

Constructible Numbers

Pranav Krishnapuram

August 2026

1 Introduction

In this paper, we study constructible numbers and develop the algebraic framework underlying classical compass-and-straightedge constructions, culminating in the Gauss–Wantzel theorem.

We begin with geometric constructions and use algebra to show that the constructible real numbers form a field that is closed under square roots of positive elements. We then develop the necessary tools from abstract algebra, including field extensions, minimal polynomials, Gauss’s lemmas, roots of unity, and cyclotomic polynomials. Finally, we apply these results to characterize the constructible regular polygons and prove the Gauss–Wantzel theorem. Standard treatments of constructibility and its field-theoretic formulation can be found in Cox, Dummit and Foote, and Hadlock [1, 2, 4].

2 Geometric Constructions

Definition 1 (Compass and Straightedge Construction). *A compass-and-straightedge construction is a finite sequence of geometric operations on $\mathbb{R}^2$, starting from the points $(0,0)$ and $(1,0)$, with the following allowed operations:*

1. *Given any two previously constructed points, construct the line through them.*
2. *Given any two previously constructed points, construct the circle centered at the first point and passing through the second.*
3. *Given any two previously constructed nonparallel lines, construct their point of intersection.*
4. *Given a previously constructed line and a previously constructed circle that intersect, construct their one or two points of intersection.*
5. *Given any two previously constructed circles that intersect, construct their one or two points of intersection.*

Lemma 1. *Given any three constructible points $A, B, C \in \mathbb{R}^2$, the circle centered at A with radius $\overline{BC}$ is also constructible.*

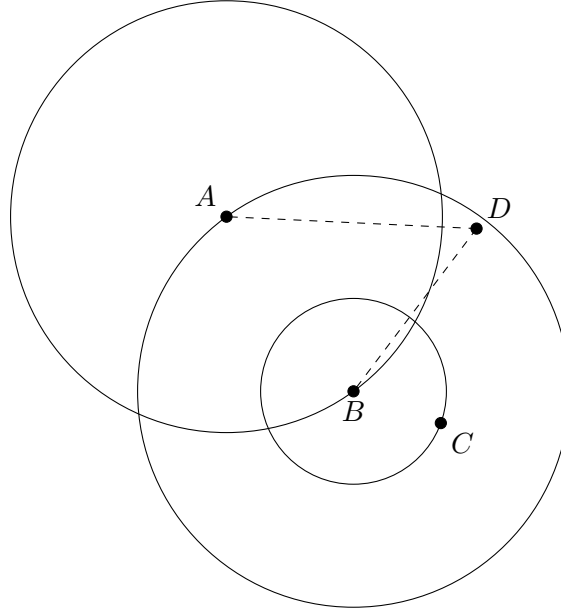
In effect, this lemma allows us to translate distances.

Proof. The construction from the original geometric argument is illustrated below. Begin with constructible points A, B, C . Construct the circles centered at B through A , centered at A through B , and centered at B through C . Let D be one of the intersections of the first two circles. Then $DA = DB = AB$. Let F be the intersection of the line DB with the circle centered at B through

C , chosen on the ray from D through B . Construct the circle centered at D through F , and let G be its intersection with the line DA , chosen on the ray from D through A . Since $DG = DF$ and $DA = DB$, we have

$$AG = DG - DA = DF - DB = BF = BC.$$

Thus the circle centered at A and passing through G has radius BC .

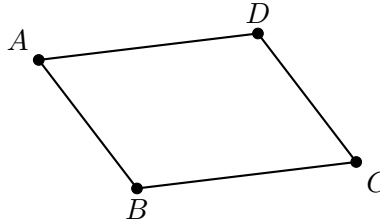


□

Lemma 2. *Given any three constructible points $A, B, C \in \mathbb{R}^2$, the line through A parallel to $\overleftrightarrow{BC}$ is constructible.*

This lemma allows us to translate line segments while preserving direction.

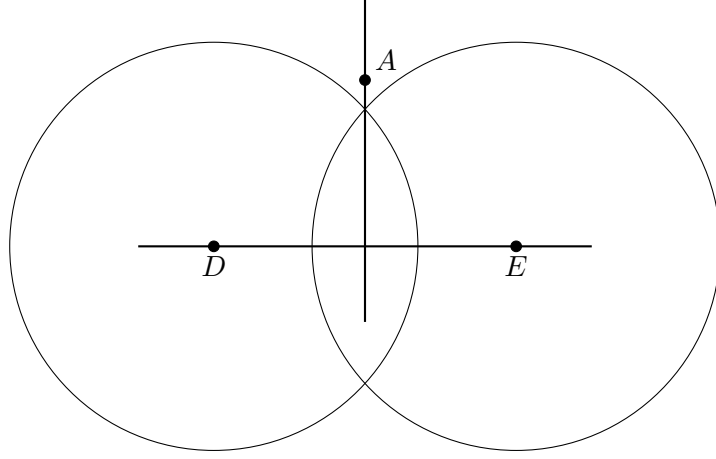
Proof. By Lemma 1, construct a circle centered at A of radius BC and a circle centered at C of radius AB . Their intersections with the appropriate circles centered at B and A produce a fourth vertex D of a parallelogram $ABCD$. Since opposite sides of a parallelogram are parallel, the line AD is parallel to BC , and it is constructible from the constructed points A and D .



□

Lemma 3. *Given any three constructible points $A, B, C \in \mathbb{R}^2$, the line through A perpendicular to $\overleftrightarrow{BC}$ is constructible.*

Proof. Choose a constructible circle centered at A large enough to meet $\overleftrightarrow{BC}$ in two points D and E . Since $AD = AE$, the point A lies on the perpendicular bisector of DE . Construct equal-radius circles centered at D and E ; their two intersections determine that perpendicular bisector. Hence the perpendicular to BC through A is constructible.



□

We now formalize constructible numbers themselves.

Definition 2. A real number a is constructible if a point whose signed distance from the origin along a fixed coordinate axis is a can be obtained by a compass-and-straightedge construction. Equivalently, $(a, 0)$ is constructible.

Theorem 1. A point $(x, y) \in \mathbb{R}^2$ is constructible if and only if both x and y are constructible real numbers.

Proof. If (x, y) is constructible, Lemmas 2 and 3 allow us to draw horizontal and vertical lines through it. Intersecting these with the coordinate axes constructs $(x, 0)$ and $(0, y)$, so x and y are constructible.

Conversely, if x and y are constructible, then $(x, 0)$ and $(0, y)$ are constructible. Construct the vertical line through $(x, 0)$ and the horizontal line through $(0, y)$ using Lemmas 2 and 3. Their intersection is (x, y) . □

Theorem 2. If $a, b \in \mathbb{R}$ are constructible, then $a + b$ is constructible.

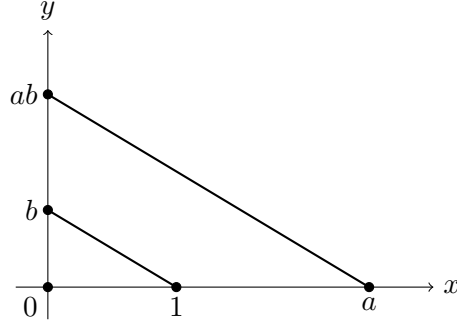
Proof. Construct $(a, 0)$ and $(b, 0)$. By Lemma 1, we may translate the distance $|b|$ to begin at $(a, 0)$ along the x -axis, choosing the appropriate direction according to the sign of b . The resulting endpoint has coordinate $(a + b, 0)$, so $a + b$ is constructible. □

Theorem 3. If $a, b \in \mathbb{R}$ are constructible, then ab is constructible.

Proof. It is enough to give the construction for positive a, b ; signs are handled by reflection. Construct $(0, 0)$, $(1, 0)$, $(a, 0)$, and $(0, b)$. Draw the line through $(1, 0)$ and $(0, b)$, then draw through $(a, 0)$ a parallel line using Lemma 2. If this line meets the y -axis at $(0, p)$, the resulting triangles are similar, so

$$\frac{p}{a} = \frac{b}{1}.$$

Hence $p = ab$, and therefore ab is constructible.



□

Theorem 4. *If $a \neq 0$ is constructible, then $1/a$ is constructible.*

Proof. Again it is enough to treat $a > 0$. Construct $(0,0)$, $(1,0)$, $(a,0)$, and $(0,1)$. Draw the line through $(0,1)$ and $(a,0)$, and through $(1,0)$ draw a parallel line. If the latter meets the y -axis at $(0,p)$, similar triangles give

$$\frac{p}{1} = \frac{1}{a},$$

so $p = 1/a$ is constructible.

□

These results already imply that the constructible real numbers are a subfield of $\mathbb{R}$. We have closure under additive inverses by reflection, closure under multiplicative inverses by Theorem 4, closure under addition and multiplication by Theorems 2 and 3, and the elements 0 and 1 are present from the initial construction. Since this field contains $\mathbb{Q}$, it is a field extension of $\mathbb{Q}$.

Definition 3. *Let $C \subseteq \mathbb{R}$ denote the field of constructible real numbers.*

We also extend the notion of constructibility to complex numbers.

Definition 4. *A complex number $z = a + bi \in \mathbb{C}$ is complex constructible if $a, b \in C$.*

Corollary 1. *The set of complex constructible numbers is a field.*

Proof. If $a, b, c, d \in C$, then

$$a + c, \quad b + d, \quad ac - bd, \quad ad + bc, \quad -a, \quad -b \in C.$$

Moreover, for $a + bi \neq 0$,

$$\frac{1}{a + bi} = \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2},$$

and both real and imaginary parts lie in C . Thus the complex constructible numbers are closed under the field operations and contain 0 and 1.

□

Definition 5. *Let $C' \subseteq \mathbb{C}$ denote the field of complex constructible numbers.*

Theorem 5. *For a constructible $a \in \mathbb{R}$, the number $\sqrt{|a|}$ is constructible.*

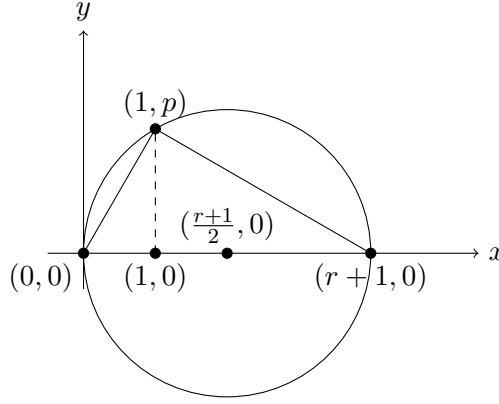
Thus C is closed under square roots of positive elements.

Proof. Let $r = |a| \geq 0$. If $r = 0$ there is nothing to prove. Since C is a field, the points $(r+1, 0)$ and $((r+1)/2, 0)$ are constructible. Construct the circle with diameter from $(0, 0)$ to $(r+1, 0)$, so its center is $((r+1)/2, 0)$. Construct the vertical line through $(1, 0)$ and let $(1, p)$ be an intersection with the circle.

The right triangle formed by $(0, 0)$, $(1, p)$, and $(r+1, 0)$ satisfies

$$\left(\frac{r-1}{2}\right)^2 + p^2 = \left(\frac{r+1}{2}\right)^2,$$

so $p^2 = r$. Hence $p = \sqrt{r} = \sqrt{|a|}$ is constructible.



□

Theorem 6. *If $a + bi \in C'$ and $z^2 = a + bi$, then $z \in C'$.*

Proof. Let

$$r = \sqrt{a^2 + b^2}, \quad u = \sqrt{\frac{r+a}{2}}, \quad v = \sqrt{\frac{r-a}{2}}.$$

Because $a, b \in C$, Theorem 5 implies that $r, u, v \in C$. If $b \neq 0$, choose $\varepsilon \in \{1, -1\}$ to have the same sign as b . Then

$$(u + i\varepsilon v)^2 = u^2 - v^2 + 2i\varepsilon uv = a + bi,$$

since $u^2 - v^2 = a$ and $2uv = |b|$. Thus the two square roots are

$$\pm \left(\sqrt{\frac{r+a}{2}} + i \operatorname{sgn}(b) \sqrt{\frac{r-a}{2}} \right),$$

and both are in C' . If $b = 0$, the result follows directly from Theorem 5, with a factor of i when $a < 0$. □

A natural question is whether the field operations and square roots are not only sufficient for many constructions, but also necessary. To answer this, we pass from geometry to field extensions. We first express the geometric intersection operations algebraically.

3 Algebra and Analytic Geometry

Lemma 4. *A circle*

$$(x - x_0)^2 + (y - y_0)^2 = r^2$$

is constructible if and only if x_0, y_0, r are constructible.

Proof. If $x_0, y_0, r \in C$, then (x_0, y_0) and $(x_0 + r, y_0)$ are constructible by Theorem 1 and closure of C . Axiom 2 therefore constructs the desired circle.

Conversely, a constructed circle is produced from its center and a point on it, so its center (x_0, y_0) is constructible. By Lemma 2, the horizontal line through the center is constructible; intersecting it with the circle gives $(x_0 \pm r, y_0)$. Hence r is constructible by closure of C under subtraction. $\square$

A nonvertical line has an equation $y = ax + b$, while a vertical line has the form $x = c$.

Lemma 5. *A line of the form $y = ax + b$ is constructible if and only if a, b are constructible.*

Proof. If $a, b \in C$, then $(0, b)$ and $(1, a + b)$ are constructible, so the line through them is constructible.

Conversely, if the line is constructible, intersect it with $x = 0$ to obtain $(0, b)$, so $b \in C$. If $a = 0$ there is nothing more to prove. Otherwise, intersect with $x = 1$ to obtain $(1, a + b)$, and then $a = (a + b) - b \in C$. For a vertical line $x = c$, its intersection with the x -axis gives $(c, 0)$, so $c \in C$. $\square$

The equations of constructible objects therefore use constructible coefficients. We now analyze what happens when such objects are intersected.

Lemma 6. *Let $F \subseteq \mathbb{R}$ be a field. If an intersection of two lines, a line and a circle, or two circles has defining coefficients in F , then each coordinate of every intersection point lies in $F(\alpha)$ for some α satisfying a polynomial of degree at most 2 over F .*

Proof. For two circles

$$(x - x_0)^2 + (y - y_0)^2 = r^2, \quad (x - x'_0)^2 + (y - y'_0)^2 = r'^2,$$

subtracting the equations produces a linear equation with coefficients in F . Thus the problem reduces to a line–circle intersection.

For a circle and a nonvertical line $y = ax + b$, substitution gives

$$\begin{aligned} 0 &= (x - x_0)^2 + (ax + b - y_0)^2 - r^2 \\ &= (a^2 + 1)x^2 + (2ab - 2ay_0 - 2x_0)x + (x_0^2 + b^2 + y_0^2 - 2by_0 - r^2), \end{aligned}$$

which is quadratic over F . Hence an x -coordinate lies in $F(\alpha)$ for a root α of a polynomial of degree at most 2, and then $y = ax + b$ lies in the same field. If the line is vertical, $x = c \in F$ and the circle equation becomes a quadratic in y .

Finally, the intersection of two nonparallel lines is obtained by solving a nonsingular 2×2 linear system over F , so both coordinates already lie in F . $\square$

Lemma 7. *Let $F \subseteq \mathbb{R}$. If two constructed points have coordinates in F , then the line and circle constructed from those points have coefficients in a field obtained from F by an extension of degree at most 2.*

Proof. The line through two F -points has coefficients in F . A circle centered at one F -point and passing through another has squared radius

$$(c - a)^2 + (d - b)^2 \in F.$$

Its equation therefore has coefficients in F when written using the squared radius; equivalently, its radius lies in at most a quadratic extension of F . This is the algebraic content of Lemmas 4 and 5. $\square$

Therefore each new constructible object or point has coefficients or coordinates in a field obtained from the field generated by the previous data by adjoining at most a quadratic root.

4 Abstract Algebra

Theorem 7. *Any constructible number lies in some field F_k in a finite sequence of fields*

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k,$$

where

$$F_{i+1} = F_i(\alpha_i)$$

for some α_i satisfying a polynomial of degree at most 2 in $F_i[x]$.

Proof. Consider a finite compass-and-straightedge construction starting from $(0, 0)$ and $(1, 0)$. We argue inductively through the construction. Initially all coordinates lie in $F_0 = \mathbb{Q}$. Suppose all coefficients and coordinates used up to a certain stage lie in F_i . By Lemmas 6 and 7, the next construction either remains in F_i or introduces coordinates obtained by solving a quadratic over F_i . Adjoining one such root α_i gives a field $F_{i+1} = F_i(\alpha_i)$ containing all previous data and the newly constructed data. Since the construction is finite, the desired number lies in some final field F_k . $\square$

By the quadratic formula, this is equivalent to saying that a constructible number can be reached through a finite tower obtained by adjoining square roots. We now develop the field-degree tools needed to exploit that observation [1, 2, 4].

Definition 6. *For fields $G \subseteq F$, let $[F : G]$, read as the degree of F over G , denote the dimension of F as a vector space over G .*

Lemma 8. *For fields $H \subseteq G \subseteq F$ of finite degree,*

$$[F : G][G : H] = [F : H].$$

Proof. Let $\{f_i\}_{i=1}^{[F:G]}$ be a basis of F over G , and let $\{g_j\}_{j=1}^{[G:H]}$ be a basis of G over H . We claim that

$$B = \{f_i g_j : 1 \leq i \leq [F : G], 1 \leq j \leq [G : H]\}$$

is a basis of F over H .

Every $f \in F$ can be written as $f = \sum_i f_i a_i$ with $a_i \in G$, and each a_i can be written as $a_i = \sum_j b_{ij} g_j$ with $b_{ij} \in H$. Hence B spans F over H .

For linear independence, suppose

$$\sum_{i,j} c_{ij} f_i g_j = 0, \quad c_{ij} \in H.$$

Grouping by i gives

$$\sum_i f_i \left(\sum_j c_{ij} g_j \right) = 0.$$

Because the f_i are linearly independent over G , each inner sum is zero; because the g_j are linearly independent over H , every $c_{ij} = 0$. Thus B is a basis and has size $[F : G][G : H]$. $\square$

Theorem 8. *For a finite tower*

$$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t,$$

we have

$$[F_t : F_0] = \prod_{i=1}^t [F_i : F_{i-1}].$$

Proof. This follows by induction from Lemma 8. The one-step case is immediate. If the formula holds through F_t , then

$$[F_{t+1} : F_0] = [F_{t+1} : F_t][F_t : F_0] = [F_{t+1} : F_t] \prod_{i=1}^t [F_i : F_{i-1}],$$

as required. $\square$

Theorem 9. *Let F be a field, and let α be a root of an irreducible polynomial $g(x) \in F[x]$ of degree n . Then*

$$[F(\alpha) : F] = n.$$

Proof. We first show that

$$B = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

is linearly independent over F . If

$$\sum_{i=0}^{n-1} f_i \alpha^i = 0,$$

then $f(x) = \sum_{i=0}^{n-1} f_i x^i$ has α as a root. If $f \neq 0$, then $\deg f < n = \deg g$, so $g \nmid f$. Since g is irreducible, $\gcd(f, g) = 1$. Bezout's identity gives $a(x)f(x) + b(x)g(x) = 1$, and evaluating at α yields $0 = 1$, a contradiction. Thus $f = 0$ and B is linearly independent.

Next, $F[\alpha]$ is a field. If $0 \neq f(\alpha) \in F[\alpha]$, then $g \nmid f$, so $\gcd(f, g) = 1$. Hence there are $a, b \in F[x]$ with

$$a(x)f(x) + b(x)g(x) = 1.$$

Evaluating at α gives $a(\alpha)f(\alpha) = 1$, so $f(\alpha)$ has an inverse in $F[\alpha]$. Thus $F(\alpha) = F[\alpha]$.

Finally, polynomial division by g reduces every power α^m with $m \geq n$ to an F -linear combination of $1, \alpha, \dots, \alpha^{n-1}$. Hence B spans $F(\alpha)$ and is a basis of size n . $\square$

Corollary 2. *For $c \in C$, the degree $[\mathbb{Q}(c) : \mathbb{Q}]$ is a power of 2.*

Proof. By Theorem 7, c lies in a tower

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t$$

in which each step is obtained by adjoining a root of a polynomial of degree at most 2. By Theorem 9, each degree $[F_i : F_{i-1}]$ is either 1 or 2. Therefore Theorem 8 gives

$$[F_t : \mathbb{Q}] = \prod_{i=1}^t [F_i : F_{i-1}] = 2^m$$

for some $m \geq 0$.

Since $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq F_t$, Lemma 8 gives

$$[F_t : \mathbb{Q}] = [F_t : \mathbb{Q}(c)] [\mathbb{Q}(c) : \mathbb{Q}].$$

Thus $[\mathbb{Q}(c) : \mathbb{Q}]$ divides a power of 2 and is itself a power of 2. $\square$

Corollary 3. *For $a + bi \in C'$, the degree $[\mathbb{Q}(a + bi) : \mathbb{Q}]$ is a power of 2.*

Proof. Combine quadratic towers containing a and b , and adjoin i , which satisfies $x^2 + 1 = 0$. The resulting field F_t is obtained from $\mathbb{Q}$ by extensions of degree 1 or 2 and contains $a + bi$. The same tower-law argument as in Corollary 2 shows that $[\mathbb{Q}(a + bi) : \mathbb{Q}]$ is a power of 2. $\square$

Our next goal is to study irreducible and minimal polynomials, which will allow us to compute the degrees of cyclotomic extensions.

Lemma 9. *Every ideal I in $F[x]$, where F is a field, is principal.*

Proof. If $I = \{0\}$, it is generated by 0. Otherwise choose a nonzero polynomial $f \in I$ of minimal degree. For any $g \in I$, the division algorithm gives

$$g = qf + r, \quad \deg r < \deg f.$$

Since I is an ideal, $r = g - qf \in I$. Minimality of $\deg f$ forces $r = 0$. Thus every $g \in I$ is divisible by f , so $I = (f)$. $\square$

Definition 7. *Let α be algebraic over a field F . A minimal polynomial of α over F is a monic polynomial $m_\alpha(x) \in F[x]$ such that $m_\alpha(\alpha) = 0$ and every polynomial in $F[x]$ having α as a root is divisible by $m_\alpha(x)$.*

Lemma 10. *Every algebraic element α over a field F has a minimal polynomial over F .*

Proof. The set

$$I = \{f(x) \in F[x] : f(\alpha) = 0\}$$

is a nonzero ideal of $F[x]$. By Lemma 9, $I = (m)$ for some nonzero m . Multiplying m by the inverse of its leading coefficient makes it monic without changing the ideal. The resulting monic generator m_α divides every polynomial in I , so it is a minimal polynomial. $\square$

Theorem 10. *A minimal polynomial $f(x)$ of an algebraic element α over $\mathbb{Q}$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose $f = gh$ with $g, h \in \mathbb{Q}[x]$ of positive degree. Since

$$0 = f(\alpha) = g(\alpha)h(\alpha),$$

we may assume $g(\alpha) = 0$. Then the defining property of the minimal polynomial gives $f \mid g$, impossible because $\deg g < \deg f$. Hence f is irreducible. $\square$

Theorem 11. *The minimal polynomial of an algebraic element α over $\mathbb{Q}$ is unique.*

Proof. If f and g are both minimal polynomials of α , then $f \mid g$ and $g \mid f$. Thus $g = cf$ for some $c \in \mathbb{Q}^\times$. Since both are monic, $c = 1$, so $f = g$. $\square$

Definition 8. *A polynomial $f(x) \in \mathbb{Z}[x]$ is primitive if the greatest common divisor of its coefficients is 1.*

Lemma 11 (Gauss's lemma). *The product of two primitive polynomials in $\mathbb{Z}[x]$ is primitive.*

Proof. Let $a, b \in \mathbb{Z}[x]$ be primitive and suppose their product ab is not primitive. Then some prime p divides every coefficient of ab , so $ab \equiv 0$ in $\mathbb{F}_p[x]$. Since $\mathbb{F}_p[x]$ is an integral domain, either $a \equiv 0$ or $b \equiv 0$ modulo p . Hence every coefficient of a or every coefficient of b is divisible by p , contradicting primitivity. $\square$

This is one standard form of Gauss's lemma. The following closely related factorization result is also commonly called Gauss's lemma; see, for example, Cox or Dummit and Foote [1, 2].

Lemma 12 (Gauss's lemma). *If $0 \neq f(x) \in \mathbb{Z}[x]$ is primitive and factors in $\mathbb{Q}[x]$ as*

$$f(x) = a(x)b(x)$$

with a, b nonconstant, then it also factors in $\mathbb{Z}[x]$ as

$$f(x) = a'(x)b'(x)$$

with a', b' nonconstant.

Proof. Clear denominators in a and b and then divide each resulting integer polynomial by the gcd of its coefficients. Thus there are primitive $a', b' \in \mathbb{Z}[x]$ and nonzero rationals q_a, q_b such that

$$a' = q_a a, \quad b' = q_b b.$$

Therefore

$$a'b' = q_a q_b f.$$

Write $q_a q_b = c/d$ in lowest terms. Because f is primitive and $a'b'$ has integer coefficients, d must be a unit. By Lemma 11, $a'b'$ is primitive, so $|c| = 1$. After changing the sign of one factor if necessary, $f = a'b'$. $\square$

Lemma 13. *Let ζ be a primitive n th root of unity, and let f be its minimal polynomial over $\mathbb{Q}$. If p is prime and $p \nmid n$, then*

$$f(\zeta^p) = 0.$$

Proof. Since $\zeta^n = 1$, the minimal polynomial f divides $x^n - 1$ in $\mathbb{Q}[x]$. By Gauss's lemma, because $x^n - 1$ is primitive and monic, we may write

$$x^n - 1 = f(x)g(x)$$

with $f, g \in \mathbb{Z}[x]$.

Assume for contradiction that $f(\zeta^p) \neq 0$. Since $\gcd(p, n) = 1$, ζ^p is again a primitive n th root of unity, and therefore $g(\zeta^p) = 0$. Hence ζ is a root of $g(x^p)$, so minimality of f gives

$$g(x^p) = f(x)h(x)$$

for some $h \in \mathbb{Z}[x]$, again using Gauss's lemma to keep integer coefficients.

Reduce coefficients modulo p and write the reductions as f_p, g_p, h_p . In $\mathbb{F}_p[x]$, the Frobenius identity gives

$$g_p(x^p) = g_p(x)^p,$$

because if $g_p(x) = \sum_i a_i x^i$, then

$$g_p(x)^p = \sum_i a_i^p x^{ip} = \sum_i a_i x^{ip} = g_p(x^p).$$

Thus

$$g_p(x)^p = f_p(x)h_p(x).$$

Let k_p be an irreducible factor of f_p . Then $k_p \mid g_p^p$, so $k_p \mid g_p$. Therefore f_p and g_p share a common factor, and $x^n - 1 = f_p g_p$ has a repeated irreducible factor over $\mathbb{F}_p$.

But

$$\frac{d}{dx}(x^n - 1) = nx^{n-1},$$

and because $p \nmid n$,

$$\gcd(x^n - 1, nx^{n-1}) = 1$$

in $\mathbb{F}_p[x]$. Hence $x^n - 1$ has no repeated irreducible factor, a contradiction. Therefore $f(\zeta^p) = 0$. $\square$

We now turn to cyclotomic polynomials and roots of unity. These are classical tools in the algebraic theory of constructibility [1, 2]. We include the relevant arguments in order to make the proof of the Gauss–Wantzel theorem largely self-contained.

Definition 9. Let $\zeta = e^{2\pi i/n}$. The n th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{1 \leq j \leq n \\ \gcd(j, n) = 1}} (x - \zeta^j).$$

Theorem 12. For every positive integer n ,

$$\Phi_n(x) \in \mathbb{Z}[x].$$

Proof. Since every n th root of unity has a unique order dividing n ,

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

We use strong induction on n . For $n = 1$, $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Suppose the result holds for every positive divisor $d < n$ and set

$$F_n(x) = \prod_{\substack{d \mid n \\ d < n}} \Phi_d(x) \in \mathbb{Z}[x].$$

Each Φ_d is monic, so F_n is monic. We have

$$x^n - 1 = F_n(x)\Phi_n(x).$$

Divide the monic polynomial $x^n - 1$ by the monic polynomial F_n in $\mathbb{Z}[x]$:

$$x^n - 1 = F_n(x)q(x) + r(x), \quad q, r \in \mathbb{Z}[x], \quad \deg r < \deg F_n.$$

Comparing with $x^n - 1 = F_n \Phi_n$ gives

$$F_n(\Phi_n - q) = r.$$

If $r \neq 0$, then $\deg r \geq \deg F_n$, a contradiction. Thus $r = 0$ and $\Phi_n = q \in \mathbb{Z}[x]$. $\square$

Theorem 13. *The polynomial $\Phi_n(x)$ is the minimal polynomial over $\mathbb{Q}$ of a primitive n th root of unity ζ . Consequently,*

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n = \varphi(n),$$

where φ is Euler's totient function.

Proof. Let f be the minimal polynomial of ζ . Since $\Phi_n(\zeta) = 0$, minimality gives $f \mid \Phi_n$ in $\mathbb{Q}[x]$.

On the other hand, let j satisfy $\gcd(j, n) = 1$. Factor j into primes. Every prime divisor of j is relatively prime to n , so repeated application of Lemma 13 shows that $f(\zeta^j) = 0$. Hence every primitive n th root of unity is a root of f . Therefore $\Phi_n \mid f$. Both f and Φ_n are monic, so $f = \Phi_n$.

There are exactly $\varphi(n)$ integers $1 \leq j \leq n$ relatively prime to n , so $\deg \Phi_n = \varphi(n)$. The final degree statement follows from Theorem 9. $\square$

Lemma 14. *If $2^a + 1$ is prime, then either $a = 0$ or a is a power of 2.*

Proof. Write $a = 2^s m$ with m odd. If $m > 1$, then

$$2^a + 1 = (2^{2^s})^m + 1,$$

and since m is odd, $x^m + 1$ is divisible by $x + 1$. Thus $2^{2^s} + 1$ is a nontrivial divisor of $2^a + 1$, contradicting primality. Hence $m = 1$ and $a = 2^s$. The case $a = 0$ gives the prime 2. $\square$

Lemma 15. *Suppose $\gcd(a, b) = 1$. If $e^{2\pi i/a}$ and $e^{2\pi i/b}$ are constructible, then $e^{2\pi i/(ab)}$ is constructible.*

Proof. By Bezout's identity, choose integers r, s such that

$$rb + sa = 1.$$

Then

$$e^{2\pi i/(ab)} = e^{2\pi i(rb+sa)/(ab)} = \left(e^{2\pi i/a}\right)^r \left(e^{2\pi i/b}\right)^s.$$

Since C' is a field, integer powers, products, and inverses of constructible complex numbers remain constructible. $\square$

Lemma 16. *For every integer $a \geq 1$, a regular 2^a -gon is constructible.*

Proof. A square is constructible. Bisecting the central angle of any constructible regular polygon produces a regular polygon with twice as many sides. Angle bisection is a standard compass-and-straightedge construction and algebraically requires only a square root. Iterating gives every regular 2^a -gon. $\square$

5 Main Results

We can now characterize the possible numbers of sides of a constructible regular polygon.

Theorem 14. *If a regular n -gon is constructible, then*

$$n = 2^e \prod_{j=1}^r p_j,$$

where $e \geq 0$ and the p_j are distinct Fermat primes, that is, primes of the form

$$p_j = 2^{2^{m_j}} + 1.$$

Proof. Let

$$\zeta = e^{2\pi i/n}.$$

If the regular n -gon is constructible, then ζ is complex constructible. By Corollary 3,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}]$$

is a power of 2. By Theorem 13,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n).$$

Thus $\varphi(n)$ is a power of 2.

Write

$$n = 2^e \prod_{j=1}^r q_j^{a_j}$$

with the q_j distinct odd primes. Euler's formula gives

$$\varphi(n) = \varphi(2^e) \prod_{j=1}^r q_j^{a_j-1} (q_j - 1).$$

Since this is a power of 2, no odd prime can divide it. Therefore $a_j = 1$ for every j , and each $q_j - 1$ is a power of 2. Write $q_j = 2^{c_j} + 1$. By Lemma 14, each positive c_j is a power of 2. Hence each q_j is a Fermat prime. The odd primes are distinct because each occurs to the first power only. $\square$

This establishes the necessity direction of the Gauss–Wantzel classification. Historically, Gauss developed the connection between regular polygon constructions and Fermat primes, while Wantzel's 1837 work supplied the field-theoretic obstruction underlying the converse direction [3, 7].

Theorem 15 (Gauss–Wantzel). *If*

$$n = 2^e \prod_{j=1}^r p_j,$$

where $e \geq 0$ and the p_j are distinct Fermat primes, then the regular n -gon is constructible.

Proof. By Lemma 16, the regular 2^e -gon is constructible. By Lemma 15, constructions for pairwise coprime factors can be combined. Therefore it remains to show that a regular p -gon is constructible whenever

$$p = 2^{2^k} + 1$$

is a Fermat prime.

Set

$$N = 2^k, \quad p = 2^N + 1, \quad \zeta = e^{2\pi i/p}.$$

Because p is prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1 = 2^N$. Choose a primitive root g modulo p . For an integer m , write

$$[m] = \zeta^m,$$

where the exponent is interpreted modulo p .

The nontrivial p th roots of unity are

$$\{[g^j] : 0 \leq j < 2^N\},$$

and their sum is

$$\sum_{j=0}^{2^N-1} [g^j] = -1.$$

Following Gauss's period construction [3, 5], for $0 \leq m \leq N$ and $0 \leq a < 2^m$, define the m -period

$$\eta_{m,a} = \sum_{j=0}^{2^{N-m}-1} \zeta^{g^{a+2^m j}}.$$

At level $m = 0$ there is only one period,

$$\eta_{0,0} = -1,$$

which is constructible. At the final level $m = N$, every period consists of a single root of unity:

$$\eta_{N,a} = \zeta^{g^a}.$$

In particular, constructing all periods recursively will construct ζ itself.

Each m -period splits into two $(m+1)$ -periods:

$$\eta_{m,a} = \eta_{m+1,a} + \eta_{m+1,a+2^m}.$$

The key Gaussian-period multiplication calculation shows that the product of these two child periods is an integer linear combination of m -periods (and possibly an integer constant). To see the mechanism, expand

$$\eta_{m+1,a}\eta_{m+1,a+2^m}$$

as a double sum. Group terms according to the difference of their exponents modulo the subgroup generated by $g^{2^{m+1}}$. Within each group, multiplication by that subgroup merely permutes the summands; each group therefore collapses to a complete m -period, with an integer multiplicity. This is the classical Gaussian-period regrouping used in Gauss's construction [3, 5].

Assume inductively that all m -periods are constructible. Then both

$$S = \eta_{m+1,a} + \eta_{m+1,a+2^m}$$

and

$$P = \eta_{m+1,a}\eta_{m+1,a+2^m}$$

are constructible, since S is the parent m -period and P is an integer linear combination of m -periods. The two child periods are therefore the roots of

$$x^2 - Sx + P = 0.$$

By Theorem 6, square roots of complex constructible numbers are complex constructible, so both child periods are constructible.

Starting from the constructible 0-period -1 and repeating this quadratic splitting N times, every final period $\eta_{N,a} = \zeta^{g^a}$ becomes constructible. Hence ζ is constructible, and therefore the regular p -gon is constructible.

Finally, Lemmas 15 and 16 combine the pairwise coprime Fermat-prime factors and the power-of-two factor, proving the result for every

$$n = 2^e \prod_{j=1}^r p_j.$$

□

Combining Theorems 14 and 15 gives the full classification: a regular n -gon is constructible if and only if

$$n = 2^e \prod_{j=1}^r p_j,$$

where the p_j are distinct Fermat primes.

The only Fermat primes currently known are

$$3, 5, 17, 257, 65537.$$

It remains unknown whether any further Fermat primes exist. This does not make the Gauss–Wantzel classification incomplete: the theorem gives an exact criterion in terms of Fermat primes, and any newly discovered Fermat prime would simply provide another allowable prime factor.

An immediate application is the classical impossibility of trisecting an arbitrary angle using only compass and straightedge. If there were a general angle-trisection construction, it could be applied to the constructible angle 60° to produce 20° . We now show that 20° is not constructible.

Corollary 4. *The angle 20° is not constructible.*

Proof. A 20° central angle on the unit circle corresponds to a primitive 18th root of unity, since

$$20^\circ = \frac{360^\circ}{18}.$$

Thus 20° is constructible if and only if the regular 18-gon is constructible. But

$$18 = 2 \cdot 3^2,$$

which is not of the form 2^e times a product of *distinct* Fermat primes. By the Gauss–Wantzel theorem, the regular 18-gon is not constructible. Hence 20° is not constructible. □

Another classical consequence concerns squaring the circle: constructing a square with the same area as a given circle. The final obstruction uses Lindemann’s 1882 theorem that π is transcendental [6], which we do not prove here.

Corollary 5. *It is impossible to square the circle using only compass and straightedge.*

Proof. Consider the unit circle, whose area is π . A square of equal area would have side length $\sqrt{\pi}$. If such a square were constructible, then $\sqrt{\pi} \in C$, and because C is a field, $\pi = (\sqrt{\pi})^2 \in C$.

However, every constructible number is algebraic over $\mathbb{Q}$ by Theorem 7, while Lindemann proved that π is transcendental. This contradiction shows that the construction is impossible. □

Acknowledgments

This work was carried out during at the AIMS Summer School in 2026 under the guidance of counselor Eli DeWitt (Michigan Technological University) and Dr. Jonathan Hanke (Princeton University). I am grateful for their guidance and encouragement throughout the project.

6 Works Cited

1. Cox, David A. *Galois Theory*. 2nd ed., John Wiley & Sons, 2012.
2. Dummit, David S., and Richard M. Foote. *Abstract Algebra*. 3rd ed., John Wiley & Sons, 2003.
3. Gauss, Carl Friedrich. *Disquisitiones Arithmeticae*. Translated by Arthur A. Clarke, Yale University Press, 1966.
4. Hadlock, Charles Robert. *Field Theory and Its Classical Problems*. Mathematical Association of America, 1978. Carus Mathematical Monographs, no. 19.
5. Kuh, David. “Constructible Regular n -gons.” Whitman College, 2013. <https://www.whitman.edu/documents/academics/Mathematics/Kuh.pdf>. Accessed 14 Aug. 2026.
6. Lindemann, Ferdinand. “Ueber die Zahl π .” *Mathematische Annalen*, vol. 20, 1882, pp. 213–225.
7. Wantzel, Pierre-Laurent. “Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas.” *Journal de Mathématiques Pures et Appliquées*, 1st ser., vol. 2, 1837, pp. 366–372.