

# Treating Sets as Types in a Proof Assistant for Ordinary Mathematics

$\frac{b}{a}$

$(a \cdot b)^n = a^n \cdot b^n$  if  $a, b \in \mathbb{R}$

$\left(\frac{b}{a}\right)^n = \frac{b^n}{a^n}$  if  $b \in \mathbb{R}, a \in \mathbb{R}, a \neq 0$

$\sqrt[n]{a}$

$\sqrt{a}$

?  $a$  is rational

$\sqrt[n]{p}$  is irrational if  $p \in \mathbb{P}$

$\sqrt{2}$  is irrational

gebra

$\sqrt[n]{p}$  is irrational

*Proof.*

Assume  $\sqrt[n]{p}$  is rational.

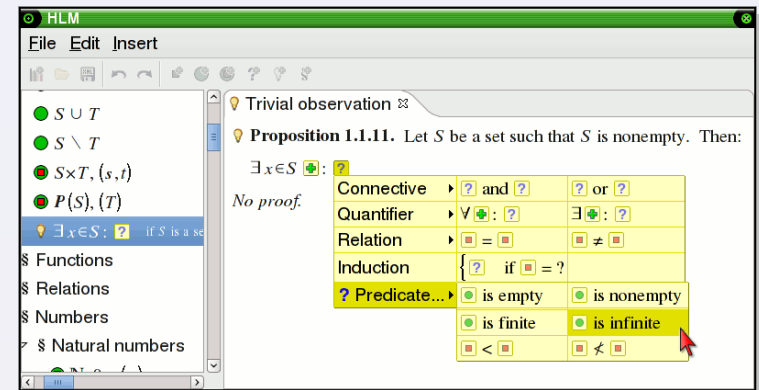
Resolve Goal...	
Use Definition	Def $\Rightarrow \sqrt[n]{p} \in \mathbb{Q}$
Substitute...	Def $\Rightarrow \exists b \in \mathbb{Z}_{>0}, c \in \mathbb{Z}: \sqrt[n]{p} = \frac{c}{b}$
Resolve...	
Repeat	Def $\Rightarrow \exists! d \in \mathbb{Z}_{>0}, e \in \mathbb{Z}, d$ and $e$ are coprime: $\sqrt[n]{p} = \frac{e}{d}$
State Formula	
Define Variable	
Use Theorem...	

and	or
$\forall x: ?$	$\exists x: ?$
$=$	$\neq$
{ ? if $=$ ? }	
is empty	is nonempty
is finite	is infinite
$<$	$\nless$

# Input Methods

Text

GUI



# Input Methods

## Text

Syntax

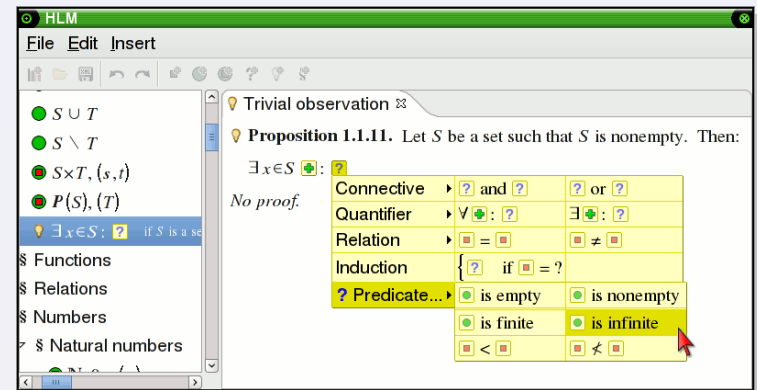
Naming

Symbol overloading

## GUI

Rendering

Selection



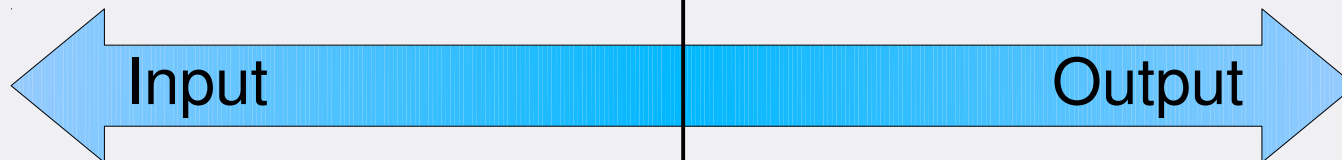
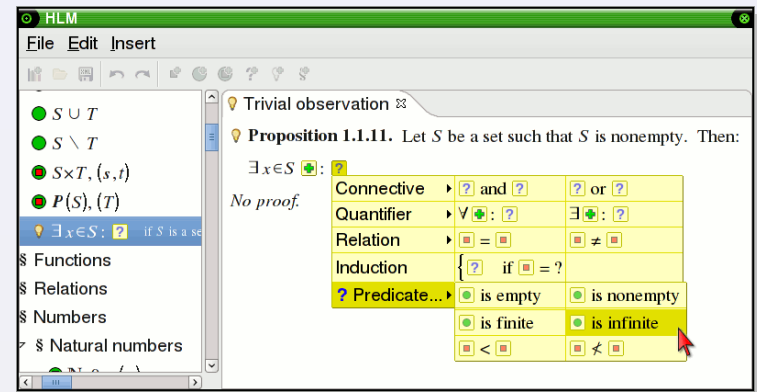
# Input Methods

## Text

Syntax  
Naming  
Symbol overloading

## GUI

Rendering  
Selection



# Input Methods

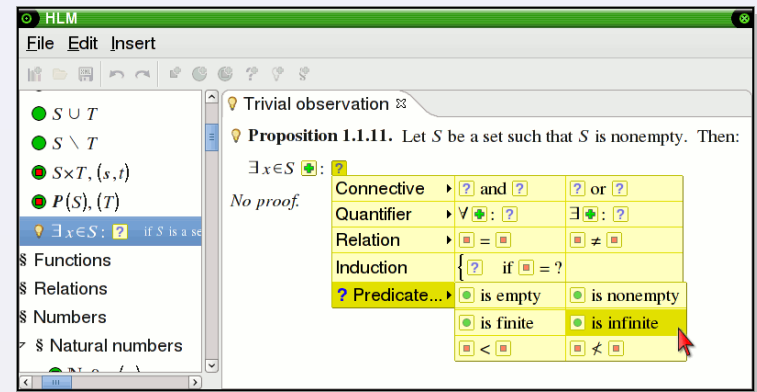
## Text

Syntax  
Naming  
Symbol overloading

*Set theory with  
soft types (→ Mizar)*

## GUI

Rendering  
Selection



Input

Output

# Input Methods

## Text

Syntax  
Naming  
Symbol overloading

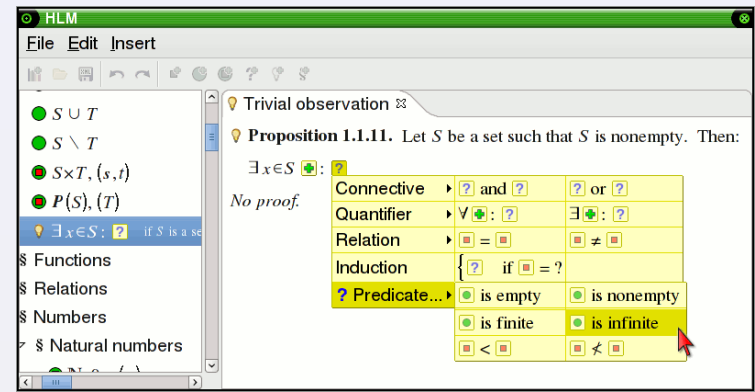
*Set theory with soft types (→ Mizar)*

## GUI

Rendering  
Selection

*Set theory*


*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

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

- $y \in \bullet$
- $S \subseteq \bullet$
- $S$  be a set
- such that  $?$
- Advanced  $\blacktriangleright$

Element

Subset

Arbitrary set

Constraint

} parameter

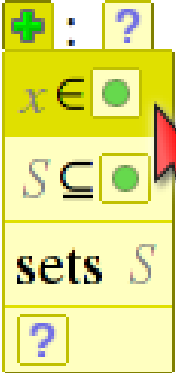


# Parameter Lists

Proposition 1.1.1.1

$\forall n \in \mathbb{N}, n < 2$

*No proof.*



Element

Subset

Arbitrary set

Constraint

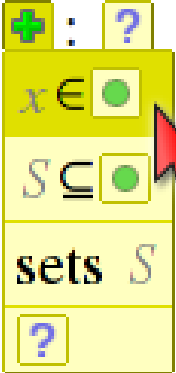
} parameter

# Parameter Lists

Proposition 1.1.1.1

$\forall n \in \mathbb{N}, n < 2$

No proof.



Element

Subset

Arbitrary set

Constraint

} Element variable

} Set variable

# Parameter Lists

Proposition 1.1.1.1

$\forall n \in \mathbb{N}, n < 2$  + ?

No proof.

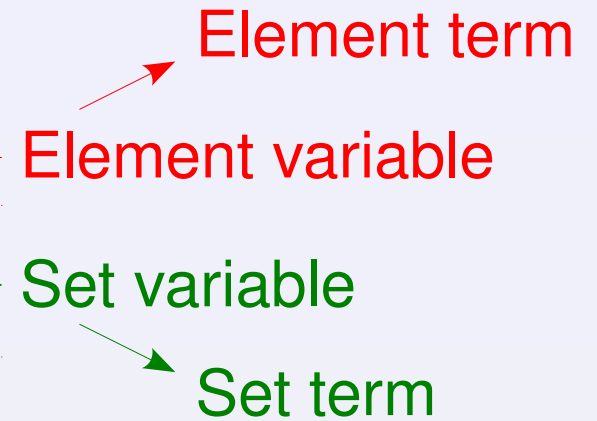
$x \in$  ●

$S \subseteq$  ●

sets  $S$

?

- ← Element
- ← Subset
- ← Arbitrary set
- ← Constraint



# Parameter Lists

Proposition 1.4.151

$\forall n \in \mathbb{N}, n < 2$  + ?

No proof.

+ ?

$x \in$  ●

$S \subseteq$  ●

sets  $S$

?

Element

Subset

Arbitrary set

Constraint

Element term

Element variable

Set variable

Set term

HLM

File Edit Insert

Search

test

Proposition 1.4.151 +

No

Connective	<span style="color: blue;">?</span> and <span style="color: blue;">?</span>	<span style="color: blue;">?</span> or <span style="color: blue;">?</span>
Quantifier	$\forall$ <span style="color: green;">+</span> <span style="color: blue;">?</span>	$\exists$ <span style="color: green;">+</span> <span style="color: blue;">?</span>
Relation	$=$	$\neq$
Induction	$\in$ <span style="color: green;">●</span>	$\notin$ <span style="color: green;">●</span>
<span style="color: blue;">?</span> Predicate...	$\subseteq$ <span style="color: green;">●</span>	$\not\subseteq$ <span style="color: green;">●</span>
	$=$ <span style="color: green;">●</span>	$\neq$ <span style="color: green;">●</span>

# Types

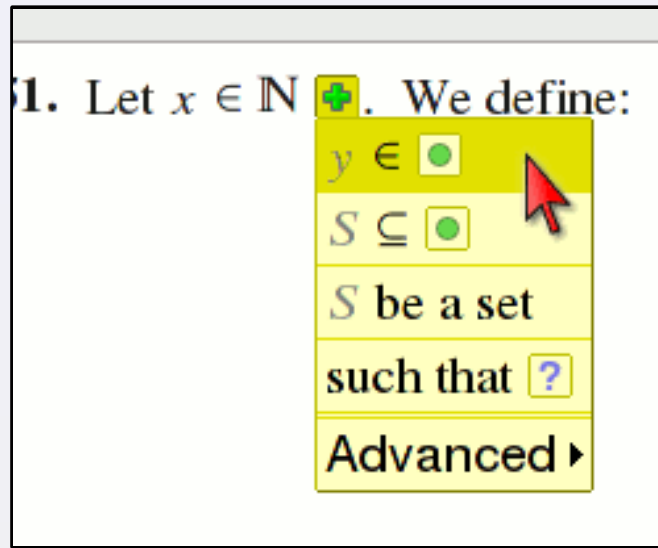
*Informal principle:*


“ $x=y$ ” 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:

- $y \in$  
- $S \subseteq$  
- $S$  be a set
- such that 
- Advanced 

# 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,  $f \in X \rightarrow Y$ ,  $S \subseteq Y$ . We define:

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

# 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,  $f \in X \rightarrow Y$ ,  $S \subseteq Y$ . 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,  $f \in X \rightarrow Y$ ,  $S \subseteq Y$ . We define:


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

# Set Operations

The screenshot shows the HLM software interface. The title bar is green and contains the text "HLM". Below the title bar is a menu bar with "File", "Edit", and "Insert". A toolbar with various icons is located below the menu bar. The main workspace is divided into two panes. The left pane contains a list of items: a question mark followed by  $a < b$ , and several entries with a green circle and a mathematical symbol:  $\mathbb{Z}_{>}$ ,  $\mathbb{Z}_{\geq}$ ,  $\mathbb{Z}_{<}$ ,  $\mathbb{Z}_{\leq}$ , and  $\mathbb{Z}_{\neq}$ . The right pane has two tabs: "Union" and "Nonzero numbers". The "Nonzero numbers" tab is active and contains the text "Definition 1.4.3.16. We define:" followed by the equation  $\mathbb{Z}_{\neq} := \{a \in \mathbb{Z} : a \neq 0\}$ . Below this, the expression  $= \mathbb{Z}_{<} \cup \mathbb{Z}_{>}$  is shown, with a yellow highlight and a red hand cursor pointing to the union symbol. A yellow tooltip box is overlaid on the right pane, containing the text "Definition 1.1.7. Let  $U$  be a set,  $S, T \subseteq U$ . We define:" followed by the equation  $S \cup T := \{x \in U : x \in S \text{ or } x \in T\}$ .

# Set Construction

The screenshot shows the HLM software interface. The title bar is green and contains the text "HLM". Below the title bar is a menu bar with "File", "Edit", and "Insert". A toolbar with various icons is located below the menu bar. On the left side, there is a sidebar with a search box and a list of items: "Library", "Essentials", "\$ Sets", "\$ Functions", "\$ Relations", "\$ Numbers", "Constructed Set(S, T), fir:", and "Algebra". The main area displays a definition for "Constructed Set(S, T)".

**Constructed Set** 

**Definition 1.5.** Let  $S$  be a set,  $T \subseteq S$ . We define:

$$\text{Constructed Set}(S, T) := \left\{ \begin{array}{l} \text{first constructor}_{S, T}(s, t) \mid s \in S, t \in T \quad \oplus \\ \text{second constructor}_{S, T}(x) \mid x \in \mathbb{N} \quad \oplus \\ \oplus \end{array} \right\}$$

A context menu is open over the definition, showing the following items:

- $y \in \bullet$
- $U \subseteq \bullet$
- $U$  is a set
- such that ?
- Advanced ▶

# Set Construction

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

$$\text{Cartesian product}(S, T) := \left\{ \begin{array}{l} \text{pair}_{S, T}(s, t) \\ \oplus \end{array} \middle| s \in S, t \in T \oplus \right\}$$

# Set Construction

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

$$S \times T := \left\{ \begin{array}{l} (s, t) \\ \oplus \end{array} \middle| s \in S, t \in T \oplus \right\}$$

# Set Construction

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

● **Definition 1.4.1.1.** We define:

$$\mathbb{N} := \left\{ \begin{array}{l} 0 \\ \mathfrak{s}(n) \mid n \in \mathbb{N} \end{array} \right\}$$

# 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:

$$P(S) := \{ (T) \mid T \subseteq S \}$$

# 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:

$$P(S) := \{ (T) \mid T \subseteq S \}$$

Definition 1.1.11. We define:

$$\text{Sets} := \left\{ \begin{array}{l} \text{set}(S) \mid S \text{ is a set} \\ \text{+} \end{array} \right\}$$

$$\text{set}(S) = \text{set}(S')$$

?



# 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:

$$P(S) := \{ (T) \mid T \subseteq S \}$$

Definition 1.1.11. We define:

$$\text{Sets} := \left\{ \begin{array}{l} \text{set}(S) \mid S \text{ is a set } \oplus \\ \oplus \end{array} \right\}$$

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

# 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:

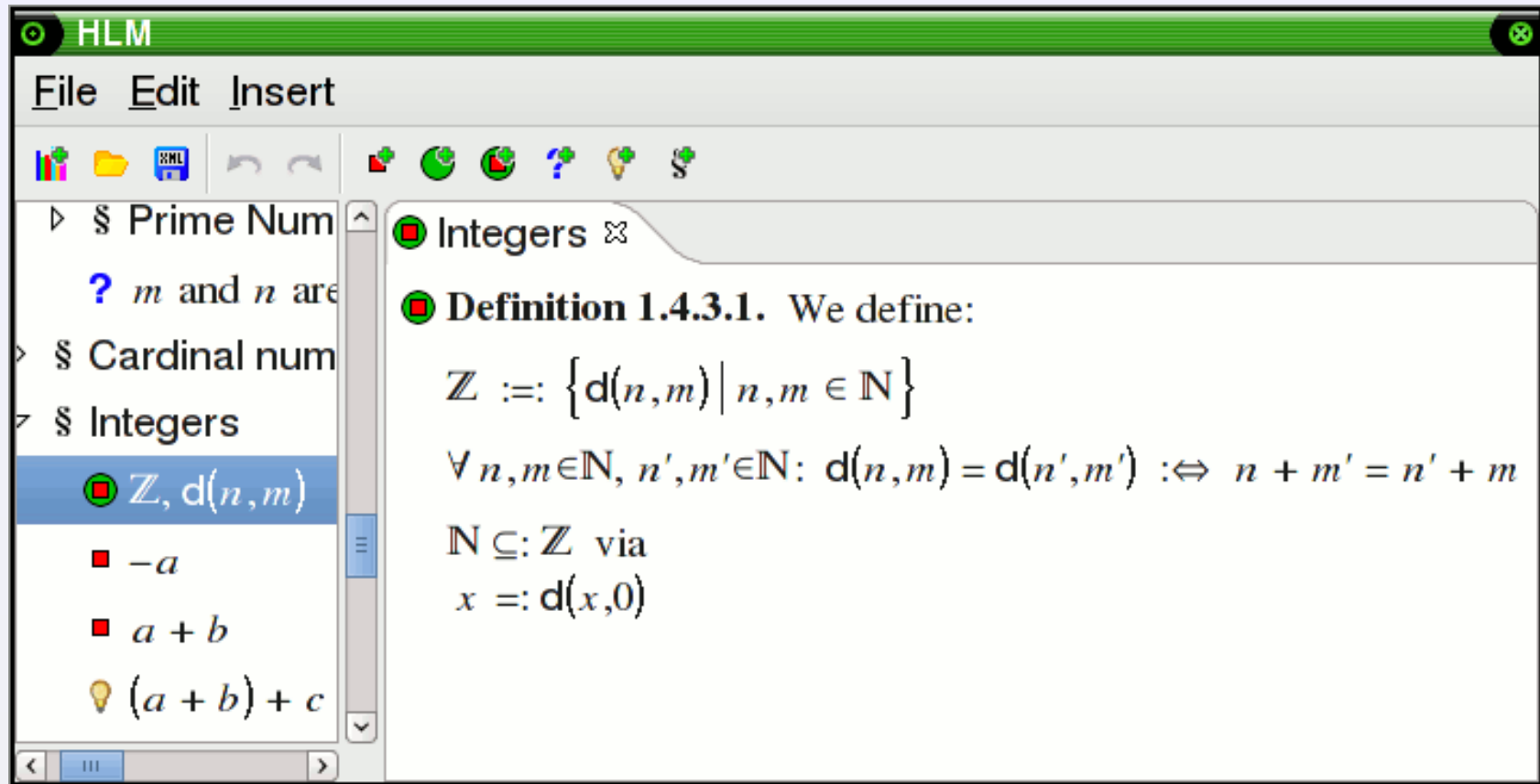
$$P(S) := \{ (T) \mid T \subseteq S \}$$

Definition 1.1.11. We define:

$$\mathbf{Sets} := \left\{ \begin{array}{l} \mathbf{set}(S) \mid S \text{ is a set} \\ \mathbf{+} \end{array} \right\}$$

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

# Embedding



The screenshot shows the HLM (Hilbert Language Manager) software interface. The window title is "HLM". The menu bar includes "File", "Edit", and "Insert". The toolbar contains various icons for file operations and editing. The left sidebar shows a tree view of the document structure:

- ▷ § Prime Num
- ?  $m$  and  $n$  are
- ▷ § Cardinal num
- ▷ § Integers
  - $\mathbb{Z}, d(n, m)$
  - $-a$
  - $a + b$
  - 💡  $(a + b) + c$

The main editor area displays the following content:

- Integers ☒
- **Definition 1.4.3.1.** We define:
  - $$\mathbb{Z} ::= \{d(n, m) \mid n, m \in \mathbb{N}\}$$
  - $$\forall n, m \in \mathbb{N}, n', m' \in \mathbb{N}: d(n, m) = d(n', m') \Leftrightarrow n + m' = n' + m$$
  - $$\mathbb{N} \subseteq: \mathbb{Z} \text{ via}$$
  - $$x ::= d(x, 0)$$

# Example

The screenshot shows the HLM software interface. The title bar is green and contains the text "HLM". Below the title bar is a menu bar with "File", "Edit", and "Insert". Underneath the menu bar is a toolbar with various icons. A search bar is located below the toolbar. The main content area is divided into two panes. The left pane contains a list of mathematical expressions, each preceded by a red square icon. The right pane contains a theorem and its proof.

**File Edit Insert**

Search

- $a \cdot b$
- $a^n$
- $a^b$
- $\frac{b}{a}$
- 💡  $(a \cdot b)^n = a^n \cdot b^n$  if  $a, b \in \mathbb{R}$
- 💡  $\left(\frac{b}{a}\right)^n = \frac{b^n}{a^n}$  if  $b \in \mathbb{R}, a \in \mathbb{R}, a \neq 0$
- $\sqrt[n]{a}$

☀️ **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.

$\stackrel{\text{def}}{\Rightarrow} \exists a \in \mathbb{Z}_{>}, b \in \mathbb{Z}, a \text{ and } b \text{ are coprime: } \sqrt[n]{p} = \frac{b}{a}$

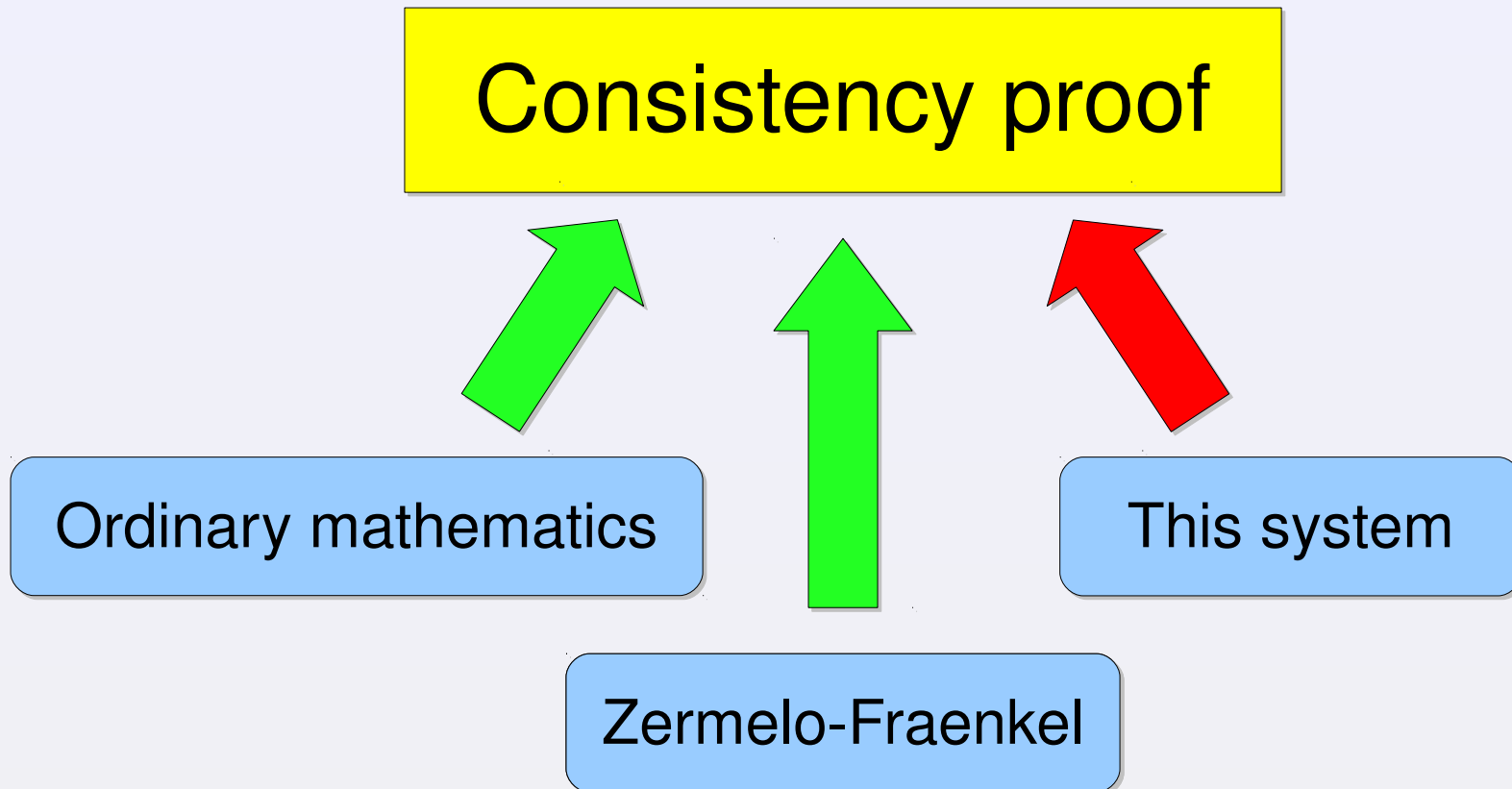
$\stackrel{\text{def}}{\Rightarrow} \left(\frac{b}{a}\right)^n = p$

$\stackrel{1.4.5.17}{\Rightarrow} \frac{b^n}{a^n} = p$

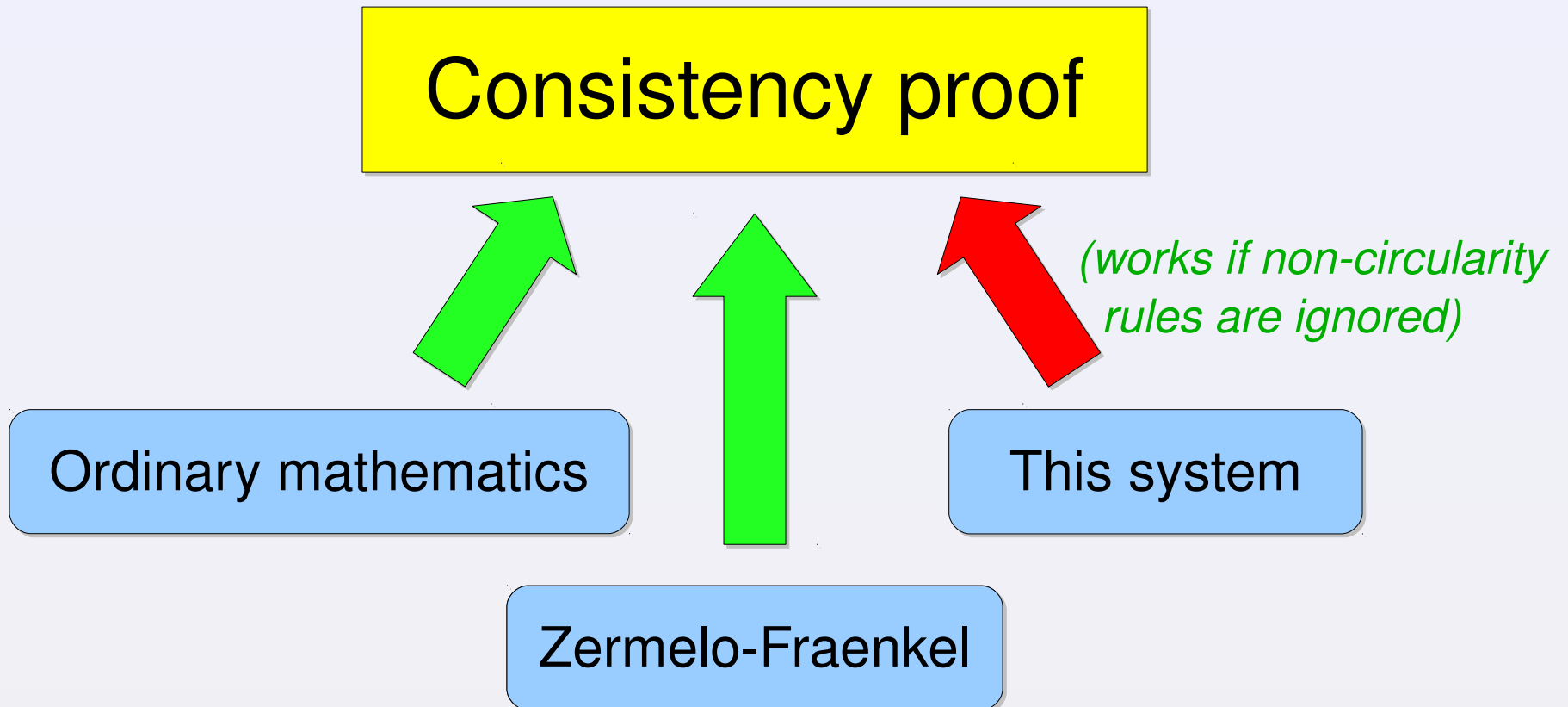
$\left(\frac{b}{a}\right)^n = \frac{b^n}{a^n} = p$

$\stackrel{\text{def}}{\Rightarrow} a^n \cdot p = b^n$

# Consistency



# Consistency



# Conclusions

- Proof assistant modeling mathematical practice
  - Looks like naive set theory
  - Restriction to meaningful inputs ( $\rightarrow$  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/>