Ex. 2.7. Why are sums like \( \sum_{i=2}^{i=4} i^2 \) or \( \sum_{i \in \{2,4,6\}} i^2 \) well-defined?

Generally, why is \( \sum_{s \in S} a_s \), where \( S \) is a finite set and \( (a_s)_{s \in S} \) is a family of numbers, well-defined?

Explanation: A number \( a \) is an element of \( A \), where \( A \) is either \( \mathbb{N} \) or \( \mathbb{Z} \) or \( \mathbb{Q} \) or \( \mathbb{R} \) or \( \mathbb{C} \).

- A family \( (a_s)_{s \in S} \) of numbers (indexed by a set \( S \)) is a choice of a number \( a_s \) for each \( s \in S \).
- A family \( (a_s)_{s \in S} \) of numbers (indexed by \( \{2,4,6\} \)) is a choice of a number \( a_2 \), a number \( a_4 \), & a number \( a_6 \).
For example,

\[
\sum_{s \in \{ -2, -1, 0, 1, 2 \}} s^3 \quad \text{equal to} \quad \left( \left( ( -2 )^3 + ( -1 )^3 \right) + 0^3 \right) + 1^3 + 2^3
\]

or equal to \( \left( ( -2 )^3 + 2^3 \right) + ( -1 )^3 \right) + 1^3 + 0^3 \quad ? \)

Why are these two sums equal?

Idea: To define \( \sum_{s \in S} q_s \) (for a finite set \( S \) & a family \( (q_s)_{s \in S} \) of numbers), use recursion:

- if \( S = \emptyset \), set \( \sum_{s \in S} q_s = 0 \);
- if \( S \neq \emptyset \), then pick \( t \in S \), and set \( \sum_{s \in S} q_s = a_t + \sum_{s \in S \setminus t} q_s \).

But why is this well-defined, i.e. why doesn't choice of \( t \) matter?

Thm. 2.8 (General commutativity). The above definition is well-defined; i.e., all choices of \( t \) lead to the same result.
To make this more rigorous, define a set of numbers

\[ \text{Sums}(a_s) \] for any finite set \( S \) and any family \( (a_s)_{s \in S} \) of numbers

as follows:

1. If \( S = \emptyset \), set \( \text{Sums}(a_s) = \{0\} \).
2. If \( S \neq \emptyset \), then \( \text{Sums}(a_s) = \{ \sum_{t \in S} a_t + a_0 \} \).

Then, Thm. 2.8 becomes:

Thm. 2.8': For any set \( S \) and any family \( (a_s)_{s \in S} \) of numbers,

\[ \text{Sums}(a_s) \] is a 1-element set.

Proof of Thm. 2.8': "Induction on \( |S| \):"
For each $n \in \mathbb{N}$, we will let $\#(n)$ be the following statement:

$\left( \text{for any } n\text{-element set } S \text{ & any family } (a_s)_{s \in S} \right)$

$\text{Sums}(a_s) \text{ is a 1-element set } \text{ for } s \in S$.

Then, $\#(0)$ clearly holds (because if $n=0$, then $S=\emptyset$, so $\text{Sums}(a_\emptyset) = \{0\}$).

Now, we need to prove: if $\#(n)$, then $\#(n+1)$.

Now, let $S$ be an $(n+1)$-element set. Let $(a_s)_{s \in S}$ be a family of numbers. We must prove that $\text{Sums}(a_s)$ is a 1-element set.

Clearly, $|S|=n+1>0$, so $S \neq \emptyset$, so $\exists p \in S$. Moreover, by $\#(n)$, the set $\text{Sums}(a_p)$ is a 1-element set. Let $w_p$ be its one element.
Then, $a_p + w_p \in \text{Sums} \left( a_s \right), \quad s \in S$

So $\text{Sums} \left( a_s \right)$ has $\geq 1$ element.

Now, let us prove that it has $\leq 1$ element.

Let $a_q + w_q$ and $a_r + w_r$ be two of its elements.

Let $a_q + w_q$ and $a_r + w_r$ be two of its elements,

Let $a_q + w_q$ and $a_r + w_r$ be two of its elements,

(with $q \in S$, $w_q \in \text{Sums} \left( a_s \right)$, $r \in S$, $w_r \in \text{Sums} \left( a_s \right)$).

We want to prove: $a_q + w_q = a_r + w_r$.

If $q = r$, then $w_q = w_r$ because $\delta(n)$ shows that

If $q = r$, then $w_q = w_r$ because $\delta(n)$ shows that

$\text{Sums} \left( a_s \right)$ is a 1-element set. So $a_q + w_q = a_r + w_r$.

$\text{Sums} \left( a_s \right)$ is a 1-element set. So $a_q + w_q = a_r + w_r$.

In this case,

In this case,

If $q \neq r$, then pick any $w_q, w_r \in \text{Sums} \left( a_s \right)$.

If $q \neq r$, then pick any $w_q, w_r \in \text{Sums} \left( a_s \right)$.

Then, $a_q + w_q \in \text{Sums} \left( a_s \right)$, and thus

Then, $a_q + w_q \in \text{Sums} \left( a_s \right)$, and thus

$w_q + w_q = a_r + w_q$, since $\text{Sums} \left( a_s \right)$ is a 1-element set.
Similarly, \( \omega_r = \omega_q, \). 

Thus, \( \omega_p = \omega_q + (\omega_q, \tau) \) 

\[ \text{associativity} \quad (\sigma_q + \sigma_r) + \omega_q, \tau \]

\[ \text{commutativity} \quad (\sigma_q + \sigma_r) + \omega_q, \tau \]

\[ \text{associativity} \quad \sigma_r + (\sigma_q + \omega_q, \tau) = \sigma_r + \omega_r. \]

In either case, we get \( \sigma_q + \omega_q = \sigma_r + \omega_r. \)

Thus, \( \sigma_{p(x)} \) has \( \leq 1 \) element.

\[ \text{So, by ind. princ., 2.4, we conclude} \]

Thus, \( \sigma(n+1) \) holds. So, by ind. princ., 2.4, we conclude that \( \sigma(n) \) holds \( \forall n \). In other words, Thm. 2.8 is proven. \( \square \)
See, [notes, Ch. 1] for lots of formulas for summation signs. One example:

**Thm. 2.9 (Splitting a sum).** Let \( S \) be a finite set. Let assume that \((S_1, \ldots, S_k)\) be a decomposition of \( S \) (i.e., \( S_1, S_2, \ldots, S_k \) are subsets of \( S \) such that each element of \( S \) lies in exactly one of them).

Let \((a_s)_{s \in S}\) be a family of numbers.

Then,

\[
\sum_{s \in S} a_s = \sum_{s \in S_1} a_s + \sum_{s \in S_2} a_s + \cdots + \sum_{s \in S_k} a_s.
\]

**Proof idea.** Induction on \(| S | \).

In the induction step, pick any \( t \in S \), and pluck out \( a_t \) from both sides.

\( \square \)
2.2. Shifted Induction

**Induction principle 2.10.** Fix \( g \in \mathbb{Z} \). Set \( \mathbb{Z}_{\geq g} = \{g, g+1, g+2, \ldots \} \).

For each \( n \in \mathbb{Z}_{\geq g} \), let \( B(n) \) be a logical statement.

Assume: \( B(g) \) holds.

\[ \forall n \in \mathbb{Z}_{\geq g}, \text{ if } B(n) \text{ holds, then } B(n+1) \text{ holds.} \]

Then, \( B(n) \) holds \( \forall n \in \mathbb{Z}_{\geq g} \).

**Proof.** Apply principle 2.1 to \( h(n) := B(n+g) \).

**Example 2.11.** Recall the ToHn.

**Prop 2.12.** \( \forall n \geq 1 \), \( \forall k \geq 2^n - 1 \), we can solve the \( n \)-disk ToHn in \( k \) steps.

**Proof.** Let \( B(n) = (\forall k \geq 2^n - 1, \text{ we can solve the } \ n \text{-disk ToHn in } k \text{ steps}). \)

We must prove this \( \forall n \geq 1 \).

\( B(1) \) is true (just move the disk around between pegs \( 1,2 \), then send it to peg 3 at the last step).
Now, let $n \in \mathbb{Z}_{\geq 1}$ and assume $B(n)$ holds.

Why does $B(n+1)$ hold?

Let $k \geq 2^{n+1} - 1$. We must show how to solve the $(n+1)$-disk ToH in $k$ steps.

Meanwhile, $B(n)$ holds, so that

$$(1) \quad \forall \ l \geq 2^n - 1, \text{ we can solve the } n\text{-disk ToH in } l \text{ steps.}$$

Now,

- first, move the disks $1, 2, \ldots, n$ to peg 2 in $2^{n+1} - 1$ steps.
  (This can be done by (1), applied to $l = 2^n - 1$.)

- then, move disk $n+1$ to peg 3 (in 1 step).

- then, move disks $1, 2, \ldots, n$ to peg 3 in $k - 2^n$ steps.
  (This can be done by (1), applied to $l = k - 2^n$, because $k - 2^n \geq 2^n - 1$ (since $k \geq 2^{n+1} - 1$).

So $(n+1)$-disk ToH is solved in $k$ steps, thus, $B(n+1)$ holds. $\square$
2.3. Limited/bounded induction

Induction principle 2.13. Fix $p, q \in \mathbb{Z}$ with $p \leq q$.

For each $n \in \{p, p+1, \ldots, q\}$, let $C(n)$ be a logical statement.

Assume:

- $C(p)$ holds,
- $\forall n \in \{p, p+1, \ldots, q-1\}$, if $C(n)$ holds, then $C(n+1)$ holds.

Then $C(n)$ holds $\forall n \in \{p, p+1, \ldots, q\}$.

Proof. Apply principle 2.10 to $g = p$ and $B(n) = (\text{if } n \leq q, \text{then } C(n))$.

Example 2.13. 30 socks are hanging from a clothesline:

- 15 white socks (W) & 15 black socks (B),
- Show that you can find 10 consecutive socks, among which 5 are W and 5 are B.

(Ex: $\overbrace{W W B W W B B B B B}^{5 \text{ white}} \overbrace{B W W B W B W B B W W}^{5 \text{ black}}$)
Idea: Proof by contradiction. (So assume \( \forall \) such 10 socks.)

For each \( i \in [21] \), let

\[
b_i = (\# \text{ of black socks among the socks } i, i+1, \ldots, i+9) - 5.
\]

By assumption, \( b_i \neq 0 \ \forall i \).

However, \( b_1 + b_{12} + b_{21} = (\# \text{ of all black socks}) - 15 = 0 \).

Now, \text{WLOG} assume \( b_1 > 0 \) (otherwise, \& flip all colors).

Furthermore, for every \( i \in [20] \),

\[
b_{i+1} - b_i = \begin{cases} 
1 & \text{if sock } i+10 \text{ is black but sock } i \text{ is white}, \\
-1 & \text{white} \\
0 & \text{black},
\end{cases}
\]

\( \implies \) \( |b_{i+1} - b_i| \leq 1 \).

So we have a sequence \( (b_1, b_2, \ldots, b_{21}) \) of integers such that

\begin{itemize}
  \item \( b_i \neq 0 \ \forall i \),
  \item \( b_1 > 0 \),
  \item \( |b_{i+1} - b_i| \leq 1 \),
\end{itemize}

Claim: \( b_i > 0 \ \forall i \).
This follows from:

**Lem 2.14** (Discrete IVT / "Discrete continuity").

Let \((b_1, b_2, \ldots, b_n)\) be a sequence of integers such that

- \(b_i \neq 0 \quad \forall i,\)
- \(b_i > 0,\)
- \(|b_{i+1} - b_i| \leq 1 \quad \forall i \in \mathbb{Z} - 1.\)

Then \(b_i > 0 \quad \forall i.\)

**Proof.** For each \(n \in \mathbb{Z} - 1\), let \(C(n)\) be the statement \((b_n > 0).\)

Use Induction Principle 2.13 to prove \(C(n)\) holds \(\forall n.\)

\(C(1)\) holds (since \(b_1 > 0),\)

Now let \(n \in \mathbb{Z} - 1\). Assume \(C(n)\) holds.

We must prove \(C(n+1)\) holds.

We have \(b_n > 0\) (since \(C(n)\) holds) \(\Rightarrow b_{n+1} \geq 1\) (since \(b_n \in \mathbb{Z}\)).

Now assumption yields \(|b_{n+1} - b_n| \leq 1\), so \(b_{n+1} \geq b_n - 1 \geq 1 - 1 = 0.\)

But assumption yields \(b_{n+1} \neq 0\). Hence \(b_{n+1} > 0.\) Thus, \(C(n+1)\) holds.

So Principle 2.13 yields \(C(n) \forall n.\) Hence Lem. 2.14 is proven. \(\square\)
Back to our example, $b_i > 0 \ \forall i$.

So $b_1 + b_{11} + b_{21} > 0 + 0 + 0 = 0$, contradicting $b_1 + b_{11} + b_{21} = 0$.

So we have proven 10 consecutive socks with 5 W & 5 B.

Variants: What if 40 socks (20 W & 20 B), and we want 10 consec. (5 W & 5 B)? Yes.

38 socks (15 W & 19 B), $\quad$ 10 $\quad$ ? Yes.

[Proof: $b_1 + b_{11} + b_{21} + b_{29} \in \{ -1, 0, 1 \}$.

But $b_i > 0$ so $b_i > 1$ so $b_1 + b_{11} + b_{21} + b_{29}$

$\quad \quad > 1 + 1 + 1 + 1 = 4$. \( \neq \)

8 socks (4W & 4B), $\quad$ 6 consec. (3 W & 3 B)? No.

2.4. Strong induction

Induction principle 2.16. Let \( g \in \mathbb{Z} \).

Let \( \mathcal{A}(n) \) be a statement for all \( n \in \mathbb{Z} \geq g \).

Assume that:

- \( \forall n \in \mathbb{Z} \geq g \), if \((\mathcal{A}(m) \text{ holds } \forall m < n)\),
  
then \( \mathcal{A}(n) \) holds.

Then, \( \mathcal{A}(n) \) holds \( \forall n \in \mathbb{Z} \geq g \).

Remark: There is no "explicit" induction base.

In other words, we don't need to assume \( \mathcal{A}(g) \).

Instead, \( \mathcal{A}(g) \) follows from our assumption
"if \((\mathcal{A}(m) \text{ holds } \forall m < n)\), then \( \mathcal{A}(n) \) holds",
because this assumption, applied to \( n = g \), says
"if \((\mathcal{A}(m) \text{ holds } \forall m < g)\), then \( \mathcal{A}(g) \) holds",

This assumes nothing

which is the same as saying "\( \mathcal{A}(g) \) holds".
Thus, a strong induction needs no induction base. Often, however, the proof of the induction step has to distinguish between cases $n=g$ & $n>g$, and then the first case is called an induction base.

For example, see [LeLeMe, 85.2].