Constructible Numbers
If \(a, b, c\) are constructible & \(> 0\),

\[
\begin{array}{c|c|c}
-1 & 0 & 1 \\
\hline
\end{array}
\]

if \(b < c\)
\[
\begin{align*}
\frac{c}{b} &= \frac{a}{x} \\
\frac{b}{c} &= \frac{x}{a} \\
x &= \frac{ac}{b}
\end{align*}
\]

So can construct \(\frac{ac}{b}\) for \(a, b, c\) positive constructed numbers. In particular, take \(b = 1\), shows can construct the product of any two constructible positive numbers.

Take \(c = 1\), show can construct quotient of any two constructible positive numbers.
Let \(C = \) set of all constructible numbers.

If \(x \in C\), \(-x \in C\).
0,1 ∈ C
If a,b ∈ C, so is a + b.

**Definition:** A subset F of R is a number field if
1) 0,1 ∈ F
2) If x,y ∈ F, so are x + y & x * y.
3) If x ∈ F, so is –x.
4) If x ∈ F & x ≠ 0, then 1/x ∈ F.

Above we showed: C is a number field.

C ⊆ Q

Eg. R, Q are number fields
Q(√2) is defined to be {a + b√2: a,b ∈ Q}

Obviously Properties 1,3,4 hold
Property 2:
\[(a + b \sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (bc + ad)\sqrt{2} ∈ Q(\sqrt{2})\]

Property 4:
\[\frac{1}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}\]

If \[a^2 - 2b^2 = 0\]
\[a^2 - 2b^2 \ (a/b)^2 = 2 \implies \sqrt{2} \text{ rational, contradiction.} \]
\[∴ \text{ If } a,b \text{ not both 0, } 1/a+b \sqrt{2} \in Q(\sqrt{2})\]

More generally, if F any number field & r ∈ F, r > 0, but √r ∈ F.
We define \[F(\sqrt{r})\] (the field of F extended by square root of r
\[= \{ a + b\sqrt{r} : a,b ∈ F \}\]

Lemma: If F, r as above, then F(√r) is a number field.
Proof: 0,1, ∈ F.
closed under +, *, -

\[\frac{1}{a+b\sqrt{r}} = \frac{a-b\sqrt{r}}{a^2-rb^2} = \frac{a}{a^2-rb^2} - \frac{b}{a^2-rb^2}\sqrt{r} \quad \text{if } a^2 - rb^2 ≠ 0\]

But if \[a^2 - rb^2 = 0\]
\[(a/b)^2 = r \implies r \in F, \text{ contradiction}\]

Eg. F = Q(√2), r = √3.
\[F(\sqrt{3}) = (Q(\sqrt{2}))(\sqrt{3})\]
\[= \{ a + b\sqrt{3} : a,b ∈ Q(\sqrt{2}) \}\]
\[= \{ a_1 + a_2\sqrt{2} + (b_1 + b_2\sqrt{2})\sqrt{3} : a_1,a_2,b_1,b_2 ∈ Q \}\]

Definition: A tower of number fields is a finite collection of number fields which each obtained from
the previous one by adjoining a square root:
F₀ a number field
F₁ = F₀(√r₀) with r₀ ∈ F, r₀ > 0, √r₀ ∉ F₀
F₂ = F₁(√r₁) with r₁ ∈ F, r₁ > 0, √r₁ ∈ F₁
Theorem: If \( r \in C \) & \( r > 0 \), then \( \sqrt{r} \in C \)

Proof:

![Diagram of proof](image)

bisect \( r + 1 \). constructing \( M = \frac{r + 1}{2} \)

Make circle center \( M \) and radius \( M \)

Erect a perpendicular at \( r \). Make Triangles.

\[ \angle OCA = 90^\circ \]
\[ \angle COD + \angle OCD = 90^\circ \]
\[ \angle DCA + \angle OCD = 90^\circ \]

\[ \therefore \angle COD = \angle DCA \]

\[ \triangle OCD \text{ is similar (\( \sim \)) to } \triangle ACD \]

\[ \therefore x/l = r/x, \quad x^2 = r \]

\[ \therefore x = \sqrt{r}, \text{ and } x \in C, \text{ so } \sqrt{r} \in C. \]

Corollary: If \( Q \subset F_1 \subset F_2 \subset F_3 \ldots \subset F_k \) is any tower

(i.e. \( F_j = F_{j-1}(\forall_{j-1}) \) with \( r_{j-1} \in F_{j-1} \) \( r_{j-1} > 0, \sqrt{r_{j-1}} \notin F_{j-1} \)), then

\( F_k \subset C \)

Definition: A surd is a number that is in some \( F_k \) that is in a tower starting at \( Q \).

Corollary: The collection of surds is contained in \( C \) (or, every surd is constructible).

Let \( S = \) set of all surds

\( C = \) set of all constructible numbers.

Proved: \( S \subset C \).

Want: \( S = C \).

To construct numbers: We start with 0.1, get \( Q \)

Note: Can construct point \( (a,b) \) in plane if and only if can construct numbers \( a \& b \).

If we can construct \( a,b \). We can construct the point \( (a,b) \).
Given the point \((a, b)\), we have \(a, b\).

\[ y - b = d - b \]
\[ x - a = c - a \]

All coefficients are in \(F\). Equation of form \(sx + ty = u\), with \(s, t, u \in F\).

This proves: a line joining points whose coordinates are in a number field \(F\) has an equation with coefficients in \(F\).

Note: If 2 lines have equations with coefficients in \(F\), then the coordinates of points of intersection one in \(F\). (solve simultaneously)

This proves: If a point is constructed as the intersection of 2 lines, both of which are determined by points with coefficients in \(S\), then that point has coefficients in \(S\).

Given a circle with center \((a, b)\) and radius \(r\), & if \(a, b, r \in F\) (\(F\) number field) an equation of circle: \((x-a)^2 + (y-b)^2 = r^2\). coefficients in \(F\).
**Lemma:** Points constructed by intersecting a line determined by surd points & a circle with surd radius and surd center has surd coordinates.

Proof: Circle has equation
\[ x^2 + b x + y^2 + cy + d = 0. \text{ } b,c,d \in S \]
Line has equation \( ex + fy + g = 0. \text{ } e,f,g \in S. \)
Simultaneous solution keeps within surd field:
\[ y = sx + t... s,t \in S \]
\[ x^2 + bx + (sx + t)^2 + c(sx + t) + d = 0. \]
Get quadratic in \( x \), use quadratic formula \( \Rightarrow \) within \( F(\sqrt{r}) \) if coefficients in \( F \& r = b^2 - 4ac. \) Stay in surds.

2 circles intersecting
\[ x^2 + ax + y^2 + by + c = 0 \]
\[ x^2 + dx + y^2 + ey + f = 0 \]
\( (a-d)x + (b-e)y + c-f = 0 \Rightarrow \) Simultaneously solve both.

\[ S = C \]

(subtraction --- share intersection)