Constructible Regular n-gons

Devin Kuh

May 8, 2013

1 Abstract

This paper will discuss the constructability of regular n-gons. The constructions will follow the rules of Euclidean Constructions. This question of which regular n-gons are constructible stems from the same era of Ancient Greek questions like doubling the cube and squaring the circle. The paper will examine both the Abstract Algebra theory and the physical constructions. The theory will center on Gauss' theorem of constructible regular n-gons and a larger result of which Gauss' theorem is a specific case of (although proven independently). Our physical constructions will look at the regular pentagon, 17-gon, 15-gon and 51-gon as specific examples to illuminate these possibilities.

2 Introduction

The theory and the application of constructible regular n-gons are seemingly very separate from one another. Gauss' Theorem states

Theorem 2.1. A regular n-gon is constructible if and only if n is of the form

$$n = 2^a p_1 p_2 p_3 \dots p_i$$

where $a \ge 0$ and $p_1, p_2, ..., p_i$ are distinct Fermat Primes (primes of the form $2^{2^l} + 1$ such that $l \in \mathbb{Z}^+$).

This does not give the reader any clue of how she might actually construct such an n-gon. One purpose of this paper will be to explore both the theory and the physical construction sides of the discussion, starting first with the physical Euclidean constructions, using only a collapsing compass and straight edge, and then moving into proofs of Gauss' Theorem and a larger result. The latter can be used as a lemma in an alternative, much simpler, proof of Gauss' theorem. It will be interesting to note how the closest link between theory and application comes when looking at why multiples of Fermat primes to the first power and powers of two are constructible. There is a theoretical background that gives us the constructability of certain building blocks, namely the regular n-gons such that n is a power of 2 or a Fermat Primes to the first power and a seemingly unconnected physical background that gives us these foundations as well. When pressed to go further and prove that the

multiples of these Fermat Primes and powers of 2, all n of the form $n = 2^a p_1 p_2 \dots p_k$, are actually possible is where these two areas collide and lead the reader to parallel proofs that connect (to some extent) the theory and the application.

En route to constructing these n-gons, one goal is to create the different interior angles of the regular n-gons. Theoretically, they are marking the n evenly spaced points around the complex unit circle. We can view these points as nth-roots of unity and are solutions to the following equation,

$$x^n - 1 = 0.$$

The solutions are powers of $\gamma_n = e^{\frac{2\pi i}{n}}$. This theoretical idea will be helpful in understanding some of the physical constructions and vital to our theoretical discussion by giving us something tangible for what these constructions mean theoretically.

We will first turn our attention towards understanding constructions as an action, discussing the constructions of regular n-gons when n is a single Fermat Prime, and proving these constructions. Here we will take a break from constructions and shift our attention to presenting the requisite algebraic background. After this, we will do a proof of Gauss' Theorem with the simpler case of n being equal to a power of a prime. We will then prove the Composition Lemma to extend this result to Gauss' full theorem. Next, we will look at how to construct more complex regular n-gons when n is composed of more than one distinct Fermat Prime and a power of 2. We will use the Composition Lemma once again in this instance. This is where the gap is bridged between theory and constructions. Finally we will present a larger theorem and its proof, and briefly look at how this proof facilitates the proof of Gauss' Theorem.

3 Introduction to Constructions

Euclidean Constructions are those constructions that can be completed using only a straight edge and a collapsing compass which closes when it is picked up. This collapsability causes problems because it means we cannot simply move a distance with a compass. There are three basic constructions that can be completed in Euclidean constructions. These constructions are

- 1. The straight line by connecting two points,
- 2. A circle of a given radius centered at a given point or
- 3. Continuing a segment infinitely.

From these given constructions a number of other constructions can be created. A number *a* is said to be **geometrically constructible** if it can be reached with a finitie number of intersections of two circles, a line and a circle and/or two lines. Two of the simplest and most important, bisecting an angle and drawing a perpendicular bisector to a segment, are outlined below. Throughout this paper, constructions were created in GeoGebra then exported as .png files and saved as .jpgs in Paint.

Angle Bisection:

- 1. Given an angle, $\angle ABC$, draw a circle of radius \overline{AB} centered at B. Name this circle's intersection with \overline{AC} , D.
- 2. Draw circles of radius \overline{AB} centered at A and D. Name the intersection of these circles within $\angle ABC$, E.
- 3. Connecting B and E creates an angle bisector of $\angle ABC$. This follows from Side-Side-Side-Side Congruence of $\triangle ABE$ and $\triangle DBE$.



Figure 1: Angle Bisection Step 1

Figure 2: Angle Bisection Step 2

Figure 3: Angle Bisection Step 3

Perpendicular Bisector:

- 1. Given a line segment, \overline{AB} , draw two circles of radius \overline{AB} , one centered at A and one centered at B.
- 2. Call the intersections of these two circles C and C'. Connecting these two points yields a perpendicular bisector.



Figure 4: Step 1 Figure 5: Step 2

This last construction is also coincidentally the construction for our simplest regular *n*-gon, the equilateral triange, ΔABC . It is clear that $\overline{AB} = \overline{BC} = \overline{CA}$, since all are radii of circles of equal radius. Thus all three sides are equal, and it follows that the angles are of equal measure as well. Throughout this paper we will use these constructions, and the ability to continue a line segment indefinitely in a straight line, to create the more complex constructions that are pertinent to our discussion.

4 Construction and proof of the regular pentagon and heptadecagon

Now we look to start laying out two of the foundational constructions in the scope of regular n-gons. As we have already constructed the regular triangle $(n = p_1 = 3 = 2^{2^0} + 1)$, we turn our attention to constructing the regular pentagon and the regular heptadecagon, $n = p_2 = 5 = 2^{2^1} + 1$ and $n = p_3 = 17 = 2^{2^2} + 1$ respectively. We will start with the regular pentagon and then move on to the construction of the regular heptadecagon.

We will in turn to show that these two constructions are in fact valid and yield two exact regular polygons, not merely two shapes that look regular. The easy way to show this is by using basic geometry and proving that all the interior angles formed by the rays from the center to adjacent verticies are in fact all congruent. This easy proof is left to the reader.

The more complex way, but yet more enlightening way is done by looking at what each individual step of our construction is doing to create the requisite interior angle. For example, we must construct an interior angle of 72° for the regular pentagon and one of $\frac{360}{17}$ ° for the regular heptadecagon. It should be clear that with this angle constructed, we can copy it n times with adjacent legs and draw a circle of any radius centered at the shared vertex and create the regular n-gon in question.

4.1 Constructing the Regular Pentagon

- 1. First, draw a line segment, \overline{AB} , and its perpendicular bisector. Name the intersection C.
- 2. Then, find the intersection of the bisector and the circle of radius |AB| centered at C. Call these intersections D and D'.



Figure 6: Step 1

Figure 7: Step 2

- 3. Next, connect D to A, forming the line segment \overline{DA} . Construct a circle, of radius $|AC| = \frac{|AB|}{2}$, centered at A. Call this circle's intersection with the line segment \overline{DA} , E
- 4. Find a perpendicular line to this new section, \overline{DA} , through the point E, Line X.



Figure 8: Step 3

Figure 9: Step 4

5. Construct a circle centered at D with radius |DD'|. Intersect line X with this circle. Call the two points of intersection F and G. 6. Construct line segments \overline{FD} and \overline{GD} .



Figure 10: Step 5

Figure 11: Step 6

7. Draw a circle, of radius |DA|, centered at D, call this circle Z. Its intersections with \overline{FD} and \overline{GD} form the adjacent vertices to A, F' and G'.



Figure 12: Step 7

- 8. Finally, draw a circle, of radius |AF'|, centered at F'. Call this intersection with circle Z, H.
- 9. Next, draw a circle centered at H with radius |F'H|. Call this intersection with circle Z, I.



Figure 13: Step 8

Figure 14: Step 9

10. Connecting A, F', G', H, I yields the regular pentagon.



Figure 15: Completed Pentagon



Proof: If we can prove that $\angle ADF' = \angle F'DH = \angle HDI = \angle IDG' = \angle G'DA = 72^{\circ}$ we will know that each interior angle of the pentagon is 72° and that the pentagon is regular.

Proof. As a convention, we will set $|\overline{DC}| = 1$. Note $|\overline{AB}| = |\overline{DC}|$ by construction. It follows that $|\overline{AC}| = \frac{1}{2}$. Considering ΔDAC , The Pythagorean Theorem yields



Figure 17: Side Measures of ΔDAC

Note that $|\overline{AE}| = \frac{1}{2}$. It follows that $|\overline{DE}| = \frac{\sqrt{5}}{2} - \frac{1}{2}$. Now considering ΔDEF note that $|\overline{DF}| = 2$. It follows that $\sin(\angle DFE) = \frac{1}{4}(\sqrt{5} - 1)$.



Figure 18: Side Measures of ΔDEF

Thus $\angle DFE = 18^{\circ}$. Since $\angle DEF = 90^{\circ}$,

$$\angle ADF = 180^{\circ} - 90^{\circ} - 18^{\circ} = 72^{\circ}$$

It follows that our pentagon is regular.



Figure 19: Final Angle Measure

4.2 Constructing the Regular Heptadecagon

Next, we turn to look at the construction of the regular heptadecagon.

- 1. Construct a circle of diameter $\overline{AB} = 8$ units.
- 2. Draw a perpendicular bisector to the segment \overline{AB} . Name the intersection with \overline{AB} , O, and its intersection with the circle, C.
- 3. Bisect this radii twice to create the point, D.
- 4. Draw line segment \overline{DA} .



Figure 20: Steps 1,2,3 and 4

5. Bisect $\angle ODA$ twice to create $\angle ODE$.

6. Construct a 45 degree angle to the left of \overline{DE} and label its intersection with \overline{AB} , F.



Figure 21: Step 5

Figure 22: Step 6

- 7. Bisect \overline{AF} , and construct a circle centered at the mid-point of \overline{AF} , called z through A. Label the intersection with the vertical radius, G.
- 8. Draw a circle centered at E through G. Name the intersections with the horizontal diameter H and K respectively.



- 9. Draw perpendiculars through H and K. Label the intersections with the large circle L and M.
- 10. Bisect $\angle MOL$. Label this intersection with the large circle N.



11. Finally, draw circles of radius \overline{LN} starting centered at L, then using each new intersection as a center. Connect all these centers.



Figure 27: Complete Regular 17-gon

12. Enjoy our regular 17-gon!



Figure 28: Pretty Regular 17-gon

Proof: We look to prove that the interior angle $\angle MOL$ is in fact $\frac{720^{\circ}}{17}$. Thus bisecting will yield the requisite interior angle. To do this, we will prove that $180^{\circ} - \angle LOH - \angle MOK = \frac{720^{\circ}}{17}$ or $180^{\circ} - \arccos \frac{\overline{OH}}{\overline{LO}} - \arccos \frac{\overline{OK}}{\overline{MO}} = \frac{720^{\circ}}{17}$. We know from our construction that $\overline{MO} = \overline{LO} = 4$ since they are radii. This leaves us with the task of finding values for \overline{OK} and \overline{OH} . We will do this with a series of trigonometric arguments. All triangles considered will be right triangles by construction.

Proof. 1. Note, $\angle ODA = \arctan 4$. This comes from the triangle in Figure 29.

2. It follows from construction that $\angle ODE = \left(\frac{\arctan 4}{4}\right)$. We will call this angle *a*. The $\triangle ODE$ yields, $\overline{OE} = \tan ODE$. We will call this length *b*.



Figure 29: Steps 1 and 2

- 3. Next, observe that by construction $\angle ODF = 45^{\circ} a$. Considering $\triangle ODF$ yields, that $\overline{OF} = \tan 45 a$. We will call this length c.
- 4. It follows from construction that $\overline{AF} = c + \overline{OA}$. Thus, $\overline{AF} = c + 4$. We will call this length d.



Figure 30: Steps 3 and 4

- 5. Remember, we are trying to find the value of \overline{OK} . Note, we have found previously \overline{OE} , so all that is left is \overline{EK} .
- 6. From our construction, observe $\overline{EG} = \overline{EK}$ since both are radii of the same circle. We will find \overline{EG} .
- 7. Note that, $\overline{OZ} = \frac{d}{2} c$ and that \overline{ZG} is a radius of a circle centered at Z through A and F. Thus, $\overline{ZG} = \frac{d}{2}$. We will call these values e and f respectively.
- 8. Using ΔOZG we can find that $\cos OZG = \frac{\overline{OZ}}{\overline{ZG}} = \frac{\frac{d}{2}-c}{\frac{d}{2}} = 1 \frac{2c}{d}$. We will let $\cos OZG = g$.
- 9. Next, solving for $\angle OZG$, we find $\angle OZG = \arccos g$. We will call this angle h.
- 10. It follows that, $\overline{OG} = f \sin h$. We will call this length *i*.
- 11. Now, we will turn to $\triangle OGE$ and use *i* to find *EG*.



Figure 31: Steps 5-13

- 12. Note, $\tan OGE = \frac{\overline{OE}}{\overline{OG}} = \frac{b}{i}$. It follows that $\angle OGE = \arctan \frac{b}{i}$. We will call this last value j.
- 13. It follows that, $\overline{EG} = \frac{\overline{OE}}{\sin OGE} = \frac{b}{\sin j} = \overline{EK}$. We will name this value k.
- 14. Thus, we can clearly see that $\overline{OK} = \overline{OE} + \overline{EK} = b + k$. We will call this *l*.
- 15. Note, $\overline{HK} = 2k$ since it is a diameter of the same circle that \overline{EK} is a radius of. This gives us $\overline{OH} = \overline{HK} l$.



Figure 32: Steps 13 and 14

- 16. We now have all the requisite values. Trigonometric calculations with ΔMOK and ΔLOH give the values of $\angle MOK$, $\angle LOH$.
- 17. These computations yield $\angle LOM = 180^{\circ} \angle LOH \angle MOK = \frac{720^{\circ}}{17}$. Thus, bisecting $\angle LOM$ yields the necessary interior angle.



Figure 33: Steps 15 and 16

Now that we have shown how to construct these two regular n-gons we will consider the algebraic foundations of these constructions.

5 Algebraic Background

Here we look to develop some of the requisite Abstract Algebra theory in order to move forward with our theoretical arguments. It will be assumed that the reader has a basic knowledge of group theory and has seen fields before although our review will start with fields.

5.1 Fields

A field is a commutative ring with unity such that each non-zero element is invertible under multiplication. Let's look at a few aspects of this statement. First, A **ring** is a set with two operations defined on it with the following properties

- 1. It is an abelian group under the additive operation.
- 2. Multiplication is associative.
- 3. Multiplication distributes over addition.

A commutative ring, R, has the property that ab = ba for any two elements $a, b \in R$. If a ring has unity, it has the property that there is an identity element under multiplication. The final requirement of a field is that every non-zero element is invertible under multiplication. An element, a, is invertible if and only if there exists an $x \in R$ such that ax = xa = 1. A good example of a commutative ring with unity for which there exists an element that is not invertible is \mathbb{Z} . In \mathbb{Z} the element 2 would have multiplicative inverse $\frac{1}{2}$ which is not an integer, thus 2 is not invertible. The only invertible elements are 1 and -1.

A field can have the **cancellation property** which states that if ab = ac then b = c. If a field has such a property it is called an **integral domain**. In other words an integral domain has no zero divisors, which are non-zero elements that when multiplied with other elements equal zero. Another important aspect of fields is their **characteristic**, which is the least positive integer n such that 1 + 1 + ... + 1 n times equals 0. If no such integer exists, the characteristic is 0.

An example of a field we will use often is the rational numbers. As a way of understanding fields let's work though showing this is in fact a field.

1. Let a, b, c, d, e and f be in \mathbb{Z} such that $b, d, e \neq 0$ and (a, b) = 1, (c, d) = 1 and (e, f) = 1. Note that, $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$. We define addition by $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$. First, consider, 0 and $\frac{-a}{b} \in \mathbb{Q}$. It follows $\frac{a}{b} + 0 = \frac{a}{b}$ and $\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-ab)}{bd} = 0$. Thus addition has an identity, 0, and each non-zero element has an additive inverse, its negative. Finally, we must show that \mathbb{Q} is associative under addition. Consider

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + ed}{df}$$
$$= \frac{cfb + edb + dfa}{dfb}$$
$$= \frac{ad + cb}{bd} + \frac{e}{f}$$
$$= \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}.$$

It follows that \mathbb{Q} is a group under addition. One can easily show that commutivity holds in \mathbb{Q} .

- 2. Consider $\left(\frac{a}{b}\right) * \left[\left(\frac{c}{d}\right) * \left(\frac{e}{f}\right)\right] = \left(\frac{a}{b}\right) * \left(\frac{ce}{df}\right) = \frac{ace}{bdf} = \frac{ac}{bd} * \frac{e}{f} = \left[\left(\frac{a}{b}\right) * \left(\frac{c}{d}\right)\right] * \left(\frac{e}{f}\right)$. Thus multiplication is associative over \mathbb{Q} .
- 3. Consider $\frac{a}{b} * [\frac{c}{d} + \frac{e}{f}] = \frac{a}{b} * \frac{cf+ed}{df} = \frac{acf+aed}{bdf} = \frac{acbf+aebd}{bdbf} = \frac{ac}{bd} + \frac{ae}{bf}$. It follows that multiplication distributes over addition.

Thus \mathbb{Q} is a ring.

• Note that $\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd} = \frac{c}{d} * \frac{a}{b}$ and that $\frac{a}{b} * \frac{b}{a} = 1$.

Thus \mathbb{Q} is a commutative ring with unity. It is clear that given a non zero element $\frac{a}{b}$ that $\frac{b}{a}$ inverts it. Thus \mathbb{Q} is a field.

5.2 Polynomials

Another important result is that if R is a commutative ring with unity then R[x], the set of polynomials with coefficients in R, is also a commutative ring with unity. We will often talk about irreducible polynomials. **Irreducible polynomials** are such that no other polynomial of smaller degree in the same ring of polynomials divides it. In other words, if p(x) is irreducible, then there exist no non-trivial polynomials of lesser degree such that a(x)b(x) = p(x). These polynomials have similar properties to prime numbers in \mathbb{Z} if our base ring is a field, namely if p(x) is irreducible and $p(x)|a_1(x)a_2(x)...a_n(x)$ then p(x) divides one of the $a_i(x)$ s. Also, there exists a unique factorization of all polynomials into a string of irreducible polynomials; this is analogous to the Fundamental Theorem of Arithmetic.

Recall from high school algebra that if a is a root of a quadratic, then one of the factors of that quadratic is x - a. This idea holds more generally to polynomials of degree n and each and every root of the polynomial. Polynomials are irreducible when those roots are not contained in the same ring as the polynomial. This is the case for $x^2 - 2 \in \mathbb{Q}[x]$. Note the two roots are $\pm \sqrt{2} \notin \mathbb{Q}$. Thus, $x^2 - 2$ cannot be factored in $\mathbb{Q}[x]$ and therefore is irreducible. All polynomials of degree n have n distinct roots and can be factored completely over the complex numbers as $a(x) = (x - b_1)(x - b_2)...(x - b_n)$ where $b_1, b_2, ..., b_n$ are the distinct roots of a(x).

Eisensteins Irreducibility Criterion is an important result from polynomial theory. It states that a polynomia with integer coefficientsl, $a(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$, is irreducible $in\mathbb{Z}[x]$ if there exists a prime integer p such that p divides each a_i such that $i \neq 0$, p does not divide a_0 and p^2 does not divide a_n . This holds for polynomials in $\mathbb{Z}[x]$ and Gauss proved a Lemma that shows that irreducibility over \mathbb{Z} implies irreducibility over \mathbb{Q} . We will use the polynomial $a(x) = 3x^2 + 4x + 2$ to show an example of the utility of Eisenstein's Irreducibility Criterion. For this polynomial, let p = 2. It is clear that two divides four, but not three, and four does not divide two. Thus, by Eisenstein's Irreducibility Criterion a(x) is irreducible. Note the two roots of this equation are $-\frac{2}{3} \pm \frac{i\sqrt{2}}{3}$. It is clear that, $[x + (\frac{2}{3} + \frac{i\sqrt{2}}{3})][(x + (\frac{2}{3} - \frac{i\sqrt{2}}{3})]$ is not in $\mathbb{Q}[x]$, and thus a(x) is irreducible over this ring.

5.3 Field Extensions

The idea of irreducible polynomials over the Rational field leads to the following question: what is the smallest field in which we can reduce a given polynomial? The Fundamental Theorem of Algebra says that all polynomials are reducible to polynomials of degree 1 over the complex field, but our polynomial may be completely reducible over a smaller field. That leads to the concept of Field Extensions.

Definition 1. Let K and F be fields. If K is a subfield of F then F is called a Field Extension of K (Pinter 270).

A field extension is called simple if it can be reached by adjoining a single element. If a field can be reached by adjoining a series of single elements, then we will have a chain of simple field extensions. More specifically, we can adjoin roots of an equation to the rational numbers, thereby creating a larger field that allows a polynomial to be further reduced. In the case of our earlier polynomial $x^2 - 2$, one larger field is $\mathbb{Q}(\sqrt{2})$ (read \mathbb{Q} adjoined with $\sqrt{2}$). The elements of this field are $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. This is also an example of a splitting field with minimum polynomial $p(x) = x^2 - 2$

Definition 2. A splitting field for a polynomial is the smallest field containing all the roots of that polynomial.

Definition 3. A complex number α has a minimum polynomial, p(x), if p(x) is the irreducible monic polynomial of lowest degree over a field K and $p(\alpha) = 0$.

Throughout this paper we will talk about the degree of these chains of simple field extensions.

Definition 4. The degree of the field extension of F over K is denoted by [F : K] and is found by finding the dimension of F as a vector space over K.

The degree of simple extension is the same as the degree of the minimum polynomial of the adjoined element. It follows from definitions 2 and 3 that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. These above definitions will be critical to our arguments in being able to show whether certain numbers are constructible by finding their minimum polynomials and showing that these splitting fields have degree extensions that are a power of two over the rationals.

An important result concerning field extensions is the Tower Law. This states that if $K \subseteq L \subseteq M$ then [M : K] = [M : L][L : K]. For a finitely generated extension such as $F(a_1, a_2, ..., a_n)$, we get

$$[F(a_1, ..., a_n) : F] = [F(a_1, ..., a_n) : F(a_1, ..., a_{n-1})] ... [F(a_1, a_2) : F(a_1)] [F(a_1) : F].$$

Since each of intermediate fields is a simple field extension then each one of these extensions has a degree equal to the minimum polynomial of the adjoined element.

5.4 Cyclotomic Field

The Cyclotomic Field, ζ_n , is the field of the rationals with the *n*-th roots of unity of adjoined. This field will be pivotal in transitioning the idea of *n* points spaced evenly around the complex circle from physical constructions to something we can work with algebraically.

Definition 5. The n-th roots of unity are the roots to the equation $x^n - 1 = 0$

A *n*th root of unity will be denoted as γ_n , and the group of all the roots will be written as ω_n . A way to geometrically think about this is as *n* points evenly spaced around the unit circle in the complex plane(See Figure 34). Note that for all *n* 1 is a *n*-th root of unity, this is demonstrated in Figure 34 as well.



Figure 34: 5th-Roots of Unity Source: Wikipedia Root of unity

5.5 Constructible Numbers

As discussed earlier, a number is geometrically constructible if it can be reached in a finite number of intersections of lines and circles. This is foreshadowing of the algebraic definition. Note, that any intersection of lines and circles will have a equation that is of degree two or fewer. It follows that all of these equations can be solved with only the rationals and square roots of rationals or square roots of square roots of rationals, etc. Algebraically, a number, a, is said to be **constructible** if there exist a chain of field extensions of degree two from the rationals to the final field containing a. This clearly parallels the fininte number of solutions to degree two or fewer.

5.6 Fermat Numbers

Fermat Numbers are numbers of the form $2^{2^k} + 1$ where $k \ge 1$. The first 5 Fermat Numbers, $F_0...F_4$ are known to be prime. These numbers are 3, 5, 17, 257 and 65537. The next number after F_5 is equal to 4, 294, 967, 297. Fermat was aware that he could not prove this claim, but as exhibited by his Little and Last Theorems, proof was never really a high priority to Fermat; testing the first few cases then conjecturing seemed to be his trend. In 1732, around 80 years after Fermat's death Euler managed to prove that F_5 was in fact composite.

At first he merely published the two divisors, 641 and 6,700,417. As an aside, the first was known to be prime at the time, 6,700,417 was not proved till later to be prime. After about 15 years, Euler published another paper with a more general proof of Fermat's Little Theorem which states:

Theorem 5.1. If neither of the numbers a and b is divisible by the prime number p, then every number of the form $a^{p-1} - b^{p-1}$ will be divisible by p.

He used this to prove an intermediate result stating that any divisor of a number in the form $a^{2m} + b^{2m}$, of which Fermat Numbers are, must be in the form $k2^{m+1} + 1$ such that $k \ge 0$. Lucas improved this to $k2^{m+2} + 1$. This gave him a starting point to test values for n which produce prime numbers and then test if those divide F_5 . It only took him six tries to find a suitable n.

In comparison to this brute force method proving composivity was relatively simple. It merely required a set of congruences to show that $2^32 \equiv 1 \pmod{641}$. Which implies that that 641 divides $2^{2^5} + 1 = F_5$. Note first that $641 = 5 * 2^7 + 1$. It directly follows that

```
5 * 2^7 \equiv -1 \pmod{641}
5^4 * 2^{28} \equiv 1 \pmod{641}
```

Note that $5^4 \equiv -2^4 \pmod{641}$. It follows that

 $-2^{32} \equiv 1 \pmod{641}$

and that 641|4, 294, 967, 297. The computing project Fermat Search has shown that F_6 through F_11 are composite. It is unknown if any larger Fermat Prime exist.

6 Gauss' Theorem

Now we will move onto discussing the central theorem of this paper, Gauss' Theorem, which states

Theorem. A regular n-gon is constructible if and only if n is of the form

$$n = 2^a p_1 p_2 p_3 \dots p_i$$

where $a \ge 0$ and $p_1, p_2, ..., p_i$ are distinct Fermat Primes.

Our proof of Gauss' Theorem will be centered on four important lemmas. The first three lemmas will be used to prove Gauss' Theorem for $n = p^k$. We will then prove the fourth lemma, the Composition Lemma, and use this to generalize our modifided proof to $n = 2^a p_1 p_2 \dots p_k$.

The conditional will depend on the definition of a constructible number, a lemma regarding the degree of the cyclotomic field over the rationals and an algebraic lemma concerning which numbers have a Euler Phi Function value that is a power of 2. The biconditional will also use the degree of the cyclotomic field over the rationals but then turn towards Galois Theory to show the existance of the chain of subfields of requisite degree.

6.1 Necessary Lemmas

In this section we will state and prove three lemmas that are integral to our proof of Gauss' Theorem.

Lemma 6.1. If a is constructible then $[\mathbb{Q}(a) : \mathbb{Q}] = 2^m$ for some integer m.

Proof. Let a be constructible. It follows from the definition of constructible numbers that there exists a chain of field extensions each of order two from \mathbb{Q} to $\mathbb{Q}(a)$. The Tower Law yields that $[\mathbb{Q}(a):\mathbb{Q}] = 2^m$.

Lemma 6.2. If $n = p^k$ then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

It is interesting to note that this lemma can be generalized for all n, but we will only use the $n = p^k$ case.

Proof. Let $n = p^k$ for some prime p and integer k. The splitting field, S, for the polynomial $x^n - 1$, is equal to $\mathbb{Q}(\gamma_n)$. Thus we need to show that $[\mathbb{Q}(\gamma_n) : \mathbb{Q}] = \phi(n)$.

To do this we will start by finding the minimal polynomial of γ_{p^k} . Consider the polynomial $q_{p^k}(x) = \frac{x^{p^k}-1}{x^{p^k-1}-1}$. We will use Eisenstein's Irreducibility Criterion to show that this is in fact both irreducible and that γ_{p^k} is a root. Note the identity $\frac{a^p-1}{a-1} = a^{p-1} + a^{p-2} + \ldots + a + 1$. We will use Eisenstein's Irreducibility Criterion and substitute x = y + 1 to prove that $q_{p^k}(x)$ is irreducible. This and our identity yield

$$q_{p^{k}}(y+1) = (y+1)^{p^{k-1}(p-1)} + (y+1)^{p^{k-1}(p-2)} + \dots + (y+1)^{p^{k-1}} + 1.$$

Note the final term of the expanded polynomial is p since there are p terms each with a 1 as a constant term. Next, we must show that p divides each coefficient except the first. We will show this by realizing that p dividing each term except the first is equivalent to saying that $q_{p^k}(y+1) \cong y^{p^{k-1}(p-1)} \pmod{p}$. This follows because the right will be our first term and the left is the rest of our equation. Congruency implies that $q_{p^k}(y+1) - y^{p^{k-1}(p-1)}$ is divisible by p. The following argument will show why this congruencey holds, and thus each coefficient except the first is divisible by p.

Pinter states the following theorem: in an integral domain, A, with characteristic p, $(a + b)^p = a^p + b^p$ for all elements a, b. This follows from the binomial expansion having a multiple of p in every term except the first and last, which leaves only those two terms, namely $a^p + b^p$ when we reduce mod p. This leads us to examine our polynomial $q_{p^k}(y+1) = \frac{(y+1)^{p^k}-1}{(y+1)^{p^{k-1}}-1} = \frac{y^{p^k}+1-1}{y^{p^{k-1}}+1-1}$. This equals,

$$y^{p^k - p^{k-1}} = y^{p^{k-1}(p-1)}.$$

Thus, we have shown that the polynomial q_{p^k} is in fact irreducible. It remains to show that $\gamma_{p^k} = \omega$ is a root of $q_{p^k}(x)$. Consider $q_{p^k}(\omega) = \frac{\omega^{p^k} - 1}{\omega^{p^{k-1}} - 1}$. Note that ω is a root of $x^{p^k} - 1$ and not of $x^{p^{k-1}} - 1$. Thus, $q_{p^k}(\omega) = 0$ and ω is a root of that polynomial. It follows that $q_{p^k}(x)$ is the minimum polynomial of ω over the rationals. Thus,

$$[\mathbb{Q}(\omega):\mathbb{Q}] = p^{k-1}(p-1) = \phi(p^k).$$

Next, we will state and prove our lemma concerning the form of numbers with an Euler Phi Function value that is a power of 2.

Lemma 6.3. If $n = 2^j + 1$ and j is not of the the form 2^l , then n is a composite.

Proof. Let j have an odd positivie integer, b, in its composition. Thus, $j = b2^{l}$ and $l \ge 0$. Thus $2^{j} + 1 = 2^{b2^{l}} + 1 = 2^{(2^{l})^{b}} + 1$. This can be factored in the following manner

$$2^{(2^{l})^{b}} + 1 = [2^{2^{l}} + 1][2^{2^{l^{(b-1)}}} - 2^{2^{l^{(b-2)}}} + 2^{2^{l^{(b-3)}}} - \dots - 2^{2^{l}} + 1].$$

It follows that if $j \neq 2^l$ then $2^j + 1$ is composite.

6.2 Proof of Gauss' Theorem for $n = p^k$

We will start with a discussion of what is necessary to for n to be a constructible regular n-gon. Note that the n-th roots of unity are n evenly spaced points around the complex unit circle that when connected form a regular n-gon and that these roots are all contained in ζ_n . It follows that being able to construct ζ_n implies that a regular n-gon will be constructible.

Theorem 6.4. A regular p^k -gon is constructible if and only if p is of the form 2^a or a Fermat Prime.

Proof. Let $n = p^k$ be a regular constructible *n*-gon. It follows from our assumption that ζ_{p^k} is constructible and thus Lemma 6.1 gives us that $[\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = 2^m$. From here Lemma 6.2 gives us that $\phi(p^k) = [\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = 2^m$ and thus

$$\phi(p^k) = 2^m$$

Note, $phi(p^k) = 2^m = p^k - p^{k-1}$. It follows that $2^m = p^{k-1}(p-1)$. There are now two cases, if k = 1 or k > 1. If k = 1 it follows that $2^m = p - 1$, and thus $p = 2^m + 1$. If k > 1, it follows that $2^m = p^{k-1}(p-1)$. Thus $p^{k-1}|2^m$ and it follows that p = 2. In conclusion, $p = 2^k$ or $2^m + 1$. Lemma 6.3 gives us that the latter is in the form of a Fermat Prime. It follows that if p^k is a constructible regular *n*-gon then $p = 2^a$ or $2^{2^l} + 1$.

Now we will shift our attention to the biconditional. Let $n = p^k$ such that $p^k = 2^a$ or p is a Fermat Prime. Consider once again the following equation, $x^{p^k} - 1$. The spitting field of this equation is $S = \mathbb{Q}(\zeta_n)$. It follows from Lemma 6.2 that $[S:\mathbb{Q}] = 2^m$. It is now necessary to show that there are no intermediate subfields with a degree extension of degree 4 or higher. In other words, we must show that the chain of field extensions of degree 2 do exist and none are a higher power of 2. Pinter gives us that there are 2^m ways to permute the roots of $x^{p^k} - 1$. Since these roots form adjoined to \mathbb{Q} form S it follows that the number of automorphisms that fix \mathbb{Q} is equal to the number of these permutations. Thus the Galois Group, the group of these autmorphims, $Gal(S : \mathbb{Q})$, has order 2^m and it is a 2-group. It follows that there exists a chain of subgroups that are order 2 over the previous group. The Fundamental Theorem of Galois Theory gives us that there exists a one to one correspondence between the descending chain of subgroups and an ascending chain of field extensions such that the order of each subgroup over the previous corresponds to the degree of each field extension over the previous. It follows that the chain of field extensions does exist and that n is a regular and constructible n-gon.

6.3 Proof of the Compisition Lemma

Now we must prove another important result in order to finish our proof of Gauss' Theorem.

Theorem 6.5. Regular n and m-gons are constructible if and only if a regular mn-gon is constructible such that (m, n) = 1.

Proof. Let a mn-gon be regular and constructible. It follows that the interior angle $\gamma_{mn} = e^{\frac{2i\pi}{mn}} = \frac{360}{mn}$ is constructible. Thus the complex circle is split into mn even segments. It follows that connecting every m points will yield a regular n-gon and connecting every n points will yield a regular m-gon is constructible then regular m and n-gons are also constructible.

Now we look at the biconditional. Let regular m and n-gons be constructible. It follows that the interior angles $\frac{360}{m}$ and $\frac{360}{n}$ are constructible. Note that (m, n) = 1 thus there exist integers a, b such that am + bn = 1 (Euclidean Algorithm). Thus

$$\frac{360}{mn} = 360 \frac{am+bn}{mn}.$$
$$\frac{360}{mn} = 360 \left(\frac{a}{n} + \frac{b}{m}\right).$$

It follows that the interior angle $\frac{360}{mn}$ is constructible, and thus the regular mn-gon is constructible.

6.4 Example of the Composition Lemma

Let m = 3 and n = 5. It should be readily clear from Figure 35 that connecting every fifth point (H, J, L) creates the equilateral triangle and connecting every third point (H, F', A, G', I) to construct the regular pentagon.



Figure 35: Composition Lemma

Note, in Figure ?? that adding two of the interior angles of the pentagon ($\angle HDI$ and $\angle IDG'$) less one interior angle of the equilateral triangle ($\angle HDL$) result in an interior angle of the regular 15-gon($\angle LDG'$).



Figure 36: Composition Lemma

Figure 37: Completed 15-gon

6.5 Proof of Gauss' Full Result

Now we will use the Composition Lemma to prove Gauss' Full Result. The theorem follows for the readers convenience.

Theorem 6.6. A regular n-gon is constructible if and only if n is of the form

$$n = 2^a p_1 p_2 p_3 \dots p_i$$

where $a \ge 0$ and $p_1, p_2, ..., p_i$ are distinct Fermat Primes.

Proof. We will begin by letting a regular *n*-gon be constructible. It follows from the Composition Lemma that each prime in the composition of *n* is also the number of sides in a regular constructible polygon. Our modified proof of Gauss' Theorem gives us that each regular and constructible *n*-gon where *n* is a power of prime *n* must be either 2^a or a Fermat Prime to the first power. It follows that $n = 2^a p_1 p_2 \dots p_i$ where $a \ge 0$ and p_1, p_2, \dots, p_i are distinct Fermat Primes.

To show the other direction, Let $n = 2^a p_1 p_2 \dots p_i$ where $a \ge 0$ and p_1, p_2, \dots, p_i are distinct Fermat Primes. It follows from our modified proof of Gauss' Theorem that each prime in the factorization of n is a constructible regular polygon. The Composition Lemma gives us that the combination of these primes is also a constructible regular polygon. \Box

It is important to note the manner in which the above proof was built up and remember that as we move into the more complex constructions below. We started with proving Gauss' Result for powers of 2 and Fermat Primes to the first power and then used the Euclidean Algorithm to generalize to combinations of these numbers. In the preceding sections concerning constructions we showed the ability to bisect angles and construct regular n-gons, where n is a Fermat Prime to the first power. In the next section, we will look more closely at the example of the 15-gon above and then use the Euclidean Algorithm to generalize how to construct more complex regular n-gons.

7 Construction of Regular n-gons, where n is not a single Fermat Prime

For this discussion, we will introduce a new definition and delineate between three different forms of n.

Definition 6. A regular n-gon such that $n = p_i$, such that p is a Fermat Prime will be called a prime regular n-gon.

If n is not a prime number it will be called composite. Composites can be made up of multiple Fermat Primes and/or powers of 2. We will look first to the trivial case of those with powers of 2 then look at odd composites.

The first few *n*-gons which are even composites are the 6-gon(n = 2*3), 10-gon(n = 2*5), and 12-gon $(n = 2^2 * 3)$. All *n*-gons of this form can be constructed by constructing the $\frac{n}{2^a}$ -gon and then bisecting the interior angle *a* times. Below is an example of using the regular pentagon to construct a regular 10-gon.



Figure 38: Regular pentagon with regular 10-gon overlaid

Next, we consider the odd composite n-gons. We will start by looking at those in which n is a composition of two Fermat Primes. Since we cannot have a Fermat Prime twice in the prime factorization, our options are

3*5=15	3*17=51	3*257=771
3*65,537=196,611	5*17=85	5*257=1,285
5* 65,537=327,685	17*257=4,369	17*65,537=1,114,129
257*65,537=16,843,009		

We will focus on the details of how to place an equilateral triangle a top of a pentagon in order to construct the regular 15-gon to give us a clear and complete example, then examine the 51-gon, and extrapolate from these two constructions a strategy to construct to the rest

of the regular n-gons, namely n-gons with an unspecified number of Fermat Primes in the factorization.

In order to construct the 15-gon we will need to construct both a regular pentagon and an equilateral triangle that share a vertex, and which are inscribed within the same circle. From this we will get eight of the 15 vertices. The other seven, will come from bisecting the segment between the closest two vertices of the triangle and pentagon, finding this bisectors intersection with the inscribing circle and then copying this length. Below is the step by step construction and proof.

1. Construct a regular pentagon as earlier described.



Figure 39: Regular Pentagon

- 2. Construct a regular equilateral triangle that shares a vertex with our pentagon, namely H. Steps 3 through 5 elaborate on how to do this.
- 3. Draw a segment connecting H and D. Construct a 60 degree angle, HDK, with this as the right leg by finding the intersection of the inscribing circle centered at D and a circle of equal radius centered at H.



Figure 40: Construction of 60 degree angle

- 4. The supplementary angle, HDL, forms an interior angle of 120 degrees. Thus \overline{HL} is one side of an equilateral triangle inscribed in our circle.
- 5. Copying this length once, produces the third vertex, J, and our requisite triangle.



Figure 41: Construction of Equilateral Triangle

- 6. Next, note that a 15-gon will have interior angles of 24°, and that $\angle HDJ = 120^{\circ}$ and $\angle HDF = 72^{\circ}$.
- 7. It follows that $\angle HDJ = 48^{\circ}$.



Figure 42: Angle Measures

8. Bisecting angle FDJ and finding the intersection of the bisecting ray with the circle will lead to the requisite spacing of verticies.



Figure 43: Angle Bisection

- 9. Note, a chord of a circle can be copied by creating a circle of that diameter centered at a end point and finding this intersection with the larger circle.
- 10. Copying this chord \overline{MJ} 15 times yields the regular 15-gon.



Figure 44: Completed Regular 15-gon

This method of placing two prime regular n-gons that are factors of our new regular n-gon on top of each other leads us to a method for construction of all of our regular n-gons. Take for example the 51-gon. Placing an equilateral triangle on top of an already constructed regular 17-gon with one vertex in common will lead to the following picture.



Figure 45: Interior angles of a 51-gon

Note that the requisite interior angle of a 51-gon is equal to $\frac{360}{51}$. Next note that angle LOE_1 is equal to $6 * \frac{360}{17}$ and that angle LOP is equal to 120 degrees. It follows that angle $POE_1 = 6 * \frac{360}{17} - 120 = \frac{360}{51}$. Thus we have the necessary interior angle and can create a 51-gon.

The above method gives us a way to create each n-gon where n only has two Fermat Primes in its prime factorization and one of them is 3. The complicated part begins when it is necessary to construct an overlaying pentagon, 17-gon, 257-gon or 65,537-gon. While the process is essentially the same, the constructions are a long and messy process we will not explore here in depth, but for the curious reader we will discuss briefly.

Use a diameter of the inscribing circle to start your construction. This will result in producing an angle with the required measure. Then use Euclids propositions of construction to copy this angle onto a leg that forms an interior angle of our original shape, so our pentagon, 17-gon, 257-gon or 65,537-gon share a vertex with the shape they are being overlaid on. Then follow the above methods to find an interior angle with requisite measure.

Constructing odd composites with more than 2 factors follows the same pattern; it just has one step more. Below is a discussion of constructing a regular 255-gon as an example of this phenomenon. Refer to Figure 46 for clarification of the below discussion. This construction will require placing an interior angle of 72 degrees into a already constructed 51-gon. Each side of the 51-gon will have 5 vertices of the 255-gon in between them and each side of the pentagon will have 51 vertices. Starting from the shared vertex, 10 of the interior angles of the 51-gon will create an angle equal that is $\frac{360}{255}^{\circ}$ less than 72°. Thus, we have created the requisite interior angle, with that 11th leg from the interior angles of the 51-gon and the second leg of the interior angle of the regular pentagon.



Figure 46: Interior angles of a 255-gon

From this it is possible to continue this pattern of overlaying prime regular n-gons, and finding the new requisite interior angle by subtracting old interior angles, and thus construct all regular n-gons.

8 Theory of Composite Regular *n*-gons

Like with everything on this topic, the theory is seemingly much more elegant than the application. In this section we will prove that all composite regular *n*-gons, such that $n = 2^a p_1 p_2 \dots p_n$ where the *p*s are distinct Fermat Primes to the first power. are constructible by showing that angles of the form $\frac{1}{n}$, the interior angles of our regular *n*-gons, are constructible with the Euclidean Algorithm. We will limit ourselves to $n = 2^0 p_1 p_2 \dots p_j$ since any introduction of a non-zero power of two will just require bisecting at the end. This paper has explicitly shown that the first three prime *n*-gons are constructible and will accept the final two as more complicated examples, but still constructible. Here we look to prove that using these prime regular *n*-gons we construct all composite regular *n*-gons.

Proof. Note, $\gamma_{p_1}, \gamma_{p_2}, \gamma_{p_3}, \gamma_{p_4}$ and γ_{p_5} are constructible angles such that p_1, p_2, p_3, p_4 and p_5 are the Fermat Primes. Consider γ_n where $n = p_1 p_2 \dots p_j$ such that $j \leq 5$. Note all the Fermat Primes are relatively prime to one another. It follows that for any integers i and k such that $1 \leq i, k \leq 5$ that there exist integers l, m such that $1 = lp_i + mp_k$ (Euclidean Algorithm). From earlier results, we can construct angles that are equal to $\frac{360}{p_i}^{\circ}$ and $\frac{360}{p_k}^{\circ}$. Dividing by $p_i p_k$,

$$\frac{360}{p_i p_k} = 360 * \frac{l p_i + m p_k}{p_i p_k}$$

Separating and reducing gives us the following equality,

$$\frac{360}{p_i p_k} = 360 * (\frac{l}{p_i} + \frac{m}{p_k}).$$

Thus when we construct the angle $l\gamma_{p_i} + m\gamma_{p_k}$, we will obtain the desired angle of $\gamma_{p_ip_k}$. Further note, p_ip_k is relatively prime to the rest of the Fermat primes and any power of 2. Thus, the same process can be used as many times as necessary to show that a given $n = 2^a p_1 p_2 \dots p_k$ is constructible from the composition of the prime regular *n*-gons and angle bisection as demonstrated above.

Note, the above is the same argument as the Composition Lemma.

9 Larger Theorem

Now that we have looked at Gauss' Theorem in both construction and in theory, we can shift our attention to a larger and more powerful result, from which Gauss' Theorem follows almost immediately.

Theorem 9.1. If α is a complex number then α , with minimum polynomial p(x) and p(x) has splitting field S, is a geometrically constructible number iff $[S : \mathbb{Q}] = 2^j$ where $j \in \mathbb{Z}^+$.

We will use the following two lemmas in order to prove our larger result.

Lemma 9.2. If α is a geometrically constructible complex number with minimal polynomial p(x), splitting field S and β is another root of p(x), then β is also a geometrically constructible complex number.

Lemma 9.3. If G is a p-group of order p^k , then there exists a descending chain of subgroups from $G = G_0 \supseteq G_1 \supseteq ... \supseteq G_k = \{e\}$ such that for each $i = 0, 1, ..., k, o(G_i) = p^{k-i}$.

This Larger Theorem 9.1 formalizes the need for the existence chain of field extensions of degree 2. When an element, α has a minimum polynomial p(x) and splitting field S it is possible for $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^j$ but $|Gal(S : \mathbb{Q})| \neq 2^m$. For example in a quartic polynomial, this occurs when adjoing a root only allows for the quartic to be reduced to a cubic. Thus the order of the Galois Group is 12 or 24 and the elements of this field are not constructible.

9.1 Two Important Lemmas

Here we prove Lemma 9.2.

Lemma. If α is a geometrically constructible complex number with minimal polynomial p(x), splitting field S and β is another root of p(x), then β is also a geometrically constructible complex number.

Proof. Let α be a geometrically constructible complex number with minimum polynomial p(x) and splitting field S. It follows that there exists a chain of field extensions, starting at the rationals, such that each extension is of degree two over the previous field. For example,

$$\mathbb{Q} \subseteq F_0 \subseteq F_1 \subseteq \ldots \subseteq F_t$$

and

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

It is also important to note that $\alpha \in F_t$ and $\alpha \notin F_{t-1}$.

Another way of thinking of this chain of extensions is that each one has a degree two minimum polynomial over the previous field. For example $x^2 - 2$ has a splitting field of $\mathbb{Q}(\sqrt{2})$ and $\sqrt{2}^2 \in \mathbb{Q}$. By the quadratic formula any element introduced in the new field has its square in the previous field. Let F_i be the extension $F_i = \mathbb{Q}(\delta_1, \delta_2, ..., \delta_i)$. Thus, by our previous statement, $\delta_i \in F_i$ implies that $\delta_i^2 \in F_{i-1}$. Now note, the following important result:

Theorem 9.4. Suppose $F \subseteq L$ are fields, and if $\nu : F \to \mathbb{C}$ is a homomorphism and k = [L : F], then there are exactly k extensions of ν to a homomorphism $\phi : L \to \mathbb{C}$.

Consider the evaluation function E_{α} that maps $\mathbb{Q}[x] \to \mathbb{C}$ by evaluating each polynomial over the rationals at α . The range of this function is $\mathbb{Q}(\alpha)$ and the kernel is generated by the multiples of p(x). The Fundamental Homomorphism Theorem yields that $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(\alpha)$. Next consider the evaluation function, $E_{\beta} : \mathbb{Q}[x] \to \mathbb{C}$. The range in this case is $\mathbb{Q}(\beta)$ and the kernel is still generated by the multiples of p(x). It follows that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(\beta)$. Thus, we have a homomorphism ν , which takes $\mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. Theorem 9.4 allows for an extension of ν to $\phi : F_t \to \mathbb{Q}(\beta)$. This function fixes \mathbb{Q} and moves $\delta_1, \delta_2, ..., \delta_t$. Let $\epsilon_1 = \phi(\delta_1), \epsilon_2 = \phi(\delta_2), ..., \epsilon_t = \phi(\delta_t)$ and note that $\epsilon \in \mathbb{Q}(\beta)$. It follows that $\phi(F_t) = \hat{F}_t = \mathbb{Q}(\epsilon_1, \epsilon_2, ..., \epsilon_t)$. Note, since ϕ is a homomorphism then $\phi(\delta_i^2) = \phi(\delta_i)^2 = \epsilon_i^2$ and that $\beta \in \hat{F}_t$.

Thus, for each $\epsilon_i \in \hat{F}_i$ then $\epsilon_i^2 \in \hat{F}_{i-1}$. It follows that β is a geometrically constructible complex number.

Next we turn to prove Lemma 9.3 which is necessary for the biconditional.

Lemma. If G is a p-group of order p^k , then there exists a descending chain of subgroups from $G = G_0 \supseteq G_1 \supseteq ... \supseteq G_k = \{e\}$ such that for each $i = 0, 1, ..., k, o(G_i) = p^k - i$.

Proof. Let G be a p-group with order p^k . We prove with induction on k. First, we will check for k = 1. Note o(G) = p and $G \cong \mathbb{Z}_p$. Letting $G_1 = \{e\}$ it follows that $o(G_1) = 1$.

Next, we will assume our lemma holds for p^{k-1} . We look to prove our lemma for p^k . Consider G such that $o(G) = p^k$. Let N be a normal subgroup of G with order p. Such a group exists by Cauchy's Theorem on groups and the fact that the center of a p-group contains more than the identity. Note, the quotient group G/N has order p^{k-1} . It follows from our inductive step that there exists a chain of subgroups $G/N = J_0 \supseteq J_1 \supseteq ... \supseteq$ $J_{k-1} = \{eN\}$ such that for each i = 0, 1, ..., k - 1 and $o(J_i) = p^{k-1-i}$. We will use a previous result, which states that if N is a normal subgroup of G and J is a normal subgroup of G/N, then $\overline{J} = \{x \in G : xN \in J\}$ is a normal subgroup of G such that $o(\overline{J}) = o(J)o(N)$. Let $G_k = \{e\}$ and $G_i = \overline{J_i}$. We find that all the G_i s are normal subgroups of G and that $o(G_i) = o(\overline{J_i})o(N) = p^{k-1-i}p = p^{k-i}$. It follows by the Principle of Mathematical Induction that for all k, if G is a p-group of order p^k , then such an ordering of subgroups does exist. \Box

Now that we have these useful lemmas in hand we will turn now to a proof of our larger theorem.

9.2 **Proof of Larger Theorem**

Here we will prove Theorem 9.1.

Theorem. If α is a complex number then α , with minimum polynomial p(x) and splitting field S, is a geometrically constructible number iff $[S : \mathbb{Q}] = 2^j$ where $j \in \mathbb{Z}^+$.

Proof. Let α be a constructible number with minimal polynomial p(x) and splitting field S. It follows from Lemma 9.2 that all other roots, $\beta, \delta, \epsilon, \ldots$ of p(x) are constructible. It follows that we will have a chain of field extensions of degree 2 from the rationals to the fields containing each one of these roots. For simplicities sake, let's assume p(x) has four roots, α, β, δ and ϵ . Consider the chains of field extensions $\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq \mathbb{Q}(a_1, a_2) \subseteq \ldots \subseteq \mathbb{Q}(a_1, a_2, \ldots, a_j); \mathbb{Q} \subseteq \mathbb{Q}(b_1) \subseteq \mathbb{Q}(b_1, b_2) \subseteq \ldots \subseteq \mathbb{Q}(b_1, b_2, \ldots, b_k); \mathbb{Q} \subseteq \mathbb{Q}(d_1) \subseteq \mathbb{Q}(d_1, d_2) \subseteq \ldots \subseteq \mathbb{Q}(d_1, d_2, \ldots, d_l); \mathbb{Q} \subseteq \mathbb{Q}(e_1) \subseteq \mathbb{Q}(e_1, e_2) \subseteq \ldots \subseteq \mathbb{Q}(e_1, e_2, \ldots, e_m)$. The complex numbers, α, β, δ and ϵ , are each in the final fields respectively. Now, consider the field,

$$\mathbb{Q}(a_1, a_2, \dots, a_j, b_1, b_2, \dots, b_k, d_1, d_2, \dots, d_l, e_1, e_2, \dots, e_m),$$

obtained by adjoing each a_i, b_i, d_i or e_i separately. This field extension has degree 2^m over the rationals since each a_i, b_i, d_i or e_i when adjoined separately to the rationals only introduced at most a degree 2 extension. Thus adjoining all of the elements togethe will introduce either a 1 or a 2 in degree with each new element adjoined. The splitting field although not necessarily this large field, is necessarily a subfield of this field. The tower law gives us that the degree of this extension must be equal to a factor of 2^m . It follows that $[S : Q] = 2^j$. This argument generalizes over n roots quite easily with just a few more ellipsies and a nifty application of the Poisson-Littlewood Conjecture.

Next we will turn our attention to the biconditional. Let S be a splitting field for p(x)and $[S:Q] = 2^j$. It follows from Pinter, that there exist 2^j automorphisms that fix \mathbb{Q} and permutate the roots of p(x). Thus, the group of automorphisms of S that fix \mathbb{Q} , contains 2^j elements and can be called, G=Gal(S:Q). It follows that this is a 2-group, or a group which has order equal to a power of 2. By Lemma 9.3, there exists a chain of subgroups from $G = G_0 \supseteq G_1 \supseteq ... \supseteq G_k = \{e\}$ such that $o(G_i) = 2^{k-i}$. The Fundamental Theorem of Galois Theory states that there exists a one to one correspondence between the subgroups of Gal(S:Q) and the intermediate fields between S and \mathbb{Q} . It follows that there exists a chain of field extensions from \mathbb{Q} to S, such that the degree of each extension over the previous is 2. It follows from our definition of constructible numbers that all the roots of p(x), namely α , are in fact constructible.

Thus we have proven our larger theorem. In the next section, we will explore how Gauss' Theorem is merely a specific example of this theorem.

10 Gauss' Theorem as a Case

Here we will prove Gauss' Theorem once again. This time however we will use our larger result as a helping tool in shortening the proof and thus showing how Gauss' Theorem follows directly from this other theorem. We will start with a restatement of Gauss' Theorem followed by the new proof.

Theorem. A regular n-gon is constructible if and only if n is of the form

$$n = 2^a p_1 p_2 p_3 \dots p_i$$

where $a \ge 0$ and $p_1, p_2, ..., p_i$ are distinct Fermat Primes.

Proof. Let n be such that a regular n-gon is geometrically constructible. It follows from the definition of constructibility that the cyclotomic field ζ_n has degree 2^m over the rationals. Note, ζ_n is the splitting field for the polynomial $p(x) = x^n - 1$ over the rationals. Note that each individual root, γ_n , of this polynomial is a geometrically constructible number. Thus our larger theorem yields that, $[\mathbb{Q}(\gamma_n) : \mathbb{Q}] = 2^l$ and the rest of the argument follows algebraically as in our original proof of Gauss' theorem. Now, we turn to the biconditional.

Now we will let $n = 2^a p_1 p_2 \dots p_i$ such that each p_i is a Fermat Prime. Note that n statisfies $\phi(n) = 2^m$. This follows because each Fermat Prime has an Euler Phi Function value that is a power of 2 and $\phi(2^a) = 2^a (1 - \frac{1}{2}) = 2^{a-1}$ and ϕ is multiplicative.

Our earlier result concerning the degree of the cyclotomic field over the rationals can be extended to all n in the following fashion: since these extensions will all be disjoint so the fields would be arranged like this $\mathbb{Q} \subseteq \mathbb{Q}(\omega_1) \subseteq \mathbb{Q}(\omega_1, \omega_2) \subseteq ... \subseteq \mathbb{Q}(\omega_1, \omega_2, ..., \omega_j)$ where $\omega_1, \omega_2, ..., \omega_j$ equal distinct groups of p_i -th roots of unity. The degree of the extensions would be as follows, $[\mathbb{Q}(\omega_1, \omega_2, ..., \omega_j) : \mathbb{Q}(\omega_1, \omega_2, ..., \omega_{j-1}] = \phi(n_j), [\mathbb{Q}(\omega_1, \omega_2, ..., \omega_{j-1}) :$ $\mathbb{Q}(\omega_1, \omega_2, ..., \omega_{j-2}] = \phi(n_{j-1}), ..., [\mathbb{Q}(\omega_1) : \mathbb{Q}] = \phi(n_1)$. The tower law yields that $[\mathbb{Q}(\omega_1, \omega_2, ..., \omega_j) :$ $\mathbb{Q}] = \phi(n_j)\phi(n_{j-1})...\phi(n_1)$.

Thus $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = 2^m$. It follows from our larger result that $\mathbb{Q}(\zeta_n)$ is constructible and thus a regular *n*-gon is constructible.

11 Conclusion

We have explored the many aspects of Gauss' Theorem. We started by looking at the building blocks necessary to form constructions and then the building blocks of the theory. We developed the concept of prime constructible regular n-gons through theory and construction. Next we moved on and used the Euclidean Algorithm and the Composition Lemma to show the complete theory and the constructions. The Composition Lemma highlights the most convergent point of the theory and the construction. This seems to fit with our intuition and mathematical background where prime numbers are these base cases that seem almost to be axiomatic, foundational or without a clear process of arriving at them. The same can be said about prime regular n-gons, the theory and ways of constructing them are unclear and seem to lack a pattern. On the other hand, once these are established, it is possible to combine these in relatively simple ways to get to the rest of the pertinent information just like composing prime numbers to form the rest of the integers.

12 References

- "Constructible Polygon." Art of Problem Solving. Web. 22 Feb 2013.
 < www.artofproblemsolving.com/Wiki/index.php/Constructiblepolygon > .
- Dutch, Steven. "Constructing 17-sided Polygon." Steven Dutch's Home Page. Web. 1 Mar 2013. < www.uwgb.edu/dutchs/pseudosc/17 - gon.HTM > .
- 3. Keef, Pat. Class Notes
- 4. Pinter, Charles. A Book of Abstract Algebra. Second Edition. Mineola, New York: Dover Publications, 1990. Print.
- 5. Sanifer, Ed. "How Euler Did It:Factoring F5." *Mathematical Association of America*. Mathematical Association of America, Web. 15 February 2013.

< www.maa.org/editorial/euler/howeulerdidit41 factoringf5.pdf > .