Proof of the Gauss–Wantzel Theorem

Raahil Mullick

September 2024

Abstract

The Gauss-Wantzel Theorem states the necessary and sufficient condition on n for a regular n-gon to be constructible using a straight-edge and compass. Specifically, the theorem states that a regular n-gon is constructible if and only if $n = 2^a p_1 p_2 \dots p_k$ for some $a \in \mathbb{N}$ and distinct Fermat primes $p_1, p_2 \dots p_k$ such that $p_i \neq p_j$ for any $i \neq j$. A proof of the theorem can be found in multiple sources; however, the clarity of reasoning is often compromised on due to concision requirements. This paper aims to delineate a complete proof of the Gauss-Wantzel Theorem using ideas from group theory, Galois theory, field extensions, and cyclotomic fields.

Contents

1 Introduction

This paper tackles the Gauss-Wantzel Theorem, which states:

Theorem 1.1 (Gauss-Wantzel). A regular n-gon is constructible with straightedge and compass if and only if n is the product of a power of 2 and zero or more distinct Fermat primes.

We present a proof which uses the properties and methods of field theory.

2 Reimagining the Problem

Constructing a regular n-gon is equivalent to constructing n equally spaced points on the unit circle (from which a regular n-gon can be obtained by connecting the points). These n equally spaced points are precisely the n^{th} roots of unity. An n^{th} root of unity is written as

$$\zeta_n^k = e^{2i\pi\frac{k}{n}} \tag{1}$$

for some $k \in \{1, 2, \ldots, n\}$. The n different values of k correspond to the n^{th} roots of unity, which are roots of the equation $x^n - 1 = 0$.

Definition 2.2 (Primitive Roots). An n^{th} root of unity is said to be *primitive* if and only if it can generate all other n^{th} roots under multiplication. The simplest primitive n^{th} root is $\zeta_n = e^{\frac{2i\pi}{n}}$. All primitive n^{th} roots take the form

$$\zeta_n^k = e^{2i\pi\frac{k}{n}} \tag{2}$$

with the condition that $\gcd(k, n) = 1$. That is, k must be coprime to n. This property follows from its analogy in group theory:

Theorem 2.3. Given a generator g of group G such that $|G| = n$, g^k is a generator if and only if $\gcd(k, n) = 1$.

Definition 2.4. The n^{th} cyclotomic field, $\mathbb{Q}(\zeta_n)$, is an extension field of $\mathbb{Q}$ obtained by adjoining a primitive n^{th} root of unity ζ_n to the rationals.

3 Extension Field $\mathbb{Q}(\zeta_n)$

Definition 3.1. Let $\mathbb{Q}[x]$ denote the field of polynomials with coefficients in $\mathbb{Q}$.

We can attempt to rewrite $\mathbb{Q}(\zeta_n)$ as $\mathbb{Q}[x]/\langle p(x)\rangle$, where $p(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$ and $\langle p(x)\rangle$ denotes the ideal generated by $p(x)$.

Definition 3.2. The n^{th} cyclotomic polynomial, $\Phi_n(x)$, is the unique irreducible polynomial with integer coefficients that is a divisor of $x^n - 1$ but is not a divisor of $x^k - 1$ for any $k < n$, which makes it the minimal polynomial of ζ_n over $\mathbb{Q}$. The n^{th} cyclotomic polynomial is given by

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - \zeta_n^k\right). \tag{3}$$

All primitive n^{th} roots and only primitive n^{th} roots are roots of $\Phi_n(x)$.

4 Interesting Properties of $\Phi_n(x)$

It is insightful to consider $\Phi_n(x)$ for a few small values of n:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
\end{aligned} \tag{4}$$

An interesting observation to note is that all of these polynomials have coefficients only in $\{-1, 0, 1\}$. One might think that this property always holds for all n. However, interestingly, this pattern holds up till $n = 104$ but fails at $n = 105$, for which we have:

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - \dots \tag{5}$$

This $-2x^{41}$ term is the first one in all of $\Phi_n(x)$, for $n \leq 105$, to have a coefficient other than $-1, 0$, or 1. This is particularly interesting because $105 = 3 \times 5 \times 7$: 105 is the first integer to have 3 distinct odd prime factors. This idea is explained by:

Theorem 4.1 (Migotti). If n has at most two distinct odd prime factors, then the coefficients of $\Phi_n(x)$ are all in $\{-1, 0, 1\}$.

While this theorem does not guarantee that a number with three or more distinct odd prime factors will have a term with coefficient other than $-1, 0$, or 1, it does explain why the pattern discussed above holds till $n = 104$.

Another interesting observation from Eq.(4) is that if p is prime, then $\Phi_p(x)$ contains all terms with exponent less than p. This pattern actually holds for all primes p.

Characterizing the n^{th} cyclotomic polynomial is not trivial and is an interesting avenue for research. Some basic generalizations are:

- If p is prime, then
$$\Phi_p(x) = \sum_{k=0}^{n-1} x^k \tag{6}$$
- If $n > 1$ is odd, then
$$\Phi_{2n}(x) = \Phi_n(-x) \tag{7}$$

Current research in cyclotomic polynomials is concerned with the coefficients of $\Phi_n(x)$. In particular, the main motivation is the maximal coefficient of $\Phi_n(x)$.

Definition 4.2. For $n \in \mathbb{N}$, let $A(n)$ denote the maximal coefficient (in absolute value) of the n^{th} cyclotomic polynomial $\Phi_n(x)$.

Theorem 4.3 (1895, A.S. Bang). Let $3 \leq p \leq q \leq r$ be three prime numbers. Then, $A(pqr) \leq p - 1$. This implies the existence of $M(p) := \max_{p \leq q \leq r} A(pqr)$ such that $1 \leq M(p) \leq p - 1$. In this case, $\Phi_{pqr}(x)$ is called *ternary*.

Conjecture 4.4 (Sister Beiter). Given conditions from Theorem 4.3, $M(p) \leq \frac{2}{3}p$.

This conjecture is an open problem, although a preprint from as recently as 2023 claims to prove it and even gives the additional proposition that

$$\lim_{p \to \infty} \frac{M(p)}{p} = \frac{2}{3}. \tag{8}$$

A fundamental relation involving cyclotomic polynomials is as follows. It is very similar to a theorem commonly used in number theory:

$$\sum_{d|n} \phi(d) = n \tag{9}$$

The analogue for cyclotomic polynomials is

$$\begin{aligned} x^n - 1 &= \prod_{k=1}^{n} \left(x - \zeta_n^k\right) \\ &= \prod_{d|n} \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=d}} \left(x - \zeta_n^k\right) \\ &= \prod_{d|n} \Phi_{\frac{n}{d}}(x) \\ &= \prod_{d|n} \Phi_d(x). \end{aligned} \tag{10}$$

The third step arises from the definition

$$\Phi_{\frac{n}{d}}(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=d}} \left(x - \zeta_n^k\right). \tag{11}$$

5 The Forward Implication

The Gauss-Wantzel Theorem is a biconditional statement. That is, an *if and only if* statement. Hence, we must individually prove both directions of the biconditional. First, we prove the forward direction.

5.1 Constructing the Field Extension

Assume that a regular n-gon is constructible. Equivalently, ζ_n is constructible, and the field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is constructible. Since

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}[x]/\langle \Phi_n(x) \rangle, \tag{12}$$

the degree of the field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is the degree of $\Phi_n(x)$, which is the number of its distinct roots, which, recalling the definition of $\Phi_n(x)$, is exactly the number of primitive n^{th} roots of unity, which is the number of $k < n$ such that $\gcd(k, n) = 1$. That is, Euler's totient function. Hence, the degree of the field extension is given by

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n). \tag{13}$$

We can obtain the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ through a chain of m field extensions:

$$\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m = \mathbb{Q}(\zeta_n) \tag{14}$$

By the characterization of constructible numbers, only quadratic field extensions can be constructed. That is, each extension $[K_{i+1} : K_i] = 2$.

Theorem 5.1 (Tower Rule). Let $K \subseteq L \subseteq M$ be a tower of three fields. Then,

$$[M : K] = [M : L] \cdot [L : K] \tag{15}$$

Using this law, for the chain of quadratic field extensions in Eq.(14), we have:

$$\begin{aligned} [\mathbb{Q}(\zeta_n) : \mathbb{Q}] &= 2^{m+1} \\ \implies \phi(n) &= 2^{m+1} \end{aligned} \tag{16}$$

5.2 $\phi(n)$ a Power of Two

Consider the prime factorization of any positive integer n:

$$n = 2^a \prod_{i=1}^{k} p_i^{e_i} \tag{17}$$

where $p_1, p_2, \ldots, p_k$ are distinct odd primes for $k \in \mathbb{N}_{\geq 0}$, $e_i \geq 1$ for all i, and $a \geq 0$. (*Note: we include the case in which p_i does not exist: that is, $n = 2^a$ is possible*). Then, we have

$$\begin{aligned} \phi(n) &= \phi\left(2^a \prod_{i=1}^{k} p_i^{e_i}\right) \\ &= 2^{a-1} \cdot \prod_{i=1}^{k} p_i^{e_i - 1} \cdot \prod_{j=1}^{k} (p_j - 1) \end{aligned} \tag{18}$$

But we know $\phi(n) = 2^b$ for some $b \in \mathbb{N}$.

$$\implies 2^{a-1} \cdot \prod_{i=1}^{k} p_i^{e_i - 1} \cdot \prod_{j=1}^{k} (p_j - 1) = 2^b \tag{19}$$

Notice that $p_i^{e_i-1} > 1$ and is odd if and only if $e_i > 1$. But an odd integer greater than one cannot divide a power of two. Hence, $e_i = 1$ for all i.

$$\implies \prod_{j=1}^{k}(p_j - 1) = 2^{b-a+1}. \tag{20}$$

Only a power of two divides a power of two. Hence, $(p_j - 1) = 2^{c_j}$ for some $c_j \in \mathbb{N}$, for all j.

$$\implies p_j = 2^{c_j} + 1 \tag{21}$$

Hence, all primes p_i are distinct Fermat primes. Recall that

$$\begin{aligned} n &= 2^a \prod_{i=1}^{k} p_i^{e_i} \\ &= 2^a \prod_{i=1}^{k} p_i \end{aligned} \tag{22}$$

for $k \in \mathbb{N}_{\geq 0}$.

Thus, n is the product of a power of 2 and zero or more distinct Fermat primes.

In conclusion, if a regular n-gon is constructible, then n is the product of a power of 2 and zero or more distinct Fermat primes.

It remains to prove the converse to achieve *if and only if*.

6 The Converse Statement

To prove the converse, we must first assume that n is the product of a power of 2 and zero or more distinct Fermat primes. That is,

$$n = 2^a \prod_{i=1}^{k} p_i \tag{23}$$

where $p_1 \dots p_k$ are distinct Fermat primes for $k \in \mathbb{N}_{\geq 0}$. Then,

$$\implies \phi(n) = 2^{a-1} \prod_{i=1}^{k} (p_i - 1) \tag{24}$$

Since p_i is a Fermat prime for all i, $p_i = 2^{b_i} + 1$ for some $b_i \in \mathbb{N}$.

$$\begin{aligned} \implies \phi(n) &= 2^{a-1} \prod_{i=1}^{k} \left(2^{b_i} + 1 - 1\right) \\ &= 2^{a-1} \prod_{i=1}^{k} 2^{b_i} \\ &= 2^{a-1+\sum_{i=1}^{k} b_i} \end{aligned} \tag{25}$$

Hence, $\phi(n)$ is a power of 2.

From Eq.(13), since $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, the degree of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a power of 2.

6.1 Introduction to Galois Theory

Proving the converse statement of the Gauss-Wantzel Theorem is not trivial, because it requires some tools of Galois theory along with more advanced group theory.

Galois theory connects group theory and field theory. This connection is the fundamental theorem of Galois theory, which will be examined in detail and applied to our

proof in Section 6.3. For now, it's important to establish a few definitions.

Definition 6.1. A splitting field of a polynomial $p(x)$ of degree n over a field K is a field extension L of K of minimal degree over which $p(x)$ factors into linear factors:

$$p(x) = c\prod_{i=1}^{n}(x - a_i) \tag{26}$$

where $c \in K$ and for each i, we have $a_i \in L$ with a_i not necessarily distinct and such that the roots a_i generate the field extension L over K. The extension L/K is then of minimal degree in which $p(x)$ splits as shown above.

Definition 6.2. A homomorphism is a structure-preserving map between two algebraic structures of the same type. Formally, given two structures $\langle G_1, \star\rangle$ and $\langle G_2, *\rangle$, a map $f : G_1 \to G_2$ is a homomorphism if and only if $f(x \star y) = f(x) * f(y)$ for all $x, y \in G_1$.

Definition 6.3. An isomorphism is a bijective homomorphism.

Definition 6.4. An automorphism of structure S is an isomorphism of S onto itself. In other words, an automorphism α of S is the isomorphism $\alpha : S \to S$.

Definition 6.5. Given a prime number p, a p-group is a group in which the order of every element is a power of p.

Corollary of 6.5. A finite group G is a p-group if and only if $|G| = p^k$ for some $k \in \mathbb{N}_{\geq 0}$.

Theorem 6.6 (Emil Artin). E/F is a Galois extension if E is a splitting field of a separable polynomial with coefficients in F.

Definition 6.7. Let E be an extension of a field F. An automorphism of E/F is defined as an automorphism of E that fixes F pointwise. Formally, an automorphism

of E/F is an isomorphism $f : E \to E$ such that $f(x) = x$ for each $x \in F$.

Definition 6.8 (Galois group). The set of all automorphisms of E/F forms a group under function composition. This group is denoted by $\mathrm{Aut}(E/F)$. If E/F is a Galois extension, then $\mathrm{Aut}(E/F)$ is termed the Galois group of E/F and is usually denoted by $\mathrm{Gal}(E/F)$.

A fact that follows intuitively from the definition of $\Phi_n(x)$ is that the extension field $\mathbb{Q}(\zeta_n)$ is the splitting field of $\Phi_n(x)$, a polynomial with coefficients in $\mathbb{Q}$. By Theorem 6.6, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension.

Additionally, the order of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is simply $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, which is a power of 2 as proven earlier. By *Corollary of 6.5*, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is a 2-group.

A lemma we require to proceed is the following version of Sylow's First Theorem.

Theorem 6.9 (Sylow). A finite group G whose order $|G|$ is divisible by p^k for some $k \in \mathbb{N}$ has a subgroup of order p^k.

7 Construction of Subgroups

We know that 2^k divides 2^m if $m > k$. By Sylow (Theorem 6.9), setting $G = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$, we have m distinct subgroups $H_i \leqslant G$, expressed by the set

$$\{H_i : |H_i| = 2^i,\ i \in \{0, 1, \ldots, m\}\}. \tag{27}$$

By iteratively setting $G = H_i$ for each i in Theorem 6.9, we can prove that H_{i-1} is a subgroup of H_i. Hence, there exists a chain of subgroups

$$\{id\} = H_0 \leqslant H_1 \leqslant \ldots \leqslant H_{m-1} \leqslant H_m = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right). \tag{28}$$

where id is the identity automorphism.

7.1 Fundamental Theorem of Galois Theory (FTGT)

The fundamental theorem of Galois theory, in essence, states that given a finite Galois extension E/F, there is a *one-to-one correspondence* between its intermediate fields (fields K satisfying $F \subseteq K \subseteq E$) and subgroups of its Galois group.

For finite extensions E/F, the correspondence can be described explicitly as follows.

- For any subgroup H of $\mathrm{Gal}(E/F)$, the corresponding *fixed field*, denoted E^H, is the set of those elements of E which are fixed by every automorphism in H.
- For any intermediate field K of E/F, the corresponding subgroup is $\mathrm{Aut}(E/K)$; that is, the set of those automorphisms in $\mathrm{Gal}(E/F)$ which fix every element of K.

The fundamental theorem states that this correspondence is one-to-one if and only if E/F is a Galois extension.

7.2 Application of FTGT

To apply this fundamental theorem to our proof, let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\zeta_n)$.

We showed on the previous page that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension. Hence, the correspondence of the fundamental theorem is indeed one-to-one. Thus, for each subgroup H_i in the chain of subgroups in Eq.(28), there exists a corresponding subfield K_i which is the fixed field of H_i. Hence, we can form a corresponding chain of field extensions

$$\mathbb{Q} = K_m \subseteq K_{m-1} \subseteq \ldots \subseteq K_1 \subseteq K_0 = \mathbb{Q}(\zeta_n) \tag{29}$$

such that each individual field extension K_i/K_{i+1} has order

$$\begin{aligned} [K_i : K_{i+1}] &= \frac{|H_{i+1}|}{|H_i|} \\ &= \frac{2^{i+1}}{2^i} = 2. \end{aligned} \tag{30}$$

By the characterization of constructible numbers, all quadratic field extensions of $\mathbb{Q}$ are constructible. We just showed that the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ can be expressed as a chain of quadratic field extensions. Hence, ζ_n is constructible, from which all n^{th} roots of unity are constructible. Thus, the regular n-gon is constructible.

We have therefore proven the implication that *if* n is the product of a power of 2 and zero or more distinct Fermat primes, *then* a regular n-gon is constructible.

That proves the converse statement, and in combination with the forward statement, concludes our proof to *Theorem 1.1*, the Gauss-Wantzel Theorem.

References

[1] Artin, Michael. *Algebra*. Prentice Hall, 1991.

[2] Dummit, David S, and Richard M. Foote. *Abstract Algebra*. 3rd ed., John Wiley & Sons, 2004.

[3] Gallian, Joseph A. *Contemporary Abstract Algebra*. 9th ed., Cengage Learning, 2017.

[4] Cuoco, Al, and Rotman, Joseph. *Learning Modern Algebra*. Mathematical Association of America, 2013.

[5] Clark, Allan. *Elements of Abstract Algebra*. Dover Publications, 1984.

[6] Pinter, Charles C. *A Book of Abstract Algebra*. 2nd ed., Dover Publications, 2010.

[7] Judson, Thomas W. *Abstract Algebra: Theory and Applications*. 2021 edition, Orthogonal Publishing L3C, 2021.

[8] Rotman, Joseph. *Advanced Modern Algebra*. 2nd ed., American Mathematical Society, 2010.

[9] Wikipedia Contributors. "Fundamental Theorem of Galois Theory." *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Fundamental_theorem_of_Galois_theory.

[10] Wikipedia Contributors. "Galois Extension." *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Galois_extension.

[11] Wikipedia Contributors. "Sylow Theorems." *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Sylow_theorems.