Real Number System Theory

Jason Sass

July 3, 2023

Construction of $\mathbb{Q}$

Proposition 1. *Let $\sim$ be a relation defined for all $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ by $(a, b) \sim (c, d)$ iff $ad = bc$.*

Then $\sim$ is an equivalence relation over $\mathbb{Z} \times \mathbb{Z}^*$.

Proof. Observe that $\sim$ is a relation over $\mathbb{Z} \times \mathbb{Z}^*$.

Let $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$.

Then $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^*$, so $n \in \mathbb{Z}$ and $n \neq 0$.

Since $mn = nm$ and $n \neq 0$, then $(m, n) \sim (m, n)$.

Therefore, $\sim$ is reflexive.

Let $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$ and $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ such that $(m, n) \sim (p, q)$.

Then $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^*$ and $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$ and $mq = np$.

Since $n \in \mathbb{Z}^*$, then $n \neq 0$.

Since $q \in \mathbb{Z}^*$, then $q \neq 0$.

Observe that $pn = np = mq = qm$.

Since $pn = qm$ and $q \neq 0$ and $n \neq 0$, then $(p, q) \sim (m, n)$, so $\sim$ is symmetric.

Let $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$ and $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ and $(r, s) \in \mathbb{Z} \times \mathbb{Z}^*$ such that $(m, n) \sim (p, q)$ and $(p, q) \sim (r, s)$.

Then $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^*$ and $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$ and $r \in \mathbb{Z}$ and $s \in \mathbb{Z}^*$ and $mq = np$ and $ps = qr$.

Since $n \in \mathbb{Z}^*$, then $n \in \mathbb{Z}$ and $n \neq 0$.

Since $s \in \mathbb{Z}^*$, then $s \in \mathbb{Z}$ and $s \neq 0$.

We right multiply the equation $mq = np$ by s to obtain $mqs = nps$.

We left multiply the equation $ps = qr$ by n to obtain $nps = nqr$.

Thus, $mqs = nps$ and $nps = nqr$, so $mqs = nqr$.

Hence, $q(ms) = q(nr)$.

Since $q \in \mathbb{Z}^*$, then $q \in \mathbb{Z}$ and $q \neq 0$.

Hence, by the multiplicative cancellation law for the integral domain $\mathbb{Z}$, we obtain $ms = nr$.

Since $ms = nr$ and $n \neq 0$ and $s \neq 0$, then $(m, n) \sim (r, s)$, so $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric, and transitive, then $\sim$ is an equivalence relation over $\mathbb{Z} \times \mathbb{Z}^*$. $\square$

Proposition 2. *Addition is a binary operation on $\mathbb{Q}$.*

Proof. Let $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ be defined by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ for all $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.

To prove addition is a binary operation on $\mathbb{Q}$, we must prove $\mathbb{Q}$ is closed under addition and addition is well defined since elements of $\mathbb{Q}$ are equivalence classes.

To prove addition is well defined, we must prove if $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ for every $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in \mathbb{Q}$.

We prove $\mathbb{Q}$ is closed under addition.

Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.

Then $a,b,c,d \in \mathbb{Z}$ and $b \neq 0$ and $d \neq 0$.

By closure of $\mathbb{Z}$ under addition and multiplication, $bd \in \mathbb{Z}$ and $ad + bc \in \mathbb{Z}$.

Since the product of any two nonzero integers is nonzero and $b \neq 0$ and $d \neq 0$, then $bd \neq 0$.

Therefore, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in \mathbb{Q}$.

We prove addition over $\mathbb{Q}$ is well defined.

Let $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in \mathbb{Q}$ such that $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$.

Then $a,b,c,d,a',b',c',d' \in \mathbb{Z}$ and $b,b',d,d' \neq 0$ and $ab' = ba'$ and $cd' = dc'$.

Observe that

$$\begin{aligned}
(ad+bc)(b'd') &= (ad)(b'd') + (bc)(b'd') \\
&= a(db')d' + b(cb')d' \\
&= a(b'd)d' + b(b'c)d' \\
&= (ab')(dd') + (bb')(cd') \\
&= (ba')(dd') + (bb')(dc') \\
&= b(a'd)d' + b(b'd)c' \\
&= b(da')d' + b(db')c' \\
&= (bd)(a'd') + (bd)(b'c') \\
&= (bd)(a'd' + b'c').
\end{aligned}$$

Therefore, $(ad+bc)(b'd') = (bd)(a'd' + b'c')$.

Since the product of any two nonzero integers is nonzero and $b \neq 0$ and $d \neq 0$ and $b' \neq 0$ and $d' \neq 0$, then $bd \neq 0$ and $b'd' \neq 0$.

Since $(ad+bc)(b'd') = (bd)(a'd' + b'c')$ and $bd \neq 0$ and $b'd' \neq 0$, then $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$.

Therefore,

$$\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd} \\
&= \frac{a'd'+b'c'}{b'd'} \\
&= \frac{a'}{b'} + \frac{c'}{d'}.
\end{aligned}$$

□

Theorem 3. ***algebraic properties of addition over*** $\mathbb{Q}$

1. $\frac{m}{n} + (\frac{p}{q} + \frac{r}{s}) = (\frac{m}{n} + \frac{p}{q}) + \frac{r}{s}$ *for all* $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$. *(associative)*
2. $\frac{m}{n} + \frac{p}{q} = \frac{p}{q} + \frac{m}{n}$ *for all* $\frac{m}{n}, \frac{p}{q} \in \mathbb{Q}$. *(commutative)*
3. $\frac{m}{n} + 0 = 0 + \frac{m}{n} = \frac{m}{n}$ *for all* $\frac{m}{n} \in \mathbb{Q}$. *(additive identity)*
4. $\frac{m}{n} + \frac{-m}{n} = \frac{-m}{n} + \frac{m}{n} = 0$ *for all* $\frac{m}{n} \in \mathbb{Q}$. *(additive inverses)*

Proof. We prove addition is associative.
Let $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$.
Then $m, n, p, q, r, s \in \mathbb{Z}$ and $n, q, s \neq 0$.
Observe that

$$\begin{aligned}
(\frac{m}{n} + \frac{p}{q}) + \frac{r}{s} &= \frac{mq+np}{nq} + \frac{r}{s} \\
&= \frac{(mq+np)s + (nq)r}{(nq)s} \\
&= \frac{mqs + nps + nqr}{nqs} \\
&= \frac{m(qs) + n(ps+qr)}{n(qs)} \\
&= \frac{m}{n} + \frac{ps+qr}{qs} \\
&= \frac{m}{n} + (\frac{p}{q} + \frac{r}{s}).
\end{aligned}$$

Therefore, addition is associative. □

Proof. We prove addition is commutative.
Let $\frac{m}{n}, \frac{p}{q} \in \mathbb{Q}$.
Then $m, n, p, q \in \mathbb{Z}$ and $n, q \neq 0$.
Observe that

$$\begin{aligned}
\frac{m}{n} + \frac{p}{q} &= \frac{mq+np}{nq} \\
&= \frac{np+mq}{nq} \\
&= \frac{pn+qm}{qn} \\
&= \frac{p}{q} + \frac{m}{n}.
\end{aligned}$$

Therefore, addition is commutative. □

Proof. We prove $\frac{m}{n} + 0 = 0 + \frac{m}{n} = \frac{m}{n}$ for all $\frac{m}{n} \in \mathbb{Q}$.
Let $\frac{m}{n} \in \mathbb{Q}$.
Then $m, n \in \mathbb{Z}$ and $n \neq 0$.
Since 0 and 1 are integers and $1 \neq 0$, then $0 = \frac{0}{1} \in \mathbb{Q}$.

Observe that

$$\begin{aligned}
\frac{m}{n} + 0 &= \frac{m}{n} + \frac{0}{1} \\
&= \frac{m \cdot 1 + n \cdot 0}{n \cdot 1} \\
&= \frac{m + 0}{n} \\
&= \frac{m}{n} \\
&= \frac{0 + m}{n} \\
&= \frac{0 \cdot n + 1 \cdot m}{1 \cdot n} \\
&= \frac{0}{1} + \frac{m}{n} \\
&= 0 + \frac{m}{n}.
\end{aligned}$$

Therefore, $\frac{m}{n} + 0 = \frac{m}{n} = 0 + \frac{m}{n}$. □

Proof. We prove $\frac{m}{n} + \frac{-m}{n} = \frac{-m}{n} + \frac{m}{n} = 0$ for all $\frac{m}{n} \in \mathbb{Q}$.
Let $\frac{m}{n} \in \mathbb{Q}$.
Then $m, n \in \mathbb{Z}$ and $n \neq 0$.
Since $m \in \mathbb{Z}$, then $-m \in \mathbb{Z}$.
Since $-m$ and n are integers and $n \neq 0$, then $\frac{-m}{n} \in \mathbb{Q}$.
Since $n \in \mathbb{Z}$ and $n \neq 0$, then $n^2 \neq 0$, so $\frac{0}{n^2} = 0$.
Observe that

$$\begin{aligned}
\frac{m}{n} + \frac{-m}{n} &= \frac{-m}{n} + \frac{m}{n} \\
&= \frac{(-m)n + nm}{n^2} \\
&= \frac{-mn + mn}{n^2} \\
&= \frac{0}{n^2} \\
&= 0.
\end{aligned}$$

Therefore, $\frac{m}{n} + \frac{-m}{n} = \frac{-m}{n} + \frac{m}{n} = 0$. □

Proposition 4. *Multiplication is a binary operation on* $\mathbb{Q}$.

Proof. Let $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ be defined by $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ for all $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.

To prove multiplication is a binary operation on $\mathbb{Q}$, we must prove $\mathbb{Q}$ is closed under multiplication and multiplication is well defined since elements of $\mathbb{Q}$ are equivalence classes.

To prove multiplication is well defined, we must prove if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$ for every $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in \mathbb{Q}$.

We prove $\mathbb{Q}$ is closed under multiplication.

Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.

Then $a, b, c, d \in \mathbb{Z}$ and $b \neq 0$ and $d \neq 0$.

By closure of $\mathbb{Z}$ under multiplication, $ac \in \mathbb{Z}$ and $bd \in \mathbb{Z}$.

Since the product of any two nonzero integers is nonzero and $b, d \in \mathbb{Z}$ and $b \neq 0$ and $d \neq 0$, then $bd \neq 0$.

Therefore, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}$, as desired.

We prove multiplication over $\mathbb{Q}$ is well defined.

Let $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in \mathbb{Q}$ such that $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$.

Then $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ and $b, b', d, d' \neq 0$ and $ab' = ba'$ and $cd' = dc'$.

Observe that

$$\begin{aligned}
(ac)(b'd') &= a(cb')d' \\
&= a(b'c)d' \\
&= (ab')(cd') \\
&= (ba')(dc') \\
&= b(a'd)c' \\
&= b(da')c' \\
&= (bd)(a'c').
\end{aligned}$$

Therefore, $(ac)(b'd') = (bd)(a'c')$.

Since the product of any two nonzero integers is nonzero and $b, d, b', d' \in \mathbb{Z}$ and $b \neq 0$ and $d \neq 0$ and $b' \neq 0$ and $d' \neq 0$, then $bd \neq 0$ and $b'd' \neq 0$.

Since $(ac)(b'd') = (bd)(a'c')$ and $bd \neq 0$ and $b'd' \neq 0$, then $\frac{ac}{bd} = \frac{a'c'}{b'd'}$.

Therefore,

$$\begin{aligned}
\frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd} \\
&= \frac{a'c'}{b'd'} \\
&= \frac{a'}{b'} \cdot \frac{c'}{d'}.
\end{aligned}$$

□

Theorem 5. ***algebraic properties of multiplication over*** $\mathbb{Q}$

1. $\frac{m}{n} \cdot (\frac{p}{q} \cdot \frac{r}{s}) = (\frac{m}{n} \cdot \frac{p}{q}) \cdot \frac{r}{s}$ *for all* $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$. *(associative)*
2. $\frac{m}{n} \cdot \frac{p}{q} = \frac{p}{q} \cdot \frac{m}{n}$ *for all* $\frac{m}{n}, \frac{p}{q} \in \mathbb{Q}$. *(commutative)*
3. $\frac{m}{n} \cdot 1 = 1 \cdot \frac{m}{n} = \frac{m}{n}$ *for all* $\frac{m}{n} \in \mathbb{Q}$. *(multiplicative identity)*
4. $\frac{m}{n} \cdot 0 = 0 \cdot \frac{m}{n} = 0$ *for all* $\frac{m}{n} \in \mathbb{Q}$.
5. $\frac{m}{n} \cdot (\frac{p}{q} + \frac{r}{s}) = \frac{m}{n} \cdot \frac{p}{q} + \frac{m}{n} \cdot \frac{r}{s}$ *for all* $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$. *(left distributive)*
6. $(\frac{m}{n} + \frac{p}{q}) \cdot \frac{r}{s} = \frac{m}{n} \cdot \frac{r}{s} + \frac{p}{q} \cdot \frac{r}{s}$ *for all* $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$. *(right distributive)*

Proof. We prove multiplication is associative.
Let $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$.
Then $m, n, p, q, r, s \in \mathbb{Z}$ and $n, q, s \neq 0$.
Observe that

$$\begin{aligned}
(\frac{m}{n} \cdot \frac{p}{q})\frac{r}{s} &= \frac{mp}{nq} \cdot \frac{r}{s} \\
&= \frac{(mp)r}{(nq)s} \\
&= \frac{m(pr)}{n(qs)} \\
&= \frac{m}{n} \cdot \frac{pr}{qs} \\
&= \frac{m}{n}(\frac{p}{q} \cdot \frac{r}{s}).
\end{aligned}$$

Therefore, multiplication is associative. □

Proof. We prove multiplication is commutative.
Let $\frac{m}{n}, \frac{p}{q} \in \mathbb{Q}$.
Then $m, n, p, q \in \mathbb{Z}$ and $n, q \neq 0$.
Observe that

$$\begin{aligned}
\frac{m}{n} \cdot \frac{p}{q} &= \frac{mp}{nq} \\
&= \frac{pm}{qn} \\
&= \frac{p}{q} \cdot \frac{m}{n}.
\end{aligned}$$

Therefore, multiplication is commutative. □

Proof. We prove $\frac{m}{n} \cdot 1 = 1 \cdot \frac{m}{n} = \frac{m}{n}$ for all $\frac{m}{n} \in \mathbb{Q}$.
Let $\frac{m}{n} \in \mathbb{Q}$.
Then $m, n \in \mathbb{Z}$ and $n \neq 0$.
Since 1 is an integer and $1 \neq 0$, then $1 = \frac{1}{1} \in \mathbb{Q}$.
Observe that

$$\begin{aligned}
\frac{m}{n} \cdot 1 &= \frac{m}{n} \cdot \frac{1}{1} \\
&= \frac{m \cdot 1}{n \cdot 1} \\
&= \frac{m}{n} \\
&= \frac{1 \cdot m}{1 \cdot n} \\
&= \frac{1}{1} \cdot \frac{m}{n} \\
&= 1 \cdot \frac{m}{n}.
\end{aligned}$$

Therefore, $\frac{m}{n} \cdot 1 = \frac{m}{n} = 1 \cdot \frac{m}{n}$. ☐

Proof. We prove $\frac{m}{n} \cdot 0 = 0 \cdot \frac{m}{n} = 0$ for all $\frac{m}{n} \in \mathbb{Q}$.
Let $\frac{m}{n} \in \mathbb{Q}$.
Then $m, n \in \mathbb{Z}$ and $n \neq 0$.
Since 0 is an integer and $0 = \frac{0}{1}$ and $1 \neq 0$, then $0 = \frac{0}{1} \in \mathbb{Q}$.
Observe that

$$\begin{aligned}
\frac{m}{n} \cdot 0 &= \frac{m}{n} \cdot \frac{0}{1} \\
&= \frac{m \cdot 0}{n \cdot 1} \\
&= \frac{0}{n} \\
&= 0 \\
&= \frac{0}{n} \\
&= \frac{0 \cdot m}{1 \cdot n} \\
&= \frac{0}{1} \cdot \frac{m}{n} \\
&= 0 \cdot \frac{m}{n}.
\end{aligned}$$

Therefore, $\frac{m}{n} \cdot 0 = 0 = 0 \cdot \frac{m}{n}$. ☐

Proof. We prove $\frac{m}{n} \cdot (\frac{p}{q} + \frac{r}{s}) = \frac{m}{n} \cdot \frac{p}{q} + \frac{m}{n} \cdot \frac{r}{s}$ for all $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$.
Let $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$.
Then $m, n, p, q, r, s \in \mathbb{Z}$ and $n, q, s \neq 0$.
Since n is a nonzero integer, then $\frac{n}{n} = \frac{1}{1}$.

Observe that

$$\begin{aligned}
\frac{m}{n}(\frac{p}{q}+\frac{r}{s}) &= \frac{m}{n}\cdot\frac{ps+qr}{qs} \\
&= \frac{m(ps+qr)}{n(qs)} \\
&= \frac{mps+mqr}{nqs} \\
&= \frac{1}{1}\cdot\frac{mps+mqr}{nqs} \\
&= \frac{n}{n}\cdot\frac{mps+mqr}{nqs} \\
&= \frac{n(mps+mqr)}{n(nqs)} \\
&= \frac{nmps+nmqr}{nnqs} \\
&= \frac{n(mp)s+nqmr}{n(nq)s} \\
&= \frac{(mp)(ns)+(nq)(mr)}{(nq)(ns)} \\
&= \frac{mp}{nq}+\frac{mr}{ns} \\
&= \frac{m}{n}\cdot\frac{p}{q}+\frac{m}{n}\cdot\frac{r}{s}
\end{aligned}$$

Therefore, multiplication is left distributive over addition. $\square$

Proof. We prove $(\frac{m}{n}+\frac{p}{q})\cdot\frac{r}{s}=\frac{m}{n}\cdot\frac{r}{s}+\frac{p}{q}\cdot\frac{r}{s}$ for all $\frac{m}{n},\frac{p}{q},\frac{r}{s}\in\mathbb{Q}$.

Let $\frac{m}{n},\frac{p}{q},\frac{r}{s}\in\mathbb{Q}$.

Then $m,n,p,q,r,s\in\mathbb{Z}$ and $n,q,s\neq 0$.

Since s is a nonzero integer, then $\frac{s}{s}=\frac{1}{1}$.

Observe that

$$\begin{aligned}
(\frac{m}{n}+\frac{p}{q})\cdot\frac{r}{s} &= \frac{mq+np}{nq}\cdot\frac{r}{s} \\
&= \frac{(mq+np)r}{(nq)s} \\
&= \frac{mqr+npr}{nqs} \\
&= \frac{mqr+npr}{nqs}\cdot\frac{1}{1} \\
&= \frac{mqr+npr}{nqs}\cdot\frac{s}{s} \\
&= \frac{(mqr+npr)s}{nqss} \\
&= \frac{mqrs+nprs}{nqss} \\
&= \frac{(mr)(qs)+(ns)(pr)}{(ns)(qs)} \\
&= \frac{mr}{ns}+\frac{pr}{qs} \\
&= \frac{m}{n}\cdot\frac{r}{s}+\frac{p}{q}\cdot\frac{r}{s}
\end{aligned}$$

Therefore, multiplication is right distributive over addition. ☐

Proposition 6. $\mathbb{Q}$ ***extends*** $\mathbb{Z}$.

Let $\mathbb{Q} = \{\frac{m}{n} : n \neq 0\}$ *where* $\frac{m}{n}$ *is the class of ordered pairs* (p,q) *in* $\mathbb{Z}\times\mathbb{Z}$ *such that* $(p,q) \sim (m,n)$ *iff* $pn = qm$ *and* $q,n \neq 0$.

$\mathbb{Q}$ *extends* $\mathbb{Z}$.

Proof. Let $S = \{\frac{n}{1} : n \in \mathbb{Z}\}$.

Then $S \subset \mathbb{Q}$.

We first prove S is a subring of $\mathbb{Q}$.

Since $\frac{1}{1} \in S$, then $S \neq \emptyset$.

Let $\frac{m}{1}, \frac{n}{1} \in S$.

Then $m, n \in \mathbb{Z}$.

Observe that $\frac{m}{1} - \frac{n}{1} = \frac{m-n}{1} \in S$ since $m-n$ is an integer.

Therefore, S is closed under subtraction.

Observe that $\frac{m}{1}\cdot\frac{n}{1} = \frac{mn}{1} \in S$ since mn is an integer.

Therefore, S is closed under multiplication.

The multiplicative identity of $\mathbb{Q}$ is $\frac{1}{1}$ and $\frac{1}{1} \in S$.

Therefore, S is a subring of $\mathbb{Q}$.

We prove S is isomorphic to $\mathbb{Z}$.

Let $f : \mathbb{Z} \to S$ be defined by $f(n) = \frac{n}{1}$ for all $n \in \mathbb{Z}$.

We prove f is a ring homomorphism.

Let $m, n \in \mathbb{Z}$.

Then

$$\begin{aligned} f(m+n) &= \frac{m+n}{1} \\ &= \frac{m}{1} + \frac{n}{1} \\ &= f(m) + f(n) \end{aligned}$$

and

$$\begin{aligned} f(mn) &= \frac{mn}{1} \\ &= \frac{mn}{1 \cdot 1} \\ &= \frac{m}{1} \cdot \frac{n}{1} \\ &= f(m) \cdot f(n) \end{aligned}$$

and $f(1) = \frac{1}{1}$ and the multiplicative identity of S is $\frac{1}{1}$.
Therefore, f is a ring homomorphism from $\mathbb{Z}$ to S.
Let $m, n \in \mathbb{Z}$ such that $f(m) = f(n)$.
Then $\frac{m}{1} = \frac{n}{1}$, so $m \cdot 1 = 1 \cdot n$.
Therefore, $m = n$, so f is injective.
Let $\frac{m}{1} \in S$.
Then m is an integer.
Hence, there is an integer m such that $f(m) = \frac{m}{1}$.
Therefore, f is surjective.
Since f is injective and surjective, then f is bijective.
Since f is a bijective ring homomorphism, then f is a ring isomorphism.
Therefore, $\mathbb{Z} \cong S$. □

Ordered Fields

Proposition 7. *Positivity of $\mathbb{Q}$ is well defined.*

Proof. To prove positivity of $\mathbb{Q}$ is well defined, let $\frac{m}{n}, \frac{m'}{n'} \in \mathbb{Q}$.
Then $m, n \in \mathbb{Z}$ and $n \neq 0$ and $m', n' \in \mathbb{Z}$ and $n' \neq 0$.
We must prove if $(m, n) \sim (m', n')$, then $\frac{m}{n}$ is positive iff $\frac{m'}{n'}$ is positive.
Let $(m, n) \sim (m', n')$.
Then $\frac{m}{n} = \frac{m'}{n'}$ and $mn' = nm'$ and $n, n' \neq 0$.
Since $(m, n) \sim (m', n')$, then $(m', n') \sim (m, n)$, so $\frac{m'}{n'} = \frac{m}{n}$.
We prove if $\frac{m}{n}$ is positive, then $\frac{m'}{n'}$ is positive.
Suppose $\frac{m}{n}$ is positive.
Then there exist positive integers a and b such that $\frac{m}{n} = \frac{a}{b}$.
Since $\frac{m'}{n'} = \frac{m}{n} = \frac{a}{b}$, then there exist positive integers a and b such that $\frac{m'}{n'} = \frac{a}{b}$.
Therefore, $\frac{m'}{n'}$ is positive.

Conversely, we prove if $\frac{m'}{n'}$ is positive, then $\frac{m}{n}$ is positive.

Suppose $\frac{m'}{n'}$ is positive.

Then there exist positive integers c and d such that $\frac{m'}{n'} = \frac{c}{d}$.

Since $\frac{m}{n} = \frac{m'}{n'} = \frac{c}{d}$, then there exist positive integers c and d such that $\frac{m}{n} = \frac{c}{d}$.

Therefore, $\frac{m}{n}$ is positive. □

Proposition 8. $(\mathbb{Q}, +, \cdot)$ *is an ordered field.*

Proof. Observe that $(\mathbb{Q}, +, \cdot)$ is a field.

Let $\mathbb{Q}^+$ be the set of all positive rational numbers.

Then $\mathbb{Q}^+ = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}^+\}$, so $\mathbb{Q}^+ \subset \mathbb{Q}$.

Since $1 \in \mathbb{Z}^+$, then $\frac{1}{1} \in \mathbb{Q}^+$, so $\mathbb{Q}^+$ is not empty.

To prove $\mathbb{Q}$ is an ordered field, we must prove $\mathbb{Q}^+$ is closed under addition and multiplication of $\mathbb{Q}$ and the trichotomy law holds.

Let $u, v \in \mathbb{Q}^+$.

Then there exist positive integers a, b, c, d such that $u = \frac{a}{b}$ and $v = \frac{c}{d}$.

We prove $\mathbb{Q}^+$ is closed under addition in $\mathbb{Q}$.

Since $a, b, c, d \in \mathbb{Z}^+$, then $ad, bc, bd \in \mathbb{Z}^+$, by closure of $\mathbb{Z}^+$ under multiplication.

Thus, $ad + bc \in \mathbb{Z}^+$, by closure of $\mathbb{Z}^+$ under addition.

Observe that $u + v = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

Therefore, there exist positive integers $ad+bc$ and bd such that $u+v = \frac{ad+bc}{bd}$, so $u + v$ is positive.

We prove $\mathbb{Q}^+$ is closed under multiplication in $\mathbb{Q}$.

Since $a, b, c, d \in \mathbb{Z}^+$, then $ac \in \mathbb{Z}^+$ and $bd \in \mathbb{Z}^+$, by closure of $\mathbb{Z}^+$ under multiplication.

Observe that $uv = \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$.

Therefore, there exist positive integers ac and bd such that $uv = \frac{ac}{bd}$, so uv is positive.

To prove trichotomy, we must prove exactly one of the following holds: $q \in \mathbb{Q}^+$, $q = 0$, $-q \in \mathbb{Q}^+$ for every $q \in \mathbb{Q}$.

Let $q \in \mathbb{Q}$.

Then there exist integers a, b with $b \neq 0$ such that $q = \frac{a}{b}$.

By trichotomy of $\mathbb{Z}$, either $a > 0$ or $a = 0$ or $a < 0$.

We consider these cases separately.

Case 1: Suppose $a = 0$.

Since $b \neq 0$, then $q = \frac{a}{b} = \frac{0}{b} = 0$.

Therefore, $q = 0$.

Case 2: Suppose $a > 0$.

Then $a \in \mathbb{Z}^+$.

Since $b \neq 0$, then either $b > 0$ or $b < 0$.

If $b > 0$, then $b \in \mathbb{Z}^+$.
Hence, $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$.
Therefore, $\frac{a}{b} = q \in \mathbb{Q}^+$.
If $b < 0$, then $-b \in \mathbb{Z}^+$.
Hence, $a \in \mathbb{Z}^+$ and $-b \in \mathbb{Z}^+$.
Therefore $\frac{a}{-b} = -\frac{a}{b} = -q \in \mathbb{Q}^+$.
Case 3: Suppose $a < 0$.
Then $-a \in \mathbb{Z}^+$.
Since $b \neq 0$, then either $b > 0$ or $b < 0$.
If $b > 0$, then $b \in \mathbb{Z}^+$.
Hence, $-a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$.
Therefore, $\frac{-a}{b} = -\frac{a}{b} = -q \in \mathbb{Q}^+$.
If $b < 0$, then $-b \in \mathbb{Z}^+$.
Hence, $-a \in \mathbb{Z}^+$ and $-b \in \mathbb{Z}^+$.
Therefore $\frac{-a}{-b} = \frac{a}{b} = q \in \mathbb{Q}^+$.
Hence, either $q \in \mathbb{Q}^+$ or $q = 0$ or $-q \in \mathbb{Q}^+$.
Therefore, the trichotomy law holds. □

Proposition 9. *Let F be an ordered field with positive subset P. Then*

1. $1 \in P$.
2. *if $x \in P$, then $x^{-1} \in P$.*
3. *if $x, y \in P$, then $\frac{x}{y} \in P$.*
4. *if $x \in F$ and $x \neq 0$, then $x^2 \in P$.*
5. *if $x \in P$, then $nx \in P$ for all $n \in \mathbb{N}$.*

Proof. We prove 1.
Since F is an ordered field, then either $1 \in P$ or $1 = 0$ or $-1 \in P$.
Since F is a field, then $1 \neq 0$.
Suppose $-1 \in P$.
Since F is a ring, then $(-1)(-1) = -(-1) = 1 \in P$.
Thus, $-1 \in P$ and $1 \in P$, a violation of trichotomy.
Hence, $-1 \notin P$.
Since $1 \neq 0$ and $-1 \notin P$, then we must conclude $1 \in P$. □

Proof. We prove 2.
Suppose $x \in P$.
Then $x \neq 0$.
Since F is a field, then every nonzero element of F has a multiplicative inverse in F, so $x^{-1} \in F$.
Either $x^{-1} \in P$ or $x^{-1} = 0$ or $-x^{-1} \in P$.
Since F is a division ring and $x \neq 0$, then $x^{-1} \neq 0$.
Suppose $-x^{-1} \in P$.
Since $x \in P$ and $-x^{-1} \in P$, then $x(-x^{-1}) \in P$, so $x(-x^{-1}) = -(xx^{-1}) = -1 \in P$.
Hence, $1 \in P$ and $-1 \in P$, a violation of trichotomy.
Thus, $-x^{-1} \notin P$.
Since $x^{-1} \neq 0$ and $-x^{-1} \notin P$, then we conclude $x^{-1} \in P$. □

Proof. We prove 3.

Let $x, y \in P$.

Since $y \in P$, then $y^{-1} \in P$.

Since $x \in P$ and $y^{-1} \in P$, then $xy^{-1} = \frac{x}{y} \in P$, by closure of P under multiplication in F. □

Proof. We prove 4.

Suppose $x \in F$ and $x \neq 0$.

By trichotomy, either $x \in P$ or $x = 0$ or $-x \in P$.

Since $x \neq 0$, then either $x \in P$ or $-x \in P$.

We consider these cases separately.

Case 1: Suppose $x \in P$.

Then $x^2 = xx \in P$, by closure of P under multiplication in F.

Case 2: Suppose $-x \in P$.

Then $x^2 = xx = (-x)(-x) \in P$, by closure of P under multiplication in F.

Therefore, in all cases, $x^2 \in P$. □

Proof. We prove 5.

Let $x \in P$.

Let $S = \{n \in \mathbb{N} : nx \in P\}$.

We prove $S = \mathbb{N}$ by induction on n.

Basis:

Since $1x = x \in P$, then $1 \in S$.

Induction:

Suppose $k \in S$.

Then $k \in \mathbb{N}$ and $kx \in P$.

Since $kx \in P$ and $x \in P$, then $kx + x \in P$, by closure of P under addition in F, so $(k+1)x = kx + x \in P$.

Since $k \in \mathbb{N}$, then $k + 1 \in \mathbb{N}$.

Since $k+1 \in \mathbb{N}$ and $(k+1)x \in P$, then $k+1 \in S$, so $k \in S$ implies $k+1 \in S$.

Hence, by induction, $S = \mathbb{N}$,

Therefore, $nx \in P$ for all $n \in \mathbb{N}$. □

Proposition 10. *Let F be an ordered field with positive subset P. Then for all $a, b \in F$*

1. $a > 0$ *iff* $a \in P$.
2. $a < 0$ *iff* $-a \in P$.
3. $a < b$ *iff* $b - a > 0$.

Proof. We prove 1.

Let $a \in F$.

Observe that

$$\begin{aligned} a > 0 &\Leftrightarrow 0 < a \\ &\Leftrightarrow a - 0 \in P \\ &\Leftrightarrow a + (-0) \in P \\ &\Leftrightarrow a + 0 \in P \\ &\Leftrightarrow a \in P. \end{aligned}$$

Therefore, $a > 0$ iff $a \in P$. ☐

Proof. We prove 2.
Let $a \in F$.
Observe that $a < 0$ iff $0 - a \in P$ iff $0 + (-a) \in P$ iff $-a \in P$.
Therefore, $a < 0$ iff $-a \in P$. ☐

Proof. We prove 3.
Let $a \in F$.
Observe that $a < b$ iff $b - a \in P$ iff $b - a > 0$.
Therefore, $a < b$ iff $b - a > 0$. ☐

Lemma 11. *Let $(F, +, \cdot, <)$ be an ordered field with $a, b \in F$.*
If $a > 0$ and $b < 0$, then $ab < 0$.

Proof. Suppose $a > 0$ and $b < 0$.
Let P be the positive subset of F.
Then $a \in P$ and $-b \in P$.
Hence, by closure of P under multiplication, $a(-b) \in P$.
Since F is a ring, then $-(ab) = a(-b)$, so $-(ab) \in P$.
Therefore, $ab < 0$. ☐

Proposition 12. *positivity of a product in an ordered field*
Let $(F, +, \cdot, <)$ be an ordered field with $a, b \in F$. Then
1. $ab > 0$ iff either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$.
2. $ab < 0$ iff either $a > 0$ and $b < 0$ or $a < 0$ and $b > 0$.

Proof. We prove 1.
Let P be the positive subset of F.
Suppose either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$ and $b > 0$.
Then $a \in P$ and $b \in P$.
Hence, by closure of P under multiplication, $ab \in P$.
Therefore, $ab > 0$.
Case 2: Suppose $a < 0$ and $b < 0$.
Then $-a \in P$ and $-b \in P$.
Hence, by closure of P under multiplication, $(-a)(-b) \in P$.
Since F is a ring, then $ab = (-a)(-b)$, so $ab \in P$.
Therefore, $ab > 0$.
Thus, in all cases, $ab > 0$, as desired.

Conversely, suppose $ab > 0$.
If $a = 0$, then $ab = 0b = 0$.
Thus, $ab > 0$ and $ab = 0$, a violation of trichotomy.
Therefore, $a \neq 0$, so either $a > 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$.
Then $a \in P$, so $a^{-1} \in P$.
Hence, $a^{-1} > 0$.
Since $a^{-1} > 0$ and $ab > 0$, then $b = 1 \cdot b = (a^{-1} \cdot a)b = a^{-1} \cdot (ab) > 0$.
Therefore, $a > 0$ and $b > 0$.
Case 2: Suppose $a < 0$.
Then $-a \in P$, so $(-a)^{-1} \in P$.
Hence, $\frac{1}{-a} \in P$, so $-\frac{1}{a} \in P$.
Thus, $-(a^{-1}) \in P$, so $a^{-1} < 0$.
Since $ab > 0$ and $a^{-1} < 0$, then by the previous lemma $b = 1 \cdot b = (a^{-1} \cdot a)b = a^{-1} \cdot (ab) = ab \cdot a^{-1} < 0$.
Therefore, $a < 0$ and $b < 0$.
Thus, either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$, as desired. □

Proof. We prove 2.
Suppose either $a > 0$ and $b < 0$ or $a < 0$ and $b > 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$ and $b < 0$.
Then by the previous lemma, $ab < 0$.
Case 2: Suppose $a < 0$ and $b > 0$.
Then $b > 0$ and $a < 0$, so by the previous lemma, $ab = ba < 0$.
Therefore, in all cases, $ab < 0$, as desired.

Conversely, suppose $ab < 0$.
Then $-(ab) > 0$.
Since F is a ring, then $a(-b) = -(ab)$, so $a(-b) > 0$.
Hence, by 1, either $a > 0$ and $-b > 0$ or $a < 0$ and $-b < 0$.
Thus, either $a > 0$ and $-(-b) < 0$ or $a < 0$ and $-(-b) > 0$.
Therefore, either $a > 0$ and $b < 0$ or $a < 0$ and $b > 0$, as desired. □

Corollary 13. *Let $(F, +, \cdot, <)$ be an ordered field.*
Let $a, b \in F$.
Then $\frac{a}{b} > 0$ iff $ab > 0$.

Proof. Suppose $\frac{a}{b} > 0$.
Then $b \neq 0$, so $\frac{1}{b} \neq 0$.
Since $\frac{a}{b} = a \cdot \frac{1}{b}$, then $a \cdot \frac{1}{b} > 0$.
Thus, either $a > 0$ and $\frac{1}{b} > 0$ or $a < 0$ and $\frac{1}{b} < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$ and $\frac{1}{b} > 0$.
Since $\frac{1}{b} > 0$, then $\frac{1}{\frac{1}{b}} > 0$, so $b > 0$.

Since $a > 0$ and $b > 0$, then $ab > 0$.
Case 2: Suppose $a < 0$ and $\frac{1}{b} < 0$.
Since $\frac{1}{b} < 0$, then $\frac{1}{-b} > 0$, so $\frac{1}{\frac{1}{-b}} > 0$.
Thus, $-b > 0$.
Since $a < 0$, then $-a > 0$.
Thus, $ab = (-a)(-b) > 0$, so $ab > 0$.
Therefore, in all cases, $ab > 0$, as desired.

Conversely, suppose $ab > 0$.
Then either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$ and $b > 0$.
Since $b > 0$, then $\frac{1}{b} > 0$.
Since $a > 0$ and $\frac{1}{b} > 0$, then $\frac{a}{b} = a \cdot \frac{1}{b} > 0$.
Case 2: Suppose $a < 0$ and $b < 0$.
Since $b < 0$, then $-b > 0$, so $-\frac{1}{b} > 0$.
Since $a < 0$, then $-a > 0$.
Hence, $\frac{a}{b} = (-a)(-\frac{1}{b}) > 0$.
Therefore, in all cases, $\frac{a}{b} > 0$, as desired. ∎

Theorem 14. ***ordered fields satisfy transitivity and trichotomy laws***
Let $(F, +, \cdot, <)$ be an ordered field. Then
1. $a < a$ is false for all $a \in F$. (Therefore, $<$ is not reflexive.)
2. For all $a, b, c \in F$, if $a < b$ and $b < c$, then $a < c$. ($<$ is transitive)
3. For every $a \in F$, exactly one of the following is true (trichotomy):
i. $a > 0$
ii. $a = 0$
iii. $a < 0$
4. For every $a, b \in F$, exactly one of the following is true (trichotomy):
i. $a > b$
ii. $a = b$
iii. $a < b$

Proof. We prove 1.
Let $a \in F$.
We must prove $a < a$ is false.
Since $a < a$ iff $a - a \in P$ iff $0 \in P$ and $0 \notin P$, then $a < a$ is false. ∎

Proof. We prove 2.
Let $a, b, c \in F$ such that $a < b$ and $b < c$.
Since $a < b$, then $b - a \in P$.
Since $b < c$, then $c - b \in P$.
Hence, $(c - b) + (b - a) \in P$, by closure of P under addition of F.
Observe that $(c - b) + (b - a) = c + (-b + b) - a = c + 0 - a = c - a$.
Therefore, $c - a \in P$, so $a < c$. ∎

Proof. We prove 3.
Let $a \in F$.
By trichotomy, exactly one of the following is true: $a \in P$, $a = 0$, $-a \in P$.
Observe that $a \in P$ iff $a > 0$ and $-a \in P$ iff $a < 0$.
Therefore, exactly one of the following is true: $a > 0$, $a = 0$, $a < 0$. ☐

Proof. We prove 4.
Let $a, b \in F$.
Since F is a ring, then F is closed under subtraction, so $a - b \in F$.
Since F is an ordered field, then by trichotomy, exactly one of the following is true: $a - b \in P$, $a - b = 0$, $-(a - b) \in P$.
Observe that $a - b \in P$ iff $b < a$ iff $a > b$.
Observe that $a - b = 0$ iff $a = b$.
Observe that $-(a - b) \in P$ iff $-a + b \in P$ iff $b - a \in P$ iff $a < b$.
Therefore, exactly one of the following is true: $a > b$, $a = b$, $a < b$. ☐

Corollary 15. *Let $(F, +, \cdot, <)$ be an ordered field.*
Let $a, b \in F$.
If $0 < a < b$, then $0 < \frac{1}{b} < \frac{1}{a}$.

Proof. Suppose $0 < a < b$.
Then $0 < a$ and $a < b$, so $0 < b$.
Since $b > 0$, then $b \in P$, so $\frac{1}{b} \in P$.
Hence, $\frac{1}{b} > 0$.
Since $a > 0$ and $b > 0$, then $a \in P$ and $b \in P$, so $ab \in P$.
Since $a < b$, then $b - a \in P$.
Thus, $\frac{b-a}{ab} \in P$, so $\frac{b-a}{ab} > 0$.
Hence, $\frac{1}{a} - \frac{1}{b} > 0$, so $\frac{1}{b} < \frac{1}{a}$.
Therefore, $0 < \frac{1}{b} < \frac{1}{a}$, as desired. ☐

Theorem 16. ***order is preserved by the field operations in an ordered field***
Let $(F, +, \cdot, <)$ be an ordered field.
Let $a, b, c, d \in F$.
1. If $a < b$, then $a + c < b + c$. (preserves order for addition)
2. If $a < b$, then $a - c < b - c$. (preserves order for subtraction)
3. If $a < b$ and $c > 0$, then $ac < bc$. (preserves order for multiplication by a positive element)
4. If $a < b$ and $c < 0$, then $ac > bc$. (reverses order for multiplication by a negative element)
5. If $a < b$ and $c > 0$, then $\frac{a}{c} < \frac{b}{c}$. (preserves order for division by a positive element)

Proof. Let P be the positive subset of F.
We prove 1.
Suppose $a < b$.
Then $b - a \in P$.

Observe that $b - a = (b - a) + 0 = (b - a) + (c - c) = b - a + c - c = b + c - a - c = (b + c) - (a + c)$.
Therefore, $(b + c) - (a + c) \in P$, so $a + c < b + c$. $\square$

Proof. We prove 2.
Suppose $a < b$.
Since $c \in F$, then $-c \in F$.
Therefore, $a + (-c) < b + (-c)$, so $a - c < b - c$. $\square$

Proof. We prove 3.
Suppose $a < b$ and $c > 0$.
Since $a < b$, then $b - a \in P$.
Since $c > 0$, then $c \in P$.
Hence, $(b - a)c \in P$, by closure of P under multiplication of F.
Since $(b - a)c = bc - ac$, then $bc - ac \in P$, so $ac < bc$. $\square$

Proof. We prove 4.
Suppose $a < b$ and $c < 0$.
To prove $ac > bc$, we must prove $bc < ac$, i.e. $ac - bc \in P$.
Since $a < b$, then $b - a \in P$.
Since $c < 0$, then $-c \in P$.
Hence, $(b - a)(-c) \in P$, by closure of P under multiplication of F.
Observe that $(b - a)(-c) = b(-c) - a(-c) = -bc + ac = ac - bc$.
Therefore, $ac - bc \in P$, as desired. $\square$

Proof. We prove 5.
Suppose $a < b$ and $c > 0$.
Since $c > 0$, then $\frac{1}{c} > 0$.
Since $a < b$ and $\frac{1}{c} > 0$, then $a \cdot \frac{1}{c} < b \cdot \frac{1}{c}$.
Therefore, $\frac{a}{c} < \frac{b}{c}$. $\square$

Proposition 17. *Let $(F, +, \cdot, <)$ be an ordered field.*
Let $a, b, c, d \in F$.
1. If $a < b$ and $c < d$, then $a + c < b + d$. (adding inequalities is valid)
2. If $0 < a < b$ and $0 < c < d$, then $0 < ac < bd$.

Proof. We prove 1.
Suppose $a < b$ and $c < d$.
Since $a < b$, then $a + c < b + c$.
Since $c < d$, then $c + b < d + b$, so $b + c < b + d$.
Since $a + c < b + c$ and $b + c < b + d$, then $a + c < b + d$. $\square$

Proof. We prove 2.
Suppose $0 < a < b$ and $0 < c < d$.
We must prove $0 < ac < bd$.
Since $0 < a < b$, then $0 < a$ and $a < b$ and $0 < b$.
Since $0 < c < d$, then $0 < c$ and $c < d$.
Since $a > 0$ and $c > 0$, then $ac > 0$.

Since $a < b$ and $c > 0$, then $ac < bc$.
Since $c < d$ and $b > 0$, then $bc < bd$.
Therefore, $ac < bc$ and $bc < bd$, so $ac < bd$.
Hence, $0 < ac$ and $ac < bd$, so $0 < ac < bd$, as desired. □

Proposition 18. *Let $(F, +, \cdot, <)$ be an ordered field.*
Let $\frac{a}{b}, \frac{c}{d} \in F$ with $b, d > 0$.
Then $\frac{a}{b} < \frac{c}{d}$ iff $ad < bc$.

Proof. We must prove $\frac{a}{b} < \frac{c}{d}$ iff $ad < bc$.
We prove if $\frac{a}{b} < \frac{c}{d}$, then $ad < bc$.
Suppose $\frac{a}{b} < \frac{c}{d}$.
Then $\frac{c}{d} - \frac{a}{b} \in P$, so $\frac{cb-da}{db} \in P$.
Hence, $\frac{cb-da}{db} > 0$.
Since $b > 0$ and $d > 0$, then $db > 0$.
We multiply by positive db to get $cb - da > 0$.
Thus, $cb > da$, so $da < cb$.
Therefore, $ad < bc$, as desired.
Conversely, we prove if $ad < bc$, then $\frac{a}{b} < \frac{c}{d}$.
Suppose $ad < bc$.
Since $b > 0$, then we divide by positive b to get $\frac{ad}{b} < c$.
Since $d > 0$, then we divide by positive d to get $\frac{a}{b} < \frac{c}{d}$, as desired. □

Theorem 19. ***density of ordered fields***
Between any two distinct elements of an ordered field is a third element.

Proof. Let $(F, +, \cdot, <)$ be an ordered field.
Since $1 \in F$ and $0 \in F$ and $1 \neq 0$, then F contains at least two elements.
Let a and b be distinct elements of F.
Then $a \in F$ and $b \in F$ and $a \neq b$.
We must prove there is at least one element c of F such that $a < c < b$.
Since $a \neq b$, then either $a < b$ or $a > b$.
Without loss of generality, assume $a < b$.
Since $a \in F$ and $b \in F$, then by closure of F under addition, $a + b \in F$.
Since $1 \in F$, then by closure of F under addition, $1 + 1 \in F$.
Define 2 to be $1 + 1$.
Then $2 \in F$ and $2 = 1 + 1$.
Since $1 > 0$, then $1 + 1 > 0$, so $2 > 0$.
Let $c = \frac{a+b}{2}$.
Since $a + b \in F$ and $2 \neq 0$, then $\frac{a+b}{2} \in F$, so $c \in F$.
Since $a < b$, then $a + a < a + b$ and $a + b < b + b$.
Thus, $2a < a + b$ and $a + b < 2b$.
Since $2 > 0$, we divide by 2 to get $a < \frac{a+b}{2}$ and $\frac{a+b}{2} < b$, so $a < \frac{a+b}{2} < b$.
Therefore, $a < c < b$, as desired. □

Corollary 20. ***ordered fields are infinite***
An ordered field contains an infinite number of elements.

Proof. Let F be an ordered field.

We prove F is infinite by contradiction.

Suppose F is not infinite.

Then F is finite, so F contains a finite number of elements.

Let n be the number of distinct elements of F.

Since $1 \neq 0$ in every field, then every field contains at least two distinct elements.

Therefore, $n \in \mathbb{N}$ and $n \geq 2$.

Let $a_1, a_2, ..., a_n$ be the elements of F arranged so that the a_i element is in the i^{th} position in the order defined by $<$ over F for each $i = 1, 2, ..., n$.

Then $F = \{a_1, a_2, ..., a_n\}$ and $a_1 < a_2 < ... < a_n$.

Since $a_1 \in F$ and $a_2 \in F$ and $a_1 < a_2$, then a_1 and a_2 are distinct elements of the ordered field F.

Therefore, by the density of F, there exists at least one element $b \in F$ such that $a_1 < b < a_2$.

Hence, $a_1 < b$ and $b < a_2$.

We prove $b \neq a_i$ for each $i = 1, 2, ..., n$.

Since $a_1 < b$, then $a_1 \neq b$, so $b \neq a_1$.

Since $b < a_2$, then $b \neq a_2$.

Since $b < a_2$ and $a_2 < a_i$ for each i such that $2 < i \leq n$, then $b < a_i$ for each i such that $2 < i \leq n$.

Thus, $b \neq a_i$ for each i such that $2 < i \leq n$.

Therefore, $b \neq a_i$ for each $i = 1, 2, ..., n$, so $b \notin F$.

Hence, we have $b \in F$ and $b \notin F$, a contradiction.

Therefore, F is not finite, so F is infinite. □

Theorem 21. ***ordered fields are totally ordered***

Let $(F, +, \cdot, \leq)$ be an ordered field. Then

1. $\leq$ is a partial order over F. Therefore, $(F, \leq)$ is a poset.

2. $\leq$ is a total order over F.

Proof. We prove 1.

Let $x \in F$.

Since equality is reflexive, then $x = x$.

Hence, $x = x$ or $x < x$, so $x < x$ or $x = x$.

Therefore, $x \leq x$, so $\leq$ is reflexive.

Let $x, y \in F$ such that $x \leq y$ and $y \leq x$.

Suppose $x \neq y$.

Since $x \leq y$ and $x \neq y$, then $x < y$.

Since $y \leq x$ and $y \neq x$, then $y < x$.

Thus, $x < y$ and $x > y$, a violation of trichotomy.

Hence, $x = y$.

Therefore, $\leq$ is antisymmetric.

Let $x, y, z \in F$ such that $x \leq y$ and $y \leq z$.

Since $x \leq y$ and $y \leq z$, then $x < y$ or $x = y$ and $y < z$ or $y = z$.

Hence, either both $x < y$ or $x = y$ and $y < z$, or both $x < y$ or $x = y$ and $y = z$.

Thus, either $x < y$ and $y < z$ or $x = y$ and $y < z$ or $x < y$ and $y = z$ or $x = y$ and $y = z$.

Therefore, there are 4 cases to consider.

Case 1: Suppose $x < y$ and $y < z$.

Since $<$ is transitive, then $x < z$.

Case 2: Suppose $x < y$ and $y = z$.

Then $x < z$.

Case 3: Suppose $x = y$ and $y < z$.

Then $x < z$.

Case 4: Suppose $x = y$ and $y = z$.

Then $x = z$.

Thus, in all cases, either $x < z$ or $x = z$, so $x \leq z$.

Therefore, $\leq$ is transitive.

Since $\leq$ is reflexive, antisymmetric, and transitive, then $\leq$ is a partial order over F, so $(F, \leq)$ is a poset. □

Proof. We prove 2.

Since $(F, \leq)$ is a poset, then $\leq$ is a total order over F iff either $x \leq y$ or $y \leq x$ for all $x, y \in F$.

Thus, to prove $\leq$ is a total order, we must prove either $x \leq y$ or $y \leq x$ for all $x, y \in F$.

Let $x, y \in F$.

To prove $x \leq y$ or $y \leq x$, assume $x \leq y$ is false.

We must prove $y \leq x$.

Since $x \leq y$ is false, then x is not less than y and $x \neq y$.

Hence, by trichotomy, $x > y$.

Therefore, $y < x$, so $y \leq x$, as desired. □

Proposition 22. *Let $(F, +, \cdot, \leq)$ be an ordered field. Then*

1. $x^2 = 0$ *iff* $x = 0$.
2. $x^2 > 0$ *iff* $x \neq 0$.
3. $x^2 \geq 0$ *for all* $x \in F$.

Proof. Since F is an ordered field, then let P be the positive subset of F.

We prove 1.

Let $x \in F$.

We must prove $x^2 = 0$ iff $x = 0$.

We prove if $x = 0$, then $x^2 = 0$.

Suppose $x = 0$.

Then $x^2 = 0^2 = 0$, so $x^2 = 0$, as desired.

Conversely, we prove if $x^2 = 0$, then $x = 0$ by contrapositive.
Suppose $x \neq 0$.
Then $x^2 \in P$.
Since $x^2 \in P$ iff $x^2 > 0$, then $x^2 > 0$.
Hence, $x^2 \neq 0$, as desired. □

Proof. We prove 2.
Let $x \in F$.
We must prove $x^2 > 0$ iff $x \neq 0$.
We prove if $x \neq 0$, then $x^2 > 0$.
Suppose $x \neq 0$.
Then $x^2 \in P$.
Since $x^2 \in P$ iff $x^2 > 0$, then $x^2 > 0$, as desired.

Conversely, we prove if $x^2 > 0$, then $x \neq 0$ by contrapositive.
Suppose $x = 0$.
Then $x^2 = 0^2 = 0 \leq 0$, so $x^2 \leq 0$, as desired. □

Proof. We prove 3.
Let $x \in F$.
Then either $x = 0$ or $x \neq 0$.
We consider these cases separately.
Case 1: Suppose $x = 0$.
Since $x^2 = 0$ iff $x = 0$, then $x^2 = 0$.
Case 2: Suppose $x \neq 0$.
Since $x^2 > 0$ iff $x \neq 0$, then $x^2 > 0$.
Thus, in all cases, either $x^2 > 0$ or $x^2 = 0$.
Therefore, $x^2 \geq 0$, as desired. □

Absolute value in an ordered field

Lemma 23. *Let F be an ordered field. Let $x \in F$.*
1. *If $x < 0$, then $\frac{1}{x} < 0$.*
2. *If $x \neq 0$, then $|\frac{1}{x}| = \frac{1}{|x|}$.*

Proof. We prove 1.
Let $x \in F$.
Suppose $x < 0$.
Then $x \neq 0$.
Since F is a field and $x \neq 0$, then $\frac{1}{x} \in F$, so $x \cdot \frac{1}{x} = 1$.
Either $\frac{1}{x} > 0$ or $\frac{1}{x} = 0$ or $\frac{1}{x} < 0$.

Suppose $\frac{1}{x} = 0$.
Then $1 = x \cdot \frac{1}{x} = x \cdot 0 = 0$, so $1 = 0$.
But, $1 \neq 0$ in an ordered field, so $\frac{1}{x} \neq 0$.

Suppose $\frac{1}{x} > 0$.
Since $\frac{1}{x} > 0$ and $x < 0$, then $1 = \frac{1}{x} \cdot x < 0$, so $1 < 0$, a contradiction.
Hence, $\frac{1}{x}$ cannot be greater than zero.
Therefore, $\frac{1}{x} < 0$. □

Proof. We prove 2.
Let $x \in F$.
Suppose $x \neq 0$.
Then either $x > 0$ or $x < 0$.
We consider these cases separately.
Case 1: Suppose $x > 0$.
Then $\frac{1}{x} > 0$.
Therefore, $|\frac{1}{x}| = \frac{1}{x} = \frac{1}{|x|}$.
Case 2: Suppose $x < 0$.
Then $\frac{1}{x} < 0$.
Therefore, $|\frac{1}{x}| = -\frac{1}{x} = \frac{1}{-x} = \frac{1}{|x|}$. □

Theorem 24. ***arithmetic operations and absolute value***
Let F be an ordered field. For all $a, b \in F$
1. $|ab| = |a||b|$.
2. if $b \neq 0$, then $|\frac{a}{b}| = \frac{|a|}{|b|}$.
3. $|a|^2 = a^2$.
4. if $a \neq 0$, then $|a^n| = |a|^n$ for all $n \in \mathbb{Z}$.

Proof. We prove 1.
Let $a, b \in F$.
Either a or b is zero or neither a nor b is zero.
Hence, either $a = 0$ or $b = 0$ or $a \neq 0$ and $b \neq 0$.
Thus, either $a = 0$ or $b = 0$, or $a > 0$ or $a < 0$ and $b > 0$ or $b < 0$.
Hence, either $a = 0$ or $b = 0$ or both $a > 0$ and $b > 0$ or both $a > 0$ and $b < 0$ or both $a < 0$ and $b > 0$ or both $a < 0$ and $b < 0$.
We consider these cases separately.
We must prove $|ab| = |a||b|$.
Case 1: Suppose $a = 0$.
Then

$$\begin{aligned} |ab| &= |0 \cdot b| \\ &= |0| \\ &= 0 \\ &= 0 \cdot |b| \\ &= |0||b| \\ &= |a||b|. \end{aligned}$$

Case 2: Suppose $b = 0$.

Then

$$\begin{aligned}
|ab| &= |a \cdot 0| \\
&= |0| \\
&= 0 \\
&= |a| \cdot 0 \\
&= |a||0| \\
&= |a||b|.
\end{aligned}$$

Case 3: Suppose $a > 0$ and $b > 0$.
Then $|a| = a$ and $|b| = b$.
Since $a > 0$ and $b > 0$, then $ab > 0$.
Hence, $|ab| = ab$.
Therefore,

$$\begin{aligned}
|ab| &= ab \\
&= |a||b|.
\end{aligned}$$

Case 4: Suppose $a > 0$ and $b < 0$.
Then $|a| = a$ and $|b| = -b$.
Since $a > 0$ and $b < 0$, then $ab < 0$.
Hence, $|ab| = -ab$.
Therefore,

$$\begin{aligned}
|ab| &= -ab \\
&= a(-b) \\
&= |a||b|.
\end{aligned}$$

Case 5: Suppose $a < 0$ and $b > 0$.
Then $|a| = -a$ and $|b| = b$.
Since $a < 0$ and $b > 0$, then $ab < 0$.
Hence, $|ab| = -ab$.
Therefore,

$$\begin{aligned}
|ab| &= -ab \\
&= (-a)b \\
&= |a||b|.
\end{aligned}$$

Case 6: Suppose $a < 0$ and $b < 0$.
Then $|a| = -a$ and $|b| = -b$.
Since $a < 0$ and $b < 0$, then $ab > 0$.
Hence, $|ab| = ab$.
Therefore,

$$\begin{aligned}
|ab| &= ab \\
&= (-a)(-b) \\
&= |a||b|.
\end{aligned}$$

Therefore, in all cases, $|ab| = |a||b|$. ☐

Proof. We prove 2.
Let $a, b \in F$.
Suppose $b \neq 0$.
Then $b^{-1} = \frac{1}{b} \neq 0$, so

$$\begin{aligned} |\frac{a}{b}| &= |ab^{-1}| \\ &= |a \cdot \frac{1}{b}| \\ &= |a| \cdot |\frac{1}{b}| \\ &= |a| \cdot \frac{1}{|b|} \\ &= \frac{|a|}{|b|}. \end{aligned}$$

☐

Proof. We prove 3.
Let $a \in F$.
We must prove $|a|^2 = a^2$.
Either $a = 0$ or $a \neq 0$.
We consider these cases separately.
Case 1: Suppose $a = 0$.
Then

$$\begin{aligned} |a|^2 &= |0|^2 \\ &= 0^2 \\ &= a^2. \end{aligned}$$

Case 2: Suppose $a \neq 0$.
Then $a^2 \in F^+$, so $a^2 > 0$.
Hence,

$$\begin{aligned} |a|^2 &= |a||a| \\ &= |aa| \\ &= |a^2| \\ &= a^2. \end{aligned}$$

Therefore, in all cases, $|a|^2 = a^2$, as desired. ☐

Proof. We prove 4.
Let $a \in F$ with $a \neq 0$.
To prove $|a^n| = |a|^n$ for all $n \in \mathbb{Z}$, we prove $|a^n| = |a|^n$ for all positive integers n and $|a^0| = |a|^0$ and $|a^n| = |a|^n$ for all negative integers n.

We prove $|a^0| = |a|^0$.
Since $a \neq 0$, then $|a^0| = |1| = 1 = |a|^0$.
Therefore, $|a^0| = |a|^0$.

We prove $|a^n| = |a|^n$ for all $n \in \mathbb{N}$ by induction on n.
Let $S = \{n \in \mathbb{N} : |a^n| = |a|^n\}$.
Basis:
Since $|a^1| = |a| = |a|^1$, then $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{N}$ and $|a^k| = |a|^k$.
Since $k \in \mathbb{N}$, then $k+1 \in \mathbb{N}$.
Observe that

$$\begin{aligned} |a^{k+1}| &= |a^k a| \\ &= |a^k||a| \\ &= |a|^k|a| \\ &= |a|^{k+1}. \end{aligned}$$

Since $k+1 \in \mathbb{N}$ and $|a^{k+1}| = |a|^{k+1}$, then $k+1 \in S$.
Thus, $k \in S$ implies $k+1 \in S$.
Since $1 \in S$ and $k \in S$ implies $k+1 \in S$, then by PMI, $S = \mathbb{N}$.
Therefore, $|a^n| = |a|^n$ for all $n \in \mathbb{N}$.

We prove $|a^n| = |a|^n$ for all negative integers n.
Let n be an arbitrary negative integer.
Then $n \in \mathbb{Z}$ and $n < 0$.
Since $n \in \mathbb{Z}$, then $-n \in \mathbb{Z}$ and $-n > 0$.
Let $k = -n$.
Then $k \in \mathbb{Z}$ and $k > 0$ and $n = -k$.
Since $k \in \mathbb{Z}$ and $k > 0$, then k is a positive integer, so $|a^k| = |a|^k$.
Since $a \neq 0$, then $a^k \neq 0$.

Observe that

$$\begin{aligned} |a^n| &= |a^{-k}| \\ &= |\frac{1}{a^k}| \\ &= \frac{1}{|a^k|} \\ &= \frac{1}{|a|^k} \\ &= \frac{1}{|a|^{-n}} \\ &= \frac{1}{\frac{1}{|a|^n}} \\ &= |a|^n. \end{aligned}$$

Therefore, $|a^n| = |a|^n$. ☐

Theorem 25. ***properties of the absolute value function***

Let $(F, +, \cdot, \leq)$ be an ordered field.
Let $a, k \in F$ and $k > 0$. Then

1. $|a| \geq 0$.
2. $|a| = 0$ *iff* $a = 0$.
3. $|-a| = |a|$.
4. $-|a| \leq a \leq |a|$.
5. $|a| < k$ *iff* $-k < a < k$.
6. $|a| > k$ *iff* $a > k$ *or* $a < -k$.
7. $|a| = k$ *iff* $a = k$ *or* $a = -k$.

Proof. We prove 1.
Let $a \in F$.
Either $a > 0$ or $a = 0$ or $a < 0$.
We consider these cases separately.
We must prove either $|a| > 0$ or $|a| = 0$.
Case 1: Suppose $a > 0$.
Then $|a| = a > 0$.
Case 2: Suppose $a = 0$.
Then $|a| = a = 0$.
Case 3: Suppose $a < 0$.
Since $-a > 0$ iff $-a \in F^+$ iff $a < 0$ and $a < 0$, then $-a > 0$.
Since $a < 0$, then $|a| = -a > 0$.
Therefore, in all cases, $|a| \geq 0$. ☐

Proof. We prove 2.
Let $a \in F$.
We must prove $|a| = 0$ iff $a = 0$.
We prove if $a = 0$, then $|a| = 0$.

Suppose $a = 0$.
Then $|a| = a = 0$.
Conversely, we prove if $|a| = 0$, then $a = 0$ by contrapositive.
Suppose $a \neq 0$.
We must prove $|a| \neq 0$.
Since $a \neq 0$, then either $a > 0$ or $a < 0$.
In either case $|a| > 0$.
Therefore, by trichotomy, $|a| \neq 0$, as desired. □

Proof. We prove 3.
Let $a \in F$.
We must prove $|-a| = |a|$.
Either $a > 0$ or $a = 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$.
Then $-a < 0$.
Therefore, $|-a| = -(-a) = a = |a|$.
Case 2: Suppose $a = 0$.
Then $|-a| = |-0| = |0| = |a|$.
Case 3: Suppose $a < 0$.
Then $-a > 0$ and $|a| = -a$.
Therefore, $|-a| = -a = |a|$.
Hence, in all cases, $|-a| = |a|$. □

Proof. We prove 4.
Let $a \in F$.
To prove $-|a| \leq a \leq |a|$, we must prove $-|a| \leq a$ and $a \leq |a|$.
Either $a \geq 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a \geq 0$.
Then $|a| = a$ and $-a \leq 0$.
Since $a \leq a$ and $a = |a|$, then $a \leq |a|$, as desired.
Since $-a \leq 0$ and $0 \leq a$, then $-a \leq a$, so $-|a| \leq a$, as desired.
Case 2: Suppose $a < 0$.
Then $|a| = -a$ and $-a > 0$.
Since $a < 0$ and $0 < -a$, then $a < -a = |a|$, so $a \leq |a|$, as desired.
Since $a \leq a$, then $-(-a) \leq a$, so $-|a| \leq a$, as desired. □

Proof. We prove 5.
Let $a, k \in F$ with $k > 0$.
We must prove $|a| < k$ iff $-k < a < k$.
We prove if $|a| < k$, then $-k < a < k$.
Suppose $|a| < k$.
We must prove $-k < a$ and $a < k$.
Either $a \geq 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a \geq 0$.

Then $a = |a| < k$.
Therefore, $a < k$, as desired.
Since $k > 0$, then $-k < 0$.
Since $-k < 0$ and $0 \leq a$, then $-k < a$, as desired.
Case 2: Suppose $a < 0$.
Since $a < 0$ and $0 < k$, then $a < k$, as desired.
Since $|a| < k$, then $k > |a| = -a$, so $k > -a$.
Therefore, $-k < a$, as desired.

Conversely, we prove if $-k < a < k$, then $|a| < k$.
Suppose $-k < a < k$.
Then $-k < a$ and $a < k$.
We must prove $|a| < k$.
Either $a \geq 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a \geq 0$.
Then $|a| = a < k$.
Therefore, $|a| < k$, as desired.
Case 2: Suppose $a < 0$.
Since $-k < a$, then $k > -a = |a|$, so $k > |a|$.
Therefore, $|a| < k$, as desired. □

Proof. We prove 6.
Let $a, k \in F$ with $k > 0$.
We must prove $|a| > k$ iff $a > k$ or $a < -k$.

We prove if $|a| > k$, then $a > k$ or $a < -k$.
Suppose $|a| > k$.
Either $a \geq 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a \geq 0$.
Then $a = |a| > k$.
Case 2: Suppose $a < 0$.
Then $-a = |a| > k$, so $-a > k$.
Hence, $a < -k$.
Therefore, either $a > k$ or $a < -k$, as desired.

Conversely, to prove if $a > k$ or $a < -k$, then $|a| > k$, we must prove both if $a > k$, then $|a| > k$ and if $a < -k$, then $|a| > k$.

We first prove if $a > k$, then $|a| > k$.
Suppose $a > k$.
Since $a > k$ and $k > 0$, then $a > 0$.
Therefore, $|a| = a > k$.

We next prove if $a < -k$, then $|a| > k$.
Suppose $a < -k$.
Then $-a > k$.
Since $-a > k$ and $k > 0$, then $-a > 0$.
Hence, $a < 0$.
Therefore, $|a| = -a > k$. □

Proof. We prove 7.
Let $a, k \in F$ with $k > 0$.
We must prove $|a| = k$ iff $a = k$ or $a = -k$.

To prove if $a = k$ or $a = -k$, then $|a| = k$, we must prove both if $a = k$, then $|a| = k$ and if $a = -k$, then $|a| = k$.
We first prove if $a = k$, then $|a| = k$.
Suppose $a = k$.
Since $k > 0$, then $|k| = k$.
Therefore, $|a| = |k| = k$.

We next prove if $a = -k$, then $|a| = k$.
Suppose $a = -k$.
Since $k > 0$, then $-k < 0$, so $a < 0$.
Therefore, $|a| = -a = k$.

Conversely, we prove if $|a| = k$, then either $a = k$ or $a = -k$.
Suppose $|a| = k$.
Either $a \geq 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a \geq 0$.
Then $k = |a| = a$, so $a = k$.
Case 2: Suppose $a < 0$.
Then $-a = |a| = k$, so $-a = k$.
Hence, $a = -k$.
Therefore, either $a = k$ or $a = -k$, as desired. □

Theorem 26. *triangle inequality*
Let $(F, +, \cdot, \leq)$ be an ordered field.
Let $a, b \in F$. Then $|a + b| \leq |a| + |b|$.

Proof. Let $a, b \in F$.
Since $a \in F$, then $-|a| \leq a \leq |a|$.
Since $b \in F$, then $-|b| \leq b \leq |b|$.
We add these inequalities to get $-(|a| + |b|) \leq a + b \leq |a| + |b|$.
Therefore, $|a + b| \leq |a| + |b|$. □

Corollary 27. *Let $(F, +, \cdot, \leq)$ be an ordered field. Then*
1. $|a - b| \geq |a| - |b|$ and $|a - b| \geq |b| - |a|$ for all $a, b \in F$.
2. $||a| - |b|| \leq |a - b| \leq |a| + |b|$ for all $a, b \in F$.

Proof. We prove 1.

Let $a, b \in F$.

Since $|a| = |(a-b)+b| \leq |a-b|+|b|$, then $|a| \leq |a-b|+|b|$, so $|a|-|b| \leq |a-b|$.

Hence, $|a-b| \geq |a|-|b|$, so $|a-b| \geq |a|-|b|$ for all $a, b \in F$.

Since $|a-b| \geq |a|-|b|$ for all $a, b \in F$, then in particular, if we switch roles of a and b, we have $|b-a| \geq |b|-|a|$.

Therefore, $|a-b| \geq |b|-|a|$. □

Proof. We prove 2.

Let $a, b \in F$.

We first prove $||a|-|b|| \leq |a-b|$.

Since $|a-b| \geq |a|-|b|$, then $|a|-|b| \leq |a-b|$.

Since $|a-b| \geq |b|-|a|$, then $-|a-b| \leq |a|-|b|$.

Thus, $-|a-b| \leq |a|-|b|$ and $|a|-|b| \leq |a-b|$, so $-|a-b| \leq |a|-|b| \leq |a-b|$.

Therefore, $||a|-|b|| \leq |a-b|$.

We next prove $|a-b| \leq |a|+|b|$.

Since $|a-b| = |a+(-b)| \leq |a|+|-b| = |a|+|b|$, then $|a-b| \leq |a|+|b|$.

Therefore, $||a|-|b|| \leq |a-b| \leq |a|+|b|$. □

Corollary 28. ***generalized triangle inequality***

Let $(F, +, \cdot, \leq)$ be an ordered field.

Let $n \in \mathbb{N}$.

Let $x_1, x_2, ..., x_n \in F$. Then

$|x_1 + x_2 + ... + x_n| \leq |x_1| + |x_2| + ... + |x_n|$.

Proof. Define predicate $p(n) : |x_1 + x_2 + ... + x_n| \leq |x_1| + |x_2| + ... + |x_n|$ over $\mathbb{N}$.

We prove $p(n)$ for all $n \in \mathbb{N}$ by induction on n.

Basis: Since $|x_1| = |x_1|$, then $|x_1| \leq |x_1|$.

Therefore, $p(1)$ is true.

Induction: Let $n \in \mathbb{N}$ such that $p(n)$ is true.

Then $|x_1 + x_2 + ... + x_n| \leq |x_1| + |x_2| + ... + |x_n|$.

To prove $p(n+1)$ is true, we must prove

$|x_1 + x_2 + ... + x_{n+1}| \leq |x_1| + |x_2| + ... + |x_{n+1}|$.

Observe that

$$\begin{aligned} |x_1 + x_2 + ... + x_{n+1}| &= |(x_1 + x_2 + ... + x_n) + x_{n+1}| \\ &\leq |x_1 + x_2 + ... + x_n| + |x_{n+1}| \\ &\leq |x_1| + |x_2| + ... + |x_n| + |x_{n+1}|. \end{aligned}$$

Thus, $p(n+1)$ is true, so $p(n)$ implies $p(n+1)$ for all $n \in \mathbb{N}$.

Hence, by induction, $p(n)$ is true for all $n \in \mathbb{N}$.

Therefore, $|x_1 + x_2 + ... + x_n| \leq |x_1| + |x_2| + ... + |x_n|$ for all $n \in \mathbb{N}$. □

Boundedness of sets in an ordered field

Theorem 29. *A subset S of an ordered field F is bounded in F iff S is bounded above and below in F.*

Proof. Let S be a subset of an ordered field F.

We prove if S is bounded in F, then S is bounded above and below in F.

Suppose S is bounded in F.

Then there exists $b \in F$ such that $|x| \leq b$ for all $x \in S$.

Thus, $-b \leq x \leq b$ for all $x \in S$, so $-b \leq x$ and $x \leq b$ for all $x \in S$.

Hence, $-b \leq x$ for all $x \in S$ and $x \leq b$ for all $x \in S$.

Since $b \in F$ and $x \leq b$ for all $x \in S$, then b is an upper bound of S, so S is bounded above in F.

Since $-b \in F$ and $-b \leq x$ for all $x \in S$, then $-b$ is a lower bound of S, so S is bounded below in F.

Conversely, we prove if S is bounded above and below in F, then S is bounded in F.

Suppose S is bounded above and below in F.

Then there is at least one upper and lower bound of S in F.

Let M be an upper bound of S in F.

Let m be a lower bound of S in F.

To prove S is bounded, we must prove there exists $b \in F$ such that $|x| \leq b$ for all $x \in S$.

Let $b = \max\{|M|, |m|\}$.

Then $|m| \leq b$ and $|M| \leq b$.

Since $|M|, |m| \in F$ and either $b = |M|$ or $b = |m|$, then $b \in F$.

Let $x \in S$.

Since m is a lower bound of S and M is an upper bound of S, then $m \leq x \leq M$.

Since $|m| \leq b$, then $-|m| \geq -b$.

Observe that

$-b \leq -|m| \leq m \leq x \leq M \leq |M| \leq b$.

Hence, $-b \leq x \leq b$, so $|x| \leq b$, as desired. □

Proposition 30. *Every element of an ordered field is an upper and lower bound of $\emptyset$.*

Proof. Let $(F, +, \cdot, \leq)$ be an ordered field.

Since $\leq$ is a partial order over F, then $(F, \leq)$ is a partially ordered set.

Since every element of a partially ordered set is an upper and lower bound of $\emptyset$, then in particular, every element of $(F, \leq)$ is an upper and lower bound of $\emptyset$. □

Proposition 31. *A subset of a bounded set is bounded.*

Let A be a bounded subset of an ordered field F.

If $B \subset A$, then B is bounded in F.

Proof. Suppose $B \subset A$.

Let $x \in B$.

Since $B \subset A$, then $x \in A$.

Since A is bounded in F, then there exists $M \in F$ such that $|x| \leq M$ for all $x \in A$.

Since $x \in A$, then $|x| \leq M$.

Since x is arbitrary, then $|x| \leq M$ for all $x \in B$.

Therefore, there is $M \in F$ such that $|x| \leq M$ for all $x \in B$, so B is bounded in F. $\square$

Proposition 32. ***A union of bounded sets is bounded.***

Let A and B be subsets of an ordered field F.

If A and B are bounded, then $A \cup B$ is bounded.

Proof. Suppose A and B are bounded.

Either $A = \emptyset$ or $A \neq \emptyset$ and either $B = \emptyset$ or $B \neq \emptyset$.

Hence, either $A = \emptyset$ and $B = \emptyset$ or $A = \emptyset$ and $B \neq \emptyset$ or $A \neq \emptyset$ and $B = \emptyset$ or $A \neq \emptyset$ and $B \neq \emptyset$.

Thus, we have 4 cases to consider:

Case 1: Suppose $A = \emptyset$ and $B = \emptyset$.

Then $A \cup B = \emptyset \cup \emptyset = \emptyset$.

Since the empty set is bounded, then $A \cup B$ is bounded.

Case 2: Suppose $A = \emptyset$ and $B \neq \emptyset$.

Then $A \cup B = \emptyset \cup B = B$.

Since B is bounded, then $A \cup B$ is bounded.

Case 3: Suppose $A \neq \emptyset$ and $B = \emptyset$.

Then $A \cup B = A \cup \emptyset = A$.

Since A is bounded, then $A \cup B$ is bounded.

Case 4: Suppose $A \neq \emptyset$ and $B \neq \emptyset$.

Since $A \neq \emptyset$, then there exists $a \in A$.

Since $A \subset A \cup B$, then $a \in A \cup B$, so $A \cup B \neq \emptyset$.

Since A is bounded, then there exists $\alpha \in F$ such that $|x| \leq \alpha$ for all $x \in A$.

Since B is bounded, then there exists $\beta \in F$ such that $|x| \leq \beta$ for all $x \in B$.

Let $S = \{\alpha, \beta\}$.

Let $\gamma = \max S$.

Let $x \in A \cup B$ be given.

Then either $x \in A$ or $x \in B$.

We consider these cases separately.

Case 4a: Suppose $x \in A$.

Then $|x| \leq \alpha$.

Since $\alpha \leq \max S$, then $|x| \leq \max S$.

Case 4b: Suppose $x \in B$.

Then $|x| \leq \beta$.

Since $\beta \leq \max S$, then $|x| \leq \max S$.

Hence, in all cases, $|x| \leq \max S$.

Thus, there exists $\max S$ such that $|x| \leq \max S$ for all $x \in A \cup B$, so $A \cup B$ is bounded. $\square$

Theorem 33. *uniqueness of least upper bound in an ordered field*
A least upper bound of a subset of an ordered field, if it exists, is unique.

Proof. Let S be a subset of an ordered field F.
We prove if a least upper bound of S exists, then it is unique.
Suppose a least upper bound of S exists in F.
Then there is at least one least upper bound of S in F.
Uniqueness:
To prove a least upper bound is unique, let L_1 and L_2 be least upper bounds of S in F.
We must prove $L_1 = L_2$.
Since L_1 is a least upper bound of S, then L_1 is an upper bound of S and $L_1 \leq M$ for any upper bound M of S.
Since L_2 is a least upper bound of S, then L_2 is an upper bound of S and $L_2 \leq M$ for any upper bound M of S.
Since $L_1 \leq M$ for any upper bound M of S and L_2 is an upper bound of S, then $L_1 \leq L_2$.
Since $L_2 \leq M$ for any upper bound M of S and L_1 is an upper bound of S, then $L_2 \leq L_1$.
Since $L_1 \leq L_2$ and $L_2 \leq L_1$, then by the anti-symmetric property of $\leq$, we have $L_1 = L_2$. □

Theorem 34. *uniqueness of greatest lower bound in an ordered field*
A greatest lower bound of a subset of an ordered field, if it exists, is unique.

Proof. Let S be a subset of an ordered field F.
We prove if a greatest lower bound of S exists, then it is unique.
Suppose a greatest lower bound of S exists in F.
Then there is at least one greatest lower bound of S in F.
Uniqueness:
To prove a greatest lower bound is unique, let L_1 and L_2 be greatest lower bounds of S in F.
We must prove $L_1 = L_2$.
Since L_1 is a greatest lower bound of S, then L_1 is a lower bound of S and $M \leq L_1$ for any lower bound M of S.
Since L_2 is a greatest lower bound of S, then L_2 is a lower bound of S and $M \leq L_2$ for any lower bound M of S.
Since $M \leq L_2$ for any lower bound M of S and L_1 is a lower bound of S, then $L_1 \leq L_2$.
Since $M \leq L_1$ for any lower bound M of S and L_2 is a lower bound of S, then $L_2 \leq L_1$.
Since $L_1 \leq L_2$ and $L_2 \leq L_1$, then by the anti-symmetric property of $\leq$, we have $L_1 = L_2$. □

Proposition 35. *1. There is no least upper bound of $\emptyset$ in an ordered field.*
2. There is no greatest lower bound of $\emptyset$ in an ordered field.

Proof. Let F be an ordered field.

We prove 1 by contradiction.

Suppose there is a least upper bound of $\emptyset$ in F.

Let b be the least upper bound of $\emptyset$ in F.

Then $b \in F$ and no element of F less than b is an upper bound of $\emptyset$.

Since $b - 1 \in F$ and $b - 1 < b$, then this implies $b - 1$ is not an upper bound of $\emptyset$.

Since every element of F is an upper bound of $\emptyset$ and $b - 1 \in F$, then $b - 1$ is an upper bound of $\emptyset$.

Thus, we have $b - 1$ is an upper bound of $\emptyset$ and $b - 1$ is not an upper bound of $\emptyset$, a contradiction.

Therefore, there is no least upper bound of $\emptyset$ in F. □

Proof. We prove 2 by contradiction.

Suppose there is a greatest lower bound of $\emptyset$ in F.

Let b be the greatest lower bound of $\emptyset$ in F.

Then $b \in F$ and no element of F greater than b is a lower bound of $\emptyset$.

Since $b + 1 \in F$ and $b + 1 > b$, then this implies $b + 1$ is not a lower bound of $\emptyset$.

Since every element of F is a lower of $\emptyset$ and $b + 1 \in F$, then $b + 1$ is a lower bound of $\emptyset$.

Thus, we have $b + 1$ is a lower bound of $\emptyset$ and $b + 1$ is not a lower bound of $\emptyset$, a contradiction.

Therefore, there is no greatest lower bound of $\emptyset$ in F. □

Theorem 36. ***approximation property of suprema and infima***

Let S be a subset of an ordered field F.

1. If $\sup S$ exists, then $(\forall \epsilon > 0)(\exists x \in S)(\sup S - \epsilon < x \leq \sup S)$.

2. If $\inf S$ exists, then $(\forall \epsilon > 0)(\exists x \in S)(\inf S \leq x < \inf S + \epsilon)$.

Proof. We prove 1.

Suppose $\sup S$ exists.

Then $\sup S \in F$.

Let $\epsilon > 0$ be given.

Then $\sup S + \epsilon > \sup S$, so $\sup S > \sup S - \epsilon$.

Since $\sup S$ is the least upper bound of S, then $\sup S \leq B$ for every upper bound B of S, so there is no upper bound B of S such that $\sup S > B$.

Since $\sup S > \sup S - \epsilon$, then this implies $\sup S - \epsilon$ cannot be an upper bound of S.

Hence, there exists $x \in S$ such that $x > \sup S - \epsilon$.

Since $\sup S$ is an upper bound of S and $x \in S$, then $x \leq \sup S$.

Therefore, $\sup S - \epsilon < x \leq \sup S$. □

Proof. We prove 2.

Suppose $\inf S$ exists.

Then $\inf S \in F$.

Let $\epsilon > 0$ be given.

Then $\inf S + \epsilon > \inf S$.

Since $\inf S$ is the greatest lower bound of S, then $B \leq \inf S$ for every lower bound B of S, so there is no lower bound B of S such that $B > \inf S$.

Since $\inf S + \epsilon > \inf S$, then this implies $\inf S + \epsilon$ cannot be a lower bound of S.

Hence, there exists $x \in S$ such that $x < \inf S + \epsilon$.

Since $\inf S$ is a lower bound of S and $x \in S$, then $\inf S \leq x$.

Therefore, $\inf S \leq x < \inf S + \epsilon$. ☐

Proposition 37. *Let S be a subset of an ordered field F.*

If $\sup S$ and $\inf S$ exist, then $\inf S \leq \sup S$.

Proof. Suppose $\sup S$ and $\inf S$ exist.

Then $\sup S \in F$ and $\inf S \in F$ and $S \neq 0$.

Let $x \in S$ be given.

Since $\inf S$ is a lower bound of S and $x \in S$, then $\inf S \leq x$.

Since $\sup S$ is an upper bound of S and $x \in S$, then $x \leq \sup S$.

Therefore, $\inf S \leq x \leq \sup S$, so $\inf S \leq \sup S$. ☐

Proposition 38. *Let S be a subset of an ordered field F.*

Let $-S = \{-s : s \in S\}$.

1. If $\inf S$ exists, then $\sup(-S) = -\inf S$.

2. If $\sup S$ exists, then $\inf(-S) = -\sup S$.

Proof. We prove 1.

Suppose $\inf S$ exists.

Then $\inf S \in F$ and $S \neq \emptyset$.

Since $S \neq \emptyset$, then there exists $s \in S$, so $-s \in -S$.

Hence, the set $-S$ is not empty.

Let $x \in -S$.

Then there exists $s \in S$ such that $x = -s$.

Since $\inf S$ is a lower bound of S and $s \in S$, then $\inf S \leq s$, so $-\inf S \geq -s$.

Thus, $-\inf S \geq x$, so $x \leq -\inf S$.

Therefore, $-\inf S$ is an upper bound of $-S$.

We prove $-\inf S$ is the least upper bound of $-S$.

Let $\epsilon > 0$.

Since $\inf S$ is the greatest lower bound of S and $\inf S+\epsilon > \inf S$, then $\inf S+\epsilon$ is not a lower bound of S, so there exists $s' \in S$ such that $s' < \inf S + \epsilon$.

Hence, there exists $-s' \in -S$ such that $-s' > -\inf S - \epsilon$.

Therefore, $-\inf S$ is the least upper bound of $-S$, so $\sup(-S) = -\inf S$. ☐

Proof. We prove 2.

Suppose $\sup S$ exists.

Then $\sup S \in F$ and $S \neq \emptyset$.

Since $S \neq \emptyset$, then there exists $s \in S$, so $-s \in -S$.

Hence, the set $-S$ is not empty.

Let $x \in -S$.
Then there exists $s \in S$ such that $x = -s$.
Since $\sup S$ is an upper bound of S and $s \in S$, then $s \leq \sup S$, so $-s \geq -\sup S$.
Thus, $x \geq -\sup S$, so $-\sup S \leq x$.
Therefore, $-\sup S$ is a lower bound of $-S$.

We prove $-\sup S$ is the greatest lower bound of $-S$.
Let $\epsilon > 0$.
Since $\sup S$ is the least upper bound of S and $\sup S - \epsilon < \sup S$, then $\sup S - \epsilon$ is not an upper bound of S, so there exists $s' \in S$ such that $s' > \sup S - \epsilon$.
Hence, there exists $-s' \in -S$ such that $-s' < -\sup S + \epsilon$.
Therefore, $-\sup S$ is the greatest lower bound of $-S$, so $\inf(-S) = -\sup S$.
□

Lemma 39. *Let S be a subset of an ordered field F.*
Let $k \in F$.
Let $K = \{k\}$.
Let $k + S = \{k + s : s \in S\}$.
Let $K + S = \{k + s : k \in K, s \in S\}$. Then
1. $\sup K = k$.
2. $\inf K = k$.
3. $k + S = K + S$.

Proof. We prove 1.
Since $k \leq k$, then k is an upper bound of K.
Let M be an arbitrary upper bound of K.
Then $k \leq M$.
Since k is an upper bound of K and $k \leq M$, then k is the least upper bound of K, so $k = \sup K$. □

Proof. We prove 2.
Since $k \leq k$, then k is a lower bound of K.
Let M be an arbitrary lower bound of K.
Then $M \leq k$.
Since k is a lower bound of K and $M \leq k$, then k is the greatest lower bound of K, so $k = \inf K$. □

Proof. We prove 3.
Let $x \in k + S$.
Then there exists $s \in S$ such that $x = k + s$.
Since $k \in K$ and $s \in S$ and $x = k + s$, then $x \in K + S$.
Therefore, $k + S$ is a subset of $K + S$.

Let $y \in K + S$.
Then there exists $s \in S$ such that $y = k + s$, so $y \in k + S$.
Therefore, $K + S$ is a subset of $k + S$.

Since $k + S$ is a subset of $K + S$ and $K + S$ is a subset of $k + S$, then $k + S = K + S$. ☐

Proposition 40. ***additive property of suprema and infima***

Let A and B be subsets of an ordered field F.

Let $A + B = \{a + b : a \in A, b \in B\}$.

1. If $\sup A$ and $\sup B$ exist, then $\sup(A + B) = \sup A + \sup B$.

2. If $\inf A$ and $\inf B$ exist, then $\inf(A + B) = \inf A + \inf B$.

Proof. We prove 1.

Suppose $\sup A$ and $\sup B$ exist in F.

Since $\sup A$ exists in F, then $A \neq \emptyset$, so there exists $a \in A$.

Since $\sup B$ exists in F, then $B \neq \emptyset$, so there exists $b \in B$.

Thus, there exists $a + b \in A + B$, so the set $A + B$ is not empty.

Let $c \in A + B$.

Then there exist $a \in A$ and $b \in B$ such that $c = a + b$.

Since $a \in A$ and $\sup A$ is an upper bound of A, then $a \leq \sup A$.

Since $b \in B$ and $\sup B$ is an upper bound of B, then $b \leq \sup B$.

Hence, $a + b \leq \sup A + \sup B$.

Thus, $c \leq \sup A + \sup B$.

Therefore, $\sup A + \sup B$ is an upper bound of $A + B$.

We prove $\sup A + \sup B$ is the least upper bound of $A + B$.

Let $\epsilon > 0$.

Then $\frac{\epsilon}{2} > 0$.

Since $\sup A$ is the least upper bound of A, then there exists $x \in A$ such that $x > \sup A - \frac{\epsilon}{2}$.

Since $\sup B$ is the least upper bound of B, then there exists $y \in B$ such that $y > \sup B - \frac{\epsilon}{2}$.

Thus, $x + y > (\sup A - \frac{\epsilon}{2}) + (\sup B - \frac{\epsilon}{2})$.

Hence, there exists $x + y \in A + B$ such that $x + y > (\sup A + \sup B) - \epsilon$.

Therefore, $\sup A + \sup B$ is the least upper bound of $A + B$, so $\sup A + \sup B = \sup(A + B)$. ☐

Proof. We prove 2.

Suppose $\inf A$ and $\inf B$ exist in F.

Since $\inf A$ exists in F, then $A \neq \emptyset$, so there exists $a \in A$.

Since $\inf B$ exists in F, then $B \neq \emptyset$, so there exists $b \in B$.

Thus, there exists $a + b \in A + B$, so the set $A + B$ is not empty.

Let $c \in A + B$.

Then there exist $a \in A$ and $b \in B$ such that $c = a + b$.

Since $a \in A$ and $\inf A$ is a lower bound of A, then $\inf A \leq a$.

Since $b \in B$ and $\inf B$ is a lower bound of B, then $\inf B \leq b$.

Hence, $\inf A + \inf B \leq a + b$.

Thus, $\inf A + \inf B \leq c$.

Therefore, $\inf A + \inf B$ is a lower bound of $A + B$.

We prove $\inf A + \inf B$ is the greatest lower bound of $A + B$.

Let $\epsilon > 0$.

Then $\frac{\epsilon}{2} > 0$.

Since $\inf A$ is the greatest lower bound of A, then there exists $x \in A$ such that $x < \inf A + \frac{\epsilon}{2}$.

Since $\inf B$ is the greatest lower bound of B, then there exists $y \in B$ such that $y < \inf B + \frac{\epsilon}{2}$.

Thus, $x + y < (\inf A + \frac{\epsilon}{2}) + (\inf B + \frac{\epsilon}{2})$.

Hence, there exists $x + y \in A + B$ such that $x + y < (\inf A + \inf B) + \epsilon$.

Therefore, $\inf A + \inf B$ is the greatest lower bound of $A + B$, so $\inf A + \inf B = \inf(A + B)$. □

Corollary 41. *Let S be a subset of an ordered field F.*

Let $k \in F$.

Let $k + S = \{k + s : s \in S\}$.

1. If $\sup S$ exists, then $\sup(k + S) = k + \sup S$.

2. If $\inf S$ exists, then $\inf(k + S) = k + \inf S$.

Proof. We prove 1.

Suppose $\sup S$ exists.

Let $K = \{k\}$.

Then $\sup K = k$.

Let $K + S = \{k + s : k \in K, s \in S\}$.

Then $k + S = K + S$.

Therefore,

$$\begin{aligned} k + \sup S &= \sup K + \sup S \\ &= \sup(K + S) \\ &= \sup(k + S). \end{aligned}$$

□

Proof. We prove 2.

Suppose $\inf S$ exists.

Let $K = \{k\}$.

Then $\inf K = k$.

Let $K + S = \{k + s : k \in K, s \in S\}$.

Then $k + S = K + S$.

Therefore,

$$\begin{aligned} k + \inf S &= \inf K + \inf S \\ &= \inf(K + S) \\ &= \inf(k + S). \end{aligned}$$

□

Corollary 42. *Let A and B be subsets of an ordered field F.*
Let $A - B = \{a - b : a \in A, b \in B\}$.
If $\sup A$ and $\inf B$ exist, then $\sup(A - B) = \sup A - \inf B$.

Proof. Suppose $\sup A$ and $\inf B$ exist.
Then $A \neq \emptyset$ and $B \neq \emptyset$.
Let $-B = \{-b : b \in B\}$.
Since $\inf B$ exists, then $\sup(-B) = -\inf B$.
Let $A + (-B) = \{a + b : a \in A, b \in -B\}$.

We first prove $A - B = A + (-B)$.
Let $x \in A - B$.
Then $x = a - b$ for some $a \in A$ and $b \in B$.
Since $b \in B$, then $-b \in -B$.
Since $a \in A$ and $-b \in -B$, then $a + (-b) = a - b = x \in A + (-B)$.
Thus, $A - B \subset A + (-B)$.

Let $y \in A + (-B)$.
Then $y = a + b$ for some $a \in A$ and $b \in -B$.
Since $b \in -B$, then $b = -b'$ for some $b' \in B$.
Since $a \in A$ and $b' \in B$, then $a - b' = a + b = y \in A - B$.
Thus, $A + (-B) \subset A - B$.
Since $A - B \subset A + (-B)$ and $A + (-B) \subset A - B$, then $A - B = A + (-B)$.
Therefore,

$$\begin{aligned} \sup(A - B) &= \sup(A + (-B)) \\ &= \sup A + \sup(-B) \\ &= \sup A - \inf B. \end{aligned}$$

∎

Proposition 43. ***comparison property of suprema and infima***
Let A and B be subsets of an ordered field F such that $A \subset B$.
1. If $\sup A$ and $\sup B$ exist, then $\sup A \leq \sup B$.
2. If $\inf A$ and $\inf B$ exist, then $\inf B \leq \inf A$.

Proof. We prove 1.
Suppose $\sup A$ and $\sup B$ exist.
Since $\sup A$ exists, then A is not empty.
Let $x \in A$.
Since $A \subset B$, then $x \in B$.
Since $\sup B$ is an upper bound of B, then $x \leq \sup B$.
Hence, $\sup B$ is an upper bound of A.
Since $\sup A$ is the least upper bound of A, then $\sup A \leq \sup B$. ∎

Proof. We prove 2.
Suppose $\inf A$ and $\inf B$ exist.
Since $\inf A$ exists, then A is not empty.
Let $x \in A$.
Since $A \subset B$, then $x \in B$.
Since $\inf B$ is a lower bound of B, then $\inf B \leq x$.
Hence, $\inf B$ is a lower bound of A.
Since $\inf A$ is the greatest lower bound of A, then $\inf B \leq \inf A$. □

Proposition 44. ***scalar multiple property of suprema and infima***
Let S be a subset of an ordered field F.
Let $k \in F$.
Let $kS = \{ks : s \in S\}$.
1. If $k > 0$ and $\sup S$ exists, then $\sup(kS) = k \sup S$.
2. If $k > 0$ and $\inf S$ exists, then $\inf(kS) = k \inf S$.
3. If $k < 0$ and $\inf S$ exists, then $\sup(kS) = k \inf S$.
4. If $k < 0$ and $\sup S$ exists, then $\inf(kS) = k \sup S$.

Proof. We prove 1.
Suppose $k > 0$ and $\sup S$ exists.
Since $\sup S$ exists, then $S \neq \emptyset$, so there exists $s \in S$.
Hence, $ks \in kS$, so the set kS is not empty.
Let $x \in kS$.
Then there exists $s \in S$ such that $x = ks$.
Since $\sup S$ is an upper bound of S and $s \in S$, then $s \leq \sup S$.
Since $k > 0$, then $ks \leq k \sup S$, so $x \leq k \sup S$.
Therefore, $k \sup S$ is an upper bound of kS.

We prove $k \sup S$ is the least upper bound of kS.
Let $\epsilon > 0$.
Since $k > 0$, then $\frac{\epsilon}{k} > 0$.
Since $\sup S$ is the least upper bound of S, then there exists $s' \in S$ such that $s' > \sup S - \frac{\epsilon}{k}$.
Since $k > 0$, then there exists $ks' \in kS$ such that $ks' > k \sup S - \epsilon$.
Therefore, $k \sup S$ is the least upper bound of kS, so $k \sup S = \sup(kS)$. □

Proof. We prove 2.
Suppose $k > 0$ and $\inf S$ exists.
Since $\inf S$ exists, then $S \neq \emptyset$, so there exists $s \in S$.
Hence, $ks \in kS$, so the set kS is not empty.
Let $x \in kS$.
Then there exists $s \in S$ such that $x = ks$.
Since $\inf S$ is a lower bound of S and $s \in S$, then $\inf S \leq s$.
Since $k > 0$, then $k \inf S \leq ks$, so $k \inf S \leq x$.
Therefore, $k \inf S$ is a lower bound of kS.

We prove $k \inf S$ is the greatest lower bound of kS.

Let $\epsilon > 0$.

Since $k > 0$, then $\frac{\epsilon}{k} > 0$.

Since $\inf S$ is the greatest lower bound of S, then there exists $s' \in S$ such that $s' < \inf S + \frac{\epsilon}{k}$.

Since $k > 0$, then there exists $ks' \in kS$ such that $ks' < k \inf S + \epsilon$.

Therefore, $k \inf S$ is the greatest lower bound of kS, so $k \inf S = \inf(kS)$. □

Proof. We prove 3.

Suppose $k < 0$ and $\inf S$ exists.

Since $k < 0$, then $-k > 0$.

Since $-k > 0$ and $\inf S$ exists, then $\inf(-kS) = -k \inf S$.

Since $\inf(-kS)$ exists, then $\sup(-(-kS)) = -\inf(-kS)$.

Therefore, $\sup(kS) = -(-k \inf S) = k \inf S$. □

Proof. We prove 4.

Suppose $k < 0$ and $\sup S$ exists.

Since $k < 0$, then $-k > 0$.

Since $-k > 0$ and $\sup S$ exists, then $\sup(-kS) = -k \sup S$.

Since $\sup(-kS)$ exists, then $\inf(-(-kS)) = -\sup(-kS)$.

Therefore, $\inf(kS) = -(-k \sup S) = k \sup S$. □

Proposition 45. ***sufficient conditions for existence of supremum and infimum in an ordered field***

Let S be a subset of an ordered field F.

1. If $\max S$ exists, then $\sup S = \max S$.

2. If $\min S$ exists, then $\inf S = \min S$.

Proof. We prove 1.

Suppose $\max S$ exists in F.

Since $(F, \leq)$ is a partially ordered set and $S \subset F$ and $\max S$ exists, then $\sup S = \max S$. □

Proof. We prove 2.

Suppose $\min S$ exists in F.

Since $(F, \leq)$ is a partially ordered set and $S \subset F$ and $\min S$ exists, then $\inf S = \min S$. □

Proposition 46. *Let S be a subset of an ordered field F.*

Let $-S = \{-s : s \in S\}$.

1. If $\min S$ exists, then $\max(-S) = -\min S$.

2. If $\max S$ exists, then $\min(-S) = -\max S$.

Proof. We prove 1.

Suppose $\min S$ exists.

Then $\min S \in S$, so $-\min S \in -S$.

Hence, the set $-S$ is not empty.

Let $x \in -S$.

Then there exists $s \in S$ such that $x = -s$.
Since $\min S$ is a lower bound of S and $s \in S$, then $\min S \leq s$.
Hence, $-\min S \geq -s$, so $-\min S \geq x$.
Thus, $x \leq -\min S$.
Therefore, $-\min S$ is an upper bound of $-S$.
Since $-\min S \in -S$ and $-\min S$ is an upper bound of $-S$, then $-\min S = \max(-S)$. ☐

Proof. We prove 2.
Suppose $\max S$ exists.
Then $\max S \in S$, so $-\max S \in -S$.
Hence, the set $-S$ is not empty.
Let $x \in -S$.
Then there exists $s \in S$ such that $x = -s$.
Since $\max S$ is an upper bound of S and $s \in S$, then $s \leq \max S$.
Hence, $-s \geq -\max S$, so $x \geq -\max S$.
Thus, $-\max S \leq x$.
Therefore, $-\max S$ is a lower bound of $-S$.
Since $-\max S \in -S$ and $-\max S$ is a lower bound of $-S$, then $-\max S = \min(-S)$. ☐

Lemma 47. *Let A and B be nonempty subsets of an ordered field F.*
Then $u \in F$ is an upper bound of $A \cup B$ iff u is an upper bound of A and B.

Proof. We prove if u is an upper bound of $A \cup B$, then u is an upper bound of A and B.
Suppose u is an upper bound of $A \cup B$ in F.
Since A is not empty, then there is at least one element in A.
Let $x \in A$.
Since $A \subset A \cup B$, then $x \in A \cup B$.
Since u is an upper bound of $A \cup B$, then $x \leq u$.
Therefore, $x \leq u$ for all $x \in A$, so u is an upper bound of A.

Since B is not empty, then there is at least one element in B.
Let $x \in B$.
Since $B \subset A \cup B$, then $x \in A \cup B$.
Since u is an upper bound of $A \cup B$, then $x \leq u$.
Therefore, $x \leq u$ for all $x \in B$, so u is an upper bound of B. ☐

Proof. Conversely, we prove if u is an upper bound of A and B, then u is an upper bound of $A \cup B$.
Suppose u is an upper bound of A and B in F.
Since A is not empty, then there is at least one element in A.
Let $a \in A$.
Since $A \subset A \cup B$, then $a \in A \cup B$.
Hence, $A \cup B$ is not empty.
Let $x \in A \cup B$.

Then either $x \in A$ or $x \in B$.
We consider these cases separately.
Case 1: Suppose $x \in A$.
Since u is an upper bound of A, then $x \leq u$.
Case 2: Suppose $x \in B$.
Since u is an upper bound of B, then $x \leq u$.
Hence, in all cases, $x \leq u$.
Therefore, u is an upper bound of $A \cup B$, as desired. □

Proposition 48. *Let A and B be subsets of an ordered field F.*
If $\sup A$ and $\sup B$ exist, then $\sup(A \cup B) = \max\{\sup A, \sup B\}$.

Proof. Suppose $\sup A$ and $\sup B$ exist.
Then $A \neq \emptyset$ and $B \neq \emptyset$.
Let $S = \{\sup A, \sup B\}$.
Since $\sup A \in F$ and $\sup B \in F$, then $S \subset F$.
Since $\sup A \in S$ and $\sup B \in S$ and either $\sup A \leq \sup B$ or $\sup B \leq \sup A$, then either $\max S = \sup B$ or $\max S = \sup A$.
Hence, $\max S \in F$ and $\sup A \leq \max S$ and $\sup B \leq \max S$.
We prove $\max S$ is an upper bound of $A \cup B$.
Since $A \neq \emptyset$, let $a \in A$.
Since $A \subset A \cup B$, then $a \in A \cup B$, so $A \cup B$ is not empty.
Let $x \in A \cup B$.
Then either $x \in A$ or $x \in B$.
We consider these cases separately.
Case 1: Suppose $x \in A$.
Since $\sup A$ is an upper bound of A, then $x \leq \sup A$.
Since $\sup A \leq \max S$, then $x \leq \max S$.
Case 2: Suppose $x \in B$.
Since $\sup B$ is an upper bound of B, then $x \leq \sup B$.
Since $\sup B \leq \max S$, then $x \leq \max S$.
Hence, in all cases, $x \leq \max S$.
Since $x \leq \max S$ for all $x \in A \cup B$, then $\max S$ is an upper bound of $A \cup B$.

To prove $\max S$ is the least upper bound of $A \cup B$, let M be an arbitrary upper bound of $A \cup B$.
Since $A \neq \emptyset$ and $B \neq \emptyset$ and M is an upper bound of $A \cup B$, then M is an upper bound of A and B.
We must prove $\max S \leq M$.
Since M is an upper bound of A and $\sup A$ is the least upper bound of A, then $\sup A \leq M$.
Since M is an upper bound of B and $\sup B$ is the least upper bound of B, then $\sup B \leq M$.
Since either $\max S = \sup A$ or $\max S = \sup B$, then this implies $\max S \leq M$.
Therefore, $\max S$ is the least upper bound of $A \cup B$, so $\max S = \sup(A \cup B)$. □

Lemma 49. *Let A and B be subsets of an ordered field F.*
If $\max A$ *and* $\max B$ *exist in F, then* $\max(A \cup B) = \max\{\max A, \max B\}$.

Proof. Suppose $\max A$ and $\max B$ exist in F.
Let $S = \{\max A, \max B\}$.
Since $\max A \in S$ and $\max B \in S$ and either $\max A \leq \max B$ or $\max B \leq \max A$, then either $\max B$ is the maximum of S or $\max A$ is the maximum of S.
Hence, $\max S$ exists.
Since either $\max S = \max A$ or $\max S = \max B$ and $\max A \in A$ and $\max B \in B$, then either $\max S \in A$ or $\max S \in B$.
Hence, $\max S \in A \cup B$.
Since $\max S$ is the maximum of S, then $\max A \leq \max S$ and $\max B \leq \max S$.
We prove $\max S$ is an upper bound of $A \cup B$.
Since $\max A$ is the maximum of A, then $\max A \in A$, so A is not empty.
Let $a \in A$.
Since $A \subset A \cup B$, then $a \in A \cup B$.
Hence, $A \cup B$ is not empty.
Let $x \in A \cup B$.
Then either $x \in A$ or $x \in B$.
We consider these cases separately.
Case 1: Suppose $x \in A$.
Since $\max A$ is an upper bound of A, then $x \leq \max A$.
Thus, $x \leq \max A$ and $\max A \leq \max S$, so $x \leq \max S$.
Case 2: Suppose $x \in B$.
Since $\max B$ is an upper bound of B, then $x \leq \max B$.
Thus, $x \leq \max B$ and $\max B \leq \max S$, so $x \leq \max S$.
Hence, in all cases, $x \leq \max S$.
Therefore, $\max S$ is an upper bound of $A \cup B$.
Thus, $\max S \in A \cup B$ and $\max S$ is an upper bound of $A \cup B$, so $\max S = \max(A \cup B)$, as desired. ☐

Theorem 50. *Every nonempty finite subset of an ordered field has a maximum.*

Proof. Let F be an ordered field.
Define the predicate $p(n)$ over $\mathbb{N}$ to be the statement:
If a subset S of F contains exactly n elements, then $\max S$ exists.
We prove $p(n)$ is true for all $n \in \mathbb{N}$ by induction on n.
Basis:
Since F is a field, then F is not empty, so there is at least one element of F.
Let x be an element of F.
Let $S = \{x\}$.
Since $x \in F$, then $S \subset F$.
Clearly, S contains exactly one element.
Since $x \in S$ and $x \leq x$, then x is the maximum of S.
Thus, $\max S$ exists.
Therefore, $p(1)$ is true.

Thus, if S is any subset of F that contains exactly one element, then $\max S$ exists.

Induction:

Let $n \in \mathbb{N}$ such that $p(n)$ is true.

Then if a subset S of F contains exactly n elements, then $\max S$ exists.

To prove $p(n+1)$ follows, we must prove if a subset A of F contains exactly $n+1$ elements, then $\max A$ exists.

Since F is an ordered field, then F is infinite, so F contains infinitely many elements.

Hence, there exist a finite number of elements of F.

In particular, there exist exactly $n+1$ elements of F.

Let A be a subset of F that contains exactly $n+1$ elements.

Then there exist $x_1, ..., x_n, x_{n+1}$ elements of F such that $A = \{x_1, ..., x_n, x_{n+1}\}$ and $A \subset F$.

Let $B = \{x_1, ..., x_n\}$ and $B' = \{x_{n+1}\}$.

Then $B \subset A$ and $B' \subset A$ and $A = B \cup B'$ and B contains exactly n elements and B' contains exactly one element.

Since $B \subset A \subset F$, then $B \subset F$.

Thus, B is a subset of F and contains exactly n elements, so by the induction hypothesis, $\max B$ exists.

Since $B' \subset A \subset F$, then $B' \subset F$.

Thus, B' is a subset of F and contains exactly one element, so $\max B'$ exists.

Since $\max B$ and $\max B'$ exist, then $\max(B \cup B') = \max\{\max B, \max B'\}$.

Thus, $\max A = \max\{\max B, \max B'\}$, so $\max A$ exists.

Thus, $p(n+1)$ is true.

Hence, $p(n)$ implies $p(n+1)$ for all $n \in \mathbb{N}$.

Since $p(1)$ is true and $p(n)$ implies $p(n+1)$ for all $n \in \mathbb{N}$, then by induction $p(n)$ is true for all $n \in \mathbb{N}$.

Thus, for all $n \in \mathbb{N}$, if a subset S of F contains exactly n elements, then $\max S$ exists.

Hence, if S is a nonempty finite subset of F, then $\max S$ exists.

Therefore, if S is a nonempty finite subset of F, then S has a maximum.

Thus, every nonempty finite subset of an ordered field has a maximum, as desired. $\square$

Complete ordered fields

Theorem 51. ***greatest lower bound property in a complete ordered field***

Every nonempty subset of a complete ordered field F that is bounded below in F has a greatest lower bound in F.

Proof. Let S be a nonempty subset of a complete ordered field F that is bounded below in F.

We must prove $\inf S$ exists in F.

Let $-S = \{-s : s \in S\}$.

Since $S \subset F$, then $-S \subset F$.
Since S is not empty, then there is at least one element of S.
Let $x \in S$.
Then $-x \in -S$, so $-S \neq \emptyset$.
Let $t \in -S$.
Then there exists $s \in S$ such that $t = -s$.
Since S is bounded below in F, then there is a lower bound of S in F.
Let L be a lower bound of S in F.
Since L is a lower bound of S and $s \in S$, then $L \leq s$, so $-L \geq -s$.
Hence, $-L \geq t$, so $t \leq -L$ for all $t \in -S$.
Therefore, $-L$ is an upper bound of $-S$, so $-S$ is bounded above in F.
Thus, $-S$ is a nonempty subset of F bounded above in F.
Since F is complete, then $\sup(-S)$ exists in F.
Hence, $\inf(-(-S)) = -\sup(-S)$, so $\inf(S) = -\sup(-S)$.
Therefore, we conclude $\inf(S)$ exists in F. □

Proposition 52. *There is no rational number x such that $x^2 = 2$.*

Proof. Suppose there is a rational number x such that $x^2 = 2$.
Then there exist a pair of integers p and q with $q \neq 0$ such that $x = \frac{p}{q}$.
Surely, if such a pair exists, then a pair exists having no common factors greater than 1.
Therefore, assume p and q have no common factors greater than 1.
Observe that $2 = x^2 = (\frac{p}{q})^2 = \frac{p^2}{q^2}$.
Thus, $p^2 = 2q^2$, so p^2 is even.
Since an integer n^2 is even if and only if n is even, then in particular, p^2 is even iff p is even.
Thus, p is even.
Hence, $p = 2m$ for some integer m.
Therefore, $2q^2 = (2m)^2 = 4m^2$, so $q^2 = 2m^2$.
Hence, q^2 is even, so q is even.
Since p and q are both even, then 2 is a common factor of both p and q and is greater than 1; but this contradicts the assumption that p and q have no common factors greater than 1.
Hence, no such pair of integers exist.
Therefore, there is no rational number x such that $x^2 = 2$. □

Proposition 53. *Let A and B be subsets of $\mathbb{R}$ such that $\sup A$ and $\sup B$ exist in $\mathbb{R}$.*
If $A \cap B \neq \emptyset$, then $\sup(A \cap B) \leq \min\{\sup A, \sup B\}$.
Moreover, if A and B are bounded intervals such that $A \cap B \neq \emptyset$, then $\sup(A \cap B) = \min\{\sup A, \sup B\}$.

Proof. Suppose $A \cap B \neq \emptyset$.
Since $A \subset \mathbb{R}$ and $B \subset \mathbb{R}$, then $A \cap B \subset \mathbb{R}$.
Let $S = \{\sup A, \sup B\}$.
Since $\sup A \in \mathbb{R}$ and $\sup B \in \mathbb{R}$, then $S \subset \mathbb{R}$.

Since $\sup A \in S$ and $\sup B \in S$ and either $\sup A \leq \sup B$ or $\sup B \leq \sup A$, then either $\sup A = \min S$ or $\sup B = \min S$.

Hence, $\min S \in \mathbb{R}$ and $\min S \leq \sup A$ and $\min S \leq \sup B$.

We prove $\min S$ is an upper bound of $A \cap B$ in $\mathbb{R}$.

Since $A \cap B$ is not empty, let $x \in A \cap B$.

Then $x \in A$ and $x \in B$.

Either $\sup A = \min S$ or $\sup B = \min S$.

We consider these cases separately.

Case 1: Suppose $\sup A = \min S$.

Since $x \in A$ and $\sup A$ is an upper bound of A, then $x \leq \sup A$.

Thus, $x \leq \min S$.

Case 2: Suppose $\sup B = \min S$.

Since $x \in B$ and $\sup B$ is an upper bound of B, then $x \leq \sup B$.

Thus, $x \leq \min S$.

Hence, in all cases, $x \leq \min S$.

Therefore, $\min S$ is an upper bound of $A \cap B$ in $\mathbb{R}$.

Thus, $A \cap B$ is bounded above in $\mathbb{R}$.

Since $A \cap B$ is a nonempty subset of $\mathbb{R}$ and is bounded above in $\mathbb{R}$ and $\mathbb{R}$ is complete, then $A \cap B$ has a least upper bound in $\mathbb{R}$.

Therefore, $\sup(A \cap B)$ is the least upper bound of $A \cap B$ in $\mathbb{R}$.

Since $\sup(A \cap B)$ is the least upper bound of $A \cap B$ and $\min S$ is an upper bound of $A \cap B$, then $\sup(A \cap B) \leq \min S$, as desired.

We prove if A and B are bounded intervals such that $A \cap B \neq \emptyset$, then $\sup(A \cap B) = \min\{\sup A, \sup B\}$.

Suppose A and B are bounded intervals such that $A \cap B \neq \emptyset$.

Since A and B are intervals, then $A \subset \mathbb{R}$ and $B \subset \mathbb{R}$.

Since A is bounded, then A is bounded above and below in $\mathbb{R}$.

Since B is bounded, then B is bounded above and below in $\mathbb{R}$.

Since $A \cap B \neq \emptyset$, then let $x \in A \cap B$.

Then $x \in A$ and $x \in B$.

Hence, A is not empty and B is not empty.

Since A is a nonempty subset of $\mathbb{R}$ that is bounded above in $\mathbb{R}$, then A has a least upper bound in $\mathbb{R}$.

Therefore, $\sup A$ is the least upper bound of A in $\mathbb{R}$.

Since A is a nonempty subset of $\mathbb{R}$ that is bounded below in $\mathbb{R}$, then A has a greatest lower bound in $\mathbb{R}$.

Therefore, $\inf A$ is the greatest lower bound of A in $\mathbb{R}$.

Since B is a nonempty subset of $\mathbb{R}$ that is bounded above in $\mathbb{R}$, then B has a least upper bound in $\mathbb{R}$.

Therefore, $\sup B$ is the least upper bound of B in $\mathbb{R}$.

Since B is a nonempty subset of $\mathbb{R}$ that is bounded below in $\mathbb{R}$, then B has a greatest lower bound in $\mathbb{R}$.

Therefore, $\inf B$ is the greatest lower bound of B in $\mathbb{R}$.

Let $S = \{\sup A, \sup B\}$.

Since A and B are subsets of $\mathbb{R}$ and $\sup A$ and $\sup B$ exist in $\mathbb{R}$ and $A \cap B \neq \emptyset$, then $\sup(A \cap B) \leq \min S$.

We must prove $\sup(A \cap B) = \min S$.

Since $\min S$ is an upper bound of $A \cap B$, then $A \cap B$ has at least one upper bound in $\mathbb{R}$.

Let K be an arbitrary upper bound of $A \cap B$ in $\mathbb{R}$.

Then $K \in \mathbb{R}$.

We must prove $\min S \leq K$.

Suppose for the sake of contradiction $\min S > K$.

Then $K < \min S$.

Since $x \in A \cap B$ and K is an upper bound of $A \cap B$, then $x \leq K$.

Hence, $x \leq K < \min S$.

Since $\min S \leq \sup A$, then $x \leq K < \min S \leq \sup A$, so $x \leq K < \sup A$.

Since A is an interval and $\sup A$ is the least upper bound of A, then if $x \in A$, then $c \in A$ if $x \leq c < \sup A$.

Since A is an interval and $x \in A$ and $x \leq K < \sup A$, then $K \in A$.

Since $\min S \leq \sup B$, then $x \leq K < \min S \leq \sup B$, so $x \leq K < \sup B$.

Since B is an interval and $\sup B$ is the least upper bound of B, then if $x \in B$, then $c \in B$ if $x \leq c < \sup B$.

Since B is an interval and $x \in B$ and $x \leq K < \sup B$, then $K \in B$.

Either $\sup A = \min S$ or $\sup B = \min S$.

We consider these cases separately.

Case 1: Suppose $\min S = \sup A$.

Since $K \in A$ and $K < \frac{K+\sup A}{2} < \sup A$, then $\frac{K+\sup A}{2} \in A$.

Since $\min S = \sup A$, then $K < \frac{K+\min S}{2} < \sup A$ and $\frac{K+\min S}{2} \in A$.

Thus, $\frac{K+\min S}{2} \in A$ and $\frac{K+\min S}{2} > K$.

Since $\min S \leq \sup B$, then either $\min S < \sup B$ or $\min S = \sup B$.

Suppose $\min S < \sup B$.

Since $\min S = \sup A$, then $\sup A < \sup B$.

Since $K \in B$ and $K < \min S < \sup B$, then $\min S \in B$.

Since B is an interval and $K \in B$ and $\min S \in B$ and $K < \frac{K+\min S}{2} < \min S$, then $\frac{K+\min S}{2} \in B$.

Thus, $\frac{K+\min S}{2} \in B$ and $\frac{K+\min S}{2} > K$.

Suppose $\min S = \sup B$.

Since $K \in B$ and $K < \frac{K+\sup B}{2} < \sup B$, then $\frac{K+\sup B}{2} \in B$.

Since $\sup B = \min S$, then $K < \frac{K+\min S}{2} < \sup B$ and $\frac{K+\min S}{2} \in B$.

Thus, $\frac{K+\min S}{2} \in B$ and $\frac{K+\min S}{2} > K$.

Thus, in either case $\frac{K+\min S}{2} \in B$ and $\frac{K+\min S}{2} > K$.

Since $\frac{K+\min S}{2} \in A$ and $\frac{K+\min S}{2} \in B$, then $\frac{K+\min S}{2} \in A \cap B$.

Hence, there exists $\frac{K+\min S}{2} \in A \cap B$ such that $\frac{K+\min S}{2} > K$.

But, this contradicts the fact that K is an upper bound of $A \cap B$.

Therefore, $\min S \neq \sup A$.

Case 2: Suppose $\min S = \sup B$.

Since $K \in B$ and $K < \frac{K+\sup B}{2} < \sup B$, then $\frac{K+\sup B}{2} \in B$.

Since $\min S = \sup B$, then $K < \frac{K+\min S}{2} < \sup B$ and $\frac{K+\min S}{2} \in B$.

Thus, $\frac{K+\min S}{2} \in B$ and $\frac{K+\min S}{2} > K$.
Since $\min S \leq \sup A$, then either $\min S < \sup A$ or $\min S = \sup A$.
Suppose $\min S < \sup A$.
Since $\min S = \sup B$, then $\sup B < \sup A$.
Since $K \in A$ and $K < \min S < \sup A$, then $\min S \in A$.
Since A is an interval and $K \in A$ and $\min S \in A$ and $K < \frac{K+\min S}{2} < \min S$, then $\frac{K+\min S}{2} \in A$.
Thus, $\frac{K+\min S}{2} \in A$ and $\frac{K+\min S}{2} > K$.
Suppose $\min S = \sup A$.
Since $K \in A$ and $K < \frac{K+\sup A}{2} < \sup A$, then $\frac{K+\sup A}{2} \in A$.
Since $\sup A = \min S$, then $K < \frac{K+\min S}{2} < \sup A$ and $\frac{K+\min S}{2} \in A$.
Thus, $\frac{K+\min S}{2} \in A$ and $\frac{K+\min S}{2} > K$.
Thus, in either case $\frac{K+\min S}{2} \in A$ and $\frac{K+\min S}{2} > K$.
Since $\frac{K+\min S}{2} \in A$ and $\frac{K+\min S}{2} \in B$, then $\frac{K+\min S}{2} \in A \cap B$.
Hence, there exists $\frac{K+\min S}{2} \in A \cap B$ such that $\frac{K+\min S}{2} > K$.
But, this contradicts the fact that K is an upper bound of $A \cap B$.
Therefore, $\min S \neq \sup A$.
Thus, in either case, $\min S \neq \sup A$ and $\min S \neq \sup B$.
This contradicts the fact that either $\min S = \sup A$ or $\min S = \sup B$.
Hence, $\min S$ cannot be greater than K.
Therefore, $\min S \leq K$, so $\min S$ is the least upper bound of $A \cap B$.
Thus, $\min S = \sup(A \cap B)$, as desired. □

Archimedean ordered fields

Theorem 54. ***Archimedean property of*** $\mathbb{Q}$
The field $(\mathbb{Q}, +, \cdot, \leq)$ *is Archimedean ordered.*

Proof. Let $a, b \in \mathbb{Q}$ such that $b > 0$.
We must prove there exists $n \in \mathbb{N}$ such that $n > \frac{a}{b}$.
Either $a \leq 0$ or $a > 0$.
We consider these cases separately.
Case 1: Suppose $a \leq 0$.
Let $n = 1$.
Then $n \in \mathbb{N}$.
Since $a \leq 0$ and $b > 0$, then $\frac{a}{b} \leq 0 < 1 = n$.
Therefore, there exists $n \in \mathbb{N}$ such that $n > \frac{a}{b}$.
Case 2: Suppose $a > 0$.
Since $a \in \mathbb{Q}$ and $a > 0$, then there exist $r, s \in \mathbb{Z}^+$ such that $a = \frac{r}{s}$.
Since $b \in \mathbb{Q}$ and $b > 0$, then there exist $t, v \in \mathbb{Z}^+$ such that $b = \frac{t}{v}$.
Let $n = rv(rv + 1)$.
Since $r, v \in \mathbb{Z}^+$ and $\mathbb{Z}^+$ is closed under addition and multiplication, then $n \in \mathbb{Z}^+$, so $n \in \mathbb{N}$.
Since $s, t \in \mathbb{Z}^+$, then $s \geq 1$ and $t \geq 1$, so $st \geq 1$.
Since $r, v \in \mathbb{Z}^+$, then $r \geq 1$ and $v \geq 1$, so $rv \geq 1$.

Since $rv \geq 1$, then $rv+1 \geq 2 > 1$, so $rv+1 > 1$.
Since $rv+1 > 1$ and $st \geq 1$, then $(rv+1)st > 1$.
Since $\frac{nb}{a} = \frac{rv(rv+1)\frac{t}{v}}{\frac{r}{s}} = \frac{r(rv+1)t}{\frac{r}{s}} = \frac{r(rv+1)st}{r} = (rv+1)st > 1$, then $\frac{nb}{a} > 1$.
Since $a > 0$, then $nb > a$.
Since $b > 0$, then $n > \frac{a}{b}$.
Therefore, there exists $n \in \mathbb{N}$ such that $n > \frac{a}{b}$. □

Theorem 55. ***Archimedean property of*** $\mathbb{R}$

A complete ordered field is necessarily Archimedean ordered.

Proof. Let F be a complete ordered field.
To prove F is Archimedean ordered, let $a, b \in F$ with $b > 0$.
We must prove there exists $n \in \mathbb{Z}^+$ such that $nb > a$.
We prove by contradiction.
Suppose there does not exist a positive integer n such that $nb > a$.
Then $nb \leq a$ for all positive integers n.
Let S be the set of all positive integer multiples of b.
Then $S = \{nb : n \in \mathbb{Z}^+\}$.
Since $b = 1b$ and $1 \in \mathbb{Z}^+$, then $b \in S$, so S is not empty.
Let $s \in S$.
Then there exists $n \in \mathbb{Z}^+$ such that $s = nb$.
Since $b \in F^+$ and $n \in \mathbb{N}$, then $s = nb \in F^+$.
Since $s \in F^+$ and $F^+ \subset F$, then $s \in F$, so $S \subset F$.
Since $n \in \mathbb{Z}^+$, then by hypothesis, $nb \leq a$, so $s \leq a$.
Therefore, a is an upper bound of S in F, so S is bounded above in F.
Hence, S is a nonempty subset of F that is bounded above in F.
Since F is complete, then S has a least upper bound in F.
Let $\sup S$ be the least upper bound of S in F.
Since $b > 0 = \sup S - \sup S$, then $\sup S + b > \sup S$, so $\sup S > \sup S - b$.
Since $\sup S - b < \sup S$, then $\sup S - b$ is not an upper bound of S, so there exists $x \in S$ such that $x > \sup S - b$.
Since $x \in S$, then there exists $m \in \mathbb{Z}^+$ such that $x = mb$, so $mb > \sup S - b$.
Hence, $(m+1)b = mb + b > \sup S$.
Since $m+1 \in \mathbb{Z}^+$, then $(m+1)b \in S$.
Hence, there exists $(m+1)b \in S$ such that $(m+1)b > \sup S$.
But, this contradicts the fact that $\sup S$ is an upper bound of S.
Therefore, there does exist a positive integer n such that $nb > a$, as desired. □

Theorem 56. $\mathbb{N}$ ***is unbounded in an Archimedean ordered field.***

Let F be an Archimedean ordered field.
Then for every $x \in F$, there exists $n \in \mathbb{N}$ such that $n > x$.

Proof. Since F is a field, then $1 \in F$, so $F \neq \emptyset$.
Let $x \in F$ be arbitrary.
Since F is Archimedean and $x \in F$ and $1 > 0$, then there exists $n \in \mathbb{N}$ such that $n \cdot 1 > x$.

Therefore, there exists $n \in \mathbb{N}$ such that $n > x$. $\square$

Proposition 57. *Let F be an Archimedean ordered field.*

For every positive $\epsilon \in F$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

Proof. Let ϵ be a positive element of F.

Then $\epsilon > 0$.

Since F is Archimedean ordered and $1 \in F$ and $\epsilon > 0$, then there exists $n \in \mathbb{N}$ such that $n\epsilon > 1$.

Since $n \in \mathbb{N}$, then $n > 0$, so $\epsilon > \frac{1}{n}$.

Therefore, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$. $\square$

Lemma 58. *Each real number lies between two consecutive integers*

For each real number x there is a unique integer n such that $n \leq x < n+1$.

Solution. We must prove: $(\forall x \in \mathbb{R})(\exists! n \in \mathbb{Z})(n \leq x < n+1)$. $\square$

Proof. **Existence:**

Let x be an arbitrary real number.

We must prove there is an integer n such that $n \leq x < n+1$.

Let $S = \{n \in \mathbb{Z} : n \leq x\}$.

Suppose for the sake of contradiction $S = \emptyset$.

Then there is no integer n such that $n \leq x$.

Hence, $n > x$ for every integer n, so for every integer n, $x < n$.

Thus, x is a lower bound of $\mathbb{Z}$, so $\mathbb{Z}$ is bounded below in $\mathbb{R}$.

Since $\mathbb{Z} \neq \emptyset$ and $\mathbb{Z}$ is bounded below in $\mathbb{R}$, then by completeness of $\mathbb{R}$, $\inf \mathbb{Z}$ exists.

Since $\inf \mathbb{Z} + 1$ is not a lower bound of $\mathbb{Z}$, then there exists $t \in \mathbb{Z}$ such that $t < \inf \mathbb{Z} + 1$.

Thus, $t - 1 < \inf \mathbb{Z}$.

Since $t \in \mathbb{Z}$, then $t - 1 \in \mathbb{Z}$.

Hence, we have $t - 1 \in \mathbb{Z}$ and $t - 1 < \inf \mathbb{Z}$.

This contradicts the fact that $\inf \mathbb{Z}$ is a lower bound of $\mathbb{Z}$.

Therefore, $S \neq \emptyset$.

Let $s \in S$ be given.

Then $s \in \mathbb{Z}$ and $s \leq x$.

Thus, $s \leq x$ for all $s \in S$, so x is an upper bound of S.

Hence, S is bounded above in $\mathbb{R}$.

Since $S \neq \emptyset$ and S is bounded above in $\mathbb{R}$, then by completeness of $\mathbb{R}$, $\sup S$ exists.

Since $\sup S - 1$ is not an upper bound of S, then there exists $n \in S$ such that $n > \sup S - 1$.

Thus, $n + 1 > \sup S$.

Since $n \in S$, then $n \in \mathbb{Z}$ and $n \leq x$.

Since $\sup S$ is an upper bound of S, then if $n \in S$, then $n \leq \sup S$.

Hence, if $n > \sup S$, then $n \notin S$.

Since $n + 1 > \sup S$, then we conclude $n + 1 \notin S$.

Since $n+1 \in S$ iff $n+1 \in \mathbb{Z}$ and $n+1 \leq x$, then $n+1 \notin S$ iff either $n+1 \notin \mathbb{Z}$ or $n + 1 > x$.

Thus, either $n + 1 \notin \mathbb{Z}$ or $n + 1 > x$.

Since $s \in \mathbb{Z}$, then $n + 1 \in \mathbb{Z}$.

Hence, we conclude $n + 1 > x$.

Therefore, there exists $n \in \mathbb{Z}$ such that $n \leq x < n + 1$. □

Proof. **Uniqueness:**

Let $x \in \mathbb{R}$.

We must prove there is a unique integer n such that $n \leq x < n + 1$.

Suppose there exist integers m and n such that $m \leq x < m+1$ and $n \leq x < n + 1$.

To prove uniqueness, we must prove $m = n$.

Since $m \leq x < m + 1$, then $m \leq x$ and $x < m + 1$.

Since $n \leq x < n + 1$, then $n \leq x$ and $x < n + 1$.

By trichotomy, either $m < n$ or $m = n$ or $m > n$.

Suppose $m < n$.

Then $n - m > 0$.

Since m and n are integers, then $n - m \geq 1$.

Hence, $n \geq m + 1$, so $m + 1 \leq n$.

Since $m + 1 \leq n \leq x$, then $m + 1 \leq x$.

Thus, we have $m + 1 \leq x$ and $m + 1 > x$, a violation of trichotomy.

Therefore, m cannot be less than n.

Suppose $m > n$.

Then $m - n > 0$.

Since m and n are integers, then $m - n \geq 1$.

Hence, $m \geq n + 1$, so $n + 1 \leq m$.

Since $n + 1 \leq m$ and $m \leq x$, then $n + 1 \leq x$.

Thus, we have $n + 1 \leq x$ and $n + 1 > x$, a violation of trichotomy.

Therefore, m cannot be greater than n.

Hence, we must conclude $m = n$, as desired. □

Theorem 59. $\mathbb{Q}$ ***is dense in*** $\mathbb{R}$

For every $a, b \in \mathbb{R}$ with $a < b$, there exists $q \in \mathbb{Q}$ such that $a < q < b$.

Proof. Let a and b be real numbers with $a < b$.

Then $b - a > 0$.

By the Archimedean property of $\mathbb{R}$, there exists a positive integer n such that $\frac{1}{n} < b - a$.

Since $n > 0$, then $1 < bn - an$, so $an + 1 < bn$.

Since every real number lies between two consecutive integers, then in particular, the real number an lies between two consecutive integers.

Hence, there exists an integer m such that $m \leq an < m + 1$.

Thus, $m \leq an$ and $an < m + 1$.
Since $m \leq an$, then $m + 1 \leq an + 1$.
Since $m + 1 \leq an + 1$ and $an + 1 < bn$, then $m + 1 < bn$.
Hence, $an < m + 1$ and $m + 1 < bn$.
Since $n > 0$, then $a < \frac{m+1}{n}$ and $\frac{m+1}{n} < b$, so $a < \frac{m+1}{n} < b$.
Let $q = \frac{m+1}{n}$.
Since $m + 1, n \in \mathbb{Z}$ and $n \neq 0$, then $q \in \mathbb{Q}$.
Therefore, there exists $q \in \mathbb{Q}$ such that $a < q < b$, as desired. □

Corollary 60. ***between any two distinct real numbers is a nonzero rational number***

For every $a, b \in \mathbb{R}$ with $a < b$, there exists $q \in \mathbb{Q}$ such that $q \neq 0$ and $a < q < b$.

Proof. Let $a, b \in \mathbb{R}$ such that $a < b$.
Either it is the case that $a < 0 < b$ or not.
We consider these cases separately.
Case 1: Suppose $a < 0 < b$.
Then $a < 0$ and $0 < b$.
Since $\mathbb{Q}$ is dense in $\mathbb{R}$ and $0 < b$, then there exists $q \in \mathbb{Q}$ such that $0 < q < b$.
Hence, $0 < q$, so $q \neq 0$.
Since $a < 0$ and $0 < q < b$, then $a < 0 < q < b$, so $a < q < b$.
Case 2: Suppose it is not the case that $a < 0 < b$.
Then it is not the case that $a < 0$ and $0 < b$, so either $a \geq 0$ or $0 \geq b$.
We consider these cases separately.
Case 2a: Suppose $a \geq 0$.
Since $\mathbb{Q}$ is dense in $\mathbb{R}$ and $a < b$, then there exists $q \in \mathbb{Q}$ such that $a < q < b$.
Hence, $a < q$.
Since $0 \leq a$ and $a < q$, then $0 < q$, so $q \neq 0$.
Case 2b: Suppose $0 \geq b$.
Since $\mathbb{Q}$ is dense in $\mathbb{R}$ and $a < b$, then there exists $q \in \mathbb{Q}$ such that $a < q < b$.
Hence, $q < b$.
Since $q < b$ and $b \leq 0$, then $q < 0$, so $q \neq 0$.
Therefore, in all cases, there exists $q \in \mathbb{Q}$ such that $q \neq 0$ and $a < q < b$, as desired. □

Existence of square roots in $\mathbb{R}$

Proposition 61. *A square root of a negative real number does not exist in $\mathbb{R}$.*

Proof. Let x be a negative real number.
Then $x \in \mathbb{R}$ and $x < 0$.
Suppose a square root of x exists in $\mathbb{R}$.
Then there is a real number y such that $y^2 = x$.
Hence, $y^2 < 0$.
Since $\mathbb{R}$ is an ordered field, then $r^2 \geq 0$ for all $r \in \mathbb{R}$.
In particular, $y^2 \geq 0$.

Thus, we have $y^2 < 0$ and $y^2 \geq 0$, a violation of trichotomy.
Therefore, a square root of x does not exist in $\mathbb{R}$. $\square$

Proposition 62. *Zero is the unique square root of* 0.

Proof. Clearly, 0 is a real number and $0^2 = 0$.
Therefore, 0 is a square root of 0.
To prove 0 is a unique square root of 0, suppose there is a real number x that is a square root of 0.
Then $x \in \mathbb{R}$ and $x^2 = 0$.
We must prove $x = 0$.
Since $\mathbb{R}$ is an ordered field, then $x^2 = 0$ iff $x = 0$.
Since $x^2 = 0$, then we conclude $x = 0$, as desired. $\square$

Lemma 63. *Let F be an ordered field.*
Let $a, b \in F$.
If $0 < a < b$, then $0 < a^2 < ab < b^2$.

Proof. Suppose $0 < a < b$.
Then $0 < a$ and $a < b$, so $0 < b$.
Since $0 < a$ and $a > 0$, then $a0 < aa$, so $0 < a^2$.
Since $a < b$ and $a > 0$, then $aa < ab$, so $a^2 < ab$.
Since $a < b$ and $b > 0$, then $ab < bb$, so $ab < b^2$.
Therefore, $0 < a^2$ and $a^2 < ab$ and $ab < b^2$, so $0 < a^2 < ab < b^2$, as desired. $\square$

Lemma 64. *Let F be an ordered field.*
Let $a \in F$.
If $|a| < \epsilon$ for all $\epsilon > 0$, then $a = 0$.

Proof. Suppose $|a| < \epsilon$ for all $\epsilon > 0$.
Since $|a| \geq 0$, then either $|a| > 0$ or $|a| = 0$.
Suppose $|a| > 0$.
Then $|a| < |a|$, a contradiction.
Therefore, $|a| = 0$, so $a = 0$, as desired. $\square$

Proof. We must prove $(\forall \epsilon > 0)(|a| < \epsilon) \rightarrow (a = 0)$.
We prove by contrapositive.
Suppose $a \neq 0$.
Let $\epsilon = \frac{|a|}{2}$.
Since $|a| \geq 0$ and $a \neq 0$, then $|a| > 0$, so $\frac{|a|}{2} > 0$.
Hence, $\epsilon > 0$.
Since $1 \geq 1/2$ and $|a| > 0$, then $|a| \geq \frac{|a|}{2} = \epsilon$.
Therefore, there exists $\epsilon > 0$ such that $|a| \geq \epsilon$, as desired. $\square$

Theorem 65. ***existence and uniqueness of positive square roots***
Let $r \in \mathbb{R}$.
A unique positive square root of r exists in $\mathbb{R}$ iff $r > 0$.

Proof. We prove if a unique positive square root of r exists in $\mathbb{R}$, then $r > 0$.

Suppose there exists a unique positive square root of r in $\mathbb{R}$.

Let x be the unique positive square root of r in $\mathbb{R}$.

Then $x \in \mathbb{R}$ and $x > 0$ and $x^2 = r$.

Since $\mathbb{R}$ is an ordered field and $x > 0$, then $x^2 > 0$, so $r > 0$, as desired. $\square$

Proof. Conversely, we prove if $r > 0$, then a unique positive square root of r exists in $\mathbb{R}$.

Suppose $r > 0$.

To prove a unique positive square root of r exists in $\mathbb{R}$, we must prove there exists a unique $\alpha \in \mathbb{R}$ such that $\alpha > 0$ and $\alpha^2 = r$.

Thus, we must prove:

1. Existence:

There exists $\alpha \in \mathbb{R}$ such that $\alpha > 0$ and $\alpha^2 = r$.

2. Uniqueness:

If α and β are positive square roots of r, then $\alpha = \beta$. $\square$

Proof. **Uniqueness:**

We prove if α and β are positive square roots of r, then $\alpha = \beta$.

Suppose α and β are positive square roots of r.

Since α is a positive square root of r, then $\alpha \in \mathbb{R}$ and $\alpha > 0$ and $\alpha^2 = r$.

Since β is a positive square root of r, then $\beta \in \mathbb{R}$ and $\beta > 0$ and $\beta^2 = r$.

Since $\alpha^2 = r = \beta^2$, then $\alpha^2 = \beta^2$, so $\alpha^2 - \beta^2 = 0$.

Hence, $(\alpha + \beta)(\alpha - \beta) = 0$, so either $\alpha + \beta = 0$ or $\alpha - \beta = 0$.

Thus, either $\alpha = -\beta$ or $\alpha = \beta$.

Suppose $\alpha = -\beta$.

Since $\beta > 0$, then $-\beta < 0$, so $\alpha < 0$.

Thus, we have $\alpha < 0$ and $\alpha > 0$, a violation of trichotomy.

Hence, $\alpha \neq -\beta$.

Therefore, $\alpha = \beta$, as desired. $\square$

Proof. **Existence:**

We prove there exists $\alpha \in \mathbb{R}$ such that $\alpha > 0$ and $\alpha^2 = r$.

Let $S = \{x \in \mathbb{R} : x > 0, x^2 \leq r\}$.

Clearly, $S \subset \mathbb{R}$.

We prove S is not empty.

Let $A = \{1, r\}$.

Since $1 \in A$ and $r \in A$ and either $1 \leq r$ or $r \leq 1$, then either $\min A = 1$ or $\min A = r$, so $\min A$ exists in $\mathbb{R}$.

Since $\min A$ is a lower bound of A and $1 \in A$, then $\min A \leq 1$.

Since either $\min A = 1$ or $\min A = r$ and $1 > 0$ and $r > 0$, then $\min A > 0$.

Since $\min A \leq 1$ and $\min A > 0$, then $(\min A)^2 \leq \min A$.

Since $\min A$ is a lower bound of A and $r \in A$, then $\min A \leq r$.

Thus, $(\min A)^2 \leq \min A \leq r$, so $(\min A)^2 \leq r$.

Since $\min A > 0$, then $(\min A)^2 > 0$.

Since $\min A \in \mathbb{R}$ and $(\min A)^2 > 0$ and $(\min A)^2 \leq r$, then $\min A \in S$.

Therefore S is not empty.

Since $1 \in A$ and $r \in A$ and either $1 \leq r$ or $r \leq 1$, then either $\max A = r$ or $\max A = 1$, so $\max A$ exists in $\mathbb{R}$.

Let $x \in \mathbb{R}$.

To prove $\max A$ is an upper bound of S, we must prove if $x \in S$, then $x \leq \max A$.

We prove by contrapositive.

Suppose $x > \max A$.

We must prove $x \notin S$.

Since $\max A$ is an upper bound of A and $1 \in A$, then $1 \leq \max A$.

Thus, $x > \max A \geq 1 > 0$, so $x > 1$ and $x > 0$ and $\max A > 0$.

Since $x > \max A$ and $x > 0$, then $x^2 > x \max A$.

Since $x > 1$ and $\max A > 0$, then $x \max A > \max A$.

Thus, $x^2 > x \max A > \max A$, so $x^2 > \max A$.

Since $\max A$ is an upper bound of A and $r \in A$, then $r \leq \max A$.

Since $x^2 > \max A$ and $\max A \geq r$, then $x^2 > r$.

Since $x \in \mathbb{R}$ and $x^2 > r$, then $x \notin S$, as desired.

Therefore, $\max A$ is an upper bound of S, so S is bounded above in $\mathbb{R}$.

Since S is a nonempty subset of $\mathbb{R}$ and is bounded above in $\mathbb{R}$ and $\mathbb{R}$ is complete, then S has a least upper bound in $\mathbb{R}$.

Let α be the least upper bound of S in $\mathbb{R}$.

Then $\alpha \in \mathbb{R}$ and α is an upper bound of S.

We prove $\alpha > 0$.

Since α is an upper bound of S and $\min A \in S$, then $\min A \leq \alpha$.

Since $0 < \min A$ and $\min A \leq \alpha$, then $0 < \alpha$, so $\alpha > 0$, as desired.

We prove $\alpha^2 = r$.

Either $\alpha^2 < r$ or $\alpha^2 = r$ or $\alpha^2 > r$.

Suppose $\alpha^2 < r$.

Let $\delta = \min\{1, \frac{r-\alpha^2}{2\alpha+1}\}$.

Since $\alpha^2 < r$, then $r - \alpha^2 > 0$.

Since $\alpha > 0$, then $2\alpha + 1 > 0$, so $\frac{r-\alpha^2}{2\alpha+1} > 0$.

Thus, $\delta > 0$.

We prove $\alpha + \delta \in S$.

Since $\alpha > 0$ and $\delta > 0$, then $\alpha + \delta > 0$.

Since $\delta \leq 1$, then $0 < \delta \leq 1$, so $\delta^2 \leq \delta$.

Since $\delta \leq \frac{r-\alpha^2}{2\alpha+1}$ and $2\alpha + 1 > 0$, then $2\alpha\delta + \delta \leq r - \alpha^2$.

Thus,

$$\begin{aligned}
(\alpha+\delta)^2 &= \alpha^2 + 2\alpha\delta + \delta^2 \\
&\leq \alpha^2 + 2\alpha\delta + \delta \\
&\leq \alpha^2 + r - \alpha^2 \\
&= r.
\end{aligned}$$

Since $\alpha + \delta > 0$ and $(\alpha + \delta)^2 \leq r$, then $\alpha + \delta \in S$.
Since $\delta > 0$, then $\alpha + \delta > \alpha$.
Thus, there exists $\alpha + \delta \in S$ such that $\alpha + \delta > \alpha$.
This contradicts the fact that α is an upper bound of S.
Therefore, α^2 cannot be less than r.

Suppose $\alpha^2 > r$.
Let $\epsilon = \min\{\alpha, \frac{\alpha^2 - r}{2\alpha}\}$.
Since $\alpha^2 > r$, then $\alpha^2 - r > 0$.
Since $\alpha > 0$, then $\frac{\alpha^2 - r}{2\alpha} > 0$, so $\epsilon > 0$.
We prove $(\alpha - \epsilon)^2 > r$.
Since $\epsilon \leq \frac{\alpha^2 - r}{2\alpha}$, then $2\alpha\epsilon \leq \alpha^2 - r$, so $r \leq \alpha^2 - 2\alpha\epsilon$.
Since $\epsilon > 0$, then $\epsilon^2 > 0$.
Thus,

$$\begin{aligned}(\alpha - \epsilon)^2 &= \alpha^2 - 2\alpha\epsilon + \epsilon^2 \\ &> \alpha^2 - 2\alpha\epsilon \\ &\geq r.\end{aligned}$$

Hence, $(\alpha - \epsilon)^2 > r$.
Let $x \in S$.
Then $x > 0$ and $x^2 \leq r$.
Suppose for the sake of contradiction $x > \alpha - \epsilon$.
Since $\epsilon \leq \alpha$, then $0 \leq \alpha - \epsilon$.
Thus, $0 \leq \alpha - \epsilon < x$, so $(\alpha - \epsilon)^2 < x^2$.
Since $x^2 \leq r$, then $(\alpha - \epsilon)^2 < r$.
But, this contradicts the fact $(\alpha - \epsilon)^2 > r$.
Therefore, $x \leq \alpha - \epsilon$.
Thus, there exists $\epsilon > 0$ such that $x \leq \alpha - \epsilon$ for each $x \in S$, so $\alpha - \epsilon$ is an upper bound of S.
Since $\alpha - \epsilon < \alpha$, then this contradicts the fact that α is the least upper bound of S.
Hence, α^2 cannot be greater than r.
Since α^2 cannot be less than r and α^2 cannot be greater than r, then we must conclude $\alpha^2 = r$. □

Proposition 66. *Let* $x \in \mathbb{R}$.
Then $\sqrt{x} \in \mathbb{R}$ *iff* $x \geq 0$.

Proof. We first prove if $x \geq 0$, then $\sqrt{x} \in \mathbb{R}$.
Suppose $x \geq 0$.
Then $x > 0$ or $x = 0$.
We consider these cases separately.
Case 1: Suppose $x = 0$.
Since $\sqrt{x} = \sqrt{0} = 0$ and $0 \in \mathbb{R}$, then $\sqrt{x} \in \mathbb{R}$.
Case 2: Suppose $x > 0$.

Then a unique positive square root of x exists in $\mathbb{R}$.
Thus, there is a unique $y \in \mathbb{R}$ such that $y^2 = x$.
Since $x > 0$ and y is a positive square root of x, then $y = \sqrt{x}$.
Since $\sqrt{x} = y$ and $y \in \mathbb{R}$, then $\sqrt{x} \in \mathbb{R}$.
Therefore, in either case, $\sqrt{x} \in \mathbb{R}$. □

Proof. Conversely, we prove if $\sqrt{x} \in \mathbb{R}$, then $x \geq 0$.
Suppose $\sqrt{x} \in \mathbb{R}$.
Let $y = \sqrt{x}$.
Since y is the nonnegative square root of x, then $y \in \mathbb{R}$ and $y^2 = x$ and $y \geq 0$.
Since $y \geq 0$, then either $y > 0$ or $y = 0$.
We consider these cases separately.
Case 1: Suppose $y = 0$.
Then $x = y^2 = 0^2 = 0$, so $x = 0$.
Case 2: Suppose $y > 0$.
Since $y \in \mathbb{R}$ and $y > 0$, then $y^2 > 0$.
Thus, $x = y^2 > 0$, so $x > 0$.
Therefore, in either case, $x \geq 0$. □

Proposition 67. *Let $x \in \mathbb{R}$.*
Then $\sqrt{x} \geq 0$ iff $x \geq 0$.

Proof. We first prove if $x \geq 0$, then $\sqrt{x} \geq 0$.
Suppose $x \geq 0$.
Then $x > 0$ or $x = 0$.
We consider these cases separately.
Case 1: Suppose $x = 0$.
Then $\sqrt{x} = \sqrt{0} = 0$.
Case 2: Suppose $x > 0$.
Then a unique positive square root of x exists in $\mathbb{R}$.
Thus, there is a unique $y \in \mathbb{R}$ such that $y^2 = x$ and $y > 0$.
Since $x > 0$ and y is a positive square root of x, then $y = \sqrt{x}$.
Thus, $\sqrt{x} = y > 0$.
Therefore, in either case, $\sqrt{x} \geq 0$. □

Proof. Conversely, we prove if $\sqrt{x} \geq 0$, then $x \geq 0$.
Suppose $\sqrt{x} \geq 0$.
Then $x > 0$ or $x = 0$.
We consider these cases separately.
Case 1: Suppose $\sqrt{x} = 0$.
Let $y = \sqrt{x}$.
Since y is the square root of x, then $y \in \mathbb{R}$ and $y^2 = x$.
Since $y = \sqrt{x} = 0$, then $y = 0$.
Thus, $x = y^2 = y \cdot y = 0 \cdot 0 = 0$, so $x = 0$.
Case 2: Suppose $\sqrt{x} > 0$.
Let $y = \sqrt{x}$.

Since y is the square root of x, then $y \in \mathbb{R}$ and $y^2 = x$.
Since $y = \sqrt{x} > 0$, then $y > 0$.
Since $y \in \mathbb{R}$ and $y > 0$, then $y^2 > 0$.
Thus, $x = y^2 > 0$, so $x > 0$.
Therefore, in either case, $x \geq 0$. □

Proposition 68. *Let $a, b \in \mathbb{R}$ with $a \geq 0$ and $b \geq 0$.*
Then $\sqrt{a} = \sqrt{b}$ iff $a = b$.

Proof. Since $a \geq 0$, then there exists a real number $x \geq 0$ such that $x^2 = a$ and $x = \sqrt{a}$.
Since $b \geq 0$, then there exists a real number $y \geq 0$ such that $y^2 = b$ and $y = \sqrt{b}$.
We prove if $\sqrt{a} = \sqrt{b}$, then $a = b$.
Suppose $\sqrt{a} = \sqrt{b}$.
Then $x = y$.
Hence, $a = x^2 = xx = xy = yy = y^2 = b$, so $a = b$, as desired. □

Proof. Conversely, we prove if $a = b$, then $\sqrt{a} = \sqrt{b}$.
Either both $x = 0$ and $y = 0$, or $x \neq 0$ or $y \neq 0$.
We consider these cases separately.
Case 1: Suppose $x = 0$ and $y = 0$.
Then $\sqrt{a} = x = 0 = y = \sqrt{b}$, so $\sqrt{a} = \sqrt{b}$.
Hence, the implication if $a = b$, then $\sqrt{a} = \sqrt{b}$ is trivially true.
Case 2: Suppose either $x \neq 0$ or $y \neq 0$.
We consider these cases separately.
Case 2a: Suppose $x \neq 0$.
Since $x \geq 0$ and $x \neq 0$, then $x > 0$.
Since $x > 0$ and $y \geq 0$, then $x + y > 0$.
Case 2b: Suppose $y \neq 0$.
Since $y \geq 0$ and $y \neq 0$, then $y > 0$.
Since $x \geq 0$ and $y > 0$, then $x + y > 0$.
Thus, in either case, $x + y > 0$, so $x + y \neq 0$.
We prove if $a = b$, then $\sqrt{a} = \sqrt{b}$ by contrapositive.
Suppose $\sqrt{a} \neq \sqrt{b}$.
Then $x \neq y$, so $x - y \neq 0$.
Since $x - y \neq 0$ and $x + y \neq 0$, then $x^2 - y^2 = (x - y)(x + y) \neq 0$, so $x^2 - y^2 \neq 0$.
Therefore, $a - b \neq 0$, so $a \neq b$, as desired. □

Proposition 69. *Let $a, b \in \mathbb{R}$.*
If $a \geq 0$ and $b \geq 0$, then $\sqrt{ab} = \sqrt{a}\sqrt{b}$.

Proof. Suppose $a \geq 0$ and $b \geq 0$.
Then $ab \geq 0$, so the square root of ab exists.
Since $a \geq 0$, then the square root of a exists, so $\sqrt{a} \geq 0$ and $\sqrt{a} \cdot \sqrt{a} = a$.
Since $b \geq 0$, then the square root of b exists, so $\sqrt{b} \geq 0$ and $\sqrt{b} \cdot \sqrt{b} = b$.

Since $\sqrt{a} \geq 0$ and $\sqrt{b} \geq 0$, then $\sqrt{a}\sqrt{b} \geq 0$.
Observe that

$$\begin{aligned}
(\sqrt{a} \cdot \sqrt{b})^2 &= (\sqrt{a} \cdot \sqrt{b})(\sqrt{a} \cdot \sqrt{b}) \\
&= \sqrt{a} \cdot (\sqrt{b} \cdot \sqrt{a}) \cdot \sqrt{b} \\
&= \sqrt{a} \cdot (\sqrt{a} \cdot \sqrt{b}) \cdot \sqrt{b} \\
&= (\sqrt{a} \cdot \sqrt{a})(\sqrt{b} \cdot \sqrt{b}) \\
&= ab.
\end{aligned}$$

Since $\sqrt{a} \cdot \sqrt{b} \geq 0$ and $(\sqrt{a} \cdot \sqrt{b})^2 = ab$ and the square root is unique, then $\sqrt{a} \cdot \sqrt{b}$ is the square root of ab.
Therefore, $\sqrt{ab} = \sqrt{a}\sqrt{b}$, as desired. □

Proposition 70. *Let $x \in \mathbb{R}$. Then*
1. $\sqrt{x} = 0$ *iff* $x = 0$.
2. $\sqrt{x^2} = |x|$.

Proof. We prove 1.
We prove if $x = 0$, then $\sqrt{x} = 0$.
Suppose $x = 0$.
Then $\sqrt{x} = \sqrt{0} = 0$.
Conversely, we prove if $\sqrt{x} = 0$, then $x = 0$.
Suppose $\sqrt{x} = 0$.
Then there exists $y \in \mathbb{R}$ such that $y^2 = x$ and $y = 0$.
Hence, $x = y^2 = 0^2 = 0$, so $x = 0$, as desired. □

Proof. We prove 2.
We must prove $\sqrt{x^2} = |x|$.
Either $x \geq 0$ or $x < 0$.
We consider these cases separately.
Case 1: Suppose $x \geq 0$.
Then $x^2 \geq 0$, so the square root of x^2 exists in $\mathbb{R}$.
Since $|x| = x \geq 0$ and $|x|^2 = x^2$ and the square root is unique, then $\sqrt{x^2} = |x|$.
Case 2: Suppose $x < 0$.
Then $x^2 > 0$, so the square root of x^2 exists in $\mathbb{R}$.
Since $|x| = -x > 0$ and $|x|^2 = (-x)^2 = x^2$ and the square root is unique, then $\sqrt{x^2} = |x|$.
Therefore, in all cases, $\sqrt{x^2} = |x|$, as desired. □

Lemma 71. *Let $x \in \mathbb{R}$.*
If $x > 0$, then $\sqrt{\frac{1}{x}} = \frac{1}{\sqrt{x}}$.

Proof. Suppose $x > 0$.
Then $\frac{1}{x} > 0$, so the square root of $\frac{1}{x}$ exists.
Since $x > 0$, then $\sqrt{x} > 0$, so $\frac{1}{\sqrt{x}} > 0$.

Observe that

$$
\begin{aligned}
(\frac{1}{\sqrt{x}})^2 &= \frac{1}{\sqrt{x}} \cdot \frac{1}{\sqrt{x}} \\
&= \frac{1 \cdot 1}{\sqrt{x} \cdot \sqrt{x}} \\
&= \frac{1}{\sqrt{x \cdot x}} \\
&= \frac{1}{\sqrt{x^2}} \\
&= \frac{1}{|x|} \\
&= \frac{1}{x}.
\end{aligned}
$$

Since $\frac{1}{\sqrt{x}} > 0$ and $(\frac{1}{\sqrt{x}})^2 = \frac{1}{x}$ and the square root is unique, then $\frac{1}{\sqrt{x}}$ is the square root of $\frac{1}{x}$.

Therefore, $\sqrt{\frac{1}{x}} = \frac{1}{\sqrt{x}}$. □

Proposition 72. *Let $a, b \in \mathbb{R}$.*
If $a \geq 0$ and $b > 0$, then $\sqrt{\frac{a}{b}} = \frac{\sqrt{a}}{\sqrt{b}}$.

Proof. Suppose $a \geq 0$ and $b > 0$.
Since $b > 0$, then $\frac{1}{b} > 0$.
Since $a \geq 0$ and $\frac{1}{b} > 0$ and $b > 0$, then

$$
\begin{aligned}
\sqrt{\frac{a}{b}} &= \sqrt{a \cdot \frac{1}{b}} \\
&= \sqrt{a} \cdot \sqrt{\frac{1}{b}} \\
&= \sqrt{a} \cdot \frac{1}{\sqrt{b}} \\
&= \frac{\sqrt{a}}{\sqrt{b}}.
\end{aligned}
$$

□

Lemma 73. *Let $a, b \in \mathbb{R}$.*
If $0 < a \leq b$, then $0 < a^2 \leq b^2$.

Proof. Suppose $0 < a \leq b$.
Then $0 < a$ and $a \leq b$.
Since $a \leq b$, then either $a < b$ or $a = b$.
We consider these cases separately.
Case 1: Suppose $a < b$.

Since $0 < a$ and $a < b$, then $0 < a < b$.
Therefore, $0 < a^2 < b^2$.
Case 2: Suppose $a = b$.
Since $a > 0$, then $a^2 > 0$.
Since $b = a$, then $b^2 = a^2$.
Therefore, $0 < a^2$ and $a^2 = b^2$, so $0 < a^2 = b^2$. □

Proposition 74. *Let $a, b \in \mathbb{R}$.*
Then $0 < a < b$ iff $0 < \sqrt{a} < \sqrt{b}$.

Proof. We prove if $0 < a < b$, then $0 < \sqrt{a} < \sqrt{b}$.
Suppose $0 < a < b$.
Then $0 < a$ and $a < b$, so $0 < b$.
Since $a > 0$, then $\sqrt{a} > 0$.
Since $b > 0$, then $\sqrt{b} > 0$.
Suppose $\sqrt{a} \geq \sqrt{b}$.
Then $0 < \sqrt{b} \leq \sqrt{a}$.
Hence, by the previous lemma $0 < (\sqrt{b})^2 \leq (\sqrt{a})^2$, so $0 < b \leq a$.
Thus, $b \leq a$, so $a \geq b$.
Therefore, we have $a < b$ and $a \geq b$, a violation of trichotomy.
Hence, $\sqrt{a} < \sqrt{b}$.
Thus $0 < \sqrt{a}$ and $\sqrt{a} < \sqrt{b}$, so $0 < \sqrt{a} < \sqrt{b}$, as desired. □

Proof. Conversely, we prove if $0 < \sqrt{a} < \sqrt{b}$, then $0 < a < b$.
Suppose $0 < \sqrt{a} < \sqrt{b}$.
Since $0 < \sqrt{a} < \sqrt{b}$ and $0 < \sqrt{a} < \sqrt{b}$, then $0 < (\sqrt{a})^2 < (\sqrt{b})^2$.
Therefore, $0 < a < b$, as desired. □

Corollary 75. *Let $x \in \mathbb{R}$.*
1. *If $0 < x < 1$, then $0 < x^2 < x < \sqrt{x} < 1$.*
2. *If $x > 1$, then $1 < \sqrt{x} < x < x^2$.*

Proof. We prove 1.
Suppose $0 < x < 1$.
Then $0 < x$ and $x < 1$.
Since $0 < x$ and $x > 0$, then $0 < x^2$.
Since $x < 1$ and $x > 0$, then $x^2 < x$.
Since $0 < x^2$ and $x^2 < x$, then $0 < x^2 < x$.
Thus, $0 < \sqrt{x^2} < \sqrt{x}$.
Since $x > 0$, then $\sqrt{x^2} = |x| = x$.
Hence, $0 < x < \sqrt{x}$, so $x < \sqrt{x}$.
Since $0 < x < 1$, then $0 < \sqrt{x} < \sqrt{1}$.
Thus, $0 < \sqrt{x} < 1$, so $\sqrt{x} < 1$.
Hence, $0 < x^2$ and $x^2 < x$ and $x < \sqrt{x}$ and $\sqrt{x} < 1$.
Therefore, $0 < x^2 < x < \sqrt{x} < 1$, as desired. □

Proof. We prove 2.
Suppose $x > 1$.
Then $x > 1 > 0$, so $x > 0$.
Since $0 < 1 < x$, then $0 < \sqrt{1} < \sqrt{x}$.
Hence, $0 < 1 < \sqrt{x}$, so $1 < \sqrt{x}$.
Since $1 < x$ and $x > 0$, then $x < x^2$.
Since $0 < x$ and $x < x^2$, then $0 < x < x^2$.
Hence, $0 < \sqrt{x} < \sqrt{x^2} = |x| = x$.
Thus, $0 < \sqrt{x} < x$, so $\sqrt{x} < x$.
Thus, $1 < \sqrt{x}$ and $\sqrt{x} < x$ and $x < x^2$.
Therefore, $1 < \sqrt{x} < x < x^2$, as desired. □

Proposition 76. ***the additive inverse of an irrational number is irrational***
Let $a \in \mathbb{R}$.
If a is irrational, then $-a$ is irrational.

Proof. We prove by contrapositive.
Suppose $-a$ is rational.
Then $-a \in \mathbb{Q}$, so $-(-a) \in \mathbb{Q}$.
Therefore, $a \in \mathbb{Q}$, so a is rational, as desired. □

Proposition 77. ***the sum of a rational and irrational number is irrational***
Let $a, b \in \mathbb{R}$.
If a is rational and b is irrational, then $a + b$ is irrational.

Proof. We prove by contrapositive.
Suppose a is rational and $a + b$ is rational.
Since a is rational, then $a \in \mathbb{Q}$, so $-a \in \mathbb{Q}$.
Since $a + b$ is rational, then $a + b \in \mathbb{Q}$.
Hence, by closure of $\mathbb{Q}$ under addition, $-a + (a + b) = (-a + a) + b = 0 + b = b \in \mathbb{Q}$.
Therefore, b is rational, as desired. □

Proposition 78. ***the reciprocal of an irrational number is irrational***
Let $a \in \mathbb{R}$.
If a is irrational, then $\frac{1}{a}$ is irrational.

Proof. We prove by contrapositive.
Suppose $\frac{1}{a}$ is rational.
Then $\frac{1}{a} \in \mathbb{Q}$ and $a \neq 0$.
Hence, $\frac{1}{a} \neq 0$, so $(\frac{1}{a})^{-1} = a \in \mathbb{Q}$.
Therefore, a is rational, as desired. □

Proposition 79. ***the product of a nonzero rational and irrational number is irrational***
Let $a, b \in \mathbb{R}$.
If a is a nonzero rational and b is irrational, then ab is irrational.

Proof. We prove by contrapositive.

Suppose a is a nonzero rational and ab is rational.

Since a is a nonzero rational, then $a \neq 0$ and $a \in \mathbb{Q}$, so $\frac{1}{a} \in \mathbb{Q}$.

Since ab is rational, then $ab \in \mathbb{Q}$.

Hence, by closure of $\mathbb{Q}$ under multiplication, $\frac{1}{a}(ab) = (\frac{1}{a}a)b = 1b = b \in \mathbb{Q}$.

Therefore, b is rational, as desired. $\square$

Corollary 80. ***the quotient of a nonzero rational and irrational number is irrational***

Let $a, b \in \mathbb{R}$.

If a is a nonzero rational and b is irrational, then $\frac{a}{b}$ is irrational.

Proof. Suppose a is a nonzero rational and b is irrational.

Since b is irrational, then $\frac{1}{b}$ is irrational.

Since a is a nonzero rational and $\frac{1}{b}$ is irrational, then $a \cdot \frac{1}{b} = \frac{a}{b}$ is irrational, as desired. $\square$

Proposition 81. $\mathbb{R} - \mathbb{Q}$ ***is dense in*** $\mathbb{Q}$

For every $a, b \in \mathbb{Q}$ with $a < b$, there exists $r \in \mathbb{R} - \mathbb{Q}$ such that $a < r < b$.

Proof. Let $a, b \in \mathbb{Q}$ such that $a < b$.

Then $a - \sqrt{2} < b - \sqrt{2}$.

Since $\mathbb{Q}$ is dense in $\mathbb{R}$, then there exists $q \in \mathbb{Q}$ such that $a - \sqrt{2} < q < b - \sqrt{2}$.

Thus, $a < q + \sqrt{2} < b$.

Let $r = q + \sqrt{2}$.

Since q is rational and $\sqrt{2}$ is irrational, then $q + \sqrt{2} = r$ is irrational.

Therefore, $r \in \mathbb{R} - \mathbb{Q}$ and $a < r < b$, as desired. $\square$

Solution. We consider the midpoint between a and b.

Since the midpoint is equidistant from a and b and the distance between a and b is $b - a$, then the midpoint is $a + (b - a)/2$.

Since $\sqrt{2}$ is irrational, we can adjust this slightly to create a potential irrational number $a + \frac{b-a}{2}\sqrt{2}$ between a and b.

We shall prove this number thus constructed is irrational and between a and b. $\square$

Proof. Let $a, b \in \mathbb{Q}$ with $a < b$.

Then $b - a > 0$.

Let $r = a + \frac{b-a}{2}\sqrt{2}$.

We must prove $r \in \mathbb{R}$ and $r \notin \mathbb{Q}$ and $a < r$ and $r < b$.

Since $a, b \in \mathbb{Q}$, then $b - a \in \mathbb{Q}$, so $\frac{b-a}{2} \in \mathbb{Q}$.

Thus, $\frac{b-a}{2}\sqrt{2} \in \mathbb{R}$, so $a + \frac{b-a}{2}\sqrt{2} = r \in \mathbb{R}$.

We prove $r \notin \mathbb{Q}$ by contradiction.
Suppose $r \in \mathbb{Q}$.
Since $r = a + \frac{b-a}{2}\sqrt{2}$, then $r - a = \frac{b-a}{2}\sqrt{2}$, so $2(r-a) = (b-a)\sqrt{2}$.
Since $b - a > 0$, then $b - a \neq 0$.
Thus, $\frac{2(r-a)}{b-a} = \sqrt{2}$.
Since $a, b, r \in \mathbb{Q}$ and $b - a \neq 0$, then by closure of $\mathbb{Q}$ under subtraction and multiplication, $\frac{2(r-a)}{b-a} \in \mathbb{Q}$.
Hence, $\sqrt{2} \in \mathbb{Q}$.
But, this contradicts the fact that $\sqrt{2} \notin \mathbb{Q}$.
Therefore, $r \notin \mathbb{Q}$.

We prove $a < r$.
Since $r = a + \frac{b-a}{2}\sqrt{2}$, then $r - a = \frac{b-a}{2}\sqrt{2}$.
Since $b - a > 0$, then $\frac{b-a}{2}\sqrt{2} > 0$, so $r - a > 0$.
Therefore, $r > a$, so $a < r$.

We prove $r < b$.
Since $\sqrt{2} < 2$, then $\frac{\sqrt{2}}{2} < 1$.
Since $b - a > 0$, then we multiply by $b - a$ to get $\frac{b-a}{2}\sqrt{2} < b - a$.
Therefore, $a + \frac{b-a}{2}\sqrt{2} < b$, so $r < b$. □

Proposition 82. $\mathbb{R} - \mathbb{Q}$ ***is dense in*** $\mathbb{R}$
For every $a, b \in \mathbb{R}$ with $a < b$, there exists $r \in \mathbb{R} - \mathbb{Q}$ such that $a < r < b$.

Proof. Let $a, b \in \mathbb{R}$ such that $a < b$.
Then $a - \sqrt{2} < b - \sqrt{2}$.
Since $\mathbb{Q}$ is dense in $\mathbb{R}$, then there exists $q \in \mathbb{Q}$ such that $a - \sqrt{2} < q < b - \sqrt{2}$.
Thus, $a < q + \sqrt{2} < b$.
Let $r = q + \sqrt{2}$.
Since q is rational and $\sqrt{2}$ is irrational, then $q + \sqrt{2} = r$ is irrational.
Therefore, $r \in \mathbb{R} - \mathbb{Q}$ and $a < r < b$, as desired. □