

LaTeXML Proof Example

Mengxiang Jiang

November 26, 2025

1 Introduction

There's an often told story of Hippasus, a mathematician during Pythagoras's time, that found out that the length of the diagonal of a square was not commensurate with the length of its side. He was apparently drowned for this discovery by the Pythagoreans. At some level, I can sympathize with the Pythagoreans, since this proof is deeply unsettling when I first read it. Like, rational numbers can be made as small and accurate as you want, what do you mean there's something it can't perfectly describe? And even after learning real analysis, the way $\sqrt{2}$ is actually described (whether it's a Dedekind cut, equivalence class of Cauchy sequences, or something else) leaves much to be desired. I much prefer the algebraic treatment of $\sqrt{2}$ instead, where just like i , we just claim it's not a part of the rationals and adjoin it, without making any claims about what it really is. So my proof won't say that $\sqrt{2}$ is irrational, but rather that the rational numbers do not have such a number.

2 The Proof

Theorem 2.1.

$$\forall q \in \mathbb{Q}, q^2 \neq 2.$$

Proof. Assume for contradiction that there does exist a number q in the rationals whose square is 2. We use the property that all rational numbers can be written in the most reduced form (proof of this property left to the reader) to write

$$q = \frac{a}{b},$$

where $a, b \in \mathbb{Z}$, $b \neq 0$, and a and b are coprime. Thus

$$q^2 = 2 = \frac{a^2}{b^2},$$

which implies

$$2b^2 = a^2.$$

We use the property that the product of even numbers is even and the product of odd numbers is odd (proof left to the reader) to conclude that a must be even since a^2 is even. Thus we can write $a = 2c$ for some $c \in \mathbb{Z}$. We then have

$$q^2 = 2 = \frac{(2c)^2}{b^2},$$

which implies

$$2b^2 = 4c^2.$$

Dividing both sides by 2, we have

$$b^2 = 2c^2,$$

which using the latter property again tells us b is even. But this contradicts the fact that a and b are coprime since they both share a factor of 2. \square

3 Conclusion

This proof demonstrates that there is no rational number whose square is 2. Here is a list of remarks regarding this proof:

- This proof can be easily adapted to show that for any prime number p , there is no rational number whose square is p .
- The constructible numbers, which are numbers that can be constructed using a compass and straightedge, include the length of the diagonal of a unit square. This proof shows that the constructible numbers are a larger number system than the rationals.
- All numbers on computers are rational numbers, since they are represented with a finite number of bits, which can only represent a finite number of fractions. This proof shows that computers cannot exactly represent the square root of 2, at least numerically.

Since the rationals do not contain such a number, we can adjoin $\sqrt{2}$ to them to form a larger number system that does contain such a number, which is called the field extension $\mathbb{Q}(\sqrt{2})$. This field extension contains all numbers of the form $a + b\sqrt{2}$, where a and b are rational numbers, and is the smallest field that contains both the rationals and $\sqrt{2}$. In closing, we will show that $\mathbb{Q}(\sqrt{2})$ is indeed a field.

3.1 Definition of a field

A field is a set F equipped with two binary operations, addition and multiplication, such that the following properties hold:

- Associativity of addition and multiplication: For all $x, y, z \in F$, we have $(x + y) + z = x + (y + z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

- Commutativity of addition and multiplication: For all $x, y \in F$, we have $x + y = y + x$ and $x \cdot y = y \cdot x$.
- Distributivity of multiplication over addition: For all $x, y, z \in F$, we have $x \cdot (y + z) = x \cdot y + x \cdot z$.
- Additive and multiplicative identities: There exist elements $0, 1 \in F$ such that for all $x \in F$, $x + 0 = x$ and $x \cdot 1 = x$
- Additive and multiplicative inverses: For every $x \in F$, there exist elements $-x, x^{-1} \in F$ such that $x + (-x) = 0$ and $x \cdot x^{-1} = 1$, where x^{-1} is defined only for $x \neq 0$.
- Distributivity of multiplication over addition: For all $x, y, z \in F$, we have $x \cdot (y + z) = x \cdot y + x \cdot z$.

Please note that many of the following steps seem trivial, but they are necessary since we want to only manipulate rational numbers using their properties without assuming they also hold for $\sqrt{2}$.

3.2 Associativity of addition and multiplication

Let $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, and $z = e + f\sqrt{2}$, where $a, b, c, d, e, f \in \mathbb{Q}$. We have

$$\begin{aligned}
(x + y) + z &= ((a + b\sqrt{2}) + (c + d\sqrt{2})) + (e + f\sqrt{2}) \\
&= (a + c + (b + d)\sqrt{2}) + (e + f\sqrt{2}) \\
&= (a + c + e) + ((b + d) + f)\sqrt{2} \\
&= a + (c + e) + b\sqrt{2} + (d + f)\sqrt{2} \\
&= (a + b\sqrt{2}) + ((c + d\sqrt{2}) + (e + f\sqrt{2})) \\
&= x + (y + z).
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
(x \cdot y) \cdot z &= ((a + b\sqrt{2}) \cdot (c + d\sqrt{2})) \cdot (e + f\sqrt{2}) \\
&= (ac + 2bd + (ad + bc)\sqrt{2}) \cdot (e + f\sqrt{2}) \\
&= (ac + 2bd)e + (ac + 2bd)f\sqrt{2} + (ad + bc)e\sqrt{2} + 2(ad + bc)f \\
&= (ace + 2bde + 2adf + 2bcf) + (acf + ade + bce)\sqrt{2} \\
&= (a + b\sqrt{2}) \cdot ((c + d\sqrt{2}) \cdot (e + f\sqrt{2})) \\
&= x \cdot (y \cdot z).
\end{aligned}$$

3.3 Commutativity of addition and multiplication

Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$, where $a, b, c, d \in \mathbb{Q}$. We have

$$\begin{aligned} x + y &= (a + b\sqrt{2}) + (c + d\sqrt{2}) \\ &= (a + c) + (b + d)\sqrt{2} \\ &= (c + d\sqrt{2}) + (a + b\sqrt{2}) \\ &= y + x. \end{aligned}$$

Similarly, we have

$$\begin{aligned} x \cdot y &= (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \\ &= ac + 2bd + (ad + bc)\sqrt{2} \\ &= (c + d\sqrt{2}) \cdot (a + b\sqrt{2}) \\ &= y \cdot x. \end{aligned}$$

3.4 Identities and Inverses

The additive identity is $0 = 0 + 0\sqrt{2}$, since for any $x = a + b\sqrt{2}$, we have

$$x + 0 = (a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2} = x.$$

The multiplicative identity is $1 = 1 + 0\sqrt{2}$, since for any $x = a + b\sqrt{2}$, we have

$$x \cdot 1 = (a + b\sqrt{2}) \cdot (1 + 0\sqrt{2}) = a + b\sqrt{2} = x.$$

The additive inverse of $x = a + b\sqrt{2}$ is $-x = -a - b\sqrt{2}$, since

$$x + (-x) = (a + b\sqrt{2}) + (-a - b\sqrt{2}) = 0 + 0\sqrt{2} = 0.$$

The multiplicative inverse of $x = a + b\sqrt{2}$ (for $x \neq 0$) is

$$\begin{aligned} x^{-1} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}, \end{aligned}$$

since

$$\begin{aligned} x \cdot x^{-1} &= (a + b\sqrt{2}) \cdot \left(\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \right) \\ &= \frac{a^2 - 2b^2}{a^2 - 2b^2} + 0\sqrt{2} \\ &= 1 + 0\sqrt{2} = 1. \end{aligned}$$

3.5 Distributivity of multiplication over addition

Let $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, and $z = e + f\sqrt{2}$, where $a, b, c, d, e, f \in \mathbb{Q}$. We have

$$\begin{aligned}x \cdot (y + z) &= (a + b\sqrt{2}) \cdot ((c + d\sqrt{2}) + (e + f\sqrt{2})) \\&= (a + b\sqrt{2}) \cdot ((c + e) + (d + f)\sqrt{2}) \\&= a(c + e) + b(c + e)\sqrt{2} + a(d + f)\sqrt{2} + 2b(d + f) \\&= (ac + ae + 2bd + 2bf) + (ad + af + bc + be)\sqrt{2} \\&= (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) + (a + b\sqrt{2}) \cdot (e + f\sqrt{2}) \\&= x \cdot y + x \cdot z.\end{aligned}$$

Thus, we have shown that $\mathbb{Q}(\sqrt{2})$ satisfies all the properties of a field.