Proof of Thm. 1.17.

CASE 1: $0 \leq k \leq n$.

CASE 2: $k < 0$.

CASE 3: $k > n$.

In Case 1: Thm. 1.28 yields $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

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

In Case 2: $k<0$, so $\binom{n}{k} = 0$.

But $n-k > n$ (since $k<0$), thus $\binom{n}{n-k} = 0$

(by Prop. 1.14, applied to $n-k$ instead of k).

Thus, $\binom{n}{k} = 0 = \binom{n}{n-k}$.

In Case 3: similar. $\square$

Prop. 1.29. Let $k \in \mathbb{Z}$. Then, $\binom{0}{k} = [k=0]$.

Here, we are using the Iverson bracket notation:

Def. For any statement $\mathcal{A}$, we let $[\mathcal{A}]$ be the truth value of $\mathcal{A}$, defined to be $\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases}$.

For example, $[1+2=3] = 1$,
$[1+2=4] = 0$,
$[\text{Thm. } 1.17] = 1$.

$\square$

Proof of Prop. 1.29. Distinguish cases $k<0$, $k=0$, $k>0$.

Proof of Thm. 1.18. We first claim:

Claim 1: $\binom{n}{k} \in \mathbb{N}$ whenever $n \in \mathbb{N}$ and $k \in \mathbb{Z}$.

Proof of Claim 1: Induction on n.

Base case: $\binom{0}{k} = [k=0] \in \{0,1\} \subseteq \mathbb{N}$.
(by Prop. 1.29)

<u>Step:</u> Let $m \in \mathbb{N}$. Assume (as the IH = induction hypothesis) that Claim 1 holds for $n = m$.

For any $k \in \mathbb{Z}$, we have

$$\binom{m+1}{k} = \underbrace{\binom{m}{k-1}}_{\substack{\in \mathbb{N} \\ \text{(by IH)}}} + \underbrace{\binom{m}{k}}_{\substack{\in \mathbb{N} \\ \text{(by IH)}}} \qquad \text{(by Thm. 1.16)}$$

$$\in \mathbb{N}.$$

Thus, Claim 1 holds for $n = m+1$.

So Claim 1 is proven.

So let us prove Thm. 1.18.

CASE 1: $n \geq 0$.

CASE 2: $n < 0$.

In Case 1, $n \in \mathbb{N}$, thus Claim 1 yields $\binom{n}{k} \in \mathbb{N} \subseteq \mathbb{Z}$.

In Case 2: $n<0$. Thus, $n \leq -1$.

Prop. 1.15 (applied to $-n$ instead of n) yields

$$\binom{n}{k} = (-1)^k \binom{-n+k-1}{k}.$$

Thus, if $-n+k-1 \in \mathbb{N}$, then Claim 1 yields

$$\binom{n}{k} = (-1)^k \underbrace{\binom{-n+k-1}{k}}_{\in \mathbb{N}} \in \mathbb{Z}.$$

What if $-n+k-1 \notin \mathbb{N}$? Thus, $-n+k-1<0$.

Adding this to $n \leq -1$, we obtain $(-n+k-1)+n<-1$.

This simplifies to $k<0$. Thus, $\binom{n}{k} = 0 \in \mathbb{Z}$. $\square$

Proof of Thm. 1.19. Induction on n.

Base: If S is a 0-element set (i.e., $S=\emptyset$), then

(# of k-elt. subsets of S)

= (# of k-elt. subsets of $\emptyset$) $= [k=0] \underset{\text{(Prop. 1.29)}}{=} \binom{0}{k}$.

<u>Step:</u> Let $m \in \mathbb{N}$. Assume (as IH) that Thm. 1.19 holds for $n = m$.

Let S be an $(m+1)$-elt. set.

Thus, S is nonempty. So $\exists\, t \in S$. Fix such a t.

Now, there are two types of subsets of S:

<u>Type 1:</u> those that contain t;

<u>Type 2:</u> those that don't contain t.

So (# of k-elt. subsets of S)

(# of k-elt. subsets of S of Type 1)

= (# of k-elt. subsets of S of Type 2).

(1) + (# of k-elt. subsets

But the subsets of S of Type 2 are exactly the subsets of $S \setminus \{t\}$. So

(# of k-elt. subsets of S of Type 2)

= (# of k-elt. subsets of $S \setminus \{t\}$) $\overset{\text{IH}}{=\!=} \dbinom{m}{k}$.

What about Type 1?

Informally: The subsets of S of Type 1 with k elements "correspond to" the subsets of $S\setminus\{t\}$ with $k-1$ elements.

Formally: The map

$$\begin{aligned}\{k\text{-elt. subsets of } S \text{ of Type } 1\} &\longrightarrow \{(k-1)\text{-elt. subsets of } S\setminus\{t\}\},\\ Q &\longmapsto Q\setminus\{t\}\end{aligned}$$

is a bijection (its inverse is

$$\begin{aligned}\{(k-1)\text{-elt. subsets of } S\setminus\{t\}\} &\longrightarrow \{k\text{-elt. subsets of } S \text{ of Type } 1\},\\ R &\longmapsto R\cup\{t\}\end{aligned}$$

).

But if X and Y are finite sets and if $\exists$ a bijection from X to Y, then $|X|=|Y|$. Thus,

$$|\{k\text{-elt. subsets of } S \text{ of Type } 1\}|$$
$$= |\{(k-1)\text{-elt. subset of } S\setminus\{t\}\}|.$$

In other words,

(# of k-elt. subsets of S of Type 1)

$= $ (# of $(k-1)$-elt. subsets of $S \setminus \{t\}$)

$$\overset{\text{IH}}{=} \binom{m}{k-1}.$$

So (1) becomes

(# of k-elt. subsets of S)

$$= \binom{m}{k-1} + \binom{m}{k} \underset{\substack{\text{Thm. 1.16} \\ \text{(applied to } n=m+1)}}{=} \binom{m+1}{k}.$$

$\square$

In other words, Thm. 1.19 holds for $n=m+1$.

<u>Proof of Thm. 1.21.</u> I will rewrite $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ as $\sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ (that is, a sum over <u>all</u> integers k).

Why is this better <u>infinite</u> sum well-defined?

Because only finitely many of its terms are $\neq 0$.
For example, if $n=3$, then it has the form

$$\cdots + 0 + 0 + 0 + x^3 + 3x^2y + 3xy^2 + y^3 + 0 + 0 + 0 + \cdots$$

An infinite sum that has only finitely many nonzero terms is always well-defined. Its value is obtained by discarding the 0's.

Since $\binom{n}{k}=0$ whenever $k \notin \{0,1,\dots,n\}$, we see that

$\sum\limits_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ is well-defined & equals $\sum\limits_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

Thus, it remains to prove

$$(2) \qquad (x+y)^n = \sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}.$$

We'll prove this by induction:

<u>Base:</u> $1=1$. ✓

~~Base~~

<u>Step</u>: Assume (2) holds for $n=m$ (where $m \in \mathbb{N}$ is fixed).

Must prove: (2) holds for $n=m+1$.

We have

$$(x+y)^{m+1} = \underbrace{(x+y)^m}_{\stackrel{IH}{=} \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k}} (x+y)$$

$$= \left(\sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k}\right)(x+y)$$

$$= \left(\sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k}\right)x + \left(\sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k}\right)y$$

$$= \sum_{k\in\mathbb{Z}} \binom{m}{k} x^{k+1} y^{m-k} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k+1}$$

$$= \sum_{k\in\mathbb{Z}} \binom{m}{k-1} x^k y^{m-k+1} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k+1}$$

(here, we substituted $k-1$ for k in the first sum)

$$= \sum_{k\in\mathbb{Z}} \underbrace{\left(\binom{m}{k-1} + \binom{m}{k}\right)}_{=\binom{m+1}{k}} x^k y^{m-k+1}$$

$$= \sum_{k\in\mathbb{Z}} \binom{m+1}{k} x^k y^{m-k+1} = \sum_{k\in\mathbb{Z}} \binom{m+1}{k} x^k y^{m+1-k}.$$

$\square$

Thus, (2) holds for $n = m+1$.

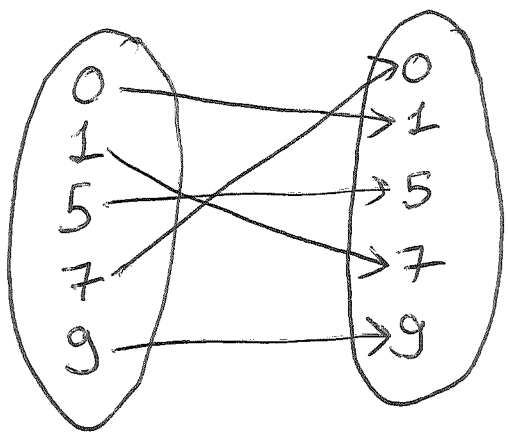
The proofs of the other remaining theorems may appear later.

1.4. Counting

Counting := enumeration := finding sizes of finite sets.
E.g., this is what we have done in Prop. 1.5 and Thm. 1.19.
Much more can be done. Some examples:

<u>Def.</u> A <u>permutation</u> of a set X is a bijection from X to X.

For example,



is a permutation of $\{0, 1, 5, 7, 9\}$

<u>Thm. 1.30.</u> Let $n \in \mathbb{N}$. Let X be an n-elt. set. Then,
$$(\# \text{ of permutations of } X) = n!.$$
(This will prove this later.)

<u>Def.</u> A <u>derangement</u> of a set X means a permutation σ of X such that $\sigma(x) \neq x \ \forall x \in X$.

How many derangements does an n-elt. set have?

<u>Def.</u> For each $n \in \mathbb{N}$, let $[n]$ be the set $\{1, 2, \ldots, n\}$.

Instead of studying arbitrary n-elt. sets X, it suffices to study $[n]$:

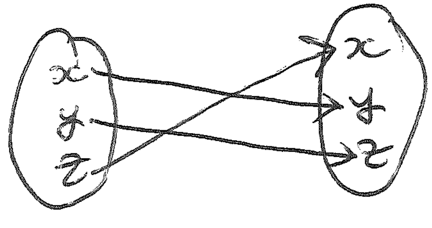
<u>Lemma 1.31.</u> Let X be any n-elt. set. Then,

(# of derangements of X) = (# of derangements of $[n]$).

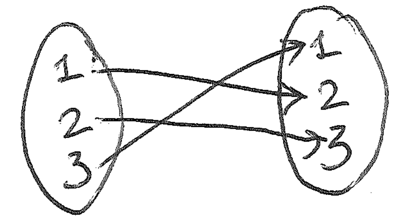
<u>Proof.</u> Fix any bijection $\phi : X \to [n]$. (It exists, since X has n elements.) Now, any derangement of X can be transformed into a derangement of $[n]$ by "relabeling" the elements of X as $1, 2, \ldots, n$ using ϕ.

For example, the derangement

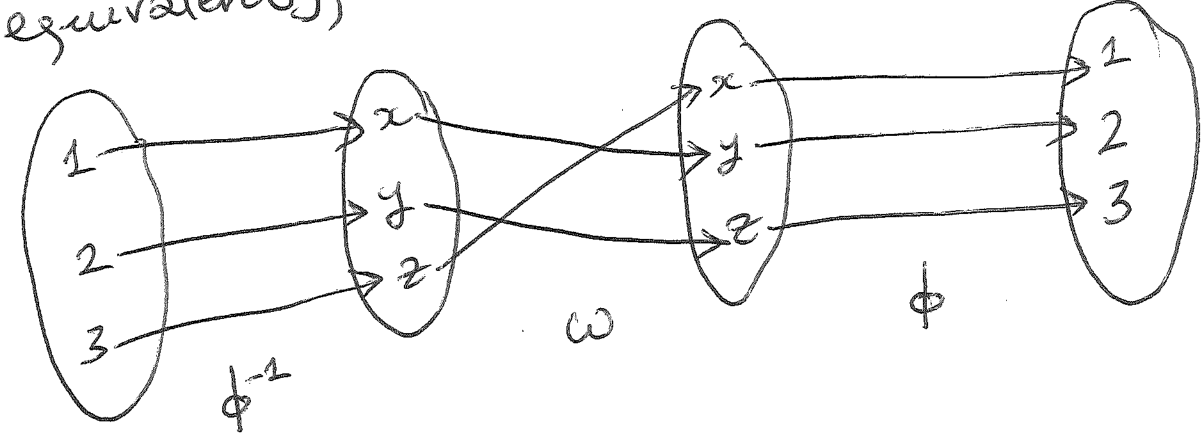
ω :



becomes



or, equivalently,



$\phi\circ\omega\circ\phi^{-1}$.

So, formally,

$$\begin{aligned}\{\text{derangements of } X\} &\longrightarrow \{\text{derangements of } [n]\},\\ \omega &\longmapsto \phi\circ\omega\circ\phi^{-1}\end{aligned}$$

is a bijection (its inverse being

$$\begin{aligned}\{\text{derangements of } [n]\} &\longrightarrow \{\text{derangements of } X\},\\ \alpha &\longmapsto \phi^{-1}\circ\alpha\circ\phi\ \ ).\end{aligned}$$

Thus, $|\{\text{derangements of } X\}| = |\{\text{derangements of } [n]\}|$.

$\square$

So it suffices to count derangements of n.

<u>Def.</u> For each $n \in \mathbb{N}$, let D_n be the # of derangements of $[n]$.

<u>Def.</u> Let $n \in \mathbb{N}$. The <u>one-line notation</u> of a permutation σ of $[n]$ is the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$.

<u>Ex.</u> The permutations of $[3]$ are (in one-line notation)

$(1,2,3)$, $(1,3,2)$, $(2,1,3)$,

$(2,3,1)$, $(3,1,2)$, $(3,2,1)$.

Only $(2,3,1)$ & $(3,1,2)$ are derangements of $[3]$.

Thus, $D_3 = 2$.

<u>Ex:</u>

$D_0 = 1$ (since $\mathrm{id}: \emptyset \to \emptyset$ is a derangement);

$D_1 = 0$ (since $\mathrm{id}: [1] \to [1]$ is not a derangement);

$D_2 = 1$; $D_3 = 2$; $D_4 = 9$.

[oeis.org: Online Encyclopedia of Integer Sequences]

Thm. 1.32. (a) $D_n = (n-1)(D_{n-1} + D_{n-2}) \quad \forall n \geq 2.$

(b) $D_n = n D_{n-1} + (-1)^n \quad \forall n \geq 1.$

(c) $n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k} \quad \forall n \in \mathbb{N}.$

(d) $D_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \quad \forall n \in \mathbb{N}.$

(e) $D_n = \text{round}\left(\frac{n!}{e}\right) \quad \forall n \geq 1.$

Here, $e \approx 2{,}718\ldots$, and $\text{round}(x) = \lfloor x + \frac{1}{2} \rfloor$.

(Some of these will be proven later.)

Def. A permutation σ of $[n]$ is <u>short-legged</u> if $\forall i \in [n]$ we have $|\sigma(i) - i| \leq 1$.

Q: How many short-legged permutations are there?

Ex: For $n=3$, these are

$(1,2,3)$, $(1,3,2)$, $(2,1,3)$, ~~(2,3,1)~~, ~~(3,1,2)~~, ~~(3,2,1)~~.

For $n=4$, these are

$(1,2,3,4)$, $(1,2,4,3)$, $(1,3,2,4)$, $(2,1,3,4)$, $(2,1,4,3)$.

Prop. 1.33. Let $n \in \mathbb{N}$. Then,

(# of short-legged permutations of $[n]$) $= f_{n+1}$.

Proof idea (1): ~~Recur Induct~~ Strong induction.

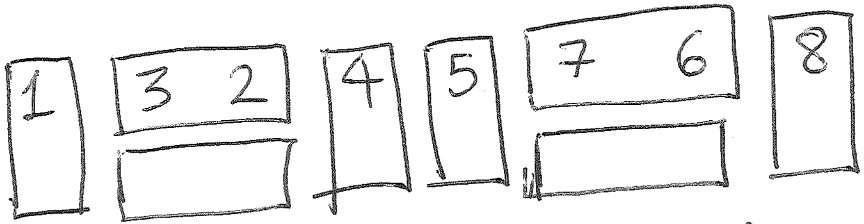
Main idea: If σ is a short-legged permutation of $[n]$, then either $\sigma(n) = n$ or $\sigma(n) = n-1$; in the latter case, $\sigma(n-1) = n$ (since otherwise, short-leggedness is violated for $i = \sigma^{-1}(n)$). ∎

Proof idea (2): A short-legged permutation of $[8]$:

$$(1, 3, 2, 4, 5, 7, 6, 8)$$

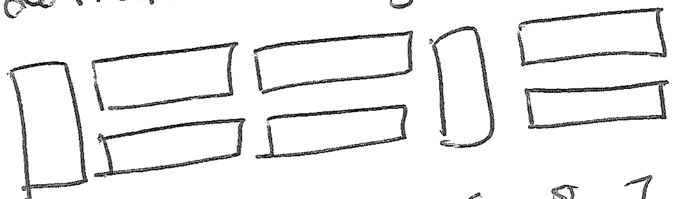
$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{matrix}$$

$\leadsto$



This gives a domino tiling of an 8×2-rectangle.

Conversely:



$\rightsquigarrow (1, 3, 2, 5, 4, 6, 8, 7)$.

Thus, we get a bijection ← needs proof

$\{$short-legged permutations of $[n]\}$

$\to \{$domino tilings of $R_{n,2}\}$.

But Prop. 1.5 yields that the # of latter is f_{n+1}. $\square$

Counting subsets...

- An n-elt. set has 2^n subsets. (HW0 exercise 1(a).)
- An n-elt. set has $\binom{n}{k}$ k-elt. subsets.

Def. A set S of integers is called <u>lacunar</u> if it contains no two consecutive integers (i.e., $\nexists\, i \in \mathbb{Z}$ such that $i \in S$ & $i+1 \in S$).

Ex: $\{1, 5, 7\}$ is lacunar, but $\{1, 5, 6\}$ is not.

Q: (a) How many lacunar subsets does $[n]$ have?

(b) How many k-elt. lacunar subsets — // — ?

(c) What is the largest size of a lacunar subset of $[n]$?