Utrecht University

Bachelor's Thesis

# Primitive elements of abelian extensions and fields generated by polygon diagonals


**Author:** Rein Ter Rele

**Supervisor:** Prof. dr. G.L.M. Cornelissen



Department of Mathematics
Utrecht University

20-6-2024

**Abstract**

In this thesis we are interested in primitive elements of abelian extensions of $\mathbb{Q}$. By the Kronecker-Weber Theorem we know that abelian extensions are subfields of cyclotomic extensions $\mathbb{Q}(\zeta_n)$. For the case where $n = p^a$ with $p$ an odd prime, we will show that the primitive elements of these field extensions are traces of powers of $\zeta_n$ over a subgroup $H$ of the Galois group. In the last part of this thesis, we will discuss field extensions that are generated by the ratio of the lengths of two diagonals of a regular polygon. More specifically, we will discuss an article concerning this subject and show that there are some false claims in the article.

# Table of Contents

## Section 1

# Introduction

The roots of unity are an important subject in Field theory and Galois theory. They are defined as the solutions to the equation $x^n = 1$, and they are especially connected to the subject of abelian field extensions of $\mathbb{Q}$. These are field extensions with an abelian Galois group. This connection is stated in the Kronecker-Weber Theorem:

**Theorem 1.1** (Kronecker-Weber)**.** Let $K$ be an finite abelian extension of $\mathbb{Q}$. Then $K$ is contained in a cyclotomic extension of $\mathbb{Q}$, i.e. $K \subseteq \mathbb{Q}(\zeta_n)$ where $\zeta_n$ is a root of unity.

Cyclotomic extensions are defined as extensions of $\mathbb{Q}$ generated by a root of unity. Later on, we will prove that the Galois group of any cyclotomic extension is isomorphic to the multiplicative group of integers modulo $n$, which we will denote by $\mathbb{Z}_n^*$. If we take $H$ to be the Galois group of $K/\mathbb{Q}$, then by the Fundamental Theorem of Galois theory, we have the following correspondence:

$$\begin{array}{cc} \mathbb{Q}(\zeta_n) & 1 \\ | & | \\ K & H \\ | & | \\ \mathbb{Q} & \mathbb{Z}_n^* \end{array}$$

By this correspondence (see Theorem 14 in Dummit and Foote [3] for more details), we have that $K$ is precisely the subfield of the cyclotomic extension that is fixed by all elements of $H$. We will denote this by $K = \mathbb{Q}(\zeta_n)^H$. Furthermore, by the Primitive Element Theorem, we know that there is some $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$, i.e. $K$ is generated by the single element $\alpha$. Now the question arises if we can construct such $\alpha$. A natural candidate is the trace of $\zeta_n$ over $H$,

$$\sum_{\sigma \in H} \sigma(\zeta_n)$$

which is the sum over all the conjugates of the root of unity over $H$. It can be easily shown that this element is fixed by $H$, and it is fundamentally linked to the group $H$. Therefore, it seems natural that $K = \mathbb{Q}(\zeta_n)^H$ is generated by this trace.
In earlier research, this problem has been divided into two intermediate problems. The first one is the question of when the trace of $\zeta_n$ over $H$ is equal to zero. If this were the case, then it is obviously not a generator. Weber [9] answered this question for $n$ being a prime and Fuchs [5] for a general $n$, only considering cases with cyclic $H$. Diamond, Gerth and Vaaler [2] proved it for

general $n$ and $H$. Their results indicate that the trace of $\zeta_n$ over $H$ is not always non-zero.
The second question is whether a non-zero trace is a generator of the subfield $\mathbb{Q}(\zeta_n)^H$. This is indeed the case, and is proven by Evans [4]. These conclusions were used by Gómez-Molleda [6] to contruct generators of abelian field extensions in every case. For traces equal to zero, Gómez-Molleda manipulates the trace in a way so that it becomes a generator. In the first part of this thesis, we will start with a recap of some theory about roots of unity and cyclotomic extensions, and then follow the proofs of Gómez-Molleda for the case when $n$ is a power of an odd prime. We will make these proofs complete by filling in the results obtained from ealier sources.

The last section of this thesis will cover diagonals of regular polygons. This subject also involves roots of unity, but from a more geometrical perspective. Roots of unity are elements of $\mathbb{C}$, and can therefore be drawn in the complex plane. Due to their symmetry, they form the vertices of a regular polygon. Then problems involving regular polygons can be interpreted as an algebraic problem using roots of unity. In the last section of this thesis, we are specifically interested in diagonals of regular polygons. To be more precise, we will be interested in the degree of $\mathbb{Q}(\frac{d_1}{d_2})$ over $\mathbb{Q}$, where $d_1$ and $d_2$ are two diagonals of a regular polygon. For any $n \geq 1$, Grubb and Wolird [7] give an upper estimate for this degree depending on $n$. However, as we will show, this estimate is false, and there are multiple other mistakes in the article by Grubb and Wolird. We will present the claims made by the authors, and give counterproofs to these claims.

## Section 2

# Roots of unity

In this thesis, we will focus on cyclotomic extensions of $\mathbb{Q}$. These are field extensions that are generated by roots of unity. To understand these better, we will give a recap of the theory of roots of unity. Not all proofs in this section will be given. They can be found in the sources. First, we will define roots of unity. For all $n \geq 1$, an $n$-th root of unity is defined to be a root of the polynomial $x^n - 1$. We can quite easily find these roots in the complex plane by using Euler's formula. We know that $e^{2\pi ik} = 1$ for all $k \in \mathbb{Z}$. We can thus deduce that $e^{\frac{2\pi ik}{n}}$ is a $n$-th root of unity for all $k$, since we have

$$(e^{\frac{2\pi ik}{n}})^n = e^{\frac{2\pi ikn}{n}} = e^{2\pi ik} = 1.$$

By the fundamental theorem of algebra there are $n$ roots for $x^n - 1$, so the roots shown above are all the $n$-th roots of unity for $0 \leq k \leq n-1$.
We can see that all the roots of unity lie on the unit circle in the complex plane. Euler's formula shows us that

$$e^{\frac{2\pi ik}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) \tag{2.1}$$

which tells us that all $n$-th roots of unity have a radius of $\cos^2\left(\frac{2\pi k}{n}\right) + \sin^2\left(\frac{2\pi k}{n}\right) = 1$, hence they lie on the unit circle. This can be seen below, where the 5th roots of unity are drawn in the plane.

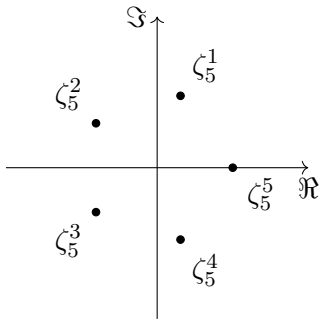


Figure 2.1: The fifth roots of unity in the complex plane

This result can also be easily deduced by using the known fact that the product of two complex numbers has a radius equal to the product of the radii of the original two numbers. If we thus want a number $c \in \mathbb{C}$ such that $c^n = 1$, we must have that the $n$-th power of the radius of $c$ is also equal to 1. It follows that the radius of $c$ must be 1, hence the number $c$, which is a root of unity in this case, must lie on the unit circle.

In the previous discussion we have already seen that there are $n$ distinct $n$-th roots of unity. However, in this thesis we will treat them mostly as algebraic elements. Therefore, we will now give an algebraic proof that there are $n$ distinct $n$-th roots of unity.

**Proposition 2.1.** There are exactly $n$ distinct $n$-th roots of unity

*Proof.* The derivative of $x^n - 1$ is equal to $D_x(x^n - 1) = nx^{n-1}$. We see that $nx^{n-1}$ only has 0 as a root. It is clear that this is never a root for $x^n - 1$. It follows that $x^n - 1$ and its derivative are coprime. By Proposition 33 in Chapter 13 of [3], we then know that $x^n - 1$ is separable. Thus all the roots of $x^n - 1$, which are the $n$-th roots of unity, are distinct. □

The set of all $n$-th roots of unity is thus a set of $n$ elements. Then the question arises if this set has some structure. As we will show here, this set is actually a group under multiplication.

**Proposition 2.2.** The set of all $n$-th roots of unity is a group under multiplication.

*Proof.* We will first prove that this set is closed under multiplication. Let $\zeta_n$ and $\eta_n$ be $n$-th roots of unity. Then we have

$$(\zeta_n \eta_n)^n = \zeta_n^n \eta_n^n = 1 \cdot 1 = 1$$

and thus the product is still a root of unity.
Clearly, 1 is the neutral element and is itself a root of unity. Furthermore, for every $n$-th roof of unity $\zeta_n$, there is an inverse $\zeta_n^{-1}$. This is still a root of unity, since

$$(\zeta_n^{-1})^n = \zeta_n^{-1 \cdot n} = (\zeta_n^n)^{-1} = 1^{-1} = 1.$$

We can thus conclude that this set is a group. □

From Proposition 18 in Chapter 9 of [3], we know that every subgroup of the multiplicative group of a field is cyclic. All roots of unity are elements of $\mathbb{C}$, so the group of $n$-th roots of unity is a subgroup of the multiplicative group of $\mathbb{C}$. Hence, it is cyclic. Any root of unity that is a generator of this cyclic group is called a *primitive* root of unity. These primitive roots of unity can also be deduced from equation (2.1). If we take $\zeta_n = e^{\frac{2\pi i}{n}}$, then for each $0 \leq k \leq n-1$, the power $\zeta_n^k = e^{\frac{2\pi i k}{n}}$ is still a root of unity. Furthermore, all these powers of $\zeta_n$ are distinct, since $0 \leq \frac{2\pi i k}{n} < 2\pi i$ for $0 \leq k \leq n-1$.
From now on, we will define $\zeta_n$ to be the first primitive $n$-th root of unity, i.e. $\zeta_n = e^{\frac{2\pi i}{n}}$.

We will give an algebraic proof of the next proposition.

**Proposition 2.3.** Let $1 \leq a < n$ be an integer. Then $\zeta_n^a$ is a primitive $n$-th roof of unity if and only if $a$ and $n$ are coprime.

*Proof.* Let $\zeta_n^a$ be a primitive root of unity. Now assume that $a$ and $n$ are not coprime. Then there is some integer $b > 1$ such that $b$ divides $a$ and $n$. We can then see that

$$(\zeta_n^a)^{n/b} = \zeta_n^{a \cdot n/b} = \zeta_n^{n \cdot a/b} = (\zeta_n^n)^{a/b} = 1^{a/b} = 1$$

and since $n/b < n$, this would contradict the fact that $\zeta_n^a$ is primitive. Therefore, $a$ and $n$ must be coprime.

Now suppose that $a$ and $n$ are coprime. We assume that $\zeta_n^a$ is not a primitive root of unity. Then there is some $m < n$ such that $(\zeta_n^a)^m = \zeta_n^{am} = 1$. Then we know that $n$ divides $am$. We know that

$n$ does not divide $m$, since $m < n$. Therefore $a$ and $n$ must have some common divisor, which is a contradiction. We conclude that $\zeta_n^a$ must be primitive. □

To end this subsection, we will give two short lemmas which can come in useful for later proofs.

**Lemma 2.4.** For any $a \in \mathbb{Z}$, we have

$$\zeta_n^a = \zeta_n^{a'}$$

for some $a' \equiv a \pmod{n}$ and $0 \leq a' < n$.

*Proof.* We know that there always exists some $0 \leq a' < n$ such that $a' \equiv a \pmod{n}$. It then follows that $a - a' = kn$ for some $k \in \mathbb{N}$, and thus $a = a' + kn$. We can then see that

$$\zeta_n^a = \zeta_n^{a'+kn} = \zeta_n^{a'}\zeta_n^{kn} = \zeta_n^{a'}(\zeta_n^n)^k = \zeta_n^{a'} \cdot 1^k = \zeta_n^{a'}$$

which proves the lemma. □

**Lemma 2.5.** Let $a \in \mathbb{Z}$ and $k$ be a positive integer. For any primitive $\zeta_n$ we then have

$$\zeta_n^a = \zeta_{kn}^{ka}.$$

where $\zeta_{kn}$ is also primitive.

*Proof.* First we can see that $(\zeta_{kn}^k)^n = \zeta_{kn}^{kn} = 1$ for all $k \in \mathbb{Z}$. Furthermore, if $m < n$, then it is clear that $(\zeta_{kn}^k)^m = \zeta_{kn}^{km} \neq 1$ since we have $km < kn$ and $\zeta_{kn}$ a primitive root of unity, hence the smallest integer such that its power of $\zeta_{kn}$ is equal to one. It then follows that $\zeta_{kn}^k$ must be a primitive $n$-th root of unity, i.e. $\zeta_{kn}^k = \zeta_n$. We then conclude that $\zeta_{kn}^{ka} = \zeta_n^a$. □

## 2.1 Cyclotomic extensions

We now shift our focus to the field extensions generated by roots of unity. Such an extension $\mathbb{Q}(\zeta_n)$ is called a *cyclotomic extension*. The degree of such an extension is equal to the degree of the minimal polynomial of $\zeta_n$ over $\mathbb{Q}$. We shall later prove that this polynomial is defined by the following:

**Definition 2.6.** The *$n$-th cyclotomic polynomial* $\Phi_n(x)$ is defined to be the polynomial whose roots are the primitive $n$-th roots of unity, i.e.

$$\Phi_n(x) := \prod_{\zeta_n \text{ primitive}} (x - \zeta_n) = \prod_{\substack{1 \leq a < n, \\ (a,n)=1}} (x - \zeta_n^a).$$

It can be quite difficult to compute this polynomial directly. However, by a simple manipulation we can show that cyclotomic polynomials can be computed iteratively. First of all, we note that

$$x^n - 1 = \prod_{a=0}^{n-1} (x - \zeta_n^a)$$

since by definition, all the $\zeta_n^a$ are the roots of the polynomial $x^n - 1$. Now every element $\zeta_n^a$ of the group of $n$-th roots of unity has an order $d \mid n$. We can group all these elements together, and rewrite the product as

$$x^n - 1 = \prod_{d|n} \prod_{\zeta_n^d = 1} (x - \zeta_n).$$

We then note that if an root of unity has order $d$, it must be a primitive $d$-th root of unity, since by definition it is the smallest integer such that $\zeta_d^d = 1$. It follows that

$$x^n - 1 = \prod_{d|n} \prod_{\substack{1 \le a < d, \\ (a,d)=1}} (x - \zeta_d^a) = \prod_{d|n} \Phi_d(x).$$

This deduction now gives us an iterative way to calculate each cyclotomic polynomial. Suppose we know $\Phi_k(x)$ for all integers $k < n$. We then have

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

$$\Phi_n(x) \prod_{d|n,\ d<n} \Phi_d(x) = x^n - 1$$

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} \Phi_d(x)}.$$

which we can calculate, since all $d$ that divide $n$ are clearly smaller than $n$, so we know all the $\Phi_d(x)$. In Lemma 40 of chapter 13 of [3] it is proven that this division exists in $\mathbb{Z}[x]$ and thus that $\Phi_n(x)$ has coefficients in $\mathbb{Z}$ for all $n$.
Using the above method, we can calculate the $p$-th cyclotomic polynomials for any prime $p$.

**Corollary 2.7.** For any prime $p$, the $p$-th cyclotomic polynomial $\Phi_p(x)$ is equal to

$$x^{p-1} + x^{p-2} + \cdots + x + 1.$$

*Proof.* By the method shown above, we can see that

$$\Phi_n(x) = \frac{x^p - 1}{\prod_{d|p,\ d<n} \Phi_d(x)} = \frac{x^p - 1}{\Phi_1(x)}.$$

It is clear that $\Phi_1(x) = x - 1$ and by using the well-known product

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

we get

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

□

Furthermore, we can give an easy calculation of the cyclotomic polynomial for any prime power.

**Proposition 2.8.** Let $p$ be a prime and $a \ge 1$ an integer. Then $\Phi_{p^a}(x) = \Phi_p(x^{p^{a-1}})$.

*Proof.* We will show this by evaluating $x^{p^a} - 1$ in two different ways. Firstly, we can see that

$$x^{p^a} - 1 = \prod_{d|p^a} \Phi_d(x)$$

and since all divisors of a prime power are smaller prime powers, we have

$$\prod_{d|p^a} \Phi_d(x) = \prod_{i=0}^{a} \Phi_{p^i}(x)$$
$$= \Phi_{p^a}(x) \prod_{i=0}^{a-1} \Phi_{p^i}(x) = \Phi_{p^a}(x)(x^{p^{a-1}} - 1).$$

Now we can also write $x^{p^a} - 1 = (x^{p^{a-1}})^p - 1$. The right side is just the polynomial $x^p - 1$ evaluated in $x^{p^{a-1}}$. By using the identity $x^p - 1 = \Phi_p(x)\Phi_1(x)$ from Corollary 2.7, we get

$$x^{p^a} - 1 = (x^{p^{a-1}})^p - 1 = \Phi_p(x^{p^{a-1}})\Phi_1(x^{p^{a-1}}) = \Phi_p(x^{p^{a-1}})(x^{p^{a-1}} - 1).$$

We now have the equality

$$\Phi_{p^a}(x)(x^{p^{a-1}} - 1) = \Phi_p(x^{p^{a-1}})(x^{p^{a-1}} - 1)$$
$$\Phi_{p^a}(x) = \Phi_p(x^{p^{a-1}})$$

which proves the statement. □

## 2.2 Galois group of cyclotomic extension

In Section 13.6 of [3], it is proven that any $n$-th cyclotomic polynomial is an irreducible monic polynomial in $\mathbb{Z}[x]$. It then follows that $\Phi_n(x)$ must be the minimal polynomial for any primitive $n$-th root of unity over $\mathbb{Q}$. By the definition of the cyclotomic polynomial, the degree of $\Phi_n(x)$ is equal to the number of primitive $n$-th roots of unity, which is equal to the number of $1 \leq a < n$ such that $(a, n) = 1$. This is precisely the value of Euler's totient function $\phi(n)$. We thus conclude that the degree of $\Phi_n(x)$ is $\phi(n)$, and hence also the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$.

Let us now look at $\Phi_8(x)$ as an example. By Propositions 2.7 and 2.8, we know that

$$\Phi_8(x) = \Phi_{2^3}(x) = \Phi_2(x^{2^2}) = \Phi_2(x^4) = 1 + x^4$$

We can check that this is indeed the 8th cyclotomic polynomial. We have for any primitive $\zeta_8$

$$1 + \zeta_8^4 = 1 + \zeta_2 = 1 + (-1) = 0$$

so any primitive 8th root of unity is a root of the polynomial. The degree of $x^4 - 1$ is equal to $4 = \phi(8)$. Furthermore, $x^4 - 1$ is clearly monic and irreducible in $\mathbb{Z}[x]$. Therefore it must be the minimal polynomial for any primitive 8th root of unity, hence the 8th cyclotomic root.
This discussion gives way for another way to proof Proposition 2.8. Let $\zeta_{p^a}$ be primitive. Then we have

$$\Phi_p(\zeta_{p^a}^{p^{a-1}}) = \Phi_p(\zeta_p) = 0$$

by Lemma 2.5. It is easy to check that $\Phi_p(x^{p^{a-1}})$ is monic and irreducible in $\mathbb{Z}[x]$. Therefore it is the unique minimal polynomial for $\zeta_{p^a}$ over $\mathbb{Q}$, and hence the cyclotomic polynomial for $p^a$, i.e. $\Phi_{p^a}(x) = \Phi_p(x^{p^{a-1}})$.

We can now find the Galois group of a cyclotomic extension. We know that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, since it is the splitting field of $x^n - 1$ which is separable (see Proposition 2.1).

As an example, let us now look at the fifth cyclotomic extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$. We know that this has degree $\phi(5) = 4$, and seeing as this extension is Galois, there must be 4 distinct automorphisms. Now let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. From Galois theory we know that $\sigma$ permutes the roots of the minimal polynomial of $\zeta_5$, hence $\sigma$ permutes the roots of $\Phi_5(x)$. It follows that $\sigma(\zeta_5)$ must be equal to one of $\zeta_5$, $\zeta_5^2$, $\zeta_5^3$ and $\zeta_5^4$. This automatically yields us the four automorphisms of the Galois group:

$$\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}), \quad \sigma_i(\zeta_5) := \zeta_5^i, \quad 1 \leq i \leq 4.$$

By composing for example $\sigma_2$ and $\sigma_4$, we get the automorphism defined by

$$\sigma_2 \circ \sigma_4(\zeta_5) = \sigma_2(\zeta_5^4) = \sigma_2(\zeta_5)^4 = \zeta_5^{2\cdot 4} = \zeta_5^8 = \zeta_5^5\zeta_5^3 = \zeta_5^3$$

from which it follows that $\sigma_2 \circ \sigma_4 = \sigma_3$. We note that this is a result of the fact that $2 \cdot 4 \equiv 3 \pmod 5$. This yields to the hypothesis that the Galois group of $\mathbb{Q}(\zeta_5)$ is isomorphic to the multiplicative group $(\mathbb{Z}/5\mathbb{Z})^*$ which also has an order of 4. We can formalise this with the following theorem. The proof is largely based on Theorem 26 of Chapter 14 in [3].

**Proposition 2.9.** Let $\mathbb{Z}_n^* = (\mathbb{Z}/n\mathbb{Z})^*$ denote the multiplicative group of integers modulo $n$. Then the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is isomorphic to $\mathbb{Z}_n^*$ by the isomorphism

$$\begin{aligned} \mathbb{Z}_n^* &\to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a &\mapsto \sigma_a \end{aligned}$$

where $\sigma_a$ is an field automorphism defined by $\sigma_a(\zeta_n) = \zeta_n^a$.

*Proof.* To start, we will show that $\sigma_a$ is a well-defined automorphism. We know that if $a \in \mathbb{Z}_n^*$, then $a$ is relatively prime to $n$, hence $\zeta_n^a$ is a primitive root of unity. As we have seen in the example above, $\sigma_a$ must send $\zeta_n$ to a primitive root, which it does in our case, so the map $\sigma_a$ is an automorphism.
We now show that the proposed isomorphism is an homomorphism. Take $a, b \in \mathbb{Z}_n^*$, then

$$\sigma_a \circ \sigma_b(\zeta_n) = \sigma_a(\zeta_n^b) = (\sigma_a(\zeta_n))^b = \zeta_n^{ab} = \sigma_{ab}(\zeta_n)$$

and by using Lemma 2.4 we get

$$\sigma_{ab}(\zeta_n) = \sigma_c(\zeta_n)$$

where $c \equiv ab \pmod n$ with $0 \leq c < n$ such that $c = ab$ as elements of $\mathbb{Z}_n^*$. Seeing as the automorphisms of these cyclotomic extensions are defined by their action on $\zeta_n$, we can see that $\sigma_a \circ \sigma_b = \sigma_c$ when $ab = c$. Therefore the given map is actually a homomorphism.
What is left to show is that this homomorphism is bijective, and thus an isomorphism. Suppose that $\sigma_a = \sigma_b$. Then also $\sigma_a(\zeta_n) = \sigma_b(\zeta_n)$ and thus $\zeta_n^a = \zeta_n^b$. This can only be true if $a \equiv b \pmod n$, but then $a = b$ as elements of $\mathbb{Z}_n^*$, proving that the homomorphism is injective. Furthermore, we know that both $\mathbb{Z}_n^*$ and the Galois group have an order of $\phi(n)$, so we can conclude that the homomorphism is bijective, and is therefore an isomorphism. □

Section 3

# Primitive elements and traces

This chapter will focus on the subfields of cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ and it will cover the question when these subfields $H$ have a trace, which we will define later, as a primitive element. By the Primitive Element Theorem, we know that these fields must have a primitive element:

**Theorem 3.1** (Primitive Element Theorem)**.** Let $K/F$ be a finite and separable extension. Then $K/F$ has a primitive element, i.e. $K = F(\alpha)$ for some $\alpha \in K$.

We will leave this theorem as given. We know that every finite extension of $\mathbb{Q}$ is separable, so every subfield $H \subseteq \mathbb{Q}(\zeta_n)$ with $\mathbb{Q} \subseteq H$ is separable, since we can see $H$ as an extension of $\mathbb{Q}$. Therefore $H$ has a primitive element. Our goal is now to construct such elements via traces. This question contains several smaller problems, corresponding to the prime factorisation of $n$. We will start with the case that $n = p$, where $p$ is an odd prime.

## 3.1 The case $n = p$

For this case, we will first discuss the subgroups of $\mathbb{Z}_p^*$. The structure of this section is based on Chapter 9.2 of the book *Galois Theory* by Cox [1]. It can be shown that $\mathbb{Z}_p^*$ has an element of order $p-1$ (see [8], Chapter VI, §2 for more details) . We know that $\mathbb{Z}_p^*$ has an order of $p-1$, so it follows that it is a cyclic group. In Theorem 7 of Chapter 2, Dummit and Foote [3] show that for a cyclic group $G$, there is a unique subgroup $H$ for every divisor of the order of the group, i.e. for every $m \mid |G|$, there is a unique subgroup $H \leq G$ with $|H| = m$. This shows that there is a unique subgroup of $\mathbb{Z}_p^*$ for every divisor of $p-1$. This will be useful in the proof that will come.
For example, let us look at the subgroups of $\mathbb{Z}_{13}^*$. We have

$$\mathbb{Z}_1 3^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

It can be shown that 2 is a generator of this group. Then the subgroups are

$$\begin{aligned}
\langle 2^2 \rangle &= \langle 4 \rangle = \{4, 3, 12, 9, 10, 1\} \\
\langle 2^3 \rangle &= \langle 8 \rangle = \{8, 12, 5, 1\} \\
\langle 2^4 \rangle &= \langle 3 \rangle = \{3, 9, 1\} \\
\langle 2^6 \rangle &= \langle 12 \rangle = \{12, 1\}
\end{aligned}$$

correspoding respectively to $6, 4, 3$ and 2, the divisors of $12 = |\mathbb{Z}_{12}^*|$. In this way, we can see that for every divisor $m$ of 12, there is a subgroup of $\mathbb{Z}_{12}^*$ with order $m$.

We can now introduce the notion of an $f$-period.

**Definition 3.2.** Let $p$ be an odd prime, and let $f$ be a divisor of $p-1$. We know that there is a unique subgroup $H_f \leq \mathbb{Z}_p^*$ of order $f$. Then for every $\lambda \in \mathbb{Z}_p^*$ we define an $f$-period by

$$(f, \lambda) = \sum_{a \in H} \zeta_p^{\lambda a}.$$

These $f$-periods are linked to the subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}_p^*$. In fact, it turns out that the subfield of $\mathbb{Q}(\zeta_p)$ fixed by the subgroup $H \leq \mathbb{Z}_p^*$ of order $f$ is generated by any $f$-period. This can be proved using standard Galois theory.

Throughout this section, we will assume that $p$ is an odd prime, and that $p-1 = ef$, so that $f$ is a divisor of $p-1$. Moreover, we will write $H_f$ for the unique subgroup of $\mathbb{Z}_p^*$ of order $f$.

**Lemma 3.3.** Let $\lambda \in \mathbb{Z}_p^*$. There are $e$ distinct conjugates of $(f, \lambda)$ over $\mathbb{Q}$ under the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

*Proof.* We will first note that we can write

$$(f, \lambda) = \sum_{a \in \lambda H_f} \zeta_p^a$$

where $\lambda H_f$ is a coset of $H_f$ in $\mathbb{Z}_p^*$. Note that $\mathbb{Z}_p^*$ is abelian, hence $H_f$ is a normal subgroup. We can then see that two $f$-periods $(f, \lambda)$ and $(f, \mu)$ for some $\lambda, \mu \in \mathbb{Z}_p^*$ are equal if and only if $\lambda H_f = \mu H_f$. The implication to the left is trivial. We will now prove the other one.
From Galois theory, we know that $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ are linearly independent over $\mathbb{Q}$. Then the assumption

$$\begin{aligned} (f, \lambda) &= (f, \mu) \\ (f, \lambda) - (f, \mu) &= 0 \\ \sum_{a \in \lambda H_f} \zeta_p^a - \sum_{b \in \mu H_f} \zeta_p^b &= 0, \end{aligned}$$

would contradict the linear independence if the $\zeta_p^a$ and $\zeta_p^b$ were distinct. Therefore we must have $\lambda H_f = \mu H_f$ if $(f, \lambda) = (f, \mu)$.
It now also follows that the number of distinct $f$-periods is equal to the number of cosets $\lambda H$ of $\mathbb{Z}_p^*$. This is equal to $[\mathbb{Z}_p^* : H_f] = \frac{p-1}{f} = e$.

We can see that a conjugate of an $f$-period is again an $f$-period. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $\sigma(\zeta_p) = \zeta_p^k$ and $k \in \mathbb{Z}_p^*$. Then we have

$$\sigma((f, \lambda)) = \sigma\left(\sum_{a \in H_f} \zeta_p^{\lambda a}\right) = \sum_{a \in H_f} \sigma(\zeta_p)^{\lambda a} = \sum_{a \in H_f} \zeta_p^{k \lambda a} = (f, k\lambda).$$

By taking all the conjugates of $(f, \lambda)$ under the Galois group, we get the set $\{(f, k\lambda) \mid k \in \mathbb{Z}_p^*\}$. Since all the non-distinct $f$-periods cancel out, the size of the set is equal to the number of distinct $f$-periods, which is $e$. As such, there are $e$ distinct Galois conjugates of $(f, \lambda)$ under the group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. □

This now gives way to the following proposition.

**Proposition 3.4.** For every $\lambda \in \mathbb{Z}_p^*$, the $f$-period $(f, \lambda)$ is a primitive element of the fixed field of $H_f$, i.e.

$$\mathbb{Q}((f, \lambda)) = \mathbb{Q}(\zeta_p)^{H_f}$$

where $\mathbb{Q}(\zeta_p)^{H_f}$ is the field consisting of elements that are fixed by the Galois group corresponding to $H_f$.

*Proof.* Let $(f, \lambda_1), \ldots, (f, \lambda_e)$ be the distinct $f$-periods. We will then show that

$$g(x) := \prod_{i=1}^{e} (x - (f, \lambda_i))$$

is the minimal polynomial of any $f$-period over $\mathbb{Q}$. It is clear that any $f$-period is a root of $g(x)$. It is then left to show that $g(x)$ is in $\mathbb{Q}[x]$ and that $g(x)$ is minimal.
We know that any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ permutes the Galois conjugates, so $\sigma$ gives a permutation of all $f$-periods. It then follows that $\sigma$ also permutes the factors $x - (f, \lambda_i)$, and thus

$$\sigma(g(x)) = \prod_{i=1}^{e} \sigma(x - (f, \lambda_i)) = \prod_{i=1}^{e} (x - (f, \lambda_i)) = g(x).$$

Since $g(x)$ is fixed by $\sigma$, its coefficients must also be fixed by $\sigma$ and thus lie in $\mathbb{Q}$, since that is the fixed field. It follows that $g(x) \in \mathbb{Q}[x]$.
We know from Galois theory that every conjugate of $(f, \lambda_i)$ must also be a root of the minimal polynomial, hence $(x-(f, \lambda_i))$ must divide the minimal polynomial for all $1 \leq i \leq e$. The polynomial $g(x)$ is the smallest polynomial for which this holds, so $g(x)$ is the minimal polynomial for all $f$-periods.
We now know that $\mathbb{Q}((f, \lambda))$ has a degree of $e$ over $\mathbb{Q}$, since $g(x)$ is the minimal polynomial and is of degree $e$. It follows that the group fixing $\mathbb{Q}((f, \lambda))$ has index $e$ in $\mathbb{Z}_p^*$, and thus that group has an order of $\frac{p-1}{e} = f$. Since there is exactly one subgroup of $\mathbb{Z}_p^*$ of order $f$, this must be the subgroup $H_f$. So $\mathbb{Q}((f, \lambda))$ is the fixed field of $H_f$, which by definition means

$$\mathbb{Q}((f, \lambda)) = \mathbb{Q}(\zeta_p)^{H_f}$$

proving the proposition. □

## 3.2 The case $n = p^a$

Let $n = p^a$ with $p$ an odd prime and $a \geq 1$. We will now continue our discussion about the primitive elements of the subfields of cyclotomic extension. The proofs in the section are largely based on the proofs given by Gómez-Molleda.
First note that in this case, the group $\mathbb{Z}_n^*$ is cyclic. A proof can be found in Chapter VI, §2 of [8]. Then, just as in the case where $n = p$, it follows that there is a unique subgroup for every divisor of the order of $\mathbb{Z}_n^*$, which is $\phi(n)$. The subgroups of $\mathbb{Z}_n^*$ can then be described as follows.

**Lemma 3.5.** Let $n = p^a$ and let $H_s \subseteq \mathbb{Z}_n^*$ be the unique subgroup of order $p^s$. Then $H_s$ is of the form

$$H_s = \{1 + ip^{a-s} : 1 \leq i \leq p^s\}.$$

*Proof.* We first note that $H_s$ is indeed a subset of $\mathbb{Z}_n^*$, since $1 + ip^{a-s}$ is clearly never divisible by a power of $p$ because of the $+1$ term. It follows that every element of $H_s$ must be coprime with $p^a$, and thus it is a subset of $\mathbb{Z}_n^*$.
We will now show that $H_s$ is closed under multiplication. Let $1 + ip^{a-s}$ and $1 + jp^{a-s}$ be elements of $H_s$ for $1 \leq i, j \leq p^s$. Then we have

$$\begin{aligned}(1 + ip^{a-s})(1 + jp^{a-s}) &= 1 + (i + j)p^{a-s} + ijp^{2(a-s)} \\ &= 1 + (i + j + ijp^{a-s})p^{a-s}.\end{aligned}$$

If $i + j + ijp^{a-s} \leq p^s$, we are done. If however $i + j + ijp^{a-s} > p^s$, then there must be some $k \geq 1$ and $0 \leq r < p^s$ such that $i + j + ijp^{a-s} = kp^s + r$. We then have

$$\begin{aligned}1 + (i + j + ijp^{a-s})p^{a-s} &= 1 + (kp^s + r)p^{a-s} \\ &= 1 + kp^a + rp^{a-s} = 1 + rp^{a-s}\end{aligned}$$

as elements of $\mathbb{Z}_n^*$. This then shows that $H_s$ is closed under multiplication.
The next step is to show that $H_s$ is a group. It is clear that 1 is an element of $H_s$, so we only have to show that each element has its inverse in the subset. Let $1 + ip^{a-s} \in H_s$. We have the formal identity

$$\left(\sum_{k=0}^{\infty}(-1)^k x^k\right)(1 + x) = 1$$

and by substituting $ip^{a-s}$ for $x$ in the sum, we get

$$\sum_{k=0}^{\infty}(-1)^k (ip^{a-s})^k = \sum_{k=0}^{a-1}(-1)^k i^k p^{k(a-s)} + \sum_{k=a}^{\infty}(-1)^k i^k p^{k(a-s)}.$$

We can see that all the terms in the second sum have a power of $p$ that is greater or equal to $a$, hence all those terms are a multiple of $p^a$, and they thus vanish in $\mathbb{Z}_n^*$. It follows that

$$\left(\sum_{k=0}^{a-1}(-1)^k i^k p^{k(a-s)}\right)(1 + ip^{a-s}) = 1$$

and thus the inverse of $(1 + ip^{a-s})$ is

$$\sum_{k=0}^{a-1}(-1)^k i^k p^{k(a-s)} = 1 + \left(\sum_{k=1}^{a-1}(-1)^k i^k p^{(k-1)(a-s)}\right)p^{a-s}.$$

This is a valid element of $H_s$, by the same argument used to prove that $H_s$ is closed under multiplication. We can see thus see that any element of $H_s$ has an inverse in the group, proving that it is a subgroup of $\mathbb{Z}_n^*$.

It is clear that there are $p^s$ elements in $H_s$, since it contains all $1 + ip^{a-s}$ for $1 \leq i \leq p^s$, and these are all distinct. We conclude that $H_s$ must be the unique subgroup of $\mathbb{Z}_n^*$ with $p^s$ elements. □

From now on, we will denote the unique subgroup of $\mathbb{Z}_n^*$ of order $p^s$ with $H_s$.
In the case where $n = p$, we saw that $f$-periods took the role as primitive elements of the subfields of cyclotomic extension. For the upcoming discussion, we need a more general concept.

**Definition 3.6.** Let $K/F$ be a field extension, and $\alpha \in K$. Then the trace of $\alpha$ is defined as

$$\mathrm{Tr}_F^K(\alpha) := \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$$

which is the sum of all the Galois conjugates of $\alpha$.

One important property of the trace is that it is transitive.

**Proposition 3.7** (Transivity of the trace)**.** Let $K/L/F$ be Galois field extensions. Then for any $x \in K$ we have

$$\mathrm{Tr}_F^K(x) = \mathrm{Tr}_F^L(\mathrm{Tr}_L^K(x)).$$

*Proof.* Let us define $G := \mathrm{Gal}(K/F)$ and $H := \mathrm{Gal}(K/L)$. By assumption, $L/F$ is also Galois, so it follows from the Fundamental Theorem of Galois Theory that $\mathrm{Gal}(L/F) \equiv G/H$. We can then see that

$$\begin{aligned}\mathrm{Tr}_F^L(\mathrm{Tr}_L^K(x)) &= \sum_{\tau \in \mathrm{Gal}(L/F)} \tau \left( \sum_{\sigma \in \mathrm{Gal}(K/L)} \sigma(x) \right) \\ &= \sum_{\tau \in G/H} \tau \left( \sum_{\sigma \in H} \sigma(x) \right).\end{aligned}$$

We can see each element $\tau \in G/H$ as a representative of the cosets of $H$ in $G$. Then each element $\gamma \in G$ can be uniquely written as $\tau\sigma$, with $\sigma \in H$. It then follows that

$$\sum_{\tau \in G/H} \tau \left( \sum_{\sigma \in H} \sigma(x) \right) = \sum_{\tau \in G/H} \sum_{\sigma \in H} \tau\sigma(x) = \sum_{\gamma \in G} \gamma(x) = \mathrm{Tr}_F^K(x)$$

which proves the statement. □

As noted in the introduction of this thesis, the trace is a natural candidate to be a primitive element of $\mathbb{Q}(\zeta_n)^H$. However, there are cases when the trace cannot be a primitive element because it vanishes. For example, let us take $n = 9 = 3^2$. Then the trace over the subgroup $H = \{1, 8\}$ of $\mathbb{Z}_9^*$ is

$$\sum_{\sigma \in H} \sigma(\zeta_9) = \sigma_1(\zeta_9) + \sigma_8(\zeta_9) = \zeta_9 + \zeta_9^8 = \zeta_9 + \zeta_9^{-1}$$

which does not vanish. Here we used the defintions of $\sigma_a$ introduced in Proposition 2.9. Moreover, we know that $\mathbb{Q}(\zeta_9)^H$ is fixed by $\sigma_1$ and $\sigma_8 = \sigma_{-1}$. The map $\sigma_{-1}$ maps all the roots of unity to their inverse, which always just the complex conjugate. Hence, the only elements invariant under $\sigma_{-1}$ are the real numbers. It can be shown that the largest real subfield of $\mathbb{Q}(\zeta_9)$ is equal to

$$\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$$

which is exactly the field generated by the trace over $H$. So in this case, the trace does not vanish and is a primitive element of $\mathbb{Q}(\zeta_9)^H$.

Now let us take the subgroup $H_1 = \{1, 4, 7\}$ by Lemma 3.5. Then the trace is

$$\begin{aligned}\sum_{\sigma \in H_1} \sigma(\zeta_9) &= \sigma_1(\zeta_9) + \sigma_4(\zeta_9) + \sigma_7(\zeta_9) \\ &= \zeta_9 + \zeta_9^4 + \zeta_9^7 \\ &= \zeta_9(1 + \zeta_9^3 + \zeta_9^6) \\ &= \zeta_9(1 + \zeta_3 + \zeta_3^2).\end{aligned}$$

However, we know by the third cyclotomic polynomial that $1 + \zeta_3 + \zeta_3^2 = 0$, so in this case the trace vanishes. It is then clear that it cannot be a primitive element. This leads us to the question of when the trace is equal to zero. Before we can answer this for the case where $n = p^a$ with $p$ an odd prime, we first need to proof a technical lemma.

**Lemma 3.8.** The set of all integers up to $p^t$, $\{m : 1 \leq m \leq p^t\}$, is equal to the set

$$\{ip^{t-1} + j : 0 \leq i \leq p-1,\ 1 \leq j \leq p^{t-1}\}$$

*Proof.* First suppose that $m = ip^{t-1} + j$ for some $0 \leq i \leq p-1$, $1 \leq j \leq p^{t-1}$. Then it easy to see that $m \geq 0 \cdot p^{t-1} + 1 = 1$ and $m \leq (p-1)p^{t-1} + p^{t-1} = p^t - p^{t-1} + p^{t-1} = p^t$, from which it follows that $1 \leq m \leq p^t$.

Now suppose that $1 \leq m \leq p^t$. Then $m = m' \pmod{p^{t-1}}$ for some $1 \leq m' \leq p^{t-1}$. It then follows that

$$\begin{aligned}m - m' &= kp^{t-1} \\ m &= kp^{t-1} + m'\end{aligned}$$

for some $k \in \mathbb{Z}$. We can see that $k \geq 0$, because otherwise, we would have $m - m' < 0$ and thus $m' < m$. This is not possible, since $m'$ is the result of taking $m$ modulo $p^{t-1}$, so it can't be larger. Furthermore, we also have $k \leq p-1$, because otherwise, we would have $k \geq p$ and thus

$$m \geq pp^{t-1} + m' = p^t + m' > p^t$$

which is a contradiction. Hence we have $0 \leq k \leq p-1$. We conclude that $m$ is of the form $ip^{t-1} + j$ with $0 \leq i \leq p-1$ and $1 \leq j \leq p^{t-1}$. □

We can now prove the theorem that shows us when the trace vanishes for $n = p^a$.

**Theorem 3.9.** Let $H$ be a proper subgroup of $\mathbb{Z}_n^*$ with $n = p^a$, $p$ an odd prime. Then $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n) = 0$ if and only if $p$ divides $|H|$.

*Proof.* We start by proving that the trace is equal to 0 in the case where $H = H_s$ for some $s \leq a-1$. This is applicable to the theorem, since $|H_s| = p^s$, and thus $p \mid |H_s|$. For $n = p^a$, we know that the $n$-th cyclotomic polynomial is

$$\Phi_n(x) = \Phi_p(x^{p^{a-1}}) = \sum_{i=0}^{p-1} x^{ip^{a-1}}$$

and noting that $\zeta_n$ is a root of the cyclotomic polynomial, we get

$$\Phi_n(\zeta_n) = \sum_{i=0}^{p-1} \zeta_n^{ip^{a-1}} = 0 \tag{3.1}$$

We then see that

$$\begin{aligned}
\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^{H_s}}(\zeta_n) &= \sum_{\sigma \in H} \zeta_n^{\sigma} \\
&= \sum_{i=1}^{p^s} \zeta_n^{1+ip^{a-s}} \\
&= \zeta_n \sum_{i=1}^{p^s} \zeta_n^{ip^{a-s}}
\end{aligned}$$

By using Lemma 3.8, we can split the sum as follows:

$$\begin{aligned}
\zeta_n \sum_{i=1}^{p^s} \zeta_n^{ip^{a-s}} &= \zeta_n \sum_{j=1}^{p^{s-1}} \sum_{i=0}^{p-1} \zeta_n^{(ip^{s-1}+j)p^{a-s}} \\
&= \zeta_n \sum_{j=1}^{p^{s-1}} \sum_{i=0}^{p-1} \zeta_n^{ip^{a-1}} \zeta_n^{jp^{a-s}} \\
&= \zeta_n \sum_{j=1}^{p^{s-1}} \zeta_n^{jp^{a-s}} \sum_{i=0}^{p-1} \zeta_n^{ip^{a-1}} \\
\text{(by (3.1))} \quad &= \zeta_n \sum_{j=1}^{p^{s-1}} \zeta_n^{ip^{a-1}} \cdot 0 = 0
\end{aligned}$$

We can thus see that the trace over $H_s$ is equal to 0.

Let us now assume that $p$ divides $|H|$. Then $|H| = mp^s$ with $m$ not divisible by $p$ and $s \geq 1$. We know that $\mathbb{Z}_n^*$ is cyclic, so $H$ is also cyclic. We know that a cyclic group has a unique subgroup for every divisor of its order. Since $p^s \mid mp^s$ we have $H_s \leq H$. From Galois Theory, we then know that $\mathbb{Q}(\zeta_n)^H$ is a subfield of $\mathbb{Q}(\zeta_n)^{H_s}$. Now by using the transivity of the trace, we see that

$$\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n) = \mathrm{Tr}^{\mathbb{Q}(\zeta_n)^{H_s}}_{\mathbb{Q}(\zeta_n)^H}\left(\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^{H_s}}(\zeta_n)\right) = \mathrm{Tr}^{\mathbb{Q}(\zeta_n)^{H_s}}_{\mathbb{Q}(\zeta_n)^H}(0) = 0$$

which proves the implication.

Let us now assume that $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n) = 0$ for some proper subgroup $H$ of $\mathbb{Z}_n^*$. Suppose that $|H| = l$. We know that $H$ is a subgroup of a cyclic group, so itself is cyclic. Suppose that it has generator $g$. We then see that

$$\begin{aligned}
\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n) &= 0 \\
\sum_{\sigma \in H} \zeta_n^{\sigma} &= 0 \\
\sum_{i=0}^{l-1} \zeta_n^{g^i} &= 0
\end{aligned}$$

It follows that the polynomial $f(x) := \sum_{i=0}^{l-1} x^{g^i}$ must have $\Phi_n(x)$ as a divisor, hence

$$f(x) = \Phi_n(x)\psi(x)$$

for some $\psi(x) \in \mathbb{Z}[x]$. By substituting $x = 1$, we get

$$\begin{aligned} f(1) &= \Phi_n(1)\psi(1) \\ l &= p \cdot \psi(1) \end{aligned}$$

and thus we can see that $p$ is a divisor of $q = |H|$, proving the theorem. □

The last part of the proof was based on §2 of the article by Fuchs [5].

Our goal is now to show that $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n)$ is the primitive element of $\mathbb{Q}(\zeta_n)^H$ when it is non-zero. This is proven by Evans [4] (Theorem 6) for general $n$. However, since in this thesis we are focused on the case that $n = p^a$, we will only prove it for that case.

**Theorem 3.10.** Let $n = p^a$ with $p$ an odd prime and let $H$ be subgroup op $\mathbb{Z}_n^*$. Then $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n)$ is a primitive element of $\mathbb{Q}(\zeta_n)^H$ if and only if $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n) \neq 0$.

*Proof.* If $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n)$ is a primitive element, then it obviously cannot be equal to zero. So the implication to the right is trivial.

Suppose now that $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n) \neq 0$. The proof will follow the same structure as the proofs of Lemma 3.3 and Proposition 3.4. We again want to prove that for $\lambda, \mu \in \mathbb{Z}_n^*$, two sums $\sum_{\sigma\in\lambda H} \zeta_n^\sigma$ and $\sum_{\tau\in\mu H} \zeta_n^\tau$ can only be equal if $\lambda H = \mu H$. Note that we can interpret any $\lambda \in \mathbb{Z}_n^*$ in two ways: firstly just as an element of $\mathbb{Z}_n^*$, and secondly as an automorphism of the $n$-th cyclotomic extension, as the Galois group is isomorphic to $\mathbb{Z}_n^*$. In the second case, we will interpret $\lambda$ as the automorphism defined by $\lambda(\zeta_n) = \zeta_n^\lambda$. Throughout this proof, we will use these two interpretation interchangeably.
We first note that we can write

$$\sum_{\sigma\in\lambda H} \zeta_n^\sigma = g(\zeta_n) + k(\zeta_n)$$

where $g$ is a polynomial such that $g(\zeta_n)$ only contains the powers $\zeta_n^i$ with $p^{a-1}(p-1) \leq i < p^a$, and $k$ a polynomial such that $k(\zeta_n)$ only contains the powers $\zeta_n^i$ with $0 \leq i < p^{a-1}(p-1)$. We can then write

$$\begin{aligned} \sum_{\sigma\in\lambda H} \zeta_n^\sigma &= g(\zeta_n) + k(\zeta_n) \\ &= \zeta_n^{p^{a-1}(p-1)} h(\zeta_n) + k(\zeta_n). \end{aligned} \tag{3.2}$$

where $h$ is a polynomial such that $h(\zeta_n)$ only contains the powers of $\zeta_n$ with exponents between 0 and $p^{a-1}$.
From the cyclotomic polynomial for $n = p^a$, we know that

$$\sum_{i=0}^{p-1} \zeta_n^{ip^{a-1}} = 0$$

and therefore

$$\zeta_n^{p^{a-1}(p-1)} = -\sum_{i=0}^{p-2} \zeta_n^{ip^{a-1}}.$$

By substituting this into (3.2), we get

$$\sum_{\sigma\in\lambda H} \zeta_n^{\sigma} = \left(-\sum_{i=0}^{p-2} \zeta_n^{ip^{a-1}}\right) h(\zeta_n) + k(\zeta_n).$$

In the same way, we can write

$$\sum_{\tau\in\mu H} \zeta_n^{\tau} = \left(-\sum_{i=0}^{p-2} \zeta_n^{ip^{a-1}}\right) \tilde{h}(\zeta_n) + \tilde{k}(\zeta_n).$$

where $\tilde{h}$ and $\tilde{k}$ have the same properties as $h$ and $k$. Now by equating the two sums, we get

$$\sum_{\sigma\in\lambda H} \zeta_n^{\sigma} = \sum_{\tau\in\mu H} \zeta_n^{\tau}$$

$$\left(-\sum_{i=0}^{p-2} \zeta_n^{ip^{a-1}}\right) h(\zeta_n) + k(\zeta_n) = \left(-\sum_{i=0}^{p-2} \zeta_n^{ip^{a-1}}\right) \tilde{h}(\zeta_n) + \tilde{k}(\zeta_n). \tag{3.3}$$

We see that all the exponents in $-\sum_{i=0}^{p-2} \zeta_n^{ip^{a-1}}$ are less or equal than $p^{a-1}(p-2)$, and we know that all exponents in $h$ and $\tilde{h}$ are strictly less than $p^{a-1}$. Therefore, all the exponents of $\zeta_n$ in (3.3) must be strictly less than $p^{a-1}(p-1)$. Hence, by shifting all the terms of (3.3) to one side, we get a polynomial $p(x)$ over $\mathbb{Q}$ with degree strictly less than $p^{a-1}(p-1)$ such that $p(\zeta_n) = 0$. We know that $\zeta_n$ has degree $p^{a-1}(p-1)$ over $\mathbb{Q}$, so this is a contradiction. The only case when this is not a contradiction, is when $p(x)$ is the zero polynomial, i.e.

$$p(x) = \left(-\sum_{i=0}^{p-2} x^{ip^{a-1}}\right) (h(x) - \tilde{h}(x)) + k(x) - \tilde{k}(x) \equiv 0.$$

By (3.3), this is equivalent with

$$\sum_{\sigma\in\lambda H} x^{\sigma} - \sum_{\tau\in\mu H} x^{\tau} \equiv 0$$

$$\sum_{\sigma\in\lambda H} x^{\sigma} \equiv \sum_{\tau\in\mu H} x^{\tau}$$

from which it follows that

$$\sum_{\sigma\in\lambda H} \zeta_n^{\sigma} = \sum_{\tau\in\mu H} \zeta_n^{\tau}$$

This is the case when $\lambda H = \mu H$ or when $\sum_{\sigma\in\lambda H} \zeta_n^{\sigma} = \sum_{\tau\in\mu H} \zeta_n^{\tau} = 0$. We assumed that $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)^H}^{\mathbb{Q}(\zeta_n)}(\zeta_n) \neq 0$, so we have

$$\sum_{\sigma\in\lambda H} \zeta_n^{\sigma} = \sum_{\sigma\in H} \zeta_n^{\lambda\sigma} = \sum_{\sigma\in H} \lambda(\zeta_n^{\sigma}) = \lambda\left(\sum_{\sigma\in H} \zeta_n^{\sigma}\right) \neq 0.$$

Since $\lambda$ is an isomorphism, it maps a non-zero element to another non-zero element, hence the sum is not equal to zero.
The only case left is that $\lambda H = \mu H$. That proves that $\sum_{\sigma\in\lambda H}\zeta_n^\sigma$ and $\sum_{\tau\in\mu H}\zeta_n^\tau$ can only be equal if $\lambda H = \mu H$. It follows that each $\sum_{\sigma\in\lambda H}\zeta_n^\sigma$ is distinct for all the different cosets $\lambda H$. Furthermore, they are all conjugates under the group $\mathbb{Z}_n^*$, since

$$\mu\left(\sum_{\sigma\in\lambda H}\zeta_n^\sigma\right) = \sum_{\sigma\in\lambda H}\mu(\zeta_n^\sigma) = \sum_{\sigma\in\lambda H}\zeta_n^{\mu\sigma} = \sum_{\sigma\in\mu\lambda H}\zeta_n^\sigma$$

for all $\mu \in \mathbb{Z}_n^*$. Therefore, just as in Lemma 3.3, the number of Galois conjugates of $\sum_{\sigma\in\lambda H}\zeta_n^\sigma$ is equal to the number of cosets of $H$, which is $|\mathbb{Z}_n^*/H|$.

Now, just as in Proposition 3.4 we can show that

$$g(x) := \prod_{\lambda\in\mathbb{Z}_n^*/H}\left(x - \sum_{\sigma\in\lambda H}\zeta_n^\sigma\right)$$

is the minimal polynomial for $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n)$. It is clear that the trace is a root of this polynomial. We will omit the other steps to show that this is indeed the minimal polynomial, since they are exactly the same as in Proposition 3.4.
We now know that $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n)$ has degree $|\mathbb{Z}_n^*/H|$ over $\mathbb{Q}$. The subgroup $H$ has an index of $|\mathbb{Z}_n^*/H|$, so by Galois theory we know that $\mathbb{Q}(\zeta_n)^H$ also has degree $|\mathbb{Z}_n^*/H|$ over $\mathbb{Q}$. The group $\mathbb{Z}_n^*$ is cyclic, so $H$ is the unique subgroup of its order. It follows that $\mathbb{Q}(\zeta_n)^H$ must be the unique subfield of $\mathbb{Q}(\zeta_n)$ with degree $|\mathbb{Z}_n^*/H|$ over $\mathbb{Q}$, and therefore

$$\mathbb{Q}(\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n)) = \mathbb{Q}(\zeta_n)^H$$

i.e. it is the primitive element of $\mathbb{Q}(\zeta_n)^H$. □

By combining this theorem and Theorem 3.9, we get the following result.

**Corollary 3.11.** Let $n = p^a$ with $p$ an odd prime and let $H$ be a subgroup of $\mathbb{Z}_n^*$. Then $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n)$ is a primitive element of $\mathbb{Q}(\zeta_n)^H$ if and only if $p$ does not divide $|H|$.

We now have a generator for every subfield of $\mathbb{Q}(\zeta_n)$ corresponding to the groups that don't have $p$ as a divisor of the order of the group. However, our goal is to show that every subfield of $\mathbb{Q}(\zeta_n)$ has some trace as a primitive element. This can be done by not taking the trace of $\zeta_n$, but of a power of $\zeta_n$. To understand these subfields based on powers of $\zeta_n$, we will start with a simple lemma.

**Lemma 3.12.** Let $n = p^a$ with $p$ an odd prime and let $H_s \leq \mathbb{Z}_n^*$ be a subgroup of order $p^s$ as described in Lemma 3.5. Then $\mathbb{Q}(\zeta_n)^{H_s} = \mathbb{Q}(\zeta_n^{p^s})$

*Proof.* Let $\sigma \in H_s$. Then, by Lemma 3.5, for some $1 \leq i \leq p^s$ we have

$$\sigma(\zeta_n^{p^s}) = (\zeta_n^{p^s})^{1+ip^{a-s}} = \zeta_n^{p^s+ip^a} = \zeta_n^{p^s}$$

and therefore $\zeta_n^{p^s}$ is fixed by $H_s$, hence $\mathbb{Q}(\zeta_n^{p^s}) \subseteq \mathbb{Q}(\zeta_n)^{H_s}$.
Assume now that for some integer $k$, the power $\zeta_n^k$ is fixed by $H_s$. We then have

$$\begin{aligned}(\zeta_n^k)^{1+ip^{a-s}} &= \zeta_n^k\\ \zeta_n^{k+kip^{a-s}} &= \zeta_n^k.\end{aligned}$$

for all $1 \leq i \leq p^s$. This is only true when

$$\begin{aligned} k + ikp^{a-s} &\equiv k \pmod{n} \\ ikp^{a-s} &\equiv 0 \pmod{n} \end{aligned}$$

for all $1 \leq i \leq p^s$. We see that this only holds when $k = p^s \pmod{n}$. Therefore $\mathbb{Q}(\zeta_n)^{H_s} \subseteq \mathbb{Q}(\zeta_n^{p_s})$, and hence $\mathbb{Q}(\zeta_n)^{H_s} = \mathbb{Q}(\zeta_n^{p^s})$. □

We can now give a proof of the final theorem of this section.

**Theorem 3.13.** Let $n = p^a$ with $p$ an odd prime and let $H \leq \mathbb{Z}_n^*$. Suppose that $|H| = mp^s$, with $1 \leq s \leq a$ and $m \geq 1$ such that $(m, p) = 1$. Then $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)^H}^{\mathbb{Q}(\zeta_n)}(\zeta_n^{p^s})$ is a primitive element of $\mathbb{Q}(\zeta_n)^H$ over $\mathbb{Q}$.

*Proof.* By Lemma 2.5 we know that $\zeta_n^{p^s} = \zeta_{n'}$ with $n' = p^{a-s}$. Our goal will thus be to reduce the trace so that is is only taken over field extensions generated by $\zeta_{n'}$, and then use Corollary 3.11. We see that $p^s \mid |H|$, and since $H$ is cyclic, we have $H_s \leq H$. By the Fundamental Theorem of Galois Theory, we then also have that $\mathbb{Q}(\zeta_n)^H$ is exactly the subfield of $\mathbb{Q}(\zeta_n)^{H_s}$ fixed by $H/H_s$, i.e. $\mathbb{Q}(\zeta_n)^H = (\mathbb{Q}(\zeta_n)^{H_s})^{H/H_s}$. By Lemma 3.12 we then have

$$\mathbb{Q}(\zeta_n)^H = \mathbb{Q}(\zeta_n^{p^s})^{H/H_s} = \mathbb{Q}(\zeta_{n'})^{H/H_s}. \tag{3.4}$$

By noting that every $\sigma \in H$ can be written as the combination of a $\tau \in H_s$ and a $\gamma \in H/H_s$, seen as representatives of the cosets of $H_s$, we can rewrite the trace as

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}(\zeta_n)^H}^{\mathbb{Q}(\zeta_n)}(\zeta_n^{p^s}) = \sum_{\sigma \in H} \zeta_n^{p^s} &= \sum_{\gamma \in H/H_s} \sum_{\tau \in H_s} \gamma\tau(\zeta_n^{p^s}) \\ &= \sum_{\gamma \in H/H_s} \gamma \left( \sum_{\tau \in H_s} \zeta_n^{\tau p^s} \right) \end{aligned} \tag{3.5}$$

and again by using Lemma 3.5, we get

$$\begin{aligned} \sum_{\gamma \in H/H_s} \gamma \left( \sum_{\tau \in H_s} \zeta_n^{\tau p^s} \right) &= \sum_{\gamma \in H/H_s} \gamma \left( \sum_{i=1}^{p^s} \zeta_n^{(1+ip^{a-s})p^s} \right) \\ &= \sum_{\gamma \in H/H_s} \gamma \left( \sum_{i=1}^{p^s} \zeta_n^{p^s + ip^a} \right) \\ &= \sum_{\gamma \in H/H_s} \gamma \left( \sum_{i=1}^{p^s} \zeta_n^{p^s} \right) = \sum_{\gamma \in H/H_s} \gamma(p^s \zeta_n^{p^s}) = p^s \sum_{\gamma \in H/H_s} \gamma(\zeta_n^{p^s}). \end{aligned} \tag{3.6}$$

Here we used that $p^s$ is an integer, and thus not changed by $\gamma$. Now we know that $\mathrm{Gal}(\mathbb{Q}(\zeta_{n'})/\mathbb{Q}(\zeta_{n'})^{H/H_s}) = H/H_s$, so therefore

$$\sum_{\gamma \in H/H_s} \gamma(\zeta_n^{p^s}) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{n'})^{H/H_s}}^{\mathbb{Q}(\zeta_{n'})}(\zeta_{n'}).$$

We know that $n' = p^{a-s}$, so it is still a power of $p$. Furthermore, $|H/H_s| = |H|/|H_s| = \frac{mp^s}{p^s} = m$, and by assumption we have $(m, p) = 1$ and thus $p$ does not divide $m = |H/H_s|$. Therefore, by Corollary 3.11, $\mathrm{Tr}^{\mathbb{Q}(\zeta_{n'})}_{\mathbb{Q}(\zeta_{n'})^{H/H_s}}(\zeta_{n'})$ is a primitive element of $\mathbb{Q}(\zeta_{n'})^{H/H_s}$. By equations (3.5) and (3.6), we already had

$$\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n^{p^s}) = p^s \mathrm{Tr}^{\mathbb{Q}(\zeta_{n'})}_{\mathbb{Q}(\zeta_{n'})^{H/H_s}}(\zeta_{n'})$$

so $\mathrm{Tr}^{\mathbb{Q}(\zeta_n)}_{\mathbb{Q}(\zeta_n)^H}(\zeta_n^{p^s})$ is also a primitive element of $\mathbb{Q}(\zeta_{n'})^{H/H_s}$, which is equal to $\mathbb{Q}(\zeta_n)^H$ by (3.4). This proves the statement. □

In this way we have found a primitive element for the cases where $|H| = mp^s$, i.e. where $p$ divides the order of $H$. Combining this with Corollary 3.11, we have found a primitive element for all cases of $H$. We thus have the conclusion for this section that if $n = p^a$ with $p$ an odd prime, for every subfield $\mathbb{Q}(\zeta_n)^H$ of $\mathbb{Q}(\zeta_n)$, there exist some trace of a power of $\zeta_n$, such that it is the primitive element of $\mathbb{Q}(\zeta_n)^H$.

## Section 4

# Fields generated by polygon diagonals

In the previous sections, we interpreted the roots of unity mostly as algebraic concepts. However, they can also be used in geometrical problems, as the roots of unity form the vertices of a regular polygon in the complex plane. This section will explore one geometrical application of roots of unity. This was originally planned to be the main subject of this thesis. However, as will be explained later, one of the main sources for this subject, the paper by Grubb and Wolird [7], revealed to have some mistakes in it, consequently limiting the possibilities to futher explore this subject. Still, we will attempt to give a clear rundown of this subject.

This section will mostly cover the diagonals of regular polygons. It is a well-known fact that the golden ratio appears in the regular pentagon as the ratio between a diagonal and an edge, as is demonstrated here below:

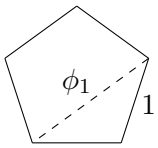


Figure 4.1: The golden ratio in the regular pentagon

This can be proven using similar triangles and basic geometry. In the parts of [7], the main problem resolves about finding the *metallic means* as diagonals in regular polygons. The golden ratio can be defined using the the polynomial problem $x^2 - x - 1 = 0$. This yields the solutions $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$, of which the first one is defined as the golden ratio. We can also generalize the golden ratio. By taking the polynomial $x^2 - mx - 1 = 0$, where $m$ is an positive integer, we get a family of positive solutions of these polynomials. These solutions are called the *metallic means* and can be written as

$$\phi_m = \frac{m + \sqrt{m^2 + 4}}{2}.$$

Using this notation, the golden ratio is written as $\phi = \phi_1$.

If we now want to find the polygons where these metallic means appear as ratios between line segments, we can use the roots of unity. As we have seen in chapter 2, the $n$-th roots of unity form the vertices of a regular $n$-gon.

Therefore, any diagonal of a regular polygon can be written as the linepiece between two roots of unity, or

$$\zeta_n^a - \zeta_n^b$$

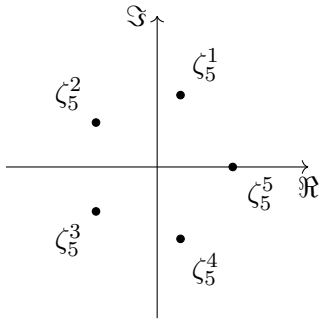


Figure 4.2: The fifth roots of unity form the regular pentagon

for $1 \leq a, b \leq n$. For instance, the diagonal between $1 = \zeta_3^0$ and $\zeta_3$ can be written as $\zeta_3 - \zeta_3^0 = \zeta_3 - 1$. For this problem, we are only interested in the ratio between line segments, hence the only important parts of the line segments are the length of the segments. We will thus look at the length of the complex numbers, in our example $|\zeta_3 - 1|$. If we write a general $n$-th root of unity as $\zeta_n^a$, where $1 \leq a < n$, then the ratio of two line segments within a regular $n$-gon can be written as

$$\frac{\left|\zeta_n^a - \zeta_n^b\right|}{|\zeta_n^c - \zeta_n^d|}$$

with $1 \leq a, b, c, d < n$. Seeing as a regular polygon is rotational symmetric and we are interested in the ratio between line segments, it is sufficient to only look at line segments that start at 1. Hence for our problem, we will look at the ratio

$$\frac{|1 - \zeta_n^a|}{|1 - \zeta_n^b|}$$

for some $1 \leq a, b < n$.

Our focus now will not be to find such ratios for metallic means, but rather to figure out the degrees of the field extensions generated by these ratios of polygon diagonals. We will write $d_1 = |1 - \zeta_n^a|$ and $d_2 = |1 - \zeta_n^b|$. Then we are interested in the degree of $\mathbb{Q}(\frac{d_1}{d_2})$ over $\mathbb{Q}$. In [7], the following result is given:

**Claim 4.1** (Theorem 2 in [7], Grubb, Wolird)**.** Let $d_1 = |1 - \zeta_n^a|$ and $d_2 = |1 - \zeta_n^b|$ be two diagonals of a regular $n$-gon with $a$ and $b$ coprime integers. Then

$$[\mathbb{Q}(\tfrac{d_1}{d_2}) : \mathbb{Q}] = \frac{\phi(4n)}{4} \quad \text{if } n \text{ is odd,}$$
$$[\mathbb{Q}(\tfrac{d_1}{d_2}) : \mathbb{Q}] \geq \frac{\phi(4n)}{10} \quad \text{if } n \text{ is even.}$$

However, this claim is not correct. Take for instance $n = 5$, $a = 1$ and $b = 4$. Then $d_1 = |1 - \zeta_5|$ and $d_2 = |1 - \zeta_5^4| = |1 - \zeta_5^{-1}|$. We now claim that the complex conjugate of any $\zeta_n$ is exactly $\zeta_n^{-1}$. We can show this by using Euler's formula on the root of unity. As we already saw in Chapter 2, we have

$$\overline{\zeta_n} = \overline{e^{\frac{2\pi k i}{n}}} = \cos(2\pi i k/n) - i \sin(2\pi i k/n).$$

We then see that

$$\begin{aligned}\zeta_n\overline{\zeta_n} &= (\cos(2\pi ik/n) + i\sin(2\pi ik/n))(\cos(2\pi ik/n) - i\sin(2\pi ik/n)) \\ &= \cos^2(2\pi ik/n) + \sin^2(2\pi ik/n) = 1\end{aligned}$$

and then by definition, we have $\overline{\zeta_n} = \zeta_n^{-1}$. We now note that 1 is on the real number line, so the distance from 1 to any complex number must be the same as the distance from 1 to the conjugate of that number, and thus

$$d_1 = |1 - \zeta_5| = |1 - \overline{\zeta_5}| = |1 - \zeta_5^{-1}| = d_2.$$

We can then conclude that $\frac{d_1}{d_2} = 1$ and thus the degree of $\mathbb{Q}(\frac{d_1}{d_2})$ over $\mathbb{Q}$ is 1 in this case. However, since 5 is odd, by the given theorem we should have $[\mathbb{Q}(\frac{d_1}{d_2}) : \mathbb{Q}] = \frac{\phi(20)}{4} = \frac{8}{4} = 2 \neq 1$. It follows that this theorem cannot be true.

The fact that Claim 4.1 is false seems to be a result of two false statements made in the paper by Grubb and Wolird. We will now cover these claims and give counterproofs to show that they are false.

In order to prove Claim 4.1, Grubb and Wolird first calculate the degrees of some larger field extensions. They note that $\frac{d_1}{d_1} \in \mathbb{Q}(d_1, d_2)$, and thus $\mathbb{Q}(\frac{d_1}{d_2}) \subseteq \mathbb{Q}(d_1, d_2)$. Additionally, by rewriting $d_1$, we get

$$\begin{aligned}d_1 = |1 - \zeta_n^a| &= \sqrt{(1 - \zeta_n^a)\overline{(1 - \zeta_n^a)}} \\ &= \sqrt{(1 - \zeta_n^a)(1 - \zeta_n^{-a})} \\ &= \sqrt{(1 - \zeta_n^a)\zeta_n^{-a}(\zeta_n^a - 1)} \\ &= \sqrt{-\zeta_n^{-a}(1 - \zeta_n^a)^2}.\end{aligned}$$

Now by using Lemma 2.5 and the fact that $i = \zeta_4 = \zeta_{4n}^n$, we get

$$\begin{aligned}\sqrt{-\zeta_n^{-a}(1 - \zeta_n^a)^2} &= \sqrt{-1 \cdot \zeta_{2n}^{-2a}(1 - \zeta_n^a)^2} \\ &= i\zeta_{2n}^{-a}(1 - \zeta_n^a) \\ &= \zeta_{4n}^n\zeta_{4n}^{-2a}(1 - \zeta_{4n}^{4a}) \\ &= \zeta_{4n}^{n-2a} - \zeta_{4n}^{n+2a} \\ &= \zeta_{4n}^{n-2a} + \zeta_{4n}^{2n}\zeta_{4n}^{n+2a} \\ &= \zeta_{4n}^{n-2a} + \zeta_{4n}^{3n+2a}\end{aligned}$$

This element is of the form $\zeta_{4n}^m + \zeta_{4n}^{-m}$ for some integer $m$. It can be proven by induction that elements of this form can be written as a combination of powers of $\zeta_{4n} + \zeta_{4n}^{-1}$. For the sake of brevity, we will omit this proof. It then follows that $d_1 \in \mathbb{Q}(\zeta_{4n} + \zeta_{4n}^{-1})$, which is also known as the largest real subfield of $\mathbb{Q}(\zeta_{4n})$, and is denoted by $\mathbb{Q}(\zeta_{4n})^+$ by Grubb and Wolird. In the same way,

it can be shown that $d_2 \in \mathbb{Q}(\zeta_{4n})^+$. Then there are the field inclusions

$$\begin{array}{c} \mathbb{Q}(\zeta_{4n}) \\ | \\ \mathbb{Q}(\zeta_{4n} + \zeta_{4n}^{-1}) \\ | \\ \mathbb{Q}(d_1, d_2) \\ | \\ \mathbb{Q}(\frac{d_1}{d_2}) \\ | \\ \mathbb{Q} \end{array} \tag{4.1}$$

We have shown in section 2.2 that $\mathbb{Q}(\zeta_{4n})$ has a degree of $\phi(4n)$ over $\mathbb{Q}$. The goal of Grubb and Wolird is now to calculate the degrees of the other subfields of $\mathbb{Q}(\zeta_{4n})$ in order to calculate the degree of $\mathbb{Q}(\frac{d_1}{d_2})$.

We know that $\zeta_{4n}+\zeta_{4n}^{-1}$ is a real number, since it is the sum a complex number and its conjugate. It follows that $\mathbb{Q}(\zeta_{4n})^+$ must be a proper subfield of $\mathbb{Q}(\zeta_{4n})$, since it is a purely real subfield, and $\mathbb{Q}(\zeta_{4n})$ is not purely real. Note that this holds because $n \geq 1$, and thus $4n \geq 4$, which implies that $\mathbb{Q}(\zeta_{4n})$ does actually contain non-real numbers (for example, this not the case for $\mathbb{Q}(\zeta_2) = \mathbb{Q}(-1, 1) = \mathbb{Q}$). We thus have $[\mathbb{Q}(\zeta_{4n}) : \mathbb{Q}(\zeta_{4n})^+] \geq 2$. Furthermore, the polynomial

$$m(x) := x^2 - (\zeta_{4n} + \zeta_{4n}^{-1})x + 1,$$

has $\zeta_{4n}$ as a root:

$$\zeta_{4n}^2 - (\zeta_{4n} + \zeta_{4n}^{-1})\zeta_{4n} + 1 = \zeta_{4n}^2 - \zeta_{4n}^2 - 1 + 1 = 0.$$

It is clear that $m(x)$ is an element of $\mathbb{Q}(\zeta_{4n})^+[x]$. Hence the minimal polynomial of $\zeta_{4n}$ over $\mathbb{Q}(\zeta_{4n})^+$ has a degree no more than 2, the degree of $m(x)$. Combining this with the fact that $[\mathbb{Q}(\zeta_{4n}) : \mathbb{Q}(\zeta_{4n})^+] \geq 2$, we see that $[\mathbb{Q}(\zeta_{4n}) : \mathbb{Q}(\zeta_{4n})^+] = 2$. By now writing the degrees of (4.1), we get

$$\begin{aligned} [\mathbb{Q}(\zeta_{4n}) : \mathbb{Q}] &= [\mathbb{Q}(\zeta_{4n}) : \mathbb{Q}(\zeta_{4n})^+][\mathbb{Q}(\zeta_{4n})^+ : \mathbb{Q}(d_1, d_2)][\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\tfrac{d_1}{d_2})][\mathbb{Q}(\tfrac{d_1}{d_2}) : \mathbb{Q}] \\ \phi(4n) &= 2 \cdot [\mathbb{Q}(\zeta_{4n})^+ : \mathbb{Q}(d_1, d_2)][\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\tfrac{d_1}{d_2})][\mathbb{Q}(\tfrac{d_1}{d_2}) : \mathbb{Q}] \\ \frac{\phi(4n)}{2} &= [\mathbb{Q}(\zeta_{4n})^+ : \mathbb{Q}(d_1, d_2)][\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\tfrac{d_1}{d_2})][\mathbb{Q}(\tfrac{d_1}{d_2}) : \mathbb{Q}]. \end{aligned} \tag{4.2}$$

The following claim is now made by Grubb and Wolird.

**Claim 4.2.** Let $d_1 = |1 - \zeta_n^a|$ and $d_2 = |1 - \zeta_n^b|$ be two diagonals of a regular $n$-gon with $a$ and $b$ coprime integers. Then $\mathbb{Q}(\zeta_{4n})^+ = \mathbb{Q}(d_1, d_2)$.

This would be very useful in the search for the degree of $\mathbb{Q}(\frac{d_1}{d_2})$, as by (4.2) we would then be able to compute the degree of $\mathbb{Q}(\frac{d_1}{d_2})$ by first computing $[\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\frac{d_1}{d_2})]$, which can be deduced more easily. However, it turns out that this claim is not true, for which we will give a simple

counterexample.
Take $n = 4$, $a = 1$ and $b = 2$, so that $d_1 = |1-\zeta_4| = |1-i| = \sqrt{2}$ and $d_2 = |1-\zeta_4^2| = |1-(-1)| = 2$. Note that $a$ and $b$ are coprime. Then it is clear that $\mathbb{Q}(d_1, d_2) = \mathbb{Q}(\sqrt{2}, 2) = \mathbb{Q}(\sqrt{2})$. However, we also have

$$\mathbb{Q}(\zeta_{4n})^+ = \mathbb{Q}(\zeta_{16})^+ = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1}).$$

We know that by adding a complex number to its conjugate, we get twice its real part. Combining this with equation (2.1) in chapter 2, we get

$$\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1}) = 2\cos\left(\frac{2\pi}{16}\right) = 2\cos\left(\frac{\pi}{8}\right) = \sqrt{2-\sqrt{2}}$$

The last equality follows from basic trigonometry. It is now clear that $\mathbb{Q}(d_1, d_2) = \mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{2-\sqrt{2}}) = \mathbb{Q}(d_1, d_2)$, hence we have found a counterexample to Claim 4.2.

In the article by Grubb and Wolird, Claim 4.2 forms the basis for the proof of Claim 4.1, or Theorem 2 in the article itself. Since Claim 4.2 is not true, the whole argument does not work anymore. This is an important factor in the failure to give an accurate computation of $[\mathbb{Q}(\frac{d_1}{d_2}) : \mathbb{Q}]$. In search to a solution to this problem, we corresponded with the original authors, and in our discussion we obtained the following new hypothesis:

**Hypothesis 4.3.** Let $d_1 = |1-\zeta_n^a|$ and $d_2 = |1-\zeta_n^b|$ be two diagonals of a regular $n$-gon with $\gcd(n, a, b) = 1$ and $n$ an odd integer. Then $\mathbb{Q}(\zeta_{4n})^+ = \mathbb{Q}(d_1, d_2)$.

This hypothesis states that the equality of Claim 4.2 is indeed true, but only for more specific cases. If this hypothesis were to be proven, a large part of the proof by Grubb and Wolird would become useful in showing the degree of $\mathbb{Q}(\frac{d_1}{d_2})$, however, only for the case when $\gcd(n, a, b) = 1$ and $n$ is odd.
In order to provide the basis for the hypothesis, we programmed some code calculating all the relevant degrees of this problem. All the possible cases up to $n = 11$ are computed. These calculations seem to comply with the hypothesis. The code can be found in the appendix.

We will now highlight one more claim made in the article by Grubb and Wolird that seems to be false.

**Claim 4.4.** Let $d_1 = |1-\zeta_n^a|$ and $d_2 = |1-\zeta_n^b|$ be two diagonals of a regular $n$-gon. The number of non-trivial automorphisms of $\mathrm{Gal}(\mathbb{Q}(d_1, d_2)/\mathbb{Q}(\frac{d_1}{d_2}))$ is equal to one half of the number of solutions for $k \pmod{4n}$ to the system of equations

$$\begin{aligned} k(n-2a) &\equiv 3n-2a \pmod{4n} \\ k(n-2b) &\equiv 3n-2b \pmod{4n}. \end{aligned}$$

This claim could be useful in the computation of $[\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\frac{d_1}{d_2})]$, which can be used in computing the degree of $\mathbb{Q}(\frac{d_1}{d_2})$ by equation (4.2). Let us now take $n = 5$, $a = 1$ and $b = 2$, the system of equations becomes

$$\begin{aligned} 3k &\equiv 13 \pmod{20} \\ k &\equiv 11 \pmod{20}. \end{aligned}$$

We can clearly see that $k \equiv 11 \pmod{20}$ is the only possible solution to this system of equations. However, Claim 4.4 now says that the number of non-trivial automorphisms of $\mathrm{Gal}(\mathbb{Q}(d_1, d_2)/\mathbb{Q}(\frac{d_1}{d_2}))$

is equal to the number of solutions, which is 1 in this case. In this case this would be $\frac{1}{2}$, but we cannot have half an automorphism, so this is not possible. Numerous other examples exist in which the number of solutions to the system of equations is an odd number, which would lead to the same problem. This shows that the claim cannot be completely true.

## Section 5

# Appendix

In this appendix, we will give the code that was used to check Hypothesis 4.3. This code was written in SageMath, and it provided a table of three degrees that are of importance to our problem. These degrees are calculated for all possible polygons and diagonals up to $n = 11$.

```
def degrees(N, a, b):
    d1 = abs(1-E(N,a))
    d2 = abs(1-E(N,b))
    zeta4Np = E(4*N) + E(4*N).conjugate()

    #Defining the polynomials
    frac = d1/d2
    f1 = (frac).minpoly()
    fd1 = d1.minpoly()
    fd2 = d2.minpoly()
    f3 = zeta4Np.minpoly()

    #Defining the field extensions
    K1.<fracd1d2> = NumberField(f1) #Q(d1/d2)
    K2.<d1d2> = (fd1*fd2).splitting_field() #Q(d1, d2)
    K3.<zeta4Np> = NumberField(f3) #Q(zeta_4N+)

    #Calculating the degrees
    degree1 = K1.absolute_degree() #[Q(d1/d2):Q]
    degree2 = (K2.absolute_degree())/degree1 #[Q(d1, d2): Q(d1/d2)]
    degree3 = (K3.absolute_degree())/(degree1*degree2) #[Q(zeta_4N+): Q(d1, d2)]

    return degree1, degree2, degree3

M = 11 #Degree up to which we want to compute the degrees
titles = ['inputs']
degrees1 = ['degree1']
degrees2 = ['degree2']
degrees3 = ['degree3']
phi = ['Phi(4N)/4']
```

```
for N in range(2, M + 1): #making the table
    for a in range(1, N):
        for b in range(a, N):
            title = str('N='+str(N)+', a='+str(a)+', b='+str(b))
            titles.append(title)
            degrees1.append(degrees(N,a,b)[0])
            degrees2.append(degrees(N,a,b)[1])
            degrees3.append(degrees(N,a,b)[2])
            phi.append(euler_phi(4*N)/4)

table(columns=[titles, phi, degrees1, degrees2, degrees3], header_row=True) #Show table
```

In the table below, we show a selection of the results of this code. Note that we have $d_1 = |1 - \zeta_n^a|$ and $d_2 = |1 - \zeta_n^b|$.

| **Inputs** | $[\mathbb{Q}(\frac{d_1}{d_2}) : \mathbb{Q}]$ | $[\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\frac{d_1}{d_2})]$ | $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}(d_1, d_2)]$ |
|---|---|---|---|
| $n = 3, a = 1, b = 2$ | 1 | 2 | 1 |
| $n = 4, a = 1, b = 2$ | 2 | 1 | 2 |
| $n = 5, a = 1, b = 2$ | 2 | 2 | 1 |
| $n = 5, a = 2, b = 3$ | 1 | 4 | 1 |
| $n = 6, a = 1, b = 2$ | 2 | 1 | 2 |
| $n = 6, a = 2, b = 3$ | 2 | 1 | 2 |
| $n = 7, a = 1, b = 2$ | 3 | 2 | 1 |
| $n = 7, a = 2, b = 3$ | 3 | 2 | 1 |
| $n = 7, a = 1, b = 3$ | 3 | 2 | 1 |
| $n = 8, a = 1, b = 2$ | 4 | 1 | 2 |
| $n = 8, a = 1, b = 3$ | 2 | 2 | 2 |
| $n = 8, a = 2, b = 4$ | 2 | 1 | 4 |
| $n = 9, a = 1, b = 2$ | 3 | 2 | 1 |
| $n = 9, a = 2, b = 4$ | 3 | 2 | 1 |
| $n = 9, a = 3, b = 3$ | 1 | 2 | 3 |
| $n = 9, a = 3, b = 6$ | 1 | 2 | 3 |
| $n = 10, a = 1, b = 2$ | 4 | 1 | 2 |
| $n = 10, a = 1, b = 3$ | 2 | 1 | 4 |
| $n = 10, a = 2, b = 3$ | 4 | 1 | 2 |
| $n = 11, a = 1, b = 2$ | 5 | 2 | 1 |
| $n = 11, a = 2, b = 3$ | 5 | 2 | 1 |
| $n = 11, a = 1, b = 10$ | 1 | 10 | 1 |

# Bibliography


[1] D. A. Cox. *Galois theory*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2012.

[2] H. G. Diamond, F. Gerth, III, and J. D. Vaaler. Gauss sums and Fourier analysis on multiplicative subgroups of $Z_q$. *Trans. Amer. Math. Soc.*, 277(2):711–726, 1983.

[3] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[4] R. J. Evans. Period polynomials for generalized cyclotomic periods. *Manuscripta Math.*, 40(2-3):217–243, 1982.

[5] I. Fuchs. Ueber die Perioden, welche aus den Wurzeln der Gleichung $w^n = 1$ gebildet sind, wenn $n$ eine zusammengesetzte Zahl ist. *J. Reine Angew. Math.*, 61:374–386, 1863.

[6] M. A. Gómez-Molleda. Gaussian periods in cyclotomic fields and relative traces as generators of intermediate subfields. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 113(2):1331–1341, 2019.

[7] T. Grubb and C. Wolird. Cyclotomic points and algebraic properties of polygon diagonals. *Integers*, 21:Paper No. A40, 22, 2021.

[8] I. M. Vinogradov. *Elements of number theory*. Dover Publications, Inc., New York, 1954. Translated by S. Kravetz.

[9] H. Weber. *Lehrbuch der Algebra*. Chelsea Pub, Co, Chelsea, 1979.