Math-123: Constructibility of the n-gon, and the fundamental theorem of algebra

Sebastien Vasey

Harvard University

April 17, 2020

Revenge of the straightedge and compass

We saw a while back that three problems from Greek geometry are impossible:

- Squaring the circle.
- Doubling the cube.
- Trisecting the angle.

Revenge of the straightedge and compass

We saw a while back that three problems from Greek geometry are impossible:

- Squaring the circle.
- Doubling the cube.
- Trisecting the angle.

Today: for which n can we construct the regular n-gon using straightedge and compass?

Revenge of the straightedge and compass

We saw a while back that three problems from Greek geometry are impossible:

- Squaring the circle.
- Doubling the cube.
- Trisecting the angle.

Today: for which n can we construct the regular n-gon using straightedge and compass?

What is a regular n-gon? A polygon with n sides of equal length, with the same angles between adjacent sides.

Revenge of the straightedge and compass

We saw a while back that three problems from Greek geometry are impossible:

- Squaring the circle.
- Doubling the cube.
- Trisecting the angle.

Today: for which n can we construct the regular n-gon using straightedge and compass?

What is a regular n-gon? A polygon with n sides of equal length, with the same angles between adjacent sides.

$n = 2$: a line segment, $n = 3$: an equilateral triangle, $n = 4$: a square, $n = 5$: a pentagon, $n = 6$: a hexagon, etc.

History of the problem

The Greek knew how to construct a 2-gon, 3-gon, 5-gon.

History of the problem

The Greek knew how to construct a 2-gon, 3-gon, 5-gon.

They also knew that if the regular n-gon can be constructed, then the regular $2n$-gon can be constructed.

History of the problem

The Greek knew how to construct a 2-gon, 3-gon, 5-gon.

They also knew that if the regular n-gon can be constructed, then the regular $2n$-gon can be constructed.

They did not know how to construct the regular n-gon for $n = 7, 9, 11, 13, \ldots$.

History of the problem

The Greek knew how to construct a 2-gon, 3-gon, 5-gon.

They also knew that if the regular n-gon can be constructed, then the regular $2n$-gon can be constructed.

They did not know how to construct the regular n-gon for $n = 7, 9, 11, 13, \ldots$.

At age 19 (1796), Gauss showed how to construct the regular 17-gon. He wanted the construction inscribed on his tomb (but it was not...).

History of the problem

The Greek knew how to construct a 2-gon, 3-gon, 5-gon.

They also knew that if the regular n-gon can be constructed, then the regular $2n$-gon can be constructed.

They did not know how to construct the regular n-gon for $n = 7, 9, 11, 13, \ldots$.

At age 19 (1796), Gauss showed how to construct the regular 17-gon. He wanted the construction inscribed on his tomb (but it was not...).

Five years later, he proved a sufficient for constructibility (and stated without proof it was necessary). In 1837, Wantzel proved that the condition was also necessary.

History of the problem

The Greek knew how to construct a 2-gon, 3-gon, 5-gon.

They also knew that if the regular n-gon can be constructed, then the regular $2n$-gon can be constructed.

They did not know how to construct the regular n-gon for $n = 7, 9, 11, 13, \ldots$.

At age 19 (1796), Gauss showed how to construct the regular 17-gon. He wanted the construction inscribed on his tomb (but it was not...).

Five years later, he proved a sufficient for constructibility (and stated without proof it was necessary). In 1837, Wantzel proved that the condition was also necessary.

In particular, it is impossible to construct the 7-gon, the 9-gon, the 11-gon, and the 13-gon....

History of the problem

The Greek knew how to construct a 2-gon, 3-gon, 5-gon.

They also knew that if the regular n-gon can be constructed, then the regular $2n$-gon can be constructed.

They did not know how to construct the regular n-gon for $n = 7, 9, 11, 13, \ldots$.

At age 19 (1796), Gauss showed how to construct the regular 17-gon. He wanted the construction inscribed on his tomb (but it was not...).

Five years later, he proved a sufficient for constructibility (and stated without proof it was necessary). In 1837, Wantzel proved that the condition was also necessary.

In particular, it is impossible to construct the 7-gon, the 9-gon, the 11-gon, and the 13-gon....

But it is possible to construct the 257-gon!

Review: constructible numbers

By definition, a point is *constructible* if it can be constructed starting from $(0, 0)$ and $(0, 1)$ using just straightedge and compass.

Review: constructible numbers

By definition, a point is *constructible* if it can be constructed starting from $(0,0)$ and $(0,1)$ using just straightedge and compass.

By definition, a real number α is *constructible* if $|\alpha|$ is the length of a straight line between two constructible points.

Review: constructible numbers

By definition, a point is *constructible* if it can be constructed starting from $(0, 0)$ and $(0, 1)$ using just straightedge and compass.

By definition, a real number α is *constructible* if $|\alpha|$ is the length of a straight line between two constructible points.

Theorem

A real number α is constructible if and only if there exists $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_m$ such that K_m is a subfield of $\mathbb{R}$ and $[K_{i+1} : K_i] = 2$ for all $i \leq m$.

Review: constructible numbers

By definition, a point is *constructible* if it can be constructed starting from $(0,0)$ and $(0,1)$ using just straightedge and compass.

By definition, a real number α is *constructible* if $|\alpha|$ is the length of a straight line between two constructible points.

Theorem

A real number α is constructible if and only if there exists $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_m$ such that K_m is a subfield of $\mathbb{R}$ and $[K_{i+1} : K_i] = 2$ for all $i \leq m$.
In particular, if α is constructible then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.

Review: constructible numbers

By definition, a point is *constructible* if it can be constructed starting from $(0, 0)$ and $(0, 1)$ using just straightedge and compass.

By definition, a real number α is *constructible* if $|\alpha|$ is the length of a straight line between two constructible points.

Theorem

A real number α is constructible if and only if there exists $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_m$ such that K_m is a subfield of $\mathbb{R}$ and $[K_{i+1} : K_i] = 2$ for all $i \leq m$.
In particular, if α is constructible then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.

By definition, an angle θ *can be constructed* if it is the angle between two lines going through several constructible points, and intersecting at a constructible point.

Review: constructible numbers

By definition, a point is *constructible* if it can be constructed starting from $(0,0)$ and $(0,1)$ using just straightedge and compass.

By definition, a real number α is *constructible* if $|\alpha|$ is the length of a straight line between two constructible points.

Theorem

A real number α is constructible if and only if there exists $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_m$ such that K_m is a subfield of $\mathbb{R}$ and $[K_{i+1} : K_i] = 2$ for all $i \leq m$.
In particular, if α is constructible then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.

By definition, an angle θ *can be constructed* if it is the angle between two lines going through several constructible points, and intersecting at a constructible point.

Fact: θ can be constructed if and only if $\cos(\theta)$ is constructible.

Definition

We say that the *regular n-gon can be constructed* if the angle $2\pi/n$ can be constructed.

Definition

We say that the *regular n-gon can be constructed* if the angle $2\pi/n$ can be constructed.

This definition makes sense: if $2\pi/n$ can be constructed, then the roots of unity $(\cos(2k\pi/n), \sin(2k\pi/n))$, $k = 1, 2, \ldots, n$ can be constructed, and they form the vertices of a regular n-gon.

Definition

We say that the *regular n-gon can be constructed* if the angle $2\pi/n$ can be constructed.

This definition makes sense: if $2\pi/n$ can be constructed, then the roots of unity $(\cos(2k\pi/n), \sin(2k\pi/n))$, $k = 1, 2, \ldots, n$ can be constructed, and they form the vertices of a regular n-gon.

Note $\cos(2\pi/n)$ is constructible if and only if $\cos(\pi/n)$ is constructible (use the half angle and double angle formulas).

Definition

We say that the *regular n-gon can be constructed* if the angle $2\pi/n$ can be constructed.

This definition makes sense: if $2\pi/n$ can be constructed, then the roots of unity $(\cos(2k\pi/n), \sin(2k\pi/n))$, $k = 1, 2, \ldots, n$ can be constructed, and they form the vertices of a regular n-gon.

Note $\cos(2\pi/n)$ is constructible if and only if $\cos(\pi/n)$ is constructible (use the half angle and double angle formulas).

Note if $n = 2$, $\cos(\pi/2) = 0$ is constructible. If $n = 3$, $\cos(\pi/3) = 0.5$ is constructible. If $n = 4$, $\cos(\pi/4) = \frac{\sqrt{2}}{2}$ is constructible.

Definition

We say that the *regular n-gon can be constructed* if the angle $2\pi/n$ can be constructed.

This definition makes sense: if $2\pi/n$ can be constructed, then the roots of unity $(\cos(2k\pi/n), \sin(2k\pi/n))$, $k = 1, 2, \ldots, n$ can be constructed, and they form the vertices of a regular n-gon.

Note $\cos(2\pi/n)$ is constructible if and only if $\cos(\pi/n)$ is constructible (use the half angle and double angle formulas).

Note if $n = 2$, $\cos(\pi/2) = 0$ is constructible. If $n = 3$, $\cos(\pi/3) = 0.5$ is constructible. If $n = 4$, $\cos(\pi/4) = \frac{\sqrt{2}}{2}$ is constructible.

In general, $\cos(\pi/n)$ is constructible, then $\cos(\pi/(2n))$ is constructible (half angle formula again).

Definition

We say that the *regular n-gon can be constructed* if the angle $2\pi/n$ can be constructed.

This definition makes sense: if $2\pi/n$ can be constructed, then the roots of unity $(\cos(2k\pi/n), \sin(2k\pi/n))$, $k = 1, 2, \ldots, n$ can be constructed, and they form the vertices of a regular n-gon.

Note $\cos(2\pi/n)$ is constructible if and only if $\cos(\pi/n)$ is constructible (use the half angle and double angle formulas).

Note if $n = 2$, $\cos(\pi/2) = 0$ is constructible. If $n = 3$, $\cos(\pi/3) = 0.5$ is constructible. If $n = 4$, $\cos(\pi/4) = \frac{\sqrt{2}}{2}$ is constructible.

In general, $\cos(\pi/n)$ is constructible, then $\cos(\pi/(2n))$ is constructible (half angle formula again).

For $n = 5$, $\cos(\pi/5) = \frac{1+\sqrt{5}}{4}$ (exercise!), so is constructible.

Constructibility of the n-gon: sufficient condition

Let $\zeta_n := e^{2\pi i/n}$. Observe that $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, so the regular n-gon can be constructed if and only if $\alpha = \zeta_n + \zeta_n^{-1}$ is constructible.

Constructibility of the n-gon: sufficient condition

Let $\zeta_n := e^{2\pi i/n}$. Observe that $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, so the regular n-gon can be constructed if and only if $\alpha = \zeta_n + \zeta_n^{-1}$ is constructible.

Thus we have to study the extension $\mathbb{Q}(\alpha)$. This is a proper subfield of $\mathbb{Q}(\zeta_n)$ (it contains only reals).

Constructibility of the n-gon: sufficient condition

Let $\zeta_n := e^{2\pi i/n}$. Observe that $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, so the regular n-gon can be constructed if and only if $\alpha = \zeta_n + \zeta_n^{-1}$ is constructible.

Thus we have to study the extension $\mathbb{Q}(\alpha)$. This is a proper subfield of $\mathbb{Q}(\zeta_n)$ (it contains only reals).

On the other hand, $\zeta_n^2 - 2\alpha\zeta_n + 1 = 0$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$.

Constructibility of the n-gon: sufficient condition

Let $\zeta_n := e^{2\pi i/n}$. Observe that $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, so the regular n-gon can be constructed if and only if $\alpha = \zeta_n + \zeta_n^{-1}$ is constructible.

Thus we have to study the extension $\mathbb{Q}(\alpha)$. This is a proper subfield of $\mathbb{Q}(\zeta_n)$ (it contains only reals).

On the other hand, $\zeta_n^2 - 2\alpha\zeta_n + 1 = 0$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$.

$\mathbb{Q}(\zeta_n)$ has degree $\phi(n)$, so $\mathbb{Q}(\alpha)$ has degree $\frac{\phi(n)}{2}$.

Constructibility of the n-gon: sufficient condition

Let $\zeta_n := e^{2\pi i/n}$. Observe that $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, so the regular n-gon can be constructed if and only if $\alpha = \zeta_n + \zeta_n^{-1}$ is constructible.

Thus we have to study the extension $\mathbb{Q}(\alpha)$. This is a proper subfield of $\mathbb{Q}(\zeta_n)$ (it contains only reals).

On the other hand, $\zeta_n^2 - 2\alpha\zeta_n + 1 = 0$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$.

$\mathbb{Q}(\zeta_n)$ has degree $\phi(n)$, so $\mathbb{Q}(\alpha)$ has degree $\frac{\phi(n)}{2}$.

If α is constructible, then $\frac{\phi(n)}{2}$ is a power of 2, so $\phi(n)$ is a power of 2.

Constructibility of the n-gon: sufficient condition

Let $\zeta_n := e^{2\pi i/n}$. Observe that $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, so the regular n-gon can be constructed if and only if $\alpha = \zeta_n + \zeta_n^{-1}$ is constructible.

Thus we have to study the extension $\mathbb{Q}(\alpha)$. This is a proper subfield of $\mathbb{Q}(\zeta_n)$ (it contains only reals).

On the other hand, $\zeta_n^2 - 2\alpha\zeta_n + 1 = 0$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$.

$\mathbb{Q}(\zeta_n)$ has degree $\phi(n)$, so $\mathbb{Q}(\alpha)$ has degree $\frac{\phi(n)}{2}$.

If α is constructible, then $\frac{\phi(n)}{2}$ is a power of 2, so $\phi(n)$ is a power of 2.

We have shown:

Theorem (Gauss)

If the regular n-gon can be constructed, then $\phi(n)$ is a power of 2.

Constructibility of the n-gon: sufficient condition

Let $\zeta_n := e^{2\pi i/n}$. Observe that $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, so the regular n-gon can be constructed if and only if $\alpha = \zeta_n + \zeta_n^{-1}$ is constructible.

Thus we have to study the extension $\mathbb{Q}(\alpha)$. This is a proper subfield of $\mathbb{Q}(\zeta_n)$ (it contains only reals).

On the other hand, $\zeta_n^2 - 2\alpha\zeta_n + 1 = 0$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$.

$\mathbb{Q}(\zeta_n)$ has degree $\phi(n)$, so $\mathbb{Q}(\alpha)$ has degree $\frac{\phi(n)}{2}$.

If α is constructible, then $\frac{\phi(n)}{2}$ is a power of 2, so $\phi(n)$ is a power of 2.

We have shown:

Theorem (Gauss)

If the regular n-gon can be constructed, then $\phi(n)$ is a power of 2.

For example, $\phi(3) = 2$, $\phi(5) = 4$ are powers of 2, but $\phi(7) = 6$ is not, so the regular 7-gon cannot be constructed.

Theorem (Wantzel)

If $\phi(n)$ is a power of 2, then the regular n-gon can be constructed.

Theorem (Wantzel)

If $\phi(n)$ is a power of 2, then the regular n-gon can be constructed.

Proof: Assume $\phi(n) = 2^m$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree 2^m, and $\mathbb{Q}(\alpha)$ has degree 2^{m-1} ($\alpha = \zeta_n + \zeta_n^{-1}$).

Theorem (Wantzel)

If $\phi(n)$ is a power of 2, then the regular n-gon can be constructed.

Proof: Assume $\phi(n) = 2^m$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree 2^m, and $\mathbb{Q}(\alpha)$ has degree 2^{m-1} ($\alpha = \zeta_n + \zeta_n^{-1}$).

Recall that Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian.

Theorem (Wantzel)

If $\phi(n)$ is a power of 2, then the regular n-gon can be constructed.

Proof: Assume $\phi(n) = 2^m$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree 2^m, and $\mathbb{Q}(\alpha)$ has degree 2^{m-1} ($\alpha = \zeta_n + \zeta_n^{-1}$).

Recall that Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian.

So $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, with abelian Galois group G of order 2^{m-1}.

Theorem (Wantzel)

If $\phi(n)$ is a power of 2, then the regular n-gon can be constructed.

Proof: Assume $\phi(n) = 2^m$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree 2^m, and $\mathbb{Q}(\alpha)$ has degree 2^{m-1} ($\alpha = \zeta_n + \zeta_n^{-1}$).

Recall that Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian.

So $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, with abelian Galois group G of order 2^{m-1}.

By basic facts about abelian groups, we can find a chain $1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{m-1} = G$ of subgroups of G, where $[G_{i+1} : G_i] = 2$ for all i.

Theorem (Wantzel)

If $\phi(n)$ is a power of 2, then the regular n-gon can be constructed.

Proof: Assume $\phi(n) = 2^m$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree 2^m, and $\mathbb{Q}(\alpha)$ has degree 2^{m-1} ($\alpha = \zeta_n + \zeta_n^{-1}$).

Recall that Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian.

So $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, with abelian Galois group G of order 2^{m-1}.

By basic facts about abelian groups, we can find a chain $1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{m-1} = G$ of subgroups of G, where $[G_{i+1} : G_i] = 2$ for all i.

Taking fixed fields (and using the fundamental theorem of Galois theory), this corresponds to a chain $\mathbb{Q} = F_{m-1} \subseteq F_{m-2} \subseteq \ldots \subseteq F_0 = \mathbb{Q}(\alpha)$ of subfields of $\mathbb{Q}(\alpha)$ with $[F_{i+1} : F_i] = 2$ for all i.

Theorem (Wantzel)

If $\phi(n)$ is a power of 2, then the regular n-gon can be constructed.

Proof: Assume $\phi(n) = 2^m$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree 2^m, and $\mathbb{Q}(\alpha)$ has degree 2^{m-1} ($\alpha = \zeta_n + \zeta_n^{-1}$).

Recall that Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian.

So $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, with abelian Galois group G of order 2^{m-1}.

By basic facts about abelian groups, we can find a chain $1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{m-1} = G$ of subgroups of G, where $[G_{i+1} : G_i] = 2$ for all i.

Taking fixed fields (and using the fundamental theorem of Galois theory), this corresponds to a chain $\mathbb{Q} = F_{m-1} \subseteq F_{m-2} \subseteq \ldots \subseteq F_0 = \mathbb{Q}(\alpha)$ of subfields of $\mathbb{Q}(\alpha)$ with $[F_{i+1} : F_i] = 2$ for all i.

Therefore α is constructible, hence the regular n-gon can be constructed.

Theorem (Gauss-Wantzel, version 1)

The regular n-gon can be constructed if and only if $\phi(n)$ is a power of 2.

Theorem (Gauss-Wantzel, version 1)

The regular n-gon can be constructed if and only if $\phi(n)$ is a power of 2.

For example, $\phi(17) = 16$ which is a power of 2, so the regular 17-gon can be constructed.

Theorem (Gauss-Wantzel, version 1)

The regular n-gon can be constructed if and only if $\phi(n)$ is a power of 2.

For example, $\phi(17) = 16$ which is a power of 2, so the regular 17-gon can be constructed.

The proof is actually constructive! DF outline how to deduce that:

$$\cos(2\pi/17) = \frac{-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}+2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-2\sqrt{2(17-\sqrt{17})}}}{16}$$

!!

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

Thus $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

Thus $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

Exercise: show that $\phi(p^k) = p^{k-1}(p-1)$ for p a prime.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

Thus $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

Exercise: show that $\phi(p^k) = p^{k-1}(p-1)$ for p a prime.

So $\phi(2^k) = 2^{k-1}$, a power of 2.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

Thus $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

Exercise: show that $\phi(p^k) = p^{k-1}(p-1)$ for p a prime.

So $\phi(2^k) = 2^{k-1}$, a power of 2.

On the other hand, for p an odd prime, $\phi(p^k) = p^{k-1}(p-1)$ is a power of 2 if and only if $k = 1$ and $p - 1$ is a power of 2.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

Thus $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

Exercise: show that $\phi(p^k) = p^{k-1}(p-1)$ for p a prime.

So $\phi(2^k) = 2^{k-1}$, a power of 2.

On the other hand, for p an odd prime, $\phi(p^k) = p^{k-1}(p-1)$ is a power of 2 if and only if $k = 1$ and $p - 1$ is a power of 2.

$p - 1 = 2^\ell$ means that $2^\ell \equiv -1 \bmod p$, so $2^{2\ell} \equiv 1 \bmod p$.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

Thus $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

Exercise: show that $\phi(p^k) = p^{k-1}(p-1)$ for p a prime.

So $\phi(2^k) = 2^{k-1}$, a power of 2.

On the other hand, for p an odd prime, $\phi(p^k) = p^{k-1}(p-1)$ is a power of 2 if and only if $k = 1$ and $p - 1$ is a power of 2.

$p - 1 = 2^\ell$ means that $2^\ell \equiv -1 \bmod p$, so $2^{2\ell} \equiv 1 \bmod p$.

By Lagrange's theorem, 2ℓ divides $p - 1$, which is a power of 2, so ℓ is a power of 2.

When is $\phi(n)$ a power of 2? We can characterize it using the prime factorization.

Say $n = p_1^{k_1} \dots p_m^{k_m}$, with $p_1, \dots, p_m$ distinct primes. Then $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_m^{k_m})$.

Thus $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

Exercise: show that $\phi(p^k) = p^{k-1}(p-1)$ for p a prime.

So $\phi(2^k) = 2^{k-1}$, a power of 2.

On the other hand, for p an odd prime, $\phi(p^k) = p^{k-1}(p-1)$ is a power of 2 if and only if $k = 1$ and $p - 1$ is a power of 2.

$p - 1 = 2^\ell$ means that $2^\ell \equiv -1 \bmod p$, so $2^{2\ell} \equiv 1 \bmod p$.

By Lagrange's theorem, 2ℓ divides $p - 1$, which is a power of 2, so ℓ is a power of 2.

Thus $p - 1$ is a power of 2 if and only if p is a prime of the form $2^{2^s} + 1$, called a *Fermat prime*.

Theorem (Gauss-Wantzel, version 2)

The regular n-gon can be constructed if and only if n is the product of a power of 2 and distinct Fermat primes.

Theorem (Gauss-Wantzel, version 2)

The regular n-gon can be constructed if and only if n is the product of a power of 2 and distinct Fermat primes.

Example of Fermat primes: $2^{2^0}+1=3$, $2^{2^1}+1=5$, $2^{2^2}=17$, $2^{2^3}+1=257$, $2^{2^4}+1=65537$... ($2^{2^5}+1$ is divisible by 641...).

Theorem (Gauss-Wantzel, version 2)

The regular n-gon can be constructed if and only if n is the product of a power of 2 and distinct Fermat primes.

Example of Fermat primes: $2^{2^0}+1=3$, $2^{2^1}+1=5$, $2^{2^2}=17$, $2^{2^3}+1=257$, $2^{2^4}+1=65537$... ($2^{2^5}+1$ is divisible by 641...).

It is not known whether there are infinitely-many Fermat primes.

The fundamental theorem of algebra

Theorem

$\mathbb{C}$ is algebraically closed: if $f(x) \in \mathbb{C}[x]$ is not constant, then it has a root in $\mathbb{C}$.

The fundamental theorem of algebra

Theorem

$\mathbb{C}$ is algebraically closed: if $f(x) \in \mathbb{C}[x]$ is not constant, then it has a root in $\mathbb{C}$.

There are *many* proofs. You may have seen some of them in real analysis, topology, or complex analysis.

The fundamental theorem of algebra

Theorem

$\mathbb{C}$ is algebraically closed: if $f(x) \in \mathbb{C}[x]$ is not constant, then it has a root in $\mathbb{C}$.

There are *many* proofs. You may have seen some of them in real analysis, topology, or complex analysis.

They all use some analysis though. At some point we have to use properties of $\mathbb{R}$...

The fundamental theorem of algebra

Theorem

$\mathbb{C}$ is algebraically closed: if $f(x) \in \mathbb{C}[x]$ is not constant, then it has a root in $\mathbb{C}$.

There are *many* proofs. You may have seen some of them in real analysis, topology, or complex analysis.

They all use some analysis though. At some point we have to use properties of $\mathbb{R}$...

Also, we don't really need this theorem. We know algebraically closed fields exist anyway.

The fundamental theorem of algebra

Theorem

$\mathbb{C}$ is algebraically closed: if $f(x) \in \mathbb{C}[x]$ is not constant, then it has a root in $\mathbb{C}$.

There are *many* proofs. You may have seen some of them in real analysis, topology, or complex analysis.

They all use some analysis though. At some point we have to use properties of $\mathbb{R}$...

Also, we don't really need this theorem. We know algebraically closed fields exist anyway.

"The fundamental theorem of algebra is neither fundamental, nor a theorem of algebra."

The fundamental theorem of algebra

Theorem

$\mathbb{C}$ is algebraically closed: if $f(x) \in \mathbb{C}[x]$ is not constant, then it has a root in $\mathbb{C}$.

There are *many* proofs. You may have seen some of them in real analysis, topology, or complex analysis.

They all use some analysis though. At some point we have to use properties of $\mathbb{R}$...

Also, we don't really need this theorem. We know algebraically closed fields exist anyway.

"The fundamental theorem of algebra is neither fundamental, nor a theorem of algebra."

Still it is fun to prove.

Analytic proof (sketch)

Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{C}[x]$ ($n \geq 1$, $a_n \neq 0$). Suppose for a contradiction $f(z) \neq 0$ for any complex number z.

Analytic proof (sketch)

Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{C}[x]$ ($n \geq 1$, $a_n \neq 0$). Suppose for a contradiction $f(z) \neq 0$ for any complex number z.

Pick z_0 such that $|f(z_0)|$ is minimal.

Analytic proof (sketch)

Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{C}[x]$ ($n \geq 1$, $a_n \neq 0$). Suppose for a contradiction $f(z) \neq 0$ for any complex number z.

Pick z_0 such that $|f(z_0)|$ is minimal.

z_0 exists: if $|z|$ is very big, then $|f(z)|$ will be dominated by $|z^n|$, hence be very big. Thus we can pick a radius $R > 0$ sufficiently large and think of f as a function with domain the closed disk of radius R. By compactness, f achieves a minimum on this disk.

Analytic proof (sketch)

Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{C}[x]$ ($n \geq 1$, $a_n \neq 0$). Suppose for a contradiction $f(z) \neq 0$ for any complex number z.

Pick z_0 such that $|f(z_0)|$ is minimal.

z_0 exists: if $|z|$ is very big, then $|f(z)|$ will be dominated by $|z^n|$, hence be very big. Thus we can pick a radius $R > 0$ sufficiently large and think of f as a function with domain the closed disk of radius R. By compactness, f achieves a minimum on this disk.

Now for ϵ a very small nonzero complex number, $f(z_0 + \epsilon)$ is very close to $f(z_0) + a_n \epsilon^n$.

Analytic proof (sketch)

Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{C}[x]$ ($n \geq 1$, $a_n \neq 0$). Suppose for a contradiction $f(z) \neq 0$ for any complex number z.

Pick z_0 such that $|f(z_0)|$ is minimal.

z_0 exists: if $|z|$ is very big, then $|f(z)|$ will be dominated by $|z^n|$, hence be very big. Thus we can pick a radius $R > 0$ sufficiently large and think of f as a function with domain the closed disk of radius R. By compactness, f achieves a minimum on this disk.

Now for ϵ a very small nonzero complex number, $f(z_0 + \epsilon)$ is very close to $f(z_0) + a_n \epsilon^n$.

Taking ϵ pointing in the right direction, we obtain a lower minimum than $f(z_0)$.

Two facts from analysis, and their translation to algebra

1. Any odd degree polynomial with real coefficients has a real root.

Two facts from analysis, and their translation to algebra

1. Any odd degree polynomial with real coefficients has a real root. *[Why: intermediate value theorem!]*.

Two facts from analysis, and their translation to algebra

1. Any odd degree polynomial with real coefficients has a real root. *[Why: intermediate value theorem!]*.
2. Any equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{C}$, $a \neq 0$, has a solution in $\mathbb{C}$.

Two facts from analysis, and their translation to algebra

1. Any odd degree polynomial with real coefficients has a real root. *[Why: intermediate value theorem!]*.
2. Any equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{C}$, $a \neq 0$, has a solution in $\mathbb{C}$. *[Why? Use the quadratic formula.]*

Translated to algebra:

Two facts from analysis, and their translation to algebra

1. Any odd degree polynomial with real coefficients has a real root. *[Why: intermediate value theorem!]*.
2. Any equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{C}$, $a \neq 0$, has a solution in $\mathbb{C}$. *[Why? Use the quadratic formula.]*

Translated to algebra:

1. The only extension of $\mathbb{R}$ with odd degree is $\mathbb{R}$ itself.

Two facts from analysis, and their translation to algebra

1. Any odd degree polynomial with real coefficients has a real root. *[Why: intermediate value theorem!]*.
2. Any equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{C}$, $a \neq 0$, has a solution in $\mathbb{C}$. *[Why? Use the quadratic formula.]*

Translated to algebra:

1. The only extension of $\mathbb{R}$ with odd degree is $\mathbb{R}$ itself. *[Why? Use the primitive element theorem: such an extension is generated by a single element whose minimal poly has odd degree.]*

Two facts from analysis, and their translation to algebra

1. Any odd degree polynomial with real coefficients has a real root. *[Why: intermediate value theorem!]*.
2. Any equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{C}$, $a \neq 0$, has a solution in $\mathbb{C}$. *[Why? Use the quadratic formula.]*

Translated to algebra:

1. The only extension of $\mathbb{R}$ with odd degree is $\mathbb{R}$ itself. *[Why? Use the primitive element theorem: such an extension is generated by a single element whose minimal poly has odd degree.]*
2. There are no extensions of $\mathbb{C}$ of degree 2.

Algebraic proof: reducing to $f(x) \in \mathbb{R}[x]$

Let $f(x) \in \mathbb{C}[x]$ of degree $n \geq 1$.

Algebraic proof: reducing to $f(x) \in \mathbb{R}[x]$

Let $f(x) \in \mathbb{C}[x]$ of degree $n \geq 1$.

If $f(x)$ has no roots in $\mathbb{C}$, then neither does the conjugate polynomial $\tau(f)(x)$, where τ is the automorphism of complex conjugation.

Algebraic proof: reducing to $f(x) \in \mathbb{R}[x]$

Let $f(x) \in \mathbb{C}[x]$ of degree $n \geq 1$.

If $f(x)$ has no roots in $\mathbb{C}$, then neither does the conjugate polynomial $\tau(f)(x)$, where τ is the automorphism of complex conjugation.

Thus the product $f(x)\tau(f)(x)$ has no roots in $\mathbb{C}$. This polynomial is fixed by τ, so has real coefficients.

Algebraic proof: reducing to $f(x) \in \mathbb{R}[x]$

Let $f(x) \in \mathbb{C}[x]$ of degree $n \geq 1$.

If $f(x)$ has no roots in $\mathbb{C}$, then neither does the conjugate polynomial $\tau(f)(x)$, where τ is the automorphism of complex conjugation.

Thus the product $f(x)\tau(f)(x)$ has no roots in $\mathbb{C}$. This polynomial is fixed by τ, so has real coefficients.

Thus there is a polynomial with real coefficients with no roots in $\mathbb{C}$. Without loss of generality, $f(x) \in \mathbb{R}[x]$.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

$|G| = 2^k m$, for m odd, $k \geq 1$. By Sylow's theorems, there exists a subgroup P_2 of G of order 2^k.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

$|G| = 2^k m$, for m odd, $k \geq 1$. By Sylow's theorems, there exists a subgroup P_2 of G of order 2^k.

P_2 has index m, so the fixed field has degree m.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

$|G| = 2^k m$, for m odd, $k \geq 1$. By Sylow's theorems, there exists a subgroup P_2 of G of order 2^k.

P_2 has index m, so the fixed field has degree m.

There are no nontrivial odd degree extension of $\mathbb{R}$, so $m = 1$.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

$|G| = 2^k m$, for m odd, $k \geq 1$. By Sylow's theorems, there exists a subgroup P_2 of G of order 2^k.

P_2 has index m, so the fixed field has degree m.

There are no nontrivial odd degree extension of $\mathbb{R}$, so $m = 1$.

Therefore G is a 2-group (its order is a power of 2). In particular, $G' = \mathrm{Aut}(K(i)/\mathbb{C})$ is also a 2-group (of order 2^{k-1}).

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

$|G| = 2^k m$, for m odd, $k \geq 1$. By Sylow's theorems, there exists a subgroup P_2 of G of order 2^k.

P_2 has index m, so the fixed field has degree m.

There are no nontrivial odd degree extension of $\mathbb{R}$, so $m = 1$.

Therefore G is a 2-group (its order is a power of 2). In particular, $G' = \mathrm{Aut}(K(i)/\mathbb{C})$ is also a 2-group (of order 2^{k-1}).

General result about p-groups, for p prime: they have subgroups of all orders. In particular (if $k \neq 1$), G' has a subgroup H of index 2.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

$|G| = 2^k m$, for m odd, $k \geq 1$. By Sylow's theorems, there exists a subgroup P_2 of G of order 2^k.

P_2 has index m, so the fixed field has degree m.

There are no nontrivial odd degree extension of $\mathbb{R}$, so $m = 1$.

Therefore G is a 2-group (its order is a power of 2). In particular, $G' = \mathrm{Aut}(K(i)/\mathbb{C})$ is also a 2-group (of order 2^{k-1}).

General result about p-groups, for p prime: they have subgroups of all orders. In particular (if $k \neq 1$), G' has a subgroup H of index 2.

The fixed field of H must be a degree 2 extension of $\mathbb{C}$, contradiction.

Algebraic proof 1, using group theory

$f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$, with no roots in $\mathbb{C}$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$.

$K(i)$ is a Galois extension of $\mathbb{R}$ (composite of K and $\mathbb{C} = \mathbb{R}(i)$).

Let G be the Galois group of $K(i)/\mathbb{R}$.

$|G| = 2^k m$, for m odd, $k \geq 1$. By Sylow's theorems, there exists a subgroup P_2 of G of order 2^k.

P_2 has index m, so the fixed field has degree m.

There are no nontrivial odd degree extension of $\mathbb{R}$, so $m = 1$.

Therefore G is a 2-group (its order is a power of 2). In particular, $G' = \mathrm{Aut}(K(i)/\mathbb{C})$ is also a 2-group (of order 2^{k-1}).

General result about p-groups, for p prime: they have subgroups of all orders. In particular (if $k \neq 1$), G' has a subgroup H of index 2.

The fixed field of H must be a degree 2 extension of $\mathbb{C}$, contradiction. Therefore $k = 1, m = 1$: $K(i) = \mathbb{C}$.

If this the first proof was too much analysis, and the second proof was too much group theory don't worry.

If this the first proof was too much analysis, and the second proof was too much group theory don't worry.

We will now look at a third proof, using "symmetric" polynomials.

Algebraic proof 2, using polynomials

As before, assume $f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$ and no roots in $\mathbb{C}$.

Algebraic proof 2, using polynomials

As before, assume $f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$ and no roots in $\mathbb{C}$.

Write $n = 2^k m$ for m odd, $k \geq 0$. Work by induction on k.

Algebraic proof 2, using polynomials

As before, assume $f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$ and no roots in $\mathbb{C}$.

Write $n = 2^k m$ for m odd, $k \geq 0$. Work by induction on k.

If $k = 0$, f has a root by the intermediate value theorem. Assume now $k \geq 1$.

Algebraic proof 2, using polynomials

As before, assume $f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$ and no roots in $\mathbb{C}$.

Write $n = 2^k m$ for m odd, $k \geq 0$. Work by induction on k.

If $k = 0$, f has a root by the intermediate value theorem. Assume now $k \geq 1$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$. As before, $K(i)/\mathbb{R}$ is Galois. Write $K = \mathbb{R}(\alpha_1, \ldots, \alpha_n, i)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$.

Algebraic proof 2, using polynomials

As before, assume $f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$ and no roots in $\mathbb{C}$.

Write $n = 2^k m$ for m odd, $k \geq 0$. Work by induction on k.

If $k = 0$, f has a root by the intermediate value theorem. Assume now $k \geq 1$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$. As before, $K(i)/\mathbb{R}$ is Galois. Write $K = \mathbb{R}(\alpha_1, \ldots, \alpha_n, i)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$.

For each $t \in \mathbb{R}$, let:

$$L_t(x) := \prod_{1 \leq i < j \leq n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$$

Algebraic proof 2, using polynomials

As before, assume $f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$ and no roots in $\mathbb{C}$.

Write $n = 2^k m$ for m odd, $k \geq 0$. Work by induction on k.

If $k = 0$, f has a root by the intermediate value theorem. Assume now $k \geq 1$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$. As before, $K(i)/\mathbb{R}$ is Galois. Write $K = \mathbb{R}(\alpha_1, \ldots, \alpha_n, i)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$.

For each $t \in \mathbb{R}$, let:

$$L_t(x) := \prod_{1 \leq i < j \leq n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$$

$L_t(x)$ is fixed by any automorphism of $K(i)$, so is in $\mathbb{R}[x]$.

Algebraic proof 2, using polynomials

As before, assume $f(x) \in \mathbb{R}[x]$ has degree $n \geq 1$ and no roots in $\mathbb{C}$.

Write $n = 2^k m$ for m odd, $k \geq 0$. Work by induction on k.

If $k = 0$, f has a root by the intermediate value theorem. Assume now $k \geq 1$.

Let $K/\mathbb{R}$ be the splitting field of $f(x)$. As before, $K(i)/\mathbb{R}$ is Galois. Write $K = \mathbb{R}(\alpha_1, \ldots, \alpha_n, i)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$.

For each $t \in \mathbb{R}$, let:

$$L_t(x) := \prod_{1 \leq i < j \leq n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$$

$L_t(x)$ is fixed by any automorphism of $K(i)$, so is in $\mathbb{R}[x]$.

It has degree $\frac{n(n-1)}{2} = 2^{k-1}m(2^k m - 1) = 2^{k-1}m'$, m' odd.

Reminder: $n = 2^k m$, working by induction on k. $\alpha_1, \ldots, \alpha_n$ roots of $f(x)$. $L_t(x) := \prod_{1 \le i < j \le n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$. $L_t(x) \in \mathbb{R}[x]$, with degree $2^{k-1}m'$, m' odd.

Reminder: $n = 2^k m$, working by induction on k. $\alpha_1, \ldots, \alpha_n$ roots of $f(x)$. $L_t(x) := \prod_{1 \leq i < j \leq n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$. $L_t(x) \in \mathbb{R}[x]$, with degree $2^{k-1}m'$, m' odd.

By the induction hypothesis, $L_t(x)$ has a root in $\mathbb{C}$. Thus for some $i < j$, $x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)$ has a root: $\alpha_i\alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$.

Reminder: $n = 2^k m$, working by induction on k. $\alpha_1, \ldots, \alpha_n$ roots of $f(x)$. $L_t(x) := \prod_{1 \le i < j \le n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$. $L_t(x) \in \mathbb{R}[x]$, with degree $2^{k-1}m'$, m' odd.

By the induction hypothesis, $L_t(x)$ has a root in $\mathbb{C}$. Thus for some $i < j$, $x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)$ has a root: $\alpha_i\alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$.

This is true for each $t \in \mathbb{R}$, there are infinitely-many and finitely-many possibilities for $i < j$. Thus there are $t \neq s$ in $\mathbb{R}$ and $i < j$ so that $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$ and $\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C}$.

Reminder: $n = 2^k m$, working by induction on k. $\alpha_1, \ldots, \alpha_n$ roots of $f(x)$. $L_t(x) := \prod_{1 \le i < j \le n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$. $L_t(x) \in \mathbb{R}[x]$, with degree $2^{k-1}m'$, m' odd.

By the induction hypothesis, $L_t(x)$ has a root in $\mathbb{C}$. Thus for some $i < j$, $x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)$ has a root: $\alpha_i\alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$.

This is true for each $t \in \mathbb{R}$, there are infinitely-many and finitely-many possibilities for $i < j$. Thus there are $t \neq s$ in $\mathbb{R}$ and $i < j$ so that $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$ and $\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C}$.

Subtract them, get that $b = \alpha_i\alpha_j \in \mathbb{C}$, and therefore $a = \alpha_i + \alpha_j \in \mathbb{C}$.

Reminder: $n = 2^k m$, working by induction on k. $\alpha_1, \dots, \alpha_n$ roots of $f(x)$. $L_t(x) := \prod_{1 \le i < j \le n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$. $L_t(x) \in \mathbb{R}[x]$, with degree $2^{k-1}m'$, m' odd.

By the induction hypothesis, $L_t(x)$ has a root in $\mathbb{C}$. Thus for some $i < j$, $x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)$ has a root: $\alpha_i\alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$.

This is true for each $t \in \mathbb{R}$, there are infinitely-many and finitely-many possibilities for $i < j$. Thus there are $t \neq s$ in $\mathbb{R}$ and $i < j$ so that $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$ and $\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C}$.

Subtract them, get that $b = \alpha_i\alpha_j \in \mathbb{C}$, and therefore $a = \alpha_i + \alpha_j \in \mathbb{C}$.

α_i, α_j are roots of $x^2 - ax + b$, so are in $\mathbb{C}$, as desired.

Reminder: $n = 2^k m$, working by induction on k. $\alpha_1, \dots, \alpha_n$ roots of $f(x)$. $L_t(x) := \prod_{1 \leq i < j \leq n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$. $L_t(x) \in \mathbb{R}[x]$, with degree $2^{k-1}m'$, m' odd.

By the induction hypothesis, $L_t(x)$ has a root in $\mathbb{C}$. Thus for some $i < j$, $x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)$ has a root: $\alpha_i\alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$.

This is true for each $t \in \mathbb{R}$, there are infinitely-many and finitely-many possibilities for $i < j$. Thus there are $t \neq s$ in $\mathbb{R}$ and $i < j$ so that $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$ and $\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C}$.

Subtract them, get that $b = \alpha_i\alpha_j \in \mathbb{C}$, and therefore $a = \alpha_i + \alpha_j \in \mathbb{C}$.

α_i, α_j are roots of $x^2 - ax + b$, so are in $\mathbb{C}$, as desired.

We will talk more about polynomials like $L_t(x)$ next time!

Summary

Theorem (Gauss-Wantzel)

The regular n-gon can be constructed if and only if n is the product of a power of 2 and distinct Fermat primes.

Theorem (Fundamental theorem of algebra)

$\mathbb{C}$ is algebraically closed: if $f(x) \in \mathbb{C}[x]$ is not constant, then it has a root in $\mathbb{C}$.