H.W. Verhoek

Class Number Parity of Real Fields of Prime Conductor

Master thesis, defended on March 8, 2006

Thesis advisor: Bart de Smit

Mathematisch Instituut, Universiteit Leiden

Contents

Chapter 1

Introduction

The parity of class numbers has already been studied intensively by various persons. Recently a paper by David Hayes appeared containing some interesting new results [2]. The purpose of the current paper is to write out details and extend some results occuring in the articles of Gras [4] and Hayes [2]. Besides that, I tried to put the entire story in a more algebraic context.

Class number parity results are found for real number fields which are subfields of cyclotomic fields of prime conductor. The main purpose of this paper is to give a practical algorithm to find a piece of the two part of the class number of such a field. Considering the fact that class numbers of cyclotomic fields of prime conductor greater than 67 are as of yet unknown, it is astonishing that the methods of Gras and Hayes give within almost no time 2-divisibility properties of these class numbers up to a million! The resources needed to accomplish this are basic Class Field Theory, the index formula that relates the class number to the index of cyclotomic units in the full unit group and a Theorem from Gras (see [4]).

A brief chronological description follows about the contents of this paper. Chapter two will deal with basic class field theory to obtain three propositions regarding unramified extensions. Three natural sign maps are constructed which will lead later on in a natural way to 2-divisibility properties of the class number. The theory in this chapter is very general and works for all number fields.

In chapter three, cyclotomic units are defined and some structure theorems about cyclotomic units are proved. Cyclotomic units are usefull in the sense that they can be written explicitly without any effort, in contrast to arbitrary units. The setting of this chapter is not as general as the setting of chapter two; the fields to work with are abelian number fields which have prime conductor.

In chapter four, a theorem of Gras is stated and proved which relates the sign maps from chapter two. It can be considered as the most important theorem in this paper, and several subsequent results rely on it.

Chapter five is about parity questions and relations between the parities of the normal class number, relative class number, the 'restricted' class number and the ray class number of conductor four.

Chapter six contains 2-divisibility properties of the class number, and finally chapter seven demonstrates how all the theory gathered so far can be applied. Chapter seven will give various examples and it is discussed how to implement the algorithms into a programming language in the most efficient way.

As a final note, I must say something regarding the notation that is used throughout the paper. In the literature, it is almost a convention that everything associated with the real cyclotomic subfield gets a + in the notation. For example, if ζ is a p-th root of unity, the class number of the maximum real subfield of $\mathbf{Q}(\zeta)$ is denoted by h_p^+ and the unit group of the same field by E^+. This + must remind one that the object is associated to a real subfield because it only makes sense for $\mathbf{R}$. However, this paper is concerned with positive elements, rather than being real. Therefore all + refer to being positive and the classical meaning does not apply!

This paper can be generalized for prime powers, but because of the additional complexity of notation I did not do this.

I'd like to thank Bart de Smit for all the sessions we've spent reviewing, and all his helpful remarks and corrections. David Hayes, who kept me up to date on his own research and gave me some helpful pointers. Hendrik Lenstra (who also came up with the idea for this thesis), Bas Edixhoven, Fabio Mainardi and Martin Lübke for being part of the graduation committee. Peter Stevenhagen for answering some questions and his helpful paper where chapter five is more or less based on. Martijn Feleus for enabling me to speed up my graduation. And last but not least my family, for their support.

Chapter 2

Sign Maps and Unramified Extensions

Let L be an arbitrary number field. For this chapter, let h be the class number of L, and O the ring of integers of L.

2.1 Unramified extensions at infinite primes

Definition 2.1. A real infinite prime of L is a field homomorphism $L \to \mathbf{R}$.

Let R_∞ be the set of real infinite primes of L. If L is Galois over $\mathbf{Q}$ and G its Galois group, a left G-action can be defined on the set of real infinite primes by requiring for $\mathfrak{p} \in R_\infty$, for all $x \in L$ and all $\sigma \in G$ that :

$$\sigma\mathfrak{p}(x) := \mathfrak{p}(\sigma^{-1}x).$$

Definition 2.2. Define for L the **real** sign map from L^* to $\mathbf{F}_2[R_\infty]$ as the map such that for all $x \in L^*$:

$$x \mapsto \sum_{\mathfrak{p} \in R_\infty} (\mathrm{sgn}(\mathfrak{p}x))\mathfrak{p}$$

where sgn is the map $\mathbf{R}^* \to \mathbf{F}_2$ such that negative elements of $\mathbf{R}$ have image 1 and positive elements have image 0.

The map is a $\mathbf{Z}$-linear homomorphism. If L is real and Galois over $\mathbf{Q}$, then sgn_∞ is G-linear with G the Galois group of L, and $\mathbf{F}_2[R_\infty]$ is a free $\mathbf{F}_2[G]$-module of rank 1. More algebraically, the archimedean sign map is equal to

$$\mathrm{sgn}_\infty : L^* \to (L \otimes \mathbf{R})^* \otimes \mathbf{F}_2 \simeq \mathbf{F}_2[R_\infty].$$

The last isomorphism follows by the next Lemma.

Lemma 2.3. *The image of L^* under sgn_∞ is equal to $\mathbf{F}_2[R_\infty]$.*

Proof. The set L^* is a dense subset of $(L \otimes \mathbf{R})$. It is immediate that $\mathrm{sgn}_\infty(L^*)$ is equal to $\mathbf{F}_2[R_\infty]$ because it intersects each connected component of $(L \otimes \mathbf{R})^*$ (the connected components are exactly the open and closed subsets of $(L \otimes \mathbf{R})^*$ having the same sign at the infinite real primes). □

Proposition 2.4. *Let $u \in L^*$. Then $L(\sqrt{u})$ is unramified at all infinite primes if and only if $u \in \ker(sgn_\infty)$.*

Proof. The extension $L(\sqrt{u})$ is unramified at all infinite primes precisely when for each real infinite prime $\mathfrak{p}$ the number $\mathfrak{p}(u)$ is positive. The converse is obvious. □

2.2 Unramified extensions at finite primes

In this section a map will be constructed which is similar to the archimedean sign map from the previous section. However, instead of considering whether an element is positive at an infinite prime, consider if such an element is a square mod 4.

For this entire section make the extra assumption that 2 does not ramify in $L/\mathbf{Q}$.

Lemma 2.5. *Suppose 2 does not ramify in L. Then the order of $(O \otimes \mathbf{F}_2)^* = (O/2O)^*$ is odd. In particular, every element of $(O/2O)^*$ is a square.*

Proof. Suppose $2 = \prod_{i=1}^{a} p_i$ is the prime decomposition of 2 in O. The norm of p_i is $N_{L|\mathbf{Q}}(p_i) = 2^{f_i}$ where f_i is the residue class degree of p_i. Then

$$\#(O/2O)^* = \prod_{i=1}^{a}(N_{K|\mathbf{Q}}(p_i) - 1) = \prod_{i=1}^{a}(2^{f_i} - 1)$$

is odd. The group homomorphism $x \mapsto x^2$ on $(O/2O)^*$ is therefore an isomorphism, hence every element in $(O/2O)^*$ is a square. □

Lemma 2.6. *Suppose 2 does not ramify in L. Define $\iota : 1 + 2(O/4O) \to O/4O$ to be the inclusion map, and $\pi : O/4O \longrightarrow O/2O$ the quotient map. The following sequence is exact and splits:*

$$1 \longrightarrow 1 + 2(O/4O) \xrightarrow{\iota} (O/4O)^* \xrightarrow{\pi} (O/2O)^* \longrightarrow 1$$

Proof. First $\iota(1 + 2(O/4O)) \subset (O/4O)^*$. For let $x = 1 + 2u \in 1 + 2O$. Then $x^2 = 1 + 4u + 4u^2$ shows that the image of x in $O/4O$ is a unit with order 2. Also $\pi((O/4O)^*) = (O/2O)^*$. It is obvious that $\mathrm{im}(\iota) = \ker(\pi)$.

The sequence splits because $1+2(O/4O)$ is the 2-sylow subgroup of $(O/4O)^*$ by Lemma 2.5. □

Lemma 2.7. *Suppose 2 does not ramify in L. Every element of $(O/4O)^* \otimes \mathbf{Z}_2$ is either trivial or has order 2.*

Proof. Tensoring the exact sequence of $\mathbf{Z}$-modules from the Lemma above preserves exactness because $\mathbf{Z}_2$ is torsion free and $\mathbf{Z}$ is principal, and this implies that $\mathbf{Z}_2$ is a flat module (see [7] page 613). Alternatively, it is exact since the sequence splits. Thus:

$$1 \longrightarrow (1 + 2(O/4O)) \otimes \mathbf{Z}_2 \longrightarrow (O/4O)^* \otimes \mathbf{Z}_2 \longrightarrow (O/2O)^* \otimes \mathbf{Z}_2 \longrightarrow 1.$$

Note that taking the tensor product with $\mathbf{Z}_2$ is nothing else than taking the 2-part of the module with which $\mathbf{Z}_2$ is tensored. Then since the order of $(O/2O)^*$ is odd, $(O/2O)^* \otimes \mathbf{Z}_2$ is trivial and $1 + 2(O/4O) \otimes \mathbf{Z}_2$ equals $1 + 2(O/4O)$. Therefore the sequence reduces to

$$1 \longrightarrow 1 + 2(O/4O) \longrightarrow (O/4O)^* \otimes \mathbf{Z}_2 \longrightarrow 1 \longrightarrow 1.$$

and $(O/4O)^* \otimes \mathbf{Z}_2 \simeq 1 + 2(O/4O)$. Every element in $1 + 2(O/4O)$ has order 1 or 2. □

The $\mathbf{Z}$-module $(O/4O)^* \otimes \mathbf{Z}_2$ is an $\mathbf{F}_2$-module since tensoring with $\mathbf{Z}_2$ cleared all elements with odd order, and by the above Lemma every element only remains to have order 2. Further, $(O/4O)^* \otimes \mathbf{Z}_2$ is isomorphic to $O/2O$ because $(O/4O)^* \otimes \mathbf{Z}_2$ is isomorphic to $1 + 2(O/4O)$ and the map that sends $(1 + 2w) \in 1 + 2(O/4O)$ to $w \in O/2O$ is an isomorphism.

If L is Galois over $\mathbf{Q}$ with Galois group G, then $(O/4O)^* \otimes \mathbf{Z}_2$ is an $\mathbf{F}_2[G]$-module and the isomorphism with $O/2O$ is $\mathbf{F}_2[G]$-linear.

Definition 2.8. Denote by $O(2)$ the nonzero elements of O prime to 2.

Definition 2.9. The **2-adic** signature map

$$\mathrm{sgn}_2 : O(2) \to (O/2O)$$

is the composition of $O(2) \to (O/4O)^* \otimes \mathbf{Z}_2$ with the isomorphism described above.

Remark that the kernel of sgn_2 consists of all the squares mod 4. In [4] the 2-adic signature map is constructed in the same way: Let $z \in O(2)$ and let t be the order of z modulo 2, i.e., $z^t \equiv 1 \pmod 2$. The image of z under this signature map is then $\beta \mod 2$ with $\beta \in O$, such that $z^t = 1 + 2\beta$. One can check that any multiple of t also suffices and $\beta \mod 2$ does not depend on t. Therefore the map is well-defined. The following Proposition shows an explicit calculation of a 2-adic image which will be used in chapter four.

Proposition 2.10. *Let $L/\mathbf{Q}$ be an abelian extension unramified at 2 and G the Galois group of this extension. Then for all $z \in O(2)$*

$$sgn_2(z) = \frac{1}{2}(1 - z^{1-2\sigma_{1/2}}),$$

where $\sigma_{1/2}$ is the inverse Frobenius at 2.

Proof. Let σ_2 denote the Frobenius automorphism at 2 of L. Then

$$\sigma_2^{-1}(z)^2 \equiv z \pmod 2.$$

Because $\sigma_2^{-1}(z)^2$ is a square, it is contained in the kernel of the 2-adic signature map, and therefore

$$\mathrm{sgn}_2(z) = \mathrm{sgn}_2(z/\sigma_2^{-1}(z)^2) = \mathrm{sgn}_2(z^{1-2\sigma_{1/2}}).$$

However, $z^{1-2\sigma_{1/2}}$ is of the form $1+2w$ with $w \in O$. It is obvious that the 2-adic image of $1+2w$ is equal to $w \in O/2O$. Therefore $\mathrm{sgn}_2(z) = \frac{1}{2}(1-z^{1-2\sigma_{1/2}})$. □

Lemma 2.11. *Suppose* 2 *does not ramify in* L*. The image of* $O(2)$ *under* sgn_2 *is equal to* $O/2O$*.*

Proof. The map $O(2) \to (O/4O)^* \otimes \mathbf{Z}_2$ is obviously surjective, and the map to compose with to obtain the 2-adic map is an isomorphism. □

The next Lemma can be interpreted as follows: An element $z \in O$ being a square modulo 4 is the $\mathbf{Q}_2$-analog of z being totally positive in $\mathbf{Q}_\infty = \mathbf{R}$.

Proposition 2.12. *Suppose* 2 *does not ramify in* L *and let* E *be the unit group of* L*. Let* $u \in E$*. Then* $L(\sqrt{u})$ *is unramified over* L *at all finite primes if and only if* $u \in \ker(sgn_2)$*.*

Proof. The only primes that can ramify are the primes lying above 2 since the discriminant of the polynomial $X^2 - u$ is the principal ideal generated by 4. By Lemma 2.5 there exists an element $v \in O$ such that $u \equiv v^2 \pmod 2$ in O. Such an element v always exists because u is prime with 2, every element in $(O/2O)^*$ is a square, and such an element can be lifted to a square. Suppose however that $u \not\equiv v^2 \pmod 4$. Let $y = v\sqrt{u^{-1}} - 1 \in L(\sqrt{u})$ and $\overline{y} = -v\sqrt{u^{-1}} - 1 \in L(\sqrt{u})$. Then $y \equiv \overline{y} \pmod 2$. Further let

$$f := (X-y)(X-\overline{y}) = X^2 + 2X - (u^{-1}v^2 - 1)$$

There exists a prime ϕ above 2 such that f is Eisenstein at this prime, otherwise $u \equiv v^2 \pmod 4$ against the assumption. So f is the minimum polynomial of y in the extension $L(\sqrt{u})/L$. Because f is Eisenstein at this prime, this prime is ramified over 2. Suppose $u \equiv v^2 \pmod 4$ holds, i.e., u is a square modulo 4. Consider the polynomial

$$f := (X - \frac{y}{2})(X - \frac{\overline{y}}{2}) = X^2 + X - (u^{-1}v^2 - 1)/4.$$

The element $y/2$ is integral in this case. Remark that $y/2 \not\equiv \overline{y}/2 \pmod 2$, otherwise this would imply $v\sqrt{u^{-1}} \equiv 0 \pmod 2$. Together with $u \equiv v^2 \pmod 2$ this implies $u \equiv v \equiv 0 \pmod 2$, contradiction. For all primes $\phi|2$ in L the polynomial f modulo ϕ has no double roots and therefore the extension is unramified. □

2.3 Totally unramified extensions

Definition 2.13. The **composed** sign map is the direct sum of sgn_∞ and sgn_2:

$$\mathrm{sgn}_{\infty,2} : O(2) \to \mathbf{F}_2[R_\infty] \times (O/2O)$$

such that for all $z \in O(2)$:

$$\mathrm{sgn}_{\infty,2}(z) = \mathrm{sgn}_\infty(z) \times \mathrm{sgn}_2(z).$$

Recall that the archimedean map was defined for all of L^* and the 2-adic map only for $O(2)$ in the most general sense, and the composed map can only be defined on the intersection of these two domains.

The kernel of the composed map is the intersection of the kernels of the archimedean and 2-adic map, and the following Proposition is a simple corollary.

Proposition 2.14. *Let $u \in E$. Then $L(\sqrt{u})$ is totally unramified if and only if $u \in \ker(sgn_{\infty,2})$.*

Proof. Combine the two previous Propositions 2.4 and 2.12. □

2.4 Kummer theory

A Kummer extension is an extension of a number field L for which there is an integer m such that L contains the group of m-th roots of unity μ_m, and the extension is obtained by adjoining m-th roots of elements in L. Let $L^* \supseteq D \supseteq L^{*m}$ and D/L^{*m} finite and $\mu_m \subset L^*$. Then $L_D = L(D^{1/m})$ is a Kummer extension. An abelian extension is of exponent m if its Galois group has exponent m. There is a bijection between finite abelian extensions of exponent m of L and such subsets D (see [7] page 214). Furthermore, there is a pairing between $G_D = \mathrm{Gal}(L_D/L)$ and D as follows: If $\sigma \in G_D$ and $x \in L_D$ such that $x^m \in D$, then $\sigma x/x$ is a m-th root of unity which is independent of x. One can see that G_D is orthogonal to L^{*m} and only the identity in G_D is orthogonal to $D \setminus L^{*m}$. Define a pairing by the following map

$$G_D \times D/L^{*m} \to \mu_m.$$

This gives an isomorphism of G_D to the dual of D/L^{*m} and vice versa (see [7] page 214 for more details).

2.5 Class field 2-divisibility

Let E be the unit group of L. Let $m = 2$ but do not consider the entire set L^{*2}, only the set E^2. The map $E/E^2 \longrightarrow L^*/L^{*2}$ is injective because of $E \cap L^{*2} = E^2$. Define E^+ to be the set consisting of all positive elements of E under all possible embeddings, and E_4 the set consisting of all elements that are

a square modulo 4. Let E_4^+ represents their intersection. The set E_4^+ is exactly the kernel of the composed sign map, i.e.,

$$\ker(E \xrightarrow{\text{sgn}_{\infty,2}} \mathbf{F}_2[R_\infty] \times O/2O) \tag{2.1}$$

Choose the set D from the previous section to be E_4^+. The module E_4^+/E^2 is isomorphic to the dual of the Galois group of the associated extension, and in particular

$$\#(E_4^+/E^2) = [L(\sqrt{E_4^+}) : L].$$

Denote by $\text{Cl}(L)$ the class group of L.

Theorem 2.15. *The* 2*-rank of* E_4^+/E^2 *is a lower bound of the* 2*-rank of* $\text{Cl}(L)$.

Proof. By Class Field Theory, there exists a field extension of L such that the Galois group of this extension is isomorphic to the class group of L. This field over L is called the Hilbert Class Field and is the maximal unramified extension of L at both finite and infinite primes. Therefore, because of Lemma 2.14, the module E_4^+/E^2 can be seen as a subgroup of the 2-torsion group of the dual of $\text{Cl}(L)$, i.e.,

$$E_4^+/E^2 \subseteq \text{Hom}(\text{Cl}(L), \mathbf{Z}/2\mathbf{Z}) =: \text{Cl}(L, \mathbf{Z}/2\mathbf{Z}).$$

□

Chapter 3

Cyclotomic Units

This chapter defines cyclotomic units. The cyclotomic unit group is a very convenient group to work with: its elements are easy to write down explicitly and its algebraic structure is simple as will be seen. Another important property is that the index of the cyclotomic units in the full unit group is finite and equals the class number.

3.1 Fields of prime conductor p

Let p be an odd prime number, g a primitive root of p and ζ a p-th root of unity. Let $\mathcal{K}$ be the maximal real subfield of the p-th cyclotomic field $\mathcal{K}^c := \mathbf{Q}(\zeta)$. Then

$$\mathcal{K} = \mathbf{Q}(\zeta + \zeta^{-1})$$

and $\mathcal{K}$ is of degree $n := \frac{p-1}{2}$ over the rationals. Let $\mathcal{G}$ be the Galois group of $\mathcal{K}/\mathbf{Q}$. The group $\mathcal{G}$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^*/\{\pm 1\}$ and it is generated by an element σ_g defined as follows:

$$\sigma_g(\zeta + \zeta^{-1}) := \zeta^g + \zeta^{g^{-1}}.$$

Let $\mathcal{O}$ denote the ring of integers of $\mathcal{K}$, then $\mathcal{O} = \mathbf{Z}[\zeta + \zeta^{-1}]$ (see [16] page 16).

Let d be a divisor of n, and denote by K the subfield of $\mathcal{K}$ of degree d over $\mathbf{Q}$. This field is unique because the cyclic group $\mathcal{G}$ has a unique subgroup H of index d, and K is the fixed field of this subgroup. The subgroup H is generated by σ_g^d. The Galois group of K over $\mathbf{Q}$ is cyclic of order d and denoted by $G \simeq \mathcal{G}/H$. A basis for K as a vector space over $\mathbf{Q}$ can be obtained by taking Galois invariants with respect to H as follows. Define for $j \in \{0, \ldots, d-1\}$

$$\theta_j := \sum_{i=0}^{(n/d)-1} (\zeta^{g^{j+id}} + \zeta^{g^{-j-id}}) = \mathrm{Tr}_{\mathcal{K}^c/\mathcal{K}} \zeta^{g^j}.$$

The θ_j are called periods and they are invariant under H and $K = \mathbf{Q}(\theta_0)$.

Let O denote the integral closure of $\mathbf{Z}$ in K. Then $O = \mathbf{Z}\theta_0 \oplus \cdots \oplus \mathbf{Z}\theta_{d-1}$ (the traces form a normal $\mathbf{Z}$-basis for O). The ring of integers O is in general not generated by powers of θ_0, see [16] page 17.

3.2 Structure theorems

Let $\mathcal{E}$ denote the multiplicative group of units of $\mathcal{O}$. Since $\mathcal{K}$ has n embeddings into $\mathbf{R}$ and no complex embeddings, Dirichlet's Unit Theorem states:

$$\mathcal{E} \simeq \langle -1 \rangle \times \mathbf{Z}^{n-1}.$$

Every unit in $\mathcal{K}^c$ can be written as a real unit times a root of unity (see [16] page 3, 40), therefore the unit group in $\mathcal{K}^c$ is isomorphic to $W \times \mathcal{E}$, where W is the set of p-th roots of unity of $\mathcal{K}^c$. The only roots of unity in $\mathcal{K}$ are ± 1. Let E be the unit group of K, that is, $E = K \cap \mathcal{E}$. Then E can be written as:

$$E \simeq \langle -1 \rangle \times \mathbf{Z}^{d-1}.$$

Define the cyclotomic units $\mathcal{C}$ of $\mathcal{K}$ as the multiplicative group generated over $\mathbf{Z}$ by

$$\epsilon_a := \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}, \quad a \in \mathbf{F}_p^*.$$

Another set of generators for the cyclotomic units that often arises consists of

$$\epsilon_a{}' = \zeta^{(1-a)/2} \frac{1 - \zeta^a}{1 - \zeta}, \quad a \in \mathbf{F}_p^*.$$

The translation between these definitions is given by the following rule:

$$\sigma_2(\epsilon_a{}') = \epsilon_a$$

with $\sigma_2 \in \mathrm{Gal}(\mathcal{K}/\mathbf{Q})$ the Frobenius at 2.

Note that $\epsilon_1 = 1$ and for all $a, b \in \mathbf{F}_p^*$ it is true that

$$\epsilon_{-a} = -\epsilon_a$$

and

$$\epsilon_{ab} = \sigma_b(\epsilon_a)\epsilon_b.$$

Lemma 3.1. *If $a \in \mathbf{Z}$ is a square modulo p, then $N_{\mathcal{K}|\mathbf{Q}}(\epsilon_a) = 1$, otherwise $N_{\mathcal{K}|\mathbf{Q}}(\epsilon_a) = -1$.*

Proof. Two different proofs follow. Let $i \in \mathbf{Z}$ and make use of the following formula:

$$\epsilon_g^{1+\sigma_g+\cdots+\sigma_g^{i-1}} = \prod_{t=0}^{i-1} \frac{\zeta^{g^{t+1}} - \zeta^{-g^{t+1}}}{\zeta^{g^t} - \zeta^{-g^t}} = \epsilon_{g^i}$$

The norm of ϵ_{g^i} is equal to $\epsilon_g^{i \cdot N}$ with N the norm element of $\mathbf{Z}[\mathcal{G}]$. Use that $N(\epsilon_g) = \epsilon_{g^n} = \epsilon_{-1} = -1$. So $N_{K|Q}(\epsilon_{g^i}) = (-1)^i$, which finishes the first proof.

The other proof is a p-adic one. Write $\epsilon_a = \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}$. Then $\epsilon_a = \zeta^{a-1} + \zeta^{a-3} + \cdots + \zeta^{-a+1}$ by calculation of the power series. Now use that $\zeta \equiv 1 \pmod{1-\zeta}$. It follows that $\epsilon_a \equiv a \pmod{1-\zeta}$ and since the conjugates are also equal to $a \mod 1-\zeta$ one obtains $N_{K|Q}(\epsilon_a) \equiv a^{(p-1)/2} \pmod{1-\zeta}$. □

As a corollary, $N_{\mathcal{K}|\mathbf{Q}}(\epsilon_g) = -1$.

The groups $\mathcal{E}$ and $\mathcal{C}$ are $\mathbf{Z}[G]$-modules. Further $\mathcal{E}/\mathcal{E}^2$ and $\mathcal{C}/\mathcal{C}^2$ are $\mathbf{F}_2[\mathcal{G}]$-modules. They are obviously $\mathcal{G}$-modules, and $\mathbf{Z}/2\mathbf{Z}$-modules by

$$x \cdot \epsilon := \epsilon^x$$

for $\epsilon \in \mathcal{E}$ and $x \in \mathbf{Z}/2\mathbf{Z}$.

Lemma 3.2. *The cyclotomic unit ϵ_g generates $\mathcal{C}$ as a $\mathbf{Z}[\mathcal{G}]$-module.*

Proof. The following identity proves the Lemma:

$$\epsilon_g^{1+\sigma_g+\cdots+\sigma_g^{i-1}} = \prod_{t=0}^{i-1} \frac{\zeta^{g^{t+1}} - \zeta^{-g^{t+1}}}{\zeta^{g^t} - \zeta^{-g^t}} = \epsilon_{g^i}.$$

□

Lemma 3.3. *Let $N_{\mathcal{G}}$ be the norm element of $\mathbf{Z}[\mathcal{G}]$. Then*

$$\mathcal{C} \simeq_{\mathbf{Z}[\mathcal{G}]} \mathbf{Z}[\mathcal{G}]/(2N_{\mathcal{G}}\mathbf{Z}).$$

and the $\mathbf{Z}$-module $\mathcal{C}/\{\pm 1\}$ is freely generated by the set

$$\{\sigma(\epsilon_g) \mid \sigma \in G, \quad \sigma \neq 1\}.$$

Proof. Consider the map $\exp_g : \mathbf{Z}[\mathcal{G}] \longrightarrow \mathcal{C}$ given by $x \mapsto \epsilon_g^x$ for $x \in \mathbf{Z}[\mathcal{G}]$. By Lemma 3.2 this map is surjective. By Lemma 3.1 the kernel of this map contains $2N_{\mathcal{G}}\mathbf{Z}$. It remains to show that the kernel is contained in $2N_{\mathcal{G}}\mathbf{Z}$.

For this consider the map $\exp'_g : \mathbf{Z}[\mathcal{G}] \longrightarrow \mathcal{C}/\{\pm 1\}$. The kernel contains $\mathbf{Z} \cdot N_{\mathcal{G}}$. The map $\exp'_g$ is also surjective, $\mathbf{Z}[\mathcal{G}]$ is a free $\mathbf{Z}$-module of rank n and $\mathcal{C}/\{\pm 1\}$ is a free $\mathbf{Z}$-module of rank $n-1$ by [16] page 145. Therefore the kernel of $\exp'_g$ must be equal to $\mathbf{Z} \cdot N_{\mathcal{G}}$, otherwise $\mathcal{C}/\{\pm 1\}$ would have a lower rank. The kernel of $\exp'_g$ strictly contains the kernel of $\exp_g$, so the kernel of $\exp_g$ must be exactly $2N_{\mathcal{G}}\mathbf{Z}$.

The given set in the Lemma is independent by [16] page 145 (the regulator is non-zero) and ϵ_g is contained in the module generated by this set because by 3.1 (use that $\epsilon_g^{N_{\mathcal{G}}} = -1$):

$$\epsilon_g = -(\epsilon_g^{-\sigma_g} \epsilon_g^{-\sigma_g^2} \ldots \epsilon_g^{-\sigma_g^{n-1}}).$$

□

Let C be the cyclotomic units of K, that is, $C = \mathcal{C} \cap K$. Cyclotomic units of a subfield obtained by intersection are called Washington units. One can also take the norm of the cyclotomic units, those units are called Sinnott units.

Sinnott units are of finite index in the group of Washington units because the Washington Units are included in E, and the index of the Sinnott units in E is finite (see the next section). [1]

Proposition 3.4. *For the field K it is true that the Sinnott units are equal to the Washington units.*

Proof. Let $H = \mathrm{Gal}(\mathcal{K}/K)$. Then $C = \mathcal{C} \cap K = \mathcal{C}^H$. Let N_H be the norm element of $\mathbf{Z}[H]$. It needs to be shown that $(\mathbf{Z}[\mathcal{G}]/2N_{\mathcal{G}}\mathbf{Z})^H = N_H(\mathbf{Z}[\mathcal{G}]/2N_{\mathcal{G}}\mathbf{Z})$. Write $z = \sum_{\sigma\in\mathcal{G}} a_\sigma \sigma \in \mathbf{Z}[\mathcal{G}]$. Suppose that for all $\tau \in H$ there exists a $k \in \mathbf{Z}$ such that $z - \tau z = 2N_{\mathcal{G}}k$. Or,

$$\sum_{\sigma\in\mathcal{G}} (a_{\tau^{-1}\sigma} - a_\sigma) \cdot \sigma = 2k \sum_{\sigma\in\mathcal{G}} \sigma.$$

The lefthand side is zero, therefore $k = 0$. In other words, for all $\tau \in H : a_{\tau^{-1}\sigma} = a_\sigma$. This means that $z \in N_H(\mathbf{Z}[\mathcal{G}])$. So $z \pmod{2N_{\mathcal{G}}\mathbf{Z}} \in N_H(\mathbf{Z}[\mathcal{G}]/2N_{\mathcal{G}}\mathbf{Z})$. □

For $H = \mathrm{Gal}(\mathcal{K}/K)$, note that for all $x \in \mathcal{K}$:

$$x^{N_H} = N_{\mathcal{K}|K}(x).$$

These two norms will be used and mixed at will.

The following Lemma is a generalization of Lemma 3.2:

Lemma 3.5. *The cyclotomic unit $N_{\mathcal{K}|K}(\epsilon_g)$ generates C as a $\mathbf{Z}[G]$-module.*

Proof. This follows by Lemma 3.2 and by the fact that the Sinnott units are equal to the Washington units. □

Lemma 3.6. *Let N_G be the norm element of $\mathbf{Z}[G]$. Then*

$$C \simeq_{\mathbf{Z}[G]} \mathbf{Z}[G]/(2N_G\mathbf{Z}).$$

and the $\mathbf{Z}$-module $C/\{\pm 1\}$ is freely generated by the set

$$\{N_{\mathcal{K}|K}(\sigma_g^i(\epsilon_g)) \mid i \in \{1, \ldots, d-1\}\}.$$

Specifically, it is a free $\mathbf{Z}$-module of rank $d-1$.

Proof. let $H = \mathrm{Gal}(\mathcal{K}/K)$. Note that $\mathbf{Z}[G]/2N_G\mathbf{Z} \simeq N_H(\mathbf{Z}[\mathcal{G}]/2N_{\mathcal{G}}\mathbf{Z})$. Then by the previous Lemma's and Proposition 3.4:

$$C = \mathcal{C}^H = \mathbf{Z}[\mathcal{G}]/2N_{\mathcal{G}}\mathbf{Z})^H \simeq N_H(\mathbf{Z}[\mathcal{G}]/2N_{\mathcal{G}}\mathbf{Z} = \mathbf{Z}[G]/2N_G\mathbf{Z}.$$

[1] That the index is finite is true even for $\mathbf{Z}_p$-extensions, see [6]. However, in the special case of this article, the index is equal to one.

The rest of the Lemma is now also obvious.

An alternative proof of the rest of the Lemma: Since $\mathcal{C}/\{\pm 1\}$ is a free $\mathbf{Z}$-module and $\mathbf{Z}$ is a principal ring, every sub-module of $\mathcal{C}/\{\pm 1\}$ is also free. Therefore $C/\{\pm 1\}$ is also free over $\mathbf{Z}$. Since $C \subset E$ the rank of $C/\{\pm 1\}$ is at most $d-1$. For $j \in \{1, \ldots, d-1\}$ let

$$N_{\mathcal{K}|K}(\sigma_g^j \epsilon_g) = \epsilon_g^{\sigma_g^j + \sigma_g^{j+d} + \cdots + \sigma_g^{(n/d-1)d+j}}.$$

These elements are independent and each element is fixed by $H = \mathrm{Gal}(\mathcal{K}/K)$. Therefore the rank is at least $d-1$. It follows that $C/\{\pm 1\}$ is a free $\mathbf{Z}$-module of rank $d-1$. □

Proposition 3.7. *The $\mathbf{F}_2[G]$-module C/C^2 is G-isomorphic to $\mathbf{F}_2[G]$.*

Proof. By the previous Lemma $C \simeq_{\mathbf{Z}[G]} \mathbf{Z}[G]/2N\mathbf{Z}$. Then also $C^2 \simeq_{\mathbf{Z}[G]} 2\mathbf{Z}[G]/2N_G\mathbf{Z}$ and

$$C/C^2 \simeq_{\mathbf{F}_2[G]} (\mathbf{Z}[G]/2N_G\mathbf{Z})/(2\mathbf{Z}[G]/2N_G\mathbf{Z}) \simeq_{\mathbf{F}_2[G]} \mathbf{Z}[G]/2\mathbf{Z}[G] \simeq_{\mathbf{F}_2[G]} \mathbf{F}_2[G].$$

□

In other words, C/C^2 is free of rank 1 over $\mathbf{F}_2[G]$. It is unknown if the module E/E^2 is always free over $\mathbf{F}_2[G]$. An article of Rene Schoof, [12], contained an incorrect example showing that for $p = 4297$, the module $\mathcal{E}/\mathcal{E}^2$ was not free, see [13].

3.3 Index equation

Denote by h the class number of K. The reason that I consider fields of prime conductor p is given by the following Theorem proved by Hasse and Leopoldt. By the importance of this result it is given its own section.

Theorem 3.8. $h = [E : C]$.

Proof. For a proof see [9] page 88 Theorem 5.3 . □

The proof is based on the analytical class number formula. Although this Theorem implies that the orders of $\mathrm{Cl}(K)$ and E/C are equal, it is not true that in general $\mathrm{Cl}(K) \simeq E/C$. Hayes gives a counterexample of this in the introduction of [2]. Also Washington mentions a counterexample on page 146 of [16].

Chapter 4

A Theorem of Gras

The main result obtained in this chapter is that the archimedean sign map and the 2-adic map are closely related. More precisely, the archimedean and 2-adic sign map are anti-G-linear isomorphic on C/C^2. This feature will be used for computations in chapter seven regarding the 2-part of h.

In this and following chapters the maps from chapter one are released on E and C as subsets of $O(2)$. Also, from now on, the maps $\mathrm{sgn}_\infty, \mathrm{sgn}_2$ and $\mathrm{sgn}_{\infty,2}$ are understood to be defined modulo squares, since squares are always contained in the kernels, and square roots of squares are trivial extensions in the sense of Lemma 2.5 and Lemma 2.13 and therefore give no information at all about the class number. From now on let $\mathrm{sgn}_\infty, \mathrm{sgn}_2$ and $\mathrm{sgn}_{\infty,2}$ act on C/C^2 and E/E^2. If the domain of such a sign function is C/C^2 then write sgn_∞^C, sgn_2^C and $\mathrm{sgn}_{\infty,2}^C$. Else, if the domain is E/E^2 write $\mathrm{sgn}_\infty^E, \mathrm{sgn}_2^E$ and $\mathrm{sgn}_{\infty,2}^E$.

4.1 Archimedean and 2-adic correspondence

Define $\mathfrak{p}_x$ to be the imbedding of $\mathbf{Q}(\zeta) \to \mathbf{C}$ given by $\zeta \mapsto -e^{ix\pi/p}$ for all $x \in \mathbf{F}_p^*$. Let R_∞ be the set of infinite primes belonging to K. Write $\mathfrak{p}_{x|K}$ for the restriction of $\mathfrak{p}_x$ to K. By saying that a map $\phi : M \to N$ with M, N $\mathbf{Z}[G]$-modules is anti-G-linear, I mean that for all $m \in M$ and $g \in G : \phi(gm) = g^{-1}\phi(m)$.

Theorem 4.1. *There exists a unique anti-G-linear automorphism $\rho_1 : C/C^2 \longrightarrow C/C^2$ such that for all $x \in \mathbf{F}_p^*$:*

$$\rho_1(N_{\mathcal{K}/K}(\epsilon_x)) = N_{\mathcal{K}/K}(\epsilon_{1/x}),$$

and a unique anti-G-linear isomorphism $\rho_2 : \mathbf{F}_2[R_\infty] \longrightarrow O/2O$ such that for all $x \in \mathbf{F}_p^*$ and $\mathfrak{p}_{x|K} \in R_\infty$:

$$\rho_2(\mathfrak{p}_x|_K) = Tr_{\mathcal{K}/K}(\zeta^x + \zeta^{-x}),$$

which together make the following diagram commutative:

$$\begin{array}{ccc} C/C^2 & \xrightarrow{sgn_\infty^C} & \mathbf{F}_2[R_\infty] \\ {\scriptstyle \rho_1}\downarrow & & \downarrow{\scriptstyle \rho_2} \\ C/C^2 & \xrightarrow{sgn_2^C} & O/2O \end{array} \tag{4.1}$$

The proof of this result is extracted from [4].

4.2 The case $K = \mathcal{K}$

Lemma 4.2. *There exists a unique anti-$\mathcal{G}$-linear automorphism ρ_1 on $\mathcal{C}/\mathcal{C}^2$ such that for all $a \in \mathbf{F}_p^* : \rho_1(\epsilon_a) = \epsilon_{1/a} = \sigma_{1/a}\epsilon_a$.*

Proof. The group of cyclotomic units can be described as a group having free abelian generators $\epsilon_1, \ldots, \epsilon_{p-1}$ divided by the relations $\epsilon_1 = 1$ and for all $x \in \mathbf{F}_p^* : \epsilon_x = -\epsilon_{-x}$. Therefore the cyclotomic units can be written as $\langle \epsilon_i : i \in \mathbf{F}_p^* \rangle / \langle \epsilon_1 = 1, \epsilon_i = -\epsilon_{-i} \rangle$. The map ρ_1 can be defined on the free abelian group $\langle \epsilon_i : i \in \mathbf{F}_p^* \rangle$, and it respects the relations $\langle \epsilon_1 = 1, \epsilon_i = -\epsilon_{-i} \rangle$ because:

$$\rho_1(\epsilon_1) = \epsilon_{1/1} = 1$$

and

$$\rho_1(\epsilon_a) = \epsilon_{1/a} = -\epsilon_{-1/a} = \rho_1(-\epsilon_{-a}).$$

So ρ_1 is well defined on the quotient group, i.e., the cyclotomic units, and for all $a, b \in \mathbf{F}_p^*$:

$$\rho_1(\epsilon_a \epsilon_b) = \rho_1(\epsilon_a)\rho_1(\epsilon_b)$$

because this is true on the free group $\langle \epsilon_i : i \in \mathbf{F}_p^* \rangle$. So ρ_1 is really a homomorphism and because $\mathcal{C}$ is generated by the various ϵ_a it is an automorphism.

It remains to prove that ρ_1 is anti-$\mathcal{G}$-linear. Using the relation $\epsilon_{ab} = \sigma_a(\epsilon_b)\epsilon_a$ for all $a, b \in \mathbf{F}_p^*$ gives:

$$\rho_1(\sigma_a \epsilon_b) = \rho_1(\epsilon_{ab}\epsilon_a^{-1}) = \epsilon_{1/ab}\epsilon_{1/a}^{-1} = \sigma_{a^{-1}}(\epsilon_{1/b}) = \sigma_a^{-1}\rho_1(\epsilon_b).$$

The map ρ_1 is unique because of the assumption that for all $a \in \mathbf{F}_p^* : \rho_1(\epsilon_a) = \epsilon_{1/a} = \sigma_{1/a}\epsilon_a$ used together with the fact that $\mathcal{C}$ is generated by such elements. □

Let $\mathcal{R}_\infty$ be the set of infinite primes belonging to $\mathcal{K}$. Let $t_a := \zeta^a + \zeta^{-a} \in \mathcal{O}/2\mathcal{O}$ for $a \in \mathbf{F}_p$.

Lemma 4.3. *There exists a unique anti-$\mathcal{G}$-linear isomorphism $\rho_2 : \mathbf{F}_2[\mathcal{R}_\infty] \to \mathcal{O}/2\mathcal{O}$ such that for all $x \in \mathbf{F}_p^*$ and $\mathfrak{p}_{x|\mathcal{K}} \in \mathcal{R}_\infty$:*

$$\rho_2(\mathfrak{p}_{x|\mathcal{K}}) = \zeta^x + \zeta^{-x}.$$

Proof. The following equality holds: $\mathfrak{p}_{x|\mathcal{K}} = \mathfrak{p}_{1|\mathcal{K}}\sigma_x = \sigma_{x^{-1}}\mathfrak{p}_{1|\mathcal{K}}$. The prime $\mathfrak{p}_{1|\mathcal{K}}$ maps to t_1, and $\mathfrak{p}_{x|\mathcal{K}}$ to t_x, so the map ρ_2 is indeed anti-$\mathcal{G}$-linear. It is obviously an isomorphism and uniqueness is clear because of its definition. □

Define a parity function $\delta : \mathbf{F}_p^* \to \mathbf{F}_2$ by demanding that the following diagram is commutative:

$$\begin{array}{ccc} \{1, 2, \ldots, p-1\} & \longrightarrow & \mathbf{Z} \\ \downarrow & & \downarrow \\ \mathbf{F}_p^* & \xrightarrow{\delta} & \mathbf{Z}/2\mathbf{Z} \end{array} \tag{4.2}$$

Note that δ is not a homomorphism. Further note the property that for $z = -e^{i\pi/p}$ and all $x \in \mathbf{F}_p^*$:

$$\mathrm{im}(z^x) > 0 \iff \delta(x) = 0.$$

Let $\mathbf{F}_p^*$ inherite the natural ordering from $\{1, 2, \ldots, p-1\}$. Define for $a \in \mathbf{F}_p^*$ the following sets:

$$\begin{aligned} X_a &:= \{x \in \mathbf{F}_p^* \mid \delta(x/a) \neq \delta(x)\} \\ Y_a &:= \{x \in \mathbf{F}_p^* \mid \delta(x/a) = \delta(x)\} \\ \mathcal{X}_a &:= \{x \in X_a \mid x > a\} \\ \mathcal{Y}_a &:= \{x \in Y_a \mid x < a\}. \end{aligned}$$

It is immediate that :

$$\begin{aligned} X_a \cup Y_a &= \mathbf{F}_p^* \\ X_a \cap Y_a &= \emptyset \\ X_a &= -X_a \\ Y_a &= -Y_a \end{aligned}$$

Lemma 4.4. *Let $a, x \in \mathbf{F}_p^*$ and $\mathfrak{p}_1$ the embedding that maps ζ to $-e^{\pi i/p}$. Then $\mathfrak{p}_x(\epsilon_a) < 0$ if and only if $x \in X_{1/a}$.*

Proof. Note that $\mathfrak{p}_x(\epsilon_a) < 0$ if and only if the images of $\mathfrak{p}_x(\zeta^a)$ and $\mathfrak{p}_x(\zeta)$ lie in two different half spaces of the complex plane seperated by the real line. But this happens if and only if $\delta(x) \neq \delta(ax)$. The last inequality happens if and only if $x \in X_{1/a}$. □

Corollary 4.5.

$$sgn_\infty^{\mathcal{C}}(\epsilon_a) = \sum_{x \in X_{1/a}, x < p/2} \mathfrak{p}_{x|\mathcal{K}} = \sum_{x \in \mathbf{F}_p^*, x < p/2} (\delta(ax) + \delta(x))\mathfrak{p}_{x|\mathcal{K}}$$

Proof. Use Lemma 4.4. □

Lemma 4.6. *For all* $a \in \mathbf{F}_p^*$: $sgn_2^{\mathcal{C}}(\epsilon_a) = \frac{t_a + t_{a-1} + t_1}{t_1 t_a}$.

Proof. First of all, write:

$$\frac{(\zeta^{a/2} - \zeta^{-a/2})^2}{\zeta^a - \zeta^{-a}} = \frac{\zeta^a + \zeta^{-a} + 2}{\zeta^a - \zeta^{-a}} = 1 - 2\frac{1 + \zeta^{-a}}{\zeta^a - \zeta^{-a}}.$$

Then

$$\begin{aligned}
\epsilon_a^{2\sigma_{1/2}-1} &= \frac{\frac{(\zeta^{a/2} - \zeta^{-a/2})^2}{\zeta^a - \zeta^{-a}}}{\frac{(\zeta^{1/2} - \zeta^{-1/2})^2}{\zeta - \zeta^{-1}}} = \frac{1 + 2\frac{1+\zeta^{-a}}{\zeta^a - \zeta^{-a}}}{1 + 2\frac{1+\zeta^{-1}}{\zeta - \zeta^{-1}}} \\
&= (1 + 2\frac{1 + \zeta^{-a}}{\zeta^a - \zeta^{-a}}) \sum_{i=0}^{\infty} (-2\frac{1 + \zeta^{-1}}{\zeta - \zeta^{-1}})^i \equiv (1 + 2\frac{1 + \zeta^{-a}}{\zeta^a - \zeta^{-a}})(1 + 2\frac{1 + \zeta^{-1}}{\zeta - \zeta^{-1}}) \\
&= (1 + 2\frac{1 + \zeta^{-a}}{t_a})(1 + 2\frac{1 + \zeta^{-1}}{t_1}) \equiv 1 + 2\frac{t_a + t_{a-1} + t_1}{t_1 t_a} \pmod 4.
\end{aligned}$$

The 2-adic image is given by $\mathrm{sgn}_2^{\mathcal{C}}(\epsilon_a) = 1/2(1 - \epsilon_a^{2\sigma_{1/2}-1})$ and the Lemma is proved. □

Lemma 4.7. *For all* $a \in \mathbf{F}_p^*$ *for which* $\delta(a) = 1$ *:*

$$\mathcal{X}_a \cup \mathcal{Y}_a = \{a + x \mid x \in X_a\}.$$

Proof. Note that both sets do not contain 0, because $\mathcal{X}_a \cup \mathcal{Y}_a$ has elements in $\mathbf{F}_p^*$, and because if $0 \in \{a+x \mid x \in X_a\}$ this would imply $-a \in X_a$, but $-a \in Y_a$. Therefore $x + a$ must satisfy $p - 1 \geq x + a > a$ or $1 \leq x + a < a$. Suppose that $p - 1 \geq x + a > a$. Then:

$$\delta(1/a(x + a)) + \delta(x + a) \equiv \delta(x/a) + \delta(x) \pmod 2$$

because $\delta(a + x) = \delta(a) + \delta(x)$ since $x + a < p$ and $\delta(x/a + 1) = \delta(x/a) + 1$. This implies that $x + a \in \mathcal{X}_a$ if and only if $x \in X_a$. A priori $x + a$ cannot be in $\mathcal{Y}_a$: all elements in $y \in \mathcal{X}_a \cup \mathcal{Y}_a$ that satisfy $p - 1 \geq y > a$ come from $\mathcal{X}_a$.

On the other hand, suppose that $1 \leq x + a < a$. Then:

$$\delta(1/a(a + x)) + \delta(a + x) \equiv \delta(x/a) + \delta(x) + 1 \pmod 2$$

since $\delta(a + x) = \delta(x) + \delta(a) + 1$ and again $\delta(1/a(a + x)) = \delta(x/a) + 1$. This implies that $x + a \in \mathcal{Y}_a$ if and only if $x \in X_a$. Again all elements $y \in \mathcal{X}_a \cup \mathcal{Y}_a$ that satisfy $a > y \geq 1$ come from $\mathcal{Y}_a$. This proves the Lemma. □

Lemma 4.8. *Let* U *be any subset of* $\mathbf{F}_p^*$ *and* $U^- := \{x \in U, -x \notin U\}$. *Then* $\sum_{x \in U} t_x \equiv \sum_{x \in U^-} t_x \pmod 2$.

Proof. Every element $x \in U \setminus U^-$ is paired with $-x$. Use that $t_x = t_{-x}$. □

Proposition 4.9. *For all* $a \in \mathbf{F}_p^*$: $sgn_2^{\mathcal{C}}(\epsilon_a) = \sum_{x \in X_a} \zeta^x$.

Proof. All ζ should be interpreted as an element of $\mathcal{O}/2\mathcal{O}$. Suppose $\delta(a) = 1$. It suffices to show that

$$t_1 t_a \sum_{x \in X_a} \zeta^x = t_1 + t_{a-1} + t_a \in \mathcal{O}/2\mathcal{O}$$

by Lemma 4.6. Write

$$\begin{aligned} t_a \sum_{x \in X_a} \zeta^x = t_a \sum_{x \in X_a, x < \frac{p}{2}} t_x = \sum_{x \in X_a, x < \frac{p}{2}} t_{a+x} + t_{a-x} \\ = \sum_{x \in X_a} t_{a+x} = \sum_{r \in \mathcal{X}_a \cup \mathcal{Y}_a} t_r. \end{aligned}$$

The last equality is due to Lemma 4.7. If $a < p/2$ then $\mathcal{X}_a^- = \{r \in X_a \mid r > -a\}$. Because if $r \in \mathcal{X}_a$ then $-r \notin \mathcal{X}_a$ is equivalent with $-r \leq a$ since $X_a = -X_a$. Note that $r = -a$ cannot occur because $a \in Y_a$ and also $-a \in Y_a$. On the other hand, $\mathcal{Y}_a^- = \mathcal{Y}_a$. Because if $r \in \mathcal{Y}_a$ then $-r \notin \mathcal{Y}_a$ is equivalent with $-r \geq a$ since $Y_a = -Y_a$. But $r < a < -a$ since $a < p/2$. From $X_a \cup Y_a = \mathbf{F}_p^*$ it follows that $-\mathcal{X}_a^- \cup \mathcal{Y}_a^- = \{1, \ldots, a-1\}$. Applying Lemma 4.8 gives:

$$t_a \sum_{x \in X_a} \zeta^x = t_1 + \cdots + t_{a-1}.$$

Similarly, if $a > p/2$ then $\mathcal{X}_a = \mathcal{X}_a^-$ and $\mathcal{Y}_a^- = \{r \in \mathcal{Y}_a \mid -r \geq a\}$. The union $-\mathcal{X}_a^- \cup \mathcal{Y}_a^-$ equals the set $\{1, \ldots, p-a\}$. Again applying Lemma 4.8 gives:

$$t_a \sum_{x \in X_a} \zeta^x = t_1 + \cdots + t_{p-a}.$$

Note that $\{p-a+1, \ldots, a-1\}$ is invariant under multiplication by -1. Glueing this at the end of the last equation gives the same result as for $a < p/2$:

$$t_a \sum_{x \in X_a} \zeta^x = t_1 + \cdots + t_{a-1}.$$

Multiplying this equality with t_1 telescopes the sum:

$$t_1 t_a \sum_{x \in X_a} \zeta^x = \sum_{r=1}^{a-1} t_{r+1} + t_{r-1} = t_1 + t_{a-1} + t_a$$

which concludes the first case.

Now suppose $\delta(a) = 0$, then look at $-a$ because $\delta(-a) = 1$. It is true that $X_{-a} = Y_a$ since

$$\delta(-x/a) + \delta(x) = \delta(x/a) + \delta(x) + 1.$$

Using that $\sum_{x \in \mathbf{F}_p} \zeta^x = 0$ yields $\sum_{x \in Y_a} \zeta^x = 1 + \sum_{x \in X_a} \zeta^x$. As mentioned before $\epsilon_{-a} = -\epsilon_a$ so

$$\epsilon_{-a}^{2\sigma_{1/2}-1} \equiv -(1 + 2\mathrm{sgn}_2^{\mathcal{C}}(\epsilon_a)) \equiv 1 + 2(1 + \mathrm{sgn}_2^{\mathcal{C}}(\epsilon_a)) \pmod 4.$$

Then $\mathrm{sgn}_2^{\mathcal{C}}(\epsilon_{-a}) = 1 + \mathrm{sgn}_2^{\mathcal{C}}(\epsilon_a)$ and finishes the argument. □

proof of Theorem 4.1 for $K = \mathcal{K}$. Follow the diagram to the right and then down. The first map sends ϵ_a to $\sum_{x \in X_{1/a}, x<p/2} \mathfrak{p}_{x|\mathcal{K}}$. The second map sends this to $\sum_{x \in X_{1/a}, x<p/2} \zeta^x + \zeta^{-x}$. Now take the second route. The map ρ_1 sends ϵ_a to $\epsilon_{1/a}$, which is sent in turn to $\mathrm{sgn}_2^{\mathcal{C}}(\epsilon_{1/a}) = \sum_{x \in X_{1/a}, x<p/2} \zeta^x + \zeta^{-x}$ by proposition 4.9 . Since the ϵ_a generate $\mathcal{C}/\mathcal{C}^2$ the diagram commutes. This finishes the proof of the special case $K = \mathcal{K}$. □

4.3 The general case

proof of Theorem 4.1. The following equalities hold:

$$\begin{aligned} \mathrm{Res}_K(\mathbf{F}_2[\mathcal{R}_\infty]) &= \mathbf{F}_2[R_\infty] \\ N_{\mathcal{K}/K}(\mathcal{C}/\mathcal{C}^2) &= C/C^2 \\ \mathrm{Tr}_{\mathcal{K}/K}(\mathcal{O}/2\mathcal{O}) &= O/2O. \end{aligned}$$

Here Res_K is the restriction map from $\mathcal{K}$ to K. The second equality is due to Proposition 3.4 and the third equality because the prime 2 is unramified in $K/\mathbf{Q}$. Next, for all $x \in \mathcal{C}/\mathcal{C}^2$:

$$\mathrm{sgn}_\infty^{\mathcal{C}}(N_{\mathcal{K}/K}(x)) = \mathrm{Res}_K(\mathrm{sgn}_\infty^{C}(x)),$$

because by Lemma 4.2 the map ρ_1 commutes with the norm $N_{\mathcal{K}/K}$ and therefore the following diagram commutes:

$$\begin{array}{ccc} \mathcal{C}/\mathcal{C}^2 & \xrightarrow{\mathrm{sgn}_\infty^{\mathcal{C}}} & \mathbf{F}_2[\mathcal{R}_\infty] \\ \Big\downarrow{\scriptstyle N_{\mathcal{K}/K}} & & \Big\downarrow{\scriptstyle \mathrm{Res}_K} \\ C/C^2 & \xrightarrow{\mathrm{sgn}_\infty^{C}} & \mathbf{F}_2[R_\infty] \end{array} \tag{4.3}$$

Similarly, because by Lemma 4.3 the map ρ_2 commutes with the trace $\mathrm{Tr}_{\mathcal{K}/K}$

$$\mathrm{sgn}_2^{\mathcal{C}}(N_{\mathcal{K}/K}(x)) = \mathrm{Tr}_{\mathcal{K}/K}(\mathrm{sgn}_2^{\mathcal{C}}(x)) = \mathrm{Res}_K(\mathrm{sgn}_2^{C}(x)).$$

Now apply the norm or trace to every object occuring in the diagram for the case $K = \mathcal{K}$ and the diagram appears for the general case. □

4.4 Different embeddings

To conclude the chapter I will describe the difference between the formulas from Hayes and Gras (or this paper since this paper is based on Gras's notation).

Definition 4.10. Define the map ρ_3 that sends an element $x \in O/2O$ to an element $\tau \in \mathbf{F}_2[G]$ such that $x = \tau \mathrm{Tr}_{\mathcal{K}|K}(\zeta + \zeta^{-1})$.

Hayes embeds $\mathcal{K}^c$ in $\mathbf{C}$ by sending ζ to $e^{2\pi i/p}$ whereas Gras sends it to $-e^{\pi i/p}$. These embeddings are only used in the archimedean sign map as a base view point to which the other embeddings are related, i.e., it only influences the indexing of elements in $\mathbf{F}_p^*$ that belong to embeddings which sent some element in K^* to a negative real number. Note that

$$\sigma_{1/2}e^{2\pi i/p} \equiv -e^{\pi i/p} \pmod 2.$$

Besides that, Hayes uses a different set of generators, namely the ϵ'_a as defined in chapter three. Together with the embedding-independent formula $\epsilon'_g = \sigma_{1/2}\epsilon_g$ this yields

$$\epsilon'_g = \epsilon_g$$

in $\mathbf{R}$. Because of this the image of ϵ'_g under the archimedean sign map appearing in the article of Hayes is the same as the image of ϵ_g under $\rho_3\rho_2\mathrm{sgn}_\infty$. Note that $\rho_3\rho_2\mathrm{sgn}_\infty$ is anti-$\mathcal{G}$-linear just as Hayes' archimedean sign map is.

In Gras's article $\varphi_K = \mathrm{sgn}_2$ is used (image in $O/2O$) for the 2-adic map and S_K for the archimedean map (not the same as sgn_∞). According to Gras

$$\varphi_K(\epsilon_g) = S_K(\sigma_{1/g}\epsilon_g) = S_K(\epsilon_{1/g}^{-1}) = S_K(\epsilon_{1/g}),$$

just like the main theorem (Gras did not state this explicitly but it is not hard to deduce this for the specific prime case). The last equality is true because an element is equal to its multiplicative inverse modulo squares.

The 2-adic sign map also occurs in the article of Hayes, it is denoted by v_2. This map is equal to $\rho_3 \circ \mathrm{sgn}_2$. Since embeddings don't play any role in the 2-adic map the equality $\epsilon'_g = \epsilon_g$ under different embeddings does not hold, but instead $\epsilon'_g = \sigma_{1/2}\epsilon_g$. Because sgn_2 is G-linear:

$$\mathrm{sgn}_2(\epsilon'_g) = \sigma_{1/2} \cdot \mathrm{sgn}_2(\epsilon_g).$$

Hayes states in Theorem 6.1 of [2] the following formula which is the analogue of the commutative diagram occuring in the main theorem:

$$v_2(\epsilon'_g) = v_\infty(\sigma_{2/g}\epsilon'_g)$$

Applying $\mathrm{sgn}_2(\epsilon'_g) = \sigma_{1/2}\mathrm{sgn}_2(\epsilon_g)$ to this gives the same statement from Gras.

From the nature of the archimedean and 2-adic sign maps, the diagram occuring in the main Theorem commutes but there must be two anti-G-linear maps in it. There is a choice of which map should be anti-G-linear: if the archimedean map is chosen to be anti-G-linear like Hayes did, then ρ_2 becomes linear, otherwise the roles are switched like in the diagram of the main Theorem.

Chapter 5

Class Number Parity

In this chapter parity criteria are given. Most of the results are based on Class Field Theory. Some criteria involve the previously constructed sign maps which yield exactly when the sign maps are injective. There are also relations of parities of class numbers given.

5.1 Injectivity of sign maps

Define for K the sets

$$\begin{aligned} E^+ &:= \ker(\mathrm{sgn}_\infty^E) \\ C^+ &:= C \cap E^+ \\ E_4 &:= \ker(\mathrm{sgn}_2^E) \\ E_4^+ &:= E_4 \cap E^+ \\ C_4^+ &:= C_4 \cap C^+. \end{aligned}$$

Let for all $x \in \mathbf{R}$ denote $\lceil x \rceil$ the smallest integer greater than or equal to x.

Proposition 5.1. $2^{\lceil \frac{ord_2 \# C_4^+/C^2}{2} \rceil}$ *divides* h.

Proof. The 2-torsion of (E/C) is isomorphic to

$$(C \cap E^2)/C^2 = (C_4^+ \cap E^2)/C^2 = (C^+ \cap E^2)/C^2 = (C_4 \cap E^2)/C^2.$$

The isomorphism is given by $x \mapsto x^2 \pmod{C^2}$ for $x \in E/C[2]$. Using this gives the following exact sequence:

$$1 \longrightarrow (E/C)[2] \longrightarrow C_4^+/C^2 \longrightarrow E_4^+/E^2.$$

The order of $(E/C)[2]$ divides h and the order of E_4^+/E^2 divides h by Theorem 2.15. This implies that C_4^+/C^2 divides h^2 and proves the Proposition. □

Proposition 5.2. *If $sgn_\infty^C : C/C^2 \longrightarrow R_\infty$ is injective, then h is odd.*

Proof. Follows from

$$1 \longrightarrow (E/C)[2] \longrightarrow C^+/C^2 \longrightarrow E^+/E^2.$$

□

The converse of the proposition is not true. If h is odd, it is not necessarily true that sgn_∞^C is injective. For example, if $p = 29$, then $h_{\max}$, the class number of $\mathcal{K}$, is odd and yet $\mathcal{C}^+/\mathcal{C}^2$ is non-trivial.

Proposition 5.3. *If sgn_2^C is injective, then h is odd.*

Proof. Follows from

$$1 \longrightarrow (E/C)[2] \longrightarrow C_4/C^2 \longrightarrow E_4/E^2.$$

□

Theorem 5.4. *The class number h is odd if and only if $sgn_{\infty,2}^C$ is injective.*

Proof. If $\mathrm{sgn}_{\infty,2}^C$ is injective then h is odd follows from

$$1 \longrightarrow (E/C)[2] \longrightarrow C_4^+/C^2 \longrightarrow E_4^+/E^2.$$

If h is odd, then E_4^+/E^2 is trivial by Theorem 2.15. Then because of the above exact sequence, C_4^+/C^2 is trivial too, or in other words, the map sgn_2^C is injective.

In words: Suppose h is even, then there exists a unit $x \in E$ such that $x^2 \in C$, but $x \notin C$. Then $x^2 \in C_4^+$ and $\mathrm{sgn}_{\infty,2}^C$ is not injective.

Suppose $\mathrm{sgn}_{\infty,2}^C$ is not injective, thus there exists an $x \in C_4^+$ and $x \notin C^2$. Suppose that $x \notin K^{*2}$, then according to Proposition 2.14 the extension $K(x)/K$ is unramified everywhere and h is even. If $x \in K^{*2}$, then it is a square in E, and accordingly $[E : C] = h$ is even, completing the proof. □

Corollary 5.5. *If $\dim(C^+/C^2) > \frac{d}{2}$ then h is even.*

Proof. By Theorem 4.1 it is true that $\dim(C^+/C^2) = \dim(C_4/C^2)$. Therefore C_4^+/C^2 cannot be trivial because the intersection of C^+/C^2 and C_4/C^2 cannot be empty. □

A similar injectivity criterion exists for the 2-adic and archimedean sign map. However, Class Field Theory is needed for this. Let again L be a general number field to work with. A cycle or divisor c is a product

$$c = \prod_v v^{m(v)}$$

where the product ranges over normalized absolute values of L. Further $m(v) \in \mathbf{Z}$ is zero for almost all v and if v is complex then let $m(v) = 0$ and if v is real, then $m(v) \in \{0, 1\}$. Write c_0 for the finite part of c, and c_∞ for the infinite part.

Let X be a subset of L. Denote by $X(c)$ all elements of X coprime with c and denote by X_c all elements α satisfying the following. If $\mathfrak{p}$ is a prime ideal associated to an absolute value occuring in the finite part of c, with multiplicity $i \in \mathbf{N}$, then α satifies:

$$\alpha \equiv 1 \pmod{\mathfrak{p}^i}.$$

If v is a real absolute value occuring in the infinite part of c, then α satifies:

$$v(\alpha) > 0.$$

Let I denote the set of fractional ideals and P the set of principal fractional ideals. Then $I(c)$ is the set of fractional ideals coprime with c, $P(c) = I(c) \cap P$ and P_c is the set of principal fractional ideals having a generator in L_c. The ray class field $\mathcal{H}(L, c)$ of L with cycle c is a field such that

$$\mathrm{Gal}(\mathcal{H}(L, c)/L) \simeq I(c)/P_c = Cl_c(L),$$

where $Cl_c(L)$ is the group of c-ideal classes, or the generalized ideal class group of conductor c.

Using the Chinese Remainder Theorem gives

$$I(c)/P(c) \simeq I/P =: \mathrm{Cl}(L),$$

the classgroup of L.

Let h be the class number of L and $h_c = \#\mathrm{Cl}_c(L)$. The quotient of h_c/h is $[P(c) : P_c]$.

Definition 5.6. The extended Euler totient function φ is the function

$$\varphi : \{\text{cycles}\} \longrightarrow \mathbf{Z}$$

such that for $c \in \{\text{cycles}\}$:

$$\varphi(c) = \varphi'(c_0)2^{\#(c_\infty)}$$

where φ' is the normal Euler totient function and $\#(c_\infty)$ is the number of real infinite primes in c_∞.

For the sake of convenience, define

$$(O/cO)^* := (O/c_0O)^* \cdot \prod_{\mathfrak{p}|c_\infty} \langle -1 \rangle.$$

Then the order of $(O/cO)^*$ is exactly $\varphi(c)$. Let E be the unit group of L.

Proposition 5.7. *The following sequence is exact where the maps are the natural ones:*

$$1 \longrightarrow E_c \longrightarrow E \longrightarrow (O/cO)^* \longrightarrow Cl_c(L) \longrightarrow Cl(L) \longrightarrow 1.$$

In particular,

$$h_c = \frac{h\varphi(c)}{[E : E_c]}.$$

Proof. Use that $P(c)/P_c \simeq L(c)/(EL_c) \simeq (O/cO)^*/\operatorname{im} E$. But $P(c)/P_c$ is exactly the kernel of $Cl_c(L) \longrightarrow \mathrm{Cl}(L)$ and of course $Cl_c(L) \longrightarrow \mathrm{Cl}(L)$ is surjective. The rest of the exactness should be clear.

It remains to show that $h_c = \frac{h\varphi(c)}{[E:E_c]}$. The group $(EL_c)/L_c$ is isomorphic to E/E_c (see [8] page 125-127). The order of $L(c)/L_c$ is easy to compute, it is equal to $\varphi(c)$. Putting this together gives:

$$\#(P(c)/P_c) = \frac{\#(L(c)/L_c)}{\#((EL_c)/L_c)} = \frac{\varphi(c)}{\#((EL_c)/L_c)} = \frac{\varphi(c)}{\#(E/E_c)}.$$

□

For a more detailed survey see [8], page 125-127. Apply this to K for $c = 4$ and $c = \infty = \{\text{set of real infinite primes}\}$. For $c = \infty$ the group $\mathrm{Cl}_\infty(K)$ is also known as the restricted class group of K, and can be written as $\mathrm{Cl}(K)^{\mathrm{res}}$.

Lemma 5.8. *$h^{res} = [\mathbf{F}_2[R_\infty] : sgn^E_\infty(E)] \cdot h$.*

Proof. It must be shown that $\varphi(c)/[E : E_c] = [\mathbf{F}_2[R_\infty] : \mathrm{sgn}^E_\infty(E)]$. But this is evident by the definition of the extended Euler totient function and the definition of the sign map. □

Theorem 5.9. *The map sgn^C_∞ is injective if and only if h^{res} is odd.*

Proof. By the previous Lemma, this is equivalent to sgn^C_∞ is injective if and only if both $\mathbf{F}_2[R_\infty] = \mathrm{sgn}^E_\infty(E)$ (because $\mathbf{F}_2[R_\infty]$ has order a power of two) and h is odd. Suppose sgn^C_∞ is injective, then h is odd as previously. Because $\#C/C^2 = \#\mathbf{F}_2[R_\infty]$ the map sgn^C_∞ is injective if and only if it is surjective. Therefore sgn^C_∞ is surjective, and because h is odd, this implies the surjectivity of sgn^E_∞.

Conversely, suppose h^{res} is odd, thus h is odd and sgn^E_∞ is surjective. Then $[\mathrm{sgn}^E_\infty(E) : \mathrm{sgn}^C_\infty(C)]$ must be odd, because

$$[\mathrm{sgn}^E_\infty(E) : \mathrm{sgn}^C_\infty(C)] \cdot [E^+ : C^+] = [E : C],$$

and $[E : C]$ is odd. On the other hand, this index must be even or equal to one, since $\mathbf{F}_2[R_\infty]$ is of order a power of two. Therefore sgn^C_∞ is surjective, hence injective. □

Lemma 5.10. *The 2-part of h_4 is equal to the 2-part of h times $[(O/2O) : sgn^E_2(E)]$.*

Proof. Choose $c = 4$ and tensor the exact sequence with $\mathbf{Z}_2$ to obtain:

$$E \otimes \mathbf{Z}_2 \longrightarrow (O/4O)^* \otimes \mathbf{Z}_2 \longrightarrow Cl_4(K) \otimes \mathbf{Z}_2 \longrightarrow \mathrm{Cl}(K) \otimes \mathbf{Z}_2 \longrightarrow 1.$$

The first map is exactly the 2-adic signature map on E and the Lemma follows in the same way as the archimedean case. □

Theorem 5.11. *The map sgn^C_2 is injective if and only if h_4 is odd.*

Proof. The proof is entirely analogous to the archimedean case. □

5.2 Parity relations between different class numbers

This section is about parity relations between different class numbers related in some way or another to K.

Theorem 5.12. *Let F_1, F_2 arbitrary number fields, and suppose the extension F_1/F_2 contains no unramified subextensions. Then the norm map from the ideal class group of F_1 to F_2 is onto.*

Proof. See [16] prop. 4.10. □

The field K has a unique totally complex extension field K^c within $\mathcal{K}^c$ of minimal degree over K. For example, if $\frac{n}{d}$ is odd, then K^c is of degree two over K.

Corollary 5.13. *The class number h divides h^c and h divides h_{max}.*

Proof. Apply the above theorem, thus $h^c = h \cdot h^{\text{rel}}$. The number h^{rel} is called the relative class number. Use that p is totally ramified in $\mathcal{K}^c/\mathbf{Q}$. □

Lemma 5.14. *The parities of h^c and h^c/h are equal.*

Proof. If h^c is odd, then trivially h^c/h is odd.

Let K^c be the CM-field of $(K^c)^+$, i.e., the maximal real subfield of K^c. The degree is always $[K^c : (K^c)^+] = 2$. Note that $(K^c)^+$ does not have to be equal to K. The unit groups of $(K^c)^+$ and K^c are equal upto a torsion group, therefore $\text{Cl}((K^c)^+) \longrightarrow \text{Cl}(K^c)$ is injective (see [16], proof of Theorem 4.14, page 40, 41. Although the setting is not entirely the same as here, by minor adjustments it works for the case needed here).

Let $N_{cl} : \text{Cl}(K^c) \longrightarrow \text{Cl}((K^c)^+)$ be the norm map of the class groups. This map respects the equivalence relation for class groups for Galois extensions since the norm of a principal ideal is principal:

$$N_{K^c|(K^c)^+}((x)) = (N_{K^c|(K^c)^+}(x)) \quad , \forall x \in K^c.$$

Also N_{cl} is surjective, see [16] page 400.

The norm of an ideal in K^c in the extension $K^c/(K^c)^+$ is the ideal squared. The square of every ideal in the intersection of $\text{Cl}((K^c)^+)$ and $\ker(N_{cl})$ is trivial. This intersection is well-defined because $\text{Cl}((K^c)^+) \longrightarrow \text{Cl}(K^c)$ is injective. Conversely, every ideal in $(K^c)^+$ whose square is principal is contained in $\ker(N_{cl}) \cap \text{Cl}((K^c)^+)$. Therefore $\ker(N_{cl}) \cap \text{Cl}((K^c)^+)$ is the 2-torsion subgroup of $\text{Cl}((K^c)^+)$.

Now suppose h^c is even and h^c/h is odd. Then also the quotient of h^c by the class number of $(K^c)^+$, which is equal to $\#(\ker(N_{cl}))$ is odd. But then the class number of $(K^c)^+$ must be even. This means that the 2-torsion subgroup of $\text{Cl}((K^c)^+)$ which is equal to $\ker(N_{cl}) \cap \text{Cl}((K^c)^+)$ is non-trivial. Therefore $\#(\ker(N_{cl}))$ must be even, contradiction. To conclude, if h^c/h is odd then h^c is odd. □

Lemma 5.15. *The parities of h^c and h^{res} are equal.*

Proof. By class field theory, there exists a unique finite abelian extension of K, called the restricted Hilbert Class Field $\mathcal{H}^{\text{res}}(K)$, such that the restricted class group of K is isomorphic to the Galois group of the extension $\mathcal{H}^{\text{res}}(K)/K$. The degree of this extension equals the restricted class number h^{res} of K. This field $\mathcal{H}^{\text{res}}(K)$ has the property that it is maximal unramified at all the finite primes. The maximum unramified field, also unramified at infinite primes, is the (normal) Hilbert Class Field, which is contained in $\mathcal{H}^{\text{res}}(K)$. Let α be such that $K^c = K(\alpha)$. Then $\mathcal{H}^{\text{res}}(K)(\alpha)$ is non-real, and therefore $\mathcal{H}^{\text{res}}(K)(\alpha)/K^c$ is unramified at both finite and infinite primes. Therefore $\mathcal{H}^{\text{res}}(K)(\alpha)$ is contained in the Hilbert Class Field of K^c and h^{res} must divide h^c. It follows that if h^{res} is even, h^c must be even.

Conversely, suppose h^c is even. Let F be the subfield of the Hilbert Class Field $\mathcal{H}(K^c)$ such that the degree of F over K^c is the 2-part of h^c, i.e., F is the Hilbert 2-Class Field of K^c. The Hilbert Class Field $\mathcal{H}(K^c)$ is Galois over $\mathbf{Q}$ by the following argument. Let $\bar{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$, and $\sigma \in \bar{\mathbf{Q}}$. Then $\sigma(K^c) = K^c$ since K^c is Galois over $\mathbf{Q}$. Now $\sigma\mathcal{H}(K^c)$ is also the Hilbert Class Field of K^c, therefore $\sigma\mathcal{H}(K^c) = \mathcal{H}(K^c)$. Since $\mathcal{H}(K^c)$ is a finite abelian extension of K^c, every subextension is also Galois over K^c. In particular, F is Galois over K^c. Even stronger, F is Galois over $\mathbf{Q}$: If for $\sigma \in \bar{\mathbf{Q}} : \sigma F \neq F$, then σF is another field containing K^c and contained in $\mathcal{H}(K^c)$ such $[\sigma F : K^c]$ equals the 2-part of h^c. However F is the unique field with this property, therefore $F = \sigma F$. In particular, F is also Galois over K.

Let G_F be the Galois group of F/K and $\mathcal{I} \subset G_F$ be the inertia subgroup associated with the prime ideal $\mathcal{P} \subset K$ extending p.

The subgroup $\mathcal{I}$ is not the entire group G_F because F/K^c is unramified. Because G_F is a 2-group there exists a normal subgroup N of index 2 in G_F by the first Sylow theorem such that N contains $\mathcal{I}$ (see [1] page 44, 45). The fixed field of N is a quadratic extension of K unramified at all finite primes since it is invariant under $\mathcal{I}$, and is therefore contained in the restricted Hilbert Class Field of K. Accordingly h^{res} is even. □

Looking at this result and comparing it with the one for sgn_∞^C, and making use of Gras's Theorem gives the following Corollary.

Corollary 5.16. *The class number h_4 is odd if and only if h^c is odd.*

Proof. Combine Theorem 5.9 and Theorem 5.11 and note that sgn_2^E is surjective if and only if sgn_∞^E is surjective. □

As a final note, it is believed that if n is prime (so $\mathcal{K}$ has no non-trivial subextensions), then $h_{\max}$ is odd. This case is called the Sophie-Germain case, and p is called a Sophie-Germain prime.

Conjecture 5.17. *If n is prime, then h_{max} is odd.*

More generally, would it be true if d is prime, then h is odd?

Chapter 6

Class Number 2-divisibility and Jordan Hölder Factors

This chapter introduces Jordan Hölder factors to find 2-divisibility properties of h. In the first section a basic 2-divisibility property of h will be deduced. Then Jordan Hölder factors will be used more extensively to enhance this result, needed to prove the Theorem stated in the first section. Hayes [2] finds the same 2-divisibility properties, only in a different way.

6.1 2-divisibility results

For a module M over some ring one can consider a chain of submodules ordered by inclusion. Such a chain is called maximal if it is of finite length, has maximal length and contains no repetitions. In a maximal chain each quotient of the consecutive modules is simple, i.e., it has only two submodules, 0 and the quotient module itself. Such a simple module is called a Jordan-Hölder factor of M, from now on JH-factor.

For each prime greater than 2 the JH-factorization of the $\mathbf{F}_2[G]$-module C_4^+/C^2 can be easily computed, see chapter seven.

Definition 6.1. Let M be a module of finite length and $q \in \mathbf{N}$. Define $j_q(M)$ as

$$j_q(M) = \#\{\text{JH-factors of } M \text{ of order } q\}.$$

For all $x \in \mathbf{R}$ the notation $\lceil x \rceil$ means the smallest integer greater than or equal to x.

Theorem 6.2. *Let q be a power of 2. Then the product $\prod_q q^{\lceil \frac{j_q(C_4^+/C^2)}{2} \rceil}$ divides h where the product ranges over all q for which there exists a JH-factor of order q of C_4^+/C^2.*

Note that $\prod_q q^{j_q(C_4^+/C^2)} = \#C_4^+/C^2$. To prove the Theorem a couple of preliminary results are needed.

Lemma 6.3. *Suppose C_4^+/C^2 has a JH-factor of order $q \in \mathbf{N}$. Then q divides the class number h.*

Proof. The exact sequence

$$1 \longrightarrow (E/C)[2] \longrightarrow C_4^+/C^2 \longrightarrow E_4^+/E^2$$

is an exact sequence of $\mathbf{F}_2[G]$-modules, and a JH-factor is simple. The factor module $C_4^+/C^2/((E/C)[2])$ goes injectively to E_4^+/E^2, which shows that each JH-factor must occur either in $(E/C)[2]$ or in E_4^+/E^2. The answer to the first question is therefore affirmative. □

Given two JH-factors of C_4^+/C^2 of orders 2^{q_1} and 2^{q_2}, it is not (in general) true that $2^{q_1+q_2}$ divides h. If this was true, then $\#C_4^+/C^2$ would divide h.

6.2 Counting JH-factors

The main Proposition to be proved in this section where Theorem 6.1 depends on is:

Proposition 6.4. *For all $q \in \mathbf{N}$ the $\mathbf{Z}_2[G]$-modules $(E/C)\otimes\mathbf{Z}_2$ and $Cl(K)\otimes\mathbf{Z}_2$ both have the same number of JH-factors of order 2^q.*

Let G be generated by $\sigma \in G$ and let as usual the order of G be denoted by d. Let l be a divisor of d and let K_l denote the subfield of K of degree l over $\mathbf{Q}$. Append to every object associated to K a subscript l to indicate it belongs to K_l.

Lemma 6.5. *For all divisors l of d :*

$$\#((E_l/C_l)\otimes\mathbf{Z}_2) = \#(Cl(K_l)\otimes\mathbf{Z}_2).$$

Proof. Follows from Theorem 3.8 (see chapter three) and tensoring with $\mathbf{Z}_2$. □

Lemma 6.6. *Let $H_l = Gal(K/K_l)$ such that $\#H_l$ is odd. Then:*

$$(E_l/C_l)\otimes\mathbf{Z}_2 \simeq (E/C)^{H_l}\otimes\mathbf{Z}_2$$
$$Cl(K_l)\otimes\mathbf{Z}_2 \simeq Cl(K)^{H_l}\otimes\mathbf{Z}_2$$

Proof. The unit group E_l is a subgroup of E and C_l is a subgroup of C, and $E_l \cap C = C_l$. The map from left to right is the natural map and E_l/C_l maps injectively to $(E/C)^{H_l}$. Tensoring with $\mathbf{Z}_2$ preserves this.

The inverse map is given by the induced norm map which is left multiplication by $\frac{1}{\#H_l}\sum_{\sigma\in H_l}\sigma$. □

Corollary 6.7. *Let H_l be the subgroup of G with odd order. Then*

$$\#(Cl(K)\otimes\mathbf{Z}_2)^{H_l} = \#((E/C)\otimes\mathbf{Z}_2)^{H_l}$$

Proof. Use Lemma 6.5 and 6.6. □

Definition 6.8. Let G^{odd} be the subgroup of G consisting of all elements of G having odd order and G^{even} the subgroup consisting of elements having even order.

Let $e = \#G^{\text{odd}}$. The ring $\mathbf{Z}_2[G^{\text{odd}}]$ is isomorphic to the polynomial ring $R := \mathbf{Z}_2[X]/(X^e - 1)$ by sending a generator $\sigma \in G^{\text{odd}}$ to X mod $X^e - 1$. Then

$$\mathbf{Z}_2[G^{\text{odd}}] \simeq \prod_{l|e} \mathbf{Z}_2[X]/\phi_l(X) \simeq \prod_{l|e} \mathbf{Z}_2 \otimes \mathbf{Z}[\zeta_l] = \prod_{l|e} \mathbf{Z}_2[\zeta_l],$$

by [7] page 149. Here $\phi_l(X)$ is the l-th cyclotomic polynomial. Define $R_l := \mathbf{Z}_2[\zeta_l] = \mathbf{Z}_2[X]/(\phi_l(X))$. The ring R_l can be considered as an extension of $\mathbf{Z}_2$. R_l is a complete $\mathbf{Z}_2[G^{\text{odd}}]$-algebra with maximal ideals $(2, f)$ where f runs over the irreducible divisors of ϕ_l in $\mathbf{Z}_2[X]$. The residue field or JH-factor belonging to such a maximal ideal is isomorphic to $\mathbf{F}_2[X]/(f)$ and the order of such residue field is therefore equal to $2^{\deg(f)}$.

Now let M be an arbitrary R-module. Then the above implies that M is a product of R_l-modules M_l. The R_l-module M_l can be considered an eigenspace of R_l. Every JH-factor of M comes from exactly one M_l. Furthermore, all JH-factors occuring in M_l are isomorphic to one of the residue fields $\mathbf{F}_2[X]/(f)$, hence have the same order.

Lemma 6.9. *Let H be a subgroup of G^{odd}. Then*

$$M^H = \prod_{l|[G^{odd}:H]} M_l$$

Proof. The module M can be decomposed as described earlier. The only M_l that are invariant under multiplication by a generator of H are the R_l-modules such that l divides $[G^{\text{odd}} : H]$. □

Lemma 6.10. *With G^{odd} and H as above:*

$$\#M_l = \prod_{H \subset G^{odd}, [G^{odd}:H]|l} \#(M^H)^{\mu([G^{odd}:H])}$$

Proof. Take the orders of the left and right side of the formula appearing in Lemma 6.8, and apply the möbius inversion function. □

proof of Proposition 6.4. Every simple $\mathbf{Z}_2[G]$-module is an $\mathbf{F}_2[G]$-module with trivial G^{even} action. The 2-part of $d = \#G$ only determines the multiplicity of JH-factors. There is a bijection between the simple $\mathbf{Z}_2[G]$-modules and the simple $\mathbf{Z}_2[G^{\text{odd}}]$-modules. Therefore the Theorem follows from the special case $G = G^{\text{odd}}$. Suppose $G = G^{\text{odd}}$. Both $E/C \otimes \mathbf{Z}_2$ and $\text{Cl}(K) \otimes \mathbf{Z}_2$ are R-modules, so they can be substituted for M. By Corollary 6.7, for all subgroups H of G:

$$\#(E/C \otimes \mathbf{Z}_2)^H = \#(\text{Cl}(K) \otimes \mathbf{Z}_2)^H.$$

Then from Lemma 6.10 it follows that for all l dividing d:

$$\#(E/C \otimes \mathbf{Z}_2)_l = \#(\mathrm{Cl}(K) \otimes \mathbf{Z}_2)_l.$$

The number of JH-factors of order q in $\mathrm{Cl}(K) \otimes \mathbf{Z}_2$ is

$$\sum_l \log_q(\#(\mathrm{Cl}(K) \otimes \mathbf{Z}_2)_l)$$

where the summation is over all l dividing d such that R_l has residue fields of order q. The same is true for $\#(E/C \otimes \mathbf{Z}_2)$. □

6.3 Dualizing

With the help of Proposition 6.4 and the following two Lemma's it can be seen why the product of the orders of JH-factors in C_4^+/C^2 which have different orders really does divide h.

Lemma 6.11. *Any finite $\mathbf{F}_2[G]$-module M is isomorphic to its dual module $Hom_{\mathbf{F}_2[G]}(M, \mathbf{F}_2[G])$.*

Proof. Write $R := \mathbf{F}_2[G] = \mathbf{F}_2[X]/(X^d - 1)$. The module M is isomorphic to $\oplus_i \mathbf{F}_2[X]/f_i$ as stated in the previous section. It is sufficient to prove the Lemma for one such $\mathbf{F}_2[X]/f_i$ since direct sums can be pulled through the functor Hom. So let $M = \mathbf{F}_2[X]/f_i$. The set $\{x \in R : xf_i = 0\}$ is a principal ideal of R generated by the polynomial $g = \frac{X^d-1}{f_i}$. Now $\mathrm{Hom}_R(M, R) \simeq (g)$ by sending $\phi \in \mathrm{Hom}_R(M, R)$ to $\phi(1)$. But (g) is isomorphic to M. □

Definition 6.12. If S is a JH-factor of a module M, denote by $l_S(M)$ the number of JH-factors contained in M isomorphic to S.

Lemma 6.13. *Let S be a JH-factor of E_4^+/E^2 over the ring $\mathbf{F}_2[G]$. Then $l_S(E_4^+/E^2) \leq l_S(Cl(K) \otimes \mathbf{Z}_2)$.*

Proof. By Theorem 2.15 E_4^+/E^2 is a subgroup of $\mathrm{Hom}_{\mathbf{F}_2}(\mathrm{Cl}(K), \mathbf{F}_2)$. Note that

$$\mathrm{Hom}_{\mathbf{F}_2}(\mathrm{Cl}(K), \mathbf{F}_2) \simeq \mathrm{Hom}_{\mathbf{F}_2[G]}(\mathrm{Cl}(K), \mathbf{F}_2[G]).$$

The latter is JH-isomorphic to its dual, which is isomorphic to $\mathrm{Cl}(K) \otimes \mathbf{F}_2$, and $\mathrm{Cl}(K) \otimes \mathbf{Z}_2$ has the same JH-factors as $\mathrm{Cl}(K) \otimes \mathbf{F}_2$. □

6.4 Putting it together

Now Theorem 6.1 can be proved.

proof of Theorem 6.1. Suppose $j_q(C_4^+/C^2)$ JH-factors of order q appear in C_4^+/C^2. Then at least $\lceil j_q(C_4^+/C^2)/2 \rceil$ must occur either in $(E/C)[2]$ or in E_4^+/E^2 by the argument that $C_4^+/C^2/((E/C)[2])$ is sent injectively in E_4^+/E^2.

Note that for a JH-factor S of $E/C[2] : l_S(E/C[2]) \leq l_S(E/C \otimes \mathbf{Z}_2)$. Then by Proposition 6.4: $j_q(\mathrm{Cl}(K) \otimes \mathbf{Z}_2) = j_q(E/C \otimes \mathbf{Z}_2)$.

On the other hand, for a JH-factor S of $E_4^+/E^2 : l_S(E_4^+/E^2) \leq l_S(\mathrm{Cl}(K) \otimes \mathbf{Z}_2)$ by Lemma 6.13. Apply Proposition 6.4 again as previously. Therefore taking the product for various q still divides h. □

The theory so far made only use of JH-factors with order some power of the prime two. For a more general context in which JH-factors occur, when divisors other than two of the class number are to be determined, see [12].

Chapter 7

Examples and Computations

This chapter gives some examples regarding the theory so far. At the end of the paper, in the Appendix, a table is given with results regarding the 2-divisibility of class numbers of $\mathcal{K}$, which were computed in the same fashion as the examples in this chapter.

7.1 A slightly different environment

The approach of the entire paper to the problem of finding 2-divisibility properties of the class number has been algebraic. In order to do computations it is necessary to be more specific about the signature maps and make a translation to a setting more natural to implement in computer programming languages. Let G be the Galois group of K of order d. Identify $\mathbf{F}_2[G]$ with the cyclic polynomial ring $\mathbf{F}_2[x]/(x^d-1)$ by sending a generator σ_g of G to $x \bmod x^d-1$ and extending by linearity. Throughout this chapter the above identification will be used implicitly for simplicitly without mentioning each time a map.

7.2 Archimedean computations

Definition 7.1. Define the **archimedean sign polynomial** as

$$P_\infty := \gcd(\sum_{t=0}^{n-1}(\delta(g^{t+2})+\delta(g^{t+1}))\cdot x^{n-1-t \bmod d},\ 1-x^d).$$

Because C is generated by $N_{\mathcal{K}|K}(\epsilon_g)$, it is sufficient to only compute this polynomial to obtain the entire image under sgn_∞.

Proposition 7.2. $sgn_\infty(N_{\mathcal{K}|K}(\epsilon_g)) = P_\infty \cdot \mathfrak{p}_{1|K}$

Proof.

$$\begin{aligned}\operatorname{sgn}_\infty(N_{\mathcal{K}|K}(\epsilon_g)) &= \sum_{u\in X_{1/g}, u\leq n} \mathfrak{p}_{u|K} \\ &= \gcd(\sum_{t=0}^{n-1}(\delta(g^{t+1})+\delta(g^t))\cdot\sigma_g^{-t},\ x^d-1)\cdot\mathfrak{p}_{1|K} \\ &= \gcd(\sum_{t=0}^{n-1}(\delta(g^{t+1})+\delta(g^t))\cdot x^{n-t \bmod d},\ x^d-1)\cdot\mathfrak{p}_{1|K} \\ &= \gcd(\sum_{t=0}^{n-1}(\delta(g^{t+2})+\delta(g^{t+1}))\cdot x^{n-1-t \bmod d},\ x^d-1)\cdot\mathfrak{p}_{1|K}\end{aligned}$$

The first and second equalities are due to Corollary 4.5 and by the proof of the general case of Theorem 4.1, the third equality is by the identification. The last equality follows without adjusting the index of the sum because the power of x is defined modulo n. □

In the setting of Coding Theory, P_∞ is called the generator polynomial of the cyclic code C/C^+. It is important however to know the kernel of the sign map, because the kernel gives a criterium about h being odd.

Corollary 7.3. $C^+/C^2 \simeq \mathbf{F}_2[x]/(P_\infty)$

Proof. In the ring $\mathbf{F}_2[x]/(x^d-1)$ the annihilator of (P_∞) is precisely C^+/C^2. □

Corollary 7.4. *If $P_\infty = 1$ then h is odd.*

Proof. If $P_\infty = 1$ then $C^+ = C^2$ by the previous Corollary. Use Corollary 5.2. □

I begin with an example for a small prime such that the calculations can be followed directly.

Example 7.5. Let $p = 3$ and $g = 2$. Then

$$P_\infty = (\delta(2)+\delta(1)) = 1$$

which implies that C^+/C^2 is trivial. Therefore h is odd.

Example 7.6. This example concerns the first prime where $P_\infty \neq 1$ for the maximal field $\mathcal{K}$. Let $p = 29$ and $g = 2$. Then first compute the coefficient of x^{13}. It equals $\delta(4)+\delta(2) \equiv 0 \pmod 2$. Move on to the coefficient for x^{12}, which is also equal to zero modulo 2. Continueing this way to x^0, and summing all subsequent results yields

$$P_\infty = \gcd(x^{10}+x^9+x^6+x^4+x^3+x^2+1, 1-x^{14}) = x^3+x^2+1$$

which implies that $\mathcal{C}^+/\mathcal{C}^2$ is non-trivial. So $h^c_{\max}$ is even but does not tell whether or not $h_{\max}$ is odd.

The next example investigates 2-divisibility properties of the subfield of $\mathcal{K}$ for $p = 29$.

Example 7.7. Again let $p = 29$ and $g = 2$, and look at the subfield of $\mathcal{K}$ of degree d. Then for $d = 2$ the gcd of $1 - x^2$ and $x^{10} + x^9 + x^6 + x^4 + x^3 + x^2 + 1$ is trivial, so h is odd for $d = 2$. For $d = 7$ it is non-trivial and equals $x^3 + x^2 + 1$. In this case nothing can be said again whether or not h is odd, only that h^c is even. Note however that for $p = 29$ all the 2-divisibility that can be calculated from the methods in this paper occurs already in this subfield.

7.3 2-adic computations

To compute the 2-adic image of the generating element ϵ_g, use Gras's Theorem from chapter four. Or more explicitly, Proposition 4.9 which gives the image. For any polynomial f, denote by $\overline{f}$ its reciprocal polynomial.

Proposition 7.8. *$sgn_\infty(N_{\mathcal{K}|K}(\epsilon_g)) = \overline{P_\infty} \cdot \sigma_2 \cdot Tr_{\mathcal{K}|K}(t_1)$ with $\sigma_2 \in G$.*

Proof.

$$\begin{aligned}
\mathrm{sgn}_2(N_{\mathcal{K}|K}(\epsilon_g)) &= \mathrm{Tr}_{\mathcal{K}|K}\Big(\sum_{u \in X_g, u \le n} t_u\Big) \\
&= \Big(\sum_{u \in X_g, u \le n} \sigma_u\Big) \cdot \mathrm{Tr}_{\mathcal{K}|K}(t_1) \\
&= \gcd\Big(\sum_{t=0}^{n-1} (\delta(g^{t-1}) + \delta(g^t)) \cdot x^{t \bmod d},\ 1 - x^d\Big) \cdot \mathrm{Tr}_{\mathcal{K}|K}(t_1) \\
&= \gcd\Big(\sum_{t=0}^{n-1} (\delta(g^{t+1}) + \delta(g^{t+2})) \cdot x^{t+2 \bmod d},\ 1 - x^d\Big) \cdot \mathrm{Tr}_{\mathcal{K}|K}(t_1). \\
&= \gcd\Big(\sum_{t=0}^{n-1} (\delta(g^{t+1}) + \delta(g^{t+2})) \cdot x^{t \bmod d},\ 1 - x^d\Big) \cdot \sigma_2 \cdot \mathrm{Tr}_{\mathcal{K}|K}(t_1).
\end{aligned}$$

The first equality is due to Proposition 4.9. The polynomial P_∞ is equal to

$$\gcd\Big(\sum_{t=0}^{n-1} (\delta(g^{t+2}) + \delta(g^{t+1})) \cdot x^{n-1-t \bmod d},\ 1 - x^d\Big).$$

Now note that the reciprocal polynomial of

$$\sum_{t=0}^{n-1} (\delta(g^{t+1}) + \delta(g^{t+2})) \cdot x^{t \bmod d}$$

is exactly

$$\sum_{t=0}^{n-1} (\delta(g^{t+2}) + \delta(g^{t+1})) \cdot x^{n-1-t \bmod d}.$$

Because $1 - x^d$ is its own reciprocal polynomial, taking the gcd of respectively

$$\sum_{t=0}^{n-1}(\delta(g^{t+1}) + \delta(g^{t+2})) \cdot x^{t \bmod d}$$

and

$$\sum_{t=0}^{n-1}(\delta(g^{t+2}) + \delta(g^{t+1})) \cdot x^{n-1-t \bmod d}$$

with $1 - x^d$ preserves this property. For every irreducible factor occuring in

$$\sum_{t=0}^{n-1}(\delta(g^{t+1}) + \delta(g^{t+2})) \cdot x^{t \bmod d}$$

its reciprocal occurs in

$$\sum_{t=0}^{n-1}(\delta(g^{t+2}) + \delta(g^{t+1})) \cdot x^{n-1-t \bmod d}.$$

If this factor divides $1 - x^d$, then so does its reciprocal. □

The polynomial $\overline{P_\infty}$ will be referred to as the 2-adic polynomial for obvious reasons. What happened is that by choosing a more convenient basis element, namely $\sigma_2 \mathrm{Tr}_{\mathcal{K}|K}(t_1)$, the convenient property arises that the archimedean polynomial and the 2-adic one are each other's reciprocal. Of course this is just a reflection of Gras's Theorem.

Corollary 7.9. $C_4/C^2 \simeq \mathbf{F}_2[x]/(\overline{P_\infty})$

Proof. Similar to the archimedean case. □

Corollary 7.10. *If* $\overline{P_\infty} = 1$ *then* h *is odd.*

Proof. Similar to the archimedean case. □

No examples are worked out for the 2-adic case, since they are the same as for the archimedean case. Once the 2-adic sign polynomials are known, similar conclusions can be deduced regarding h_4 as were deduced regarding h^c for the archimedean case.

7.4 Combined computations

The combined sign map was defined as the direct product of the archimedean and 2-adic maps,

$$\mathrm{sgn}_{\infty,2} = \mathrm{sgn}_\infty \times \mathrm{sgn}_2.$$

Definition 7.11. Define the combined sign polynomial as

$$P_{2,\infty} := \gcd(P_\infty, \overline{P_\infty}).$$

It might seem odd to take the gcd here and not the direct product, but the next proposition explains this.

Proposition 7.12. $C_4^+/C^2 \simeq \mathbf{F}_2[x]/(P_{2,\infty})$.

Proof. When trying to assiociate a polynomial to combined map, remember that the module of interest is C_4^+/C^2, the intersection of C_4/C^2 and C^+/C^2. Therefore the kernels of sgn_∞ and sgn_2 should be intersected, which means taking the dual of the gcd of P_∞ and P_2 in $\mathbf{F}_2[x]/(x^d - 1)$. □

Corollary 7.13. *The class number h is odd if and only if $P_{2,\infty} = 1$.*

Proof. If $P_{2,\infty} = 1$ then $C_4^+ = C^2$. Now use Theorem 5.4 . □

Example 7.14. Reconsider the example where $p = 29$ and $g = 2$ with $K = \mathcal{K}$. The archimedean map alone could not conclude if $h_{\max}$ is odd or not. The reciprocal polynomial p of P_∞ is $x^3 + x + 1$. Computing the gcd of the archimedean polynomial yields that the combined polynomial is trivial. Therefore $h_{\max}$ is odd.

Example 7.15. As it turns out, the first prime number for which $P_{2,\infty}$ is nontrivial for $K = \mathcal{K}$ is 163. For $p = 163$ the combined polynomial is $x^2 + x + 1$. Therefore $h_{\max}$ is even.

7.5 Jordan Hölder computations

Factor the polynomial $P_{2,\infty}$ into irreducible polynomials. Each such irreducible polynomial corresponds exactly to a JH-factor of C_4^+/C^2. The degree of the polynomial factor is the dimension of a JH-factor occuring in C_4^+/C^2.

Algorithm 7.16. *To compute a lower boundary of the 2-divisibility of a class number of a field of prime conductor, and to find the parity of the class number, do the following:*

1. *Compute the archimedean sign polynomial P_∞.*
2. *Compute the gcd of P_∞ and of $\overline{P_\infty}$ to obtain $P_{2,\infty}$.*
3. *If $P_{2,\infty} = 1$ then h is odd and the algorithm stops, otherwise it is even.*
4. *Sort the irreducible factors of degree a together. Let $q = 2^a$. If there are m such factors the number $q^{\lceil m/2 \rceil}$ divides h.*
5. *Multiply all numbers of the previous with each other. The result divides h.*

In practice the combined sign polynomial turns out to be rather small, and the computation of the gcd of P_∞ and $1-x^d$ is by far the most time-consuming. The following alternative algorithm uses the knowledge one has about $1-x^d$.

Algorithm 7.17 (alternative). *To compute a lower boundary of the 2-divisibility of a class number of a field of prime conductor, and to find the parity of the class number, do the following:*

1. *Factor* $1-x^d = \prod_{l|d} \phi_l(x) = \prod_{l|d}(\prod_{f_l} f_l(x))$ *into irreducible polynomials.*
2. *Collect the same irreducible polynomials together, and set the multiplicity of them to* m_l.
3. *Compute the archimedean sign polynomial* $v = P_\infty$.
4. *Divide* v *by a distinct irreducible polynomial* f_l.
5. *If* f_l *divides* v, *set* $v = v/f_l$. *Otherwise go back to the previous step and choose a new different polynomial and which isn't a reciprocal of a polynomial already tried. If there are no more such polynomials goto step 7.*
6. *If* $\overline{f_l} = f_l$ *then* f_l *corresponds to the JH-factor* $/FF_2[X]/(f_l)$ *of* C_4^+/C^2. *Go back to step the previous step and repeat at most* $\lceil m_l/2-1 \rceil$ *times. Else if* $\overline{f_l}$ *divides* v, *set* $v = v/\overline{f_l}$, *and both* f_l *and* $\overline{f_l}$ *correspond to JH-factors of* C_4^+/C^2. *Go back to the previous step and repeat at most* m_l *times. If* $\overline{f_l}$ *doesn't divide* v *then go back to step 3 and choose a new different polynomial which isn't a reciprocal of a polynomial already tried. If there are no more such polynomials goto step 7.*
7. *Sort the JH-factors of the same order a together. Let* $q = 2^a$. *If there are* m *such factors the number* $q^{\lceil m/2 \rceil}$ *divides* h.
8. *Multiply all numbers of the previous with each other. The result divides* h.

The above algorithm can be modified so that it becomes faster but unfortunately an uncertainty slips into it additionally. For large d only the irreducible polynomials of the first few cyclotomic divisors of $1-x^d$ can be used. Of course it must be faster because fewer things are calculated, but there might be bigger JH-factors 'out there' which are skipped. Therefore, if there are no JH-factors found, the conclusion that h is odd cannot be made and the algorithm loses its conclusiveness.

It must be noted however, that from the tables provided by Hayes and my own computations, only small JH-factors seem to occur, not larger than ones dividing $1-x^{31}$ for primes up to a million. See [12] for probabilities of the occurence of big JH-factors.

Example 7.18. Let $p = 277$. Then $P_{2,\infty} = (x^2+x+1)^2$. Then $h_{\max}$ is at least divisible by $2^{2*2/2} = 4$.

Example 7.19. Let $p = 32371$. Then $P_{2,\infty} = x^6 + x^4 + x^3 + x^2 + 1 = (x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$. Then $h_{\max}$ is at least divisible by $2^4 * 2^2 = 64$.

Example 7.20. Let $p = 63337$ and $g = 5$. Then

$$P_{2,\infty} = (x^2 + x^1 + 1)^3 * (x^3 + x^1 + 1)^2.$$

Therefore $h_{\max}$ is divisible by $4^2 * 8 = 128$.

Example 7.21. Take the same p and g as in the previous example. Let $d = 7$, then

$$P_{2,\infty} = \gcd((x^2 + x^1 + 1)^3 * (x^3 + x^1 + 1)^2, 1 - x^7) = (x^3 + x^2 + 1)^2.$$

By this h is divisible by 8.

Chapter 8

Appendix

8.1 Example source code

I wrote a program in C++ that calculates the polynomials $P_{2,\infty}$ for $K = \mathcal{K}$ and p in some given range using the alternative algorithm. Before the computation starts, a list is made of all irreducible polynomials dividing some cyclotomic polynomials up to a given bound.

```
#include <cmath>
#include <iostream>
#include <sstream>
#include <vector>
#include <algorithm>
#include <fstream>
#include <string>
#include <pari.h>
#include <errno.h>

using namespace std;

class pol {
  public:
    vector<int> coeff;
    vector<pol> factor;

    pol();
    ~pol();
    void clean();
    pol gcd(const pol &);
    pol operator+(const pol &);
    pol &operator=(const pol &);
    bool operator==(const pol &);
```

```
    int deg() const;
    pol shift(int);
    pol quotient(const pol &);
    bool divides(const pol &);
    string print() const;
    pol reverse();
    int cl2 ();
    void add_coeff (int);
  private:
};


vector<pol> cyc[200];
vector<long int> cycm[200]; // multiplicity

pol::pol () {}
pol::~pol () {}

void pol::clean() {
  coeff.erase(coeff.begin(),coeff.end());
  factor.erase(factor.begin(),factor.end());
}

pol pol::reverse () {
  int max;
  pol r;

  max=coeff[coeff.size()-1];
  for (int i=coeff.size()-1;i>-1;i--) {
    r.coeff.push_back(max-coeff[i]);
  }

  return r;
}

pol pol::quotient(const pol &f) {
    pol a, b, q;
    int diff;
vector<int> qcoeff;

    if (deg() < f.deg()) { return q; }

    a=*this;
    b=f;

    do {
```

```
      diff=a.deg() - b.deg();
      qcoeff.push_back(diff);
      a=a+b.shift(diff);
    } while (a.deg() >= b.deg());

    if (a.deg() == -1) {
        // q is sorted
for (int i=qcoeff.size()-1;i>-1;i--) {
q.coeff.push_back(qcoeff[i]);
}
      return q;
    }
    q.clean();
    return q;
}

bool pol::divides (const pol &f) {
  pol a, b, q;
  if (deg() < f.deg()) { return 0; }

  a=*this;
  b=f;

  do {
    a=a+b.shift(a.deg() - b.deg());
  } while (a.deg() >= b.deg());

  return (a.deg() && -1);
}

int pol::cl2 () {
  vector<pol> tmp;
  bool skip;
  int mul, q, h=1;

  for (unsigned int i=0;i<factor.size();i++) {
    skip=0;
    mul=1;
    q=1;
    for (unsigned int j=0;j<tmp.size();j++) {
      if ( tmp[j].deg() == factor[i].deg() ) { skip=1;break; }
    }
    if (skip) { continue; }

    for (unsigned int j=i+1;j<factor.size();j++) {
      if (factor[j].deg() == factor[i].deg()) { mul++; }
```

```
    }
    for (int k=0;k<factor[i].deg();k++) {
      q=2*q;
    }
    for (int k=0;k<(mul+1)/2;k++) {
      h=q*h;
    }
    tmp.push_back(factor[i]);
  }
  return h;
}


string pol::print () const {
  if (!coeff.size()) { return "0"; }

  string res;
  ostringstream ostr;

  for (int i=coeff.size()-1;i>-1;i--) {
    ostr.str("");
    ostr.clear();
    if (i==0) {
      if (!coeff[0]) {
        res+="1";
      } else {
        ostr << coeff[i];
        res+="x^" + ostr.str();
      }
    } else {
      ostr << coeff[i];
      res+="x^" + ostr.str() + "+";
    }
  }
  return res;
}

int pol::deg () const {
  if (!coeff.size()) { return -1; }
  //pol is sorted
  return coeff[coeff.size()-1];
}

bool pol::operator==(const pol &f) {
  if (this == &f) { return 1; }
```

```
  if (this->coeff.size() != f.coeff.size()) { return 0; }

  for (unsigned int i=0;i<this->coeff.size();i++) {
    if (this->coeff[i] != f.coeff[i]) { return 0; }
  }

  return 1;
}

pol& pol::operator=(const pol &f) {
  if (this != &f) {
    clean();
    coeff=f.coeff;
    factor=f.factor;
  }
  return *this;
}

void pol::add_coeff (int i) {
  pol n;
  n.coeff.push_back(i);
  // inefficient
  *this=*this+n;
}

pol pol::operator+(const pol &f) {
  int imax,jmax;

  imax=coeff.size();
  jmax=f.coeff.size();

  if (!imax) {
    return f;
  } else if (!jmax) {
    return *this;
  }

  int i=0,j=0;

  pol sum;

  while (j < jmax && i < imax) {
    if (coeff[i] < f.coeff[j]) {
      sum.coeff.push_back(coeff[i]);
      i++;
    } else if (coeff[i] > f.coeff[j]) {
```

```
      sum.coeff.push_back(f.coeff[j]);
      j++;
    } else {
      i++;
      j++;
    }
  }

  if (i==imax) {
    for (i=j;i<jmax;i++) {
      sum.coeff.push_back(f.coeff[i]);
    }
  } else if (j==jmax) {
    for (j=i;j<imax;j++) {
      sum.coeff.push_back(coeff[j]);
    }
  }

  return sum;
}

pol pol::shift(int t) {
  pol r;

  for (unsigned int i=0;i<coeff.size();i++) {
    r.coeff.push_back(coeff[i]+t);
  }
  return r;
}

pol pol::gcd (const pol &f) {
  pol a,b,r,q;
  int diff;
  int count=0;

  if (deg() > f.deg()) {
    a=*this;
    b=f;
  } else {
    a=f;
    b=*this;
  }

  do {
    r=a;
    do {
```

```
      a=r;
      diff=a.deg() - b.deg();
      r=a+b.shift(diff);
    } while (r.deg() >= b.deg());
    a=b;
    b=r;
    count++;
  } while (r.deg() > -1);
  return a;
}

int findmaxm(int n, int acc, pol f)
{
  int m=0;
  for (int i=0;i< acc && i<n;i++) {
if ( n % (i+1) ) continue;
for (unsigned int j=0;j<cyc[i].size();j++) {
  if ( f == cyc[i][j] ) { m++; }
}
  }
  return m;
}

void calculate (int p, int acc) {
  int a, g1, g2, g;
  pol r_pol, v, q;
  vector<pol> skippol;
  int h;
  bool skip;
  int maxmul;

  g=itos(lift(gener(stoi(long(p)))));
  int n=(p-1)/2;
  for (int i=0;i<n;i++) {
    g1=g2=1;
    for (a=1;a<=(n-1-i)+1;a++) {g1=(g1*g) % p;}
    for (a=1;a<=(n-1-i)+2;a++) {g2=(g2*g) % p;}
    if ((g1+g2) % 2) {  v.coeff.push_back(i); }
  }
  pol vtmp=v, testpol;

  for (int i=0;i<acc && i < n;i++) {
if ( n % (i+1) ) { continue; }
for (unsigned int j=0;j<(cyc[i]).size();j++) { //cyc[i][j] are distinct
skip=0;
for (unsigned int k=0;!skip && k<skippol.size();k++) {
```

```
if ( skippol[k] == cyc[i][j] || skippol[k] == cyc[i][j].reverse()) { skip = 1; }
}
if (skip) { continue; }
    testpol=vtmp.quotient(cyc[i][j]);

maxmul = findmaxm(n, acc, cyc[i][j]);
// loop for multiplicity, check for maximum multiplicity occuring in 1-x^n
for (int k=0;k < maxmul && testpol.deg() != -1;k++) {
vtmp=testpol;
if (cyc[i][j] == cyc[i][j].reverse()) {
v.factor.push_back(cyc[i][j]);
testpol=vtmp.quotient(cyc[i][j]);
} else {
testpol=vtmp.quotient(cyc[i][j].reverse());
if (testpol.deg() != -1) {
v.factor.push_back(cyc[i][j]);
v.factor.push_back(cyc[i][j].reverse());
vtmp=testpol;
testpol=vtmp.quotient(cyc[i][j]);
}
}
}
skippol.push_back(cyc[i][j]);
skippol.push_back((cyc[i][j]).reverse());
}
  } //for

  if (v.factor.size() > 0) {
cout << "\x1b[31m" << p << "\x1b[0m " << flush;
ofstream ff("data",ios::app);
if (!ff) {
perror("error opening file");
exit(1);
}
ff << p << " " ;
  for (unsigned int j=0;j<v.factor.size();j++) {
    ff << "(" << v.factor[j].print() << ")";
    if (j != v.factor.size()-1) {
ff << "*";
    }
  }
h = v.cl2();
ff <<  " " <<  h << endl;
ff.close();
  } else {
cout << p << " " << flush;
```

```
  }
}

//compute list of cyclotomic polynomials
void generate_cyc_vec(int n) {
  pol f;
  GEN g, gf, gfl;

  for (int i=1;i<=n;i++) {
    g=cyclo(i,-1);
    gf=factmod(g,stoi(long(2)));

    GEN primes = (GEN)gf[1];
    GEN exponents=(GEN)gf[2];
//all primes are necessarily different by pari
    for (long j=1;j<lg(primes);j++) {
f.clean();
gfl = lift((GEN) primes[j]);

for (int k=0;k<=degree(g);k++) {
   if (itos(polcoeff0(gfl,k,-1)) % 2) { f.coeff.push_back(k); }
}
(cyc[i-1]).push_back(f);
(cycm[i-1]).push_back(itos((GEN)exponents[j]));
    }
  }
}


int main (int argc, char *argv[]) {
  int p, maxp;
string acc_string;
int acc;

  if (argc != 4) {
    cout << "usage: cl2 <startprime> <endprime> <cyclotomic accuracy>" << endl;
    return 1;
  }

  pari_init(1000000, 100000);

  istringstream istrp(argv[1]);
  istrp >> p;
  istrp.clear();
  istrp.str(argv[2]);
  istrp >> maxp;
```

```
  istrp.clear();
  istrp.str(argv[3]);
  istrp >> acc;

  maxp=itos(precprime(stoi(maxp)));
  p=itos(nextprime(stoi(p)));

  generate_cyc_vec(acc);

  cout << "calculating 2-divisibility of primes, writing to file ./data" << endl;
  while (p <= maxp) {
    calculate(p,acc);
    p=itos(nextprime(stoi(p+1)));
  }

  return 0;
}
```

8.2 Some 2-divisibility data

Only the first few computated results are given, and only for the maximum field $\mathcal{K}$. There exists a bigger list on my homepage:

`http://www.math.leidenuniv.nl/~hverhoek/cl2data`

The results are computed by the algorithm given by Algorithm 7.17. Note that a polynomial f corresponding to Jordan-Hölder factor is not f but $\mathbf{F}_2[x]/(f)$.

prime	*polynomials corresponding to Jordan-Hölder factors*	*2-part*
163	(x^2+x^1+1)	4
277	$(x^2+x^1+1)(x^2+x^1+1)$	4
349	$(x^2+x^1+1)(x^2+x^1+1)$	4
397	$(x^2+x^1+1)(x^2+x^1+1)$	4
491	$(x^3+x^1+1)(x^3+x^2+1)$	8
547	(x^2+x^1+1)	4
607	(x^2+x^1+1)	4
709	$(x^2+x^1+1)(x^2+x^1+1)$	4
827	$(x^3+x^1+1)(x^3+x^2+1)$	8
853	(x^2+x^1+1)	4
937	(x^2+x^1+1)	4
941	$(x^4+x^3+x^2+x^1+1)(x^4+x^3+x^2+x^1+1)$	16
1009	(x^2+x^1+1)	4
1399	(x^2+x^1+1)	4
1699	(x^2+x^1+1)	4
1777	$(x^2+x^1+1)(x^2+x^1+1)$	4
1789	$(x^2+x^1+1)(x^2+x^1+1)$	4
1879	(x^2+x^1+1)	4
1951	(x^2+x^1+1)	4
2131	(x^2+x^1+1)	4
2161	$(x^4+x^3+x^2+x^1+1)$	16
2311	(x^2+x^1+1)	4
2689	(x^2+x^1+1)	4
2797	$(x^2+x^1+1)(x^2+x^1+1)$	4
2803	(x^2+x^1+1)	4
2927	$(x^3+x^1+1)(x^3+x^2+1)$	8
3037	$(x^2+x^1+1)(x^2+x^1+1)$	4
3271	(x^2+x^1+1)	4
3301	$(x^4+x^3+x^2+x^1+1)$	16
3517	(x^2+x^1+1)	4
3727	(x^2+x^1+1)	4
3931	$(x^4+x^3+x^2+x^1+1)$	16
4099	(x^2+x^1+1)	4
4219	(x^2+x^1+1)	4

Bibliography

[1] Hall, M., *The Theory of Groups*, The MacMillan Company, 1959

[2] Hayes, D., Fisher, B., *The 2-divisibility of* h_p^+, preprint of author

[3] Gras, G., *Parité du nombre de classes et unités cyclotomiques*, Astérique 24-25, (1975) 1-22

[4] Gras, G., Gras. M.-N. *Signatures des unites cyclotomiques et parité du nombre de classes des extensions cycliques de Q de degré premier impair*, Ann. Inst. Fourier, Grenoble 25, 1975, 37-45

[5] Gras, G., *Class Field Theory, From Theory to Practice*, Springer-Verlag, 2003

[6] Kucera, R., Nekovar, J., *Cyclotomic Units in* $\mathbf{Z}_p$*-extensions*, `http://www.math.jussieu.fr/~nekovar/pu/unit.ps`

[7] Lang, S., *Algebra Revised Third Edition*, Springer-Verlag, 2002

[8] Lang, S., *Algebraic Number Theory 2nd. Edition*, Springer-Verlag, 1994

[9] Lang, S., *Cyclotomic Numbers*, Springer-Verlag, 1978

[10] Lang, S., *Cyclotomic Numbers 2*, Springer-Verlag, 1980

[11] Ribenboim, P., *Classical Theory of Algebraic Numbers*, Springer-Verlag, 2001

[12] Schoof, R., *Class Numbers of Real Cyclotomic Fields of Prime Conductor*, Math. Comp., 72 (2003) 913 937

[13] Schoof, R., *Errata of Class Numbers of Real Cyclotomic Fields of Prime Conductor*, `http://www.mat.uniroma2.it/~schoof/errcycl.txt`

[14] Serre, J.-P., *Linear Representations of Finite Groups*, Springer-Verlag, 1977

[15] Stevenhagen, P., *Class number parity for the pth cyclotomic field*, Math. Comp., 63 (1994) 773-784

[16] Washington, L., *Introduction to Cyclotomic Fields 2nd. Edition*, Springer-Verlag, 1997