Square Roots

Theorem Let (F, P) be an ordered field.
Let $a \in P$. (0 is always its only sqroot.)

Define, $S_a := \{x \in F \mid x^2 \leq a\}$

Then,

1. $S_a \neq 0$ (as 0 is in the set)
2. S_a is bounded above (by $a+1$)

now we must show

3. $\sup(S_a)$ exists $\iff$ $x^2 = a$ has a solution in F and so $x^2 = \sup(S_a)$

Pf $\Leftarrow$

$x^2 = a$ has a solution in F. Let $b \in F$ be one such solution. As $(-b)^2 = b^2$, wlog we can say $b \in P$. (note $b \neq 0$ as $a > 0$).

note: $s \in S_a$ implies

$$s^2 \leq a = b^2 \quad \text{so} \quad s^2 \leq b^2 \quad \text{by hw2}$$

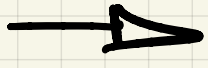
$$s \leq |s| \leq b$$

That is $\forall s \in S_a$, $s \leq b$, so b is an upper bound for S_a.

Furthermore, $b \in S_a$ as $b^2 = a \leq a$

So, b is a maximal element of S_a.

So, $b = \sup(S_a)$.



$\Rightarrow$ assume $\sup(S_a)$ exists and let $b = \sup(S_a)$

we want to show $b^2 = a$ why?

What can we say about b?

As $0 \in S_a$ (since $0 < a^2$ $\forall a \in P$)

So, $b \geq 0$.

We will show $b \neq 0$.

Claim: if $b = 0$, then

$S_a = \{0\}$ → If another element exists in S_a it is positive so $\sup(A)$ is positive. $\because (-b)^2 = b^2$

Lets now show $S_a \neq 0$.

Recall) $a > 0$ & if $a > 1$ then $a^2 > a > 1 = 1^2$

So, $1 \in S_a$

if $a \leq 1$, then $a^2 \leq a$ so, $a \in S_a$.

In either case $S_a \neq \{0\}$

So $b \neq 0$ and $b > 0$.

We want to show $b^2 = a$, by trichotomy exactly 1 of the 3 holds:

(I) $b^2 = a$ (II) $b^2 > a$ (III) $b^2 < a$

We want to exclude (II) and (III).

Assume (III) holds, i.e. $b^2 < a$

Set $\varepsilon_0 := a - b^2 > 0$

set $\varepsilon := \min\left(1, \frac{\varepsilon_0}{2+4b}\right) \in P$ as $b \in P$

set $b' := b + \varepsilon > 0$

since $\varepsilon > 0$ $b' > b$

Plan Show $(b')^2 < a$

if we do this $b' \in A$. But, $b' > b$ and b is defined to be the supremum so, oops.

$$(b')^2 = (b^2 + 2b\varepsilon + \varepsilon^2)$$

$$b^2 = (a - \varepsilon_0) \quad \text{(by our definition of } \varepsilon_0\text{)}$$

$$(b')^2 = (a - \varepsilon_0) + 2b\varepsilon + \varepsilon^2$$

So $(b')^2 \leq a$ iff $-\varepsilon_0 + 2b\varepsilon + \varepsilon^2 \leq 0$, so lets show that this holds.

$\varepsilon^2 + 2b\varepsilon \leq \varepsilon_0$

↳ $\varepsilon(2b + \varepsilon)$ as $\varepsilon \leq 1$ this is less than or equal to $\varepsilon(2b+1) \leq \frac{\varepsilon_0(2b+1)}{2+4b}$ as $\varepsilon \leq \frac{\varepsilon_0}{2+4b}$

$= \frac{\varepsilon_0}{2}$ which is certainly less than ε_0.

$\therefore (b')^2 < a$ And we get a contradiction so (III) doesn't hold.

Assume (III) holds, spose $b^2 > a$.

set $\varepsilon_0 := b^2 - a > 0$

set $\varepsilon := \min\left(b, \frac{\varepsilon_0}{2+4b}\right)$ $\in P$ for the same reason as earlier ($b > 0$).

$b' := b - \varepsilon$

As $\varepsilon \leq b$ we know

$b' \geq 0$ and $b' < b$.

Plan Show $a < (b')^2$. Then b' is an upper bound for S_a as $S_a := \{x \in F \mid x^2 \leq a\}$

fix $y \in S_a \Rightarrow y^2 \leq a < b^2 \Rightarrow y^2 < b'^2 \Rightarrow |y| < |b|$

$y \leq |y| < |b|$

if b' is an upper bound we have a problem as $b' < b$ and b is $\sup(S_a)$. oops!

lets show $(b')^2 \geq a$

$$(b')^2 = (b-\varepsilon)^2 = b^2 - 2b\varepsilon + \varepsilon^2$$
$$= (\varepsilon_0 + a) - 2b\varepsilon + \varepsilon^2$$

if $a < (b')^2$ then, $\varepsilon_0 - 2b\varepsilon + \varepsilon^2 > 0$,

$$\varepsilon_0 - 2b\varepsilon + \varepsilon^2 = \varepsilon_0 + \varepsilon(\varepsilon - 2b) \quad \text{as } -1 < \varepsilon$$
$$> \varepsilon_0 + \varepsilon(-1 - 2b)$$
$$> \varepsilon_0 - \varepsilon(1 + 2b)$$
$$\geq \varepsilon_0 - \frac{\varepsilon_0}{2+4b}(1+2b)$$
$$= \frac{\varepsilon_0}{2}$$

So, garbage $> \frac{\varepsilon_0}{2} > 0$ $\therefore$ garbage $\in P$.

$\therefore a < (b')^2 \rightarrow$ contradiction

So, (II) doesn't hold. By trichotomy,

$$b^2 = a$$

□

What did we just prove?

↳ in an ordered field, we now know exactly when a postive element has a square root. It is when $\sup(S_a)$ exists in F.

$S_a := \{x \in F \mid x^2 \leq a\}$

Corollary due to completeness all positive elements of $\mathbb{R}$ have square roots in $\mathbb{R}$.

Weak Induction

Def The $S \subseteq \mathbb{N}$ is said to be weakly inductive if
1. $1 \in S$
2. $k \in S \rightarrow k+1 \in S$

Thm Every weakly inductive $S \subseteq \mathbb{N}$ causes $S = \mathbb{N}$.

Pf Clear since every weakly inductive set is inductive and $\mathbb{N}$ is the smallest inductive set so, $\mathbb{N} \subseteq S$. By 2 way containment $S = \mathbb{N}$.

Real Important Lemma

Lemma $\forall n \in \mathbb{N}, \; n \geq 1$.

Ie: 1 is the minimal element of $\mathbb{N}$.

Pf Define $S := \{m \in \mathbb{N} \mid m \geq 1\}$

Show S is weakly inductive

- $1 \in S$? yes
- fix $x \in S$

$\Rightarrow x \geq 1$

$\Rightarrow x+1 \geq 2 > 1 \quad \Rightarrow x+1 > 1 \Rightarrow x+1 \geq 1$

So $x+1 \in S$

$\therefore S$ is weakly inductive and the property holds for all $n \in \mathbb{N}$.

BIG PROOF Incoming →

Lemma $\forall n, m \in \mathbb{N}$ we have

$$m > n \iff m \geq n+1$$

Corollary $\forall n, m \in \mathbb{N}$, we have

$$n < m \leq n+1 \iff m = n+1$$

Immediate from lemma. $\Leftarrow$ is free

$\Rightarrow$

$n < m \leq n+1$

↳ by lemma $m \geq n+1$ } $m \geq n+1$, $m \leq n+1$ } $m = n+1$

Pf fix $m, n \in \mathbb{N}$

note: $\Leftarrow$ is immediate

$m \geq n+1 > n$

$\Rightarrow$

Note: Things get messy and we will do a double induction

fix $m, n \in \mathbb{N}$, assume $m > n$.

Def given $k \in \mathbb{N}$

$$T_k := \{ l \in \mathbb{N} \mid l \leq k \text{ or } l = k'+1 \text{ for some } k' \in \mathbb{N} \text{ w/ } k' \geq k \}$$

Consider T_n. If we show $m \in T_n$, we're done. because then we know either $m = n+1$ for $n' \geq n$ $n' \in \mathbb{N}$ or $m < n$ ↳ false.

↳ if true $m = n'+1 \geq n+1$ as $n' \geq n$.

We want $m \in T_n$. It will be enough to show $T_n = \mathbb{N}$ as $m \in \mathbb{N}$.

Show $T_n = \mathbb{N}$. Here it goes ...

Consider $T := \{ s \in \mathbb{N} \mid T_s = \mathbb{N} \}$

If we show $T = \mathbb{N}$ we win

Claim: T is weakly inductive

- $1 \in T$? Lets check. We must show T_1 is weakly inductive

$T_1 := \{ l \in \mathbb{N} \mid l \leq 1 \text{ or } l = n'+1 \text{ for } n' \in \mathbb{N}, n' \geq 1 \}$

→ $1 \in T_1$? yes

→ $x \in T_1 \rightarrow x+1 \in T_1$.

If $x \in T_1$, we know $x \leq 1$ or $x > 1$.

↳ by our lemma

$x > 1$ and $x \in T_1$

$\exists n' \in \mathbb{N}$ $x = n'+1$ $n' \geq 1$

$x = 1$ so $x+1 = 2$ which is in T_1

Then $x+1 = n'+1+1$

So is $(x+1) \in T_1$? Yes as $n'+1 > n \geq 1$

$\Rightarrow$ T_1 is weakly inductive

- Spose $k \in T$ show $k+1 \in T$

Since $k \in T$ we know $T_k = \mathbb{N}$

$T_k := \{ l \in \mathbb{N} \mid l \leq k \text{ or } l = n'+1 \text{ for } n' \in \mathbb{N}, n' \geq k \}$

We need to get $T_{k+1} = \mathbb{N}$

We need to get $T_{k+1} = \mathbb{N}$ by 2 way containment.

By definition $T_{k+1} \subseteq \mathbb{N}$. So lets show $\mathbb{N} \subseteq T_{k+1}$

Let $r \in \mathbb{N}$. Show $r \in T_{k+1}$

Since $r \in \mathbb{N}$ either $r \leq k+1$ or $r > k+1$

If $r \leq k+1$ $r \in T_{k+1}$

If $r > k+1$ we need to show $\exists\, n'' \in \mathbb{N}$ with $n'' \geq k+1$ s.t $r = n''+1$

Since $T_1 = \mathbb{N}$ and $r \in \mathbb{N}$ we know $r \in T_1$, this means that $r=1$ or $\exists\, n' \in \mathbb{N}$ s.t $n' \geq 1$ $r = n'+1$ since $r > k+1$, $r \neq 0$.

↳ Using this, we proceed.

Because $k \in T$, we know $n' \in T_k$ so,

$n' \leq k$ or $n' = n''' + 1$ where $n''' \geq k$

$r > k+1$ by def

$r = n'+1$

$n'+1 > k+1$

$\Rightarrow$ $n' > k$ so this is true

Putting everything together

$r = n'+1$, $n' \geq 1$

$n' = n'''+1$, $n''' \geq k$

$r = (n'''+1)+1$ where $n'''+1 \geq k+1$

So $r \in T_{k+1}$

$\therefore$ $T_{k+1} = \mathbb{N}$

So T is inductive and $T = k$

So, $\forall\, n, m \in \mathbb{N}$ $m > n \iff m \geq n+1$

Defn Let (F,P) be an ordered field the subset $U \subseteq F$ is said to be well ordered p.t every nonempty $V \subseteq U$ has a minimal element.

Thm $\mathbb{N}$ is well ordered as a subset of $\mathbb{R}$.

Pf Let $V \subseteq \mathbb{N}$ be non-empty

Task: Show V has a minimal element.

Consider: $L_V := \{k \in \mathbb{N} \mid k$ is a strict lower bound for $V\}$ ↪ lower bound and $k \notin V$

What can we say about L_V? Focus on 1.

① $1 \notin L_V$, this means $1 \in V$. Why, because if $1 \notin V$, then $1 < v \ \forall v \in V$. In this case 1 is a strict lower bound for V so $1 \in L_V$.

We are happy because in this case 1 is a min elt.

② $1 \in L_V$,

Since $V \neq \emptyset$, we know $L_V \neq \mathbb{N}$ because $L_V \cap V = \emptyset$.

This means L_V contains 1 and $L_V \neq \mathbb{N}$.

As $L_V \neq \mathbb{N}$ L_V isn't inductive, so a criteria of inductivity must fail. As $1 \in L_V$, the $x \in L_V \to x+1 \in L_V$ criterion fails.

So, $\exists k \in L_V$ s.t $k+1 \notin L_V$.

Thus $k < n \ \forall n \in V$ as $k \in L_V$

$\bullet \exists n_0 \in V$ s.t $k+1 \geq n_0$] $k+1 \notin L_V$

Putting this together we have.

since $n_0 \in V$ and $k \in L_V$, $k < n_0 \leq k+1$ ↪ by lemma

$n_0 = k+1$

Claim $n_0 = \min(V)$

true since $\forall n \in V$, $n < k \Rightarrow n \leq k+1$ (by lemma)

So, $n \leq n_0$

So n_0 is a lower bound for V and $n_0 \in V$. $\therefore n_0 = \min(V)$

Defn $S \subseteq \mathbb{N}$ is strongly inductive s.t $\forall n \in \mathbb{N}$ if,

$$\{k \in \mathbb{N} \mid k < n\} \subseteq S$$

then $n \in S$

Remark: if $S \subseteq \mathbb{N}$ has this property we automatically get $1 \in S$ as $\emptyset \subseteq S$.

Thm If $S \subseteq \mathbb{N}$ is strongly inductive $S = \mathbb{N}$.

Pf Spose $S \subseteq \mathbb{N}$ is strongly inductive. If $S \neq \mathbb{N}$, then $V = \mathbb{N} \setminus S \neq \emptyset$. Let $v = \min(V)$ (as $\mathbb{N}$ is well ordered). If $n \in \mathbb{N}$, $n < v$, then $n \notin V$, and $n \in S$. Thus we have $\forall n < v \; n \in S \Rightarrow v \in S$ because S is strongly inductive. ← definition.

as $v = s'$ in context of $\mathbb{N}$.

But this is bad because $v \in V$ and $S \cap V = \emptyset$ by definition. oops.

So $S = \mathbb{N}$.

Recursion: Spivak

Big Deal: Division alg.

$\forall D, d \in \mathbb{N}$ $\exists!$ $q, r \in \mathbb{N} \cup \{0\}$ with $r < d$ s.t

$D = d \cdot q + r$

Pf Since there are 2 assertions, prove uniqueness first.

fix $d, D \in \mathbb{N}$

spose $D = q'd + r' = qd + r$ for $q, q', r, r' \in \mathbb{N} \cup \{0\}$ $r, r' < d$.

wlog, spose $r \geq r' \to r - r' \in P$

Then, $0 = d(q'-q) + (r'-r)$

$0 \leq r - r' = d(q'-q)$

$r - r' < d$ → by definition as $r, r' < d$

$0 \leq d(q'-q) < d$

$0 \leq q' - q < 1$

by our lemma,

$q' - q = 0$ ⇒ $q' = q$

Using this its easy to show $r' = r$

Pf of Existence

Fix $d \in \mathbb{N}$ → ignore fixing D for now.

Consider $S = \{D \in \mathbb{N} \mid D = qd + r$ for $q, r \in \mathbb{N}$ w/ $r < d\}$

↳ the set of all numbers that can be written as a linear combination of d or $qd+r$ (intuitively this is all of $\mathbb{N}$)

Show S is strongly inductive. ∴ $S = \mathbb{N}$ ∴ $D \in S$.

Fix $D_0 \in \mathbb{N}$, so that $D \in S$ whenever $D < D_0$.

Show $D_0 \in S$. There are 3 possibilities,

I $D_0 = d$

take $q = 1$, $r = 0$, $D_0 = qd + r = d$ so $D_0 \in S$

II $D_0 < d$

take $q = 0$, $r = D_0$, $D_0 = d$, so $D_0 \in S$

2 $D_0 > d$

So, $D_0 - d \in \mathbb{N}$

and $D_0 - d < D_0$ as d is non-zero

we have by assumption,

$D_0 - d \in S$ so strong induction

$\exists\, q, r \in \mathbb{N} \cup \{0\}$ with $r < d$ s.t

$D_0 - d = qd + r$ thus,

$D_0 = (q+1)d + r$ so $D_0 \in S$

In all 3 cases $D_0 \in S$. So, S is strongly inductive. So, we are done as $D \in S$.

Lets talk about integers !!

$\mathbb{Z} = \{x \in \mathbb{R} \mid |x| \in \mathbb{N} \cup \{0\}\}$

Define Let $a, b \in \mathbb{N}$. The element a is called a divisor of b pt $\exists\, m \in \mathbb{N}$ s.t

$$b = a \cdot m$$

in this case $a \mid b$ so a divides b

Define let $a, b \in \mathbb{N}$. The gcd (a,b) is their greatest common divisor.

$S = \{d \in \mathbb{N} \mid d \mid a \text{ and } d \mid b\}$

S is nonempty as $1 \mid a$ and $1 \mid b$.

Bounded above by $\min(a,b)$.

Does it have a maximal element

This is a finite set (see HW3).

By HW3, this set has a maximal element.

Bezout Lemma

Spose $a, b \in \mathbb{N}$. Then $\exists m, n \in \mathbb{Z}$ s.t.
$a \cdot m + b \cdot n = \gcd(a, b)$

Caution: no claim about uniqueness of a and b.

Pf fix $a, b \in \mathbb{N}$

let $S = \{ am + bn \mid m, n \in \mathbb{Z},\ am+bn \in \mathbb{N} \}$

note: (1) $S \neq \emptyset$ $\quad a = a \cdot 1 + b \cdot 0 \in S$

(2) $S \subseteq \mathbb{N}$

(1) + (2) imply S has a least element $\rightarrow$ well ordered

Lets call this element s'.

So, $s' = a \cdot m' + b \cdot n'$ for some $m', n' \in \mathbb{Z}$

We will show $s' \mid a$ and $s' \mid b$.

But we also need to show that it is the greatest common divisor.

(A) Show $s' \mid a$

by division alg,

$\exists q, r \in \mathbb{N} \cup \{0\}$ with $r < s'$

s.t. $a = q \cdot s' + r$

$r = a - q \cdot s'$

$= a - (q(am' + bm'))$

$r = (1 - qm') \cdot a - (qn')b$

Is this in the set S? Its of the right form but it is only in S iff it is positive. If so, it implies $r \in S$. But since $r < s'$ (which is $\min(S)$), oops.

Thus, the expression isn't positive. Since $r \in \mathbb{N} \cup \{0\}$, it can't be negative. $\therefore$ by trichotomy it is 0 and $r = 0$.

So, $a = q \cdot s'$

$s' \mid a$

(B) Similar argument for B $\quad s' \mid b$

(A)(B) $\rightarrow$ s' is a common divisor of a and b.

We are done if $s' = \gcd(a,b)$ as it shows for some element in the set Bezout it satisfied.

Last part Let d be a common factor of a and b.

We must show $d \geq s'$.

Since $d \mid a$ and $d \mid b$,

$d \mid (a \cdot m' + b n')$

So $d \mid s'$

$\Rightarrow \exists\, q \in \mathbb{N}$ st

$s' = q \cdot d$, $\quad q \geq 1$

$dq \geq d$

$s' \geq d$

$\therefore$ s' is the gcd (a,b) and we win