Here, the symbol “\( \equiv \)” means that the left hand side and the right hand side differ only in addends that are 0, and thus are equal. Thus, Thm. 2.18 is proven.

\[ x \in \mathbb{N}. \]

2nd proof of Thm. 2.18 for the case when \( x, y \in \mathbb{N} \):

How many ways \( \sum \) are there to choose an \( n \)-element subset of \( \{1, 2, \ldots, x\} \cup \{-1, -2, \ldots, -y\} \)?

1st answer: \( \binom{x+y}{n} \).

2nd answer: First, decide how many positive elements our subset will have. Let’s say it will have \( k \) positive elements (\( k \in \{0, 1, \ldots, n\} \)). Then, choose these \( k \) positive elements (this gives \( \binom{x}{k} \) choices). Then, choose the remaining \( n-k \) elements (this gives \( \binom{y}{n-k} \) choices). \( \Rightarrow \) The answer is \( \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \).

Now, compare the 2 answers. This proves Thm. 2.18 when
3rd proof for all $x \& y$. See [detnede, first proof of Thm. 2.29 (or 3.29 in future versions)], (Induction on $n$, using $n(y) = y \left(\frac{y-1}{n-1}\right)$ (the "absorption identity").)

(by Prop. 2.2, applied to $y, n, 1$ instead of $n, q, b$)

Cor. **2.19.** Let $n \in \mathbb{N}$. Then, \[
\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.
\]

Proof. Thm. 2.18 (applied to $x=n \& y=n$) yields

\[
\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k} \binom{n}{n-k} = \sum_{k=0}^{n} \binom{n}{k} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k}^2.
\]

(by symmetry)

**Rule.** No formula for \[\sum_{k=0}^{n} \binom{n}{k}^3\] is known. However, there are such formulas for \[\sum_{k=0}^{n} (-1)^k \binom{n}{k}^i\] with
\[ i = 1, 2, 3. \] We've seen the one for \( i = 1 \), and will soon see the one for \( i = 2 \).

Next, I claim that just one trick suffices to make the first two proofs of Thm. 2.18 yield it for ALL \( x, y \in \mathbb{R} \).

This is the "polynomial identity trick":

A reminder on polynomials: Polynomials are NOT functions!

Informally, a polynomial (with rational coefficients, in 1 variable \( X \)) is a "formal expression" of the form
\[ \alpha X^a + \beta X^b + \gamma X^c + \ldots + \omega X^z \] with \( \alpha, \beta, \gamma, \omega \in \mathbb{Q} \) and \( a, b, c, \ldots, z \in \mathbb{N} \).

These expressions obey rules:
- \( \psi X^n + \varphi X^n = (\psi + \varphi) X^n \) ("combining like terms");
- 0 \( X^0 \) can be removed;
- terms can be swapped;
- \( X^0 \) is written as 1; \( X^1 \) is written as \( X \).
subtraction is defined by
\[(\alpha X^a + \beta X^b) - (\gamma X^c + \delta X^d) = \alpha X^a + \beta X^b - (\gamma) X^c + (-\delta) X^d,\]
multiplication is defined by distributivity and \((\alpha X^a)(\beta X^b) = \alpha \beta X^{a+b},\)

the degree of a polynomial is the largest exponent appearing in it with coefficient \(\neq 0\).

Substituting a number (or matrix, or another polynomial) \(x\) into a polynomial \(P = \alpha X^a + \beta X^b + \gamma X^c + \cdots\)
yields \(\alpha x^a + \beta x^b + \gamma x^c + \cdots\). This result is called \(P(x)\).

A number \(x (\in \mathbb{Q} or \in \mathbb{R} or \in \mathbb{C})\) is a root of a polynomial \(P\) if \& only if \(P(x) = 0\).

For a formal definition of polynomials, see [Edtnotes, §1.5] or [Loehr] (most recommended) or most good algebra texts or one of the later chapters of this class.
Thm. 2.20. (the "polynomial identity trick")

(a) A polynomial (with rational coefficients, in 1 variable \(x\)) of degree \( \leq n \) (for a given \( n \in \mathbb{N} \)) has \( \leq n \) roots (in \( \mathbb{Q} \), in \( \mathbb{R} \) or in \( \mathbb{C} \), unless it is the 0 polynomial (i.e., its coefficients are all 0)).

(b) If a polynomial \( p \) has infinitely many roots, then \( p \) is the 0 polynomial.

(c) Let \( p \) and \( q \) be polynomials. If \( p(x) = q(x) \quad \forall x \in \mathbb{N}, \)
then \( p = q \).


Salvaging our 1st proof of Thm. 2.18. Fix \( y \in \mathbb{R} \) and \( n \in \mathbb{N} \). We've already proven...
\[
\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}
\]

for all \(x \in \mathbb{N}\), we want to prove it for all \(x \in \mathbb{R}\).

Define two polynomials \(P\), \(Q\) by

\[
P = \binom{x+y}{n} \quad \text{and} \quad Q = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}.
\]

These are well-defined polynomials, since

\[
P = \binom{x+y}{n} = \frac{(x+y)(x+y-1) \cdots (x+y-n+1)}{n!}
\]

and

\[
Q = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} = \sum_{k=0}^{n} \frac{x(x-1) \cdots (x-k+1)}{k!} \binom{y}{n-k}.
\]

Thus, \(P(x) = Q(x) \quad \forall x \in \mathbb{N}\) (since we have proven \(6)\) for all \(x \in \mathbb{N}\). Hence, Thm. 2.20(c) yields \(P = Q\).

Hence, \(P(x) = Q(x) \quad \forall x \in \mathbb{R}\). In other words, \(7)\) holds for all \(x \in \mathbb{R}\). This completes the 1st proof of Thm. 2.18. \(\square\)
Salvaging our 2nd proof of Thm. 2.18.

Same idea, but now we need to do it twice:

**Step 1:** Fix \( y \in \mathbb{N} \), and \( n \in \mathbb{N} \). Use the same argument as before to prove that (7) holds for all \( x \in \mathbb{R} \).

**Step 2:** Fix \( x \in \mathbb{R} \), and \( n \in \mathbb{N} \). Use an analogous argument (using \( y \) instead of \( x \)) to prove that (7) holds for all \( y \in \mathbb{R} \).

\( \square \)

**Remk.** Thm. 2.20 (c) can be applied to other identities:

- Prop. 2.2 (binomial revision) says
  \[
  \binom{n}{a} \binom{a}{b} = \binom{n}{b} \binom{n-b}{a-b} \quad \forall n, a, b \in \mathbb{R}.
  \]
  We gave a bijective proof for the \( n, a, b \in \mathbb{N} \) case.

Using Thm. 2.20 (c), we can extend this to \( n \in \mathbb{R} \), but \( a, b \) still have to stay in \( \mathbb{N} \), since "(X)" does not make sense.
- Cor. 2.3 said \[ \sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n=0] \forall n \in \mathbb{N}. \]

This cannot be generalized to \( n \in \mathbb{Q} \) or \( n \in \mathbb{R} \), since \( n \) appears as the upper bound of the sum.

- Thm. 2.15 said \[ k^n = \sum_{i=0}^{n} \text{sur}(m,i) \binom{k}{i} \forall k \in \mathbb{N} \forall n \in \mathbb{N}, \]

Thm. 2.20(c) yields that this holds for all \( k \in \mathbb{R} \) and \( m \in \mathbb{N} \).

But not for \( m \in \mathbb{R} \).

- HW 2 Exe 2 said \[ \sum_{i=0}^{n} \binom{n}{i} \binom{n-i}{k-2i} 2^{k-2i} = \binom{2n}{k} \forall n \in \mathbb{N} \forall k \in \mathbb{N}, \]

per se, we cannot generalize this to \( n \in \mathbb{R} \) or \( k \in \mathbb{R} \).

But we can replace \( \sum_{i=0}^{n} \) by \( \sum_{i=0}^{\lfloor k/2 \rfloor} \) and then we can let \( n \in \mathbb{R} \).

- HW 2 Exe 4 said \[ \sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m} \forall n \in \mathbb{N} \forall m \in \mathbb{N}, \]

Thm. 2.20(c) lets us extend this to \( n \in \mathbb{R} \), but not to \( m \in \mathbb{R} \).
Thm. 2.18 is called the (Chu-)Vandermonde identity. It has several "mutated" versions. The following two identities can be used to "mutate" it:

- **Up Neg** (= upper negation = Prop. 1.15):
  \[
  \binom{-n}{k} = (-1)^k \binom{n+k-1}{k} \quad \forall n \in \mathbb{N}, \; k \in \mathbb{Z}
  \]

- **Symm** (= symmetry = Thm. 1.17):
  \[
  \binom{n}{k} = \binom{n}{n-k} \quad \forall n \in \mathbb{N}, \; k \in \mathbb{Z}
  \]

Here is one example of "mutated" Vandermonde identity: Prop. 2.21 ("upside-down Vandermonde"). Let \( n, x, y \in \mathbb{N} \).

Then,
\[
\binom{n+1}{x+y+1} = \sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y}
\]

Rmk. This cannot be generalized using Thm. 2.20 (c), since the RHS is not a polynomial function in any of \( n, x, y \). And indeed, the equality is false for \( n=6, x=-1, y=3 \).
1st proof of Prop. 2.21. (from [dotnotes, 2.2.3 ?] )

If \( n < x + y \), then both sides are 0

(ind indeed, any each addend on the RHS is 0, because if \( k \in \{0, 1, \ldots, n\} \) there is such that

\[
\binom{k}{n-k} \binom{n-k}{y} = 0, \quad \text{then} \quad \binom{k}{x} = 0 \Rightarrow k > x
\]

and \( \binom{n-k}{y} = 0 \Rightarrow n-k \geq y \)

and thus \( n = \frac{k}{2} + \frac{n-k}{2} \geq x + y \) \( \forall \).

So we WLOG assume \( n \geq x + y \). Thus,

\[
\sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y} = 0 = \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{y}
\]

\[\xrightarrow{\text{Symm}}\]

\[
\sum_{k=x}^{n} \binom{k}{n-k} \sum_{k-x}^{n-k} \binom{n-k}{n-k-y}
\]

\[\xrightarrow{\text{UpNeg}}\]

\[
(-1)^{k-x} \binom{k-x}{-x-1} (-k+(k-x)-1) \left( \frac{-y-1}{n-k-y} \right)
\]

\[\xrightarrow{\text{UpNeg}}\]

\[
(-1)^{n-k-y} \binom{n-k}{y} \binom{n-k-y}{n-k-y}
\]
\[
\sum_{k=x}^{n-y} (-1)^{k-x} \binom{-x-1}{k-x} (-1)^{n-k-y} \binom{-y-1}{n-k-y}
\]

\[
\sum_{k=x}^{n-y} (-1)^{n-x-y} (-x-1) \binom{-x-1}{k-x} (-y-1) \binom{-y-1}{n-k-y}
\]

\[
(-1)^{n-x-y} \sum_{k=x}^{n-y} (-x-1) \binom{-x-1}{k-x} (-y-1) \binom{-y-1}{n-k-y}
\]

\[
\sum_{k=0}^{n-x-y} (-x-1) \binom{-x-1}{k} (-y-1) \binom{-y-1}{n-x-y-k}
\]

\[
\binom{-x-1}{n-x-y} \binom{-y-1}{n-x-y}
\]

(by Thm. 2.18, applied to 
\(n-x-y\), \(-x-1\) and \(-y-1\)
instead of \(n\), \(x\) and \(y\))
\[\begin{align*}
&= (-1)^{n-x-y} \binom{n-x-y}{n-x-y} \\
&\uparrow \text{Nes} \downarrow \\
&\binom{n-x-y}{x-y} \binom{n-x-y}{n-x-y} \frac{(-1)^{n-x-y}}{((-1)^{n-x-y} + (n-x-y) - 1)} \\
&= \binom{n+1}{n-x-y} \frac{n+1}{n+1-(n-x-y)} = \frac{n+1}{x+y+1}.
\end{align*}\]

2nd proof of Prop. 2.21. Double-count the number of \((x+y+1)\)-elt subsets of \([n+1]\):

1st answer: \(\binom{n+1}{x+y+1}\),

2nd answer: Construct such a subset as follows:

- Choose the \((x+1)\)-th smallest element of this subset.
- Call it \(k+1\). Thus, \(k \in \{0, 1, \ldots, n\}\).
• Choose the \( x \) smallest elements of this subset. There are \( \binom{x}{x} \) options for this (since they need to be chosen from the \( k \)-elt. set \( \{1, 2, \ldots, k\} \)).

• Choose the remaining \( y \) elements of this subset. There are \( \binom{n-k}{y} \) options for this (why?).

\( \Rightarrow \) The answer is \( \sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y} \).

Compare the 2 answers \( \Rightarrow \binom{n+1}{x+y+1} = \sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y} \). \( \square \)

2.5. Counting subsets again

Recall Thm. 1.19: If \( S \) is an \( n \)-elt. set and \( k \in \mathbb{Z} \), then \( \binom{n}{k} = \# \text{ of } k \text{-elt. subsets of } S \).

We proved this by induction. We'll now re-prove this by "multijection" procedure.
**Def.** Let $S$ be a set, let $k \in \mathbb{N}$.

A $k$-tuple $(s_1, s_2, \ldots, s_k) \in S^k$ is called *injective* if $s_1, s_2, \ldots, s_k$ are distinct.

Let $S^k_{\text{dist}}$ be the set of all injective $k$-tuples in $S^k$.

**Ex:** $(3, 2, 5)$ is injective, but $(4, 2, 4)$ is not.

Note that injective $k$-tuples are also known as "$k$-samples without replacement".

**Prop. 2.22.** Let $S$ be a set, let $k \in \mathbb{N}$. Then, $|S^k_{\text{dist}}| = |S|^k$.

**Proof.** The injective $k$-tuples are in 1-to-1 correspondence with the injective maps from $[k]$ to $S$.

Rigorously: There is a bijection

$\{\text{injective maps from } [k] \to S \} \rightarrow S^k_{\text{dist}},$

$f \mapsto (f(1), f(2), \ldots, f(k))$. 
Thus,
\[ |S^{k}_{\text{dist}}| = |\{\text{inj. maps from } [k] \text{ to } S\}| = (\# \text{ of inj. maps from } [k] \text{ to } S) = |S|^k \]
(by Thm. 2.5, applied to \( A = [k], B = S, m = k, n = |S| \)).

2nd proof of Thm. 1.19. WLOG assume \( k \geq 0 \) (else, we just claim \( 0 = 0 \)). Then, \( |S| = n \), so Prop. 2.22 yields
\[ |S^{k}_{\text{dist}}| = |S|^k = n^k \]
But
\[ |S^{k}_{\text{dist}}| = (\# \text{ of injective } k\text{-tuples } s \in S^k) \]
\[ = \sum_{\substack{W \subseteq S; \\text{\#}W = k}} (\# \text{ of injective } k\text{-tuples } s \in W^k \text{ such that the set of entries of } s \text{ is } W) \]
\[ = (\# \text{ of injective } k\text{-tuples } s \in W^k) \]
\[ \uparrow \text{by observation 1 (below)} \]