dots \sqcup A_{k-1}' \sqcup (A_k' \cup \{a\})$

$D' \longleftrightarrow D_1, D_2, \dots, D_k$

There are $S_{n-1,k}$ and $D' \Rightarrow \exists k\, S_{n-1,k}$ such $D_1, \dots, D_k$.

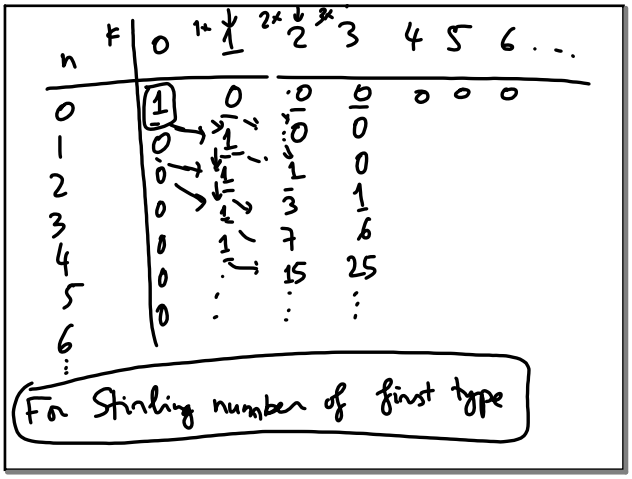
By Summation rule:

$S_{n,k} = \underbrace{S_{n-1,k-1}}_{(a \text{ is a block itself})} + \underbrace{k\, S_{n-1,k}}_{(n \text{ belongs to one of the } k \text{ blocks, \& } n \text{ is not a block itself.})}$

This can be regarded as just convenience

$S_{0,0} = 1$, $S_{0,k} = 0$ $(k>0)$, $S_{n,0} = 0$ for $n>0$.

Triangle for $S_{n,k}$



$S_{n,k} = S_{n-k,k-1} + (n-1) S_{n-1,k}$

(Different from that for $S_{n,k}$)

Proof: Similar to that for $S_{n,k}$, in that we consider cycles if $a=n$ is a cycle itself ([a]) in the decomposition of a permutation π.

Case 1: If $a=n$ is a cycle itself in π, then we can write

$\pi = \pi' \circ [a]$

$(k-1)$-permutation of $\{1,\dots,n\} \setminus \{a\}$

There are $S_{n-1,k-1}$ such π' (& also such π).

Case 2: If a is not a cycle itself, then we can write:

$\pi = \pi_1^* \circ \dots \circ \pi_k^*$, &

$a \in \pi_j \Rightarrow \pi = \pi_1' \circ \dots \circ \pi_j' \circ (a\ b \dots) \circ \pi_{j+1}' \circ \dots \circ \pi_k'$

where $\pi_1', \dots, \pi_k'$ is a k-decomposition of a permutation of $\{1,\dots,n\} \setminus \{a,b\}$.

π': k-permutation of $\{1,\dots,n-1\}$ $\longrightarrow$ π: k-permutation of $\{1,\dots,n\}$

$\pi_1' \circ \pi_2' \circ \dots \pi_j' \circ \dots \pi_k' \mapsto$ $n-1$ permutations where we put n in front of 1 of the cycles.

What does this mean? Say $n=9$. & we have a cycle $[1\ 3\ 4\ 6]$

$[1\ 3\ 4\ 6] = [3\ 4\ 6\ 1]$

$= [4\ 6\ 1\ 3] = [6\ 1\ 3\ 4]$

If we put 9 in front of these cycles we get 4 different cycles:

$[1\ 3\ 4\ 6] \xrightarrow{\text{add } 9} [9\ 1\ 3\ 4\ 6] \neq$
$[3\ 4\ 6\ 1] \xrightarrow{\text{add } 9} [9\ 3\ 4\ 6\ 1] \neq$
$[4\ 6\ 1\ 3] \xrightarrow{\text{add } 9} [9\ 4\ 6\ 1\ 3] \neq$
$[6\ 1\ 3\ 4] \xrightarrow{\text{add } 9} [9\ 6\ 1\ 3\ 4]$

This is why we have the $n-1$ factor. □

We can get a triangle for $S_{n,k}=0$ by using $S_{0,0}=1$ → convenience! $S_{0,k}=0$, $S_{n,0}=0$ → $n,k>0$.

Polynomial method:

We proved several recurrences for positive integer arguments (which make the proof easy). But then we can extend these recurrences to more general arguments, for example $\mathbb{R}$ or $\mathbb{C}$.

Example: $\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$ holds for $n,k\in\mathbb{N}$.

But now we can define for general $z\in\mathbb{C}$:

$$\binom{z}{k}=\frac{z(z-1)\cdots(z-k+1)}{k!},\quad k\in\mathbb{N}$$

& then we claim that

$$\binom{z}{k}=\binom{z-1}{k-1}+\binom{z-1}{k}\quad \forall z\in\mathbb{C}.$$

This is because $\binom{z}{k}=$ is a polynomial in z (of degree k).

Also $\binom{z-1}{k-1}+\binom{z-1}{k}$ is a polynomial of degree $\leq k$ in z.

We knew that (for a fixed k)

$$\binom{z}{k}=\binom{z-1}{k-1}+\binom{z-1}{k}\quad \forall z\in\mathbb{N}.$$

Fundamental theorem of algebra says that the polynomial

$$\binom{z}{k}-\left[\binom{z-1}{k-1}+\binom{z-1}{k}\right]$$

which has degree $\leq k$, and has infinitely many zeros ($z\in\mathbb{N}$) must be 0 identically.