The Limitations of Ruler-and-Compass Constructions

Hayden Jananthan

Vanderbilt University

The setting is $\mathbb{R}^2$.

The setting is $\mathbb{R}^2$.
Ruler and compass constructions involve the following tools:

The setting is $\mathbb{R}^2$.
Ruler and compass constructions involve the following tools:

- Given constructed points A, B, we can draw the line $\overleftrightarrow{AB}$ or the line segment $\overline{AB}$.

The setting is $\mathbb{R}^2$.
Ruler and compass constructions involve the following tools:

- Given constructed points A, B, we can draw the line $\overleftrightarrow{AB}$ or the line segment $\overline{AB}$.
- Given constructed points A, B, we can draw the circle C with center A which passes through B.

The setting is $\mathbb{R}^2$.

Ruler and compass constructions involve the following tools:

- Given constructed points A, B, we can draw the line $\overleftrightarrow{AB}$ or the line segment $\overline{AB}$.
- Given constructed points A, B, we can draw the circle C with center A which passes through B.

What are "constructed points"? We define them inductively:

The setting is $\mathbb{R}^2$.

Ruler and compass constructions involve the following tools:

- Given constructed points A, B, we can draw the line $\overleftrightarrow{AB}$ or the line segment $\overline{AB}$.
- Given constructed points A, B, we can draw the circle C with center A which passes through B.

What are "constructed points"? We define them inductively:

- We start by letting $(0, 0)$ and $(0, 1)$ be constructed.

The setting is $\mathbb{R}^2$.

Ruler and compass constructions involve the following tools:

- Given constructed points A, B, we can draw the line $\overleftrightarrow{AB}$ or the line segment $\overline{AB}$.
- Given constructed points A, B, we can draw the circle C with center A which passes through B.

What are "constructed points"? We define them inductively:

- We start by letting $(0, 0)$ and $(0, 1)$ be constructed.
- If lines ℓ_1, ℓ_2 have been constructed already, then their intersection point have been constructed.

The setting is $\mathbb{R}^2$.
Ruler and compass constructions involve the following tools:

- Given constructed points A, B, we can draw the line $\overleftrightarrow{AB}$ or the line segment $\overline{AB}$.
- Given constructed points A, B, we can draw the circle C with center A which passes through B.

What are "constructed points"? We define them inductively:

- We start by letting $(0, 0)$ and $(0, 1)$ be constructed.
- If lines ℓ_1, ℓ_2 have been constructed already, then their intersection point have been constructed.
- If (distinct) circles C_1, C_2 have been constructed already, then their intersection points have been constructed.

The setting is $\mathbb{R}^2$.
Ruler and compass constructions involve the following tools:

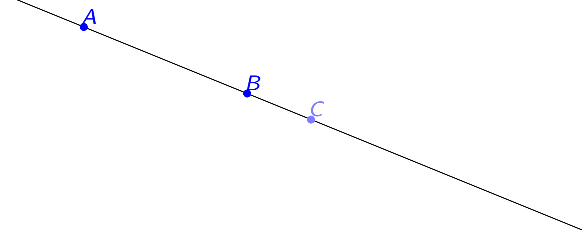
- Given constructed points A, B, we can draw the line $\overleftrightarrow{AB}$ or the line segment $\overline{AB}$.
- Given constructed points A, B, we can draw the circle C with center A which passes through B.

What are "constructed points"? We define them inductively:

- We start by letting $(0, 0)$ and $(0, 1)$ be constructed.
- If lines ℓ_1, ℓ_2 have been constructed already, then their intersection point have been constructed.
- If (distinct) circles C_1, C_2 have been constructed already, then their intersection points have been constructed.
- If the line ℓ and circle C have been constructed already, then their intersection points have been constructed.

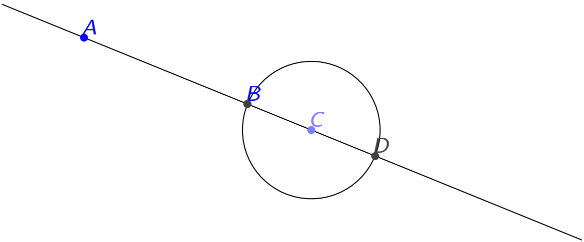
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 1: C incident to ℓ



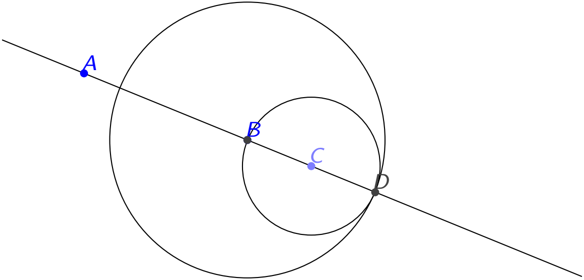
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 1: C incident to ℓ



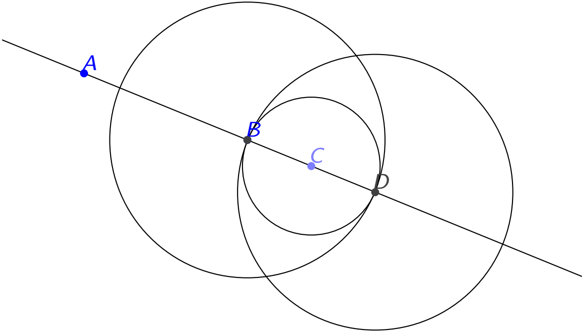
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 1: C incident to ℓ



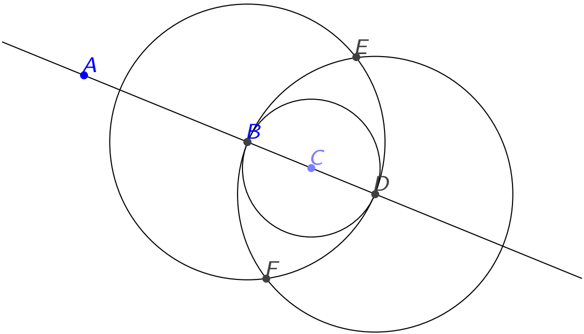
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 1: C incident to ℓ



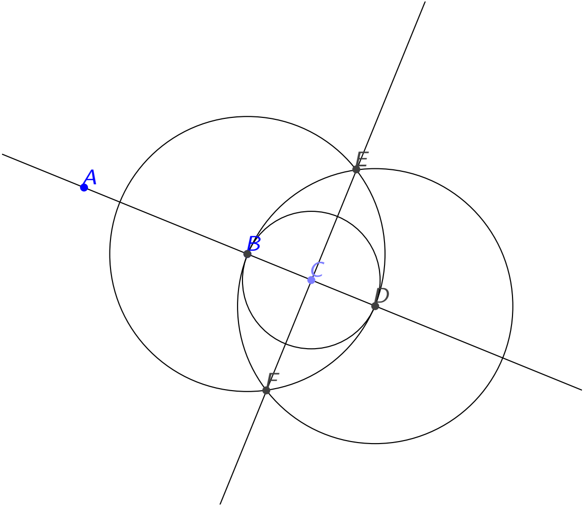
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 1: C incident to ℓ



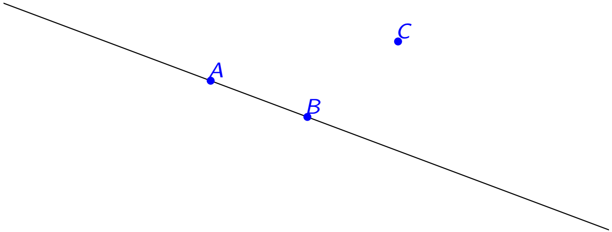
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 1: C incident to ℓ



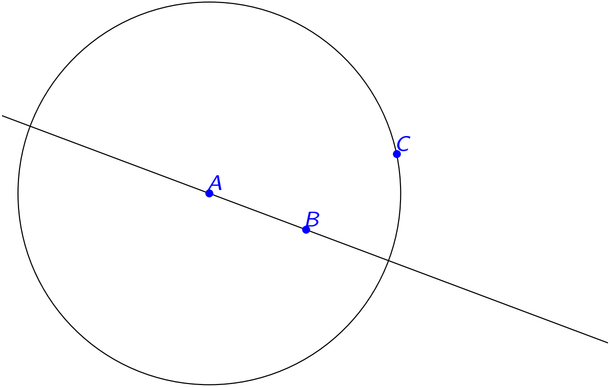
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 2: C not incident to ℓ



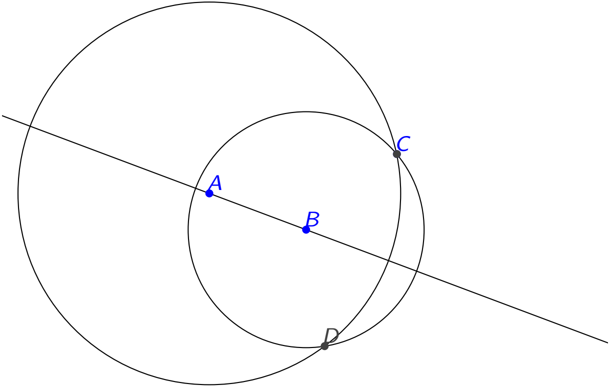
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 2: C not incident to ℓ



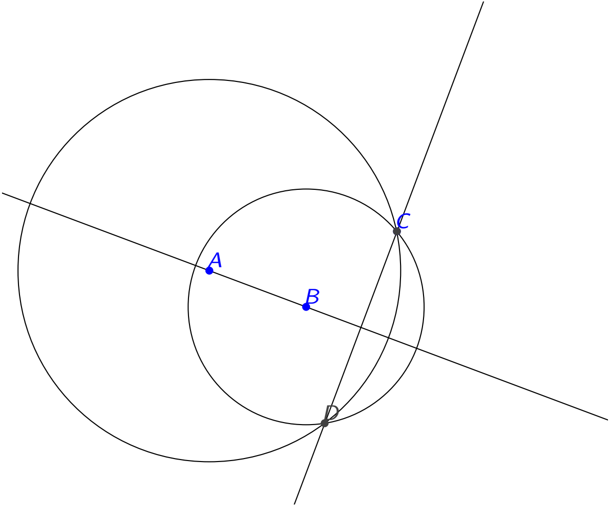
Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

Case 2: C not incident to ℓ

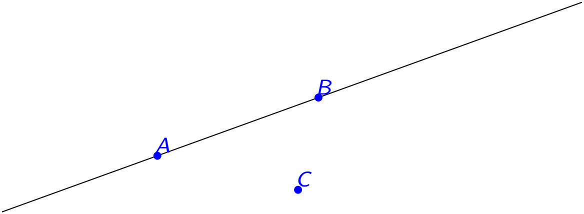


Construct Perpendicular Line $\ell_\perp$ to line $\ell = \overleftrightarrow{AB}$ through point C

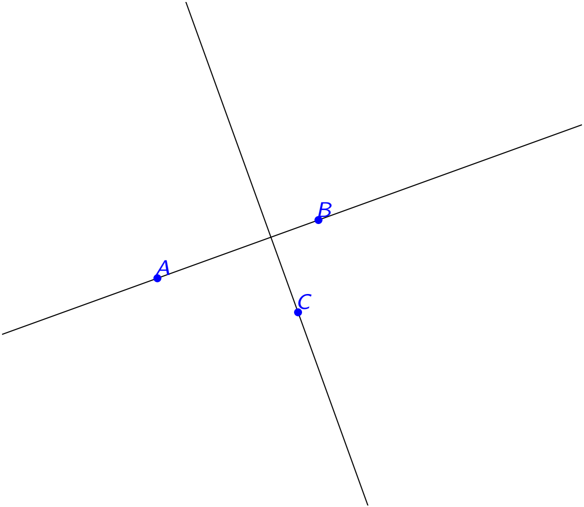
Case 2: C not incident to ℓ



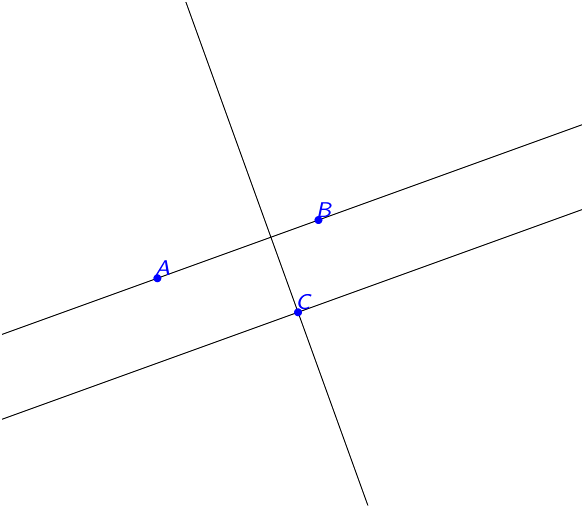
Draw Parallel Line Through Given Point



Draw Parallel Line Through Given Point

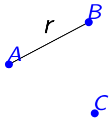


Draw Parallel Line Through Given Point



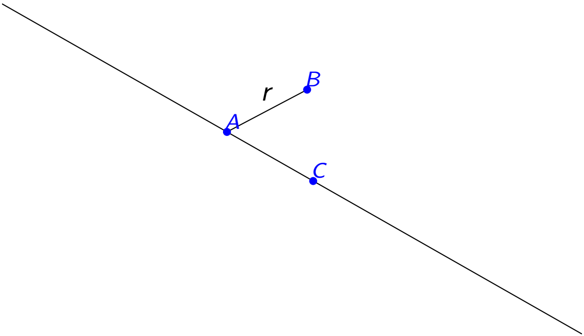
Translate Line Segment

Case 1: Non-collinear



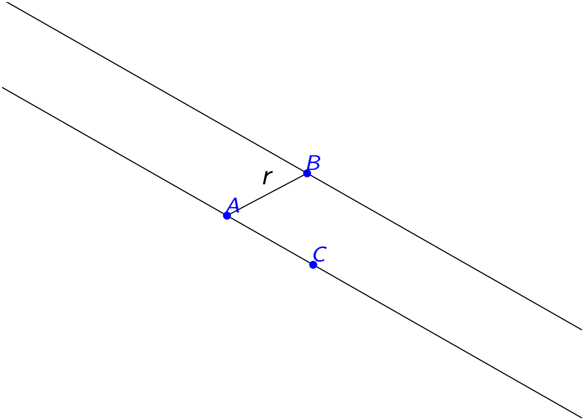
Translate Line Segment

Case 1: Non-collinear



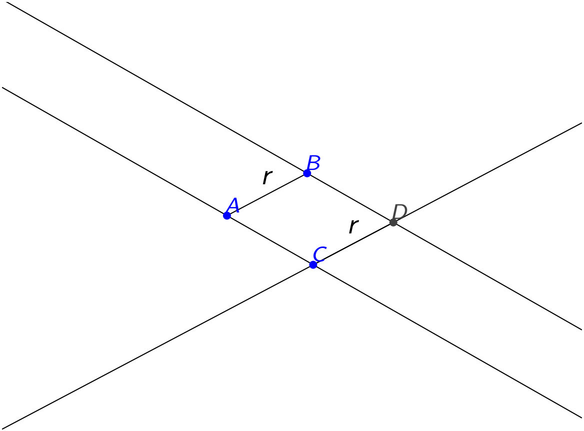
Translate Line Segment

Case 1: Non-collinear



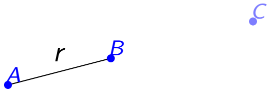
Translate Line Segment

Case 1: Non-collinear



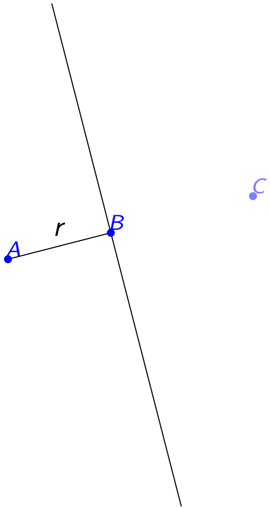
Translate Line Segment

Case 2: Collinear



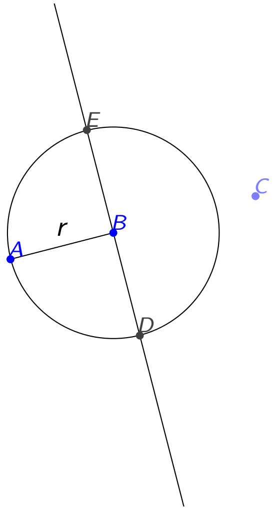
Translate Line Segment

Case 2: Collinear



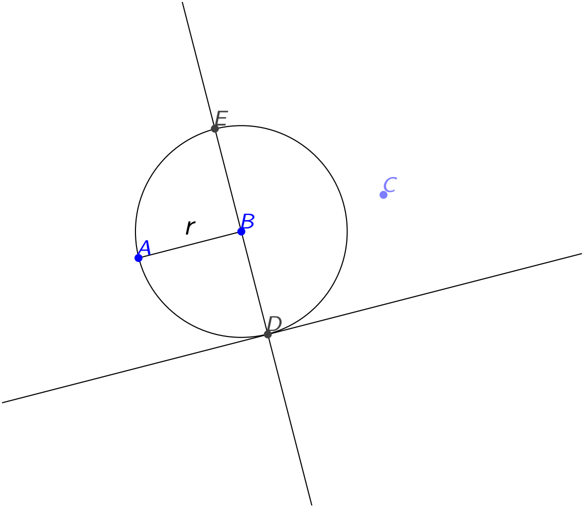
Translate Line Segment

Case 2: Collinear



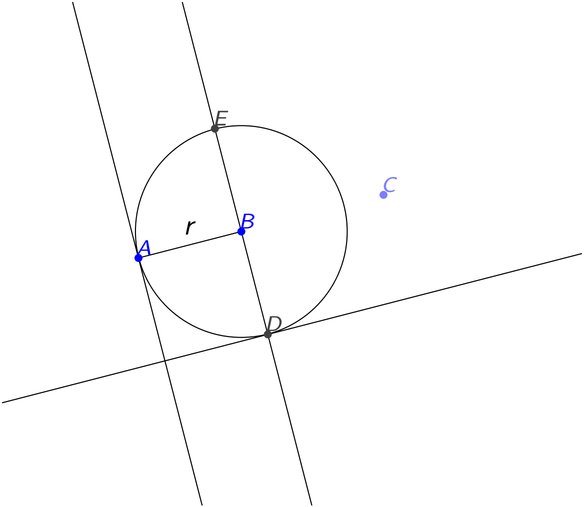
Translate Line Segment

Case 2: Collinear



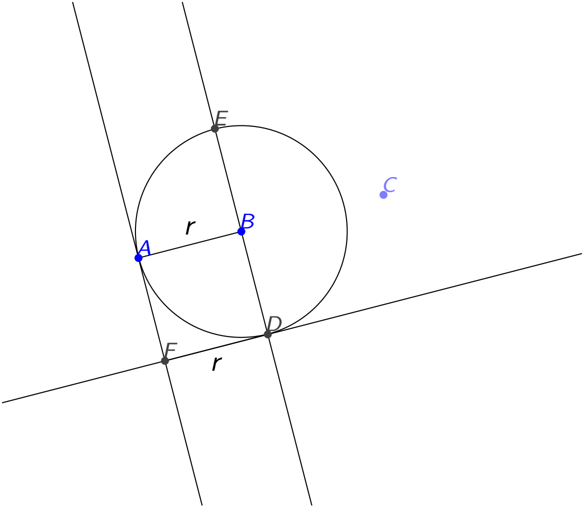
Translate Line Segment

Case 2: Collinear



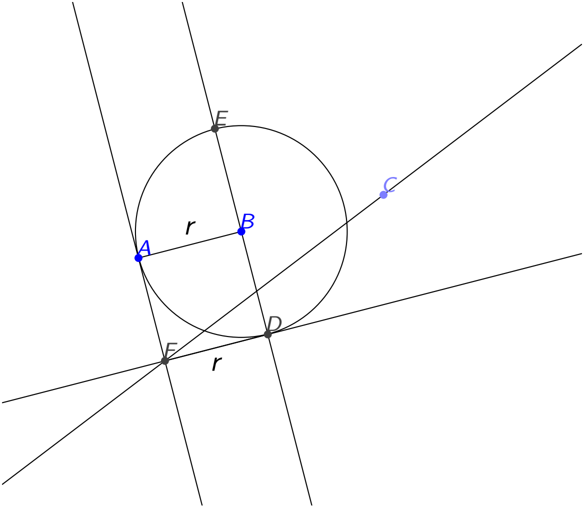
Translate Line Segment

Case 2: Collinear



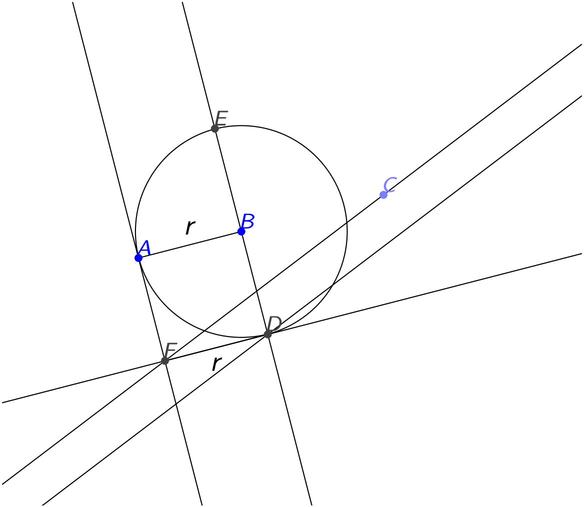
Translate Line Segment

Case 2: Collinear



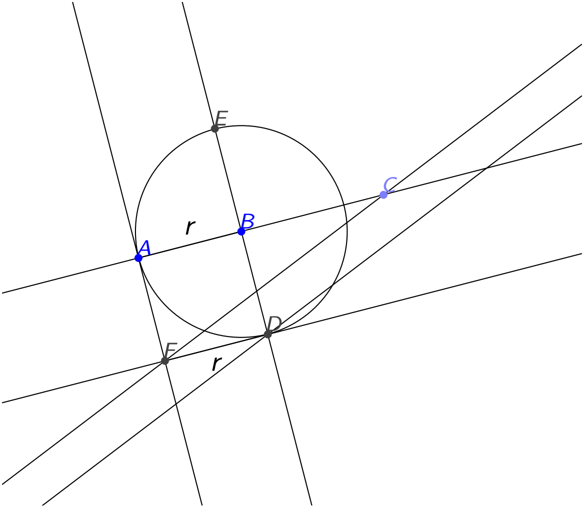
Translate Line Segment

Case 2: Collinear



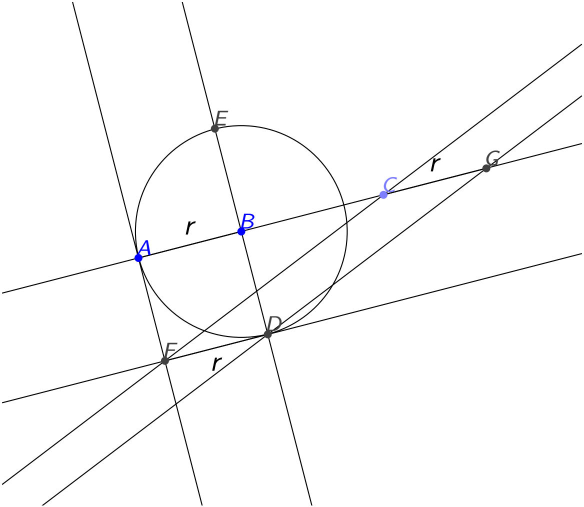
Translate Line Segment

Case 2: Collinear



Translate Line Segment

Case 2: Collinear



Limitations of Ruler and Compass Constructions

It seems like we can construct a lot using only an unmarked ruler and a compass. There were three problems the ancient Greeks couldn't seem to solve though:

Limitations of Ruler and Compass Constructions

It seems like we can construct a lot using only an unmarked ruler and a compass. There were three problems the ancient Greeks couldn't seem to solve though:

Squaring the Circle: constructing a circle with Area π. Equivalently, constructing a line segment of length $\sqrt{\pi}$.

Limitations of Ruler and Compass Constructions

It seems like we can construct a lot using only an unmarked ruler and a compass. There were three problems the ancient Greeks couldn't seem to solve though:

Squaring the Circle: constructing a circle with Area π. Equivalently, constructing a line segment of length $\sqrt{\pi}$.

Doubling the Cube: Constructing a line segment of length $\sqrt[3]{2}$ (a cube with side length $\sqrt[3]{2}$ has volume 2).

Limitations of Ruler and Compass Constructions

It seems like we can construct a lot using only an unmarked ruler and a compass. There were three problems the ancient Greeks couldn't seem to solve though:

Squaring the Circle: constructing a circle with Area π. Equivalently, constructing a line segment of length $\sqrt{\pi}$.

Doubling the Cube: Constructing a line segment of length $\sqrt[3]{2}$ (a cube with side length $\sqrt[3]{2}$ has volume 2).

Angle trisection: Showing that any angle which can be constructed can also be trisected, e.g. a 60° angle can be constructed, so can a 20° angle be constructed as well?

Limitations of Ruler and Compass Constructions

It seems like we can construct a lot using only an unmarked ruler and a compass. There were three problems the ancient Greeks couldn't seem to solve though:

Squaring the Circle: constructing a circle with Area π. Equivalently, constructing a line segment of length $\sqrt{\pi}$.

Doubling the Cube: Constructing a line segment of length $\sqrt[3]{2}$ (a cube with side length $\sqrt[3]{2}$ has volume 2).

Angle trisection: Showing that any angle which can be constructed can also be trisected, e.g. a 60° angle can be constructed, so can a 20° angle be constructed as well?

It wasn't until the 1800s that these constructions were proven to *not* be possible.

Constructible Numbers

A point (a, b) is **constructible** if it can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.

Constructible Numbers

A point (a, b) is **constructible** if it can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.
A real number r is **constructible** if $(r, 0)$ is constructible.

Constructible Numbers

A point (a, b) is **constructible** if it can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.
A real number r is **constructible** if $(r, 0)$ is constructible.

Lemma

Let r be a real number. The following are equivalent:

Constructible Numbers

A point (a, b) is **constructible** if it can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.
A real number r is **constructible** if $(r, 0)$ is constructible.

Lemma

Let r be a real number. The following are equivalent:

1. *r is constructible.*

Constructible Numbers

A point (a, b) is **constructible** if it can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.
A real number r is **constructible** if $(r, 0)$ is constructible.

Lemma

Let r be a real number. The following are equivalent:

1. *r is constructible.*
2. *A line segment of length $|r|$ can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.*

Proof.

Constructible Numbers

A point (a, b) is **constructible** if it can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.
A real number r is **constructible** if $(r, 0)$ is constructible.

Lemma

Let r be a real number. The following are equivalent:

1. *r is constructible.*
2. *A line segment of length $|r|$ can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.*

Proof.

1 $\Rightarrow$ 2 : If r is constructible, then the line segment from $(0, 0)$ to $(|r|, 0)$ has length $|r|$.

Constructible Numbers

A point (a, b) is **constructible** if it can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.
A real number r is **constructible** if $(r, 0)$ is constructible.

Lemma

Let r be a real number. The following are equivalent:

1. *r is constructible.*
2. *A line segment of length $|r|$ can be constructed in a finite number of steps starting with the constructed points $(0, 0)$ and $(1, 0)$.*

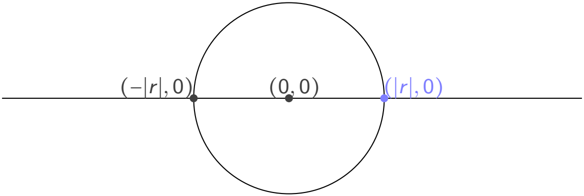
Proof.

1 $\Rightarrow$ 2 : If r is constructible, then the line segment from $(0, 0)$ to $(|r|, 0)$ has length $|r|$.

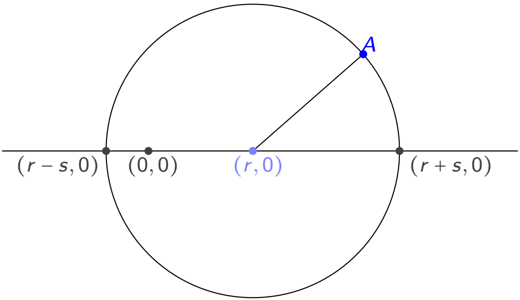
2 $\Leftarrow$ 1 : Suppose $\overline{AB}$ is a line segment of length $|r|$. Translate $\overline{AB}$ to $\overline{OC}$, where O = origin. Draw circle centered at O going through C. This intersects the x-axis at the point $(|r|, 0)$.

□

Consider below diagram:



$-r$ is one of $|r|$ or $-|r|$.

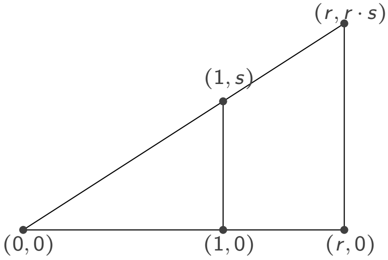


For $r, s \geq 0$, the above construction shows $r + s$ and $r - s$ are constructible.
If r is negative, then

$$r + s = -\big((-r) + (-s)\big)$$

Properties of Constructible Numbers

Closure under Multiplication



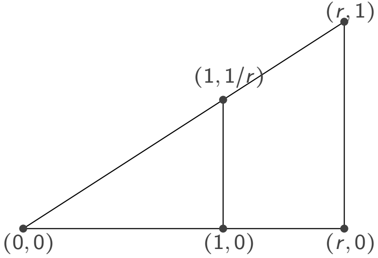
For $r, s \geq 0$, the above construction shows there is a line segment of length $r \cdot s$.

If either r or s are negative, then

$$r \cdot s = -\big((-r) \cdot s\big) = -\big(r \cdot (-s)\big) = (-r) \cdot (-s)$$

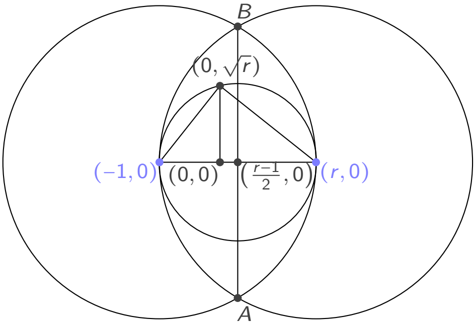
Properties of Constructible Numbers

Closure under Reciprocation



For $r > 0$, the above construction shows there is a line segment of length $1/r$.
If $r < 0$, then

$$\frac{1}{-r} = -\frac{1}{r}$$



We construct the circle of radius $\frac{1+r}{2}$ centered at $\left(\frac{r-1}{2}, 0\right)$.
This circle intersects the y-axis at $(0, \pm\sqrt{r})$.

The Structure of Constructible Numbers

Theorem

Suppose r is a real number. The following are equivalent:

The Structure of Constructible Numbers

Theorem

Suppose r is a real number. The following are equivalent:

1. *r is constructible.*

The Structure of Constructible Numbers

Theorem

Suppose r is a real number. The following are equivalent:

1. *r is constructible.*
2. *r is the result of starting with 0 and 1 and applying the operations of addition, subtraction, multiplication, division, and taking square roots.*

The Structure of Constructible Numbers

Theorem

Suppose r is a real number. The following are equivalent:

1. *r is constructible.*
2. *r is the result of starting with 0 and 1 and applying the operations of addition, subtraction, multiplication, division, and taking square roots.*

Proof.

The Structure of Constructible Numbers

Theorem

Suppose r is a real number. The following are equivalent:

1. *r is constructible.*
2. *r is the result of starting with 0 and 1 and applying the operations of addition, subtraction, multiplication, division, and taking square roots.*

Proof.

- 2 $\Rightarrow$ 1 Previously shown that the set of constructible numbers is closed under the given operations. $0, 1$ are defined to be constructible.

The Structure of Constructible Numbers

Theorem

Suppose r is a real number. The following are equivalent:

1. *r is constructible.*
2. *r is the result of starting with* 0 *and* 1 *and applying the operations of addition, subtraction, multiplication, division, and taking square roots.*

Proof.

- 2 ⇒ 1 Previously shown that the set of constructible numbers is closed under the given operations. $0, 1$ are defined to be constructible.
- 1 ⇒ 2 Must analyze three kinds of intersections:
  - two lines
  - a circle and a line
  - two circle

How Constructed Points Arise

Intersection of two Lines

Suppose ℓ_1, ℓ_2 are the lines

$$\ell_1 a_1 x + b_1 y = c_1$$
$$\ell_2 a_2 x + b_2 y = c_2$$

How Constructed Points Arise

Intersection of two Lines

Suppose ℓ_1, ℓ_2 are the lines

$$\ell_1 a_1 x + b_1 y = c_1$$
$$\ell_2 a_2 x + b_2 y = c_2$$

At least one of a_1, b_1 are $\neq 0$, say $a_1 \neq 0$. Then

$$a_1 x + b_1 y = c_1 \Leftrightarrow x = \frac{c_1}{a_1} - \frac{b_1}{a_1} y$$

How Constructed Points Arise

Intersection of two Lines

Suppose ℓ_1, ℓ_2 are the lines

$$\ell_1 a_1 x + b_1 y = c_1$$
$$\ell_2 a_2 x + b_2 y = c_2$$

At least one of a_1, b_1 are $\neq 0$, say $a_1 \neq 0$. Then

$$a_1 x + b_1 y = c_1 \Leftrightarrow x = \frac{c_1}{a_1} - \frac{b_1}{a_1} y$$

so

$$a_2 \left(\frac{c_1}{a_1} - \frac{b_1}{a_1} y \right) + b_2 y = c_2$$

How Constructed Points Arise

Intersection of two Lines

Suppose ℓ_1, ℓ_2 are the lines

$$\ell_1 a_1 x + b_1 y = c_1$$
$$\ell_2 a_2 x + b_2 y = c_2$$

At least one of a_1, b_1 are $\neq 0$, say $a_1 \neq 0$. Then

$$a_1 x + b_1 y = c_1 \Leftrightarrow x = \frac{c_1}{a_1} - \frac{b_1}{a_1} y$$

so

$$a_2 \left(\frac{c_1}{a_1} - \frac{b_1}{a_1} y \right) + b_2 y = c_2$$

This is linear in y.

How Constructed Points Arise

Intersection of two Lines

Suppose ℓ_1, ℓ_2 are the lines

$$\ell_1 a_1 x + b_1 y = c_1$$
$$\ell_2 a_2 x + b_2 y = c_2$$

At least one of a_1, b_1 are $\neq 0$, say $a_1 \neq 0$. Then

$$a_1 x + b_1 y = c_1 \Leftrightarrow x = \frac{c_1}{a_1} - \frac{b_1}{a_1} y$$

so

$$a_2 \left(\frac{c_1}{a_1} - \frac{b_1}{a_1} y \right) + b_2 y = c_2$$

This is linear in y.
Thus, x and y are obtained from $a_1, b_1, c_1, a_2, b_2, c_2$ using the operations of addition, subtraction, multiplication, and division.

Suppose C is the circle

$$C: \quad (x-h)^2 + (y-k)^2 = r^2$$

How Constructed Points Arise

Intersection of a Circle and Line

Suppose C is the circle

$$C: \quad (x-h)^2 + (y-k)^2 = r^2$$

and ℓ is the line

$$\ell: \quad ax + by = c$$

where h, k, r, a, b, c are numbers which have already been constructed.

Suppose C is the circle

$$C: \quad (x-h)^2 + (y-k)^2 = r^2$$

and ℓ is the line

$$\ell: \quad ax + by = c$$

where h, k, r, a, b, c are numbers which have already been constructed. Then either $a \neq 0$ or $b \neq 0$. Say $a \neq 0$, so

$$ax + by = c \Leftrightarrow x = \frac{c}{a} - \frac{b}{a}y$$

How Constructed Points Arise

Intersection of a Circle and Line

Suppose C is the circle

$$C: \quad (x-h)^2 + (y-k)^2 = r^2$$

and ℓ is the line

$$\ell: \quad ax + by = c$$

where h, k, r, a, b, c are numbers which have already been constructed. Then either $a \neq 0$ or $b \neq 0$. Say $a \neq 0$, so

$$ax + by = c \Leftrightarrow x = \frac{c}{a} - \frac{b}{a}y$$

Substituting into the equation for C gives a quadratic equation in y.

How Constructed Points Arise

Intersection of a Circle and Line

Suppose C is the circle

$$C: \quad (x-h)^2 + (y-k)^2 = r^2$$

and ℓ is the line

$$\ell: \quad ax + by = c$$

where h, k, r, a, b, c are numbers which have already been constructed. Then either $a \neq 0$ or $b \neq 0$. Say $a \neq 0$, so

$$ax + by = c \Leftrightarrow x = \frac{c}{a} - \frac{b}{a} y$$

Substituting into the equation for C gives a quadratic equation in y. Thus, x and y are obtainable from h, k, r, a, b, c using the operations of addition, subtraction, multiplication, division, and taking square roots.

How Constructed Points Arise

Intersection of Circles

Suppose C_1, C_2 are circles

$$C_1 : (x - h_1)^2 + (y - k_1)^2 = r_1^2$$
$$C_2 : (x - h_2)^2 + (y - k_2)^2 = r_2^2$$

where $h_1, k_1, h_2, k_2, r_1, r_2$ are numbers which have already been constructed.

How Constructed Points Arise

Intersection of Circles

Suppose C_1, C_2 are circles

$$C_1 : (x - h_1)^2 + (y - k_1)^2 = r_1^2$$
$$C_2 : (x - h_2)^2 + (y - k_2)^2 = r_2^2$$

where $h_1, k_1, h_2, k_2, r_1, r_2$ are numbers which have already been constructed.
Then

$$\begin{aligned}(x - h_1)^2 + (y - k_1)^2 - r_1^2 &= (x - h_2)^2 + (y - k_2)^2 - r_2^2 \\ x^2 - 2h_1x + h_1^2 + y^2 - 2k_1y + k_1^2 - r_1^2 &= x^2 - 2h_2x + h_2^2 + y^2 - 2k_2y + k_2^2 - r_2^2 \\ 2(h_2 - h_1)x + (h_1^2 + k_1^2 - r_1^2) &= 2(k_1 - k_2)y + (h_2^2 + k_2^2 - r_2^2) \\ ax + by &= c\end{aligned}$$

where $a = 2(h_2 - h_1)$, $b = 2(k_2 - k_1)$, and $c = h_1^2 - h_2^2 + k_1^2 - k_2^2 + r_2^2 - r_1^2$.
This reduces to the case of a circle and a line.

How Constructed Points Arise

Intersection of Circles

Suppose C_1, C_2 are circles

$$C_1 : (x - h_1)^2 + (y - k_1)^2 = r_1^2$$
$$C_2 : (x - h_2)^2 + (y - k_2)^2 = r_2^2$$

where $h_1, k_1, h_2, k_2, r_1, r_2$ are numbers which have already been constructed.
Then

$$(x - h_1)^2 + (y - k_1)^2 - r_1^2 = (x - h_2)^2 + (y - k_2)^2 - r_2^2$$
$$x^2 - 2h_1x + h_1^2 + y^2 - 2k_1y + k_1^2 - r_1^2 = x^2 - 2h_2x + h_2^2 + y^2 - 2k_2y + k_2^2 - r_2^2$$
$$2(h_2 - h_1)x + (h_1^2 + k_1^2 - r_1^2) = 2(k_1 - k_2)y + (h_2^2 + k_2^2 - r_2^2)$$
$$ax + by = c$$

where $a = 2(h_2 - h_1)$, $b = 2(k_2 - k_1)$, and $c = h_1^2 - h_2^2 + k_1^2 - k_2^2 + r_2^2 - r_1^2$.

How Constructed Points Arise

Intersection of Circles

Suppose C_1, C_2 are circles

$$
\begin{aligned}
C_1 :& (x - h_1)^2 + (y - k_1)^2 = r_1^2 \\
C_2 :& (x - h_2)^2 + (y - k_2)^2 = r_2^2
\end{aligned}
$$

where $h_1, k_1, h_2, k_2, r_1, r_2$ are numbers which have already been constructed.
Then

$$
\begin{aligned}
(x - h_1)^2 + (y - k_1)^2 - r_1^2 &= (x - h_2)^2 + (y - k_2)^2 - r_2^2 \\
x^2 - 2h_1x + h_1^2 + y^2 - 2k_1y + k_1^2 - r_1^2 &= x^2 - 2h_2x + h_2^2 + y^2 - 2k_2y + k_2^2 - r_2^2 \\
2(h_2 - h_1)x + (h_1^2 + k_1^2 - r_1^2) &= 2(k_1 - k_2)y + (h_2^2 + k_2^2 - r_2^2) \\
ax + by &= c
\end{aligned}
$$

where $a = 2(h_2 - h_1)$, $b = 2(k_2 - k_1)$, and $c = h_1^2 - h_2^2 + k_1^2 - k_2^2 + r_2^2 - r_1^2$.
This reduces to the case of a circle and a line.

Some Algebra Background

Proposition

Suppose r is a root of the irreducible polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

where each a_k is a root of an irreducible polynomial p_k with rational coefficients. Then r is the root of an irreducible polynomial with rational coefficients.

Some Algebra Background

Proposition

Suppose r is a root of the irreducible polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

where each a_k is a root of an irreducible polynomial p_k with rational coefficients. Then r is the root of an irreducible polynomial with rational coefficients.
Moreover, the degree of that irreducible polynomial divides $n \cdot \deg(p_0) \cdots \deg(p_n)$.

Application to Constructibility

Corollary

Suppose r is constructible. Then r is the root of an irreducible polynomial with rational coefficients of degree 2^n *for some n.*

Application to Constructibility

Corollary

Suppose r is constructible. Then r is the root of an irreducible polynomial with rational coefficients of degree 2^n for some n.

Proof.

Induction on the number k of square roots used to construct r.

Application to Constructibility

Corollary

Suppose r is constructible. Then r is the root of an irreducible polynomial with rational coefficients of degree 2^n for some n.

Proof.

Induction on the number k of square roots used to construct r.
If $k = 0$, r is rational. Hence root of linear equation (degree $1 = 2^0$).

Application to Constructibility

Corollary

Suppose r is constructible. Then r is the root of an irreducible polynomial with rational coefficients of degree 2^n for some n.

Proof.

Induction on the number k of square roots used to construct r.
If $k = 0$, r is rational. Hence root of linear equation (degree $1 = 2^0$).
Induction hypothesis: assume true for constructible numbers using k square roots.

Application to Constructibility

Corollary

Suppose r is constructible. Then r is the root of an irreducible polynomial with rational coefficients of degree 2^n for some n.

Proof.
Induction on the number k of square roots used to construct r.
If $k = 0$, r is rational. Hence root of linear equation (degree $1 = 2^0$).
Induction hypothesis: assume true for constructible numbers using k square roots.
Suppose r uses $k + 1$ square roots, so $r = a + b\sqrt{c}$ where a, b, c use at most k square roots. Then r is a root of the quadratic

$$(x - a)^2 - b^2 c$$

Application to Constructibility

Corollary

Suppose r is constructible. Then r is the root of an irreducible polynomial with rational coefficients of degree 2^n for some n.

Proof.
Induction on the number k of square roots used to construct r.
If $k = 0$, r is rational. Hence root of linear equation (degree $1 = 2^0$).
Induction hypothesis: assume true for constructible numbers using k square roots.
Suppose r uses $k + 1$ square roots, so $r = a + b\sqrt{c}$ where a, b, c use at most k square roots. Then r is a root of the quadratic

$$(x - a)^2 - b^2 c$$

Proposition implies r is root of an irreducible polynomial with rational coefficients with degree dividing

$$2 \cdot 2^k \cdot 2^k \cdot 2^k = 2^{3k+1}$$

□

Impossibility of Squaring the Circle

Corollary

Using ruler-and-compass constructions, it is not possible to square the circle, i.e. create a square with the same area as a unit circle.

Impossibility of Squaring the Circle

Corollary

Using ruler-and-compass constructions, it is not possible to square the circle, i.e. create a square with the same area as a unit circle.

Proof.
Squaring the circle is possible if and only if $\sqrt{\pi}$ is constructible.

Impossibility of Squaring the Circle

Corollary

Using ruler-and-compass constructions, it is not possible to square the circle, i.e. create a square with the same area as a unit circle.

Proof.
Squaring the circle is possible if and only if $\sqrt{\pi}$ is constructible.

But if $\sqrt{\pi}$ is constructible, it is the root of a polynomial.

Impossibility of Squaring the Circle

Corollary

Using ruler-and-compass constructions, it is not possible to square the circle, i.e. create a square with the same area as a unit circle.

Proof.
Squaring the circle is possible if and only if $\sqrt{\pi}$ is constructible.

But if $\sqrt{\pi}$ is constructible, it is the root of a polynomial.

π is *transcendental*, not the root of any polynomial, so neither is $\sqrt{\pi}$. $\square$

Impossibility of Doubling the Cube

Corollary

Using ruler-and-compass constructions, it is not possible to construct a main diagonal of a unit cube.

Impossibility of Doubling the Cube

Corollary

Using ruler-and-compass constructions, it is not possible to construct a main diagonal of a unit cube.

Proof.
Doubling the cube is possible if and only if $\sqrt[3]{2}$ is constructible.

Impossibility of Doubling the Cube

Corollary

Using ruler-and-compass constructions, it is not possible to construct a main diagonal of a unit cube.

Proof.
Doubling the cube is possible if and only if $\sqrt[3]{2}$ is constructible.

If $\sqrt[3]{2}$ is constructible, it is the root of a polynomial $p(x)$ with rational coefficients of degree 2^n for some n.

Impossibility of Doubling the Cube

Corollary

Using ruler-and-compass constructions, it is not possible to construct a main diagonal of a unit cube.

Proof.
Doubling the cube is possible if and only if $\sqrt[3]{2}$ is constructible.

If $\sqrt[3]{2}$ is constructible, it is the root of a polynomial $p(x)$ with rational coefficients of degree 2^n for some n.

But $\sqrt[3]{2}$ is also the root of the irreducible polynomial $x^3 - 2$, so $x^3 - 2$ must divide $p(x)$. This is impossible since 3 does not divide 2^n. □

Impossibility of Trisecting Arbitrary Angles

Corollary

Using ruler-and-compass constructions, it is not always possible to trisect an arbitrary constructible angle.

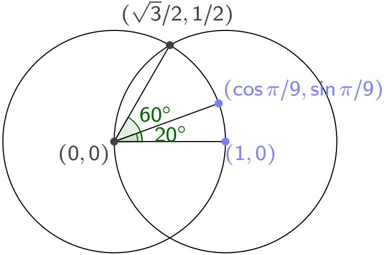
Impossibility of Trisecting Arbitrary Angles

Corollary

Using ruler-and-compass constructions, it is not always possible to trisect an arbitrary constructible angle.

Proof.

If trisecting arbitrary angles is possible, then a 20° angle in primary position can be constructed since a 60° angle in primary position can be constructed. This angle intersects the unit circle at $\left(\cos\frac{\pi}{9}, \sin\frac{\pi}{9}\right)$. Suffices to show $\cos\frac{\pi}{9}$ is not constructible.



□

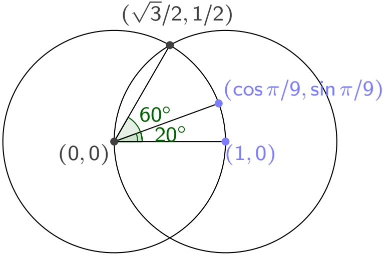
Impossibility of Trisecting Arbitrary Angles

Corollary

Using ruler-and-compass constructions, it is not always possible to trisect an arbitrary constructible angle.

Proof.

If trisecting arbitrary angles is possible, then a 20° angle in primary position can be constructed since a 60° angle in primary position can be constructed. This angle intersects the unit circle at $\left(\cos\frac{\pi}{9}, \sin\frac{\pi}{9}\right)$. Suffices to show $\cos\frac{\pi}{9}$ is not constructible.



The triple angle formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ implies that $\cos\frac{\pi}{9}$ is a root of the cubic $4x^3 - 3x - \frac{1}{2}$. But 3 does not divide 2^n for any n, so $\cos\frac{\pi}{9}$ cannot be constructible.

□