1.2 Irrational Square Root

Prove there is no rational number whose square is 12.
Assume that there exists a rational number $x$ such that $x^2 = 12$. Since $x$ is rational, it can be written $m/n$, where $gcd(m, n) = 1$.

\[
\begin{align*}
x^2 &= 12 \\
m^2 &= 12n^2 \\
m^2 &= 3 \cdot 2^2 n^2
\end{align*}
\]

Thus $m$ must have a prime factor of 3, $m = 3k$ for some integer $k$.

\[
\begin{align*}
(3k)^2 &= 3(2n)^2 \\
3^2 k^2 &= 3 \cdot 4n^2 \\
3k^2 &= 4n^2
\end{align*}
\]

Thus $n$ must have a prime factor 3, so $gcd(m, n) \geq 3$. This is a contradiction. Therefore, there is no rational number whose square is 12.

1.3 Field Multiplication Properties (Prop 1.15)

(a) If $x \neq 0$ and $xy = xz$ then $y = z$.
Assume $x \neq 0$ and $xy = xz$, the axioms (M on p.5) give

\[
y = 1 \cdot y = \frac{x}{x} y = \frac{xy}{x} = \frac{xz}{x} = z
\]

(b) If $x \neq 0$ and $xy = x$ then $y = 1$.

\[
\begin{align*}
xy &= x \\
xy &= x \cdot 1
\end{align*}
\]

By (a) $y = 1$.

(c) If $x \neq 0$ and $xy = 1$ then $y = 1/x$.

\[
\begin{align*}
xy &= 1 \\
xy &= x \cdot \frac{1}{x}
\end{align*}
\]

By (a) $y = 1/x$.

(d) If $x \neq 0$ then $1/(1/x) = x$. 

Let $x = 1/z$, since $x \neq 0$, then $z \neq 0$. Also, let $y = \frac{1}{x}$. By (c)

\[
\begin{align*}
xy &= 1 \\
\frac{1}{x} &= 1 \\
\frac{1}{z} &= \frac{1}{1/z} = 1 \\
\frac{z \cdot 1}{1/z} &= z \\
\frac{1}{1/z} &= z
\end{align*}
\]

1.5

Let $A$ be a nonempty set of real numbers which is bounded below. Let $-A$ be the set of all numbers $-x$, where $x \in A$. Prove that

\[\inf A = -\sup(-A)\]

Let $\inf A = \alpha$. Then by definition,

\[\forall \gamma \in A, \gamma \geq \alpha\]

Now, take the negative of both sides of the inequality.

\[\forall \gamma \in A, -\gamma \leq -\alpha\]

\[\forall \gamma' \in -A, \gamma' \leq -\alpha\]

Thus $-\alpha$ is an upper bound of $-A$. Let $\beta \in \mathbb{R}, \beta < -\alpha$, then $-\beta > \alpha = \inf A$. Therefore, there exists some $\gamma \in A$ s.t. $\gamma < -\beta$. This means $-\gamma > \beta$. Since $-\gamma \in -A$, then $\beta$ is not an upper bound of $-A$.

Therefore, $-\alpha$ is the supremum of $-A$, and

\[\inf A = \alpha = -(-\alpha) = -\sup(-A)\]

1.6 Fix $b > 1$.

(a) If $m, n, p, q$ are integers, $n > 0, q > 0$, and $r = m/n = p/q$, prove that

\[(b^m)^{1/n} = (b^p)^{1/q}\]

First, I'll prove some needed properties of exponentials.

Let $x, y$ be integers and $y > 0$.

\[b^{xy} = (b^x)^y\]

This is trivially true by the definition of integer exponentiation.

\[\left((b^y)^{1/y}\right) = b\]

is trivially true by definition of $b^{1/x} = y$ s.t. $y^x = b$ (Thm 1.21).
Also, for roots let \(a, b, n \in \mathbb{Z}^+\) where \(n = ab\). Let \(x, y \in \mathbb{R}\) s.t. \(y = x^{1/n}\). This is also written \(y^n = x\).

\[
x = y^n = y^{ab}
= (y^a)^b
x^{1/b} = y^a
(x^{1/b})^{1/a} = y = x^{1/ab}
\]

Without loss of generality, also \(y = x^{1/ab} = (x^{1/a})^{1/b}\).

Let \(r = x/y\), such that \(gcd(x, y) = 1\). Let \(d = gcd(m, n)\) and \(f = gcd(p, q)\). Thus, \(m = dx, n = dy, p = fx, q = fy\).

Then, we simplify \((b^m)^{1/n}\),

\[
(b^m)^{1/n} = (b^{dx})^{1/ab}
= ((b^x)^d)^{1/ab}
= ((b^x)^d)^{1/ab}
= (b^x)^{1/ab}
\]

Similarly, simplifying \((b^p)^{1/q}\),

\[
(b^p)^{1/q} = (b^{fx})^{1/ab}
= ((b^x)^f)^{1/ab}
= ((b^x)^f)^{1/ab}
= (b^x)^{1/ab}
\]

Therefore,

\[
(b^m)^{1/n} = (b^p)^{1/q}
\]

(b) Prove that \(b^{r+s} = b^r b^s\) if \(r\) and \(s\) are rational.
Since \(r, s\) are rational, they can be written \(r = m/n\) and \(s = p/q\) where \(m, n, p, q \in \mathbb{Z}\) and \(n > 0, q > 0\).

\[
b^{r+s} = b^{m/n+p/q} = b^{m/n+p/q}
= (b^{m/n})^{m/q}
= (b^{m/q})^{m/q}
\]

by multiplicative commutativity

\[
= b^{m/m} b^{m/q} \quad \text{by corollary to Thm 1.21}
= b^{m/q} = b^r b^s
\]

(c) If \(x\) is real, define \(B(x)\) to be the set of all numbers \(b^t\), where \(t\) is rational and \(t \leq x\). Prove that

\[
b^r = \sup B(r)
\]

when \(r\) is rational.

If \(r, s \in \mathbb{Q}\) and \(s < r\),

\[
b^s - b^r = b^s - b^{r+(r-s)}
= b^s - b^{s+(r-s)}
= b^s - b^s b^{r-s}
= b^s (1 - b^{r-s})
\]
Since $b > 1$ and $r - s > 0$, then $b^{r-s} > 1$ and $b^s > 0$. Thus,

$$b^s(1 - b^r) < 0$$

Therefore $b^r$ is an upper bound of the set $B(r)$.

Now, consider $s > r$.

$$b^s - b^r = b^{s + (r - r)} - b^r = b^r b^{s-r} - b^r = b^r(b^{s-r} - 1)$$

Since $b > 1$ and $s - r > 0$, then $b^{s-r} > 1$ and $b^r > 0$. Thus,

$$b^r(b^{s-r} - 1) > 0$$

Therefore there is no $s > r$ in the set $B(r)$.

This means that we have proven

$$b^r = \sup B(r)$$

(d) Prove that $b^{x+y} = b^x b^y$ for all real $x$ and $y$.

$$b^{x+y} = \sup B(x + y)$$

This means it is the supremum of the set of all numbers $b^t$, where $t$ is rational and $r + s < x + y$.

Since every rational $t$, where $t < x + y$ can be written as the sum of two rationals $r, s$ where $r + s = t$ and $r < x$ and $s < y$, then the set $B(x + y)$ is equivalent to the set $\{b^{r+s} : (r, s) \in B(x) \times B(y)\}$.

Therefore, since $b > 1$ and all $b^s > 0$, then $\sup B(x + y) = \sup B(x) \sup B(y)$, and

$$b^{x+y} = b^x b^y$$

---

**Extra Induction Practice**

Prove that $1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$ for all positive integers $n$.

**Base Case** It can easily be shown that $1^3 = 1^2 = 1$.

**Inductive Case** Assume that for some $n \in \mathbb{Z}^+$, $1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$. Take $n + 1$, then

$$1^3 + 2^3 + ... + n^3 + (n + 1)^3 = (1 + 2 + ... + n)^2 + (n + 1)^3$$

$$= \left(\frac{n(n + 1)}{2}\right)^2 + (n + 1)^3$$

$$= \frac{n^2(n + 1)^2}{4} + (n + 1)^3$$

$$= \frac{n^2(n + 1)^2 + 4(n + 1)^3}{4}$$

$$= \frac{(n + 1)^2(n^2 + 4(n + 1))}{4}$$

$$= \frac{(n + 1)^2(n^2 + 4n + 4)}{4}$$

$$= \frac{(n + 1)^2(n + 2)^2}{4}$$

$$= (1 + 2 + ... + n + (n + 1))^2$$

Therefore, by induction, $1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$ for all positive integers $n$. 

\[ \square \]