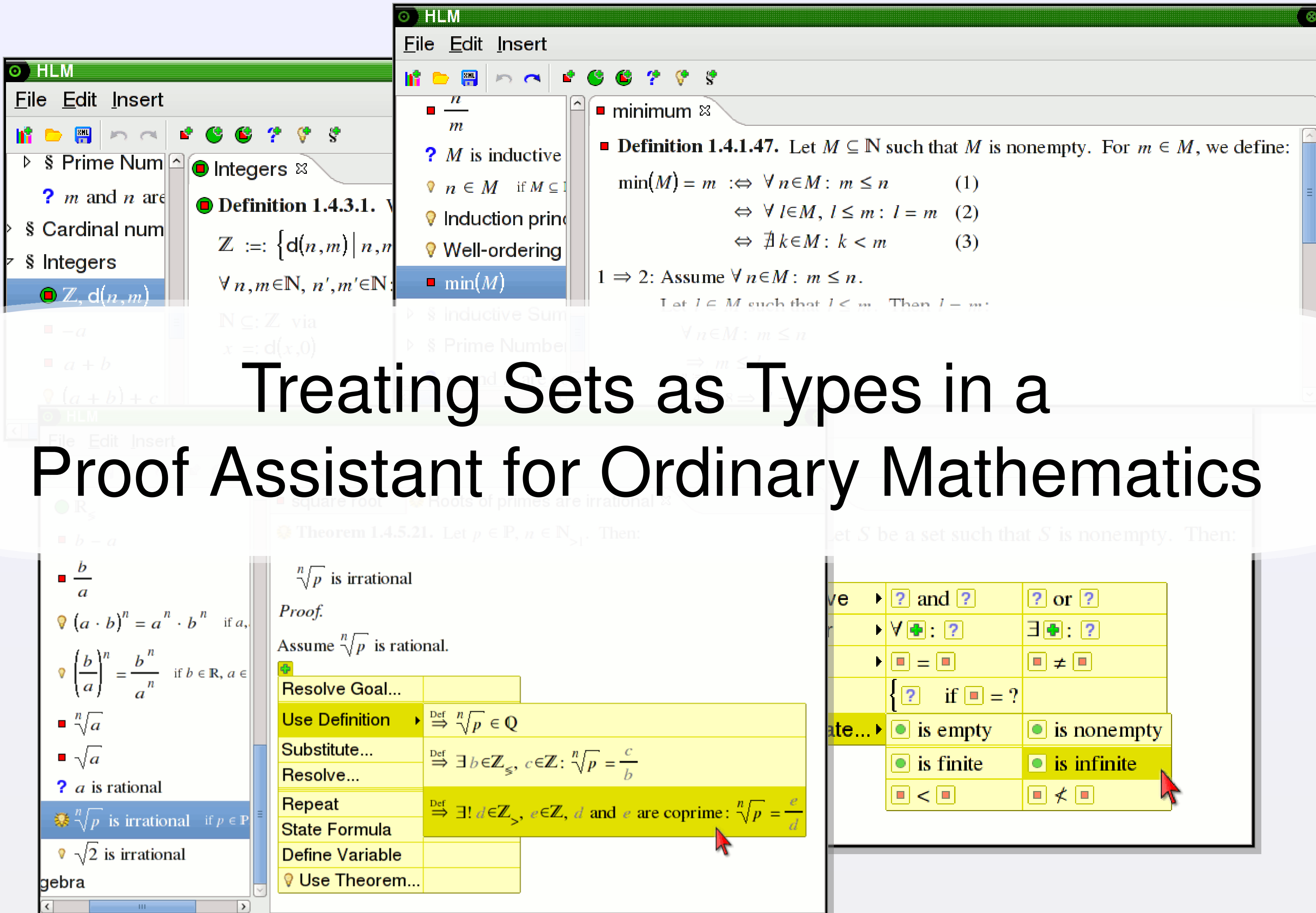


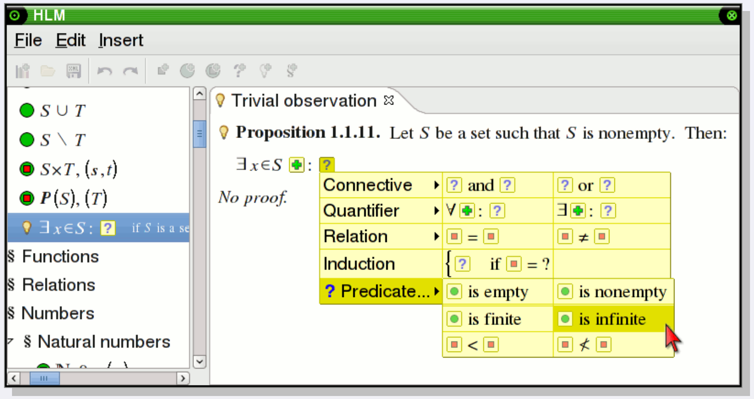
Treating Sets as Types in a Proof Assistant for Ordinary Mathematics

Sebastian Reichelt

Input Methods

Text

GUI



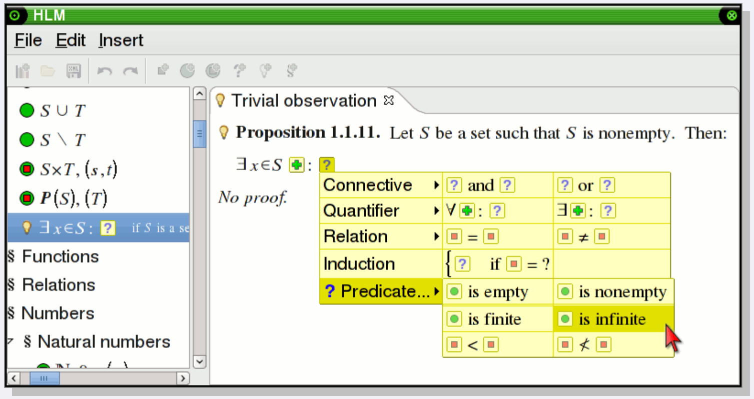
Input Methods

Text

Syntax
Naming
Symbol overloading

GUI

Rendering
Selection



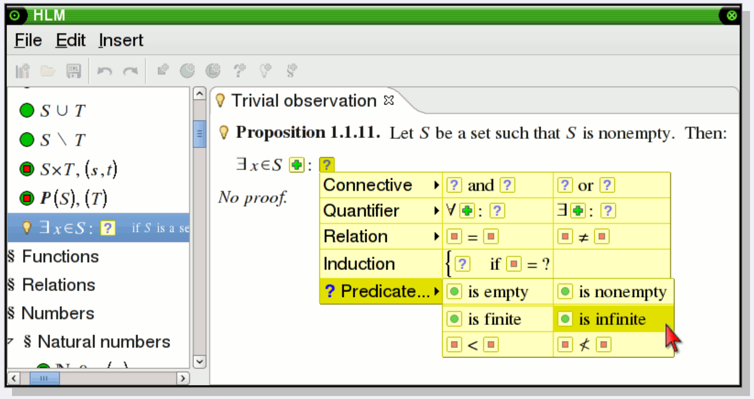
Input Methods

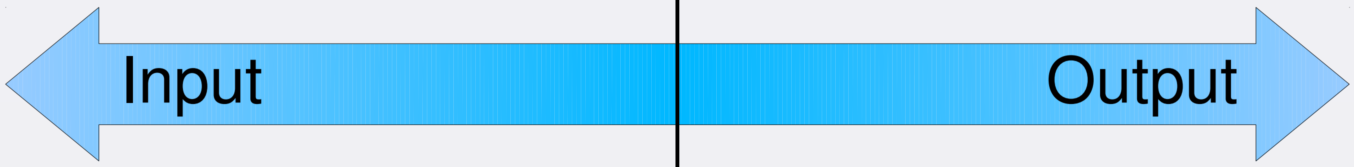
Text

Syntax
Naming
Symbol overloading

GUI

Rendering
Selection





Input Methods

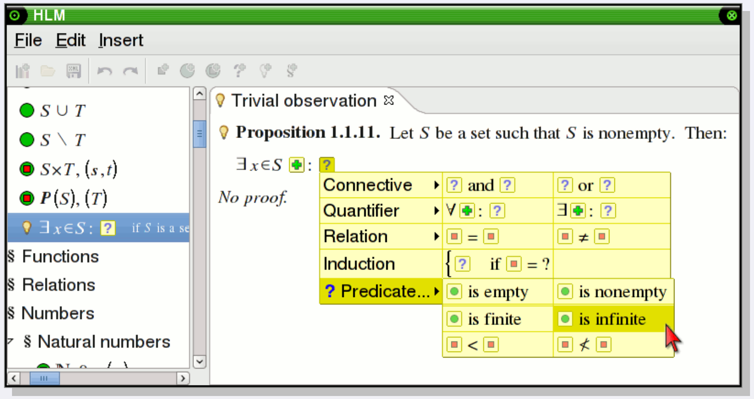
Text

Syntax
Naming
Symbol overloading

Set theory with soft types (→ Mizar)

GUI

Rendering
Selection



Input ↔ Output

Input Methods

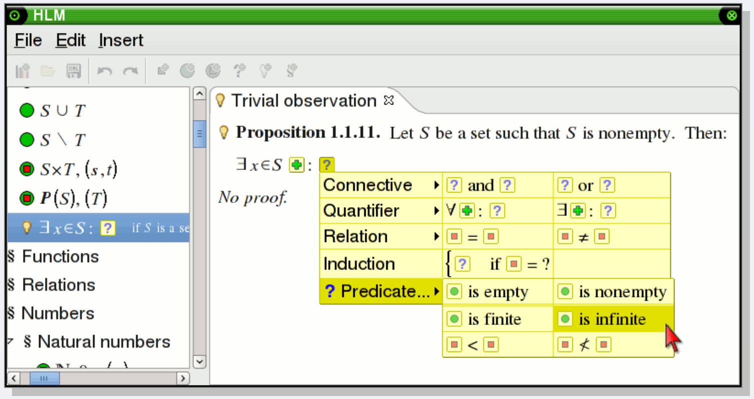
Text

Syntax
Naming
Symbol overloading

Set theory with soft types (→ Mizar)

GUI

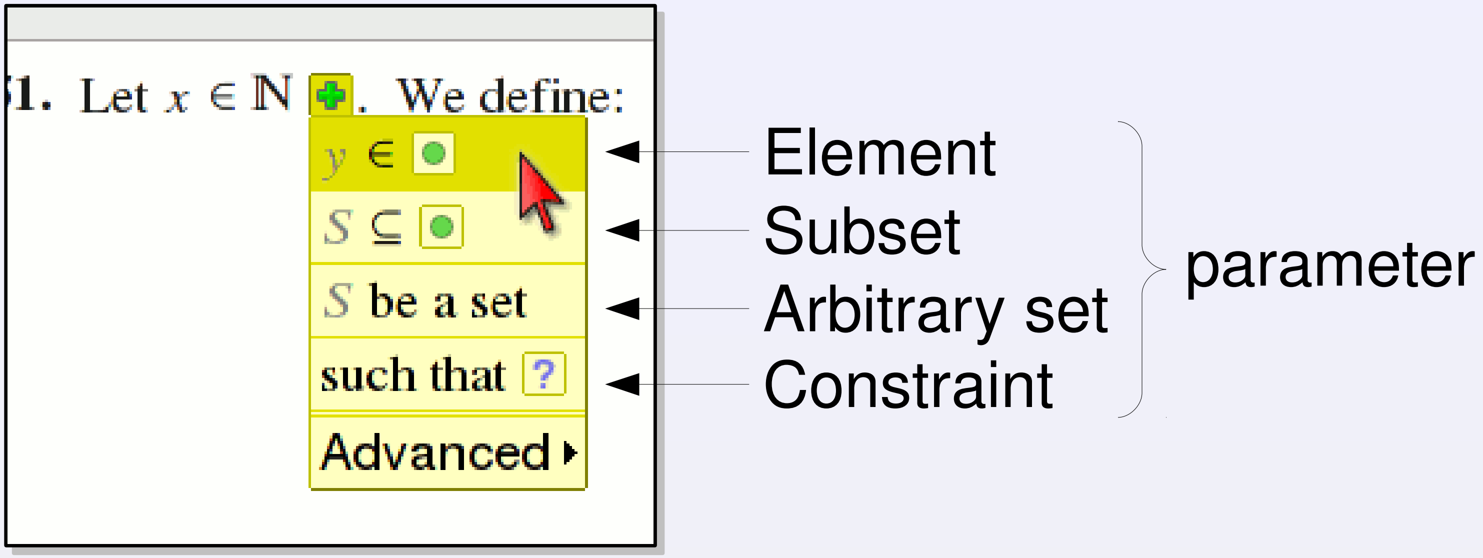
Rendering — *Set theory*
Selection — *Type theory*



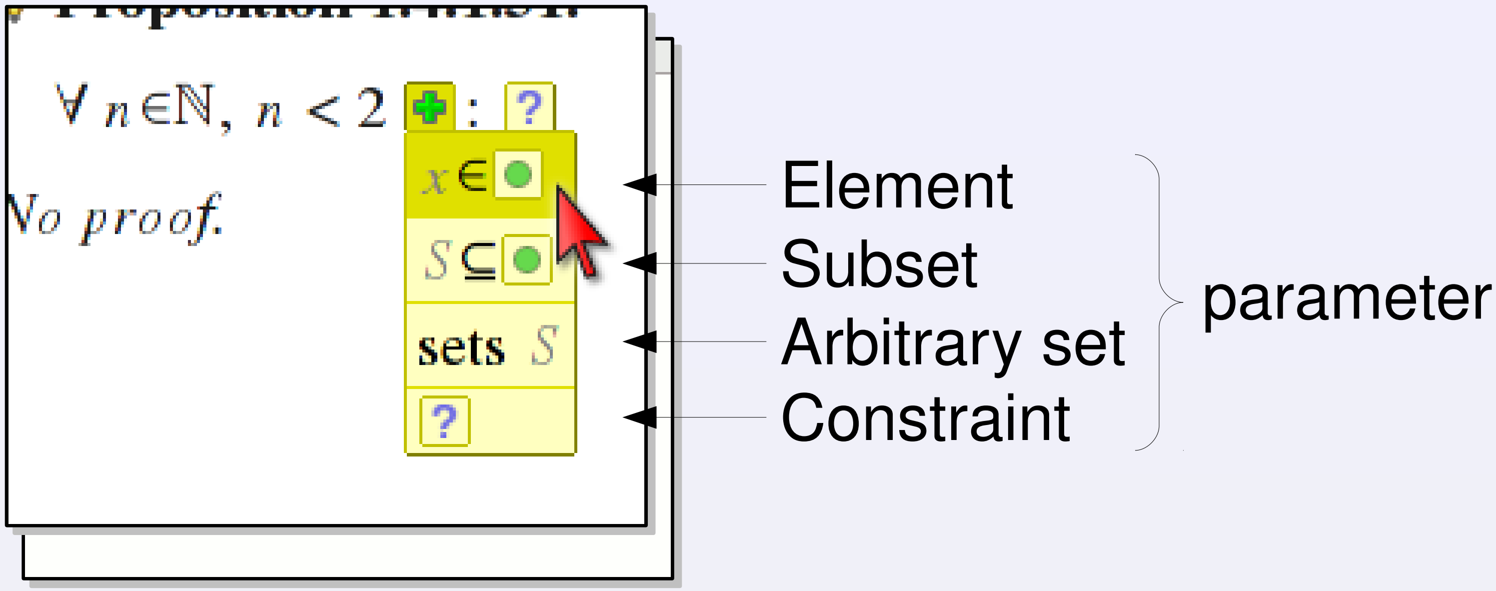
"Theoretically, it seems to be perfectly legitimate to ask whether the union of the cosine function and the number *e* contains a finite geometry" – de Bruijn

Demo

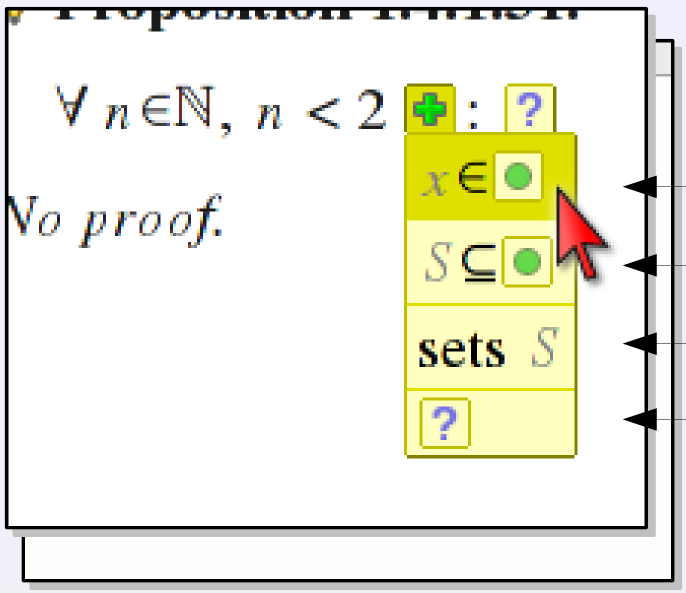
Parameter Lists



Parameter Lists



Parameter Lists

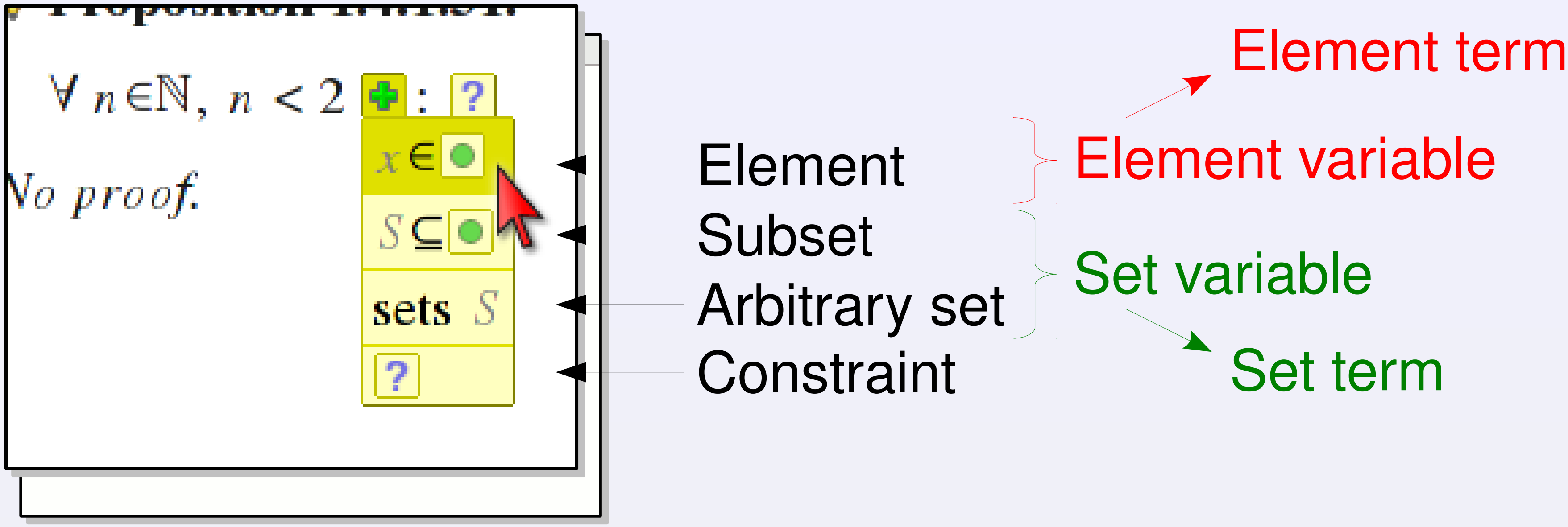


- Element
- Subset
- Arbitrary set
- Constraint

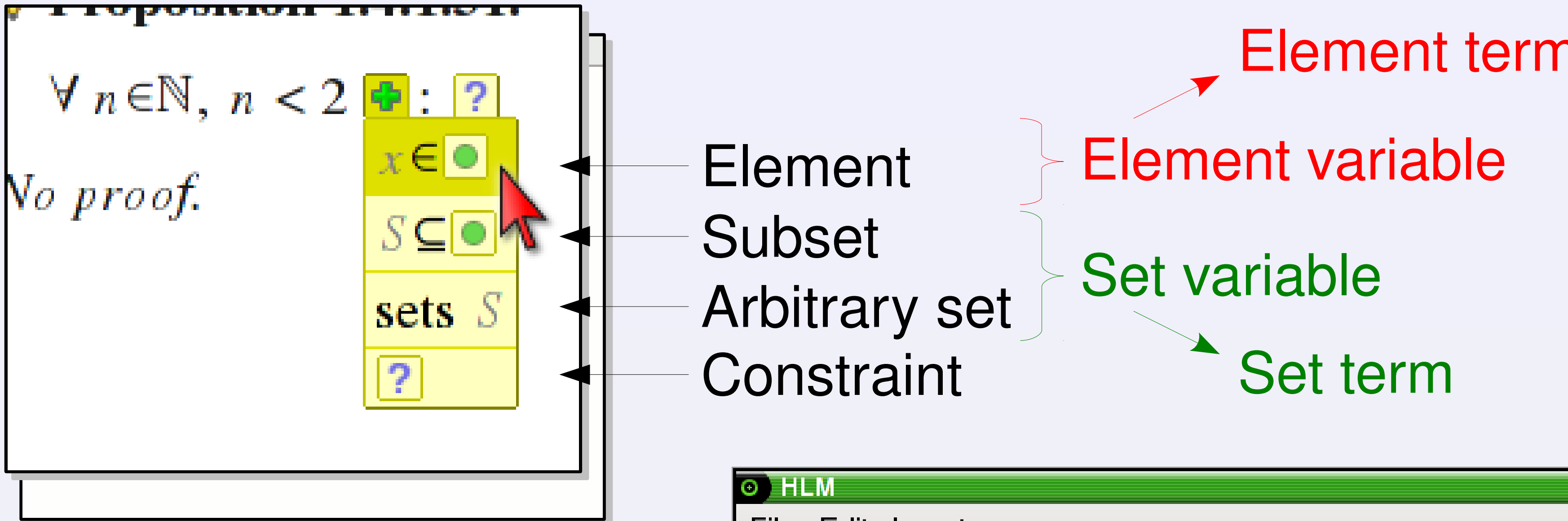
Element variable

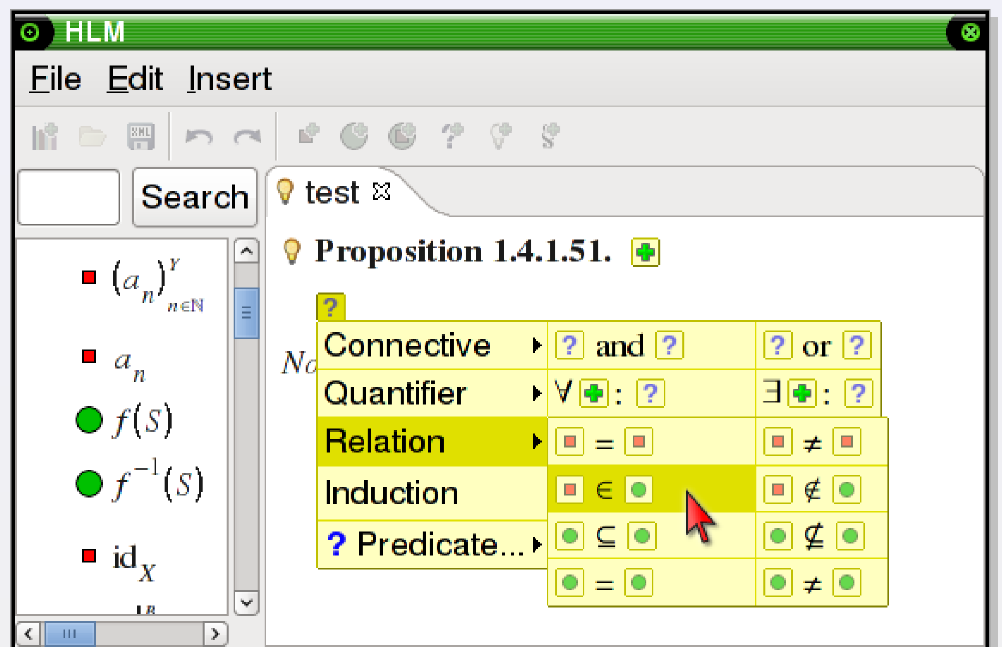
Set variable

Parameter Lists



Parameter Lists





Types

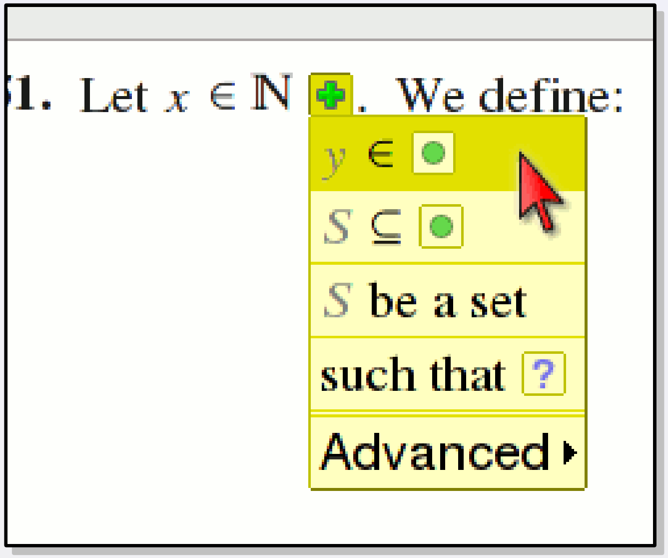
Informal principle:

"x=y" is valid iff x and y are syntactically known to be members of the same set.

Types

Informal principle:

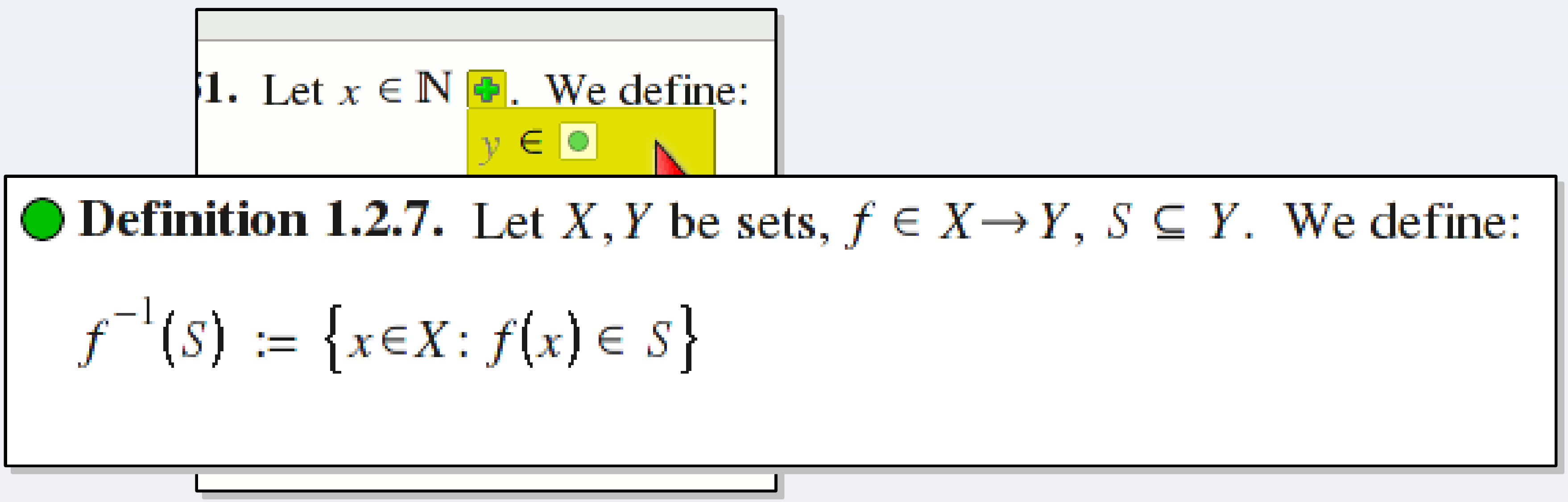
"$x=y$" is valid iff x and y are syntactically known to be members of the same set.



Types

Informal principle:

> "*x*=*y*" is valid iff *x* and *y* are syntactically known to be members of the same set.



Types

Informal principle:

"x=y" is valid iff x and y are syntactically known to be members of the same set.

1. Let $x \in \mathbb{N}$. We define:

$y \in$

Definition 1.2.7. Let X, Y be sets, $f \in X \to Y$, $S \subseteq Y$. We define:

$$f^{-1}(S) := \{x \in X : f(x) \in S\}$$

Y Y

Types

Informal principle:

> "x=y" is valid iff x and y are syntactically known to be members of the same set.

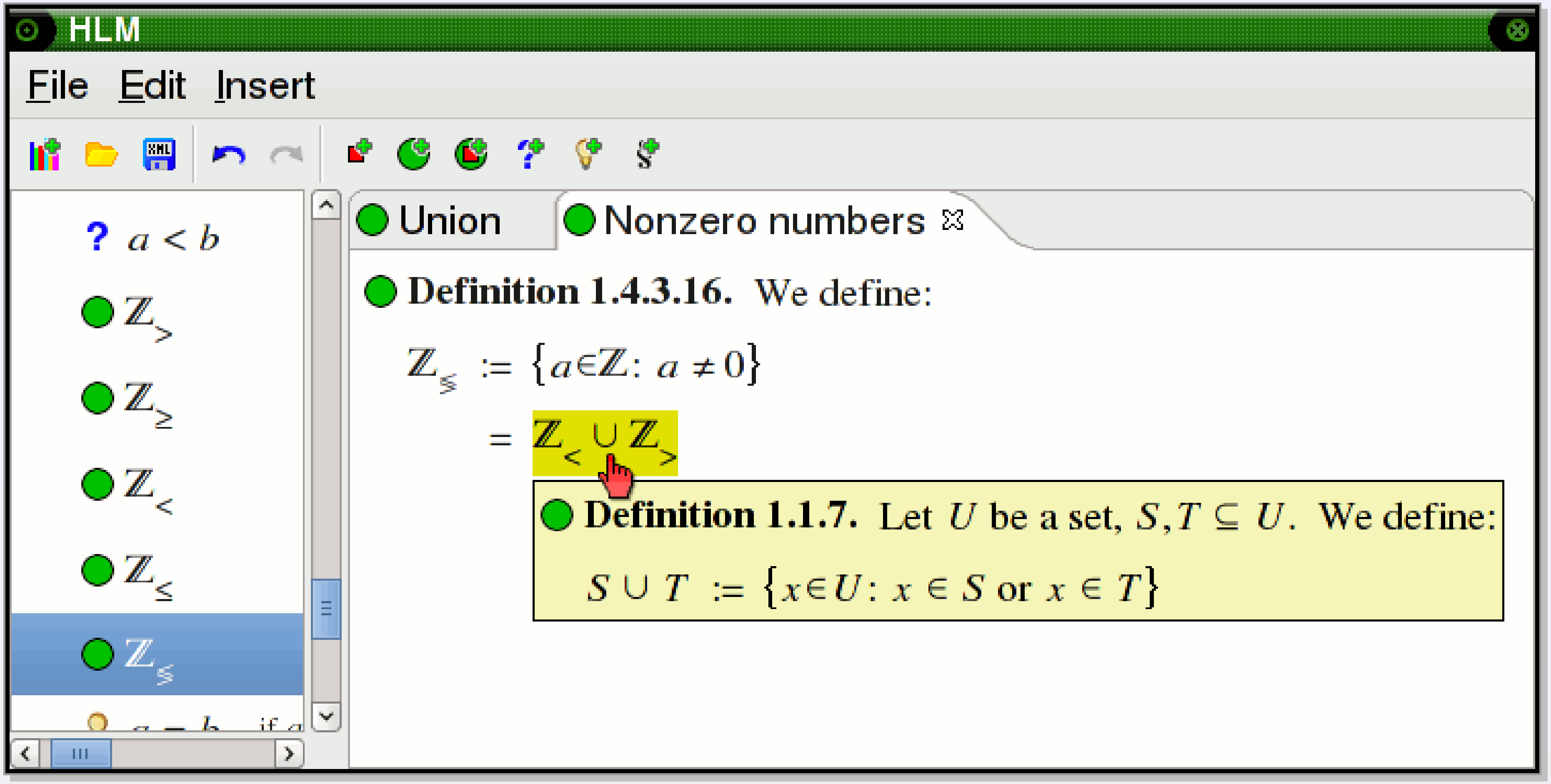
1. Let $x \in \mathbb{N}$. We define:

$y \in$

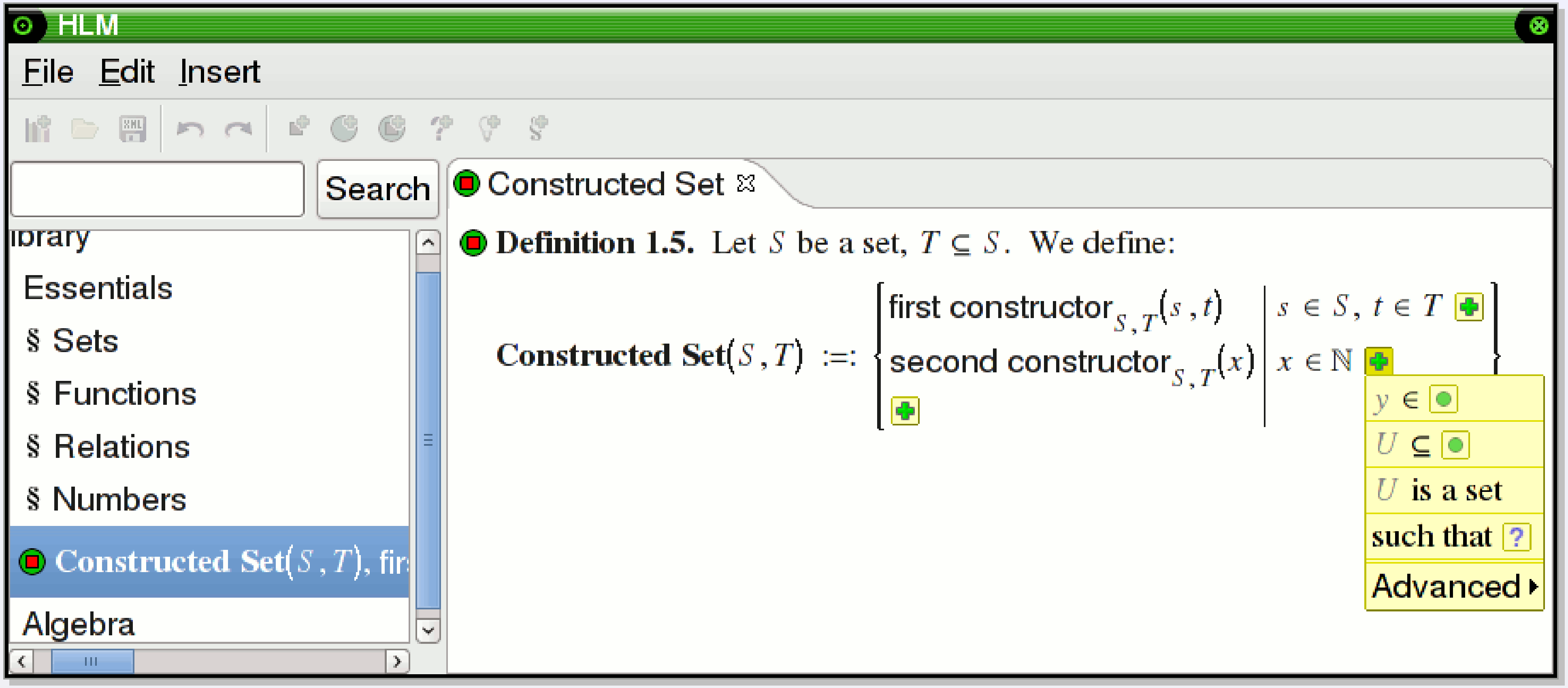
Definition 1.2.7. Let X, Y be sets, $f \in X \to Y$, $S \subseteq Y$. We define:

$$f^{-1}(S) := \underbrace{\{x \in X : f(x) \in S\}}_{X}$$

Set Operations



Set Construction



Set Construction

Definition 1.1.9. Let S, T be sets. We define:

$$\textbf{Cartesian product}(S, T) :=: \left\{ \mathsf{pair}_{S,T}(s, t) \;\middle|\; s \in S,\ t \in T \right\}$$

Set Construction

Definition 1.1.9. Let S, T be sets. We define:

$$S \times T := \left\{ (s, t) \,\middle|\, s \in S,\ t \in T \right\}$$

Set Construction

Definition 1.1.9. Let S, T be sets. We define:

S

Definition 1.4.1.1. We define:

$$\mathbb{N} := \left\{ \begin{matrix} 0 \\ \mathsf{s}(n) \end{matrix} \middle| \; n \in \mathbb{N} \right\}$$

Set Construction

Definition 1.1.9. Let S, T be sets. We define:

S

Definition 1.4.1.1. We define:

$\mathbb{N}$

Definition 1.1.10. Let S be a set. We define:

$$\boldsymbol{P}(S) := \left\{ (T) \,\middle|\, T \subseteq S \right\}$$

Set Construction

Definition 1.1.9. Let S, T be sets. We define:

S

Definition 1.4.1.1. We define:

$\mathbb{N}$

Definition 1.1.10. Let S be a set. We define:

$$P(S) \;:=:\; \left\{ (T) \,\middle|\, T \subseteq S \right\}$$

Definition 1.1.11. We define:

$$\mathbf{Sets} \;:=:\; \left\{ \mathsf{set}(S) \,\middle|\, S \text{ is a set} \right\}$$

[redacted] $\mathsf{set}(S) = \mathsf{set}(S')$ [redacted]

?

Set Construction

Definition 1.1.9. Let S, T be sets. We define:

Definition 1.4.1.1. We define:

Definition 1.1.10. Let S be a set. We define:

$$P(S) \;:=:\; \left\{ (T) \,\middle|\, T \subseteq S \right\}$$

Definition 1.1.11. We define:

$$\mathbf{Sets} \;:=:\; \left\{ \mathrm{set}(S) \,\middle|\, S \text{ is a set} \right\}$$

$\forall$ sets S, S': $\mathrm{set}(S) = \mathrm{set}(S') \;:\Leftrightarrow$?

Set Construction

Definition 1.1.9. Let S, T be sets. We define:

S

Definition 1.4.1.1. We define:

$\mathbb{N}$

Definition 1.1.10. Let S be a set. We define:

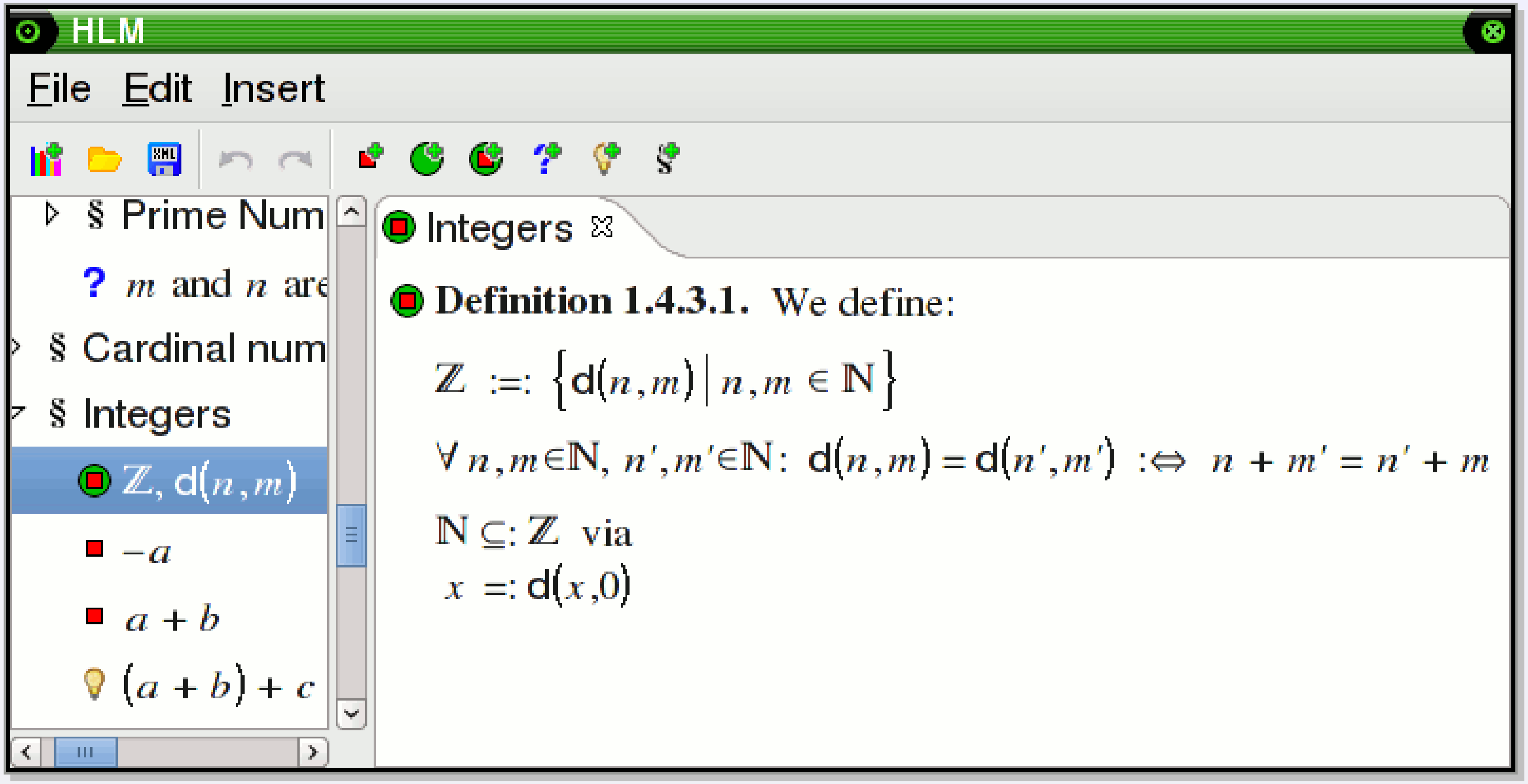
$$\boldsymbol{P}(S) \;:=:\; \left\{ (T) \;\middle|\; T \subseteq S \right\}$$

Definition 1.1.11. We define:

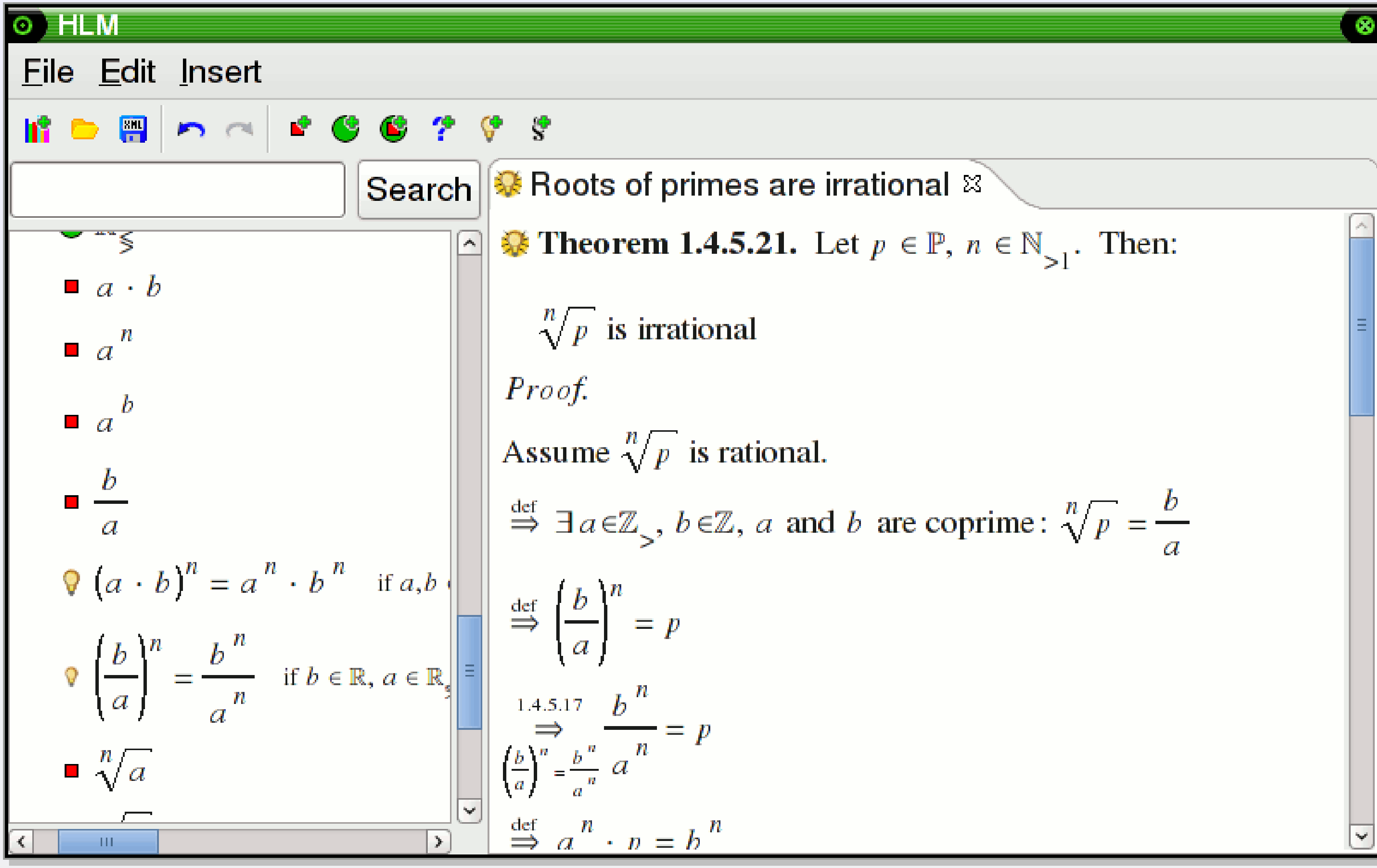
$$\textbf{Sets} \;:=:\; \left\{ \mathsf{set}(S) \;\middle|\; S \text{ is a set} \right\}$$

$$\forall \text{sets } S, S' : \; \mathsf{set}(S) = \mathsf{set}(S') \;:\Leftrightarrow\; \exists f \in S \leftrightarrow S'$$

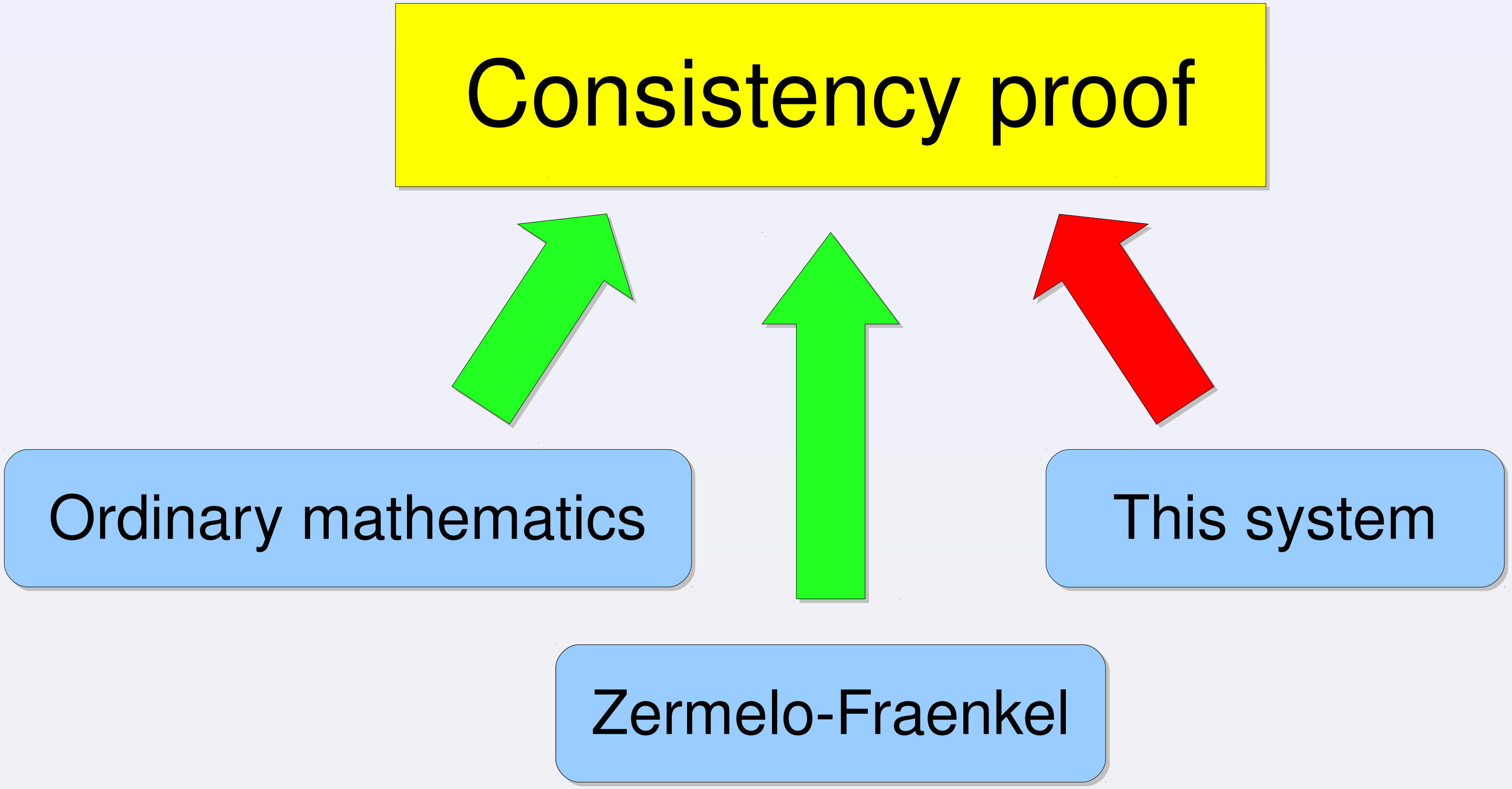
Embedding


HLM
File Edit Insert
§ Prime Num
? m and n are
§ Cardinal num
§ Integers
ℤ, d(n, m)
−a
a + b
(a + b) + c
Integers
Definition 1.4.3.1. We define:
ℤ := {d(n,m) | n,m ∈ ℕ}
∀ n,m∈ℕ, n′,m′∈ℕ: d(n,m) = d(n′,m′) :⇔ n + m′ = n′ + m
ℕ ⊆: ℤ via
x =: d(x,0)

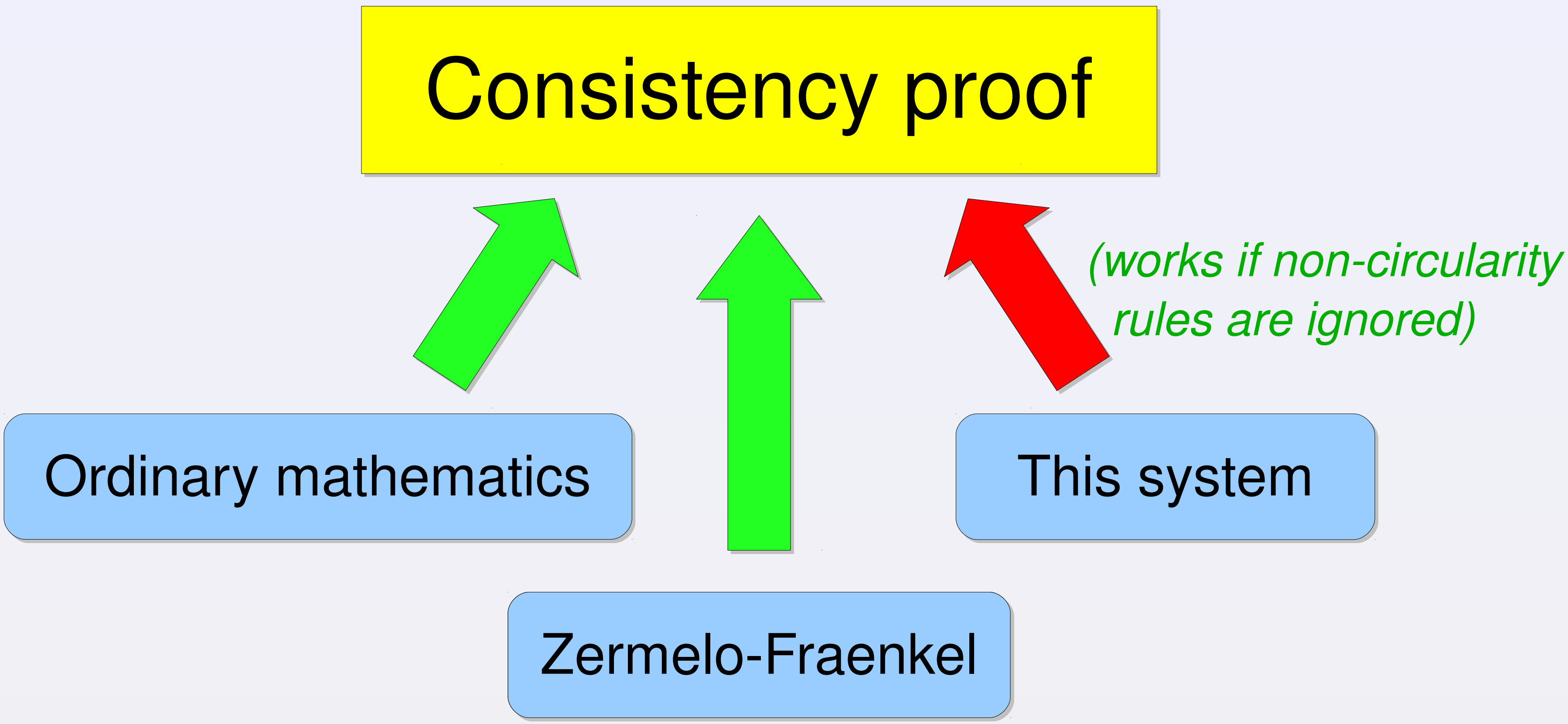
Example


HLM
File
Edit
Insert
Search
Roots of primes are irrational
Theorem 1.4.5.21. Let $p \in \mathbb{P}$, $n \in \mathbb{N}_{>1}$. Then:
$\sqrt[n]{p}$ is irrational
Proof.
Assume $\sqrt[n]{p}$ is rational.
$\overset{def}{\Rightarrow} \exists a \in \mathbb{Z}_{>}, b \in \mathbb{Z}$, a and b are coprime : $\sqrt[n]{p} = \frac{b}{a}$
$\overset{def}{\Rightarrow} \left(\frac{b}{a}\right)^n = p$
$\overset{1.4.5.17}{\Rightarrow} \frac{b^n}{a^n} = p$
$\left(\frac{b}{a}\right)^n = \frac{b^n}{a^n}$
$\overset{def}{\Rightarrow} a^n \cdot p = b^n$
$a \cdot b$
a^n
a^b
$\frac{b}{a}$
$(a \cdot b)^n = a^n \cdot b^n$ if a,b
$\left(\frac{b}{a}\right)^n = \frac{b^n}{a^n}$ if $b \in \mathbb{R}$, $a \in \mathbb{R}$
$\sqrt[n]{a}$

Consistency



Consistency



Conclusions

- Proof assistant modeling mathematical practice
  - Looks like naive set theory
  - Restriction to meaningful inputs (→ types)
- Parameter lists in definitions, theorems, quantifiers, and constructors
- Sets of all structures up to isomorphism
- Embedding
- Consistency

Thank you!

Prototype:
http://hlm.sourceforge.net/