Ruler and Compass Construction of Regular Polygons

Xavier Mbaale (xavier@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Dr Arnold Keet
Stellenbosch University, South Africa

22 May 2014

Submitted in partial fulfillment of a structured masters degree at AIMS South Africa

Abstract

Among the ancient Greeks, the perfect geometric figures were the circle and straight line. As such, they restricted performing geometrical constructions to two instruments: the ruler and compass. In this essay, we discuss which regular polygons are constructible by ruler and compass. For instance, a regular $p-$gon for p a prime is constructible if p is of the form $2^{2^n}+1$. These primes are known as Fermat primes. But before the development of field theory, Gauss had explicitly constructed a $17-$gon. Therefore as an explicit example of a constructible polygon, we shall describe Gauss's construction of a $17-$gon and explain how it works using Galois theory.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Xavier Mbaale, 22 May 2014

Contents

1. Introduction

The study of constructible regular polygons can be traced back to the time of ancient Greek mathematicians. The Greeks knew how to construct certain regular polygons using a ruler and compass. Despite the Greeks early involvement in constructible regular polygons, it was a German mathematician by the name of Gauss who in 1796 was able to show which regular polygons could be constructible and which ones could not. Gauss was able to show that a $17-$gon could be constructed by ruler and compass. He generalised this idea by showing that for a prime p, a regular $p-$gon was constructible if p was of the form $2^{2^k}+1$, primes known as Fermat primes named after the French mathematician Pierre de Fermat. In order to construct a regular polygon, the number that dictates the vertices of the polygon must be constructible and therefore, in this essay we shall dedicate section 2.1 to discussing constructible numbers.

The Greeks had three classical construction problems: how can we double a cube, is it possible to trisect an angle and can we square a circle. In the case of trisecting an angle, let's say for example we use an angle of 60 degrees. It turns out that this is the same as looking for solutions to the cubic irreducible minimal polynomial given by;

$$\cos 3\beta = 4\cos^3\beta - 3\cos\beta. \tag{1.0.1}$$

Letting $\beta = 20$ and $\cos\beta = y$, then $\cos 3\beta = \frac{1}{2}$ so that equation 1.0.1 becomes $8y^3 - 6y - 1 = 0$ and if $y = 2x$, then we have $x^3 - 2x - 1 = 0$. The cubic roots of this equation are not constructible. As we shall see in this essay, a number is only constructible if the degree of its minimal polynomial is a power of 2. Hence given an arbitrary angle, it is not possible to trisect it. However, there are some particular angles that can be trisected e.g $180°$. This then reduces the study of constructibles to the study of polynomials, which we shall discuss in section 2.2.

The study of polynomials and their roots gave rise to an area of study known as Galois Theory named after mathematician Evariste Galois. Galois Theory can be described as the study of groups formed by permutations and their effects when they act upon roots of a polynomial. To be more formal, let $g(x) \in K[x]$ and L be the splitting field of $g(x)$ over K. Then L/K is a field extension such that $K \subset L$. The set of automorphisms of L that fixes K forms a group under composition denoted by $Aut(L/K)$, with order less than or equal to the degree of the extension denoted by $[L : K]$. These automorphisms permute the roots of $g(x)$ over L. When $|Aut(L/K)| = [L : K]$, the group of automorphisms $Aut(L/K)$ is said to be Galois denoted by $Gal(L/K)$. If a polynomial $g(x)$ is separable over K and splits completely over L, then $Gal(L/K)$ is said to be the Galois group of $g(x)$.

This motivates the study of Galois extensions known as cyclotomic extensions given by $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where ζ_n is a primitive nth root of unity. A cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is the splitting field for the cyclotomic polynomial $x^n - 1 \in \mathbb{Q}[x]$. The roots of the polynomial $x^n - 1$ are fundamental to the constructibility of polygons as they dictate the position of the vertices of polygons. A regular polygon will be constructible if the degree of the minimal polynomial of the primitive nth roots of unity is a power of 2. In general, an $n-$gon is constructible if all its odd factors are distinct Fermat primes.

In Chapter 2, we give the pre-requisite knowledge needed to understand this essay such as constructible numbers, polynomial factorisation, splitting fields and field extensions. Chapter 3 is dedicated to understanding the Galois group and the cyclotomic extension, and in Chapter 4, we describe values of n for which a regular $n-$gon is constructible. As an explicit example, the last part of Chapter 4 shall use Galois Theory to show that a regular $17-$gon is constructible by ruler and compass.

2. Preliminaries

In this Chapter, we discuss the pre-requisite knowledge needed to understand this essay.

2.1 Constructible Numbers

In this section we want to investigate which numbers are constructible. The question we will be answering is, "if we have a line segment of length 1 in the plane , using rule and compass, what lengths or numbers α can we construct?". As such, in this essay, when we say that a number is constructible, we mean it can be constructed by ruler and compass.

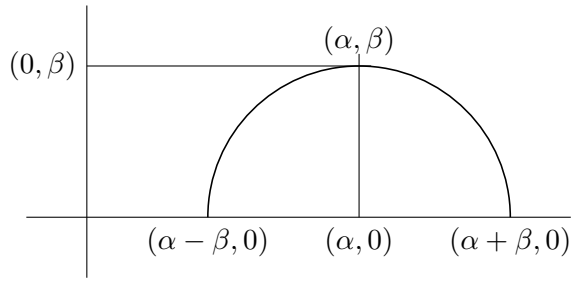
2.1.1 Definition. A number $\alpha \in \mathbb{C}$ is called constructible if a line segment of length $|\alpha|$ is constructible using a finite sequence of compass and ruler constructions beginning with an edge of length 1, where $|\alpha|$ means the absolute value of α.

The construction of every number starts with a length of 1. For example we can construct a number 5 by beginning with a length of 1, and then using rule and compass, we add to the initial length of 1, four more lengths of 1 on a straight edge. From just these simple operations, we see that all natural numbers are constructible. For the case of the construction of a point in the Cartesian plane, we need to start with constructible points $(0,0)$ and $(1,0)$. Thus, if $(\alpha,0)$ is constructible, so is $(0,\alpha)$ since a circle of radius α, with centre origin will cut the y-axis at $(0,\alpha)$. Additionally, if $(\alpha,0)$ and $(\beta,0)$ are constructible, we can construct (α,β) because by drawing a straight line through $(\alpha,0)$ parallel to the $y-$axis and a straight line through $(0,\beta)$ parallel to the $x-$axis, the two lines will meet at (α,β) Howie (2006). Therefore, we can now state the following Lemma that shows some arithmetic that we can perform on these constructible numbers.

2.1.2 Lemma. Let $(1,0)$,$(0,0)$, $(\alpha,0)$ and $(\beta,0)$ be constructible, then $\alpha+\beta$, $\alpha-\beta(\alpha>\beta)$, $\alpha\beta$ and if $\beta \neq 0$, $\frac{\alpha}{\beta}$ are constructible.

Proof. Some ideas in the proof of this Lemma are adopted from (Stewart, 1973). Since $(\alpha,0)$ and $(\beta,0)$ are constructible, then (α,β) is constructible as described above. To show that $\alpha+\beta$ and $\alpha-\beta$ are constructible, draw a circle with centre $(\alpha,0)$ passing through (α,β). This circle meets the $x-$axis at points $(\alpha-\beta,0)$ and $(\alpha+\beta,0)$, hence these points are constructible.

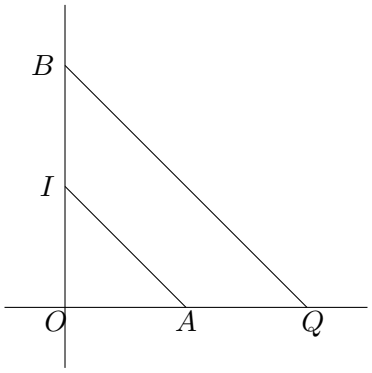
Figure 2.1: Shows the construction of $\alpha+\beta$ and $\alpha-\beta$



To show that $\alpha\beta$ is constructible, let $A=(\alpha,0)$, $B=(0,\beta)$ and $I=(0,1)$. Then draw the straight line from B and parallel to the line AI. Let $Q=(x,0)$ be the point where this line intercepts the $x-$axis

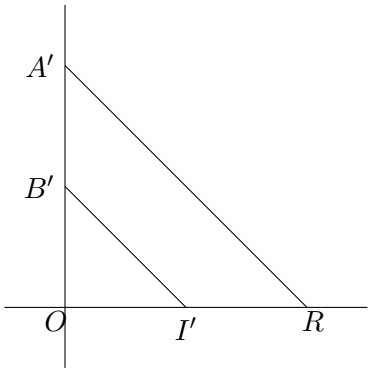
as shown the diagram below

Figure 2.2: Shows the construction of $\alpha\beta$



By similarities of $\triangle OAI$ to $\triangle OQB$, $\frac{OI}{OA} = \frac{OB}{OQ}$. This implies that $x = \alpha\beta$. Hence $\alpha\beta$ is constructible. We finally show that $\frac{\alpha}{\beta}$ is constructible. Let $I' = (1, 0), B' = (0, \beta)$ and $A' = (0, \alpha)$. Then draw a line from A' and parallel to $B'I'$ meeting the x-axis at a point $R(x, 0)$ as shown in the diagram below

Figure 2.3: Shows the construction of $\frac{\alpha}{\beta}$



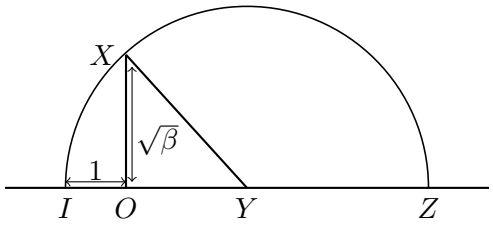
By similarities of $\triangle OB'I'$ to $OA'R$, $\frac{OB'}{OI'} = \frac{OA'}{OR}$, then $x = \frac{\alpha}{\beta}$. Hence $\frac{\alpha}{\beta}$ is constructible. □

It is important at this point to note that we can subtract, multiply, add and divide (with non zero numbers) constructible numbers and still get another constructible number. Therefore, we see that all rational numbers are constructible. In fact, the set of constructible numbers form a field. But the question is, are these the only operations we can perform on constructible numbers? It turns out that we still have another operation. We can find the square root of a constructible number as illustrated in the following Lemma.

2.1.3 Lemma. If a number $\beta > 0$ is constructible, then its square root $\sqrt{\beta}$ is constructible.

Proof. (Skorobogatov, 2006). On the the same axis (say the x-axis), construct adjacent segments of length $\beta = |OZ|$ and $1 = |OI|$ and let Y to be the midpoint of ZI. Draw a circle centred at Y with radius YZ. Draw a line perpendicular to ZI from O and call its intersection with the circle X as shown in the diagram below.

Figure 2.4: Shows the construction of $\sqrt{\beta}$



Then $|XY| = \frac{\beta+1}{2}$ and $|OY| = |IY| - 1 = \frac{\beta+1}{2} - 1 = \frac{\beta-1}{2}$. And by Pythagoras' theorem,

$$|OX| = \sqrt{\left(\frac{\beta+1}{2}\right)^2 - \left(\frac{\beta-1}{2}\right)^2} = \sqrt{\beta}.$$

Hence the square root of a constructible number can be constructed. □

With the square root operation on constructible numbers, we observe that if α, β and $e > 0 \in \mathbb{Q}$ are constructible, so is $\alpha + \beta\sqrt{e}$ and the set of all numbers of the form $\alpha + \beta\sqrt{e}$ form a field. This field is called the extension of $\mathbb{Q}$ by $\sqrt{e}$ and is denoted by $\mathbb{Q}(\sqrt{e})$. If $\sqrt{e} \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{e}) = \mathbb{Q}$, but if $\sqrt{e} \notin \mathbb{Q}$, then $\mathbb{Q} \subset \mathbb{Q}(\sqrt{e})$. In the latter case, $\mathbb{Q}(\sqrt{e})$ is called a quadratic extension of $\mathbb{Q}$.

Therefore, we can then say a number is constructible if that number can be obtained or calculated from rationals by a finite sequence of rational operations i.e additional, subtraction, division (by non-zero number) and multiplication and the square root operation.

2.1.4 Example. The number $\sqrt[4]{7+\sqrt{5+3\sqrt{11}}}$ can be constructible by using the following sequence,

$$11, \sqrt{11}, \sqrt{11}+\sqrt{11}+\sqrt{11} = 3\sqrt{11}, 5, 5+3\sqrt{11}, \sqrt{5+3\sqrt{11}}, 7, 7+\sqrt{5+3\sqrt{11}},$$
$$\sqrt{7+\sqrt{5+3\sqrt{11}}}, \sqrt{\sqrt{7+\sqrt{5+3\sqrt{11}}}} = \sqrt[4]{7+\sqrt{5+3\sqrt{11}}}.$$

The following Lemma gives the conditions for which a number can be constructible.

2.1.5 Lemma. A number α is constructible if there exists a finite sequence of fields $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$ with $\alpha \in K_n$ such that for $0 \leq i \leq n-1$, K_{i+1} is a quadratic extension of K_i, i.e $[K_{i+1} : K_i] = 2$

Proof. We shall prove by induction on n. Suppose $n = 0, \Rightarrow \alpha \in \mathbb{Q}$, hence constructible. Now suppose α is constructible for all $n \leq r$, we want to show that α is constructible if $\alpha \in K_{r+1}$. $\alpha \in K_{r+1} \Rightarrow \alpha = c + d\sqrt{e}$, where $c, d, e \in K_r$. But by hypothesis, c, d and e are contructible and hence $c + d\sqrt{e} \in K_{r+1}$ is constructible. □

2.2 Polynomial Factorization

Let K be a field. Then $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in K[x]$, where $a_j \in K, j = 0, 1, \ldots, d$ is called a polynomial in one variable x and the a_j are called the coefficients of f. The degree of

such a polynomial denoted by deg $f(x)$ is the highest exponent of x with a non-zero coefficient . The coefficient a_j corresponding to the degree of the polynomial is referred to as the leading coefficient. If the leading coefficient of f is 1, then the polynomial is said to be monic. We say that an element r is a root of a polynomial f if $f(r) = 0$.

2.2.1 Definition. If we have a field K and p be the smallest integer such that $\overbrace{1+1+\cdots+1}^{p \text{ summands}} = 0$. Then K is said to have characteristic p. The field K is said to be of characteristic zero if such a p does not exist. We denote the characteristic of a field K by $charK$.

2.2.2 Definition. Let $p(x), r(x) \in K[x]$, where deg $r(x) \leq$ deg $p(x)$. We say that $r(x)$ divides $p(x)$ if there exists $h(x) \in K[x]$ such that $p(x) = r(x)h(x)$.

2.2.3 Theorem. *Let K be a field and $p(x) \in K[x]$, then a number β is a root of a polynomial p if and only if $(x - \beta)$ divides p.*

Proof. We use the approach by (Howie, 2006). Suppose $(x-\beta)|p$ (where $(x-\beta)|p$ means $x-\beta$ divides p), then we show that β is a root of p. If $(x - \beta)|p, \Rightarrow p(x) = (x - \beta)r(x)$ with deg $r(x) =$ deg $p(x) - 1$. Now $p(\beta) = (\beta - \beta)r(\beta) = 0r(\beta) = 0$. Hence β is a root of p.

Conversely, suppose β is a root of $p(x)$, we want to show that $(x - \beta)|p$. Suppose $(x - \beta) \not| p$, then by the Euclidean division algorithm, there exists $r(x), h(x) \in K[x]$ such that $p(x) = (x - \beta)r(x) + h(x)$, where deg $h(x) < 1$. But since β is a root of $p(x)$, then $0 = p(\beta) = (\beta - \beta)r(\beta) + h(\beta), \Rightarrow h(x) = 0$ for all x and thus $p(x) = (x - \beta)r(x)$. Therefore $x - \beta$ divides $p(x)$. □

2.2.4 Definition. A polynomial, with coefficients in a commutative ring K is said to be irreducible over K if it is not invertible nor zero and cannot be factored into the product of two non-invertible polynomials with coefficients in K.

2.2.5 Example. Over the ring $\mathbb{Z}$ of integers, the polynomial $4x^2-2$ is reducible since $4x^2-2 = 2(2x^2-1)$ and the factor 2 is not invertible in integers. However, the polynomial $t^2 - 3$ is irreducible over $\mathbb{Z}$ since it cannot be expressed as a linear product polynomials in $\mathbb{Z}$. This is because the polynomial $t^2 - 3$ has no roots in $\mathbb{Z}$. But it is reducible over $\mathbb{R}$ because in $\mathbb{R}$

$$t^2 - 3 = (t - \sqrt{3})(t + \sqrt{3}).$$

Therefore, we see that reducibility depends on the commutative ring or field in question. Given a polynomial in a field K, it is not so easy to see whether it is not irreducible or reducible. Thus we now discuss results that will help determine when a polynomial is irreducible and when it is not.

2.2.6 Lemma (Gauss's Lemma)**.** Let $p(x) \in \mathbb{Z}[x]$ be a polynomial irreducible over $\mathbb{Z}$, then $p(x)$, considered as a polynomial over $\mathbb{Q}$ is also irreducible over $\mathbb{Q}$.

Proof. For the proof of this Lemma, see page 22 of (Stewart, 1973) □

2.2.7 Remark. The factorization of a polynomial over $\mathbb{Z}$ just means factorization over $\mathbb{Q}$. Therefore, if we have a polynomial over $\mathbb{Z}$ and it is irreducible over $\mathbb{Z}$, it follows immediately from this Lemma that that polynomial will be irreducible over $\mathbb{Q}$.

2.2.8 Lemma. Let $g(x) \in K[x]$ be an irreducible polynomial over the field K. If f and h are polynomials over K such that $g|fh$, then either g divides f or g divides h.

The proof has been omitted but can be found on pages 20-21 of (Stewart, 1973).

2.2.9 Theorem. *Every polynomial which is non zero over the field K is a product of irreducible polynomials over K. This factorisation of polynomials over K into irreducible polynomials is unique up to constant factors and the order in which the factors are written.*

Proof. The approach taken in this proof is according to (Stewart, 1973) and (Howie, 2006). We shall prove by induction on the degree n of the polynomial $g(x) \in K[x]$. Suppose $n = 0$ or 1, then the result is obvious. If $n > 1$, then either $g(x)$ is irreducible, for which case we are done or $g(x) = p(x)h(x)$, with degree $h(x), p(x) <$ degree $g(x)$. Then by induction $p(x)$ and $h(x)$ are products of irreducible polynomials. Hence g is a product of irreducible polynomials over K.

To prove uniqueness, lets suppose $g = f_1 \dots f_r = h_1 \dots h_s$ where the polynomials $f_1, \dots, f_r, h_1, \dots, h_s$ are irreducible over K. suppose all the f_i are constant, then $g \in K$ and all h_js are constants. Otherwise, we can assume no f_i is a constant (this can be done by dividing all terms that are constants). Thus $f_1 | h_1 \dots h_s$ and by Lemma 2.2.8, $f_1 | h_i$ for some i. Without any loss of generality, assume $i = 1$, then $f_1 | h_1$. But f_1 and h_1 are irreducible, and f_1 is not a constant multiple. So $f_1 = a_1 h_1$, where a_1 is a constant. In the similar way, $f_2 = a_2 h_2, \dots, f_r = a_r h_r$, where $a_2, \dots, a_r$ are constants. If $s > r$, the h_j for $j > r$ must be constants or else degree of $h_1 \dots h_s$ would be higher. Hence the proof. □

2.2.10 Theorem (Eisenstein's Irreducibility Criterion)**.** *Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ be a polynomial over $\mathbb{Z}$. If there is a prime p such that,*

(i) $p \not| a_n$.

(ii) $p | a_i, i = 0, 1, \dots, n-1$.

(iii) $p^2 \not| a_0$.

Then f is irreducible over $\mathbb{Q}$.

Proof. For this proof, we shall use the approach in (Howie, 2006). By Lemma 2.2.6, we only need to show that f, is irreducible over $\mathbb{Z}$. Suppose f is reducible in $\mathbb{Z}$, then $f = hg$, where

$$h = b_s x^s + b_{s-1} x^{s-1} + \dots + b_1 x + b_0$$
$$g = c_r x^r + c_{r-1} x^{r-1} + \dots + c_1 x + c_0.$$

with $s + r = n$ and $s, r < n$. Then observe that $a_0 = b_0 c_0$ and since $p | a_0 \Rightarrow p | b_0 c_0$. But $p^2 \not| a_0$, which implies that either $p | b_0$ or $p | c_0$ and not both. Without any loss of generality, suppose $p | b_0$ but $p \not| c_0$. Now $a_n = b_s c_r$ and $p \not| a_n$, which implies that $p \not| b_s c_r$. If all the b_is are divisible by p, then a_n will be divisible by p which will be a contradiction to part i. Now let b_i be the first coefficient of h such that $p \not| b_i$. Then comparing the coefficients of x^i in the equation $f = gh$, on the left a_i is divisible by p but on the right,

$$a_i = b_0 c_i + b_1 c_{i-1} + \dots + b_i c_0, \quad \text{where} \quad i \leq s < n.$$

which is not divisible by p since if it were p must divide c_0. This is because $p | b_k$ $k = 0, 1, \dots, i-1$ but not b_i. Hence a contradiction. Therefore f is irreducible. □

2.3 Field Extensions

As earlier observed, quadratic field extensions are fundamental to the theory of constructibility. Therefore, in this section, we shall discuss extensions of fields.

2.3.1 Definition. Given a field L containing a subfield K, we say that L is an extension field of K, denoted by L/K and say " L over K".

Here, L/K does not mean quotient of L by K but just describes the relation of L with K as a field.

2.3.2 Definition. A simple extension is an extension L/K having the property that $L = K(\alpha)$ for some $\alpha \in L$.

2.3.3 Definition. Let $K(\alpha)/K$ be a simple extension. If there exist a non-zero polynomial p over K such that $p(\alpha) = 0$, then α is an algebraic element over K and the extension is a simple algebraic extension. Otherwise α is transcendental over K and $K(\alpha)/K$ is a simple transcendental extension.

2.3.4 Definition. An extension L/K is algebraic if every element of L is algebraic over K.

If K and L are fields and $K \subset L$, then L is said to be a field extension of K. In which case one can view L as a vector space over K.

2.3.5 Definition. The dimension of the vector space L over K is called the degree of the extension and it is denoted by $[L : K]$. The degree of the extension is said to be finite if $[L : K] = n < \infty$.

2.3.6 Example. $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$, since the basis of $\mathbb{Q}(\sqrt[4]{3})$ over $\mathbb{Q}$ is $\left\{1, \sqrt[4]{3}, \left(\sqrt[4]{3}\right)^2, \left(\sqrt[4]{3}\right)^3\right\}$. Similarly, the degree $[\mathbb{Q}(\sqrt{3}, \sqrt{2}, \sqrt{5}) : \mathbb{Q}] = 8$, since the basis of $\mathbb{Q}(\sqrt{3}, \sqrt{2}, \sqrt{5})$ over $\mathbb{Q}$ is

$$\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{30}\right\}.$$

All these elements are linearly independent and hence form basis. See (Hadlock, 2000) for details of why these are bases.

However, this is not a convenient way of finding the degree of a field extension. We now develop a way of finding the field extension by means of using minimal polynomial.

2.3.7 Definition. Let L/K be a field extension and $\alpha \in L$ be algebraic over K. Then the minimal polynomial of α over K is the monic polynomial f over K of smallest degree such that $f(\alpha) = 0$. Its degree is called the degree of α over K denoted by $\deg_K \alpha$.

2.3.8 Theorem. *Let $f \in \mathbb{Q}[x]$ and suppose $f(\alpha) = 0$. Then f is the minimal polynomial for α over $\mathbb{Q}$ if and only if f is irreducible over $\mathbb{Q}$.*

Proof. (Howie, 2006). Suppose f is the minimal polynomial for α over $\mathbb{Q}$, we want to show that f is irreducible over $\mathbb{Q}$. Suppose f is reducible, then $f = gh$, where deg $g, h <$ deg f. But then it implies that $0 = f(\alpha) = g(\alpha)h(\alpha)$. Therefore, either $g(\alpha) = 0$ or $h(\alpha) = 0$ which is a contradiction to the minimality of f. Hence f is irreducible.

Conversely, suppose f is irreducible , we show that f is minimal. Let g be the minimal polynomial of α such that $g(\alpha) = 0$. Then we can write $f = gh + r$, where deg $r <$ deg g. Now $0 = f(\alpha) = g(\alpha)h(\alpha) + r(\alpha)$, $\Rightarrow r(\alpha) = 0$ but since g is minimal $r = 0$ and therefore, $f = gh$. Now since f

is irreducible and g is minimal, it implies that h must be a constant. Hence, since deg $g \geq 1$ and is minimal, then deg $g =$ deg f and thus f is the minimal polynomial. □

2.3.9 Theorem. *If α is algebraic over K, then $[K(\alpha) : K] = deg_K \alpha$. If α is transcendental over K, then $[K(\alpha) : K] = \infty$.*

The proof has been omitted but it can be found on pages 74-75 of (Hadlock, 2000). However we illustrate the idea behind the theorem in the following example.

2.3.10 Example. In example 2.3.6, the minimum polynomial of $\sqrt[4]{3}$ is $x^4 - 3$ which is irreducible over $\mathbb{Q}$ by Theorem 2.2.10 where $p = 3$ and we say that it is Eisenstein at 3. Therefore, the degree of the extension $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$, which is the degree of its minimal polynomial.

2.3.11 Theorem. *Let K, E and L be fields such that $K \subset E \subset L$. Then $[L : K] = [L : E][E : K]$.*

Proof. This proof is adapted from (Howie, 2006). Without any loss of generality, let $e_1, e_2, \ldots, e_r$ be the basis of L over E and $k_1, k_2, \ldots, k_m$ be a basis of E over K. Then both e_is and k_js are respectively linearly independent. Now we need to show that rm vectors $e_i k_j$ for $1 \leq i \leq r$, $1 \leq j \leq m$ are linearly independent vectors of L over K. Suppose a finite linear combination of these rm vectors is equal to zero, i.e

$$\sum_{i=1}^{r} \sum_{j=1}^{m} (a_{ij} k_j)\, e_i = 0, \quad a_{ij} \in \mathbb{K}.$$

But the e_is are linearly independent over E, then it follows that for each i, $\sum_{j=1}^{m} a_{ij} k_j = 0$. Also the linear independence of the k_js implies that each $a_{ij} = 0$. Therefore, the elements $e_i k_j$ are linearly independent.

We can now take the e_is and k_js as defined earlier to be the spanning sets for their respective vector spaces. Hence it only remains to be shown that the set of rm vectors $e_i k_j$ span L over K. Let $x \in L$ be an arbitrary element. Since the vectors $e_1, e_2, \ldots, e_r$ form a basis for L over E, $\exists \beta_1, \beta_2, \ldots, \beta_r$ of E such that

$$x = \sum_{i=1}^{r} \beta_i e_i, \quad \beta_i \in E. \tag{2.3.1}$$

But the $\beta_i \in E$ can be expressed as

$$\beta_i = \sum_{j=1}^{m} a_{ij} k_j, \quad a_{ij} \in K. \tag{2.3.2}$$

Thus equations 2.3.1 and 2.3.2 implies that

$$x = \sum_{j=1}^{m} \sum_{i=1}^{r} a_{ij} k_j e_i,$$

which represents a linear combination over K of the $e_i k_j$ and hence spanning L over K. □

As a consequence, we have the following corollary that generalizes this result.

2.3.12 Corollary. Let $K_n \supset K_{n-1} \supset \cdots \supset K_1 \supset K_0$ be a finite sequence of field extension, then $[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \ldots [K_1 : K_0]$.

2.3.13 Example. The degree of the extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ can be found by finding intermediate fields $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(\sqrt{2})$. Since

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i),$$

then

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

But it can be shown that $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ since $i \notin \mathbb{Q}(\sqrt[4]{2})$, $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$ since $(\sqrt{2})^{\frac{1}{2}} \notin \mathbb{Q}(\sqrt{2})$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since $\sqrt{2} \notin \mathbb{Q}$. Therefore,

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 2^3 = 8.$$

Having established all these results, we can now state one of the important results about constructible numbers.

2.3.14 Theorem. *If α is constructible, then $\deg_{\mathbb{Q}}\alpha$ must be a power of 2.*

Proof. (Hadlock, 2000). Since α is constructible, then there exits a finite sequence of field extensions

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

such that $\alpha \in K_n$ and for each i, K_{i+1} is quadratic extension of K_i. Thus $[K_{i+1} : K_i] = 2$ and by Corollary 2.3.12 $[K_n : \mathbb{Q}] = 2^n$. Now since $\alpha \in K_n$, then $\mathbb{Q}(\alpha) \subset K_n$ and thus we have that

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Since $[K_n : \mathbb{Q}] = 2^n$, then both $[K_n : \mathbb{Q}(\alpha)]$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ are powers of 2. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ must be a power of 2 and we know that this equals $\deg_{\mathbb{Q}}\alpha$. □

2.4 Splitting Fields

2.4.1 Definition. If K is a field and p is a polynomial over K, then p splits over K if p can be written as a product of linear factors $p(z) = a(z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_s)$, where $a, \alpha_1, \alpha_2, \ldots, \alpha_s \in K$.

2.4.2 Definition. Let L/K be a finite field extension and $f(x) \in K[x]$. Then the extension L of K is said to be the splitting field of f over K if f splits over L and f never split overs any proper subfield E of L.

Given a field K and a polynomial $f \in K[x]$, we can always construct an extension L over K such that f splits in L. This is done by adjoining to K, the roots of f not in K i.e $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f such that $\alpha_1, \alpha_2, \ldots, \alpha_n \notin K$.

2.4.3 Example. We determine the splitting field over $\mathbb{Q}$ of the polynomial $(x^3 - 1)(x^2 + 2)$. In $\mathbb{C}$, the polynomial $(x^3 - 1)(x^2 + 2)$ factorizes as follows:

$$(x^3 - 1)(x^2 + 2) = (x - 1)\left(x + \frac{1 - i\sqrt{3}}{2}\right)\left(x + \frac{1 + i\sqrt{3}}{2}\right)\left(x - i\sqrt{2}\right)\left(x + i\sqrt{2}\right).$$

Therefore, the field $\mathbb{Q}\left(\frac{1-i\sqrt{3}}{2}, i\sqrt{2}\right) = \mathbb{Q}(i\sqrt{3}, i\sqrt{2}) \subseteq \mathbb{C}$ is the splitting field of the polynomial $(x^3 - 1)(x^2 + 2)$.

If we have a monic irreducible polynomial g over a field E, then we can write $F = E[x]/ < g(x) >$ and F is a field . In fact, the field $F = E[x]/ < g(x) >$ is an algebraic extension $E[\beta]$ of E and is simple. Additionally, $g(x)$ is the minimal polynomial of $\beta = x+ < g(x) >$ over E.

2.4.4 Theorem. *If E is any field and f is any polynomial over E with degree m, then there exits a splitting field F for f over E.*

Proof. We use the approach from (Howie, 2006). Let g be an irreducible factor of f (g may be f itself). Let $F_1 = E[x]/ < g(x) >$ be a field where $g(x)$ is the minimal polynomial of $\beta = x+ < g(x) >$ over E, then $g(\beta) = 0$. Therefore, g has a linear factor $x - \beta$ in $F_1[x]$.

Proceeding by induction, suppose for each i in $\{1, 2, \ldots, m-1\}$, we can construct an extension F_i of E such that f has atleast i linear factors in $F_i[x]$. Then in $F_i[x]$,

$$f = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_i)h, \quad \text{where deg} \quad h = m - i.$$

Repeating the process described in the preceding paragraph, we can construct an extension F_{i+1} of F_i in which h has a linear factor $x - \beta_{i+1}$. Therefore by induction, there exists a field F_m such that f splits over F_m. Thus letting $F = E(\beta_1, \beta_2, \ldots, \beta_m) \subseteq F_m$ where $\beta_1, \beta_2, \ldots, \beta_m$ (not necessary distinct) are roots of f in F_m. Then f splits over F and can not split over any proper subfield of F. □

It is important to note here that splitting fields are unique up to isomorphism as illustrated in the following Theorem.

2.4.5 Theorem. *If E and E' are fields, and $\phi : E \longrightarrow E'$ is an isomorphism, then an isomorphism $\phi' : E[x] \longrightarrow E'[x]$ extends ϕ. Let $g \in E[x]$, and let F, F' be splitting fields of g over E and $\phi'(g)$ over E' respectively. Then there is an isomorphism $\phi^* : F \longrightarrow F'$ extending ϕ.*

This proof has been omitted but can be found on pages 81-82 of (Howie, 2006).

3. Understanding The Galois Group and Cyclotomic Extensions

3.1 Galois Group

3.1.1 Definition. An extension L/K is a normal extension if L is the splitting field of a polynomial over K.

3.1.2 Example. The extension $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ is not normal. Consider the minimal polynomial of $\sqrt[4]{2}$, which is x^4-2 . This polynomial is irreducible since it is Eisenstein at 2 but x^4-2 does not have all its roots in $\mathbb{Q}\left(\sqrt[4]{2}\right)$. Nevertheless, it is possible to make this extension normal by ensuring that all the roots of the minimal polynomial x^4-2 are in the extension. In $\mathbb{C}$, the polynomial x^4-2 splits as follows:

$$\left(x-i\sqrt[4]{2}\right)\left(x+i\sqrt[4]{2}\right)\left(x-\sqrt[4]{2}\right)\left(x+\sqrt[4]{2}\right).$$

Therefore $\mathbb{Q}\left(\sqrt[4]{2},i\sqrt[4]{2}\right)=\mathbb{Q}\left(\sqrt[4]{2},i\right)$ is the splitting field for x^4-2 and thus $\mathbb{Q}\left(\sqrt[4]{2},i\right)/\mathbb{Q}$ is a normal extension.

3.1.3 Definition. Let g be an irreducible polynomial in $K[x]$ with roots in the splitting field L of g. Then g is separable over K if its roots are distinct in the splitting field of g. Otherwise it is inseparable.

A polynomial with roots of multiplicity greater than 1 in its splitting field is not separable.

3.1.4 Definition. If L/K is an algebraic extension, then an element $\alpha\in L$ is separable over K if its minimal polynomial over K is separable over K and the algebraic extension L/K said to be a separable extension if every $\alpha\in L$ is separable over K.

3.1.5 Example. In example 3.1.2, the irreducible polynomial x^4-2 is separable over $\mathbb{Q}$ since all its roots over the splitting field $\mathbb{Q}(\sqrt[4]{2},i)$ are distinct. And also the extension $\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}$, is a separable extension.

3.1.6 Proposition. Every irreducible polynomial g over K is separable if K is a field of characteristic 0.

Proof. A more detailed proof can be found on pages $110-111$ of (Howie, 2006). Let $g(x)=b_0+b_1x+\cdots+b_nx^n$ be an irreducible polynomial over K with deg $g=n\geq 1$. Suppose that $g\in K[x]$ is not separable then $g(x)$ and $g'(x)$ have a common factor r and this factor will be degree atleast 1 in both $g(x)$ and $g'(x)$. Due to irreducibility of g, the factor r must be a constant multiple of g and r will divide $g'(x)$ only if $g'(x)=b_1+2b_2x+\cdots+nb_nx^{n-1}$ is a zero polynomial. Therefore, $b_1=2b_2=\cdots=nb_n=0$ and since K has $char\ 0$, it follows that g must be constant polynomial b_0 and hence a contradiction since deg $g=n\geq 1$. Therefore, g over K must be separable. □

Therefore, when working in a field with characteristic 0, we shall not worry about separability.

If L is a finite extension of a field K, then an automorphism σ of L is said to be a $K-$automorphism if $\sigma(x)=x$, $\forall x\in K$. The collection of all these automorphisms of L over K form a group under

composition and it is denoted by $Aut(L/K)$. The order of $Aut(L/K)$ is $\leq [L : K]$. However, the following theorem gives a necessary condition for $|Aut(L/K)| = [L : K]$.

3.1.7 Theorem. *If L/K is the splitting field of a separable polynomial $f(x) \in K[x]$, then $|Aut(L/K)| = [L : K]$.*

The proof to this theorem has been omitted but can be found on page 8 of (Conrad, 2010). However, we observe from this result that there is a strong link between the roots of a polynomial and the group of automorphisms over a field. Recall that two roots of a polynomial are conjugates of each other if they have a common minimal polynomial over a field. If $f(x)$ is a polynomial over K which splits in L, then the $K-$automorphisms of L permute the roots, also known as the $K-$conjugates of $f(x)$ in L. But for a separable polynomial, all the roots are distinct and so there will be distinct automorphisms equal to the number of roots and the number of these roots is equal to the degree of the extension.

3.1.8 Definition. If order $Aut(L/K) = [L : K]$, then L is a Galois extension of K and $Aut(L/K)$ is called the Galois group denoted by $Gal(L/K)$.

We can therefore now state the following Theorem that gives the necessary and sufficient condition for a finite extension to be Galois.

3.1.9 Theorem. *Let L be a finite extension over K. Then L is Galois over K if and only if L is the splitting field of a separable polynomial over K.*

Therefore, the extension L/K is Galois if it is both a separable and normal extension. Behind the main results of the Galois extension are the following correspondences between intermediate fields and subgroups of $Gal(L/K)$. Let H be a subgoups of the group $Aut(L/K)$ and E be an intermediate field $K \subset E \subset L$. Then for each subfield E, we define a group

$$Aut(L/E) = \{\sigma \in Aut(L/K) | \sigma(x) = x, \forall x \in E\}. \tag{3.1.1}$$

In fact, $Aut(L/E)$ is a subgroup of $Aut(L/K)$. Certainly Aut(L/E) is non empty since the identity $i \in Aut(L/E)$ and $i(x) = x, \forall x \in E$. Also since $K \subset E$, then every automorphism that fixes E automatically will fix $K, \Rightarrow Aut(L/E) \subset Aut(L/K)$ and for $\sigma, \tau \in Aut(L/E)$.

$$\begin{aligned} \sigma\left(\tau^{-1}(z)\right) &= \sigma\left(\tau^{-1}(\tau(z))\right), \quad \text{since} \quad \tau(z) = z \\ &= \sigma(z) = z. \end{aligned}$$

Therefore, $\sigma\tau^{-1} \in Aut(L/E)$ and hence $Aut(L/E)$ is a subgroup of $Aut(L/K)$. Also, for each subgroup H of $Aut(L/K)$, we can define a field

$$L^H := \{c \in L | \sigma(c) = c, \forall \sigma \in H\}. \tag{3.1.2}$$

This is a subfield of L because if we have $a, b \neq 0 \in L^H$ and $\sigma \in H$, $\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$ then $a - b \in L^H$. Also

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)\left(\sigma(b)\right)^{-1} = a(b)^{-1} = ab^{-1}.$$

Hence $ab^{-1} \in L^H$. Since every automorphism of $Aut(L/K)$ fixes K, then $K \subseteq L^H$. This correspondence established in 3.1.1 and 3.1.2 between intermediate field E of the extension L/K, $E \rightsquigarrow Aut(L/E)$ and subgroups of $Gal(L/K), H \rightsquigarrow L^H$ are inclusion-reversing. Therefore if E and E' are subfields of L such that $K \subset E \subset E' \subset L$ then $Aut(L/E) \supseteq Aut(L/E')$. Also If H and H' are subgroups of

$Aut(L/K)$ such that $H \subseteq H'$, then $L^H \supseteq L^{H'}$. For a finite field extension L/K, we have so far established that

$$E \subseteq L^{Aut(L/E)} \quad \text{and} \quad H \subseteq Aut(L/L^H). \tag{3.1.3}$$

In fact, if the finite extension L/K is a Galois extension, then $L^{Gal(L/E)} = E$ and $|Gal(L/K)| = [L : K]$. Therefore, we now sate the following theorem that gives properties of a finite extension which is Galois.

3.1.10 Theorem. *A finite extension L/K that satisfies the following equivalent statements is Galois:*

(i) $Aut(L/K) = [L : K]$,

(ii) $L^{Aut(L/K)} = K$,

(iii) L/K *is separable and normal,*

(iv) L *is the splitting field over* K *of as separable polynomial.*

The proof has been omitted but can be found in (Hadlock, 2000).

3.1.11 Theorem. *Let L/K be a finite Galois extension and $K \subset E \subset L$, then the extension L/E is Galois.*

Proof. Since L/K is a Galois extension and $K \subset E \subset L$, then L/K is separable and normal. Now a minimal polynomial of any element of L over E divides its minimal polynomial over K and therefore, there is preservation of separability and normality from L/K to L/E. □

3.1.12 Remark. Let $K \subset E \subset L$, then the extension E/K need not be Galois when the extension L/K is Galois.

3.1.13 Example. The extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is Galois and one can easily see that $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$, but the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois. This is because the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is neither normal nor separable.

After developing all these ideas about the Galois group, we now state the following theorem known as the Fundamental theorem of Galois theory which gives a glimpse of the structure we have been discussing.

3.1.14 Theorem (The Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite Galois extension and $G = Gal(L/K)$. The maps*

$$E \rightsquigarrow Gal(L/E) \quad i.e\,\{\text{automorphisms of } G \text{ that fix } E\} \text{ and}$$
$$H \rightsquigarrow L^H \quad i.e\,\{\text{elements of } L \text{ fixed by } H\}$$

between a subfield E of L that contains K and a subgroup H of G forms a one to one correspondence i.e $(E = L^H, H = Gal(L/E))$ and satisfies the following properties:

(a) $|H| = [L : E]$ *and* $[E : K] = [G : H]$, *where* $[G : H]$ *means the index of* H *in* G,

(b) the correspondence reverses inclusions i.e $E \subset E'$ *if and only if* $Gal(L/E) \supset Gal(L/E')$,

(c) The extension E/K is Galois if and only if H is a normal subgroup of G, in which case $Gal(E/K)$ is isomorphic to G/H.

Recall that when we have a finite extension L/K and an intermediate field E, the extension E/K was not necessarily Galois when L/K was a Galois extension. However, it is important to note here that the last part of the properties in Theorem 3.1.14 gives the condition under which the extension E/K will be Galois. Therefore, the extension E/K will be Galois only when the subgroup H corresponding to E is a normal subgroup of the group $Gal(L/K)$.

The following example demonstrates how the Fundamental Theorem of Galois theory can be used. We shall see later that a field obtained by adjoining the primitive nth roots of unity ζ_n to $\mathbb{Q}$ is called the cyclotomic field denoted by $\mathbb{Q}(\zeta_n)$ and the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is known as the cyclotomic extension.

3.1.15 Example. Given a Galois extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$, we want to use the Fundamental Theorem of Galois theory to find the intermediate fields. The minimal polynomial of ζ_5 over $\mathbb{Q}$ is given by

$$\Phi(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1.$$

We shall see later that the group $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^*$, an isomorphism defined by $\sigma^i(\zeta_5) = \zeta_5^i, i = 1, 2, 3, 4$. Since 2 is the generator for the group $(\mathbb{Z}/5\mathbb{Z})^*$, then $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ will be generated by σ^2 because $\left(\sigma^2(\zeta_5)\right)^4 = \zeta_5$. Therefore, the elements of $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ are $\left\{\sigma^1, \sigma^2, \sigma^3, \sigma^4\right\}$, where σ^1 is the identity of the group since $\sigma^1(\zeta_5) = \zeta_5$. $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is a cyclic group of order 4 and so by Langarage, the only non trivial proper subgroup of $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ must be of order 2. Considering the group $(\mathbb{Z}/5\mathbb{Z})^*$, its only non trivial proper subgroup is $\{1, 4\}$ and therefore, the only non-trivial proper subgroup of $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ must be $\left\{\sigma^1, \sigma^4\right\}$.

Figure 3.1: Shows Fields and corresponding group

$$\begin{array}{ccc} K_2 = \mathbb{Q}(\zeta_5) & & H_2 = \{1\} \\ \Big| & & \Big| \\ K_1 & & H_1 = \left\{\sigma^1, \sigma^4\right\} \\ \Big| & & \Big| \\ K_0 = \mathbb{Q} & & H_0 = Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \end{array}$$

To be able to find the field K_1, lets define a period $(\zeta_5, 4)$ of length 4 given by

$$(\zeta_5, 4) = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5.$$

From the tower of fields and their corresponding groups, we observe that K_1 is fixed by σ^4 and so we can claim, that $K_1 = \mathbb{Q}((\zeta_5, 2))$, where we define $(\zeta_5, 2)$ to be a period of length 2 fixed by H_1 and is given by,

$$\begin{aligned} (\zeta_5, 2) &= \zeta_5^1 + \zeta_5^4 \quad \text{and} \\ \sigma^2(\zeta_5, 2) &= \zeta_5^2 + \zeta_5^3. \end{aligned}$$

Now

$$(\zeta_5, 2) + \sigma^2(\zeta_5, 2) = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 = -1,$$

since $\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$ and

$$(\zeta_5, 2)\sigma^2(\zeta_5, 2) = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 = -1$$

by the same reason. Then $(\zeta_5, 2)$ and $\sigma^2(\zeta_5, 2)$ are roots of a quadratic equation

$$x^2 + x - 1 = 0 \quad \text{with roots} \quad \frac{-1 \pm \sqrt{5}}{2}.$$

Therefore, the field $K_1 = \mathbb{Q}(\sqrt{5})$. It is also important to note that the group $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is abelian and thus its subgroup H_1 is normal in $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. This shows us that the extension $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is normal but it is also easy to see since the minimal polynomial $x^2 - 5$ of $\sqrt{5}$ splits over $\mathbb{Q}(\sqrt{5})$. Hence we have an isomorphism $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})/H_1 \cong Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$.

3.2 Cyclotomic Extensions

The polynomial $x^n - 1 \in \mathbb{Q}[x]$ has n distinct roots which can be given by the complex exponential function $\mathrm{e}^{\frac{2ik\pi}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, 1 \leq k \leq n$. These roots are called nth roots of unity and are going to be important in the construction of regular polygons. The collection of nth roots of unity forms a multiplicative group with order n. In fact, this group is cyclic with generators called primitive nth roots of unity. We say x is a primitive nth root of unity if $x^n = 1$ and $x^k \neq 1$ for $0 < k < n$. Therefore, if ζ is a primitive nth root of unity, then $\zeta, \zeta^2, \ldots, \zeta^n = 1$ is a complete list of the nth roots of unity. This is so because for $1 \leq a < b \leq n$, then

$$(\zeta^a)^n = (\zeta^n)^a = 1^a = 1.$$

These roots are also distinct because suppose if

$$\zeta^a = \zeta^b \Rightarrow \zeta^{a-b} = 1,$$

which is a contradiction to the primitivity of ζ since $a - b < n$.

3.2.1 Proposition. If ζ_n is a primitive nth root of unity, then ζ_n^a is a primitive nth root of unity if and only if $(a, n) = 1$ and the number of primitive nth roots of unity is equal to $\phi(n)$ i.e the number of i with $1 \leq i \leq n$ such that $(i, n) = 1$, the Euler $\phi-$function.

Proof. Let a and n be coprime, then we want show that ζ_n^a is a primitive nth root of unity. Suppose there exists $1 \leq m < n$, such that

$$\zeta_n^{am} = 1.$$

Then am is an integer multiple of n. Otherwise, there exist $1 \leq r < n, s \in \mathbb{Z}$ such that $am = ns + r$ and so,

$$(\zeta_n^a)^m = \zeta_n^{ns}\zeta_n^r = \zeta_n^r = 1,$$

which is a contradiction since $r < n$. Therefore, $n|am$. But since $(a, n) = 1$, then $n|m$ which is not possible since $n > m$. Hence such an m does not exist and thus ζ_n^a is a primitive nth root of unity.

Conversely, let ζ_n^a be a primitive nth root of unity. We show that $(a, n) = 1$. Suppose $(a, n) = d > 1$, then there exist $m = \frac{n}{d} < n$ such that

$$(\zeta_n^a)^{\frac{n}{d}} = (\zeta_n^n)^{\frac{a}{d}} = (1)^{\frac{a}{d}} = 1,$$

which is a contradiction to ζ_n^a being primitive. Hence $d = 1$, so a and n must be coprime. The last statement follows from the fact that $1 \leq a \leq n$, such that $(a, n) = 1$ which shows that $\phi(n)$ is the number of primitive nth roots of unity. □

A field obtained by adjoining the primitive nth roots of unity ζ_n to $\mathbb{Q}$ is called the cyclotomic field denoted by $\mathbb{Q}(\zeta_n)$ and the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is known as the cyclotomic extension. "The term cyclotomic extensions means circle dividing and it comes from the fact that the nth roots of unity divide a circle into arcs of equal length" Conrad (2011).

In a field, any two primitive nth roots of unity are powers of each other. Therefore, the extension $\mathbb{Q}(\zeta_n)$ is not dependant on the choice of a primitive root ζ_n and so $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_1, \zeta_2, \ldots, \zeta_n)$. Therefore, $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$. Also, since $\mathbb{Q}$ is of $Char\ 0$, then $x^n - 1$ is separable over $\mathbb{Q}$. Hence the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, is a Galois extension. At this juncture, let us understand the Galois group $Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$ starting with the following Lemma.

3.2.2 Lemma. For $\tau \in Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$, there is an integer a, with $(a, n) = 1$ such that $\tau(\zeta) = \zeta^a$ for all ζ.

Proof. Let ζ_n be a primitive nth root of a unity. Then $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$, for all $k, 1 \leq k < n$. Thus $\tau\left(\zeta_n\right)^n = \tau\left(\zeta_n^n\right) = 1$ and for all $1 \leq k < n$, $\tau\left(\zeta_n\right)^k \neq 1$. This mean that $\tau\left(\zeta_n\right)$ is a primitive nth root of unity. Which implies that $\tau\left(\zeta_n\right) = \zeta_n^a$ where $(a, n) = 1$. □

Because of the way the exponent a is defined in Lemma 3.2.2, it is well defined modulo n. We can think of a as an element of $(\mathbb{Z}/n\mathbb{Z})^*$, where $(\mathbb{Z}/n\mathbb{Z})^*$ is a group of integers modulo n and each element of $(\mathbb{Z}/n\mathbb{Z})^*$ has a multiplicative inverse. Therefore, there exist a map between $Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$ and $(\mathbb{Z}/n\mathbb{Z})^*$. In fact, this map is an isomorphism as we show in the following result.

3.2.3 Theorem. *Let $\psi : Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ be a map defined by $\psi(\sigma) = i \pmod n$ if and only if $\sigma(\zeta) = \zeta^i$ for all i such that $(i, n) = 1$ and ζ an nth root of unity. This map ψ is a group isomorphism.*

Proof. We first show that ψ is a homomorphism. Let $\sigma, \tau \in Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$ where $\psi(\tau) = j \pmod n$ and $\psi(\sigma) = k \pmod n$. Then

$$\sigma\tau\left(\zeta\right) = \sigma\left(\zeta^j\right) = \left(\zeta^j\right)^k = \zeta^{kj}.$$
$$\therefore \psi(\sigma\tau) = kj \pmod n = (k \pmod n)(j \pmod n) = \psi(\sigma)\psi(\tau).$$

Hence ψ is a homomorphism. To show that ψ is injective, let σ be in the kernel of ψ, then $\psi(\sigma) = 1 \pmod n$ and so $\sigma(\zeta) = \zeta$. Thus σ also fixes all elements of $\mathbb{Q}(\zeta_n)$. Thus σ is the identity in the group $Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$. Hence ψ is one to one. ψ is surjective since $|Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)| = |\left(\mathbb{Z}/(n)\mathbb{Z}\right)^*|$. Therefore, ψ is an isomorphism. □

3.2.4 Corollary. The Galois group $Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$ is abelian.

The proof to this corollary follows immediately from Theorem 3.2.3 since the group $(\mathbb{Z}/n\mathbb{Z})^*$ is abelian, so $Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$ must be abelian.

We have shown that the collection of nth roots of unity form a multiplicative group. Let's denote this group by μ_n,then $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ an isomorphism defined by $\zeta_n^k \to k$, where ζ_n is the nth root of unity and $k \in \mathbb{Z}/n\mathbb{Z}$. Therefore, we now show that the degree of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $\phi(n)$.

Firstly, observe that in $\mathbb{C}$, the primitive nth roots of unity ζ_n are $\mathbb{Q}-$ conjugate. And we know that two roots of a polynomial are conjugate if they have the same minimal polynomials. Therefore, the primitive nth roots of unity have a common polynomial over $\mathbb{Q}[x]$. This polynomial is called the cyclotomic

polynomial and is denoted by $\Phi_n(x)$. If $n = p^r$, a prime power, the cyclotomic polynomial will be given by,

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \sum_{k=0}^{p-1} x^{kp^{(r-1)}}.$$

3.2.5 Example. If $n = 11$, this is just 11^1 and thus,

$$\Phi_{11}(x) = \frac{x^{11^1} - 1}{x^{11^{1-1}} - 1} = \frac{x^{11} - 1}{x - 1} = \sum_{k=0}^{10} x^k.$$

Similar, if $n = 16 = 2^4$, then,

$$\Phi_{2^4}(x) = \frac{x^{2^4} - 1}{x^{2^3} - 1} = \sum_{k=0}^{1} x^{8k} = 1 + x^8.$$

We note here that $\Phi_n(x)$ has degree $\phi(n)$, where ϕ is the Euler function. But for $\Phi_n(x)$ to be the minimal polynomial of ζ_n, we need to check that $\Phi_n(x)$ is irreducible. Therefore we state the following Lemma which we shall not prove.

3.2.6 Lemma. Let $\zeta \in \mathbb{C}$ be a root of $g(x)$ and p be a prime such that $p \nmid n$. If $g(x)$ is an irreducible monic factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$, then $g(\zeta^p) = 0$

The proof to this lemma can be found on page 258-260 of (Tignol, 1988).

3.2.7 Theorem. *For all $n \geq 1$, the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Let ζ be a root of $g(x)$, where $g(x)$ is an irreducible monic factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$. Then ζ is a primitive nth root unity. Recall that ζ^a for $(a, n) = 1$ gives the other primitive nth root of unity. Now a can be factored into prime factors $a = p_1 p_2 \dots p_s$ for p_i prime. Since $(a, n) = 1$, then $p_i \nmid n$.

Also since $g(\zeta) = 0$, then by Lemma 3.2.6,we have that $g(\zeta^{p_1}) = 0$ and $g(\zeta^{p_1 p_2}) = 0$. Repeatedly applying Lemma 3.2.6 shows that

$$g(\zeta^a) = g(\zeta^{p_1 p_2 \dots p_s}) = 0.$$

Remember that a was arbitrary chosen, where $(a, n) = 1$, for $1 \leq a \leq n$. So g is a root of all primitive nth roots of unity. Thus $\Phi_n(x) | g(x)$. But by our assumption, $g(x)$ is an irreducible monic factor of $\Phi_n(x)$, which implies that $g(x)$ and $\Phi_n(x)$ are monic and hence $g(x) = \Phi_n(x)$. Therefore, any primitive nth root of unity is a root of $\Phi_n(x)$. But $\Phi_n(x)$ is irreducible and it follows that it is the minimal polynomial for all primitive nth root of unity. □

Therefore, the degree of the extension $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is equal to $\phi(n)$, the Euler $\phi-$function, which is also the degree of the minimal irreducible polynomial of ζ_n. In his studies on cyclotomic fields, Gauss made remarkable progress by showing that for a prime p, a $p-$gon was constructible if $\phi(p) = 2^k$.

4. Constructable regular Polygons

4.1 Regular polygons

In section 2.1, we discussed constructible numbers and showed some results necessary for a number α to be constructible. In this section, the question we will be answering is, "for which values of n is a regular $n-$gon constructible?". However we should note that for construction to be possible, the numbers or values required must be obtained by the rational operations i.e multiplication, addition, subtraction, division(by non-zero numbers) and the square root operation. We must mention here that, when we talk of a constructible polygon, we shall mean a regular polygon and constructibility is by ruler and compass. To show construction of a regular polygon, we need to show that the numbers that dictate position of vertices of the regular polygon are constructible. But these are just primitive nth roots of unity given by $\mathrm{e}^{\frac{2ik\pi}{n}} = cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, which is a point in the Cartesian plane. Therefore, we state the following theorem that shows that a point that lies in field L, which is a quadratic extension of $\mathbb{Q}$ is constructible.

4.1.1 Theorem. *Let $P \subseteq \mathbb{R}^2$, such that $P = \{(0,0),(1,0)\}$. Suppose K is a subfield of $\mathbb{R}$ generated by the coordinates of points in the subset P. Let $a, b \in L$ where L is a finite extension of K, contained in $\mathbb{R}$, such that there exist a finite sequence of subfields*

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

with $[K_{i+1} : K_i] = 2, i = 0, 1, 2, \ldots, n-1$. Then (a, b) is constructible from P.

Proof. The ideas in this proof are from (Stewart, 1973) and (Howie, 2006). We shall prove by induction on n. Suppose $n = 0$, then (a, b) is constructible by Corollary 2.3.12. Suppose (a, b) is constructible for every point with coordinates in K_{n-1}. We now show that (a, b) is constructible for every point with coordinates in K_n. But since $[K_n : K_{n-1}] = 2$, then we can conclude that $K_n = K_{n-1}(\alpha)$, where α is an arbitrary element of K_n not in K_{n-1}. Thus the minimal polynomial of α is

$$X^2 + cX + d, \quad \text{with} \quad c, d \in K_{n-1} \quad \text{and discriminant} \quad \Delta = c^2 - 4d.$$

Since K_n is a subset of $\mathbb{R}$, then $\Delta \geq 0$. Therefore, $\alpha = \dfrac{-c \pm \sqrt{\Delta}}{2}$ and $K_n = K_{n-1}(\sqrt{\Delta})$, where $\Delta \in K_{n-1}$ and constructible by induction. Using Lemmas 2.1.2 and 2.1.3, $(\sqrt{\Delta}, 0)$ and consequently $(p + q\sqrt{\Delta}, r + s\sqrt{\Delta}) = (a, b)$, where $p, q, r, s \in K_{n-1}$ is constructible. Hence (a, b) is constructible from P. □

Here is another theorem that gives more conditions sufficient for constructibility.

4.1.2 Theorem. *Let $P = \{(0,0),(1,0)\} \subset \mathbb{R}^2$ and $K \subseteq \mathbb{R}$ generated by the coordinate points in P. Let $\alpha, \beta \in L$ where L is a normal extension over $\mathbb{Q}$, such that $L \subseteq \mathbb{R}$ and $[L : \mathbb{Q}] = 2^m, m \geq 0$. Then we can construct (α, β) from P.*

Proof. (Stewart, 1973). Since $\mathbb{Q}$ is of $char$ 0, the extension $L/\mathbb{Q}$ is separable by Proposition 3.1.6 . Then $G = Gal(L/\mathbb{Q})$ and by Theorem 3.1.14 $|G| = 2^m$, so that G is a $2-$group (a finite group with

its order a power of a prime 2). From group theory, if G is a finite $p-$group of order p^n, then G has a finite series of normal subgroups

$$1 = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_m = G,$$

such that $|H_i| = 2^i (i = 0, 1, \ldots, m)$. By 3.1.14, there exists subfields

$$L = L^{H_0} \supset L^{H_1} \supset \cdots \supset L^{H_m} = \mathbb{Q},$$

with $[L : L^{H_i}] = 2^i (i = 0, 1, \ldots, m)$. Hence $[L^{H_i} : L^{H_{i+1}}] = 2, \forall i = 0, 1, \ldots, m.$ and thus by Theorem 4.1.1, we can construct (α, β) from P. □

From Theorem 2.3.14, we know that a number n is constructible if the degree of its minimal polynomial is a power of 2. And now we have established that if we have a normal extension with degree a power of 2, then points in the extension field are constructible. In order for an $n-$gon to be constructible, the degree of the cyclotomic extension (note that these extensions are normal) $\phi(n)$ must be a power of 2.

Let's now describe values of n for which a regular $n-$gon is constructible by looking at the following Lemmas.

4.1.3 Lemma. If $\alpha \geq 2$, the regular $2^\alpha-$gon is constructible.

Proof. The regular $2^\alpha-$gon is constructible by repeated bisecting of 2π. □

By using bisecting of angles, the regular polygons of vertices $6, 8, 10, 12, 16,$ etc can be constructible.

4.1.4 Lemma. Let $n \in \mathbb{N}$ such that the regular $n-$gon is constructible. If $m \geq 3$ divides n, then the regular $m-$gon is also constructible.

Proof. Since m divides n, $\exists d$ such that $n = md$. The regular $m-$gon is constructible by joining every dth vertex of the regular $n-$gon. □

The Greeks had defined rules of constructing a regular triangle, square and pentagon. They knew too how to double the sides of a given polygon and how to combine two constructible polygons together, provided the sides of the polygons were relatively prime. As a result, a $15-$gon could be constructed from a triangle and a pentagon. Before Gauss's description of the construction of a $17-$gon, the only odd polygons the Greeks could construct were the triangle, pentagon and the $15-$gon. Thus this reduces the problem to looking at prime numbers. Here is a Lemma according to Gauss that describes constructible $p-$gons, for p a prime.

4.1.5 Lemma. Let p be an old prime. If n is a constructible regular $n-$gon and if p divides n, then p is of the form $2^{2^k} + 1$.

Proof. Since p divides n, then by Lemma 4.1.4, a regular $p-$gon is constructible. Therefore, this means that the pth roots of unity are constructible. But these are roots of the cyclotomic polynomial

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

which is irreducible by Theorem 3.2.7 and has degree $p - 1$. To be constructible, $p - 1$ must be a power of 2 by Theorem 2.3.14. Thus $p - 1 = 2^m, m \geq 1$. However, $p = 2^m + 1$ is only a prime number if

$m = 2^k, k \geq 0$. Suppose this was not the case, then m can be written as $m = qr$, with r is an odd factor. Therefore,

$$\begin{aligned} p &= 2^m + 1, \\ &= (2^q)^r - (-1)^r, \\ &= [2^q - (-1)] \left[(2^q)^{r-1} - (2^q)^{r-2} + (2^q)^{r-3} - \cdots + 1 \right], \end{aligned}$$

which is a contradiction if p is prime. Hence $p = 2^{2^k} + 1$ as require. □

The primes of the form $p = 2^{2^k} + 1$ are known as Fermat primes and the only known Fermat primes to date are $3, 5, 17, 257$ and 65537. Therefore, if a regular $n-$gon is constructible, then all its old prime factors must be Fermat primes. Additionally, every Fermat prime divides n only once as shown in the following Lemma.

4.1.6 Lemma. If p is an odd prime and the regular $n-$gon is constructible, then p^2 does not divide n.

Proof. (Hadlock, 2000). To prove this Lemma, we need to show that a p^2-gon is not constructible for p an odd prime. Now, the minimum polynomial for the p^2th roots of unity is given by

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

and is of degree $\phi(p^2) = p(p-1)$. Thus if $p^2|n$, then $p(p-1)$ primitive p^2 roots of unity must be constructible. But observe that the degree $p(p-1)$ has an odd factor hence it is not a power of 2 and not constructible. □

Gauss was able to show that for a regular $n-$gon to be constructible, all the old factors of n must be distinct Fermat primes. But before we state this main result, here is a Lemma which is important for this result.

4.1.7 Lemma. If the regular $m-gon$ and $n-$gon are constructible, where $(n, m) = 1$, then the regular $nm-$gon is also constructible.

Proof. The approach is according to (Hadlock, 2000). $\frac{2\pi}{m}$ and $\frac{2\pi}{n}$ are constructible by our hypothesis. Now since m and n are co-prime, there exits $r, s \in \mathbb{Z}$ such that,

$$\begin{aligned} 1 &= sn + rm, \\ \frac{1}{nm} &= \frac{s}{m} + \frac{r}{n}, \\ \frac{2\pi}{nm} &= s\frac{2\pi}{m} + r\frac{2\pi}{n}. \end{aligned}$$

Thus $\frac{2\pi}{nm}$ is constructible as a sum of multiple of $\frac{2\pi}{n}$ and $\frac{2\pi}{m}$. □

If we combine all the lemmas under this section, we are then ready to state the major result according to Gauss as to which numbers n the regular $n-$gon is constructible.

4.1.8 Theorem. *The regular $n-$gon is constructible for $n \geq 3$ if and only if n is of the form $2^\alpha p_1 p_2 \ldots p_m$ where the $p_i (i = 1, 2, \ldots, m)$ are distinct Fermat primes and α, m are integers greater than or equal to zero.*

Proof. The proof of this Theorem follows immediately from the results obtained from Lemmas 4.1.4 to Lemma 4.1.7. □

We have now completely described the numbers for which a regular $n-$gon is constructible. For example, a regular $255-$gon is constructible since its prime factors $3, 5$ and 17 are all distinct Fermat primes. But on the other hand a $258-$gon with factors $2, 3$ and 43 is not construct, since one of its odd factors, 43 is not a Fermat prime. For details see (Eekhoff, May, 2009).

According to Gauss, for a regular $p-$gon with p a prime, if $p-1$ is a power of 2, then the corresponding cyclotomic polynomial could be represented by a nested series of quadratic equations. The solutions to this cyclotomic polynomial will be found by solving these quadratic equations where the coefficients of the next quadratic equation are determined by the solutions of the previous quadratic equation. Using these ideas and what we have so far discussed in this paper, we have the following explicit example of the construction of a regular $17-$gon.

4.2 Gauss's explicit Example

Let $\varphi = \mathrm{e}^{\frac{2i\pi}{17}}$ be a primitive 17th root of unity. From Theorem 3.2.3, we know that $Gal(\mathbb{Q}(\varphi)/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^*$, thus $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$ is a cyclic group of order 16. Now 3 is the generator for the group $(\mathbb{Z}/17\mathbb{Z})^*$ and if we define a map $\sigma(\varphi) = \varphi^3$, then the cyclic group $Gal(\mathbb{Q}(\varphi)/\mathbb{Q}) =< \sigma >$, since $\sigma^{16}(\varphi) = (\sigma(\varphi))^{16} = \varphi$. The elements of the group $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$ are;

$$\left\{\sigma, \sigma^2, \sigma^3, \ldots, \sigma^{16} = 1\right\}.$$

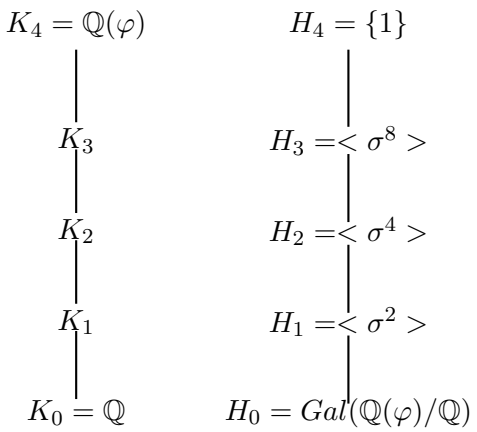
Therefore, the only subgroups $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$ are,

$$\begin{aligned} H_0 &= Gal(\mathbb{Q}(\varphi)/\mathbb{Q}) \\ H_1 &=< \sigma^2 > & H_2 &=< \sigma^4 > \\ H_3 &=< \sigma^8 > & H_4 &= \{1\}. \end{aligned}$$

Now since $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$ is cyclic and hence abelian, each H_{i+1} is normal in H_i, for $i = 0, 1, 2, 3, 4$. Since $\mathbb{Q}$ is of $Char\ 0$, the minimal polynomial of φ over $\mathbb{Q}$ has distinct roots and this polynomial splits completely over $\mathbb{Q}(\varphi)$, therefore the extension $\mathbb{Q}(\varphi)/\mathbb{Q}$ is normal and separable. Hence, by the Galois correspondence, for each subgroup of $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$, we can find a corresponding field. But before we do that, we observe that the index $[H_i : H_{i+1}] = 2$ for $i = 0, 1, 2, 3, 4$, since each H_{i+1} has two distinct cosets in H_i. Therefore, $[H_0 : H_4] = 2^4$ which is a power of 2 and hence showing that a $17-$gon is constructible.

By Galois correspondence, we have the following tower. On the left we have fields and on the right the corresponding subgroups of $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$ that fixes the given field.

Figure 4.1: Shows Fields and the corresponding group



The primitive 17th roots of a unity are all roots of the cyclotomic polynomial

$$\frac{x^{17}-1}{x-1} = x^{16} + x^{15} + \cdots + x^2 + x + 1.$$

This polynomial is irreducible over $\mathbb{Q}$ because it becomes Eisenstein at 17, that is if we replace x by $y+1$ then we have,

$$\frac{(y+1)^{17}-1}{y} = y^{16} + \binom{17}{1}y^{15} + \binom{17}{2}y^{14} + \cdots + \binom{17}{2}y + 17.$$

Therefore, $x^{16} + x^{15} + \cdots + x^2 + x + 1$ is a minimal polynomial of φ over $\mathbb{Q}$. If we let g be a primitive root modulo p and φ a primitive pth root of a unity, then φ^{g^i} for $i = 0, 1, \ldots, p-1$, is also a primitive pth root of unity. Fixing $p = 17$, the primitive root modulo 17 is 3 since

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^k \pmod{17}$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Now if we fix $\sigma(\varphi) = \varphi^3$ as a generator of $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$, we should be able to get the explicit four quadratic equations required to solve the polynomial $x^{16} + x^{15} + \cdots + x^2 + x + 1$ and hence find the explicit fields K_0, K_1, K_2, K_3, K_4. Additionally, all the primitive 17th root of unity are going to be given by $\varphi, \varphi^2, \varphi^3, \ldots, \varphi^{16}$ which are all distinct. The following diagram shows a sketch of the location of these roots where φ^i is labelled i and $(1, 0)$ is labelled 17.

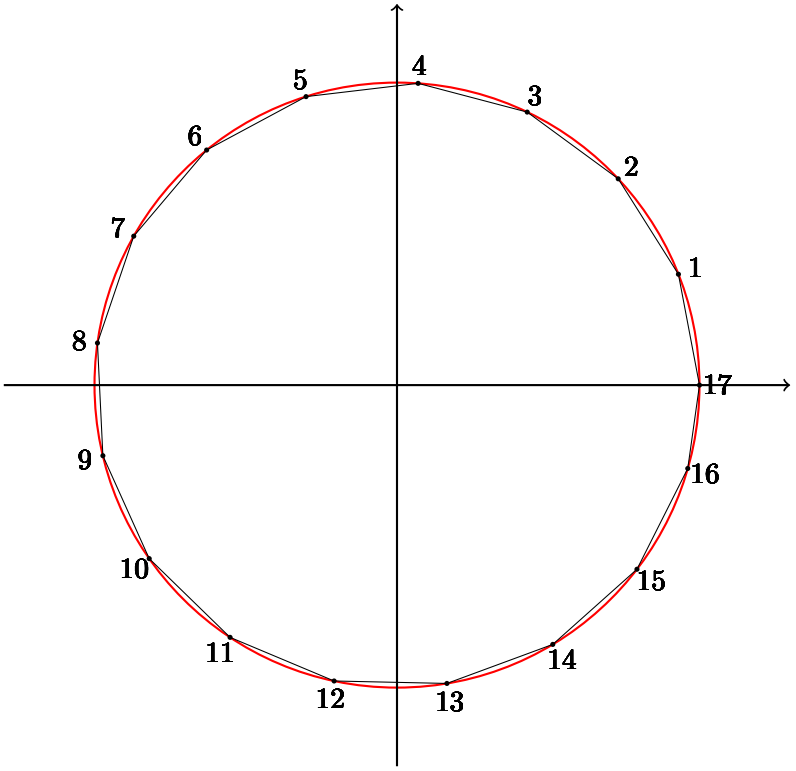


Figure 4.2: Sketch of a $17-$gon

Using these 17th roots of unity, we shall construct sums called periods which are just roots of the quadratic equations. Let $(\varphi, 16)$ denote the period of length 16 defined by

$$\begin{aligned}(\varphi, 16) &:= \varphi^{3^0} + \varphi^{3^1} + \varphi^{3^2} + \cdots + \varphi^{3^{15}} + \varphi^{3^{16}}, \\ &= \varphi^1 + \varphi^2 + \cdots + \varphi^{16}.\end{aligned}$$

We observe that $\sigma(\varphi, 16) = (\varphi, 16)$, hence fixed by σ, which implies that $\varphi^1 + \varphi^2 + \cdots + \varphi^{16} \in \mathbb{Q} = K_0$ and also $\varphi^1 + \varphi^2 + \cdots + \varphi^{16} = (\varphi, 16) = -1$, since $\varphi^1 + \varphi^2 + \cdots + \varphi^{16} + 1 = 0$.

By our construction, K_1 is fixed by σ^2 and thus we can claim that $K_1 = \mathbb{Q}((\varphi, 8))$ where $(\varphi, 8)$ is a period of length 8 given by

$$\begin{aligned}(\varphi, 8) &:= \varphi^{3^0} + \varphi^{3^2} + \varphi^{3^4} + \varphi^{3^6} + \varphi^{3^8} + \varphi^{3^{10}} + \varphi^{3^{12}} + \varphi^{3^{14}}, \\ &= \varphi + \varphi^9 + \varphi^{13} + \varphi^{15} + \varphi^{16} + \varphi^8 + \varphi^4 + \varphi^2 \quad \text{and} \\ \sigma(\varphi, 8) &= \left(\varphi^{3^0}\right)^3 + \left(\varphi^{3^2}\right)^3 + \left(\varphi^{3^4}\right)^3 + \left(\varphi^{3^6}\right)^3 + \left(\varphi^{3^8}\right)^3 + \left(\varphi^{3^{10}}\right)^3 + \left(\varphi^{3^{12}}\right)^3 + \left(\varphi^{3^{14}}\right)^3, \\ &= \varphi^3 + \varphi^{10} + \varphi^5 + \varphi^{11} + \varphi^{14} + \varphi^7 + \varphi^{12} + \varphi^6.\end{aligned}$$

Therefore, $\sigma(\varphi, 8)$ and $(\varphi, 8)$ periods of length 8 are roots of a quadratic equation

$$X^2 - [\sigma(\varphi, 8) + (\varphi, 8)]X + \sigma(\varphi, 8)(\varphi, 8) = 0.$$

Now we observe that

$$\sigma\left[(\varphi, 8) + \sigma(\varphi, 8)\right] = \sigma(\varphi, 8) + \sigma^2(\varphi, 8) = \sigma(\varphi, 8) + (\varphi, 8)$$

and

$$\sigma\left[(\varphi,8)\sigma(\varphi,8)\right]=\sigma(\varphi,8)(\varphi,8),$$

hence the coefficients of this equation are fixed by σ, which implies that the quadratic equation

$$X^2-[\sigma(\varphi,8)+(\varphi,8)]X+\sigma(\varphi,8)(\varphi,8)=0,$$

has coefficients in $\mathbb{Q}$. Thus,

$$\sigma(\varphi,8)+(\varphi,8)=\varphi^1+\varphi^2+\varphi^3+\cdots+\varphi^{15}+\varphi^{16}=(\varphi,16)=-1.$$

But what is

$$\sigma(\varphi,8)(\varphi,8)?$$

Since $(\varphi,8)$ and $\sigma(\varphi,8)$ each has 8 terms in powers of φ, the product has 64 terms in powers of φ. Therefore,

$$\sigma(\varphi,8)(\varphi,8)=a_1\varphi+a_2\varphi^2+a_3\varphi^3+\cdots+a_{16}\varphi^{16}\in\mathbb{Q}\quad\Rightarrow a_i\in\mathbb{Q},\forall i=1,2,\ldots,16.$$

We claim that $a_1=a_2=\cdots=a_{16}$. To prove this claim, suppose $a_i\neq a_j$. Recall that $\varphi,\varphi^2,\ldots,\varphi^{16}$ are roots of the minimal polynomial for φ over $\mathbb{Q}$ and these roots are linearly independent over $\mathbb{Q}$. Now since the extension $\mathbb{Q}(\varphi)/\mathbb{Q}$ is Galois, then for any two roots $\varphi^i,\varphi^j, i\neq j$, there exist $\sigma\in Gal\left(\mathbb{Q}(\varphi)/\mathbb{Q}\right)$ such that $\sigma(\varphi^i)=\varphi^j$, where φ^j is a conjugate of $\sigma(\varphi^i)$. But we know that σ fixes

$$a_1\varphi+a_2\varphi^2+a_3\varphi^3+\cdots+a_{16}\varphi^{16}.$$

Which implies that,

$$\begin{aligned}a_1\varphi+a_2\varphi^2+a_3\varphi^3+\cdots+a_{16}\varphi^{16}&=\sigma\left(a_1\varphi+a_2\varphi^2+a_3\varphi^3+\cdots+a_{16}\varphi^{16}\right),&(4.2.1)\\&=a_1\sigma(\varphi)+\cdots+a_i\sigma(\varphi^i)=a_i\varphi^j+\cdots+a_j\sigma(\varphi^j)+\ldots&(4.2.2)\end{aligned}$$

If $a_i\neq a_j$ then they are two different $\mathbb{Q}-$linear combinations of roots $\varphi,\varphi^2,\ldots,\varphi^{16}$ which are equal and hence a contradiction. Therefore, for the equality in equations 4.2.1 and 4.2.2 to hold, we need $a_i=a_j$. So that,

$$\begin{aligned}(\varphi,8)\sigma(\varphi,8)&=a\left(\varphi^1+\varphi^2+\varphi^3+\cdots+\varphi^{16}\right),\\&=a(\varphi,16),\\&=-a.\end{aligned}$$

Hence a must be equal to 4. Which implies that $(\varphi,8)$ and $\sigma(\varphi,8)$ are roots of the quadratic equation,

$$X^2+X-4=0,\tag{4.2.3}$$

which has roots $\frac{-1\pm\sqrt{17}}{2}$. Therefore, $K_1=\mathbb{Q}(\sqrt{17})$. We now determine which root is $(\varphi,8)$ and which one is $\sigma(\varphi,8)$. Let $\beta=\frac{2\pi}{17}$, we observe that for $1\leq j\leq 16$,

$$\begin{aligned}\varphi^j&=\cos(j\beta)+i\sin(j\beta)\quad\text{and}\\\varphi^{17-j}&=\varphi^{-j}=\cos(-j\beta)+i\sin(-j\beta),\quad\text{since}\quad\varphi^{17}=1,\\&=\cos(j\beta)-i\sin(j\beta),\\&=\overline{(\varphi^j)},\quad\text{the conjugate of }\varphi^j\text{ and therefore}\\\varphi^j+\varphi^{17-j}&=2Re(\varphi^j)=2\cos j\beta.\end{aligned}$$

where Re denotes the real part of the given number φ. After doing some calculations, we discover that,

$$0 < j\beta < \frac{\pi}{2}, \quad \text{for} \quad 1 \leq j \leq 4, \quad \frac{\pi}{2} < j\beta < \pi, \quad \text{for} \quad 5 \leq j \leq 8$$
$$\pi < j\beta < \frac{3\pi}{2}, \quad \text{for} \quad 9 \leq j \leq 12, \quad \frac{3\pi}{2} < j\beta < 2\pi, \quad \text{for} \quad 13 \leq j \leq 16.$$

which means that

$$\cos j\beta > 0, \quad \text{for} \quad 1 \leq j \leq 4, 13 \leq j \leq 16 \quad \text{and}$$
$$\cos j\beta < 0, \quad \text{for} \quad 5 \leq j \leq 12,$$

Now since

$$(\varphi, 8) = 2\left(\cos\beta + \cos 2\beta + \cos 4\beta + \cos 8\beta\right) \quad \text{and}$$
$$\sigma(\varphi, 8) = 2\left(\cos 3\beta + \cos 7\beta + \cos 5\beta + \cos 6\beta\right),$$

we observe that all the angles for $(\varphi, 8)$ and $\sigma(\varphi, 8)$ lie between 0 and π, and since cosine is a decreasing function on this interval, then

$$\cos\beta + \cos 2\beta > 2\cos\frac{\pi}{4} = \sqrt{2}.$$

Hence

$$\cos\beta + \cos 2\beta + \cos 8\beta > \sqrt{2} + \cos 8\beta > \sqrt{2} - 1 > 0.$$

Also since

$$4\beta = \frac{8\pi}{17} < \frac{\pi}{2}, \quad \text{then} \quad \cos 4\beta > 0.$$

so that $(\varphi, 8) > 0$ which implies that $(\varphi, 8) > \sigma(\varphi, 8)$ and therefore,

$$(\varphi, 8) = \frac{-1 + \sqrt{17}}{2} \quad \text{and} \quad \sigma(\varphi, 8) = \frac{-1 - \sqrt{17}}{2}.$$

In a similar manner, we can find K_2. K_2 is fixed by σ^4 and we claim that $K_2 = \mathbb{Q}\left((\varphi, 4)\right)$ where we define $(\varphi, 4)$ to be a period of length 4 given by,

$$\begin{aligned}(\varphi, 4) :&= \varphi^{3^0} + \varphi^{3^4} + \varphi^{3^8} + \varphi^{3^{12}},\\ &= \varphi + \varphi^{13} + \varphi^{16} + \varphi^4 \quad \text{and}\\ \sigma^2(\varphi, 4) &= \varphi^{3^2} + \varphi^{3^6} + \varphi^{3^{10}} + \varphi^{3^{14}},\\ &= \varphi^9 + \varphi^{15} + \varphi^8 + \varphi^2.\end{aligned}$$

Therefore, $(\varphi, 4)$ and $\sigma^2(\varphi, 4)$ are roots of the quadratic equation

$$X^2 - [(\varphi, 4) + \sigma^2(\varphi, 4)]X + (\varphi, 4)\sigma^2(\varphi, 4) = 0.$$

Now observe that

$$\sigma^2[(\varphi, 4) + \sigma^2(\varphi, 4)] = \sigma^2(\varphi, 4) + \sigma^4(\varphi, 4) = \sigma^2(\varphi, 4) + (\varphi, 4)$$

and also

$$\sigma^2[(\varphi,4)\sigma^2(\varphi,4)] = \sigma^2(\varphi,4)\sigma^4(\varphi,4) = \sigma^2(\varphi,4)(\varphi,4),$$

hence both are fixed by σ^2. Which implies that

$$X^2 - [(\varphi,4) + \sigma^2(\varphi,4)]X + (\varphi,4)\sigma^2(\varphi,4) \in K_1[X].$$

But

$$\begin{aligned}(\varphi,4) + \sigma^2(\varphi,4) &= \varphi^{3^0} + \varphi^{3^2} + \varphi^{3^4} + \varphi^{3^6} + \varphi^{3^8} + \varphi^{3^{10}} + \varphi^{3^{12}} + \varphi^{3^{14}},\\ &= (\varphi,8).\end{aligned}$$

We now find out what $(\varphi,4)\sigma^2(\varphi,4)$ is

$$\begin{aligned}(\varphi,4)\sigma^2(\varphi,4) &= \left(\varphi + \varphi^{13} + \varphi^{16} + \varphi^4\right)\left(\varphi^9 + \varphi^{15} + \varphi^8 + \varphi^2\right),\\ &= \varphi^{10} + \varphi^{16} + \varphi^9 + \varphi^3 + \varphi^5 + \varphi^{11} + \varphi^4 + \varphi^{15} + \varphi^8 + \varphi^{14} + \varphi^7 + \varphi + \varphi^{13} + \varphi^2 + \varphi^{12} + \varphi^6,\\ &= (\varphi,16) = -1.\end{aligned}$$

Therefore, the quadratic equation becomes

$$X^2 - (\varphi,8)X - 1 = 0,$$

with roots given by $\dfrac{(\varphi,8) \pm \sqrt{(\varphi,8)^2+4}}{2}$. Hence $K_2 = \mathbb{Q}\left(\sqrt{(\varphi,8)^2+4}\right)$. But which root is $(\varphi,4)$ and which one is $\sigma^2(\varphi,4)$? Here, we observe that,

$$\begin{aligned}(\varphi,4) &= 2\left(\cos\beta + \cos 4\beta\right) \quad \text{and}\\ \sigma^2(\varphi,4) &= 2\left(\cos 2\beta + \cos 8\beta\right).\end{aligned}$$

Clearly, $(\varphi,4) > \sigma^2(\varphi,4)$ since $\cos\beta > \cos 2\beta$ and $\cos 4\beta > \cos 8\beta$ hence,

$$(\varphi,4) = \frac{(\varphi,8) + \sqrt{(\varphi,8)^2+4}}{2} \quad \text{and} \quad \sigma^2(\varphi,4) = \frac{(\varphi,8) - \sqrt{(\varphi,8)^2+4}}{2}.$$

Now for K_3, we also claim that $K_3 = \mathbb{Q}((\varphi,2))$ where $(\varphi,2)$ is defined to be a period of length 2 given by,

$$\begin{aligned}(\varphi,2) &= \varphi^{3^0} + \varphi^{3^8} = \varphi + \varphi^{16} \quad \text{and}\\ \sigma(\varphi,2) &= \varphi^{3^4} + \varphi^{3^{12}} = \varphi^{13} + \varphi^4.\end{aligned}$$

Thus $(\varphi,2)$ and $\sigma^4(\varphi,2)$ are roots of the quadratic equation

$$X^2 - [(\varphi,2) + \sigma^4(\varphi,2)]X + (\varphi,2)\sigma^4(\varphi,2) = 0.$$

It is easy to see that the coefficients of this equation are in K_2, by showing that they are fixed by σ^4.

Now we have that,

$$\begin{aligned}(\varphi,2) + \sigma^4(\varphi,2) &= \varphi + \varphi^{16} + \varphi^{13} + \varphi^4 = (\varphi,4) \quad \text{and}\\ (\varphi,2)\sigma^4(\varphi,2) &= \left(\varphi + \varphi^{16}\right)\left(\varphi^{13} + \varphi^4\right),\\ &= \varphi^{14} + \varphi^5 + \varphi^3 + \varphi^{12},\\ &= \sigma(\varphi,4), \quad \text{since} \quad \sigma(\varphi + \varphi^{13} + \varphi^{16} + \varphi^4) = \varphi^{14} + \varphi^5 + \varphi^3 + \varphi^{12}.\end{aligned}$$

Therefore the quadratic equation now becomes

$$X^2 - [(\varphi,4)]X + \sigma(\varphi,4) = 0, \quad \text{with roots} \quad \frac{(\varphi,4) \pm \sqrt{(\varphi,4)^2 - 4\sigma(\varphi,4)}}{2}.$$

Now since

$$(\varphi,2) = 2\cos\beta \quad \text{and} \quad \sigma^4(\varphi,2) = 2\cos 4\beta$$

then we see that $(\varphi,2) > \sigma^4(\varphi,2)$ and hence,

$$\begin{aligned}(\varphi,2) &= \frac{(\varphi,4) + \sqrt{(\varphi,4)^2 - 4\sigma(\varphi,4)}}{2} \quad \text{and} \\ \sigma^4(\varphi,2) &= \frac{(\varphi,4) - \sqrt{(\varphi,4)^2 - 4\sigma(\varphi,4)}}{2}.\end{aligned}$$

But what is $\sigma(\varphi,4)$?.

Observe that $\sigma(\varphi,4) = (\varphi,2)\sigma^4(\varphi,2) \in K_2, \Rightarrow \sigma(\varphi,4) \in K_2$. Therefore, $\sigma(\varphi,4)$ is a root of a quadratic with coefficients in K_1 and these coefficients of the quadratic in K_1, must be roots of a quadratic with coefficients in $\mathbb{Q}$ as we illustrate now. When finding the quadratic field K_2, there were two periods $\sigma(\varphi,4)$ and $\sigma^3(\varphi,4)$ of length 4 which we did not consider but both of them are fixed by σ^4. Now,

$$\begin{aligned}\sigma(\varphi,4) + \sigma^3(\varphi,4) &= \sigma\left((\varphi,4) + \sigma^2(\varphi,4)\right), \\ &= \sigma\left((\varphi,8)\right) = \sigma(\varphi,8) \quad \text{and} \\ \sigma(\varphi,4)\sigma^3(\varphi,4) &= \sigma\left((\varphi,4)\sigma^2(\varphi,4)\right) = \sigma\left((\varphi,16)\right), \\ &= (\varphi,16) = -1.\end{aligned}$$

Therefore, $\sigma(\varphi,4)$ is a root of the quadratic,

$$X^2 - \sigma(\varphi,8)X - 1 \in K_1, \tag{4.2.4}$$

$$\text{with roots} \quad \frac{(\varphi,8) \pm \sqrt{(\sigma(\varphi,8))^2 + 4}}{2}. \tag{4.2.5}$$

But since

$$\begin{aligned}\sigma(\varphi,4) &= 2\left(\cos 3\beta + \cos 5\beta\right) \quad \text{and} \\ \sigma^3(\varphi,4) &= 2\left(\cos 6\beta + \cos 7\beta\right),\end{aligned}$$

then $\sigma(\varphi,4) > \sigma^3(\varphi,4)$ and thus

$$\begin{aligned}\sigma(\varphi,4) &= \frac{(\varphi,8) + \sqrt{(\sigma(\varphi,8))^2 + 4}}{2} \\ \sigma^3(\varphi,4) &= \frac{(\varphi,8) - \sqrt{(\sigma(\varphi,8))^2 + 4}}{2}.\end{aligned}$$

And from equation 4.2.3, we know that $\sigma(\varphi,8)$ is a root of the quadratic equation,

$$X^2 + X - 4 = 0 \in \mathbb{Q}[X]. \tag{4.2.6}$$

Therefore, $\sigma(\varphi,4)$ is obtained by finding roots of equation 4.2.6 and then roots of equation 4.2.4. Hence $K_3 = \mathbb{Q}\left(\sqrt{(\varphi,4)^2 - 4\sigma(\varphi,4)}\right)$.

For K_4, we know that $K_4 = \mathbb{Q}(\varphi)$. By our notation, $\varphi = (\varphi,1)$ where $(\varphi,1)$ is a period of length 1 and its conjugate will be given by $\sigma^8(\varphi,1) = \varphi^{16} = \overline{\varphi}$. Thus φ and $\overline{\varphi}$ are roots of the quadratic equation

$$X^2 - [\varphi + \overline{\varphi}]X + \varphi\overline{\varphi} = 0.$$

One can easily show that σ^8 fixes the coefficients of this equation. Additionally,

$$\begin{aligned} &\varphi + \overline{\varphi} = (\varphi,2) \quad \text{and} \\ &(\varphi)\overline{\varphi} = 1. \end{aligned}$$

Thus the quadratic equation becomes

$$X^2 - (\varphi,2)X + 1 = 0.$$

Now since

$$(\varphi,2) = \varphi + \overline{\varphi} = 2\cos\beta, \quad \text{then} \quad (\varphi,2)^2 - 4 < 0.$$

Therefore the roots φ and $\overline{\varphi}$ of the quadratic equation are given by

$$\frac{(\varphi,2) \pm \sqrt{(\varphi,2)^2 - 4}}{2} = \frac{(\varphi,2) \pm i\sqrt{4 - (\varphi,2)^2}}{2}.$$

By our choice of φ, we must have that

$$\varphi = \frac{(\varphi,2) + i\sqrt{4 - (\varphi,2)^2}}{2},$$

where $\dfrac{(\varphi,2)}{2}$ and $\dfrac{\sqrt{(\varphi,2)^2 - 4}}{2}$ are just expressions of numbers with only rationals and square roots. In Section 2.1, we showed that such a number calculated from rationals by a finite sequence of rational and square roots operations is constructable. Thus we can construct the number φ by ruler and compass. In fact, for the construction a regular $17-$gon, we just needed to show that $\cos\beta = \dfrac{(\varphi,2)}{2}$ is constructible because the construction of a regular polygon with n sides is the same as dividing a circle into n equal parts. Since φ is a primitive 17th root of unity, we can find the other roots by taking all its powers which will give the other vertices for the $17-$gon. Therefore, $17-$gon can be constructible by ruler and compass.

Lastly, the corresponding chain of fields for the normal subgroups of $Gal(\mathbb{Q}(\varphi)/\mathbb{Q})$ are

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{17}) \subset \mathbb{Q}\left(\sqrt{(\varphi,8)^2 + 4}\right) \subset \mathbb{Q}\left(\sqrt{(\varphi,4)^2 - 4\sigma(\varphi,4)}\right) \subset \mathbb{Q}(\varphi).$$

and $[\mathbb{Q}(\varphi) : \mathbb{Q}] = 2^4$ which is a power of 2 hence also showing that φ is constructible.

5. Conclusion

In this essay, we have established that a number α is constructible if the degree of its minimal polynomial is a power of 2. We described how investigating constructibles reduces to the study of polynomials, their roots and field extensions. This led us to the study of Galois Theory. We described the one to one Galois correspondence between the intermediate fields of a field extension and the subgroups of a Galois group and used this idea to show explicitly that a $17-$gon can be constructed. Further, we showed that a regular $n-$gon was constructible if all the odd factors of n where distinct primes of the form $2^{2^k}+1$, known as Fermat primes.

Acknowledgements

I would like to express my sincere appreciation to my supervisor Dr. Anold Keet. This essay would not have been possible without his advice, comments and our weekly meetings. I would also like thank Professor Ravi Ramakrishna, Tovondrainy Christalin Razafindramahatsioro and Danny Parsons for their advice, comments and insight to the editing process. To the AIMS family and friends, I say thanks for your continued support and making my stay at AIMS a delight. To mom, dad, my sisters and brother, I say thanks for all your love, encouragements, help and all the sacrifices you have made in life for my sake.

Finally I would like to thank God for the good health and life to be able to do this work.

References

K. Conrad. The Galois Correspondance, 2010. http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/galoiscorr.pdf.

K. Conrad. Cyclotomic Extensions, 2011. http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cyclotomic.pdf.

E. T. Eekhoff. Constructibilty of Regular Polygons, May, 2009. http://www.math.iastate.edu/thesisarchive/MSM/EekhoffMSMSS07.pdf.

C. R. Hadlock. *Field Theory and Its Classical Problems*. The Mathematical Association of America, 2000.

G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Amen House, London E.c.4, 1954.

J. M. Howie. *Fields and Galois Theory*. Springer-Verlag London Limited, 2006.

D. Savitt. The Mathematics of Gauss, June 2008. http://www.math.cornell.edu/~web401/steve.gauss17gon.pdf.

A. Skorobogatov. Rings and Fields, 2006. http://www2.imperial.ac.uk/~anskor/notesM2P4.pdf.

I. Stewart. *Galois Theory*. Chapman and Hall, 1973.

H. Stichtenoth. *Algebraic Function Fields and Codes*. Spriger-Verlag Berlin Heidelberg, 2009.

J.-P. Tignol. *Galois Theory of Algebraic Equations*. Longman Scientific and Technical, Harlow, 1988.

A. J. Wills. Topics on galois theory. Master's thesis, Virgin Polytechnic Institute and State University, April 19,2011.