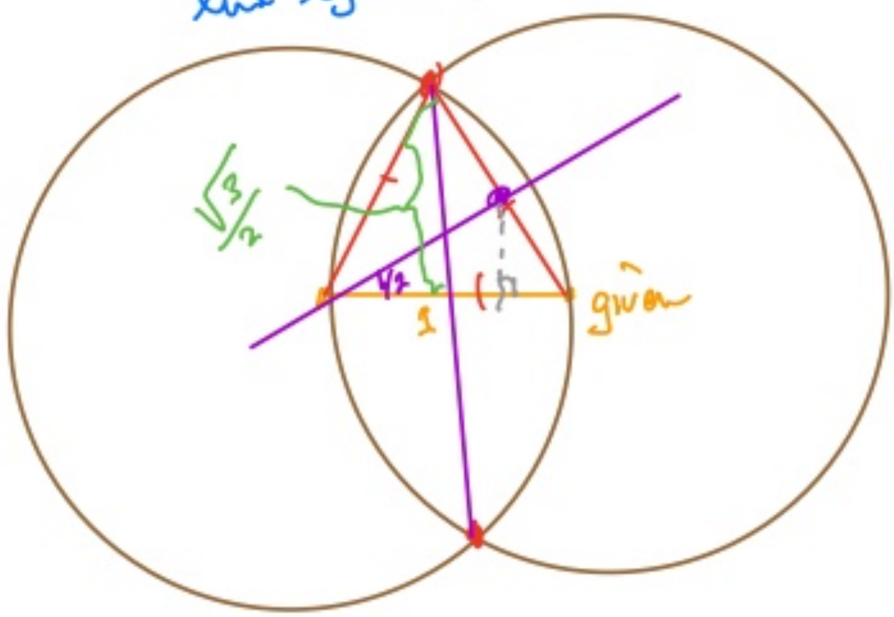
Application of Extension Fields

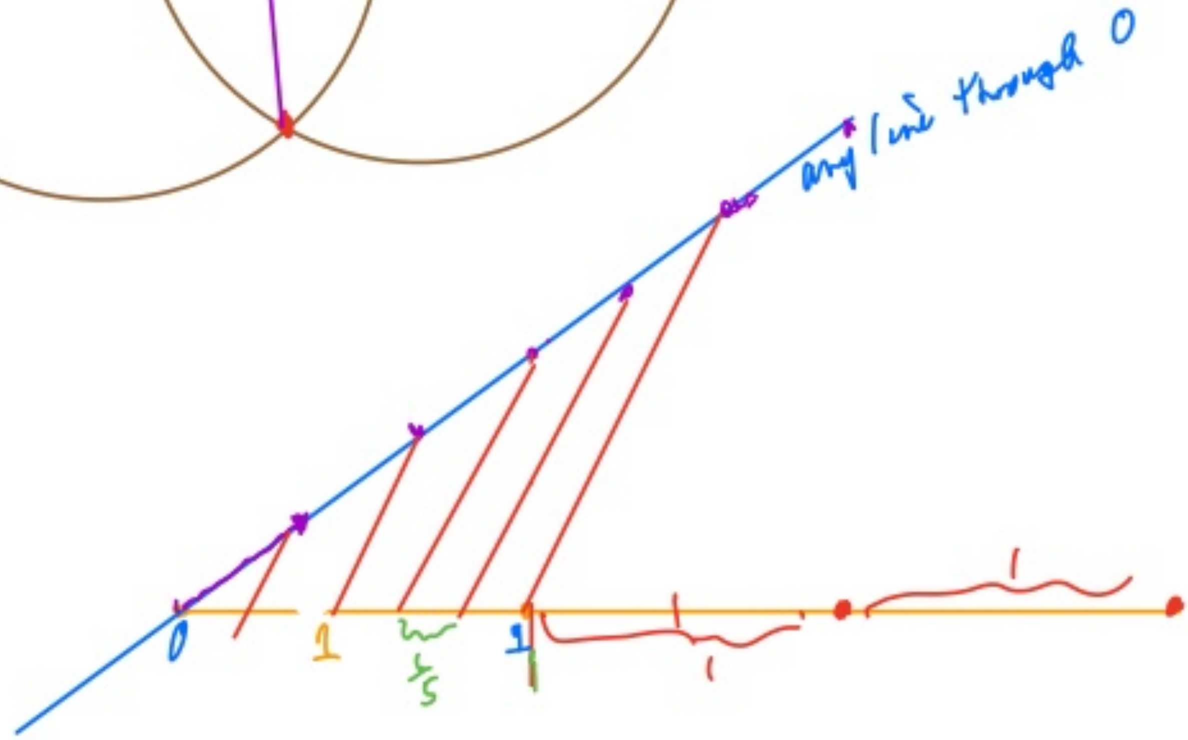
Recall: Geometric constructions in the plane.

— allowed to use an unmarked straight edge (SE) — can use that to draw the line segment (or line) connecting any two given points in the plane.

— given a compass (collapsing) (C) — you can draw a circle with any given center & a point on the circle.

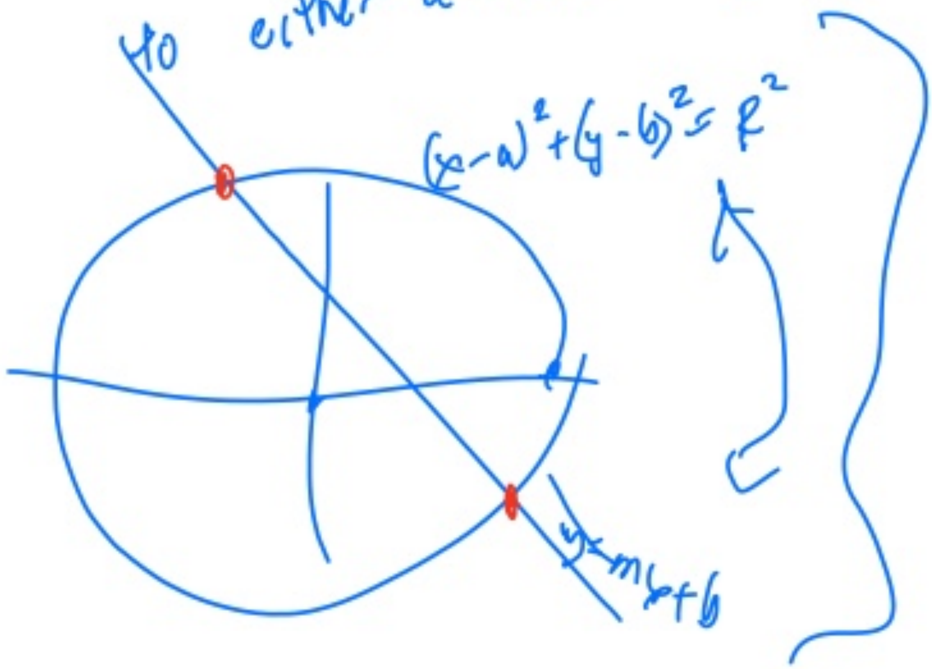
A constructible number is a length of a line segment that could be constructed using a SE & C, given a line segment of length 1.





Thus every element $x \in \mathbb{Q}_{>0}$ is constructible.

When using each of the operations allowed, the coordinates of the new points are solutions to either a linear or quadratic equation.

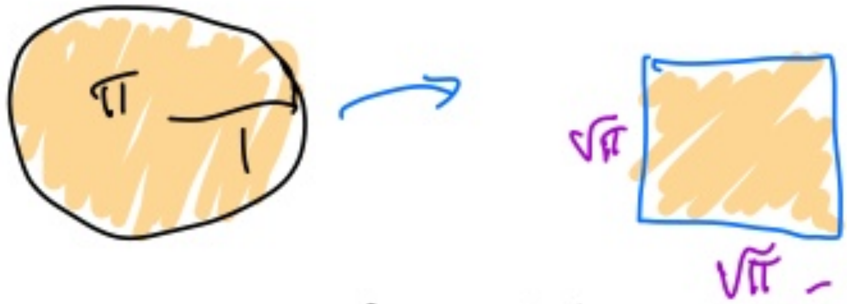


$\Rightarrow$ All constructible numbers α satisfy

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k \text{ for some } k \geq 0.$$

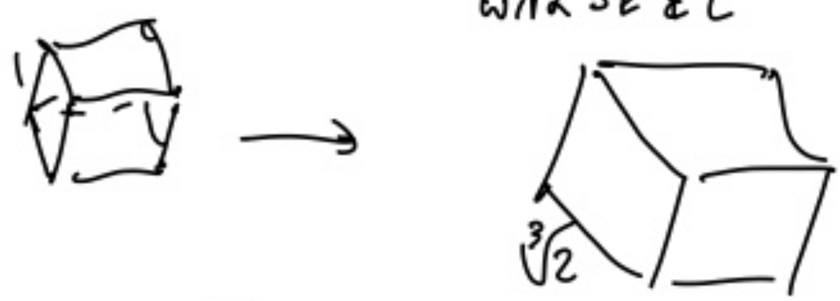
<u>Consequences:</u> ① Can you square the circle?

with SE & C, can you construct a square with the same area as a given circle?



This is impossible: $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$
(not 2^k).

② Can you duplicate the cube? with SE & C



But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

$\therefore$ impossible

③ Can we trisect a given angle?

If we could, we know we can construct a 60° angle $\Rightarrow$ can construct $\cos(60^\circ) = \frac{1}{2}$
$\sin(60^\circ) = \frac{\sqrt{3}}{2}$.

Suppose we are able to construct a 20° angle.

$\Rightarrow$ $\cos(\underset{\theta}{20^\circ})$ is a constructable #.

But: $\frac{1}{2} = \cos(3\theta) = \cos(2\theta + \theta) = \cos(2\theta)\cos(\theta) - \sin(2\theta)\sin(\theta)$
$= (2\cos^2\theta - 1)\cos\theta - 2\sin^2\theta\cos\theta$

$$= 2\cos^3\theta - \cos\theta - 2((1-\cos^2\theta)\cos\theta)$$

$$\frac{1}{2} = 4\cos^3\theta - 3\cos\theta$$

$\Rightarrow \cos(20^\circ)$ is a root of $4x^3 - 3x - \frac{1}{2} = 0$

a root of $8x^3 - 6x - 1$

rational roots test: $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$

$\Rightarrow$ no linear factor

$\Rightarrow 8x^3 - 6x - 1$ is irred over $\mathbb{Q}$.

$$\therefore [\mathbb{Q}(\cos(20^\circ)) : \mathbb{Q}] = 3$$

$\therefore \cos(20^\circ)$ is not constructable.

Finite Fields — suppose F has characteristic p and is finite. As an abelian group, every element must have order p.

prime

FTFGAG $\Rightarrow$ as an abelian group,

$$F \underset{\text{Group}}{\cong} \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}$$ This means $|F| = p^k$ for some k.

Note every F of char p contains a subgroup of $\mathbb{Z}_p$. $\{1, 1+1, \ldots, \overbrace{1+1+\cdots 1}^{p}\}$
0

(actually a subfield of F)

$$\mathbb{Z}_p \leq F$$

Prop Suppose F is a field of order q. ($q = p^k$) Then every finite extension E of F has order q^n. ($q^n = p^{kn}$)

Pf. We can choose a basis of E over F to be $\{1, \alpha_1, \alpha_2, \dots, \alpha_m\}$ for some n.

Then $E = \{x_0 1 + x_1\alpha_1 + x_2\alpha_2 + \dots + x_m\alpha_m : x_j \in F \ \forall j\}$.

— has order q^{m+1}. $\blacksquare$

Cor. If F is a finite field of char p, then $|F| = p^n$ for some $n \geq 0$.