Square roots, and the existence of irrational numbers.

Definition. If \( b^2 = a \), then we say that \( b \) is a square root of \( a \).

A negative number has no square root (see Theorem I.20), and the number 0 has only one square root, namely 0. We shall show that a positive real number has exactly two square roots, one positive and one negative.

**Theorem.** Let \( a > 0 \). Then there is a number \( b > 0 \) such that \( b^2 = a \).

**Proof. Step 1.** Let \( x \) and \( y \) be positive numbers. Then \( x < y \) if and only if \( x^2 < y^2 \).

If \( x < y \), we multiply both sides, first by \( x \) and then by \( y \), to obtain the inequalities

\[
x \cdot x < y \cdot x \quad \text{and} \quad y \cdot x < y \cdot y.
\]

Thus \( x^2 < y^2 \). Conversely if \( x^2 < y^2 \), then it cannot be true that \( x = y \) (for that would imply \( x^2 = y^2 \)), or that \( y < x \) (for that would imply, by what we just proved, that \( y^2 < x^2 \)). Hence we must have \( x < y \).

**Step 2.** We construct \( b \) as follows: Consider the set

\[
S = \{ x \mid x > 0 \text{ and } x^2 < a \}.
\]

The set \( S \) is nonempty; indeed if \( x \) is a number such that \( 0 < x \leq 1 \) and \( x < a \), then

\[
x^2 < ax \leq a \cdot 1 = a,
\]

so that \( x \) is in \( S \). Furthermore, \( S \) is bounded above; indeed, \( 1 + a \) is an upper bound on \( S \).
For if $x$ is in $S$, then $x^2 < a$; since
\[ a < 1 + 2a + a^2 = (1+a)^2, \]
it follows from Step 1 that $x < 1 + a$.

Let $b$ denote the supremum of $S$; we show that $b^2 = a$. We verify this fact by showing that neither inequality $b^2 < a$ or $b^2 > a$ can hold.

**Step 3.** Assume first that $b^2 < a$. We shall show that there is a positive number $h$ such that $(b+h)^2 < a$. It then follows that $b + h$ belongs to $S$ (by definition of $S$), contradicting the fact that $b$ is an upper bound for $S$.

To find $h$, we proceed as follows: The inequality $(b+h)^2 < a$ is equivalent to the inequality
\[ h(2b+h) < a-b^2. \]
Now $a - b^2$ is positive; it seems reasonable that if we take $h$ to be sufficiently small, this inequality will hold. Specifically, we first specify that $h \leq 1$; then we have
\[ h(2b+h) \leq h(2b+1). \]
It is then easy to see how small $h$ should be; if we choose $h < (a-b^2)/(2b+1)$, then
\[ h(2b+1) < a - b^2 \]
and we are finished.

**Step 4.** Now assume that $b^2 > a$. We shall show that there is a number $h$ such that $0 < h < b$ and $(b-h)^2 > a$. It follows that $b - h$ is an upper bound for $S$: For
if \( x \) is in \( S \), then \( a > x^2 \), so that \((b-h)^2 > x^2\), whence by Step 1, \( b - h > x \). This contradicts the fact that \( b \) is the least upper bound for \( S \).

To find \( h \), we proceed as follows: The inequality \((b-h)^2 > a\) is equivalent to the inequality
\[
h(2b-h) < b^2 - a.
\]
Now \( b^2 - a \) is positive; it seems reasonable that if \( h \) is sufficiently small, this inequality will hold. Our first requirement is that \( 0 < h < b \). Then we note that \( h(2b-h) = 2hb - h^2 < 2hb \). It is now easy to see how small \( h \) should be; if we choose \( h < (b^2 - a)/2b \), then
\[
2hb < b^2 - a
\]
and we are finished. \(\square\)

**Corollary. If \( a > 0 \), then \( a \) has exactly two square roots.**

We denote the positive square root of \( a \) by \( \sqrt{a} \).

**Proof.** Let \( b > 0 \) and \( b^2 = a \). Then \((-b)^2 = a \). Thus \( a \) has at least two square roots, \( b \) and \(-b \). Conversely, if \( c \) is any square root of \( a \), then \( c^2 = a \), whence
\[
(b+c)(b-c) = b^2 - c^2 = 0.
\]
It follows that \( c = -b \) or \( c = b \). \(\square\)

We now demonstrate the existence of irrational numbers.

**Theorem.** Let \( a \) be a positive integer; let \( b = \sqrt{a} \). Then either \( b \) is a positive integer or \( b \) is irrational.

**Proof.** Suppose that \( b = \sqrt{a} \) and \( b \) is a rational number that is not an integer. We derive a contradiction.

Let us write \( b = m/n \), where \( m \) and \( n \) are positive integers and \( n \) is as small as possible. (I.e., we choose \( n \) to be the smallest positive integer such that \( nb \) is an integer, and we set \( m = nb \).)

Choose \( q \) to be the unique integer such that
\[ q < \frac{m}{n} < q+1. \]

Then
\[ qn < m < qn + n, \text{ or} \]

\[ (*) \]
\[ 0 < m - qn < n. \]

We compute as follows:
\[ (\frac{m}{n})^2 = b^2 = a, \]
\[ m^2 = n^2 a \]
\[ m(m - qn) = n(na - qm). \]

Then using \((*)\), we can write
\[ b = \frac{m}{n} = \frac{na - qm}{m - qn}. \]

This equation expresses \(b\) as a ratio of positive integers; and by \((*)\) the denominator is less than \(n\). Thus we reach a contradiction. \(\Box\)

\begin{center}
\framebox{Corollary. \(\sqrt{2}\) is irrational.}
\end{center}

\textit{Proof.} Let \(b = \sqrt{2}\). Then \(b\) cannot be an integer, for the square of 1 equals 1 while the square of any integer greater than 1 is at least 4. It follows that \(b\) is irrational. \(\Box\)

The same proof shows that the number \(\sqrt{n}\) is irrational whenever \(n\) is a positive integer less than 100 that is not one of the integers 1, 4, 9, 16, 25, 36, 49, 64, or 81.