A proof of the irrationality of $\sqrt{2}$

Leslie Lamport

December 1, 1993

Abstract
Printable version of a sample proof that uses Lamport’s proof style [1], illustrating how structured proofs can be converted to HTML pages via \LaTeX\ enrichment with extensions for Lamport’s proof style.

Theorem There does not exist $r$ in $\mathbb{Q}$ such that $r^2 = 2$.

Proof sketch: We assume $r^2 = 2$ for $r \in \mathbb{Q}$ and obtain a contradiction. Writing $r = m/n$, where $m$ and $n$ have no common divisors (step ⟨1⟩1), we deduce from $(m/n)^2 = 2$ and the lemma that both $m$ and $n$ must be divisible by 2 (⟨1⟩2 and ⟨1⟩3).

Assume: 1. $r \in \mathbb{Q}$
   2. $r^2 = 2$

Prove: False

⟨1⟩1. Choose $m$, $n$ in $\mathbb{Z}$ such that
   1. $\gcd(m, n) = 1$
   2. $r = (m/n)$

⟨2⟩1. Choose $p$, $q$ in $\mathbb{Z}$ such that $q \neq 0$ and $r = p/q$.
   Proof: By assumption ⟨0⟩1.

Let: $m \triangleq p/\gcd(p, q)$
   $n \triangleq q/\gcd(p, q)$

⟨2⟩2. $m, n \in \mathbb{Z}$
   Proof: ⟨2⟩1 and definition of $m$ and $n$.

⟨2⟩3. $r = m/n$
   Proof: $m/n = p/\gcd(p, q)$ [Definition of $m$ and $n$]
   \[= p/q\] [Simple algebra]
   \[= r\] [By ⟨2⟩1]

⟨2⟩4. $\gcd(m, n) = 1$
   Proof: By the definition of the gcd, it suffices to:
   Assume: 1. $s$ divides $m$
   2. $s$ divides $n$
   Prove: $s = \pm 1$
   ⟨3⟩1. $s \cdot \gcd(p, q)$ divides $p$.  

1
Proof: \langle 2 \rangle:1 and the definition of \( m \).

\( \langle 3 \rangle 2 \). \( s \cdot \gcd(p, q) \) divides \( q \).

Proof: \langle 2 \rangle:2 and definition of \( n \).

\( \langle 3 \rangle 3 \). Q.E.D.

Proof: \langle 3 \rangle:1, \langle 3 \rangle:2, and the definition of \( \gcd \).

\( \langle 2 \rangle 5 \). Q.E.D.

\( \langle 1 \rangle 2 \). \( 2 \) divides \( m \).

(\langle 2 \rangle 1 \). \( m^2 = 2n^2 \)

Proof: \langle 1 \rangle:1 implies \( (m/n)^2 = 2 \).

(\langle 2 \rangle 2 \). Q.E.D.

Proof: By \langle 2 \rangle:1 and the lemma.

\( \langle 1 \rangle 3 \). \( 2 \) divides \( n \).

(\langle 2 \rangle 1 \). Choose \( p \) in \( \mathbb{Z} \) such that \( m = 2p \).

Proof: By \langle 1 \rangle:2.

(\langle 2 \rangle 2 \). \( n^2 = 2p^2 \)

Proof: \( 2 = (m/n)^2 \) \[\langle 1 \rangle:1.2 \text{ and } \langle 0 \rangle:2\]

\( = (2p/n)^2 \) \[\langle 2 \rangle:1\]

\( = 4p^2/n^2 \) \[\text{Algebra}\]

from which the result follows easily by algebra.

(\langle 2 \rangle 3 \). Q.E.D.

Proof: By \langle 2 \rangle:2 and the lemma.

(\langle 1 \rangle 4 \). Q.E.D.

Proof: \langle 1 \rangle:1.1, \langle 1 \rangle:2, \langle 1 \rangle:3, and definition of \( \gcd \).

References