Universiteit Utrecht

Bachelor Thesis

Gaussian periods

Djurre Tijsma

Supervisor:
Prof. dr. Frits Beukers

June 2016

Contents

1 Introduction

The main object of study of this thesis are Gaussian periods. A Gaussian period is a sum of roots of unity with a build-in symmetry. These periods were introduced by Carl Friedrich Gauss in his Disquisitiones Arithmeticae and he used them to give a construction using only a compass and straightedge for the regular 17-gon. He extended his result to cover the cases of constructing a regular p-gon where p is a Fermat prime. In this thesis I study these Gaussian periods, I derive some properties for these periods and I use them to give a construction for the regular p-gons with p a Fermat prime.

This thesis consist of two parts. In the first part I introduce some necessary theory for the last chapter about Gaussian periods. In the first chapter I treat some algebraic number theory because I need the concepts of number fields, rings of integers and integral bases. Chapter two is devoted to proving some basic, but non-trivial, facts about cyclotomic extensions. I give a proof that the ring of integers of a cyclotomic extension has a very nice form. To show this I need some techniques from the first chapter. The third chapter begins by introducing characters of finite abelian groups and ends with Dirichlet characters, Gauss sums and Jacobi sums.
The second part is devoted to the study of the Gaussian periods. I first give a definition of a Gaussian period and then I derive some elementary properties. In the next section I investigate when the Gaussian periods form an integral basis for the ring of integers of a cyclotomic extension. I obtain a partial answer to this question. In the following section I give an estimate for the coefficients of certain Gaussian periods in a product of two Gaussian periods. In the final section I use the Gaussian periods to give a construction for the regular p-gons where p is a Fermat prime.

2 Algebraic number theory

In this chapter we introduce some algebraic number theory including some linear algebra for number fields. We will need this in the following chapter for explicit calculations with cyclotomic extensions of $\mathbb{Q}$. It is not a complete treatment of basic algebraic number theory and we merely state the theorems and lemmas without proofs. We start by introducing the basic concepts of number fields and their ring of integers. Next we introduce the embeddings of a number field into $\mathbb{C}$ for computational purposes. Finally we state some linear algebra theorems to determine when a given set is a $\mathbb{Q}$-basis for a number field or an integral basis for the ring of integers. Complete proofs of all lemmas and theorems can be found in [1].

2.1 Number fields and rings of integers

Let K be a field containing $\mathbb{Q}$. We call an $\alpha \in K$ algebraic if there exists a non-trivial polynomial $P(X) \in \mathbb{Q}[X]$ such that $P(\alpha) = 0$. For an algebraic element $\alpha \in K$ there exists a unique monic polynomial $P(X) \in \mathbb{Q}[X]$ of smallest degree such that $P(\alpha) = 0$. This polynomial is called the minimal polynomial of α. It is necessarily irreducible. If α is algebraic then every element in $\mathbb{Q}(\alpha)$ can be written as a polynomial in α with coefficients in $\mathbb{Q}$ i.e. $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

Every field extension $K/\mathbb{Q}$ can be considered as a vector space over $\mathbb{Q}$. The dimension of this vector space is denoted by $[K : \mathbb{Q}]$, which can be infinite, it is also called the degree of K over $\mathbb{Q}$. If α is algebraic then the degree of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is equal to the degree of the minimal polynomial of α and hence finite. We now give the definition of a number field.

Definition 2.1. *Let K be a field containing $\mathbb{Q}$. We call K a number field if it is a finite extension of $\mathbb{Q}$.*

The only difference between a number field K and an arbitrarily field extension of $\mathbb{Q}$ is that $[K : \mathbb{Q}] < \infty$. This restriction on the degree of the field extension gives the number field some very special properties. For instance, every subring of a number field is Noetherian and all of its non-zero prime ideals are maximal.
Every number field contains a very special and interesting subring, the ring of integers of a number field. It is this ring we will use a lot in the later chapters. Before we can define what the ring of integers is, we define first what an algebraic integer is.

Definition 2.2. *Let K be a field containing $\mathbb{Q}$. An element α of K is called an algebraic integer if the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

In general it is difficult to show if the minimal polynomial of α in a field extension of $\mathbb{Q}$ has coefficients in $\mathbb{Z}$. It turns out that if α is a zero of a non-trivial polynomial with coefficients in $\mathbb{Z}$ then its minimal polynomial also has coefficients in $\mathbb{Z}$. We are now ready to introduce the special subring of a number field K we are looking for.

Definition 2.3. *Let K be a number field. The set*

$$\mathcal{O}_K = \{\alpha \in K |\ \alpha \text{ is an algebraic integer}\}$$

is an integral domain and is called the ring of integers of K.

Knowing how the ring of integers of a number field looks like is very important in algebraic number theory. In chapter 2 we will prove that the ring of integers of a cyclotomic extension, $K = \mathbb{Q}(\omega_n)$ with ω_n a primitive n^{th} root of unity, is of the form $\mathcal{O}_K = \mathbb{Z}[\omega_n]$. Not all rings of integers have this compact form. For quadratic extensions there is also a complete characterization of the ring of integers.

Example 2.4. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension of $\mathbb{Q}$ with d a square-free integer not equal to 1. Then for $d \equiv 2, 3 \mod 4$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and for $d \equiv 1 \mod 4$ we have $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. For the latter note that if $d \equiv 1 \mod 4$ then $\frac{1+\sqrt{d}}{2}$ is a zero of the polynomial $f(X) = X^2 - X + \frac{1-d}{4}$ which has coefficients in $\mathbb{Z}$.*

2.2 Prime ideals in the ring of integers

For a number field K the ring of integers $\mathcal{O}_K$ has the special property of being a Dedekind domain. This means that $\mathcal{O}_K$ is Noetherian, integrally closed in K and that every non-zero prime ideal is maximal. If a ring is Noetherian then every ascending chain of ideals eventually stabilizes. Integrally closed in K means that for every monic polynomial f with coefficients in $\mathcal{O}_K$, every zero of f belonging to K also belongs to $\mathcal{O}_K$. This is a technical definition of being a Dedekind domain and we will only use one special property of the fact that $\mathcal{O}_K$ is a Dedekind domain.

Theorem 2.5. *If K is a number field then every non-zero proper ideal in $\mathcal{O}_K$ can be factored uniquely as a product of non-zero prime ideals in $\mathcal{O}_K$.*

A proper ideal is an ideal not equal to the whole ring. If $\mathfrak{p}$ is a non-zero prime ideal satisfying $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ then we say that $\mathfrak{p}$ extends p. If p is a prime number

then there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ extending p and positive integers $e(\mathfrak{p}_1), \ldots, e(\mathfrak{p}_k)$ such that $(p) = \mathfrak{p}_1^{e(\mathfrak{p}_1)} \ldots \mathfrak{p}_k^{e(\mathfrak{p}_k)}$. The multiplicity for which a prime ideal $\mathfrak{p}$ (extending p) divides p is the ramification index $e(\mathfrak{p})$, if $\mathfrak{p}$ doesn't extend p then $e(\mathfrak{p}) = 0$. For a given prime number p there are only finitely many prime ideals extending p. Since all prime ideals are maximal the quotient ring $\mathcal{O}_K/\mathfrak{p}$ is a field and it turns out that it is a finite field extension of $\mathbb{F}_p$ (the finite field with p elements). We will denote the degree of the field extension $\mathbb{F}_p \subset \mathcal{O}_K/\mathfrak{p}$ by $f(\mathfrak{p})$.

There is an important relation between the ramification indices $e(\mathfrak{p})$ and $f(\mathfrak{p})$ for a prime ideal $\mathfrak{p}$ extending p with p a prime number. The following theorem is a special case of a more general theorem.

Theorem 2.6. *Let K be a number field then for a prime number p we have*

$$\sum_{\mathfrak{p}} e(\mathfrak{p}) f(\mathfrak{p}) = [K : \mathbb{Q}]$$

where the sum ranges over all prime ideal $\mathfrak{p}$ extending p.

We will use this theorem in the next chapter.

2.3 Linear algebra for number fields

For every number field K of degree n we know that there exist elements $x_1, \ldots, x_n \in K$ which form a $\mathbb{Q}$-basis of K. Using the primitive element theorem, which states for number fields that there exists an algebraic $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. This gives us a $\mathbb{Q}$-basis of K consisting of the elements $1, \alpha, \ldots, \alpha^{n-1}$. One can ask whether the same is true for $\mathcal{O}_K$. It turns out that it is partly true. There exists a basis for $\mathcal{O}_K$ but not always a basis consisting of powers of a single element. In the end of this section we see some ways for determining if some set is a basis for $\mathcal{O}_K$.

Every number field K can be embedded in $[K : \mathbb{Q}]$ ways into $\mathbb{C}$. These embeddings are useful for computations with number fields and especially if K is a Galois extension of $\mathbb{Q}$. The precise definition of an embedding is given in the following lemma.

Lemma 2.7. *For a number field K write $K = \mathbb{Q}(\alpha)$, set $n = [K : \mathbb{Q}]$ and let $\alpha_1, \ldots, \alpha_{\in}\mathbb{C}$ be the roots of the minimal polynomial of α over $\mathbb{Q}$. There exist n injective field homomorphisms $\sigma_i : K \to \mathbb{C}$. These field homomorphisms σ_i are called embeddings and they are defined by*

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\alpha_i + \ldots + a_{n-1}\alpha_i^{n-1}\,.$$

Every field homomorphism $K \to \mathbb{C}$ is of this form. In particular the embeddings are independent of the primitive element α chosen.

In the case $K = \mathbb{Q}(i)$, the Gaussian rationals, these embeddings have a very simple form.

Example 2.8. *For $K = \mathbb{Q}(i)$ with $i^2 = -1$ the embeddings of K into $\mathbb{C}$ are given by σ and τ where $\sigma : a + bi \mapsto a + bi$ and $\tau : a + bi \mapsto a - bi$ for $a, b \in \mathbb{Q}$.*

Having defined the embeddings we can now define the norm of an element of a number field.

Definition 2.9. *Let K be a number field with $n = [K : \mathbb{Q}]$, if $\{\sigma_1, \ldots, \sigma_n\}$ are the embeddings of K into $\mathbb{C}$ then the norm of $x \in K$ is defined as*

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)\,.$$

The norm function has some useful properties. When K is a number field the norm of $x \in K$ lies in $\mathbb{Q}$, i.e. $N_{K/\mathbb{Q}}(x) \in \mathbb{Q}$ and if $x \in \mathcal{O}_K$ then we even have $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. We need the following definition of the discriminant of a set of elements of a number field, it assigns to a set a number.

Definition 2.10. *Let K be a number field and $\{\sigma_1, \ldots, \sigma_n\}$ the embeddings of K in $\mathbb{C}$. The discriminant, $\Delta(\omega_1, \ldots, \omega_n)$, of the set $\{\omega_1, \ldots, \omega_n\}$ where $\omega_i \in K$ is defined as $\det(M)^2$ where M is the following matrix:*

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{pmatrix}.$$

We will use the discriminant of a set later in lemmas and theorems concerning integral bases. The following lemma is very useful in the computation of the discriminant of some set consisting of powers of a single element. This is used in the next chapter where we take powers of a root of unity.

Lemma 2.11. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n and let f be the minimal polynomial of α over $\mathbb{Q}$. Let D be the discriminant of the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in a splitting field of f. Then D equals both sides of the following equation*

$$\prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha))\,.$$

The left-hand side equals the discriminant of the polynomial f and in the right-hand side f' stands for the formal derivative of f.

The following definition defines for a ring of integers $\mathcal{O}_K$ of a number field K what an integral basis is.

Definition 2.12. *Let K be a number field with $n = [K : \mathbb{Q}]$. Call $\{\alpha_1, \ldots, \alpha_n\}$ an integral basis of $\mathcal{O}_K$ when every element of $\mathcal{O}_K$ can be uniquely expressed as a $\mathbb{Z}$-linear combination of elements of this set.*

We know that there is always a $\mathbb{Q}$-basis for a number field, but is there always an integral basis for the ring of integers? The following theorem guarantees it does.

Theorem 2.13. *Let K be a number field. Then the ring of integers $\mathcal{O}_K$ has an integral basis.*

It turns out that every two bases of the ring of integers of a number field K have the same discriminant and that this discriminant lies in $\mathbb{Z}$. We therefore say that the discriminant of K is the discriminant of $\mathcal{O}_K$, notation: Δ_K. The discriminant of a number field is a very important algebraic invariant of the number field. It tells us for which prime numbers p there exists a prime ideal $\mathfrak{p}$ extending p with $e(\mathfrak{p}) > 1$.

Example 2.14. *For a square-free integer d not equal to 1 the quadratic field $K = \mathbb{Q}(\sqrt{d})$ has discriminant $\Delta_K = d$ if $d \equiv 1 \mod 4$ and $\Delta_K = 4d$ if $d \equiv 2, 3 \mod 4$.*

Example 2.15. *The number field $K = \mathbb{Q}(\alpha)$ with α satisfying the relation $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$ has ring of integers $\mathcal{O}_K = \mathbb{Z}[\alpha, \frac{\alpha+\alpha^2}{2}]$ and $\mathcal{O}_K \neq \mathbb{Z}[\beta]$ for every $\beta \in \mathcal{O}_K$.*

Example 2.15, due to Dedekind, shows that an integral basis for the ring of integers doesn't necessarily consists of powers of a single element.
For a given number field one can find the ring of integers after a finite computation. This can only be done for one number field at a time, so proving something about

the ring of integers for a collection of number fields is more difficult. The following theorem is very helpful in doing just that. First we need a lemma about the ring of integers as a subset of another set, we use this in the next chapter.

Lemma 2.16. *Let K be a number field with $n = [K : \mathbb{Q}]$. Suppose that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ is a $\mathbb{Q}$-basis K then*

$$\mathcal{O}_K \subseteq \tfrac{1}{\Delta(\alpha_1,\ldots,\alpha_n)} \left(\mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n\right) .$$

The following theorem gives us conditions for finding the ring of integers of the composite $\mathbb{Q}(\alpha, \beta)$ of the number rings $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$ under suitable conditions.

Theorem 2.17. *Let $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$ be two number fields of degree m and n respectively such that $M = \mathbb{Q}(\alpha, \beta)$ has degree mn over $\mathbb{Q}$. Suppose that $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_n\}$ are integral bases for K and L respectively with discriminants Δ_K and Δ_L. If Δ_K and Δ_L are coprime, then $\{\alpha_i\beta_j\}_{i,j}$ forms an integral basis for M with discriminant $\Delta_K^n \Delta_L^m$.*

Theorem 2.17 shows how important the discriminant of a number field is.

3 Cyclotomic extensions of $\mathbb{Q}$

In this section we study cyclotomic extension and some of their properties. We start by introducing roots of unity, then we turn to the cyclotomic polynomials, the minimal polynomials of the roots of unity over $\mathbb{Q}$. We then continue with proving that $\mathbb{Z}[\omega_n]$ is the ring of integers of $\mathbb{Q}(\omega_n)$ with n a prime power and finally we deduce from this the general case where n is an arbitrary positive integer.

3.1 Roots of unity

One can define roots of unity for arbitrary fields but we focus instead on fields with $\mathbb{Q}$ as a subfield. This gives us the advantage that certain polynomials are separable. Let $n \in \mathbb{N}$, by a n^{th} root of unity we mean a solution to the equation $X^n = 1$ in a field extension of $\mathbb{Q}$. Because $\mathbb{Q}$ is a field there are at most n roots of $X^n - 1$ and so there are at most n n^{th} roots of unity in any extension of $\mathbb{Q}$. A root of unity is a n^{th} root of unity for some n. Let ω be a root of unity then the extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is called a cyclotomic extension of $\mathbb{Q}$. It is clear that the n^{th} roots of unity in a field form a group. The following theorem tells us in particular that this group is cyclic. But first we need a lemma about finite abelian groups.

Lemma 3.1. *Let G be a finite abelian group. If G has elements of order a and b then G has an element of order $lcm(a, b)$ (lcm stands for least common multiple).*

Proof. If g is an element of G with order n and d divides n then G has an element of order d (namely $g^{\frac{n}{d}}$). Write $a = p_1^{e_1} \dots p_k^{e_k}$ and $b = p_1^{f_1} \dots p_k^{f_k}$ with p_i different primes and $e_i, f_i \geq 0$. Let $a' = \prod_{e_i \geq f_i} p_i^{e_i}$ and let $b' = \prod_{e_i < f_i} p_i^{f_i}$ then $\gcd(a', b') = 1$, $a' \mid a$, $b' \mid b$ and $n = a'b'$. We know that there exist elements $x, y \in G$ of order a', b' respectively. Because $\gcd(a', b') = 1$ we have $\langle x \rangle \cap \langle y \rangle = \{e\}$. So $(xy)^t = e$ if and only if $x^t = y^{-t}$ if and only if $x^t = y^t = e$ which can only happen if and only $\operatorname{lcm}(a, b) \mid t$. The order of xy is therefore $\operatorname{lcm}(a, b)$ and we are done. □

We can now proof the theorem from which it follows immediately that the group of n^{th} roots of unity is cyclic.

Theorem 3.2. *Let K be a field. Any finite subgroup of $K^* = K \backslash \{0\}$ is cyclic.*

Proof. Let G be a finite subgroup of K^* of order n. Let m be equal to the least common multiple of the orders of all elements in G. Since

$$\operatorname{lcm}(a_1, \ldots, a_{k-2}, \operatorname{lcm}(a_{k-1}, a_k)) = \operatorname{lcm}(a_1, \ldots, a_k)$$

for any $k \geq 3$ and $a_1, \ldots, a_k \in \mathbb{Z}$ we can use induction together with the previous lemma to see that there exists an element of G of order m. By the theorem of Lagrange we have $m \mid n$. The orders of all elements divide m so all elements of G are zeros of the polynomial $X^m - 1$, which has at most m zeros since we work over a field. It follows that $n \leq m$. Together this gives $m = n$ and since we also have an element of order m we see that G is cyclic. □

Let$n \in \mathbb{N}$. We call a n^{th} root of unity ω primitive if $\omega^n = 1$ and $\omega^k \neq 1$ for $1 \leq k < n$. Let ω_n be a primitive n^{th} root of unity in a splitting field of $X^n - 1$. For $k \in \mathbb{Z}$ the order of ω_n^k is $n/\gcd(k, n)$ so ω_n^k is primitive if and only if $\gcd(k, n) = 1$. It follows that there are $\varphi(n)$ primitive n^{th} roots of unity in the splitting field of $X^n - 1$. Here $\varphi(n)$ denotes the Euler-phi function.

Let $\mathbb{Q}(\omega)/\mathbb{Q}$ be a cyclotomic extension with ω a root of unity. Let n be the order of ω so that ω is a primitive n^{th} root of unity. All powers of ω are roots of $X^n - 1$. In a splitting field of $X^n - 1$ all the roots of $X^n - 1$ are different since $X^n - 1$ is separable over $\mathbb{Q}$. Since the group of n^{th} roots of unity is cyclic in this splitting field, adjoining any primitive n^{th} root of unity of this splitting field to $\mathbb{Q}$ gives the same cyclotomic extension. We can therefore write any cyclotomic extension of $\mathbb{Q}$ as $\mathbb{Q}(\omega_n)/\mathbb{Q}$ where ω_n is some primitive n^{th} root of unity.

Since $X^n - 1$ is separable over $\mathbb{Q}$ we have that $\mathbb{Q}(\omega_n)/\mathbb{Q}$ is a Galois extension because it is a splitting field of $X^n - 1$. We are now going to determine the Galois group of the Galois extension $\mathbb{Q}(\omega_n)/\mathbb{Q}$. We first prove a little lemma relating the Galois group to $(\mathbb{Z}/n\mathbb{Z})^*$ the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$.

Lemma 3.3. *Let $n \in \mathbb{N}$ and ω_n be a primitive n^{th} root of unity. For all $\sigma \in \operatorname{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ there exists an integer $a = a_\sigma$ relatively prime to n such that $\sigma(\omega) = \omega^a$ for all n^{th} roots of unity ω.*

Proof. Since σ is an automorphism and ω_n is a primitive n^{th} root of unity we have $\sigma(\omega_n)^n = 1$ and $\sigma(\omega_n)^k \neq 1$ for $1 \leq k < n$. It follows that $\sigma(\omega_n)$ is also a primitive n^{th} root of unity, so $\sigma(\omega_n) = \omega_n^a$ for some integer a with $\gcd(a, n) = 1$. Every n^{th} root of unity is a power of ω_n hence $\sigma(\omega) = \omega^a$ for all n^{th} roots of unity ω. □

We are now going to prove that $\mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. We will use more than once a consequence of the lemma of Gauss for polynomials, stating that for a monic $f \in \mathbb{Z}[X]$ with $f = gh$ for monic $g, h \in \mathbb{Q}[X]$ we have $g, h \in \mathbb{Z}[X]$.

Lemma 3.4. *Let $f \in \mathbb{Q}[X]$ be the minimal polynomial of ω_n a n^{th} root of unity for some positive integer n. For each prime p with $\gcd(p, n) = 1$ the minimal polynomial of ω_n^p is also f.*

Proof. For $n = 1$ the statement is clear. Let $n \geq 2$. We will prove the statement by contradiction. Suppose for some prime p with $\gcd(p, n) = 1$ the root of unity ω_n^p is not a zero of f. Let $g \in \mathbb{Q}[X]$ be a monic factor of $X^n - 1$ relatively prime to f such that $g(\omega_n^p) = 0$. We then have $f(X)g(X) \mid X^n - 1$ so $X^n - 1 = f(X)g(X)h(X)$ for some $h \in \mathbb{Q}[X]$. By Gauss' lemma we have $f, g, h \in \mathbb{Z}[X]$. Reducing this equation modulo p we get $X^n - 1 = \bar{f}(X)\bar{g}(X)\bar{h}(X)$. Because f, g are both monic and of positive degree their reductions are also monic and of positive degree. From $n(X^n - 1) - (nX^{n-1}) = -n$ and $\gcd(p, n) = 1$ it follows that $X^n - 1$ and nX^{n-1} are relatively prime so $X^n - 1$ is separable over $\mathbb{F}_p[X]$. The reductions $\bar{f}, \bar{g}$ are therefore relatively prime. It is given that f is irreducible and since $f(\omega_n) = g(\omega_n^p) = 0$ we see that $f(X)k(X) = g(X^p)$ for some monic $k(X) \in \mathbb{Z}[X]$ by Gauss' lemma. Reducing this equation modulo p gives $\bar{f}(X)\bar{k}(X) = \bar{g}(X^p) = \bar{g}(X)^p$. It follows that $\bar{f}$ and $\bar{g}$ share a common irreducible factor. This contradicts that $\bar{f}$ and $\bar{g}$ are relatively prime. □

Using Lemma 3.4 we can now proof that *Gal*$(\mathbb{Q}(\omega_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.

Theorem 3.5. *The map $\phi : \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ defined by $\sigma \mapsto a_\sigma$ is a group isomorphism.*

Proof. We will first show that ϕ is a homomorphism of groups. Let
$\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ then $\omega_n^{a_{\sigma\tau}} = \sigma\tau(\omega_n) = \sigma(\omega_n^{a_\tau}) = \omega^{a_\sigma a_\tau}$ so $a_{\sigma\tau} \equiv a_\sigma a_\tau \mod n$. The identity automorphism, id, in $\mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ fixes every element of $\mathbb{Q}(\omega_n)$ so it is send to 1 by ϕ. It follows that ϕ is indeed a group homomorphism.
Suppose $\sigma \in \ker\phi$ then $a_\sigma \equiv 1 \mod n$ so $\sigma(\omega_n) = \omega_n$ hence $\sigma = \mathrm{id}$ since σ also fixes $\mathbb{Q}$ and ϕ. It follows that ϕ is injective.
We will now show that ϕ is surjective, the difficult part of the proof. The root of unity ω_n^a with a an integer relatively prime to n depends only on $a \mod n$ so we may take without loss of generality $a > 1$. Write $a = p_1 \dots p_r$ with p_i not necessarily distinct prime factors of a satisfying $\gcd(n, p_i) = 1$ for $i = 1, \dots, r$. The above lemma implies that ω_n and ω_n^p have the same minimal polynomial for all prime numbers p with $\gcd(p, n) = 1$. So inductively we find that ω_n and ω_n^a have the

same minimal polynomial over $\mathbb{Q}$. This implies that $\#\mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \geq \varphi(n)$. Since $\#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$ and ϕ is injective it follows that ϕ is surjective. So ϕ is indeed a group isomorphism. □

3.2 Cyclotomic polynomials

For $n \in \mathbb{N}$ let K_n be the splitting field of $X^n - 1$ over $\mathbb{Q}$. Define the cyclotomic polynomial $\Phi_n(X) \in K_n[X]$ by

$$\Phi_n(X) = \prod_{\substack{1 \leq a \leq n, \\ \gcd(a,n)=1}} (X - \omega_n^a).$$

Applying $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ to $\Phi_n(X)$ shows that σ permutes the factors $(X - \omega_n^a)$ so $\sigma\Phi_n = \Phi_n$ and hence $\Phi_n \in \mathbb{Q}[X]$. We have $X^n - 1 = \prod_{d|n} \Phi_d(X)$ since every n^{th} root of unity is a primitive d^{th} root of unity for some $d \mid n$ and every primitive d^{th} root of unity is a n^{th} root of unity. Using Gauss' lemma we see that $\Phi_n \in \mathbb{Z}[X]$ since all the factors in the product are monic. A few cyclotomic polynomials are given in the following example.

Example 3.6. *Using the relation $X^n - 1 = \prod_{d|n} \Phi_d(X)$ together with $\Phi_1(X) = X - 1$ we can compute the first ten cyclotomic polynomials:*

$$\begin{aligned}
\Phi_1(X) &= X - 1 & \Phi_6(X) &= X^2 - X + 1 \\
\Phi_2(X) &= X + 1 & \Phi_7(X) &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\Phi_3(X) &= X^2 + X + 1 & \Phi_8(X) &= X^4 + 1 \\
\Phi_4(X) &= X^2 + 1 & \Phi_9(X) &= X^6 + X^3 + 1 \\
\Phi_5(X) &= X^4 + X^3 + X^2 + X + 1 & \Phi_{10}(X) &= X^4 - X^3 + X^2 - X + 1
\end{aligned}$$

Besides having integer coefficients it is also true that $\Phi_n(X)$ is irreducible as is shown in the following theorem.

Theorem 3.7. *For any $n \geq 1$ the cyclotomic polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible.*

Proof. For $n = 1$ it is clear, suppose now that $n \geq 2$. If $\Phi_n(X)$ is not irreducible, let $f \in \mathbb{Q}[X]$ be the irreducible monic factor of $\Phi_n(X)$ with ω_n as zero and let $g \in \mathbb{Q}[X]$ be monic such that $\Phi_n = fg$. Because $\Phi_n(X)$ is not irreducible there exists a primitive n^{th} root of unity ω such that $f(\omega) \neq 0$ but $g(\omega) = 0$. Because ω_n and ω are primitive we can find not necessarily distinct prime numbers $p_1, \ldots, p_r$

relatively prime to n such that $\omega = \omega_n^{p_1 \cdots p_r}$. Using Lemma 3.4 it follows inductively that $\omega_n^{p_1 \cdots p_j}$ is a zero of f since $\omega_n^{p_1 \cdots p_k}$ for any k is again a primitive n^{th} root of unity. This implies that ω is also a zero of f. This is a contradiction, so $\Phi_n(X)$ is irreducible. $\square$

There are $\varphi(n)$ primitive roots of unity so the degree of Φ_n is $\varphi(n)$. Using the relation $X^n - 1 = \prod_{d|n} \Phi_n(X)$ for $n = p$ with p prime gives $\Phi_p(X) = X^{p-1} + \ldots + 1$. If $n = p^k$ is a prime power then we know that Φ_n has degree $\varphi(p^k) = p^{k-1}(p-1)$. If ω_n is a primitive $(p^k)^{\text{th}}$ root of unity then $\omega_{p^k}^{p^{k-1}}$ is a primitive p^{th} root of unity hence a root of Φ_p hence ω_{p^k} is a root of

$$\Phi_p(X^{p^{k-1}}) = (X^{p^{k-1}})^{p-1} + \ldots + X^{p^{k-1}} + 1 \tag{1}$$

which has degree $p^{k-1}(p-1)$ so $\Phi_p(X^{p^{k-1}})$ is in fact the minimal polynomial of ω_{p^k}.

3.3 Ring of integers of prime power cyclotomic extension

In this section we will prove that the ring of integers of $K = \mathbb{Q}(\omega_n)/\mathbb{Q}$ with n a prime power is $\mathbb{Z}[\omega_n]$. A key ingredient in the proof is the determination of the discriminant Δ_K. In preparation of the proof we need first some helpful results. For the rest of this section let $n = p^r$ with p a prime number and $r \in \mathbb{N}$, let ω_n be a primitive n^{th} root of unity and set K equal to $\mathbb{Q}(\omega_n)/\mathbb{Q}$.

Lemma 3.8. *Let ω and ω' be primitive n^{th} roots of unity. Then $u = \frac{1-\omega'}{1-\omega}$ is a unit in $\mathbb{Z}[\omega_n]$, hence in the ring of algebraic integers.*

Proof. Since ω is primitive there exists $k \in \mathbb{N}$ such that $\omega' = \omega^k$ so that

$$u = \frac{1-\omega^k}{1-\omega} = 1 + \omega + \ldots + \omega^{k-1} \in \mathbb{Z}[\omega_n]$$

In an analogous way we can show that $v = \frac{1-\omega}{1-\omega'}$ is in $\mathbb{Z}[\omega_n]$. Since $\mathbb{Z}[\omega_n] \subseteq \mathcal{O}_K$ the result follows. $\square$

We need a lemma about two important ideals in $\mathcal{O}_K$.

Lemma 3.9. *The ideals $(1-\omega_n)^{\varphi(p^r)}$ and (p) coincide in $\mathcal{O}_K$.*

Proof. Using (1) gives

$$p = \Phi_{p^r}(1) = \prod(1-\omega) = (1-\omega)^{\varphi(p^r)} \prod \frac{1-\omega'}{1-\omega} = v(1-\omega)^{\varphi(p^r)}$$

where the product runs over all primitive n^{th} roots of unity. By Lemma 3.8 we know that v a unit in $\mathbb{Z}[\omega_n]$. □

In the calculation of the discriminant we need some preliminary results about norms of certain elements.

Lemma 3.10. *For all integers $0 \leq s \leq r$ we have $N_{K/\mathbb{Q}}(1-\omega_n^{p^s}) = p^{p^s}$.*

Proof. Composing every Galois automorphism with the ring homomorphism $f : K \to \mathbb{C} : \omega_n \to e^{\frac{2\pi i}{n}}$ we get each of the $[K:\mathbb{Q}]$ embeddings into $\mathbb{C}$. Hence we see that $N_{K/\mathbb{Q}}(1-\omega_n^{p^s})$ is equal to the image of $\prod_{k=1}^{\varphi(p^r)} \sigma_k(1-\omega_n^{p^s})$ under f. Consider the natural map $\phi : (\mathbb{Z}/p^r\mathbb{Z})^* \to (\mathbb{Z}/p^{r-s}\mathbb{Z})^*$ sending $x \mod p^r$ to $x \mod p^{r-s}$. One checks easily that ϕ is a surjective group homomorphism with a kernel of size p^s. Since $\omega = \omega_n^{p^s}$ is a primitive $(p^{r-s})^{\text{th}}$ roof of unity it follows that

$$\prod_{k=1}^{\varphi(p^r)} \sigma_k(1-\omega_n^{p^s}) = \left(\prod_{k \in (\mathbb{Z}/p^s\mathbb{Z})^*} (1-\omega^k) \right)^{p^s} = \Phi_{p^s}(1)^{p^s} = p^{p^s}$$

□

We are now ready to calculate the discriminant of a set of powers of ω_n.

Lemma 3.11. *Let D be the discriminant of the set $\{1, \omega_n, \ldots, \omega_n^{\varphi(p^r)-1}\}$, then D equals $\pm p^{p^{r-1}(r(p-1)-1)}$.*

Proof. Using Lemma 2.11 with $n = p^r$ gives $D = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(\Phi'_n(\omega_n))$. If we differentiate the equation $(X^{p^{r-1}}-1)\Phi_{p^r}(X) = X^{p^r}-1$ we get

$$p^{r-1}X^{p^{r-1}-1}\Phi_{p^r}(X) + \Phi'_{p^r}(X)(X^{p^{r-1}}-1) = p^r X^{p^r-1}$$

inserting ω_n for X gives $\Phi'_{p^r}(\omega_n)(\omega_n^{p^{r-1}}-1) = p^r\omega_n^{p^r-1}$. We now have to find the norms of $p^r\omega_n^{p^r-1}$ and $\omega_n^{p^{r-1}}-1$ to find D. First of all note that $N_{K/\mathbb{Q}}(\omega_n) = 1$ and $N_{K/\mathbb{Q}}(p^r) = p^{r\varphi(p^r)} = p^{rp^{r-1}(p-1)}$. Using Lemma 3.10 gives

$$N_{K/\mathbb{Q}}(\omega_n^{p^{r-1}}-1) = (-1)^{\varphi(p^r)} p^{p^{r-1}}$$

and from this it follows that $D = (-1)^{\frac{(n-1)n}{2} - \varphi(p^r)} p^{rp^{r-1}(p-1)-p^{r-1}}$. So we have indeed $D = \pm p^{p^{r-1}(r(p-1)-1)}$. □

We continue with another lemma relating $\mathbb{Z}[\omega_n]$ to $\mathcal{O}_K$.

Lemma 3.12. *For every positive integer m, we have $\mathbb{Z}[\omega_n] + \pi^m\mathcal{O}_K = \mathcal{O}_K$ where $\pi = 1 - \omega_n$.*

Proof. First of all we have that (π) is a prime ideal. If it wasn't then since $(p) = (\pi)^{\varphi(p^r)}$ the ideal (p) would have more than $\varphi(p^r)$ prime ideal factors. This contradicts however Theorem 2.6. So (π) is a prime ideal and the same theorem also gives that $f((\pi)) = 1$. Consider the injective natural map $\mathbb{Z} \to \mathcal{O}_K$ this gives us the inclusion $f : \mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/(\pi) : n \mapsto n \mod \pi$ since $(p) = (\pi)^{\varphi(p^r)}$. As $f((\pi)) = 1$ we see that $\mathcal{O}_K/(\pi)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ hence we have an inclusion. For $n \in \mathbb{Z}$ we can now (because of the isomorphism) find an $\alpha \in \mathcal{O}_K$ such that $n = \alpha \mod \pi$ so $\alpha - n$ is a multiple of π, hence α can be written as $n + \pi\beta$ for some $\beta \in \mathcal{O}_K$. It follows that $\mathcal{O}_K \subset \mathbb{Z} + \pi\mathcal{O}_K$ and we even have equality since the reverse inclusion is obviously true so $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$.

We will prove with induction to m that $\mathbb{Z}[\omega_n] + \pi^m\mathcal{O}_K = \mathcal{O}_K$. The case $m = 1$ is already dealt with. Suppose now that it is true for $m = k$ then we have $\mathbb{Z}[\omega_n]+\pi^k\mathcal{O}_K = \mathcal{O}_K$ and using the base case we also have $\pi^k\mathbb{Z}[\omega_n]+\pi^{k+1}\mathcal{O}_K = \pi^k\mathcal{O}_K$ hence

$$\mathcal{O}_K = \mathbb{Z}[\omega_n] + (\pi^k\mathbb{Z}[\omega_n] + \pi^{k+1}\mathcal{O}_K) = \mathbb{Z}[\omega_n] + \pi^{k+1}\mathcal{O}_K\,.$$

So it is also true for $m = k + 1$. The result follows. □

If we set $m = \varphi(p^r)k$ in Lemma 3.12 then since $\pi^m\mathcal{O}_K = up^k\mathcal{O}_K = p^k\mathcal{O}_K$ with $u \in \mathbb{Z}[\omega_n]$ a unit we get $\mathbb{Z}[\omega_n] + p^k\mathcal{O}_K = \mathcal{O}_K$. We are now ready to prove the final result of this section.

Theorem 3.13. *For $n = p^r$ with p a prime number and $r \in \mathbb{N}$ let $K = \mathbb{Q}(\omega_n)/\mathbb{Q}$ be a cyclotomic extension with ω_n a primitive n^{th} root of unity. The set $\{1, \omega_n, \ldots, \omega_n^{\varphi(p^r)-1}\}$ is an integral basis $\mathcal{O}_K$ with $\Delta_K = \pm p^{p^{r-1}(r(p-1)-1)}$.*

Proof. Because $\mathbb{Z}[\omega_n] + p^k\mathcal{O}_K = \mathcal{O}_K$ for all $k \geq 1$ setting $k = p^{r-1}(r(p-1)-1)$ and noting that $p^k = \pm\Delta(1, \omega_n, \ldots, \omega_n^{\varphi(p^r)-1})$ we see that

$$\mathcal{O}_K = \mathbb{Z}[\omega_n] + \Delta(1, \omega_n, \ldots, \omega_n^{\varphi(p^r)-1})\mathcal{O}_K \subseteq \mathbb{Z}[\omega_n]$$

by Lemma 2.16. It follows immediately that $\mathcal{O}_K = \mathbb{Z}[\omega_n]$ since the reverse inclusion is obviously. We also get that $\Delta_K = \pm p^{p^{r-1}(r(p-1)-1)}$. □

3.4 Ring of integers for arbitrary cyclotomic extensions

In this section we show the general result for the ring of integers of a cyclotomic extension.

Theorem 3.14. *Let n be a positive integer and let ω_n be a primitive n^{th} root of unity. The ring of integers of $K = \mathbb{Q}(\omega_n)/\mathbb{Q}$ is $\mathbb{Z}[\omega_n]$.*

Proof. For $n = 1$ the statement is trivial and the case that is n a prime power is treated in the previous theorem. We may therefore assume that n is not a prime power and $n \geq 2$. Write n as $n = p_1^{e_1} \dots p_k^{e_k}$ with p_i different prime numbers and $e_i \geq 1$. Let ω_i be a primitive $(p_i^{e_i})^{\text{th}}$ root of unity, let K_i be $K_i = \mathbb{Q}(\omega_i)/\mathbb{Q}$ and define for $1 \leq i \leq k$ the field $L_i = \mathbb{Q}(\omega_1, \dots, \omega_i)$.
The number fields L_1 and K_2 have degrees $\varphi(p_1^{e_1})$ and $\varphi(p_2^{e_2})$ respectively. The number field $L_2 = \mathbb{Q}(\omega_1, \omega_2)$ is the same field as $\mathbb{Q}(\omega_{p_1^{e_1} p_2^{e_2}})$ since $\omega_1\omega_2$ is a primitive $(p_1^{e_1}p_2^{e_2})^{\text{th}}$ root of unity because $\langle\omega_1\rangle \cap \langle\omega_2\rangle = \{1\}$. Hence it has degree $\varphi(p_1^{e_1}p_2^{e_2}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2})$. Since $\gcd(\Delta_{K_1}, \Delta_{K_2}) = 1$ we may apply Theorem 2.17 to conclude that $\{\omega_1^{f_1}\omega_2^{f_2}\}_{0 \leq f_i \leq \varphi(p_i^{e_i})}$ is an integral basis for $\mathcal{O}_{L_2}$.
We can repeat the above procedure to L_i and K_{i+1} repeatedly since $\mathbb{Q}(\omega_{p_1^{e_1} \dots p_i^{e_i}}, \omega_{i+1}) = \mathbb{Q}(\omega_{p_1^{e_1} \dots p_{i+1}^{e_{i+1}}}) = L_{i+1}$ and because the discriminant of L_i contains only the prime factors $p_1, \dots, p_i$. It follows that $\{\omega_1^{f_1}\omega_2^{f_2} \dots \omega_k^{f_k}\}_{0 \leq f_j \leq \varphi(p_j^{e_j})}$ is an integral basis of $\mathcal{O}_K$.

Every element of $\{\omega_1^{f_1}\omega_2^{f_2} \dots \omega_k^{f_k}\}_{0 \leq f_j \leq \varphi(p_j^{e_j})}$ is a power of ω_n since we can choose ω_n such that $\omega_n = \omega_1 \dots \omega_k$. Because each power of ω_n can be expressed as a $\mathbb{Z}$-linear combination of the powers $1, \omega_n, \dots, \omega_n^{\varphi(n)-1}$ (note that Φ_n has degree $\varphi(n)$) and an integral basis of $\mathcal{O}_K$ contains $\varphi(n)$ elements we see that $\{1, \omega_n, \dots, \omega_n^{\varphi(n)-1}\}$ is also an integral basis for $\mathcal{O}_K$. We therefore have $\mathcal{O}_K = \mathbb{Z}[\omega_n]$ as claimed. □

In the case of n being square-free we can give another set which forms an integral basis for the ring of integers.

Theorem 3.15. *Let $n > 1$ be a square-free integer. An integral basis for the ring of integers of $K = \mathbb{Q}(\omega_n)/\mathbb{Q}$ is given by the set $\{\omega_n^k\}_{1 \leq k \leq n, \gcd(k,n)=1}$.*

Proof. We will use the first result in the proof of Theorem 3.14 that
$B = \{\omega_1^{f_1}\omega_2^{f_2} \dots \omega_k^{f_k}\}_{1 \leq f_j \leq \varphi(p_j)}$ is an integral basis for $\mathcal{O}_K$. Without altering the proof we may assume that the primitive $(p_i)^{\text{th}}$ root of unity ω_i equals $\omega_n^{\frac{n}{p_i}}$. We can now rewrite B to $B = \{\omega_n^{\sum_{i=1}^{k} \frac{n}{p_i} f_i}\}_{1 \leq f_j \leq \varphi(p_j)}$. We will now show that the sums

$S = \sum_{i=1}^{k} \frac{n}{p_i} f_i$ are different modulo n and that they are pairwise prime with n. Reducing S modulo p_i gives $S \equiv \frac{n}{p_i} f_i \mod p_i$ which is non-zero since n is square-free and $1 \leq f_i \leq p_i - 1$. Because this is true for all i we see that S is relatively prime to n. Suppose now that $\sum_{i=1}^{k} \frac{n}{p_i} f_i = \sum_{i=1}^{k} \frac{n}{p_i} f_i'$ for some integers $1 \leq f_i, f_i' \leq p_i - 1$. Reducing again modulo p_i gives $\frac{n}{p_i} f_i' \equiv \frac{n}{p_i} f_i \mod p_i$ and since $\frac{n}{p_i}$ is relatively prime to p_i it follows that $f_i \equiv f_i' \mod p_i$ hence $f_i = f_i'$ and the result follows. $\square$

4 Characters and Gauss sums

In this chapter we look at characters on finite abelian groups. We will need them in the next chapter about Gaussian periods. We start by defining characters of abelian groups then we prove some useful properties of these characters. In the last section we define Dirichlet characters, Gauss sums and Jacobi sums. The first section is based upon the notes of Keith Conrad about characters [4].

4.1 Characters of abelian groups

One can define characters for every group not necessarily for abelian ones. This is part of representation and character theory an important part of mathematics. The theory does becomes more complicated. We restrict our attention to the abelian case which is already interesting in its own right.
Define $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ as the unit circle in $\mathbb{C}$.

Definition 4.1. *A character χ on a finite abelian group G is a homomorphism $\chi : G \to S^1$.*

In this chapter we will write groups multiplicative so in the case of the definition we have $\chi(1) = 1$ and $\chi(gh) = \chi(g)\chi(h)$ for all $g, h \in G$. We start our investigation of characters on abelian groups by considering the special case of cyclic groups.

Theorem 4.2. *Let $G = \langle g \rangle$ be a cyclic group of order n. Then there are n characters of G defined by sending g to different powers of $e^{\frac{2\pi i}{n}}$.*

Proof. Because g generates G a character is determined by where it sends g. Since $1 = \chi(1) = \chi(g^n) = \chi(g)^n$ we see that $\chi(g)$ is a n^{th} root of unity so we have at most n characters on G. One sees easily that each choice of n^{th} root of unity for $\chi(g)$ gives a character on G. Hence there are n characters of G defined by sending g to different powers of $e^{\frac{2\pi i}{n}}$. □

If H is a subgroup of a finite abelian group G then we can extend characters of H to characters of G as the following lemma shows.

Lemma 4.3. *Let H be a subgroup of G. Any character of H can be extended to G in precisely $[G : H]$ ways.*

Proof. We will use induction on the index $[G : H]$. Let H be a proper subgroup of G, pick $a \in G \backslash H$ then $H \subsetneq \langle H, a\rangle \subset G$. Let χ be a character on H. We will extend χ to a character $\widetilde{\chi}$ on $\langle H, a\rangle$ and count in how many ways we can do this. Let k be the minimal positive integer such that $a^k \in H$ then $\widetilde{\chi}(a^k) = \chi(a^k)$ and $k = [\langle H, a\rangle : H]$. If $\widetilde{\chi}$ is a character then it is a k^{th} root of $\chi(a^k)$. Define $\widetilde{\chi}(a) \in S^1$ as a k^{th} root of $\chi(a^k)$, so $\widetilde{\chi}(a)^k = \chi(a^k)$. We will show that all possible k^{th} roots of $\chi(a^k)$ work.
Define now $\widetilde{\chi}$ on $\langle H, a\rangle$ as $\widetilde{\chi}(ha^i) := \chi(h)\widetilde{\chi}(a)^i$ for all i. Note that $\widetilde{\chi}$ is now defined on all of H. Before we proceed further we need to check first if $\widetilde{\chi}$ is well defined. Suppose $xa^i = ya^j$ for some $x, y \in H$ and $a^i, a^j \in \langle a\rangle$ then $a^{i-j} \in H$ hence $i \equiv j \mod k$ since k is the order of a in G/H. Write $j = i + kt$ so $x = ya^{kt}$. We now see that

$$\chi(y)\widetilde{\chi}(a)^j = \chi(y)\widetilde{\chi}(a)^i\widetilde{\chi}(a)^{kt} = \chi(y)\widetilde{\chi}(a)^i\chi(a^k)^t = \chi(ya^k)\widetilde{\chi}(a)^i = \chi(x)\widetilde{\chi}(a)^i\,,$$

hence the map $\widetilde{\chi} : \langle H, a\rangle \to S^1$ is well-defined. One can check easily that $\widetilde{\chi}$ is a homomorphism. It restricts to χ on H by construction. The number of extensions $\widetilde{\chi}$ of χ to $\langle H, a\rangle$ equals the number of possible values for $\widetilde{\chi}(a)$ which is $k = [\langle H, a\rangle : H]$. With an easy induction it follows now that there are $[G : H]$ extensions of a character on H to a character on G. □

Using the previous lemma we can now prove the following lemma.

Lemma 4.4. *For every non-identity element g of a finite abelian group G there exists a character χ of G such that $\chi(g) \neq 1$. There are precisely $\#G$ characters of G.*

Proof. The group $\langle g\rangle$ is a cyclic group of order $n > 1$ and the set of n^{th} roots of unity in S^1 is also a cyclic group of order n, hence we have an isomorphism between the two groups. We can view this isomorphism as a character on $\langle g\rangle$ by Lemma 4.3 it extends to a character on G. This extended character doesn't send g to 1. Applying Lemma 4.3 to $H = \{1\}$ shows that there are $\#G$ characters on G. □

To every character χ of a finite abelian group G we can associate the so-called conjugate character $\overline{\chi}$ which is defined as $\overline{\chi}(g) := \overline{\chi(g)}$ for all $g \in G$. One easily checks that $\overline{\chi}$ is a character. Note that $\chi(g)\overline{\chi}(g) = 1$ for all $g \in G$.

Definition 4.5. *The dual group, denoted by $\widehat{G}$, of the finite abelian group G is defined as the set of characters of G with multiplication defined by $(\chi\phi)(g) = \chi(g)\phi(g)$ for all $g \in G$ and $\chi, \phi \in \widehat{G}$. The inverse of χ is $\overline{\chi}$ and the identity element is the character 1_G defined by $1_G(g) = g$ for all $g \in G$.*

We will show that G is isomorphic to $\widehat{G}$. We first check whether this is true for cyclic groups.

Theorem 4.6. *If G is a cyclic group then $G \cong \widehat{G}$.*

Proof. Let n be the order of $G = \langle g \rangle$ and consider the character $\chi : G \to S^1 : g^j \to e^{\frac{2\pi i j}{n}}$. For any other character $\phi \in \widehat{G}$ we have $\phi(g) = e^{\frac{2\pi i k}{n}}$ for some integer k, so $\phi(g) = \chi(g)^k$ hence $\phi(g^j) = \phi(g)^j = \chi(g)^{kj} = \chi(g^j)^k$. It follows that χ generates $\widehat{G}$. Since G and $\widehat{G}$ have the same size by Theorem 4.2 the isomorphism follows. □

The following lemma tells us that the dual group of the direct product of two groups is isomorphic to the direct product of their dual groups. This will enable us in the next theorem to prove that for any finite abelian group G and $\widehat{G}$ are isomorphic.

Lemma 4.7. *If G and H are finite abelian groups then $\widehat{A \times B} \cong \widehat{A} \times \widehat{B}$.*

Proof. Let χ be a character on $A \times B$. Define the characters χ_A on A and χ_B on B (it is easy to check that they are characters) as follows: $\chi_A(a) := \chi(a, 1)$ and $\chi_B(b) := \chi(1, b)$. We have $\chi(a, b) = \chi((a, 1)(1, b)) = \chi_A(a)\chi_B(b)$ so we get a map $\widehat{A \times B} \to \widehat{A} \times \widehat{B} : \chi \to (\chi_A, \chi_B)$. One can check that this is in fact a group homomorphism. This homomorphism is injective since if χ_A and χ_B are both the identity then χ is too. By Lemma 4.4 we see that both groups have the same size so we have in fact an isomorphism. □

We are now ready to extend the result of Theorem 4.6 to arbitrary finite abelian groups.

Theorem 4.8. *Suppose G is a finite abelian group then $G \cong \widehat{G}$.*

Proof. We already know this in the case that G is cyclic. By induction and Lemma 4.7 we see that $\widehat{A_1 \times \ldots \times A_k} \cong \widehat{A_1} \times \ldots \times \widehat{A_k}$ with $\widehat{A_i} \cong A_i$ for all i. Every finite abelian group is isomorphic to a direct product of cyclic groups and since the dual group of every finite product of cyclic groups is isomorphic to itself the result follows. □

We need the following definition.

Definition 4.9. *For a subgroup H of the finite abelian group G define $H^\perp$ as the set $\{\chi \in \widehat{G} \mid \chi(H) = 1\}$.*

The next lemma tells us some more about $H^\perp$ and it shows us why $H^\perp$ is important.

Lemma 4.10. *If is H a subgroup of the finite abelian group G then $H^\perp$ is a subgroup of $\widehat{G}$ and $\widehat{G}/H^\perp \cong H$. In particular we have $\#H^\perp = [G : H]$.*

Proof. One checks easily that $H^\perp$ is a subgroup of $\widehat{G}$. Consider the map $\varphi : \widehat{G} \to \widehat{H}$ by sending χ to its restriction χ_H on H. It is an exercise to check that φ is a group homomorphism. We see that $\ker \varphi = \{\chi \in \widehat{G} \mid \chi_H = 1\} = \{\chi \in \widehat{G} \mid \chi = 1 \text{ on } H\} = H^\perp$. Any character of H can be extended to G, so when we restrict characters on G to H we certainly get all of them hence φ is surjective. It follows that $\widehat{G}/H^\perp \cong H$ and so $\#H^\perp = [G : H]$ since they are all finite groups. □

Besides multiplying characters we can also add them. The following theorem is easy to prove but of great importance.

Theorem 4.11. *Let G be a finite abelian group then we have*

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G & \text{if } \chi = 1_G \\ 0 & \text{if } \chi \neq 1_G \end{cases}$$

and

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} \#G & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases}.$$

Proof. If χ is trivial on G then $\sum_{g \in G} \chi(g) = \#G$. If not then $\chi(g') \neq 1$ for some $g' \in G$ hence $\chi(g') \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g'g) = \sum_{g \in G} \chi(g)$ since if g runs through G then so does $g'g$ and the result follows. For the second identity if $g = 1$ then the result is easily seen to be true. If $g \neq 1$ then by Lemma 4.4 there exists a $\phi \in \widehat{G}$ such that $\phi(g) \neq 1$ so $\phi(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\phi\chi)(g)$ and if χ runs through $\widehat{G}$ so does $\phi\chi$. The result follows. □

The previous theorem has the following important consequence.

Corollary 4.12 (**Orthogonality relations**). *Let G be a finite abelian group. For characters $\chi, \phi \in \widehat{G}$ and $g, h \in G$ we have*

$$\sum_{g \in G} \chi(g)\overline{\phi}(g) = \begin{cases} \#G & \text{if } \chi = \phi \\ 0 & \text{if } \chi \neq \phi \end{cases}$$

and

$$\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi}(h)=\begin{cases}\#G & \text{if } g=h\\ 0 & \text{if } g\neq h\end{cases}.$$

Proof. For the first identity apply the previous theorem by replacing χ with $\chi\overline{\phi}$. For the second identity apply the previous theorem to $g=gh^{-1}$. □

The following lemma is a generalization of Theorem 4.11.

Lemma 4.13. *Let H and G be a finite abelian groups with H a subgroup of G. For a character $\chi\in\widehat{G}$ we have*

$$\sum_{h\in H}\chi(h)=\begin{cases}\#H & \text{if } H\leq\ker\chi\\ 0 & \text{otherwise}\end{cases}.$$

Proof. If $H\leq\ker\chi$ it is clear that the sum equals $\#H$. If $H\not\leq\ker\chi$ then there exists $g\in H$ such that $\chi(g)\neq 1$, using $gH=H$ we see

$$\sum_{h\in H}\bar{\chi}(h)=\sum_{h\in H}\bar{\chi}(gh)=\chi(g)\sum_{h\in H}\bar{\chi}(h)$$

and the result follows. □

4.2 Gauss sums

We will now use characters of finite abelian groups to define Gauss sums. We use them in the next chapter to write certain constants as a sum of Gauss sums and approximate them in the end. Proofs of the theorems and lemmas can be found in chapter 8 of [5].

Let $n\geq 2$ be an integer. Write $\overline{a}$ for the residue class of $a \mod n$ then we know that $(\mathbb{Z}/n\mathbb{Z})^*=\{\overline{a}\mid\gcd(a,n)=1\}$. Any character $\widetilde{\chi}$ of $(\mathbb{Z}/n\mathbb{Z})^*$ can be lifted to a map $\chi:\mathbb{Z}\to\mathbb{C}$ by defining

$$\chi(a):=\begin{cases}\widetilde{\chi}(\overline{a}) & \text{if } \gcd(a,n)=1\\ 0 & \text{if } \gcd(a,n)\neq 1\end{cases}$$

for every $a \in \mathbb{Z}$. This new map χ has the following properties as one can easily check: $\chi(1) = 1$, $\chi(ab) = \chi(a)\chi(b)$, $\chi(a) = \chi(b)$ if $a \equiv b \mod n$ and $\chi(a) = 0$ if $\gcd(a, n) \neq 1$. Any map χ satisfying the previous four properties is called a Dirichlet character modulo n. If χ is a Dirichlet character then it has a corresponding character $\widetilde{\chi}$ on $(\mathbb{Z}/n\mathbb{Z})^*$. In the same way as we did with characters on finite abelian groups we can define the product of two Dirichlet characters. It turns out that the Dirichlet characters modulo n form a group under this multiplication with identity χ_0 satisfying $\chi_0(a) = 1$ if $\gcd(a, n) = 1$ and 0 otherwise. Inverses are given by taking the complex conjugate.
We couldn't define the product of two characters on different finite abelian groups, but we can define the product of two Dirichlet characters with different moduli. If ϕ and χ are Dirichlet characters modulo m and n respectively then $\phi\chi$ is a Dirichlet character modulo $\text{lcm}(m, n)$.

For Dirichlet characters there also exist orthogonality relations.

Theorem 4.14 (**Orthogonality relations**). *Let $n \geq 2$ be an integer and χ, ϕ Dirichlet characters modulo n. We then have*

$$\sum_{(\mathbb{Z}/n\mathbb{Z})^*} \chi(a)\overline{\phi(a)} = \begin{cases} \varphi(n) & \text{if } \chi = \phi \\ 0 & \text{if } \chi \neq \phi \end{cases}$$

and

$$\sum \chi(a)\overline{\chi(b)} = \begin{cases} \varphi(n) & \text{if } \gcd(ab, n) = 1 \text{ and } a \equiv b \mod n \\ 0 & \text{otherwise} \end{cases}$$

where the sums runs over all Dirichlect characters modulo n.

Let χ be a Dirichlet character modulo n and d a positive divisor of n. We say that χ is induced by a Dirichlet character ϕ modulo d if $\chi(a) = \phi(a)$ for all integers a with $(a, n) = 1$. We will need the following definition of the conductor of a Dirichlet character.

Definition 4.15. *Let $n \geq 2$ be an integer. The conductor of a Dirichlet character χ modulo n, denoted by f_χ, is the greatest common divisor of all integers d such that χ is induced by a character modulo d.*

The following lemma tells us that there is only one Dirichlet character modulo f_χ inducing the Dirichlet character χ modulo n.

Lemma 4.16. *Let χ be a Dirichlet character modulo n then there exists a unique Dirichlet character modulo f_χ inducing χ.*

We are now ready to define the Gauss sums. In the rest of this section we let ω_n be the primitive n^{th} root of unity $e^{\frac{2\pi i}{n}}$ in $\mathbb{C}$ for $n \geq 1$.

Definition 4.17. *Let $n \in \mathbb{N}$, χ be a Dirichlet character of $(\mathbb{Z}/n\mathbb{Z})^*$ and set $K = \mathbb{Q}(\omega_n)$. The Gauss sum $g(\chi)$ corresponding to χ is the sum*

$$g(\chi) = \sum_{t \in (\mathbb{Z}/n\mathbb{Z})^*} \chi(t)\omega_n^t \,.$$

If $n = p$ is an odd prime we have some nice results about Gauss sums. In Corollary 4.27 we generalize this theorem.

Theorem 4.18. *Let p be an odd prime. If χ is a non-trivial Dirichlet character modulo p then*

$$g(\chi)g(\overline{\chi}) = \chi(-1)p \text{ and } |g(\chi)|^2 = p \,.$$

We have $g(\chi) \in \mathbb{Q}(\omega_{n\varphi(n)})$ since $\operatorname{im}\chi \subseteq \langle e^{\frac{2\pi i}{\varphi(n)}} \rangle$. In particular in the case of an odd prime p we have that $g(\chi) \in \mathbb{Q}(\omega_{p(p-1)})$. It turns out that a certain quotient of Gauss sums lies in the smaller field $\mathbb{Q}(\omega_{p-1})$. For this we need the definition of the Jacobi sum.

Definition 4.19. *Let p be an odd prime and χ, ψ be Dirichlet characters modulo p. The Jacobi sum is defined by*

$$J(\chi, \psi) = \sum_{t=2}^{p-1} \chi(t)\psi(1-t) \,.$$

Theorem 4.20. *Let p be an odd prime and χ, ψ be Dirichlet character modulo p with χ and ψ not each others inverse. We then have*

$$g(\chi)g(\psi) = J(\chi, \psi)g(\chi\psi) \,.$$

The previous theorem has the following nice corollary.

Corollary 4.21. *Using the same notation as in Theorem 4.20 then if χ and ψ are not each others inverse we have $|J(\chi, \psi)| = \sqrt{p}$.*

Proof. This follows from Theorem 4.18 and Theorem 4.20. □

Gauss sums behave well under the Galois action of $\operatorname{Gal}(\mathbb{Q}(\omega_{n\varphi(n)})/\mathbb{Q})$ as the following lemma shows.

Lemma 4.22. *Let $n \geq 2$ be an integer, χ a Dirichlet character modulo n, $d \in (\mathbb{Z}/n\varphi(n)\mathbb{Z})^*$ and $\sigma_d \in Gal(\mathbb{Q}(\omega_{n\varphi(n)})/\mathbb{Q})$. We then have $\sigma_d(g(\chi)) = \overline{\chi}^d(d)g(\chi^d)$.*

Proof. By definition of the Gauss sum we have

$$\sigma_d(g(\chi)) = \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \sigma_d(\chi(t))\sigma_d(\omega_n^t) = \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \chi^d(t)\omega_n^{dt}$$

since $\gcd(d,n) = 1$ we have $d(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^*$ hence

$$\sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \chi^d(t)\omega_n^{dt} = \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \chi^d(td^{-1})\omega_n^{t} = \overline{\chi}^d(d)g(\chi^d)$$

by replacing t with td^{-1}. □

We will now show that Gauss sums corresponding to a Dirichlet character modulo n can be factored in the case of n being square-free. It is also true for general n but the case n square-free is the only case we need. Hence it suffices often to prove something only for the factors in order to prove it for the general Gauss sum. We start by factoring Dirichlet characters.
Write $n = p_1 \dots p_r$ with p_i distinct prime numbers. If a is an integer we know by the Chinese remainder theorem that we can find integers a_i such that $a_i \equiv a \mod p_i$ and $a_i \equiv 1 \mod p_j$ for all $j \neq i$. If χ is a Dirichlet character modulo n then define the map $\chi_i : Z \to \mathbb{C}$ by $\chi_i(a) := \chi(a_i)$. It is not difficult to show that χ_i is a well-defined character modulo p_i.

Lemma 4.23. *We can factor the Dirichlet character χ modulo n uniquely as $\chi = \chi_1 \dots \chi_r$ where χ_i is defined in the previous paragraph.*

The following lemma shows that conductors factor in a similar way as the Dirichlet character.

Lemma 4.24. *The conductor of the Dirichlet character χ in Lemma 4.23 factors as $f_\chi = f_{\chi_1} \dots f_{\chi_r}$.*

We are now ready to prove that we can factorize Gauss sums.

Theorem 4.25. *Let χ be a Dirichlet character modulo n with n square-free. Let χ_i be defined as in the previous paragraph then the Gauss sums $g(\chi)$ factors as*

$$g(\chi) = \prod_{i=1}^{r} \chi_i(\tfrac{n}{p_i})g(\chi_i)\,.$$

Proof. We have by using the definition of the χ_i's that

$$g(\chi) = \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \chi(t)\omega_n^t = \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \prod_{i=1}^{r} \chi_i(t_i)\omega_n^{t_i}\,.$$

Since $\omega_n = \omega_{p_i}^{\frac{p_i}{n}}$ for all i we have

$$g(\chi) = \prod_{i=1}^{r} \sum_{t\in(\mathbb{Z}/p_i\mathbb{Z})^*} \chi_i(t)\omega_{p_i}^{t\frac{p_i}{n}} = \prod_{i=1}^{r} \sum_{t\in(\mathbb{Z}/p_i\mathbb{Z})^*} \chi_i(\frac{n}{p_i}t)\omega_{p_i}^{t}$$

where the last equality is true because if t runs through $(\mathbb{Z}/p_i\mathbb{Z})^*$ then so does $\frac{n}{p_i}t$ since $\gcd(\frac{n}{p_i}, p_i) = 1$ for all i. It follows that

$$g(\chi) = \prod_{i=1}^{r} \chi_i(\tfrac{n}{p_i})g(\chi_i)\,.$$

□

Theorem 4.25 has the following two consequences.

Corollary 4.26. *If n is square-free and χ_0 is the trivial Dirichlet character modulo n then $g(\chi_0) \neq 0$.*

Proof. Since $\omega_p + \omega_p^2 + \ldots + \omega_p^{p-1} = -1$ for prime numbers p we have that $g(\chi_{p,0}) = -1$ where $\chi_{p,0}$ is the trivial Dirichlet character modulo p. If $n = p_1 \ldots p_r$ where the p_i are different prime numbers then

$$g(\chi_0) = \prod_{i=1}^{r} g(\chi_{p_i,0}) = (-1)^r$$

so $|g(\chi_0) = 1|$ and the result follows. □

The following corollary is a generalization of Theorem 4.18. It relates the Euclidian norm of $g(\chi)$ to f_χ with χ a Dirichlet character modulo a square-free integer n.

Corollary 4.27. *If n is square-free and χ is a Dirichlet character modulo n then $|g(\chi)|^2$ is equal to the conductor f_χ.*

Proof. Using Theorem 4.25 we see that

$$|g(\chi)|^2 = \prod_{i=1}^{r} |g(\chi_i)|^2 \tag{2}$$

with $n = p_1 \dots p_r$. Since χ_i is a Dirichlet character modulo a prime number we have that $g(\chi_i) = -1$ if and only if χ_i has conductor 1. It follows that the right-hide side of (2) is equal to $f_{\chi_1} \dots f_{\chi_r}$. □

5 Gaussian periods

In this chapter we treat the main subject of this paper: Gaussian periods. In the first section we define Gaussian periods and we prove some useful results about them. In the second section we try to answer the question when some set of Gaussian periods is an integral basis for the ring of integers of a subfield of a cyclotomic extension. In the third section we estimate certain coefficients related to the Gaussian periods. In the final section we give a construction for regular p-gons with p a Fermat prime using Gaussian periods.

5.1 Introduction

We start by introducing some notation which we will use frequently throughout the chapter. For a $n \in \mathbb{N}$ let ω_n be a primitive n^{th} root of unity. Consider the field extension $K = \mathbb{Q}(\omega_n)/\mathbb{Q}$. In chapter 3 we have shown that it is a Galois extension of degree $\varphi(n)$ with Galois group $\text{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$ such that for each $a \in (\mathbb{Z}/n\mathbb{Z})^*$ the automorphism $\sigma_a \in \text{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ is defined by $\sigma_a(\omega_n) = \omega_n^a$. By Galois correspondence we can uniquely associate to each subgroup G of $(\mathbb{Z}/n\mathbb{Z})^*$ its fix field $K^G = \{x \in K \mid \sigma_g(x) = x \text{ for all } g \in G\}$.
The main focus of this chapter lies with certain special sums inside the cyclotomic extension K, the so called Gaussian periods.

Definition 5.1. *For a subgroup G of $(\mathbb{Z}/n\mathbb{Z})^*$ and an $a \in \mathbb{Z}/n\mathbb{Z}$ define the Gaussian period $S(G, a)$ as*

$$S(G, a) = \sum_{g \in G} \omega_n^{ag}\,.$$

Note that $ag = a \cdot g$ is defined in the ring $\mathbb{Z}/n\mathbb{Z}$ where $(\mathbb{Z}/n\mathbb{Z})^*$ is the set of units of $\mathbb{Z}/n\mathbb{Z}$. We identify $\mathbb{Z}/n\mathbb{Z}$ with the numbers $\{0, 1, 2, \ldots, n-1\}$. Because ω_n is a primitive n^{th} root of unity the exponentiation is well-defined.

Example 5.2. *Let $n = 13$ then $G = \langle 8 \rangle$ is a subgroup of $(\mathbb{Z}/13\mathbb{Z})^*$ of order 4. Some of the Gaussian periods belonging to G are $S(G, 1) = \omega_{13} + \omega_{13}^5 + \omega_{13}^8 + \omega_{13}^{12}$, $S(G, 2) = \omega_{13}^2 + \omega_{13}^3 + \omega_{13}^{10} + \omega_{13}^{11}$ and $S(G, 4) = \omega_{13}^4 + \omega_{13}^6 + \omega_{13}^7 + \omega_{13}^9$.*

As we shall see the Gaussian periods in the previous example are all different. This is however not always the case.

Example 5.3. *Let $n = 12$ and consider the subgroup $G = \langle 7 \rangle$. If ω_{12} is a primitive 12^{th} root of unity then ω_{12}^6 is a primitive second root of unity hence equal to -1. Therefore $S(G, 1) = \omega_{12} + \omega_{12}^7 = 0$ and hence $S(G, a) = 0$ for all $a \in (\mathbb{Z}/12\mathbb{Z})^*$ by applying a field automorphism.*

The Gaussian periods are constructed by summing over group elements. We may therefore expect that the Gaussian periods have some special properties. The next lemma shows that the Gaussian periods behave well under field automorphisms.

Lemma 5.4. *Let G be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and let $b \in (\mathbb{Z}/n\mathbb{Z})^*$ then $\sigma_b(S(G, a)) = S(G, ab)$.*

Proof. Since σ_b is a field automorphism of $\mathbb{Q}(\omega_n)$ we get

$$\sigma_b(S(G, a)) = \sum_{g \in G} \sigma_b(\omega_n^{ag}) = \sum_{g \in G} \omega_n^{abg} = S(G, ab)\,.$$

□

We see that $\mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ permutes the Gaussian periods. We can even say more about this when we assume that b lies in G.

Lemma 5.5. *Let G be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and a an arbitrary element of $\mathbb{Z}/n\mathbb{Z}$. If b is an element of G then $\sigma_b(S(G, a)) = S(G, a)$ for all $a \in \mathbb{Z}/n\mathbb{Z}$ so that $S(G, a)$ lies in the fixed field K^G of G.*

Proof. Using Lemma 5.4 gives

$$\sigma_b(S(G, a)) = S(G, ab) = \sum_{g \in G} \omega_n^{abg} = \sum_{g \in G} \omega_n^{ag}$$

where the last equality holds because if g runs through G then so does bg if $b \in G$. So we have $\sigma_b(S(G, a)) = S(G, a)$ and from the definition of K^G it follows immediately since b was an arbitrary element of G that $S(G, a) \in K^G$ for every a. □

Because $(\mathbb{Z}/n\mathbb{Z})^*$ is abelian we can form the quotient group $(\mathbb{Z}/n\mathbb{Z})^*/G$ for a subgroup $G \leq (\mathbb{Z}/n\mathbb{Z})^*$.

Lemma 5.6. *Suppose the elements $a, b \in G$ lie in the same coset of $(\mathbb{Z}/n\mathbb{Z})^*/G$ then $S(G, a) = S(G, b)$.*

Proof. This follows from the fact that $aG = bG$ so that

$$S(G, a) = \sum_{g \in G} \omega_n^{ag} = \sum_{g \in G} \omega_n^{bg} = S(G, b) .$$

□

For a $x \in (\mathbb{Z}/n\mathbb{Z})^*/G$ define σ_x as σ_a for some $a \in G$ lying in the coset x. Since $S(G, a)$ is constant on cosets of G in $(\mathbb{Z}/n\mathbb{Z})^*$ this is well defined and σ_x is a field automorphism.

From the Gaussian periods belonging to a certain group H we can find the Gaussian periods belonging to every group G which contains H as a subgroup.

Lemma 5.7. *Let H, G be subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ with $H \leq G$. Then*

$$S(G, a) = \sum_{x \in G/H} \sigma_x(S(H, a)) .$$

Proof. Because G/H is a quotient group we can write G as a finite disjoint sum of cosets of H i.e. $G = \cup_i g_i H$ with $g_i H \cap g_j H = \emptyset$ if and only if $g_i \neq g_j$. So

$$S(G, a) = \sum_{g \in G} \omega_n^{ag} = \sum_i \sum_{h \in H} \omega_n^{ag_i h} = \sum_{g_i} \sigma_{g_i}(S(H, a)) .$$

□

Besides behaving nice under field automorphisms the Gaussian periods also behave well under multiplication. The product of two Gaussian periods is equal to a sum of Gaussian periods as the following lemma shows.

Lemma 5.8. *Let G be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ for $a, b \in \mathbb{Z}/n\mathbb{Z}$ we have*

$$S(G, a)S(G, b) = \sum_{g \in G} S(G, a + bg) .$$

Proof. Using the definition of Gaussian periods we see

$$S(G, a)S(G, b) = \sum_{g,h \in G} \omega_n^{ah+bg} = \sum_{g,h \in G} \omega_n^{(a+bgh^{-1})h}$$

if g runs through G then so does gh hence

$$\sum_{g,h\in G} \omega_n^{(a+bgh^{-1})h} = \sum_{g,h\in G} \omega_n^{(a+bg)h} = \sum_{g\in G} S(G, a+bg)\,.$$

□

In a way multiplying Gaussian periods becomes adding Gaussian periods which is easier to deal with.

5.2 Gaussian periods as an integral basis for subfields of cyclotomic extension

In this section we will show that the Gaussian periods are a basis for the ring of integers of a subfield of a square-free cyclotomic extension, more precisely we will show that the set $\{S(G,a)\}_{a\in(\mathbb{Z}/n\mathbb{Z})^*/G}$ is an integral basis for $\mathcal{O}_{K^G}$ for every subgroup $G \leq (\mathbb{Z}/n\mathbb{Z})^*$ if and only if n is square-free. For non square-free extensions some subfields do have a basis consisting of Gaussian periods and others do not. We give some partial results for this.

We first need a lemma concerning the order of $1+\frac{n}{m}$ for integers m and n with $m^2 \mid n$ in $(\mathbb{Z}/n\mathbb{Z})^*$.

Lemma 5.9. *Let n be a positive integer and let m be an integer such that $m^2 \mid n$. The order of $1+\frac{n}{m}$ in $(\mathbb{Z}/n\mathbb{Z})^*$ is equal to m.*

Proof. Using the binomial theorem we see that

$$(1+\tfrac{n}{m})^k = 1 + \binom{k}{1}\frac{n}{m} + \binom{k}{2}\frac{n^2}{m^2} + \ldots + \binom{k}{k}\frac{n^k}{m^k}$$

for $k \geq 0$. For $l \geq 2$ we have $m^l \mid n^{l-1}$ since $m^2 \mid n$ hence $\frac{n^l}{m^l}$ is divisible by n for $l \geq 2$. This gives

$$(1+\tfrac{n}{m})^k \equiv 1 + k\frac{n}{m} \mod n\,.$$

Now $1+k\frac{n}{m}$ is equal to 1 modulo n if $k\frac{n}{m}$ is zero modulo n and this happens if and only if k is a multiple of m since $n \neq 0$. It follows that $1+\frac{n}{m}$ indeed has order m in $(\mathbb{Z}/n\mathbb{Z})^*$. □

The following lemma shows for non-square-free n that some of the Gaussian periods are zero.

Lemma 5.10. *Let m be an integer such that $m^2 \mid n$ for a positive integer n then $S(\langle 1 + \frac{n}{m} \rangle, 1) = 0$.*

Proof. Using Lemma 5.9, we have

$$\sum_{k=0}^{m-1} \omega_n^{(1+\frac{n}{m})^k} = \sum_{k=0}^{m-1} \omega_n^{1+k\frac{n}{m}} = \omega_n \sum_{k=0}^{m-1} (\omega_n^{\frac{n}{m}})^k$$

since $\omega_n^{\frac{n}{m}}$ is a primitive m-th root of unity it follows that

$$\omega_n \sum_{k=0}^{m-1} (\omega_n^{\frac{n}{m}})^k = \omega_n \frac{(\omega_n^{n/m})^m - 1}{\omega_n^{n/m} - 1} = 0$$

since $(\omega_n^{n/m})^m = 1$. □

Lemma 5.10 together with Lemma 5.7 gives the following corollary.

Corollary 5.11. *Let G be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ such that $\langle 1 + \frac{n}{m} \rangle \leq G$ for some $m^2 \mid n$ then $S(G, a) = 0$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^*$.*

Proof. Setting $H = \langle 1 + \frac{n}{m} \rangle$ a lemma from the first section of this chapter gives

$$S(G, a) = \sum_{x \in G/H} \sigma_x(S(H, a))$$

and since $S(H, a) = \sigma_a(S(H, 1)) = 0$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$ the result follows. □

As a consequence we see that for $\{S(G, a)\}_{a \in (\mathbb{Z}/n\mathbb{Z})^*/G}$ to be a basis of $\mathcal{O}_{K^G}$ for every subgroup G of $(\mathbb{Z}/n\mathbb{Z})^*$ we need to have that n is square-free. It only remains to show that being square-free is also sufficient.

The following lemma gives us an explicit primitive element for K^G when G is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ with n square-free.

Lemma 5.12. *If n is square-free then $S(G, 1)$ generates K^G i.e. $K^G = \mathbb{Q}(S(G, 1))$.*

Proof. We already know that $S(G,1) \in K^G$, so we need to prove that it isn't contained in a subfield. Suppose K^H is a subfield containing $S(G,1)$ with H a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, by Galois correspondence every subfield is of this form and also by the Galois correspondence we have $G \leq H$. Suppose there is an $a \in H \backslash G$ such that $\sigma_a(S(G,1)) = S(G,1)$ then

$$\sum_{g \in G} \omega_n^g = \sum_{g \in G} \omega_n^{ag}.$$

Note that the set $\{g \mid g \in G\} \cup \{ag \mid g \in G\}$ contains precisely $2\#G$ different invertible elements modulo n. Because $\{\omega_n^b\}_{b,\gcd(b,n)=1}$ is an integral basis for $\mathcal{O}_K$ by Theorem 3.15 it follows that there is a non-trivial $\mathbb{Z}$-linear dependency between the elements of $\{\omega_n^b\}_{b,\gcd(b,n)=1}$. A contradiction when n is square-free. It follows that $G = H$ and $S(G,1)$ isn't contained in a smaller field so by Galois correspondence it follows that we must have $K^G = \mathbb{Q}(S(G,1))$. □

Applying a field automorphism to $S(G,1)$ shows that $K^G = \mathbb{Q}(S(G,a))$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^*$. We are now ready to prove the converse.

Lemma 5.13. *Let n be a square-free positive integer, G any subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ then $\mathcal{O}_{K^G}$ the ring of integers of the fix field K^G has $\{S(G,h)\}_{h \in (\mathbb{Z}/n\mathbb{Z})^*/G}$ as an integral basis.*

Proof. Suppose $x = \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^*} c_k \omega_n^k \in \mathcal{O}_{K^G}$ for some $c_k \in \mathbb{Z}$. We can write x in this way since $\mathcal{O}_{K^G} \subset \mathcal{O}_K$. Since $\sigma_g(x) = x$ for all $g \in G$ it follows that

$$x = \sigma_g(x) = \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^*} c_k \omega_n^{gk} = \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^*} c_{g^{-1}k} \omega_n^k.$$

Since $\{\omega_n^b\}_{b,\gcd(b,n)=1}$ is an integral basis for $\mathcal{O}_K$ it follows that $c_k = c_{g^{-1}k}$ for all $g \in G$ hence c_k is constant on cosets of G in $(\mathbb{Z}/n\mathbb{Z})^*$. This gives

$$x = \sum_{h \in (\mathbb{Z}/n\mathbb{Z})^*/G} c_h S(G,h)$$

for some $c_h \in \mathbb{Z}$. We see that $\mathcal{O}_{K^G}$ is spanned by $\{S(G,h)\}_{h \in (\mathbb{Z}/n\mathbb{Z})^*/G}$, which are $\frac{\varphi(n)}{\#G}$ elements. we also know that $\mathcal{O}_{K^G}$ is spanned by $[K^G : \mathbb{Q}]$ elements. Since $[K^G : \mathbb{Q}] = \frac{[K:\mathbb{Q}]}{[K:K^G]} = \frac{\varphi(n)}{\#G}$ by the tower relation for field extensions we have that $\{S(G,h)\}_{h \in (\mathbb{Z}/n\mathbb{Z})^*/G}$ is an integral basis for $\mathcal{O}_{K^G}$. □

We have now proven the following theorem.

Theorem 5.14. *The ring of integers $\mathcal{O}_{K^G}$ of the fix field K^G belonging to $G \leq (\mathbb{Z}/n\mathbb{Z})^*$ in $\mathbb{Q}(\omega_n)$ has $\{S(G,h)\}_{h\in(\mathbb{Z}/n\mathbb{Z})^*/G}$ as an integral basis if and only if n is square-free.*

When n is square-free we get a very nice result. What happens when n is not square-free? Calculating the subgroup diagram for various cyclotomic extensions $\mathbb{Q}(\omega_n)$ for small n we see that in those cases $S(G,1)$ generates K^G precisely when G has no subgroups of the form $\langle 1+\frac{n}{p}\rangle$ with p a prime such that $p^2 \mid n$. This lead to the following conjecture:

Conjecture. *Let G be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ for some positive integer n. We have $\mathbb{Q}(S(G,1)) = K^G$ if and only if G doesn't contain any subgroups of the form $\langle 1+\frac{n}{p}\rangle$ with p a prime satisfying $p^2 \mid n$.*

We saw that this is true for n square-free. If n is an odd prime power then we can show the weaker statement that $S(G,1) \neq 0$ when G doesn't contain any subgroups of the form $\langle 1+\frac{n}{p}\rangle$.

Theorem 5.15. *Let $n = p^k$ with p an odd prime and $k \geq 1$ then $S(G,1) \neq 0$ if and only if $\langle 1+\frac{n}{p}\rangle$ is not a subgroup of G.*

Proof. The element $1+\frac{n}{p}$ has order p in the cyclic group $(\mathbb{Z}/n\mathbb{Z})^*$ (here we need that n is an odd prime power) hence $\langle 1+\frac{n}{p}\rangle$ is the unique cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ of order p. All subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ with order divisible by p have $\langle 1+\frac{n}{p}\rangle$ as a subgroup. We already saw that for those groups G we have $S(G,a) = 0$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. This proves one part of the theorem. Suppose G is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ such that $\langle 1+\frac{n}{p}\rangle$ is not a subgroup of G. As $\langle 1+\frac{n}{p}\rangle$ is the unique subgroup of order p it follows that $\#G$ is not divisible by p. Consider the polynomial $f_G(x) = \sum_{g\in G} x^g$ then $f_G(1) = \#G$ which is not divisible by p. Suppose on the contrary that $S(G,1) = 0$ then $f_G(\omega_n) = 0$ so that $\Phi_n(x)$ is a factor of $f_G(x)$ since $\Phi_n(x)$ is the minimal polynomial of ω_n. This gives however $p = \Phi_n(1) \mid f_G(1) = \#G$ since n is a prime power. A contradiction, so if $\langle 1+\frac{n}{p}\rangle$ is not a subgroup of G then $S(G,1) \neq 0$. □

Even if the conjecture is true then we cannot take the $\mathbb{Q}$-conjugates of $S(G,1)$ to generate $\mathcal{O}_{K^G}$ as the following example shows.

Example 5.16. *Take $n = 20$ and consider the subgroup $\langle 19\rangle$ of $(\mathbb{Z}/20\mathbb{Z})^*$. It is easy to check that it doesn't have any subgroups of the form $\langle 1+\frac{n}{m}\rangle$. The Gaussian periods $\{S(G,a)\}_{a\in(\mathbb{Z}/20\mathbb{Z})^*}$ satisfy $S(G,3) = S(G,1)^3 - 3S(G,1)$, $S(G,7) = -S(G,3)$,*

$S(G,9) = -S(G,1)$ *and* $S(G,a+10) = S(G,a)$ *for all* a. *The set* $\{S(G,a)\}_{a\in(\mathbb{Z}/20\mathbb{Z})^*}$ *consists therefore of the elements* $\{\pm S(G,1), \pm S(G,3)\}$. *We see that* $S(G,3)^2$ *isn't contained in the span.*

As the $\mathbb{Q}$-conjugates of $S(G,1)$ don't generate $\mathcal{O}_{K^G}$ the next question would be if the set $\{S(G,a)\}_{0\leq a\leq n}$ generates $\mathcal{O}_{K^G}$. The following example shows that this is also not the case.

Example 5.17. *Let* $n = 16$ *and consider the subgroup* $\langle 9\rangle$ *of* $(\mathbb{Z}/16\mathbb{Z})^*$. *The corresponding fix field is* $\mathbb{Q}(\omega^2)$ *with* $\omega = \omega_{16}$. *The* $\mathbb{Z}$*-span of all elements of the form* $S(\langle 9\rangle, a)$ *is equal to the* $\mathbb{Z}$*-span of the four elements* $2, 2\omega^2, 2\omega^4, 2\omega^6$. *These elements are* $\mathbb{Z}$*-independent because otherwise the minimal polynomial of* ω *would have degree less or equal to* 6. *Which is impossible. Since* $\omega^2 \in \mathcal{O}_{K^{\langle 9\rangle}}$ *the element* ω^2 *is not in this span.*

5.3 Estimating the coefficients of $S(G,c)$ in $S(G,a)S(G,b)$

In the first section we saw that the product of two Gaussian periods is a sum of Gaussian periods. In the case that n is a square-free positive integer we can say more. If G is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ the set $\{S(G,h)\}_{h\in(\mathbb{Z}/n\mathbb{Z})^*/G}$ forms an integral basis of $\mathcal{O}_{\mathbb{Q}(\omega_n)}$. As a consequence for $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ there exist unique integers N_{ab}^c such that

$$S(G,a)S(G,b) = \sum_{c\in(\mathbb{Z}/n\mathbb{Z})^*/G} N_{ab}^c S(G,c)\,.$$

As indicated the integers N_{ab}^c depend on a, b and c. We can simplify this by applying σ_a for $a \in (\mathbb{Z}/n\mathbb{Z})^*/G$ to

$$S(G,1)S(G,ba^{-1}) = \sum_{d\in(\mathbb{Z}/n\mathbb{Z})^*/G} N_{ba^{-1}}^d S(G,d)$$

which gives

$$S(G,a)S(G,b) = \sum_{d\in(\mathbb{Z}/n\mathbb{Z})^*/G} N_{ba^{-1}}^d S(G,ad)\,.$$

Since the integers N_{ab}^c are unique it follows that $N_{ab}^{ad} = N_{ba^{-1}}^d$ for all $d \in (\mathbb{Z}/n\mathbb{Z})^*$. So knowing what the coefficients N_a^c are in $S(G,1)S(G,a)$ is enough for determining how to write $S(G,a)S(G,b)$ for arbitrary $a, b \in \mathbb{Z}/n\mathbb{Z}$ as a sum of Gaussian periods. When the integers N_{ab}^c are all known we also completely understand the multiplication table for the Gaussian periods.

In the case of square-free n we can use Gauss sums to estimate the integers N_{ab}^c in terms of n and $\#G$. We have a field isomorphism $\mathbb{Q}(\omega_n) \cong \mathbb{Q}(e^{\frac{2\pi i}{n}})$ where ω_n is some n^{th} root of unity. So instead of letting ω_n be an arbitrary n^{th} root of unity we take without loss of generality $\omega_n = e^{\frac{2\pi i}{n}}$.
Consider the extension $K = \mathbb{Q}(\omega_{n\varphi(n)})/\mathbb{Q}$ where $\omega_{n\varphi(n)}$ is a primitive $n\varphi(n)^{\text{th}}$ root of unity. It contains $\mathbb{Q}(\omega_n)$ and $\mathbb{Q}(\omega_{\varphi(n)})$ as subfields with $\omega_{\varphi(n)}$ a primitive $\varphi(n)^{\text{th}}$ root of unity. Let χ be a Dirichlet character modulo n then $\operatorname{im}\chi \subseteq \langle\omega_{\varphi(n)}\rangle \cup \{0\}$ hence the Gauss sum

$$g(\chi) = \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \chi(t)\omega_n^t$$

lies in K. We can write $S(G,a)$ for $a \in (\mathbb{Z}/n\mathbb{Z})^*$ as a linear combination of Gauss sums.

Lemma 5.18. *Let n be a square-free integer, G a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and $a \in (\mathbb{Z}/n\mathbb{Z})^*$. We can write $S(G,a)$ as the sum*

$$S(G,a) = \frac{\#G}{\varphi(n)} \sum_{\chi\in G^\perp} g(\chi)\bar{\chi}(a)\,.$$

Proof. For $a \in (\mathbb{Z}/n\mathbb{Z})^*$ we see that

$$\frac{1}{\varphi(n)} \sum_{\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^*}} \bar{\chi}(a)g(\chi) = \frac{1}{\varphi(n)} \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^*} \omega_n^t \sum_{\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^*}} \chi(ta^{-1}) = \omega_n^a$$

by using the definition of $g(\chi)$ in the first equality and the orthogonality relations

$$\sum_{\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^*}} \chi(ta^{-1}) = \begin{cases} \varphi(n) & \text{if } t = a \\ 0 & \text{otherwise} \end{cases}$$

in the last equality. It follows that we can write $S(G,a)$ as

$$S(G,a) = \frac{1}{\varphi(n)} \sum_{h\in G} \sum_{\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^*}} \bar{\chi}(ah)g(\chi)\,.$$

Using Lemma 4.13 we see that we can further simplify this to

$$S(G,a) = \frac{\#G}{\varphi(n)} \sum_{\chi\in G^\perp} g(\chi)\bar{\chi}(a)\,.$$

□

Using Lemma 5.18 we obtain the following formula for $S(G,a)S(G,b)$:

$$S(G,a)S(G,b) = \left(\frac{\#G}{\varphi(n)}\right)^2 \sum_{\chi,\psi\in G^\perp} g(\chi)g(\psi)\bar{\chi}(a)\bar{\psi}(b)\,. \tag{3}$$

Since n is square-free all Gauss sums $g(\chi)$ with $\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^*}$ are non-zero, this follows from Corollary 4.27 because the conductor is never zero. We may therefore divide by $g(\chi)$.

Definition 5.19. *For $a,b \in (\mathbb{Z}/n\mathbb{Z})^*$ and $c \in (\mathbb{Z}/n\mathbb{Z})^*/G$ define T_{ab}^c as the following sum*

$$\left(\frac{\#G}{\varphi(n)}\right)^2 \sum_{\chi,\psi\in G^\perp} \frac{g(\chi)g(\psi)}{g(\chi\psi)}\bar{\chi}(a)\bar{\psi}(b)(\chi\psi)(c)\,.$$

If we use (3) then we see that

$$S(G,a)S(G,b) = \sum_{c\in(\mathbb{Z}/n\mathbb{Z}/G)^*} T_{ab}^c\omega_n^c\,.$$

We want to show that the T_{ab}^c are integers because then we have $T_{ab}^c = N_{an}^c$ for all a,b and c. We know that $\{\omega_n^c\}_{c\in(\mathbb{Z}/n\mathbb{Z})^*}$ forms an integral basis of $\mathcal{O}_{\mathbb{Q}(\omega_n)}$ but we cannot use this here to deduce that $T_{ab}^c \in \mathbb{Z}$ because T_{ab}^c can be anything in the field K. If we can show that it lies in $\mathbb{Q}$ then we can use the fact about the integral basis to conclude that T_{ab}^c lives in $\mathbb{Z}$. We will use Galois theory to show that $T_{ab}^c \in \mathbb{Q}$.

Lemma 5.20. *For every $a,b \in (\mathbb{Z}/n\mathbb{Z})^*$ and $c \in (\mathbb{Z}/n\mathbb{Z})^*/G$ we have $T_{ab}^c \in \mathbb{Q}$.*

Proof. Every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_{n\varphi(n)})/\mathbb{Q})$ is of the form $\sigma = \sigma_d$ for a $d \in (\mathbb{Z}/n\varphi(n)\mathbb{Z})^*$, it sends $\omega_{n\varphi(n)}$ to $\omega_{n\varphi(n)}^d$ and hence it sends $\omega_n, \omega_{\varphi(n)}$ to $\omega_n^d, \omega_{\varphi(n)}^d$ respectively. Applying σ_d to T_{ab}^c and using Lemma 4.22 gives

$$\sigma_d(T_{ab}^c) = \left(\frac{\#G}{\varphi(n)}\right)^2 \sum_{\chi,\psi\in G^\perp} \frac{g(\chi^d)g(\psi^d)}{g(\chi^d\psi^d)}\bar{\chi}^d(a)\bar{\psi}^d(b)(\chi\psi)^d(c)\,. \tag{4}$$

Because $\gcd(d,n) = 1$ we have $\{\chi\}_{\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^*}} = \{\chi^d\}_{\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^*}}$ so we see that (4) is just T_{ab}^c. Since d was arbitrary it follows that $T_{ab}^c \in \mathbb{Q}$. □

By the discussion above we have that $T_{ab}^c = N_{ab}^c \in \mathbb{Z}$.

We can estimate N_{ab}^c now by using results from the previous chapter.

Lemma 5.21. *For all $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ and $c \in (\mathbb{Z}/n\mathbb{Z})^*/G$ we have*

$$|N_{ab}^c| \leq \tfrac{2m-1}{m^2} + +n(1-\tfrac{1}{m})^2\,.$$

Proof. Let $m = \frac{\varphi(n)}{\#G}$. If we estimate N_{ab}^c first by the triangle inequality we get

$$|N_{ab}^c| \leq \left(\frac{\#G}{\varphi(n)}\right)^2 \sum_{\chi,\psi\in G^\perp} \frac{|g(\chi)||g(\psi)|}{|g(\chi\psi)|}$$

since characters have absolute value 1. Using Corollary 4.27 we see that

$$|N_{ab}^c| \leq \left(\frac{\#G}{\varphi(n)}\right)^2 \sum_{\chi,\psi\in G^\perp} \sqrt{\frac{f_\chi f_\psi}{f_{\chi\psi}}}\,.$$

Because $f_{\chi_0} = 1$ we see that $\frac{f_\chi f_{\chi_0}}{f_{\chi\chi_0}} = 1$ so together with $1 \leq \frac{f_\chi f_\psi}{f_{\chi\psi}} \leq n^2$ since $1 \leq f_\chi \leq n$ for all $\chi \in G^\perp$ we get

$$|N_{ab}^c| \leq \tfrac{2m-1}{m^2} + n(1-\tfrac{1}{m})^2,\,.$$

□

In the case of $n = p$ a prime number we can say much more since we can calculate exactly some parts of the sum N_{ab}^c. From now on let $n = p$ be a prime number and for convenience define $m = \frac{p-1}{\#G}$ and $\epsilon = \chi_0$ the trivial Dirichlet character modulo p. It turns out that some of the results depend upon $-ba^{-1}$ and other elements being an element of G. For this purpose we define the indicator function $\delta_G(x)$ to be equal to 1 if $x \in G$ and 0 otherwise.

Lemma 5.22. *For $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ and $c \in (\mathbb{Z}/n\mathbb{Z})^*/G$ the sum*

$$S = \frac{1}{m^2} \sum_{\chi,\psi\in G^\perp,\chi\psi=\epsilon} \frac{g(\chi)g(\psi)}{g(\chi\psi)} \overline{\chi}(a)\overline{\psi}(b)$$

equals

$$\frac{p-1}{m^2} - \tfrac{p}{m}\delta_G(-ba^{-1})\,.$$

Proof. Since $g(\epsilon) = -1$ we can rewrite S to

$$m^2 S = -1 - \sum_{\chi\in G^\perp,\chi\neq\epsilon} g(\chi)g(\overline{\chi})\chi(ba^{-1})\,.$$

Because χ is a Dirichlet character modulo p we have by Theorem 4.18 for $\chi \neq \epsilon$ that $g(\chi)g(\overline{\chi}) = p\chi(-1)$ so

$$m^2 S = -1 - p \sum_{\chi \in G^\perp, \chi \neq \epsilon} \chi(-ba^{-1}) \,.$$

Using the orthogonality relations we see that

$$\sum_{\chi \in G^\perp, \chi \neq \epsilon} \chi(-ba^{-1}) = -1 + m\delta_G(-ba^{-1})$$

It follows that

$$S = \frac{p-1}{m^2} - \tfrac{p}{m}\delta_G(-ba^{-1}) \,.$$

□

Using Lemma 5.22 we can simplify the expression for N_{ab}^c to

$$N_{ab}^c + \tfrac{1}{m^2}(1 - p + p\delta_G(-ba^{-1})) = \tfrac{1}{m^2} \sum_{\chi,\psi \in G^\perp, \chi\psi \neq \epsilon} \frac{g(\chi)g(\psi)}{g(\chi\psi)} \bar{\chi}(a)\bar{\psi}(b)(\chi\psi)(c) \,.$$

We can calculate a part of

$$\sum_{\chi,\psi \in G^\perp, \chi\psi \neq \epsilon} \frac{g(\chi)g(\psi)}{g(\chi\psi)} \bar{\chi}(a)\bar{\psi}(b)(\chi\psi)(c)$$

explicitly. So we can refine our estimate.

Lemma 5.23. *For $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ and $c \in (\mathbb{Z}/n\mathbb{Z})^*/G$ the sum*

$$S = \sum_{\chi,\psi \in G^\perp, \psi = \epsilon, \chi \neq \epsilon} \frac{g(\chi)g(\psi)}{g(\chi\psi)} \bar{\chi}(a)\bar{\psi}(b)(\chi\psi)(c)$$

equals

$$1 - m\delta_G(ca^{-1}) \,.$$

Proof. Since $\psi = \epsilon$ (so $g(\psi) = -1$) we can rewrite S to

$$S = -\sum_{\chi \in G^\perp, \chi \neq \epsilon} \chi(ca^{-1})$$

which is equal to $1 - m\delta_G(ca^{-1})$ by the orthogonality relations. □

Using Lemma 5.22, Lemma 5.23 and the symmetric version of Lemma 5.23 we see that we have

$$N_{ab}^c + \tfrac{1}{m^2}(-1-p+m(\delta_G(-ba^{-1})+\delta_G(ca^{-1})+\delta_G(cb^{-1}))$$

equals

$$\tfrac{1}{m^2}\sum_{\chi,\psi\in G^\perp,\chi,\psi,\chi\psi\neq\epsilon}\frac{g(\chi)g(\psi)}{g(\chi\psi)}\overline{\chi}(a)\overline{\chi}(b)(\chi\psi)(c)\,. \tag{5}$$

Using the triangle inequality and the fact that $|g(\chi)| = \sqrt{p}$ for a non-trivial Dirichlet character χ modulo p gives that the absolute value of (5) is smaller of equal to

$$\tfrac{1}{m^2}(m^2-3m+2)\sqrt{p}$$

since we sum over m^2-3m+2 pairs of Dirichlet characters (χ,ψ). This implies that

$$|N_{ab}^c + \tfrac{1}{m^2}(-1-p+m(p\delta_G(-ba^{-1})+\delta_G(ca^{-1})+\delta_G(cb^{-1})))| \leq \tfrac{1}{m^2}(m^2-3m+2)\sqrt{p}\,.$$

Because $\frac{1}{m^2}(m^2-3m+2)\sqrt{p} < \sqrt{p}$ we see that N_{ab}^c is bounded in some way by $\sqrt{p}$. Note also that

$$-\frac{p+1}{m^2} \leq \tfrac{1}{m^2}(-1-p+m(p\delta_G(-ba^{-1})+\delta_G(ca^{-1})+\delta_G(cb^{-1}))) \leq 1$$

5.4 Constructing regular polygons

The ancient Greeks were already interested in which regular n-gons could be constructed using ruler and compass only. They knew that it could be done for $n = 2^k$ with $k \geq 2$ and $n = 2^k \cdot 3$, $2^k \cdot 5$, $2^k \cdot 3 \cdot 5$ for $k \geq 0$. Beyond that they didn't know if there were other constructible regular n-gons but they also couldn't show that these were the only ones. For almost two thousand years no progress was made until Carl Friedrich Gauss proved in 1796 that the regular 17-gon was constructible. Some years later he generalized his method and he proved that a regular n-gon is constructible if and only if it is of the form $n = 2^m$ with $m \geq 2$ and $n = 2^m p_1 \dots p_k$ with p_i different Fermat prime numbers and $m \geq 0$. A Fermat prime number F_n is a prime number of the form $F_n = 2^{2^n}+1$ with $n \in \mathbb{Z}_{\geq 0}$. So far there are only 5 Fermat prime numbers known: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$. The next twenty-eight numbers $F_5, \dots, F_{32}$ are known to be composite. Gauss used the Gaussian periods for proving that the regular 17-gon is constructible.

In this section we will prove that every F_n-gon with F_n a Fermat prime is constructible and we will also give a procedure to do this. We start by introducing some preliminary notation and some lemmas.

Let $p = F_n$ be a Fermat prime with $n \geq 0$. Let $\omega = \omega_p = e^{\frac{2\pi i}{p}}$ be a primitive p^{th} root of unity in $\mathbb{C}$. Our aim is to show first that $\omega + \omega^{-1} = 2\cos(\frac{2\pi}{p})$ is constructible because then we can construct the angle $\frac{2\pi}{p}$. We know that $\mathbb{Z}/p\mathbb{Z}$ is cyclic and in the case of Fermat prime numbers F_n we know by a result of Pépin (1877) an explicit generator if $n \geq 1$.

Lemma 5.24. *For any Fermat prime F_n with $n \geq 1$ we have $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$ hence $\langle 3 \rangle = \mathbb{Z}/F_n\mathbb{Z}$.*

Proof. Because F_n is an odd prime we have by the quadratic reciprocity law

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \equiv \left(\frac{F_n}{3}\right) \equiv \left(\frac{-1}{3}\right) \equiv -1 \mod F_n$$

where we used $F_n \equiv (-1)^{2^n} + 1 \equiv -1 \mod 3$ for $n \geq 1$ in the third congruence. It follows that the order of 3 in $\mathbb{Z}/F_n\mathbb{Z}$ doesn't divide $\frac{F_n-1}{2}$ hence the order must be equal to $F_n - 1$. The result follows. □

We know that $K = \mathbb{Q}(\omega)$ is a Galois extension of degree $p - 1 = 2^{2^n}$ with $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* = \langle 3 \rangle$. For $k = 0, \ldots, 2^n$ define G_{2^k} as the cyclic group $\langle 3^{2^{2^n-k}} \rangle$ of order 2^k then we have the following chain of subgroups $\{1\} = G_1 \leq G_2 \leq G_4 \leq \ldots \leq G_{2^{2^n}} = \langle 3 \rangle$ where $[G_{2m} : G_m] = 2$ for $m = 1, 2, 4, \ldots, 2^{2^n-1}$. Using the Galois correspondence we have the fields $\mathbb{Q} = K_1 \subset K_2 \subset K_4 \subset \ldots \subset K_{2^{2^n}} = \mathbb{Q}(\omega)$ where K_{2^k} is the fix field of $G_{2^{2^n-k}}$ for $k = 0, \ldots, 2^{2^n}$. The degree of the field extension $K_{2^k}/\mathbb{Q}$ is 2^k.
Because $[K_{2k} : K_k] = 2$ for $k = 1, 2, 4, \ldots, 2^{2^n-1}$ the field K_{2k} is a quadratic extension of K_k. Using ruler and compass we can construct the sum, difference, product, quotient and square root of constructible numbers. If we are able to construct an element of K_{2k} by using only elements of K_k for each $k = 1, 2, 4, \ldots, 2^{2^n-1}$ then we can construct $\omega + \omega^{-1}$.

Using Gaussian periods we will give a method to construct the subfields $K_1, K_2, K_4, \ldots, K_{2^{2^n}}$. We know by Lemma 5.12 that $K_{2^m} = \mathbb{Q}(S(G_{2^{2^n-m}}, a))$ for every $a \in (\mathbb{Z}/p\mathbb{Z})^*$. So it is enough to construct the Gaussian periods $S(G_{2^{2^n-1}}), S(G_{2^{2^n-2}}), \ldots, G_1$ inductively. To do this we need the following lemma which tells us what the minimal polynomial of $S(G_{2^k}, a)$ is in $K_{2^{2^n-(k+1)}}[X]$.

Lemma 5.25. *For $k = 0, 1, \ldots, 2^n$ and every $a \in (\mathbb{Z}/p\mathbb{Z})^*$ the minimal polynomial of $S(G_{2^k}, a)$ over $K_{2^{2^n-(k+1)}}$ is given by $f_{2^k}(X) = X^2 - S(G_{2^{k+1}}, a)X + S(G_{2^k}, a)S(G_{2^k}, ab)$ with b an element from $aG_{2^{k+1}} \backslash G_{2^k}$.*

Note that the elements $S(G_k, a)$ and $S(G_k, ab)$ are not elements of K_{2k} but it turns out that their product is. It is in fact a $\mathbb{Z}$-linear combination of the conjugates of $S(G_{2^{k+1}}, 1)$.

Proof. Let $k \in \{0, 1, 2, \ldots, 2^n\}$ be arbitrary and take $a = 1$. We can get the statement in the lemma for arbitrary $a \in (\mathbb{Z}/p\mathbb{Z})^*$ by applying the field automorphism $\sigma_a : \omega \mapsto \omega^a$.
We check first if $S(G_{2^k}, 1)$ is a zero of f_{2^k}. We know $b \in G_{2^{k+1}} \backslash G_{2^k}$ and $[G_{2^{k+1}} : G_{2^k}] = 2$ so $G_{2^k} \cup bG_{2^k} = G_{2^{k+1}}$ which gives the relation $S(G_{2^k}, 1) + S(G_{2^k}, b) = S(G_{2^{k+1}}, 1)$. Now we see easily that

$$f_{2^k}(S(G_{2^k}, 1)) = S(G_{2^k}, 1)(S(G_{2^k}, 1) + S(G_{2^k}, b) - S(G_{2^{k+1}}, 1)) = 0\,.$$

In the same way we can show that $S(G_{2^k}, b)$ is another zero of f_{2^k}. It is a different zero because $b \in G_{2^{k+1}} \backslash G_{2^k}$ and $\{S(G_{2^k}, c)\}_{c \in (\mathbb{Z}/p\mathbb{Z})^*/G_{2^k}}$ is an integral basis for $\mathcal{O}_{K_{2^k}}$. We know that f_{2^k} has two different roots in $K_{2^{2^n-k}}$ so in order to show that f_{2^k} is the minimal polynomial of $S(G_{2^k}, a)$ over $K_{2^{2^n-(k+1)}}$ we need to show that its coefficients lie in $K_{2^{2^n-(k+1)}}$. We obviously have $S(G_{2^{k+1}}, 1) \in K_{2^{2^n-(k+1)}}$ and we can check that $S(G_{2^k}, 1)S(G_{2^k}, b) \in K_{2^{2^n-(k+1)}}$ by using Galois theory as follows.
Let c be an element of $G_{2^{k+1}}$ then $S(G_{2^k}, c) = S(G_{2^k}, c)$ and $S(G_{2^k}, bc) = S(G_{2^k}, b)$ if $c \in G_k$ and $S(G_{2^k}, c) = S(G_{2^k}, b)$ and $S(G_{2^k}, bc) = S(G_{2^k}, 1)$ if $c \notin G_{2^k}$. In both cases we get $\sigma_c(S(G_{2^k}, 1)S(G_{2^k}, b)) = S(G_{2^k}, c)S(G_{2^k}, bc) = S(G_{2^k}, 1)S(G_{2^k}, b)$ where $\sigma_c : \omega \mapsto \omega^c$ is a field automorphism. We see that we have indeed that $S(G_{2^k}, 1)S(G_{2^k}, b) \in K_{2^{2^n-(k+1)}}$. Which concludes the proof. □

As shown in the proof of Lemma 5.25 the product $S(G_{2^k}, 1)S(G_{2^k}, b)$ lies in $K_{2^{2^n-(k+1)}}$ but it also lies in $\mathcal{O}_K$ so the product lies in $\mathcal{O}_K \cap K_{2^{2^n-(k+1)}} = \mathcal{O}_{K_{2^{2^n-(k+1)}}}$ and since $\mathcal{O}_{K_{2^{2^n-(k+1)}}}$ has $\{S(G_{2^{k+1}}, c)\}_{c \in (\mathbb{Z}/p\mathbb{Z})^*/G_{2^{k+1}}}$ as an integral basis it can be written as a unique $\mathbb{Z}$-linear combination of elements from this basis. Because $S(G, a)S(G, b) = \sum_{g \in G} S(G, a + bg)$ we only have to look at $a + bg \mod p$.
If $a + bg$ is always non-zero modulo p then we only have to check in which coset of G in $(\mathbb{Z}/p\mathbb{Z})^*$ the element $a + bg$ lies. If some $a + bg$ is zero modulo p then since $a + bg \equiv 0 \mod p$ if and only if $g \equiv -ab^{-1} \mod p$ there is only one g for which $a + bg$ is zero modulo p. In that case we have

$$S(G, a)S(G, b) = \#G + \sum_{g \in G, g \neq -ab^{-1}} S(G, a + bg)$$

and noting that $-1 = \sum_{g \in (\mathbb{Z}/p\mathbb{Z})^*/G}$ we can find the coefficient in the same way as before.

There are two things we still need to do. We need to find a way to express $S(G,a)$ as a polynomial in $S(G,1)$ for $a \in (\mathbb{Z}/p\mathbb{Z})^*$ and we have to determine which of the two solutions to the minimal polynomial f_{2^k} is which.

Since $K_{2^k} \subset \mathbb{R}$ for $k = 0, 1, \ldots, 2^n$ (note that $\omega_p + \omega_p^{-1} \in \mathbb{R}$) we can approximate $S(G_{2^k}, a)$ by real numbers. In this way we can compare $S(G_{2^k}, a)$ and $S(G_{2^k}, b)$. We have

$$S(G_{2^k}, a) = \sum_{j=1}^{2^k} \omega_p^{a3^{j2^{2^n-k}}} = \sum_{j=1}^{2^{k-1}} \omega_p^{a3^{j2^{2^n-k}}} + \omega_p^{-a3^{j2^{2^n-k}}} = \sum_{j=1}^{2^{k-1}} \cos(\tfrac{2\pi a}{p} 3^{j2^{2^n-k}}) \,. \quad (6)$$

We can therefore perform a numerical approximation of the zeros of f_{2^k} to determine which is which.

We know by Lemma 5.12 that $K_{2^k} = \mathbb{Q}(S(G_{2^k}, 1))$ so the powers of $S(G_{2^k}, 1)$ are a $\mathbb{Q}$-basis of K_{2^k}. Every power of $S(G_{2^k}, 1)$ can be expressed as a $\mathbb{Z}$-linear combination of the elements $S(G_{2^k}, a)$ for $a \in (\mathbb{Z}/p\mathbb{Z})^*/G_{2^k}$ since they form an integral basis of $\mathcal{O}_{K_{2^{2^n-k}}}$. Let $S(G_{2^k}, 1)S(G_{2^k}, x_m) = a_{m1}S(G_{2^k}, x_1) + \ldots + a_{m2^k}S(G_{2^k}, x_{2^k})$ where $x_1, \ldots, x_{2^k}$ are representatives for the cosets of G in $(\mathbb{Z}/p\mathbb{Z})^*/G$ and $1 \leq m \leq 2^k$. This gives us the matrix $A = (a_{ij})_{1 \leq i,j \leq 2^k}$ with $a_{ij} \in \mathbb{Z}$.

Lemma 5.26. *For every $m \geq 1$ the coefficients for $S(G_{2^k}, x_1), \ldots, S(G_{2^k}, x_{2^k})$ when writing $S(G_{2^k}, 1)^m$ as a linear combination of $S(G_{2^k}, x_i)$'s are given by $(A^t)^{m-2}(a_{11}, \ldots, a_{12^k})^t$.*

Proof. This follows easily with induction using that

$$S(G_{2^k}, 1)^m = S(G_{2^k}, 1)S(G_{2^k}, 1)^{m-1} \,.$$

□

The previous lemma gives us the following lemma.

Lemma 5.27. *Let v^t be the second row of the matrix A. Define the matrix B by $B^t = ((A^t)^{-1}v, v, A^t v, \ldots, (A^t)^{2^k} v)$ then B is invertible and*

$$(S(G_{2^k}, 1), S(G_{2^k}, 1)^2, \ldots, S(G_{2^k}, 1)^{2^{2^n-1}})^t = B(S(G_{2^k}, x_1), \ldots, S(G_{2^k}, x_{2^k}))^t \,.$$

Proof. For the first part note that $\{S(G_{2^k}, 1), S(G_{2^k}, 1)^2, \ldots, S(G_{2^k}, 1)^{2^{2^n-1}}\}$ and $\{S(G_{2^k}, x_1), \ldots, S(G_{2^k}, x_{2^k})\}$ are bases of $\mathcal{O}_{K_{2^{2^n-k}}}$ so A is invertible. It is not difficult to check that this implies that B is invertible. The last part comes down to writing out the definitions. □

As a corollary of Lemma 5.27 we see that we only have to invert B to obtain an expressions for $S(G_{2^k}, x_i)$ as a rational polynomial in $S(G_{2^k}, 1)$.

Given a Fermat prime p we can follow the steps below to construct a regular p-gon with ruler and compass only.

- Calculate the groups $G_1, G_2, G_4 \ldots, G_{2^{2^n}}$ and use Lemma 5.25 to calculate the minimal polynomial of $S(G_{2^k}, 1)$ for each $k = 0, 1, \ldots, 2^n$.
- Start with $K_1 = \mathbb{Q}$ and do inductively the following steps:
- Use Lemma 5.27 for every $k \geq 1$ to express the coefficients of f_{2^k} as a rational polynomial in $S(G_{2^{k-1}}, 1)$.
- Construct the coefficients of f_{2^k} and solving the quadratic equation $f_{2^k} = 0$ to construct the zeros of f_{2^k}.
- Use the cosines in (6) to approximate the zeros of f_{2^k} to see which of the two constructed zeros is $S(G_{2^k}, 1)$. When $k < 2^n$ go to the second step, if $k = 2^n$ then the element $\omega_p + \omega_p^{-1}$ is constructed and you're done.

References

[1] *Algebraic Number Theory*. Frazer Jarvis. Springer, 2014

[2] *Number rings*. Peter Stevenhagen. Leiden, 2012.
http://websites.math.leidenuniv.nl/algebra/ant.pdf

[3] *Cyclotomic extensions*. Keith Conrad.
http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/cyclotomic.pdf

[4] *Characters of finite abelian groups (short version)* Keith Conrad.
http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/charthyshort.pdf

[5] *Introduction to Analytic Number Theory*. Tom M. Apostol. Springer-Verlag, 1976