Constructibility by Straightedge and Compass

Liam Moore

July 13, 2026

Abstract

This paper maps the physical constraints of an idealized straightedge and collapsing compass to linear and quadratic algebraic operations. By analyzing the intersections of lines and circles, we demonstrate that every elementary construction step generates a field extension over the rational numbers $\mathbb{Q}$ of degree at most 2. Using the multiplicativity of degrees via the Degree Formula, we prove that the coordinate field of any constructible number must reside within a tower of quadratic field extensions, implying its overall extension degree is a power of 2. Furthermore, we evaluate how irreducible and minimal polynomials help compute these degrees in practice, analyzing illustrative examples like $\sqrt{2}$ and $\sqrt{2+\sqrt{2}}$. Finally, we bridge these concepts into splitting fields and Galois groups to outline the necessary and sufficient criteria for constructibility, ultimately proving the impossibility of the three classical Problems of Antiquity, and concluding with an analysis of cyclotomic polynomials and the Gauss-Wantzel Theorem to determine the constructibility of regular n-gons.

Contents

1 Introduction

This paper serves primarily as a rigorous yet intuitive body of text that teaches Galois Theory and Field Theory through the motivating example of constructibility with a straightedge and compass, i.e., to discover everything that can be constructed with a straightedge and compass.

Straightedge and compass constructions are classic geometry problems that determine which lengths and shapes can be created using only an idealized ruler (a ruler without markings, i.e., a straightedge) and a compass. Since antiquity, mathematicians have inquired about geometric constructions using the aforementioned classic geometric tools. Ancient Greek mathematicians first utilized these tools as mathematical models of what could be *perfectly* drawn and constructed in plane geometry; although they solved several fundamental problems, such as: bisecting a line segment or angle, constructing equilateral triangles, drawing a line parallel to another line, and other notable achievements, they faced the three elusive Geometric Problems of Antiquity: doubling the cube (constructing a cube exactly twice the volume of a given cube), trisecting the angle (dividing an arbitrary angle into three equal parts), and squaring the circle (constructing a perfect square with the same area as a given circle). The answers to these problems waited for approximately two millennia until the Algebraic Revolution. During the 19th century, through developments in abstract algebra and field theory, mathematicians like Carl Friedrich Gauss and Pierre Wantzel made significant advancements in this field: Gauss proved the constructibility criterion for regular polygons (1796), particularly identifying when regular n-gons are constructible. Pierre Wantzel later proved (1837) the impossibility of the Geometric Problems of Antiquity, and established the general algebraic criterion for straightedge and compass constructibility.

There are three fundamental constructions with the straightedge and compass: finding the intersections of line-line, line-circle, and circle-circle systems. We examine the Algebra, Geometry, Field Theory, and Galois theory necessary to understand constructibility via straightedge and compass. First, we examine the straightedge and compass as linear and quadratic operations. Then, we propose the Degree Formula in order to examine the polynomials' towers of quadratic field extensions. Next, we define irreducible polynomials, Eisenstein's Criterion, and minimal polynomials in order to compute the degree of a polynomial's field. Next, we analyze splitting fields, Galois

groups, and the Fundamental Theorem of Galois Theory to determine the sufficient criteria for a polynomial to be constructed by an idealized straightedge and compass. Finally, we prove the impossibility of the Geometric Problems of Antiquity and define cyclotomic polynomials and the Gauss-Wantzel Theorem for a different perspective of geometric constructibility with the aforementioned tools.

2 Definitions

Definition 2.1. The straightedge is an infinitely long edge with no markings on it, and it can only be used to either draw a line segment between two points or to extend an existing line segment.

Definition 2.2. The compass can have an arbitrarily large radius with no markings on it. Circles and circular arcs can be drawn starting from two given points: the center and a point on the circle. The compass collapses, erasing its *stored* radius.

Remark. A collapsing compass would appear to have less functions; however, by the compass equivalence theorem in Proposition 2 of Book 1 of Euclid's Elements, no power is lost by using a collapsing compass [Euc56].

Assumption 2.3. Constructed line segments and circles have infinite precision and zero width.

3 Constructible Numbers from Compass and Straightedge

The constraints of the straightedge and compass (intersections of line-line, line-circle, and circle-circle systems) create a particular field of constructible numbers. Specifically, compasses and straightedges can perform addition, subtraction, multiplication, division, and square root operations, as illustrated in the following figures labeled (a) through (c), starting from the left and going right.

Image (a) illustrates how straightedge and compass constructions can perform multiplication.

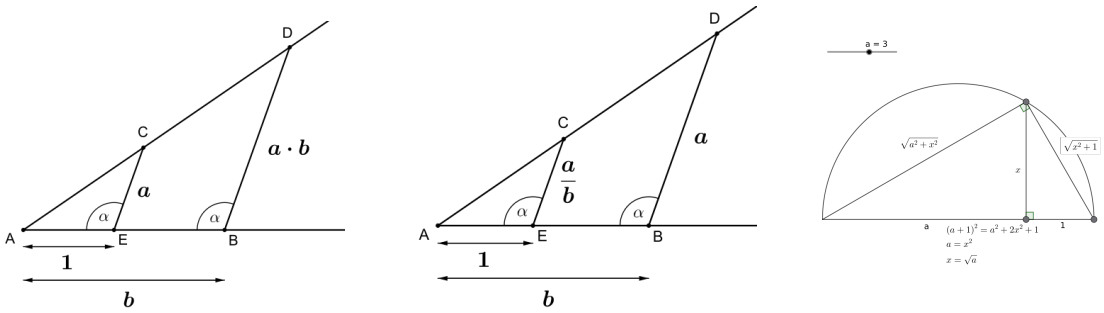
Theorem 3.1. *Intercept Theorem*

Proof Sketch. Constructing two similar triangles such that one side of the smaller triangle has length a and therefore, by similar triangles, the corresponding side of the larger triangle is a times the scaling factor b, i.e., ab. □

Similarly, image (b) depicts how a straightedge and compass can perform division by doing the process just mentioned, but in reverse.

Theorem 3.2. *Intercept Theorem*

Proof Sketch. The larger triangle has a side length of a and the smaller, similar triangle has a side length of a scaled down by a factor of b, therefore, $\frac{a}{b}$. □



(a) Multiplication (b) Division (c) Square Root

Figure 2: Straightedge and compass constructions for arithmetic operations: (a) multiplication, (b) division, and (c) square root.

The final image (c) proves how a straightedge and compass can perform the square root operation.

Theorem 3.3. *Geometric Mean Theorem*

Proof Sketch. Construct a right triangle with legs of length $\sqrt{a^2+x^2}$ and $\sqrt{x^2+1}$, a hypotenuse of length $a+1$ and a height of length x from the vertex between the two legs extended to hypotenuse. Therefore, the Pythagorean theorem gives

$$\begin{aligned}(a+1)^2 &= (\sqrt{a^2+x^2})^2 + (\sqrt{x^2+1})^2 \\ a &= x^2 \\ x &= \sqrt{a}\end{aligned}$$

□

Proposition 3.4. *Starting from a field F, every arithmetic construction obtainable by straightedge and compass produces numbers contained in a field obtained from F by adjoining finitely many square roots.*

3.1 The Compass and Straightedge as Linear and Quadratic Operations

We wish to create a "field" of the coordinates already constructed in a particular number system, and to do this, we first define a field:

Definition 3.5. (Milne, 2022) A field is a set F with binary operations $+$ and $\cdot$ such that:

1. $(F, +)$ is a commutative group;
2. $(F^\times, \cdot)$, where $F^\times \stackrel{\text{def}}{=} F \setminus \{0\}$, is a commutative group;
3. the distributive law holds.

Thus, a field is a nonzero commutative ring such that every nonzero element has an inverse. In particular, it is an integral domain. A field contains at least two distinct elements, 0 and 1. The smallest, and one of the most important, fields is $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. A subfield S of a field F is a subring that is closed under passage to the inverse. It inherits the structure of a field from that on F.

In other words, a field is a set F, containing at least two elements, in which the operations of addition and multiplication are defined so that for each pair of elements $x, y \in F$ there are unique elements $x+y$ and $x \cdot y$ in F for which the following conditions hold for all elements $x, y, z \in F$:

1. $x + y = y + x$ (commutativity of addition)
2. $(x + y) + z = x + (y + z)$ (associativity of addition)
3. There is an element $0 \in F$, called zero, such that $x + 0 = x$. (existence of an additive identity)
4. For each x, there is an element $-x \in F$ such that $x + (-x) = 0$. (existence of additive inverses)
5. $xy = yx$ (commutativity of multiplication)
6. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)
7. $(x + y) \cdot z = x \cdot z + y \cdot z$ and $x \cdot (y + z) = x \cdot y + x \cdot z$ (distributivity)
8. There is an element $1 \in F$, such that $1 \neq 0$ and $x \cdot 1 = x$. (existence of a multiplicative identity)
9. If $x \neq 0$, then there is an element $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. (existence of multiplicative inverses)

Example 3.6. (Murnaghan) Some examples of fields include the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. However, the set $\mathbb{Z}$ of integers is not a field, since in $\mathbb{Z}$, besides 1 and -1, the integers do not have multiplicative inverses. For example, 2 is a nonzero integer. If 2 had a multiplicative inverse in $\mathbb{Z}$, there would be an integer n such that $2n = 1$; however, the obvious solution of $n = \frac{1}{2}$ is not an integer, and in general it is impossible, since 1 is an odd integer, and not an even integer.

Now that we understand what a field is, let $F \subset \mathbb{R}$ be a subfield of the real numbers, representing the set of coordinates currently known or constructed. A point $P = (x, y) \in \mathbb{R}^2$ is defined to be constructible over F if its coordinates x and y can be obtained via a finite sequence of standard straightedge and compass operations. As stated previously, these operations can only be the following: the intersection of two lines, the intersection of a line and a circle, or the intersection of two circles. Now we explore each of the operations. Consequently, to understand constructible numbers, it suffices to determine the degree of these three intersections.

Line-Line Intersection

Let L_1 and L_2 be two intersecting lines defined by pairs of previously constructed points whose coordinates lie in F. The equations of these lines can be expressed as the following equations with coefficients in F:

$$L_1 : a_1x + b_1y = c_1, \quad a_1, b_1, c_1 \in F$$

$$L_2 : a_2x + b_2y = c_2, \quad a_2, b_2, c_2 \in F$$

The intersection point $P = (x_0, y_0)$ is determined by solving the linear system

Remark. Solving the linear system can be done via graphing, substitution, elimination, Cramer's Rule:

$$x_0 = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1}, \quad y_0 = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}$$

, or many other methods.

Because F is a field, it is closed under addition, subtraction, multiplication, and division by non-zero elements. Since $a_1b_2 - a_2b_1 \neq 0$, the coordinates x_0 and y_0 must belong to F. Thus, finding the intersection point of two straight lines whose slopes and intercepts are in our base field F always leads to a solution that is also in F. In the language of field theory, the intersection generates an extension field of degree 1 over the base field, which means we have not actually expanded our field of numbers at all. This motivates the formal definition of a field extension and the degree of a field:

Definition 3.7. A field extension is the adjoining of an element: if $F \subseteq K$, then K is an extension field of F. For example, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ If K is a field containing the subfield F, then K is said to be an extension field of F, denoted K/F. This notation can be read as "K over F."

Definition 3.8. The degree of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F.

A field extension of degree 1 can be written mathematically as the following:

$$[F(x_0, y_0) : F] = 1$$

Line-Circle Intersection

Let L be a line passing through points in F, and let C be a circle centered at a point (h, k) with a radius r, where $h, k, r^2 \in F$. The system of equations is given by:

$$L : y = mx + d, \quad m, d \in F$$

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

Substituting equation L into equation C gives:

$$(x - h)^2 + ((mx + d) - k)^2 = r^2$$

Regrouping the terms inside the second square to isolate x

$$(x - h)^2 + (mx + (d - k))^2 = r^2$$

Expanding both squared terms

$$(x^2 - 2hx + h^2) + \left[(mx)^2 + 2(mx)(d-k) + (d-k)^2\right] = r^2$$

$$x^2 - 2hx + h^2 + m^2x^2 + 2(md - mk)x + (d^2 - 2dk + k^2) = r^2$$

Subtracting r^2 from both sides to set to zero

$$x^2 + m^2x^2 - 2hx + 2mdx - 2mkx + h^2 + d^2 - 2dk + k^2 - r^2 = 0$$

Grouping coefficients by powers of x

$$(1 + m^2)x^2 + 2(md - h - mk)x + (h^2 + d^2 - 2dk + k^2 - r^2) = 0$$

If the discriminant of this quadratic equation $\Delta \geq 0$, the coordinates of the intersection points lie in the field extension $F(\sqrt{\Delta})$, so the degree of this field extension is at most 2:

$$[F(\sqrt{\Delta}) : F] \leq 2$$

Circle-Circle Intersection

Let C_1 and C_2 be two distinct, intersecting circles centered at coordinates in F with radii whose squares are in F:

$$C_1 : x^2 + y^2 + D_1x + E_1y + F_1 = 0, \quad D_1, E_1, F_1 \in F$$

$$C_2 : x^2 + y^2 + D_2x + E_2y + F_2 = 0, \quad D_2, E_2, F_2 \in F$$

Subtracting the equation of C_2 from C_1 eliminates the quadratic terms x^2 and y^2, yielding the equation:

$$(D_1 - D_2)x + (E_1 - E_2)y + (F_1 - F_2) = 0 \tag{1}$$

Because $D_i, E_i, F_i \in F$, the coefficients of (1) lie within F, the intersection points of C_1 and C_2 are also the intersection points of the circle C_1 and (1). This makes the circle-circle intersection case equivalent to the line-circle intersection case. Therefore, the coordinates of the intersection points lie within a quadratic extension $F(\sqrt{\Delta})$, where $\Delta \in F$:

$$[F(x_0, y_0) : F] \in \{1, 2\}$$

Theorem 3.9. ***Geometric Construction Theorem*** *Every elementary construction step produces an extension of degree at most* 2

Proof. By the previous three subsections, the three cases of line-line intersection, line-circle intersection, and circle-circle intersection gave degree 1, at most 2, and again at most 2, respectively. And hence, all of the cases have been exhausted and shown to produce a field extension of degree either 1 or 2 □

Theorem 3.10. ***Field of Constructible Numbers Theorem.*** *(Rotman, 1998) The set of all constructible numbers forms a subfield of* $\mathbb{R}$ *that is closed under taking square roots of positive elements.*

Proof. The previous sections established that straightedge and compass constructions can perform addition, subtraction, multiplication, division by nonzero elements, and square root operations.

Suppose a and b are constructible numbers. Since addition and subtraction can be carried out geometrically, both $a + b$ and $a - b$ are constructible. Likewise, the multiplication and division constructions show that ab and $\frac{a}{b}$ (provided $b \neq 0$) are constructible.

Furthermore, the geometric mean construction proves that whenever $a > 0$ is constructible, the number $\sqrt{a}$ is also constructible.

Therefore, the constructible numbers are closed under the field operations together with taking square roots of positive elements. Hence they form a subfield of $\mathbb{R}$ that is closed under square roots. □

3.2 Towers of Quadratic Field Extensions and a Degree Condition for Constructibility

The sequence of drawing new lines and circles, moving from the rational numbers $\mathbb{Q}$ to a final coordinate field E creates a tower of intermediate fields:

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = E$$

If every individual step in this construction is a single quadratic extension, then by definition $[F_i : F_{i-1}] = 2$. And, we can sequentially apply the following theorem (the Degree Formula 3.2) to show that the total degree of the top field E over $\mathbb{Q}$ is the product of the degrees of these individual steps:

$$[E : \mathbb{Q}] = [F_n : F_{n-1}] \times [F_{n-1} : F_{n-2}] \times \cdots \times [F_1 : F_0]$$

Since there are exactly n steps, each with a degree of 2, the product becomes:

$$[E : \mathbb{Q}] = 2 \times 2 \times \cdots \times 2 = 2^m, m \leq n$$

To prove the Degree Formula we present a couple of definitions and lemmas. Specifically, the following definitions and lemmas allow us to compute the degree of the total construction field and since field extensions are vector spaces, the degree of an extension equals its dimension. Ultimately, the lemmas allow us to prove the multiplicativity of degrees.

Lemma 3.11. *(Axler, 2024) A list $v_1, \ldots, v_m$ of vectors in V is called linearly independent if the only choice of $a_1, \ldots, a_m \in \mathbf{F}$ that makes*

$$a_1 v_1 + \cdots + a_m v_m = 0$$

is

$$a_1 = \cdots = a_m = 0$$

Example 3.12. (Axler, 2024) Take for example the list $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$. It is linearly independent in $\mathbf{F}^4$, suppose

$$a_1, a_2, a_3 \in \mathbf{F}$$

and

$$a_1(1,0,0,0) + a_2(0,1,0,0) + a_3(0,0,1,0) = (0,0,0,0)$$

Thus

$$(a_1, a_2, a_3, 0) = (0,0,0,0)$$

Definition 3.13. (Axler, 2024) The set of all linear combinations of a list of vectors $v_1, \ldots, v_m$ in V is called the span of $v_1, \ldots, v_m$, denoted by $\text{span}(v_1, \ldots, v_m)$. In other words,

$$\text{span}(v_1, \ldots, v_m) = \{a_1 v_1 + \cdots + a_m v_m : a_1, \ldots, a_m \in \mathbf{F}\}$$

Example 3.14. (Axler, 2024) $(17, -4, 2) \in \text{span}((2,1,-3),(1,-2,4))$

Example 3.15. (Axler, 2024) $(17, -4, 5) \notin \text{span}((2,1,-3),(1,-2,4))$

Definition 3.16. (Axler, 2024) A basis of V is a list of vectors in V that is linearly independent and spans V

Example 3.17. (Axler, 2024) The list $(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)$ is a basis of $\mathbf{F}^n$, called the standard basis of $\mathbf{F}^n$.

Example 3.18. (Axler, 2024) The list $(1,2,-4),(7,-5,6)$ is linearly independent in $\mathbf{F}^3$ but is not a basis of $\mathbf{F}^3$ because it does not span $\mathbf{F}^3$.

Theorem 3.19. *(Rotman, 1998)* ***Degree Formula*** *If $F \subseteq B \subseteq E$ are fields with $[E:B]$ and $[B:F]$ finite, then E/F is finite and $[E:F] = [E:B][B:F]$.*

Proof. Let $\{a_1, \ldots, a_m\}$ be a basis of E/B, and let $\{\beta_1, \ldots, \beta_n\}$ be a basis of B/F. It suffices to prove that $\{\beta_j a_i \mid 1 \le i \le m, 1 \le j \le n\}$ is a basis of E/F.

This set spans E. If $y \in E$, then there are $b_i \in B$ with $y = \sum b_i a_i$. But each $b_i = \sum c_{ij}\beta_j$ for $c_{ij} \in F$; hence $y = \sum c_{ij}\beta_j a_i$.

To see that this set is linearly independent, assume that $\sum c_{ij}\beta_j a_i = 0$ for $c_{ij} \in F$. Now $b_i = \sum c_{ij}\beta_j \in B$, so that the independence of the a_i over B implies that $b_i = 0$ for all i. Hence $\sum c_{ij}\beta_j = 0$ for all i, and so the independence of the β_j over F implies that $c_{ij} = 0$ for all i, j, as desired. □

Corollary 3.20. *If*

$$Q = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$$

is a tower of quadratic extensions, then

$$[F_n : Q] = 2^n$$

At last, we can now prove the following theorem about the degree extension of a constructible number.

Theorem 3.21. *The Geometric Constructibility Extension Theorem. The total degree of the extension containing any constructible number α over the rational numbers must be a power of 2*

Proof. By the Geometric Construction Theorem 3.1, since we can only solve equations of degree 1 or 2 with the straightedge and compass, every step of a geometric construction gives a field extension of degree 1 or 2; and, using the Degree Formula 3.2, k geometric operations starting from $\mathbb{Q}$ generates a tower of fields; and therefore, the total degree of the extension containing any constructible number α over the rational numbers must be a power of 2:

$$[E : \mathbb{Q}] = \prod_{i=1}^{k} [F_i : F_{i-1}] = 2^m \quad (m \leq k)$$

□

Theorem 3.22. ***Quadratic Tower Characterization of Constructibility.*** *(Rotman, 1998) A real number α is constructible by straightedge and compass if and only if there exists a tower of fields*

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

such that

$$\alpha \in F_n$$

and

$$[F_i : F_{i-1}] \leq 2$$

for every i.

Proof. Suppose first that α is constructible. Every elementary straightedge and compass construction is one of three possible operations: the intersection of two lines, the intersection of a line and a circle, or the intersection of two circles. By the Geometric Construction Theorem, each construction step enlarges the current field by an extension of degree either 1 or 2. Repeating this process produces a sequence of intermediate fields

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

whose final field contains α, and every extension satisfies

$$[F_i : F_{i-1}] \leq 2.$$

Conversely, suppose there exists such a tower of fields. If

$$[F_i : F_{i-1}] = 1,$$

then no new numbers are introduced. If

$$[F_i : F_{i-1}] = 2,$$

then the extension is obtained by adjoining the solution of a quadratic equation whose coefficients lie in the previous field. Solving a quadratic equation requires only the arithmetic operations together with the extraction of a square root, all of which

can be carried out by straightedge and compass constructions established earlier in this section. Therefore every field in the tower can be constructed successively, and consequently the final element α is constructible.

Hence a real number is constructible if and only if it belongs to a tower of quadratic field extensions. □

3.3 Extension Degrees via Minimal Polynomials

The previous section gives a criterion for constructibility, namely that the degree of the field generated by a constructible number must be a power of two. However, this criterion is only useful if we have a method for computing the degree of the field; and, instead of constructing the field, there is a simpler tool: the minimal polynomial. We first define a monic polynomial, an irreducible polynomial, a criterion to determine if a polynomial is irreducible; then, we ultimately define that the degree of the minimal polynomial of a number is exactly the degree of the field extension it generates.

Definition 3.23. (Belk) A polynomial is monic if its leading coefficient is equal to one

Definition 3.24. (Belk) Let F be a field, and let $f(x)$ be a monic polynomial over F with $\deg(f) \geq 1$. We say that $f(x)$ is irreducible if the only monic divisors of $f(x)$ are 1 and $f(x)$.

Example 3.25. (Belk) The only irreducible polynomials over $\mathbb{C}$ are the monic linear polynomials $\{x-a \mid a \in \mathbb{C}\}$. By the fundamental theorem of algebra, every monic polynomial over $\mathbb{C}$ can be expressed as a product of these irreducible polynomials.Over $\mathbb{R}$, irreducible polynomials include all monic linear polynomials and quadratic polynomials $x^2 + bx + c$ with a negative discriminant ($b^2 - 4c < 0$), such as $x^2 + 1$.

Remark. There are a variety of methods to quickly determine if a polynomial is irreducible, such as the Rational Root Theorem or Eisenstein's Criterion. We now present Eisenstein's Criterion

Theorem 3.26. *(Russell, 2009) Eisenstein's Criterion. Let R be a unique factorization domain. Suppose $0 \neq f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ is a monic polynomial in $R[X]$, and $p \in R$ is a prime such that $p \mid a_{n-1}, \ldots, a_0$ but $p^2 \nmid a_0$. Then $f(X)$ is irreducible.*

Proof. (Russell, 2009) Suppose not, so $f(X) = (X^r + b_{r-1}X^{r-1} + \cdots + b_0)(X^s + c_{s-1}X^{s-1} + \cdots + c_0)$ with $0 < r, s < n$. Take i least such that $p \nmid b_i$ (where we allow the case $i = r$ and $b_r = 1$), and j least such that $p \nmid c_j$ (where we allow the case $j = s$ and $c_s = 1$). Now the $(i + j)$-th coefficient a_{i+j} of the product is $a_{i+j} = b_i c_j + (b_{i-1}c_{j+1} + \dots) + (b_{i+1}c_{j-1} + \dots)$ and so is a sum of $b_i c_j$ and terms divisible by p. As $p \nmid b_i c_j$, $p \nmid a_{i+j}$. But $p^2 \nmid a_0 = b_0 c_0$ and so p cannot divide both b_0 and c_0, and so either $i = 0$ or $j = 0$ and so $i + j < n$. So we contradict $p \mid a_{i+j}$ □

Definition 3.27. Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$, which has α as a root. Furthermore, a polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$. The polynomial $m_{\alpha,F}(x)$ is called the minimal polynomial for α over F. The degree of $m_{\alpha,F}(x)$ is called the degree of α and can be denoted

$$\deg(m_{\alpha,F}) = [F(\alpha) : F]$$

.

Corollary 3.28. *If the minimal polynomial of α does not have degree equal to a power of 2, then α is not constructible.*

4 Examples of Constructible and Nonconstructible Numbers

To help the reader understand how field extensions and degree conditions govern straightedge and compass constructibility, we analyze two examples. Recall that a number α is constructible if and only if it lies within a tower of quadratic extensions over $\mathbb{Q}$, which implies that the degree of its minimal polynomial must be a power of 2.

4.1 The Square Root of Two: $\sqrt{2}$

We begin with the following example: $\alpha = \sqrt{2}$. To find its minimal polynomial over $\mathbb{Q}$, we set $x = \sqrt{2}$ and square both sides to clear the radical:

$$x^2 - 2 = 0$$

Let $f(x) = x^2 - 2$. By Eisenstein's Criterion applied at the prime $p = 2$, $f(x)$ is irreducible over $\mathbb{Q}[x]$. Because $f(x)$ is monic and irreducible, it is the minimal polynomial $m_{\sqrt{2},\mathbb{Q}}(x)$.

The degree of the extension is given by:

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(m_{\sqrt{2},\mathbb{Q}}(x)) = 2 = 2^1$$

Since the extension degree is a power of 2, $\sqrt{2}$ satisfies the necessary degree condition. Thus, $\sqrt{2}$ is constructible.

Remark. Geometrically, $\alpha = \sqrt{2}$ is easily constructed as the hypotenuse of a right isosceles triangle with leg lengths of 1.

4.2 A Nested Radical: $\sqrt{2+\sqrt{2}}$

Next, consider the nested radical $\alpha = \sqrt{2+\sqrt{2}}$. We find its minimal polynomial by solving for when it equals 0:

$$\begin{aligned} x &= \sqrt{2+\sqrt{2}} \\ x^2 &= 2+\sqrt{2} \\ x^2 - 2 &= \sqrt{2} \\ (x^2-2)^2 &= 2 \\ x^4 - 4x^2 + 2 &= 0 \end{aligned}$$

Let $f(x) = x^4 - 4x^2 + 2$. Applying Eisenstein's Criterion at $p = 2$, we see that $2 \mid -4$, $2 \mid 2$, but $2^2 \nmid 2$. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$, making it the minimal polynomial for α.

The degree of this extension is:

$$[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}] = \deg(f(x)) = 4 = 2^2$$

Since 4 is a power of 2, this number can be broken down into a tower of quadratic extensions by the Degree Formula 3.2:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$$

Each step in the tower is a field extension of degree 2 because $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is obtained by taking the square root of $(2+\sqrt{2})$ already contained in the base field $\mathbb{Q}(\sqrt{2})$, $\sqrt{2+\sqrt{2}}$ is constructible.

4.3 Insufficient Criterion

The Geometric Constructibility Extension Theorem (3.2) proves that every constructible number generates an extension whose degree is a power of two. However, the converse is suprisingly not true. And hence, we now present an example of why the Geometric Constructibility Extension Theorem is not sufficient to determine if a number is constructible.

Example 4.1. Consider the polynomial

$$f(x) = x^4 - x - 1$$

It is irreducible over $\mathbb{Q}$, so for any root α,

$$\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = 2^2$$

Thus, the degree condition is satisfied. However, none of the roots of $f(x)$ are constructible by straightedge and compass since the degree of the extension alone is unable to distinguish this polynomial from a constructible quartic extension such as

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

.

Thus, although the Geometric Constructibility Extension Theorem is valid, it has been proven to be an insufficient condition in determining if a number is constructible. Meaning that if a number satisfies the Geometric Constructibility Extension Theorem, it is not necessarily constructible; however the converse is true, if a number is constructible, it satisfies Geometric Constructibility Extension Theorem. We will now investigate the other criterion besides the Geometric Constructibility Extension Theorem to determine the criteria for a number to be constructible.

5 Galois Theory for Constructibility

The Geometric Constructibility Extension Theorem established that every constructible number generates a field extension whose degree is a power of 2. However, as demon-

strated by the polynomial

$$x^4 - x - 1,$$

this condition alone is not sufficient to determine constructibility. Although adjoining one of its roots produces a field extension of degree 4, none of its roots are constructible by straightedge and compass.

To determine whether an algebraic number is constructible, we require additional information beyond the degree of a field extension; and, instead of studying only one root of a polynomial, Galois Theory studies all of its roots simultaneously together with the algebraic symmetries between them. And at last, this additional theory provides the missing criterion for constructibility.

We begin by introducing splitting fields; then, we define Galois groups; finally, we state the Fundamental Theorem of Galois Theory, which relates the symmetries of a polynomial's roots to intermediate field extensions and ultimately explains why extension degree alone is not sufficient to determine constructibility.

5.1 Splitting Fields

When adjoining a single root of an irreducible polynomial to a base field, the polynomial's other roots are not necessarily included.

Definition 5.1. (Rotman, 1998) A splitting field of $f(x) \in F[x]$ is a field extension E/F in which $f(x)$ splits (it is a product of linear factors) while $f(x)$ does not split in any proper subfield of E.

Essentially, for a polynomial $f(x)$ of degree $d = \deg(f)$, an extension field E of F is a splitting field for $f(x)$ over F if $f(x)$ factors completely into linear factors over $E[x]$, i.e.,

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

where $c \in F$ and $\alpha_i \in E$, and E is generated over F by the roots of $f(x)$, i.e.,

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$

To study the symmetries of a polynomial, every root must lie in the same field; and, if a field contains only a subset of the roots, then not every algebraic transformation between the roots can be described. Splitting fields provide the smallest extension field in which every root is simultaneously present.

Consider the irreducible polynomial

$$f(x) = x^3 - 2$$

over $\mathbb{Q}$. The three distinct complex roots of this polynomial are

$$\alpha_1 = \sqrt[3]{2}, \qquad \alpha_2 = \sqrt[3]{2}\omega, \qquad \alpha_3 = \sqrt[3]{2}\omega^2,$$

where

$$\omega = e^{\frac{2\pi i}{3}} = \frac{-1 + i\sqrt{3}}{2}$$

is a primitive cube root of unity.

If we adjoin only the real root α_1 to our base field, we produce the extension

$$F_1 = \mathbb{Q}(\sqrt[3]{2}).$$

Notice that

$$F_1 \subset \mathbb{R}.$$

Because α_2 and α_3 contain nonzero imaginary parts, they do not belong to F_1. Thus,

$$F_1$$

is not a splitting field for $x^3 - 2$. To obtain the splitting field, we must adjoin the remaining roots, giving

$$E = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

Here,

$$[E : \mathbb{Q}] = 6,$$

whereas

$$[F_1 : \mathbb{Q}] = 3.$$

Although $\mathbb{Q}(\sqrt[3]{2})$ contains one solution of $x^3 - 2$, it does not contain enough information to describe the complete algebraic structure of the polynomial; and hence, the splitting field is necessary.

5.2 Galois Groups

The splitting field contains every root of a polynomial; however, to determine whether a polynomial can be solved through successive quadratic extensions, we must study how these roots are related, which is accomplished through *automorphisms* of the splitting field. The author will briefly define an *isomorphism* and *automorphism.*

Definition 5.2 (other textbook not rotman)**.** A group isomorphism is a group morphism that is a bijection. Then, automatically, the inverse bijection is also a group morphism.

Example 5.3. The map $\phi : \mathbb{Z} \to n\mathbb{Z}$ defined by $\phi(m) = nm$ is a group isomorphism.

Definition 5.4. (Rotman, 1998) If E is a field, then an automorphism of E is an isomorphism of E with itself. If E/F is a field extension, then an automorphism σ of E fixes F pointwise if $\sigma(c) = c$ for every $c \in F$.

Essentially, an automorphism is a transformation of a field that preserves both addition and multiplication. Therefore, every algebraic relation satisfied before the transformation must remain satisfied afterward; and since the coefficients of the polynomial remain fixed, automorphisms cannot send a root to an arbitrary element; instead, they can only permute the roots of the polynomial among themselves. In other words, an automorphism is a bijective mapping onto itself that preserves all operations. We will now prove the latter statement.

Theorem 5.5. *(Rotman, 1998) Let $f(x) \in F[x]$ and let E/F be an extension field of F. If $\sigma : E \to E$ is an automorphism fixing F pointwise, and if $a \in E$ is a root of $f(x)$, then $\sigma(a)$ is also a root of $f(x)$.*

Proof. Let $f(x) = c_0 + c_1x + \cdots + c_nx^n$, so that $c_0 + c_1a + \cdots + c_na^n = 0$. Applying σ gives

$$\begin{aligned}\sigma(c_0) + \sigma(c_1)\sigma(a) + \cdots + \sigma(c_n)\sigma(a)^n &= c_0 + c_1\sigma(a) + \cdots + c_n\sigma(a)^n \\ &= 0\end{aligned}$$

because σ fixes F. Therefore, $\sigma(a)$ is a root of $f(x)$. □

The previous theorem shows that every automorphism fixing the base field must send roots of a polynomial to other roots of the same polynomial.

Definition 5.6. (Rotman, 1998) Let E/F be a field extension. Its Galois group is

$$\mathrm{Gal}(E/F) = \{\text{automorphisms } \sigma \text{ of } E \text{ fixing } F \text{ pointwise}\}$$

under the binary operation of composition. If $f(x) \in F[x]$ has splitting field E, then the Galois group of $f(x)$ is $\mathrm{Gal}(E/F)$. It is easy to check that $\mathrm{Gal}(E/F)$ is a group; it is a subgroup of the group of all automorphisms of E.

The elements of $\mathrm{Gal}(E/F)$ act as permutations of the roots. Because every automorphism fixes the coefficients of a polynomial in $F[x]$, it can only permute roots having the same algebraic properties.

Consider the polynomial

$$f(x) = x^2 - 2$$

over $\mathbb{Q}$. Its roots are

$$\pm\sqrt{2},$$

and its splitting field is

$$E = \mathbb{Q}(\sqrt{2}).$$

Every element of E can be written uniquely in the form

$$a + b\sqrt{2}, \qquad a, b \in \mathbb{Q}.$$

The Galois group

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$$

contains exactly two automorphisms:

the identity automorphism,

$$\iota(\sqrt{2}) = \sqrt{2}.$$

and the conjugation automorphism,

$$\sigma(\sqrt{2}) = -\sqrt{2}.$$

and no other automorphisms are possible, so once the image of $\sqrt{2}$ is chosen, every element of the field is determined. Therefore,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2.$$

Next, return to the splitting field of

$$f(x) = x^3 - 2,$$

namely,

$$E = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

Since every automorphism fixing $\mathbb{Q}$ must permute the three distinct roots

$$\left\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\right\},$$

there are at most

$$3! = 6$$

possible automorphisms; and in this case, all six permutations are algebraically valid. Therefore,

$$\mathrm{Gal}(E/\mathbb{Q}) \cong S_3,$$

the symmetric group on three elements.

An important distinction between these two polynomials can be noticed: although both polynomials are irreducible, the quadratic polynomial has only two algebraic symmetries, whereas the cubic polynomial has six; and, it is these symmetries, instead of the extension degree alone, that ultimately determine whether a polynomial can be constructed using only a straightedge and compass.

5.3 The Fundamental Theorem of Galois Theory

> *"Given a Galois extension E/F, the fundamental theorem will show a strong connection between the subgroups of* $\mathrm{Gal}(E/F)$ *and the intermediate fields between F and E."*
> — Rotman

In other words, Rotman is explaining how the Fundamental Theorem of Galois Theory connects splitting fields and Galois Groups by establishing a correspondence between subgroups of the Galois group and intermediate fields of the splitting field.

As a consequence, field extensions can be *translated* into groups, and vice versa. And, this allows Galois Theory to determine whether a field extension can be decomposed into a sequence of quadratic extensions; and hence, whether a polynomial can be constructed with only a straightedge and compass.

Theorem 5.7 (Fundamental Theorem of Galois Theory)**.** *Let E/F be a Galois extension with Galois group*

$$G = \mathrm{Gal}(E/F).$$

(i) The function

$$\gamma : \mathrm{Sub}(G) \to \mathrm{Lat}(E/F),$$

defined by

$$H \mapsto E^H,$$

is an order reversing bijection with inverse

$$\beta : B \mapsto \mathrm{Gal}(E/B).$$

(ii)

$$E^{\mathrm{Gal}(E/B)} = B$$

and

$$\mathrm{Gal}(E/E^H) = H.$$

(iii)

$$E^{H\vee K} = E^H \cap E^K, \qquad E^{H\wedge K} = E^H \vee E^K,$$
$$\mathrm{Gal}(E/B \vee C) = \mathrm{Gal}(E/B) \cap \mathrm{Gal}(E/C), \quad \mathrm{Gal}(E/B \wedge C) = \mathrm{Gal}(E/B) \vee \mathrm{Gal}(E/C).$$

(iv)

$$[B : F] = [G : \mathrm{Gal}(E/B)]$$

and

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

(v) B/F is a Galois extension if and only if $\mathrm{Gal}(E/B)$ is a normal subgroup of G.

Remark. The complete proof of the Fundamental Theorem of Galois Theory is beyond the scope of this paper and may be found in [Rot98]. For the purposes of constructibility, the necessary condition is the correspondence between intermediate fields and subgroups of the Galois group.

In particular, larger intermediate fields correspond to smaller subgroups, while smaller intermediate fields correspond to larger subgroups; consequently, studying the subgroup structure of a Galois group is equivalent to studying the possible intermediate field extensions.

And since straightedge and compass constructions produce towers of quadratic field extensions, the subgroup structure of the Galois group determines if such a tower can exist.

Remark. The correspondence reverses inclusion; so, if an intermediate field contains more elements, then an automorphism must fix more elements in order to belong to the corresponding subgroup. Hence, fewer automorphisms satisfy this condition, producing a smaller subgroup. And conversely, smaller intermediate fields have less restrictions and therefore correspond to larger subgroups. Figure 5.3 illustrates this inclusion reversing correspondence.

5.4 The Necessary Criteria: Why Degree 2^k Alone Is Not Sufficient

While it is true that a constructible number α must satisfy $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ (Theorem 3.2, a field extension whose total degree is a power of 2 is not automatically guaranteed to be constructible.

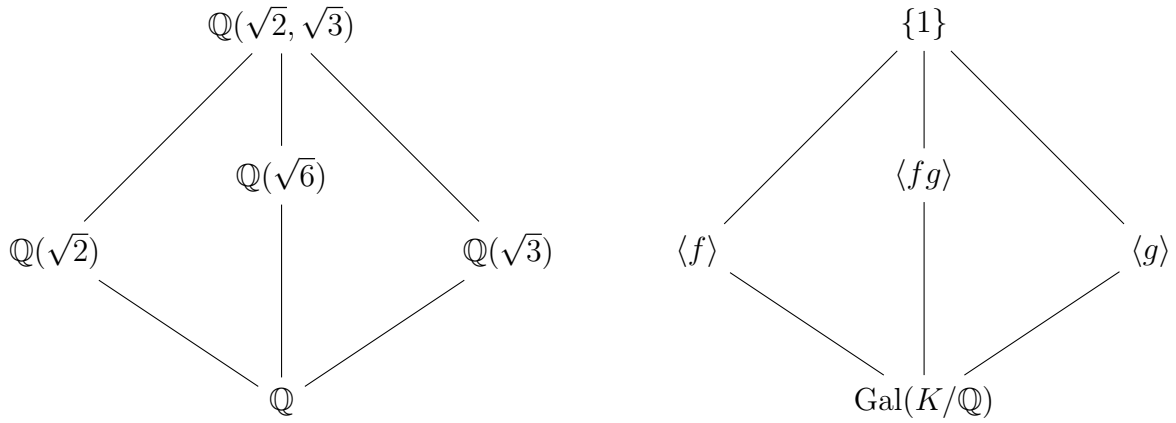


Figure 3: Lattice of subfields of $K/\mathbb{Q}$ (left) and the inverted lattice of subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ (right). Source: Wikipedia, *Fundamental theorem of Galois theory.*

For a number to be constructible, it cannot just live inside an extension of degree 2^n (as illustrated in example 4.1); rather, through the Fundamental Theorem of Galois Theory, the Galois group of its Galois closure over $\mathbb{Q}$ must be a 2-group (a finite group whose order is a power of 2).

If the Galois group of the splitting field contains any non-quadratic factors (such as 3-cycles or simple groups not of order 2^k), the extension cannot be broken down into a series of square root steps, making the length impossible to construct with a straightedge and compass.

Consider again the polynomial $f(x) = x^4 - x - 1$ over $\mathbb{Q}$. This polynomial is irreducible, and let α be one of its roots. Because the polynomial has a degree of 4, the simple extension field has a degree of:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = 2^2$$

. If degree alone were sufficient, α should be constructible. However, if we look at the splitting field (or Galois closure) E of this polynomial, its Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to S_4. The order of S_4 is $4! = 24$. Because 24 is not a power of 2, S_4 is not a 2-group. By the Fundamental Theorem of Galois Theory, because $|S_4| = 24 = 2^3 \cdot 3$, there exists a subgroup of index 3, corresponding to an intermediate field of degree 3 over $\mathbb{Q}$. Since straightedge and compass constructions can only produce towers of linear or quadratic extensions, a cubic step cannot occur.

Theorem 5.8. ***Idealized Straightedge and Compass Constructibility*** *A number is constructible with an idealized straightedge and compass if and only if the Galois group of its Galois closure over $\mathbb{Q}$ is a finite 2-group*

Proof. Suppose first that α is constructible. By the Geometric Constructibility Extension Theorem (3.2), there exists a tower of fields

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$$

such that $\alpha \in F_n$ and

$$[F_{i+1} : F_i] = 2$$

for every i.

Let E denote the Galois closure of F_n over $\mathbb{Q}$. Since E contains every conjugate of every element of F_n, it is a finite Galois extension of $\mathbb{Q}$, and

$$G = \mathrm{Gal}(E/\mathbb{Q})$$

is well defined.

Because each extension F_{i+1}/F_i is quadratic, adjoining all conjugates produces a corresponding tower of Galois closures

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E,$$

where each extension E_{i+1}/E_i has degree a power of 2. Consequently,

$$[E : \mathbb{Q}] = \prod_{i=0}^{n-1} [E_{i+1} : E_i]$$

is itself a power of 2. Since

$$|G| = [E : \mathbb{Q}],$$

the Galois group G has order equal to a power of 2, and therefore G is a finite 2-group.

Conversely, suppose

$$G = \mathrm{Gal}(E/\mathbb{Q})$$

is a finite 2-group, where E is the Galois closure of $\mathbb{Q}(\alpha)$.

Every finite 2-group possesses a normal series

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\},$$

whose successive quotients satisfy

$$|G_i : G_{i+1}| = 2.$$

By the Fundamental Theorem of Galois Theory, this normal series corresponds to a tower of intermediate fields

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = E,$$

with

$$[K_{i+1} : K_i] = 2$$

for every i.

Since $\alpha \in E$, it belongs to a tower of quadratic extensions over $\mathbb{Q}$. Therefore, by the Geometric Constructibility Extension Theorem (3.2), α is constructible with an idealized straightedge and compass. □

6 Applications

The previous sections developed the theorem necessary (5.8) for straightedge and compass constructibility, and we now apply these results to the Geometric Problems of Antiquity mentioned in the Introduction (1).

6.1 The Delian Problem

The Delian Problem asks whether it is possible to construct the edge of a cube having twice the volume of a given cube using only a straightedge and compass.

Suppose the given cube has side length 1. If the desired cube has side length x, then

$$x^3 = 2.$$

Hence the required length is

$$x = \sqrt[3]{2}.$$

The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is

$$f(x) = x^3 - 2.$$

By Eisenstein's Criterion with the prime 2, this polynomial is irreducible over $\mathbb{Q}$. Therefore,

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

Since 3 is not a power of 2, Theorem 3.2 implies that $\sqrt[3]{2}$ is not constructible. Therefore, doubling the cube is impossible with a straightedge and compass.

6.2 Angle Trisection

The problem of angle trisection asks whether an arbitrary angle can be divided into three equal angles using only a straightedge and compass.

It is sufficient to consider the angle 60°. If this angle were trisectable, then 20° would be constructible.

Using the triple-angle identity,

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta,$$

and setting $\theta = 20°$ gives

$$4\cos^3(20°) - 3\cos(20°) = \frac{1}{2}.$$

Let

$$x = \cos(20°).$$

Then

$$8x^3 - 6x - 1 = 0.$$

The polynomial

$$f(x) = 8x^3 - 6x - 1$$

is irreducible over $\mathbb{Q}$, so

$$[\mathbb{Q}(x) : \mathbb{Q}] = 3.$$

Again, the degree is not a power of 2. Therefore $\cos(20^\circ)$ is not constructible, implying that a 60° angle cannot be trisected with a straightedge and compass. Hence angle trisection is impossible in general.

6.3 Squaring the Circle

Squaring the circle asks whether a square can be constructed having the same area as a given circle.

Assume the circle has radius 1. Its area is

$$\pi.$$

If the square has side length s, then

$$s^2 = \pi,$$

so

$$s = \sqrt{\pi}.$$

Therefore, squaring the circle is equivalent to constructing $\sqrt{\pi}$.

However, Lindemann proved that π is transcendental [vL82]. Consequently, $\sqrt{\pi}$ is also transcendental, since otherwise $\pi = (\sqrt{\pi})^2$ would be algebraic.

Every constructible number is algebraic. Therefore $\sqrt{\pi}$ is not constructible, and squaring the circle is impossible with a straightedge and compass.

7 Cyclotomic Fields and Regular Polygons

The previous sections developed the algebraic criterion for straightedge and compass constructibility by combining field extensions, minimal polynomials, and Galois Theory. We now apply these results to one of the oldest problems in classical geometry: determining exactly which regular polygons can be constructed with an idealized straightedge and compass.

The key algebraic objects are the *cyclotomic polynomials*, whose roots are the complex roots of unity. These polynomials generate field extensions whose Galois groups possess a particular structure that allows Galois Theory to determine when a regular polygon is constructible.

Throughout this section, we first introduce cyclotomic polynomials and their basic algebraic properties. We then examine the Galois groups of cyclotomic fields before stating the Gauss–Wantzel Theorem, which classifies the constructible regular polygons.

7.1 Cyclotomic Polynomials

The vertices of a regular n-gon inscribed in the unit circle are naturally described using the complex roots of unity. Consequently, before studying constructible polygons, we first introduce the polynomial whose roots are precisely these numbers.

Definition 7.1. (Rotman, 1998) Let n be a positive integer. A complex number ζ_n is called a *primitive nth root of unity* if

$$\zeta_n^n = 1$$

and no smaller positive power of ζ_n equals 1. The nth cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - \zeta_n^k\right).$$

Equivalently, $\Phi_n(x)$ is the unique monic polynomial whose roots are exactly the primitive nth roots of unity.

Every root is obtained from a single primitive root of unity by raising it to an exponent relatively prime to n.

For example, when $n = 5$, the primitive fifth roots of unity are

$$\zeta_5,\ \zeta_5^2,\ \zeta_5^3,\ \zeta_5^4,$$

where

$$\zeta_5 = e^{2\pi i/5}.$$

Consequently,

$$\Phi_5(x) = (x - \zeta_5)(x - \zeta_5^2)(x - \zeta_5^3)(x - \zeta_5^4),$$

which expands to

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

More generally, when p is prime, every nontrivial pth root of unity is primitive. Therefore the pth cyclotomic polynomial has the particularly simple form

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

The importance of cyclotomic polynomials comes from the fact that they are irreducible over the rational numbers.

Theorem 7.2 (Irreducibility of Prime Cyclotomic Polynomials (Rotman, 1998))**.** *Let p be prime. Then*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

Proof Sketch. A direct application of Eisenstein's Criterion is not possible because none of the coefficients of $\Phi_p(x)$ are divisible by p. Instead, substitute $x+1$ for x to obtain the translated polynomial

$$\Phi_p(x+1).$$

Using the Binomial Theorem, every coefficient except the leading coefficient is divisible by p, while the constant term is divisible by p but not by p^2. Thus the translated polynomial satisfies the hypotheses of Eisenstein's Criterion with the prime p and is therefore irreducible over $\mathbb{Q}$. Since translating a polynomial does not affect irreducibility, the original cyclotomic polynomial $\Phi_p(x)$ is also irreducible. □

This theorem immediately determines the degree of the field generated by a primitive root of unity. If ζ_p denotes a primitive pth root of unity, then ζ_p satisfies the irreducible polynomial $\Phi_p(x)$. Consequently, the minimal polynomial of ζ_p over $\mathbb{Q}$ is $\Phi_p(x)$.

Corollary 7.3. *If p is prime and ζ_p is a primitive pth root of unity, then*

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(\Phi_p(x)) = p - 1.$$

The field

$$\mathbb{Q}(\zeta_p)$$

contains every root of $\Phi_p(x)$, making it the splitting field of the polynomial over $\mathbb{Q}$. Because all primitive roots of unity lie in the same field, we can now study the algebraic symmetries between them through their automorphisms. As in the previous chapter, these automorphisms form the Galois group of the field extension, and their structure ultimately determines whether the corresponding regular polygon is constructible.

7.2 Galois Groups of Cyclotomic Fields

The previous subsection established that adjoining a primitive root of unity produces a finite field extension whose degree is determined by the corresponding cyclotomic polynomial. The next natural question is how the roots of this polynomial are related to one another. As in the previous chapter, these relationships are described by the automorphisms of the splitting field.

Recall that an automorphism of a field extension preserves both addition and multiplication while fixing every element of the base field. Consequently, an automorphism cannot send a root of a polynomial to an arbitrary complex number; it must send the root to another root satisfying exactly the same algebraic relations. This observation determines the structure of the Galois group of every cyclotomic field.

Theorem 7.4. *(Rotman, 1998) Let ζ_n be a primitive nth root of unity. Then*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

where $(\mathbb{Z}/n\mathbb{Z})^\times$ denotes the multiplicative group of units modulo n.

Proof Sketch. Every automorphism of $\mathbb{Q}(\zeta_n)$ fixing $\mathbb{Q}$ is completely determined by the image of the generator ζ_n. Since automorphisms preserve multiplication and the multiplicative order of elements, ζ_n must be mapped to another primitive nth root of unity.

Every primitive nth root of unity has the form

$$\zeta_n^k,$$

where

$$\gcd(k, n) = 1.$$

Conversely, each such exponent defines a unique automorphism by

$$\sigma_k(\zeta_n) = \zeta_n^k.$$

Composing two automorphisms corresponds to multiplying their exponents modulo n, which is precisely the group operation in $(\mathbb{Z}/n\mathbb{Z})^\times$. Therefore,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

A complete proof may be found in Rotman [Rot98]. □

An immediate consequence is that every cyclotomic extension has an abelian Galois group. Unlike the symmetric groups encountered in many polynomial splitting fields, the automorphisms of a cyclotomic field commute with one another because multiplication modulo n is commutative.

Corollary 7.5. *For every positive integer n,*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

is an abelian group.

Proof. By the previous theorem,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian under multiplication modulo n. Since isomorphic groups share the same algebraic structure, the Galois group is also abelian. □

To illustrate this result, consider the cyclotomic field generated by a primitive fifth root of unity. Let

$$\zeta_5 = e^{2\pi i/5}.$$

Since

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

the extension has degree

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4.$$

The units modulo 5 are

$$(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\},$$

which form a cyclic group of order four. Each element determines an automorphism of the cyclotomic field by

$$\sigma_k(\zeta_5) = \zeta_5^k, \qquad k \in \{1, 2, 3, 4\}.$$

Thus,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4,$$

where C_4 denotes the cyclic group of order four.

This example highlights a key feature of cyclotomic fields. Instead of having a complicated, non-commutative symmetry group like S_3 or S_4, their automorphisms behave according to standard modular arithmetic. This comparatively simple algebraic structure ultimately makes it possible to determine exactly which regular polygons are constructible using only a straightedge and compass.

7.3 The Gauss–Wantzel Theorem

The previous subsection established that the Galois group of a cyclotomic field is completely determined by the multiplicative group of units modulo n. Combining this result with the constructibility criterion developed in Chapter 6 yields one of the most celebrated results in classical geometry: a complete classification of the regular polygons that can be constructed with an idealized straightedge and compass.

Recall from Theorem 5.8 that an algebraic number is constructible if and only if the Galois group of its Galois closure is a finite 2-group. Therefore, to determine whether a regular n-gon is constructible, it suffices to determine when the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

has order equal to a power of two.

Since

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

its order is

$$\left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \varphi(n),$$

where $\varphi(n)$ denotes Euler's totient function.

The complete answer is given by the following theorem.

Theorem 7.6 (Gauss–Wantzel (Gauss, 1796; Wantzel, 1837))**.** *A regular n-gon is constructible with an idealized straightedge and compass if and only if*

$$n = 2^k p_1 p_2 \cdots p_r,$$

where

1. $k \geq 0$,

2. *each* p_i *is a distinct Fermat prime, and*

3. *every Fermat prime has the form*

$$p_i = 2^{2^m} + 1$$

for some nonnegative integer m.

The complete proof requires a detailed analysis of cyclotomic fields together with properties of Euler's totient function and finite abelian groups. Since these ideas extend beyond the scope of this paper, we omit the proof and instead explain why the theorem follows naturally from the constructibility criterion established earlier.

Suppose a regular n-gon is constructible. Its vertices are the nth roots of unity, so constructing the polygon is equivalent to constructing a primitive root of unity

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

Because ζ_n is constructible, Theorem 5.8 implies that the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

must be a finite 2-group.

By the previous theorem,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

whose order is

$$\varphi(n).$$

Therefore,

$$\varphi(n) = 2^m$$

for some nonnegative integer m.

Gauss showed that this arithmetic condition holds when

$$n = 2^k p_1 p_2 \cdots p_r,$$

where the p_i are distinct Fermat primes. Wantzel later proved that this condition is not merely necessary but also sufficient, thereby completing the classification of constructible regular polygons.

Only five Fermat primes are currently known:

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

These correspond to the regular polygons whose classical straightedge and compass constructions were discovered by Gauss and later justified algebraically through Galois Theory.

7.4 Illustrated Example of the Pentagon

To construct a regular pentagon, you need a root of the 5th cyclotomic polynomial:

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = 0$$

The degree of this polynomial is 4. Its Galois group has a size of 4, which is 2^2, a power of 2. Because the group size is a power of 2, the field is already its own Galois closure. This means a quadratic tower exists. Constructing a regular pentagon requires constructing the quantity $\frac{\sqrt{5}}{5}$. This corresponds algebraically to adjoining $\sqrt{5}$ to $\mathbb{Q}$, producing the quadratic extension $\mathbb{Q}(\sqrt{5})$. Our new field is $F_1 = \mathbb{Q}(\sqrt{5})$. Next, the polynomial transforms now that $\sqrt{5}$ the original degree-4 polynomial factors into two degree-2 polynomials:

$$\left(x^2 + \frac{1-\sqrt{5}}{2}x + 1\right)\left(x^2 + \frac{1+\sqrt{5}}{2}x + 1\right) = 0$$

Applying the quadratic formula takes the final square root to solve these remaining degree-2 polynomials, which corresponds to the final geometric construction via compass and straightedge. The polynomial splits into four degree-1 factors, and the pentagon is constructed. For the reader interested in what this construction geometrically looks like, they may refer to the following link: Geometric Construction of the Regular Pentagon via Ruler and Compass

Remark. The roots of the 5th cyclotomic polynomial Figure 4

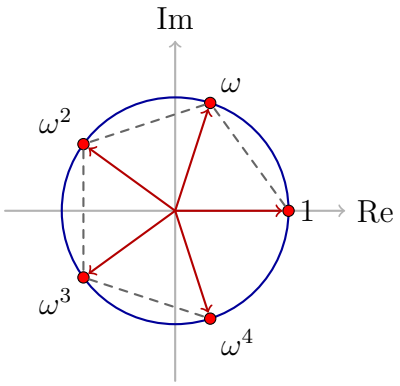


Figure 4: The fifth roots of unity plotted on the complex plane forming a regular pentagon.

Conclusion

Throughout this paper, we developed the necessary Algebra, Field, Theory, and Galois Theory to answer many questions about straightedge and compass constructions.

However, the field is still very active and open with many other geometric constructibility methods, such as paper strips and origami. And, with many open questions

such as what polygons can be formed through a sequence of specific folds, classifying and limiting the maximum number of edges a polygon can possibly have when constructed from a single continuous flat paper strip, or the number of Fermat primes which would determine the straightedge and compass constructible regular-polygons.

Moreover, this area of math has numerous real world applications. For example, masons use straightedges, string, and templates to draw two-dimensional geometric constructions onto stone; these 2D drawings display the angles the stone must be chiseled at to ensure the final 3D arch does not collapse. Another example includes aerospace machinists who use specialized physical compasses and straightedges to scratch lines directly onto blocks of titanium or steel, and by using constructibility steps, they ensure the layout is mathematically *possible* before the metal is cut. And in similar fields such as origami constructibility, NASA (National Aeronautics and Space Administration) and JAXA (Japan Aerospace Exploration Agency) use the Miura-ori fold to pack massive solar panels into 1/25th of their original size.

Acknowledgments

I am very thankful for Elsa Frankel for her patience, inspiring conversations, helpful comments, and discussions. I would also like to thank the Euler Circle for guiding me on this research, the classes, assistance with writing LaTeX, and the incredible guest lectures on mathematics. Also, I thank my peers for their many questions and comments during the Euler Circle Symposium.

References

[Axl24] Sheldon Axler. *Linear Algebra Done Right*. Springer, 4th edition, 2024. Open Access.

[Bel26] James Belk. Number theory for polynomials. Cornell University Lecture Notes, 2026. Accessed: July 3, 2026.

[Euc56] Euclid. *The Thirteen Books of Euclid's Elements*. Dover Publications, New York, 1956. Translated with introduction and commentary.

[Mil22] James S. Milne. Fields and galois theory (v5.10), 2022. Available at www.jmilne.org/math/.

[Mur] Fiona Murnaghan. MAT 240 - Algebra I: Fields. https://www.math.toronto.edu/fiona/courses/mat240/field.pdf. Course lecture notes, Department of Mathematics, University of Toronto.

[Rot98] Joseph J. Rotman. *Galois Theory*. Universitext. Springer-Verlag, New York, NY, 1998.

[Rus09] Paul Russell. Eisenstein's irreducibility criterion. University of Cambridge, DPMMS Lecture Notes, 2009. Based on lectures by J. M. E. Hyland; Accessed: July 3, 2026.

[vL82] Ferdinand von Lindemann. Über die zahl π. *Mathematische Annalen*, 20(2):213–225, 1882.