UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA

Annihilators of Class Groups

André Filipe Braga Lelis

Rio de Janeiro

Annihilators of Class Groups

de

André Filipe Braga Lelis
Orientador: Aftab Pande

Dissertação de Mestrado submetida ao Programa de Pós-Graduação do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Agradecimentos

À minha família por todo apoio, paciência e carinho nessa jornada.

Aos meus amigos pelo suporte e infinitas conversas sejam matemáticas ou não.

Aos professores que sempre pavimentaram o caminho que trilhei.

Ao meu orientador Aftab Pande pela excelente orientação.

Ao CNPq e CAPES pelo suporte financeiro.

A Deus sem o qual nada é possível.

Abstract

In this thesis, we prove theorems that relate some units of an abelian number with annihilators of its class group. In first part we prove Thaine's Theorem and in the second part we prove a more general result from Rubin.

Keywords: Algebraic Number Theory, Number Field, Class Field, Class Group, annihilators.

Resumo

Nesta dissertação nós provamos teoremas que relacionam determinadas unidades de corpos de números abelianos com os anuladores de seu grupo de classe. Na primeira parte provamos o Teorema de Thaine e na segunda parte provamos um resultado mais genérico devido ao Rubin.

Palavras-chaves: Teoria Algebrica dos Números, Corpos de Números, Corpos de Classe, Grupo de Classe, anuladores.

Contents

Introduction

Given a number field K, we have an important structure associated with K, its ideal class group $Cl(K)$. The ideal class group is defined as quotient group of fractional ideals of $\mathcal{O}_k$ over its principal ideals. Therefore, to find annihilators for class group is to study how a fractional ideals become principal ideals.

A basic result from Algebraic Number Theory states that K is a unique factorization domain if, and only if, the cardinality of $CL(K)$ is one. This result illustrates some of the importance of this kind of annihilators.

An important result about annihilators of class group is known as Stickelberger's Theorem and states:

Let F be an abelian number field. Then, the Stickelberger's ideal of F annihilates the class group of F, where the Stickelberger's Ideal is $\mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$ with $G = Gal(F/\mathbb{Q})$ and $\theta = \sum_{(a,m)=1}\{\frac{a}{m}\}\sigma_a^{-1}$

In 1988, Thaine created a method to create annihilators of the class group of real abelian number fields from cyclotomic units. For example, an elementary proof of the following theorem, that is now known as Thaine's Theorem, is obtained by his method.

Let p be an odd prime number, and $\mathbb{Q}(\zeta_p)^+$ the real subfield of $\mathbb{Q}(\zeta_p)$. Let $\mathcal{U}$,$\mathcal{U}_{cycl}$ and A the global units, cyclotomic units and the p-part of the ideal class group, respectively, of $\mathbb{Q}(\zeta_p)^+$. Then, for any non-trivial even Dirichlet character χ modulo p, $|(\mathcal{U}/\mathcal{U}_{cycl})^\chi|$ annihilates A^χ.

In this thesis, we prove Thaine's theorem and study the generalization of Thaine's method presented by Rubin in his paper *Global units and ideal class groups*.

The application of the results presented in this thesis allow us to determine the order of the Shafarevic-Tate Group. This result is very deep and strong, and is showed in the paper *"Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication"*. However, it is beyond the scope of this thesis.

This thesis is organized in 3 chapters.

In the first chapter, we review number theory and algebra.

In the second chapter, we prove Thaine's theorem with Thaine's method.

In the third chapter, we fix notation and state the main theorem. In the second section, we use Kummer Theory to obtain lemmas that are very useful. In the third, fourth and sixth sections, we apply our main result in a different context. Finally, in section 5, we give a complete proof of our main theorem.

Chapter 1

Brief Review

This section is a quick review of some concepts and results that will be useful in this thesis.

1.1 Basic Algebraic Number Theory

Every theorem and its proof can be found in any book of Algebraic Number Theory e.g. [3] or [4].

Definition 1. We define a **number field** as a finite field extension of $\mathbb{Q}$. In particular, **an abelian number field** F is a number field such that $Gal(F/\mathbb{Q})$ is abelian.

Definition 2. Let K be a number field. We define $\mathcal{O}_K$ the set of $x \in K$ such that x is a root of some monic polynomial of $\mathbb{Z}[X]$. This set is well-known to be a ring which is called the **ring of integers of** K

Theorem 1. *$\mathcal{O}_K$ is a Dedekind domain.*

Proof. See[4], theorem 14, page 56 □

Remark: 1. Dedekind domain is an integral domain that is noetherian, every prime is maximal and integrally closed.

In consequence, we have:

Corollary 2. *Every ideal of $\mathcal{O}_K$ has a unique decomposition in prime ideals.*

Proof. (See[4], theorem 16, page 59) □

This corollary is very important, because if we lose unique factorization by number, we receive information about ideals.

From algebra, we have that:

Proposition 3. *A Dedekind domain R is a unique factorization domain $\Leftrightarrow$ R is a principal domain.*

Proof. See[4], theorem 18, page 62. □

Let P be a prime in $\mathcal{O}_K$ and let F be a finite field extension of K. Suppose that P splits in F as $P\mathcal{O}_F = \prod_{i=1}^{m} Q_i^{e_1}$. By the corollary, this decomposition is unique. Then we said that Q_i is a prime lying above P. Of course, P is prime above some rational prime, i.e., $P \cap \mathbb{Z} = p$ for some prime number p.

Definition 3. In the same situation as above, we say that P ramifies in F, if any of e_i is bigger than 1. Otherwise, we say that P is **unramified**. In addition, we define the **ramification degree** $e(Q_i|P) = e_i$.

Definition 4. We also define the **inertia degree** of Q_i that is $f_i = [\mathcal{O}_F/Q_i : \mathcal{O}_K/P]$.

This definition makes sense since $\mathcal{O}_F/Q_i$ is a finite extension of $\mathcal{O}_K/P$ and both are finite fields with characteristic $p = P \cap \mathbb{Z}$.

We also say that P splits completely if $e_i = f_i = 1$ for all i.

Proposition 4. *Suppose that F/K is a Galois extension of number fields. The Galois group $G = Gal(F/K)$ acts transitively on the set of all prime ideal Q_i lying above P, i.e., these prime ideals are conjugates of each other.*

Proof. See[4], theorem 23, page 70 □

Theorem 5. *If F/K is Galois extension of number fields and let P be a prime of $\mathcal{O}_K$ and $P = \prod_{i=1}^{g} Q_i^{e_i}$ in $\mathcal{O}_F$, then $[K : L] = n = \sum_{i=1}^{g} e_i f_i$.*

Proof. See[4], theorem 21, page 65 □

Definition 5. Let K be a number field of degree n over $\mathbb{Q}$. Let $\{b_1, ..., b_n\}$ be a basis of O_K as $\mathbb{Z}-module$. Then we define $disc(K/\mathbb{Q}) = (det(\sigma_i(b_j)))^2$

We have a great information about what primes ramify in some extension.

Theorem 6. *Let p be a prime number. Then p ramifies in $K/\mathbb{Q} \iff p \mid disc(K/\mathbb{Q})$.*

Proof. See[4], theorem 24, page 72. □

Definition 6. If $Q \in \mathcal{O}_F$ and $Q \cap \mathcal{O}_K = P$, we define the **norm of Q as** $N_{F/K}(Q) = P^{f(Q/P)}$. This norm is multiplicative, so we can extend for arbitrary ideals. Furthermore, $N_{F/K} = N_{E/K} \circ N_{F/E}$.

Definition 7. We define the **decomposition group** of $P \in \mathcal{O}_F$ over K as

$$G_Q = \{\sigma \in G | \sigma(Q) = Q\}$$

The fixed field associated with G_Q is called the **decomposition field** Z_Q.

We conclude immediately that if Q is lying above P, then:

1. $G_Q = \{Id\} \iff Z_Q = F \iff P$ is totally split.

2. $G_Q = G \iff Z_Q = \{Id\} \iff P$ is nonsplit.

We also have that if $\sigma \in G_Q$, then σ acts on $\mathbb{F}_Q = \mathcal{O}_F/Q$ fixing $\mathbb{F}_P = \mathcal{O}_K/P$, where Q lies over P. Actually, we have this strong proposition:

Proposition 7. *The homomorphism $G_Q \to Gal(\mathbb{F}_Q/\mathbb{F}_P)$ is surjective. Also, the extension $\mathbb{F}_Q/\mathbb{F}_P$ is normal.*

Proof. See[3] proposition 9.4, page 56. □

Definition 8. We define the kernel of the homomorphism $G_Q \to Gal(\mathbb{F}_Q/\mathbb{F}_P)$ is called the **Inertia group**, and its associated fixed field is called **inertia field**.

We have the following exact sequence:

$$1 \to I_Q \to G_Q \to Gal(\mathbb{F}_Q/\mathbb{F}_P) \to 1$$

Observe that if $G_Q \cong Gal(\mathbb{F}_Q/\mathbb{F}_P)$, then $e(Q/P) = 1$ and G_Q is cyclic with order f.

Definition 9. In this case, we called the generator of G_Q the **Frobenius element** at Q.

We denote $\sigma = (\frac{Q}{F/K}) = (Q, F/K)$.

Proposition 8. *The Frobenius element at Q is the unique element of $Gal(F/K)$ that satisfies $\sigma(\alpha) \equiv \alpha^{NP} \mod Q \; \forall \alpha \in \mathcal{O}_K$.*

Proof. Suppose that $\sigma(\alpha) \equiv \alpha^{NP} \mod Q \; \forall \alpha \in \mathcal{O}_K$, then $\sigma(Q) \subset Q \Rightarrow \sigma(Q) = Q \therefore \sigma \in G_Q$. By isomorphism, we have the result. □

Proposition 9. *If $Gal(F/K)$ is abelian, then the Frobenius map $(\frac{Q}{F/K})$ depends only of P.*

Proof. Suppose that Q and Q' are prime ideals lying above P. Then write σ and σ' for their respective Frobenius maps. By proposition 4, there is τ such that $\tau(Q) = \tau(Q')$.

Now $\tau(\sigma(\alpha)) \equiv \tau(\alpha^{NP}) \equiv \tau(\alpha)^{NP} \mod Q'$

But $Gal(F/K)$ is abelian. Then, we have that $\sigma\tau = \tau\sigma$. It implies in $\sigma(\tau(\alpha)) \equiv \tau(\alpha)^{NP} \mod Q'$.

However, τ is bijective, then $\sigma(\alpha) \equiv \alpha^{NP} \; \forall \alpha \in \mathcal{O}_F$. □

Theorem 10. *Let K/L be an abelian extension. We define L^{I_Q} to be the inertial field and L^{D_Q} to be the decomposition field. Then, P splits completely in L^D/L. The primes above P remain inert in L^I/L^D and totally ramify in K/L^I.*

Proof. See [4], theorem 28, page 100. □

Definition 10. A **fractional ideal of** $\mathcal{O}_K$ is a $\mathcal{O}_K$-submodule I such that $dI = \{dm | m \in I\}$ is contained in $\mathcal{O}_K$ for some $d \in K$.

Proposition 11. *The set of fractional ideals of $\mathcal{O}_K$, $Id(K)$, is a free abelian group on the set of nonzero prime ideals.*

Proof. See[4], theorem 3.20, page 53. □

Definition 11. We define the **class group of** K, $Cl(K)$, as the quotient group $Id(K)/P(K)$, where $P(K)$ is the group of principal ideals.

Theorem 12. *If K is a number field, then $|Cl(K)|$ is finite*

Proof. See[3], theorem 6.3, page 36. □

From Proposition 3, we have that O_k is UFD $\iff |Cl(K)| = 1$. Then, in some sense, the size of class group measures what is the distance of the ring of integers from being a unique factorization domain.

The following sequence is exact:

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \longrightarrow P(K) \longrightarrow Cl(K) \longrightarrow 1$$

Remark: 2. Actually, the Class Group of some number field K is the Picard Group of $\mathcal{O}_K$. The Picard Group is a more generic definition than the Class Group.

Remember that if G is a finitely generated abelian group, then $G \cong G_{tors} \oplus \mathbb{Z}^t$ for some t where G is the finite group of torsion elements and t is called the rank of G.

Theorem 13. *(Dirichlet's Unit Theorem) The groups of units in a number field K is finitely generated with rank equal to $r + s - 1$ where r is the number of real embedding of a number field K and $2s$ is the number of non-real complex embeddings.*

Proof. See [4] theorem 38, page 142. □

Definition 12. A Dirichlet series is any serie with the following form

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

These series have many properties. One important particular cases is the **Riemann Zeta function** $\zeta(s) = \frac{1}{n^s}$.

We are more interested in **Dedekind Zeta Function**. Let K be an algebraic number field and $\mathcal{I}$ vary through the nonzero integral ideals. The Dedekind Zeta Function of K is

$$\zeta_K(s) = \sum_{\mathcal{I}} \frac{1}{N\mathcal{I}^s}$$

Definition 13. Let $\mathcal{S}$ be any set of primes. If

$$\lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{S}} p^{-s}}{log(\frac{1}{s-1})} = \delta$$

exists, then we call δ the **Dirichlet density** of $\mathcal{S}$. It's clear that a finite set has density 0.

One important theorem that will be useful for us is

Theorem 14. *(Chebotarev Density Theorem). Let $K \subset L$ be galois extension, and let $C \subset G = Gal(L/K)$ be a conjugacy class. Then $\{I : I \quad a \quad prime \quad of \quad K, \quad I \nmid disc(L/K), \sigma_I = \sigma Frob_I \sigma^{-1} \in C\}$ has Dirichlet density $|C|/|G|$.*

Proof. See [3],theorem 13.4, page 545 □

.

Corollary 15. *Let L/K be Galois. Define $\mathcal{S} = \{P \in \mathcal{O}_K | P \quad splits \quad completely \quad in \quad L/K\}$. Then $\delta(\mathcal{S}) = \frac{1}{[L:K]}$*

1.2 Class Field Theory

Class Field Theory provides many important results, especially a description of abelian extensions. In this section, we will see some of these results.

Definition 14. Let α be an element of some number field K. If $\sigma(\alpha) > 0$ for every real embedding σ, we say that α is **totally positive** and write $\alpha >> 0$.

Definition 15. We define P_μ^+ as the subgroup of P_F generated by $\{\langle\alpha\rangle | \alpha \in \mathcal{O}_K, \alpha \equiv 1 \mod \mu\}$ where μ is a non-zero ideal of $\mathcal{O}_K$. In fact, we can define $P_\mu = \{\langle\alpha\rangle | \alpha \equiv 1 \mod P^{ord_P(\mu)} \quad \forall P | \mu\}$

Another important set is $I_K(\mu) = \{m \in Id(K) | ord_\mu m = 0 \quad \forall P \mid \mu\}$, where $Id(K)$ is the set of integral ideals of K.

Definition 16. We define the **ray class group of** K for μ as $\mathcal{R}_{F,\mu} = I_F(\mu)/P_{K,\mu}$.

For example, the ray class group for $\mathbb{Q}$ and $\mu = (\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$

Definition 17. Let K/F be Galois extension and μ be an integral ideal of $\mathcal{O}_F$ and let $\mathcal{H}$ be a subgroup of $I_F(\mu)$ such that $P_{F,\mu}^+ < \mathcal{H} < I_F(\mu)$.

We say that K is the **class field** over F of $\mathcal{H}$ if the set of prime ideals that splits completely in K/F differs of primes ideals in $\mathcal{H}$ by a set with Dirichlet density zero.

Theorem 16. *If the class field K of $\mathcal{H}$ exists, then it is unique.*

Proof. We know that $\delta_F(\mathcal{S}_{K/F}) = \frac{1}{K:F}$.

Define $K = K_1K_2$ where K_1 and K_2 are two classes fields for $\mathcal{H}$.

Now, we have that $\mathcal{S}_{K/F} = \mathcal{S}_{K_1/F}\} \cap \mathcal{S}_{K_2/F} \approx \{P \in \mathcal{H}\}$.

Then, $[K_1 : F] = [K_2 : F] = [K : F]$ □

We state the following results without proofs.

Theorem 17. *For any $\mathcal{H}$, with $P^+_{F,\mu} < \mathcal{H} < I_F(\mu)$, there is a class field K associated to $\mathcal{H}$*

Proof. See [15], theorem 2.7, page 245. □

Theorem 18. *For any abelian extension K/F, there is some μ and some $\mathcal{H}$ such that K is the class field over F of $\mathcal{H}$.*

Proof. □

One important theorem that can be prove using class field is the Kronecker-Weber theorem:

Theorem 19. *(Kronecker-Weber) If K is abelian number field, then exist m such that $K \subset \mathbb{Q}(\zeta_m)$.*

Proof. See [15], theorem 3.8, page 153. □

Definition 18. Let K be an abelian number field. The maximal unramified abelian extension of K is called the **Hilbert Class Field** of K.

Theorem 20. *If H is the Hilbert Class Field of K, then $Gal(H/K) \cong Cl(K)$.*

In particular, $|Cl(K)| = |Gal(H/K)|$ and the maximal unramified abelian extension is a finite extension.

In fact, this theorem is the consequence of more a general theorem:

Theorem 21. *If F is the Class Field over K of $\mathcal{H}$ and $P^+_\mu < \mathcal{H} < I_{F,\mu}$, then $Gal(F/K) \cong I_K(\mu)/\mathcal{H}$.*

Proof. The proof follows from one the major results in Algebraic Number Theory that is **Artin Reciprocity** □

Theorem 22. ***(Artin Reciprocity)*** *Let K/F be an abelian extension of number fields, and assume μ is an ideal of $\mathcal{O}_F$, divisible by all the ramifying primes. Let $G = Gal(K/F)$. Then*

1. *$\mathcal{A} : I_F(\mu) \to G$ given by $Q \to (\frac{Q}{K/F})$ is surjective.*
2. *the ideal μ of $\mathcal{O}_F$ can be chosen so that is divisible only by the ramified primes and satisfies $P_\mu^+ \subset \ker(\mathcal{A})$*
3. *$\mathcal{N}_{K/F}(\mu) \subset \ker \mathcal{A}$, where $\mathcal{N}_{K/F}(\mu) = \{I \in I_F(\mu) | I = N_{K/F}(U), U \in Id_K\}$.*

1.3 Representation Theory

Definition 19. Let G be a group and R a ring. We define the elements of $R[G]$ as the formal sum $\sum r_g g = \alpha$, where r_g are elements of R and g elements of G.

In this set, we define a sum of two elements as $(\sum r_g g) + (\sum r'_g g) = \sum (r'_g + r_g) g$. And their product $(\sum r_g g).(\sum r'_g g') = \sum r_g r_{g'} g g'$.

With these operators, we call $R[G]$ **the group ring of** G **over** R. If R is commutative, $R[G]$ is also called **group algebra of** G **over** R**.**

Definition 20. The homomorphism: $f : R[G] \to R$ given by $\sum r_g g \mapsto \sum r_g$ is called the **augmentation map** and its kernel is called the **augmentation ideal.**

Proposition 23. *The set $\{g - 1 | g \neq 1 \in G\}$ generates the augmentation ideal.*

Proof. If $\alpha = \sum r_g g \in ker(f)$, then $\sum r_g = 0$. Therefore, $\alpha - 0 = \sum r_g g - \sum r_g = \sum r_g (g - 1)$.

On the other hand, is clear that all α generated by this set is contained in the augmentation ideal. □

Definition 21. Let G be a group , R a commutative ring and V a free R-module of finite rank. A representation of G is a group homomorphism $\rho : G \to GL(V)$, where $GL(V)$ is the set of invertible matrices with entries in V. The rank of V is called the degree of the representation ρ. In our case, we consider V a finite-dimensional vector space.

Definition 22. Let $\rho : G \to GL(V)$ be a linear representation. ρ is irreducible if V is not 0 and V has no submodule stable under G. In other words, there is not a $W \subset V$ such that $\rho_g(W) = W$ for all $g \in G$. Of course any one-dimensional representation is irreducible.

Definition 23. Let $V = W \oplus W'$ be a decomposition of V. The map p which sends each $x \in V$ to its components $w \in W$ is called projection of V onto W.

Theorem 24. *Let $\rho : G \to GL(V)$ be a linear representation of a finite group G in V and let W be a vector subspace of V stable under G. Then there exists a complement W^0 of W in V which is stable under G.*

Proof. Let W' be an arbitrary complement of W in V and let p be the projection of V into W.

Define $p^0 = \frac{1}{|G|} \sum \rho_g p \rho_g^{-1}$.

Let $x \in W$. ρ_g preserves W, and as $\rho_g^{-1}(x) \in W$, we see $p(\rho_g^{-1}(x)) = \rho_g^{-1}(x)$, $\rho p \rho_g^{-1}(x) = x$ and $p^0 x = x$.

Thus p^0 is a projection of V onto W corresponding to some complement W^0 of W. Furthermore, $\rho_g p = p \rho_g$.

Now, $\rho_g p^0 \rho_g^{-1} = \frac{1}{|G|} \sum_{s \in G} \rho_g \rho_s p \rho_g^{-1} \rho_s^{-1} = p^0$.

If $x \in W^0$ and $g \in G$, we have $p^0 x = 0$ and $p^0 \rho_g(x) = \rho_g p^0 x = 0$. Therefore, $\rho_g(x) \in W^0$. It means that W^0 is stable under G. □

Theorem 25. *Every representation of finite group is a direct sum of irreducible representations.*

Proof. We give a proof with G finite. If $\dim V = 0$, the theorem is obvious. Suppose $\dim(V) \geq 1$. If V is irreducible, the we are done.

If V is reducible: By the last theorem, we can write $V = W \oplus W'$ where $dim(W) \leq n - 1$ and $dim(W') \leq n - 1$, then we apply the induction hypothesis. □

Corollary 26. *Every representation of a finite group G over a field F with characteristic not dividing the order of G is a direct sum of irreducible representations.*

The next theorem will allow us to for each decomposition into irreducible over a finite field with characteristic p to find a correspondent decomposition in $\mathbb{Z}_p$.

Theorem 27. *Let $\overline{A} = A/N$, where N is a two-side ideal of A contained in radical of A. Assume that either*

1. *A is left artinian or*
2. *A is an R-algebra, finitely generated as R-module, where R is a commutative complete local noetherian ring.*

Then A is complete in the N-adic topology and each decomposition $A = Ae_1 \oplus ... \oplus Ae_n$ into indecomposable left ideals $\{Ae_i\}_{i=1}^{n}$ of $\overline{A}$ yelds a decomposition $\overline{A} = \overline{A}e_1 \oplus ... \oplus \overline{A}e_n$

Conversely, each such decomposition of $\overline{A}$ comes from a decomposition of A.

Furthermore, $Ae_i \cong Ae_j \iff \overline{A}\overline{e}_i \cong \overline{A}\overline{e}_j$

Proof. See [9] Theorem 6.8, page 124. □

Definition 24. Let $\rho : G \to GL(V)$ be a linear representation of finite group G and V finite-dimensional vector space. For each $\sigma \in G$, we define $\chi_\rho(\sigma) = Tr(\rho(g))$. χ_ρ is called character of the representation ρ.

Chapter 2

Thaine's Method

Thaine's method shows a relation between the group of units and the ideal class group of real abelian number fields.

Other results, such as Stickelberger's Theorem, do not give specific information about annihilators of totally real abelian fields.

Since we want to show a relation between certain units and the ideal class group, we begin with definition related with units.

Definition 25. $C_j(X) = \{f(X) = \pm \prod_{i=1}^{j} \prod_{k=1}^{m-1} (X^i - \zeta_m^k)^{a_{ik}} | a_{ik} \in \mathbb{Z}, f(X) \in K(X) \quad and \quad f(1) \in \mathcal{O}_K^* = E\}$

$C = \cup_{j=1}^{\infty} C(1)$ is defined as **circular units**. Sinnot in [16] defines also circular, but his definition is different, however Gunter Lettil in [5] proved that these sets are equal. Also, Sinnot proves that this set has finite index in the group of units. Furthermore, since $\mathcal{O}_K$ is noetherian, there exists l such that $C = \cup_{j=1}^{l} C_j$

The aim of this chapter is to prove the following theorem:

Let K be a real abelian field and E its unit group, C its group of circular units, $Cl(K)$ its class field group. Let p be a prime such that $p \nmid [K : \mathbb{Q}]$. Define $W = E/C$. Let $(W)_p$ and $(Cl(K))_p$ be the p-sylow subgroups of these groups. If $\theta \in \mathbb{Z}[Gal(K/\mathbb{Q})]$ is such that θ annihilates $(W)_p$ then 2θ annihilates $(Cl(K))_p$.

2.1 Obtaining principal ideals

In the rest of this chapter, we will consider K to be a real abelian number field. C, l as in the previous section. Let q be a prime such that $q > l$ and q splits completely in K. We define $L = K(\zeta_q)$. We will denote $G = Gal(L/K)$. When necessary some order in K we will fix some embedding of K into $\mathbb{R}$ and $|x| = \sup\{x, -x\}$.

By the Kronecker-Weber theorem, we have that exists a minimal $m \in \mathbb{Z}$ such that $K \subset \mathbb{Q}(\zeta_m)$.

Proposition 28. *If $f(X) \in C_l(X)$ then $N_{K/L}(f(\zeta_q)) = 1$.*

Proof. $N_{L/K}(f(\zeta_q)) = N_{L/K}(\prod_{i=1}^{j}\prod_{k=1}^{m-1}(\zeta_q^i - \zeta_m^k)^{a_{ik}})$.

From Galois Theory, we know that $Gal(L/K) \simeq Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$.

In the order hand, $q \nmid m$ since q splits completely in K, so $(m, q) = 1$, where (m, q) means the greatest common divisor of m and q. Then, $Gal(\mathbb{Q}(\zeta_{mq})/L) \simeq Gal(\mathbb{Q}(\zeta_m)/K)$ and $Gal(\mathbb{Q}(\zeta_{mq})/\mathbb{Q}(\zeta_m) \simeq Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$.

$N_{L/K}(f(\zeta_q)) = \prod_{i=1}^{l}\prod_{k=1}^{m-1} N_{\mathbb{Q}(\zeta_{mq}/\mathbb{Q}(\zeta_m))}(\zeta_q^i - \zeta_m^k)^{a_{ik}}) = \prod_{i=1}^{l}\prod_{k=1}^{m-1}(\frac{1-\zeta_m^{qk}}{1-\zeta_m^k})^{a_{ik}} = f(1)^{\sigma_q - 1}$

σ_q is the Frobenius map for q in $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Since q splits completely, then $\sigma_q|_K$ is identity. Thus, we have the result. □

Let $Q \in K$ be a prime above q and B the only above Q in L.

Proposition 29. *If $f(X) \in C_l(X)$, then there is $\alpha \neq 0 \in L$ such that $\tau(\alpha) = f(\zeta_q)\alpha$. In addition, for any such element α, we have that*

$$\langle \alpha \rangle = I \prod_{\sigma \in Gal(L/\mathbb{Q}(\zeta_q))} \sigma^{-1}(B)^{r_\sigma} \tag{2.1}$$

where I is the lift of some ideal of K prime to q and $r_q \in \mathbb{Z}$.

Moreover, $s^{r_\sigma} \equiv \sigma(f(1)) \mod Q$, where s is some primitive root of $\mathbb{Z}/q\mathbb{Z}$.

Proof. We know from Hilbert's Theorem 90 that if α is such that $N(\alpha) = 1$ and $Gal(A/B)$ is cyclic generated by τ, then $\alpha = \frac{\tau(\beta)}{\beta}$ for some $\beta \in A$. Applying to the last proposition, we have that there is α such that $\sigma(\alpha) = f(\zeta_q)\alpha$.

Since $f(\zeta_q)$ is an unit, then $\langle \tau(\alpha) \rangle = \langle \alpha \rangle$. Thus the ideal generated by α is fixed by $Gal(L/K)$. We can conclude as desired.

Now, we define $\gamma = \frac{\alpha}{(\zeta_q - 1)^{r_\sigma}}$. Note that we have $(\zeta_q - 1)\mathcal{O}_L = \prod_{\sigma \in Gal(L/\mathbb{Q}(\zeta_q))} \sigma(B)$. Then, if v is the valuation associated with B, we have that $v(\gamma) = 0$. Thus, there are $\lambda, \mu \in \mathcal{O}_L$ with both non-divisible by $\sigma^{-1}(B)$ such that $\gamma = \frac{\lambda}{\mu}$.

Note that $Gal(K(\zeta_q)/K)$ is cyclic. Let τ be the generator of $Gal(L/K)$ and $\sigma \in Gal(L/\mathbb{Q}(\zeta_q))$. Then we have that $\tau(\lambda) \equiv \lambda$ and $\tau(\mu) \equiv \mu \mod \sigma^{-1}(B)$.

$\alpha = \gamma(\zeta_q - 1)^{r_\sigma} \Rightarrow \tau(\alpha) = \tau(\gamma)(\zeta_q^s - 1)^{r_\sigma}$, where s is some primitive root of $\mathbb{Z}/q\mathbb{Z}$, but $\tau(\alpha) = f(\zeta_q)\alpha$. Then, $f(\zeta_q)\alpha = \tau(\gamma)(\zeta_q^s - 1)^{r_\sigma} \Rightarrow \gamma(\zeta_q - 1)^{r_\sigma} f(\zeta_q) = \tau(\gamma)(\zeta_q^s - 1)^{r_\sigma}$.

Therefore, $s^{r_\sigma}\gamma \equiv (\frac{\zeta_q^s - 1}{\zeta_q - 1})^{r_\sigma}\tau(\gamma) = f(\zeta_q)\gamma \equiv f(1)\gamma \mod \sigma^{-1}(B)$.

Concluding that $s^{r_\sigma} \equiv \sigma(f(1)) \mod B$ and since $f(1) \in K$ also $\mod Q$.

□

It implies that

$$N_{L/K}(\alpha) = I^{q-1} \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma^{-1}(Q)^{r_\sigma} \tag{2.2}$$

Definition 26. Let b be a positive integer and let $\mathcal{C}$ be an ideal class of K, we define $\mathcal{P}(\mathcal{C}, b)$ as the set of primes $Q \in \mathcal{C}$ above rational primes q such that q splits completely in K and $q \equiv 1 \mod b$.

Proposition 30. *Let $f(X) \in C_l(X)$, $\delta = f(1) \in C$ and $\sigma \in G$. Then for each $Q \in \mathcal{P}(\mathcal{C}, b)$ exists $\beta_Q \in \mathbb{Z}$ such that $\sigma(\delta) \equiv \beta_Q^g \mod Q$ where g is completely defined by $\sigma(\delta)$ and b.*

Proof. By the last results, if $\mathcal{P}(\mathcal{C}, b)$ is nonempty, then for each $Q \in \mathcal{P}(\mathcal{C}, b)$ exists R_Q such that $R_Q^b \prod_{\sigma \in G} \sigma^{-1}(Q)^{r_\sigma^Q}$ is principal and $s_Q^{r_\sigma^Q} \equiv \sigma(\delta) \mod Q$ for some primitive root of $\mathbb{Z}/q\mathbb{Z}$. Let g be the greatest common divisor of b and r_σ^Q, and define $\beta_Q = s_Q^{r_\sigma^Q/g}$. □

So we want that $P(\mathcal{C}, b) \neq \emptyset$, because with this condition we have a way to obtain a principal ideal. The next proposition gives a condition for it happens.

Proposition 31. *Fix an embedding of K into $\mathbb{R}$. Let H be the Hilbert Class Field of K. Define $\varphi \in Gal(H/K)$ the homomorphism corresponding to $\mathcal{C}$ by* *the isomorphism map between $Gal(H/K)$ and $Cl(K)$. Then, $\mathcal{P}(\mathcal{C},b) \neq \emptyset \Leftrightarrow$ restriction of φ to $K(\zeta_b) \cap H$ is identity map.*

Proof. $\Rightarrow$ If $Q \in \mathcal{P}(\mathcal{C},b) \neq \emptyset$. We have that Q splits completely in $K(\zeta_b)$ since $q \equiv 1 \mod b$. Furthermore, φ is the frobenius map for Q, then the restriction to $K(\zeta_b) \cap H$ is identity.

($\Leftarrow$) $J = K(\zeta_q) \cap H$. We have that $\varphi|_J = Id$, then we can extend φ to automorphism φ' of $H(\zeta_b)$ φ' where $\varphi'(\zeta_b) = \zeta_b$. We know that there are infinitely many prime ideals P of $H(\zeta_b)$ that are unramified over $\mathbb{Q}$ and $P \cap \mathbb{Z} \neq 2$ such that the Frobenius map φ_P for $H(\zeta_b)/K(\zeta_b)$ is φ' and $P' \in K(\zeta_b)$ below P has absolute degree $1(\mathcal{O}_{K(\zeta_b)}/P' \cong \mathbb{Z}/q\mathbb{Z})$. For each P, $\varphi_P|_H = \varphi$ is the Frobenius map for $Q = P \cap \mathcal{O}_K$. Then $Q \in \mathcal{C}$. Since P is unramified over $\mathbb{Q}$, then Q is unramified. Therefore $q = Q \cap \mathbb{Z}$ is congruent to 1 modulus b. It implies that $Q \in \mathcal{P}(\mathcal{C},b)$. □

Corollary 32. *If $\mathcal{P}(\mathcal{C},b) \neq \emptyset$. Then this set is an infinite set.*

Corollary 33. *If K is abelian and the order of $\mathcal{C}$ is prime to $[K:\mathbb{Q}]$, then $\mathcal{P}(\mathcal{C},b)$ is nonempty.*

Proof. We define $J = K(\zeta_b) \cap H$. J is abelian over $\mathbb{Q}$ and unramified over K. If $p \mid [J:K]$, but $p \nmid [K:\mathbb{Q}]$, then there is unramified extension of $\mathbb{Q}$ with degree p, which it is impossible. Therefore, if $\mathcal{C}$ is prime to $[K:\mathbb{Q}]$, then it is prime to $[J:\mathbb{Q}]$. Since the order of φ is equal to the order of $\mathcal{C}$, we have that $\varphi_J = Id$. Now, it follows from the proposition. □

Corollary 34. *If $K \subset \mathbb{Q}(\zeta_{p^r})$ and $b = p^n$ with r, n positive integers, then $\mathcal{P}(\mathcal{C},b)$ is nonempty.*

Proof. When this condition is satisfied, we have that $K(\zeta_b) \subset \mathbb{Q}(\zeta_{p^{n+r}})$. Hence $J = K(\zeta_b) \cap H$ is totally ramified and unramified over K, so $J = K$. Thus, $\varphi|_J = Id$. Now, we apply the proposition. □

2.2 Annihilators of ideals classes

With these results, we can find annihilators under some conditions.

Equation (2.2) implies that for all $Q \in \mathcal{P}(\mathcal{C}, b)$ exists $D_Q \in Cl(K)$ such that

$$D_Q^b \prod_{\sigma \in G} \sigma^{-1}(\mathcal{C})^{r_\sigma(Q)} = 1 \tag{2.3}$$

Theorem 35. *Let p^n be an exponent of $(Cl(K))_p$. If $\mathcal{C} \in (Cl(K))_p$, $Q \in \mathcal{P}(\mathcal{C}, p^n)$ and $r_\sigma = r_\sigma(Q)$, $\sigma \in G$, then $\lambda = \lambda_Q = \sum_\sigma r_\sigma(Q)\sigma^{-1}$ annihilates $\mathcal{C}$.*

Proof. Note that $p^n \mid q - 1$. $\mathcal{C} \in (Cl(K))_p \Rightarrow \mathcal{C}^{p^n} = 1$. Then (2.3) holds for $b = p^n$. $(Cl(K))_p$ is closed under conjugation, then $D_Q^{p^n} \in (Cl(K))_p$. So, $D_Q \in (Cl_K)_p$, thus $D_Q^{p^n} = 1$. Therefore $\mathcal{C}^\lambda = 1$. □

By the last corollaries in the last section, we have that $\mathcal{P}(\mathcal{C}, p^n)$ is nonempty whenever $p \nmid [K : \mathbb{Q}]$ or $K \subset \mathbb{Q}(\zeta_{p^r})$. Then, in these cases we found annihilators for $\mathcal{C}$.

Definition 27. $g = g(\delta, \mathcal{C}, b, \sigma)$, g is the greatest common divisor between b and all $r_\sigma(Q)$. Note that this is the same g that is used in proposition 25.

Proposition 36. *Suppose that $\mathcal{P}(\mathcal{C}, b)$ is nonempty. Let $\gamma \in \mathcal{O}_K$ and $c > 0, c \mid b$. For almost every $Q \in \mathcal{P}(\mathcal{C}, b)$ there exists $\beta_Q \in \mathcal{O}_K$ such that $\gamma \equiv \beta_Q^c \mod Q$. Then $\gamma = \beta^c$ if c is odd and $\gamma = \beta^{c/2}$ if c is even, for some $\beta \in \mathcal{O}_K$.*

Proof. Let $z = \gamma^{1/c}$ be the positive c-th root of γ. Consider L the galois closure of $K(z)$ over K. Then, L is the splitting field of the minimal polynomial of z over K, $p(x)$. Then $p(x) | X^c - \gamma$. Thus, $L = K(z, \zeta_d)$.

Claim: It's enough to prove that $L \subset H(\zeta_b)$, where H is the Hilbert Class Field of K.

Proof: Suppose that this condition holds. Then, L/K and $K(z)/K$ are abelian. So they are normal. $K(z) = L$, then ζ_d need to be real, $\zeta_d = \pm 1$. Thus $p(x) = X - z$ or $p(x) = X^2 - z^2$.

So, now we will prove that $L \subset H(\zeta_b)$

Let $Q \in \mathcal{P}(\mathcal{C}, b)$ be such that Q does not divide γ and does not belong to the finite set of prime ideals that are exceptions, then Q splits completely in $K(z)$, because $p(X)$ reduced modulo Q splits completely over $\mathcal{O}_K/Q$ and Q does not divide the discriminant of z over K.

Define $M = LH(\zeta_b)$ and $\varphi \in Gal(H/K)$ corresponding to $\mathcal{C}$. By the hypothesis and other propositions, we know that $\varphi|_{K(\zeta_b)\cap H} = Id$. Therefore, we can extend φ to automorphism $\tilde{\varphi}$ of M such that $\tilde{\varphi}(\zeta_b) = \zeta_b$.

Now consider $f \in \tilde{\varphi}Gal(M/H(\zeta_b))$. We know that there are infinitely primes $P \in M$ such that P is unramified and do not divide 2, such that $P' = P \cap \mathcal{O}_{K(\zeta_b)}$ has inertia degree 1 and frobenius map at P,ϕ_P, for $M/K(\zeta_b)$ is f.

Therefore, we have that $\phi_P|_H = f|_H = \varphi$ is the Frobenius map for $Q = P \cap \mathcal{O}_K$ with respect to H/K. Thus, $Q \in \mathcal{C}$. We have that P' is unramified and absolute degree 1, hence $Q \cap \mathbb{Z} = q$ and $q \equiv 1 \mod b$. Therefore, $Q \in \mathcal{P}(\mathcal{C}, b)$.

There are infinitely many of these P, so we can choose P to avoid the finite set of prime that β_Q^c is not congruent to γ modulo Q. It implies, that Q obtain in last paragraph splits completely in L. So, we have $f|_L = \phi_P|_L = Id$, then $f \in Gal(M/L)$. But $f \in \tilde{\varphi}Gal(M/H(\zeta_b)) \Rightarrow Gal(M/H(\zeta_b)) \subset Gal(M/L)$. Hence, $L \subset H(\zeta_b)$. □

Definition 28. For each unit $\epsilon \neq \pm 1$, $\epsilon \in \mathcal{O}_K$. We define $\Phi(\epsilon)$ as the greatest integer k such that $\epsilon = x^k$ for some $x \in K$.

Theorem 37. *Let $\delta \in C \setminus \{\pm 1\}$ and $\mathcal{P}(\mathcal{C}, b)$ as above and let $g = g(\delta, \mathcal{C}, b, \sigma)$. Then:*

1. *If b is odd, then $g = (\Phi(\delta), b)$*
2. *If b is even and $\sigma(\delta) > 0$, then $g = (\Phi(\delta), b)$ or $g = 2(\Phi(\delta), b)$.*
3. *if b is even and $\sigma(\delta) < 0$, then g divides $(4/(2, b/g))(\Phi(|\delta|), b)$ and is divisible by $(\Phi(\delta), b)$.*

Proof. We need the following lemma:

Lemma 38. *Let δ be as in the last theorem. If $\delta = \beta^c$ with $\beta \in K$, then $c \mid \Phi(\delta)$.*

Proof: Let $v \in K$ be such that $\delta = v^{\Phi}$. Let $d = (c, \Phi)$ and $x, y \in \mathbb{Z}$ such that $xc + y\Phi = d$. Then $\delta = (v^x \beta^y)^{[c,\Phi]}$, where $[c, \Phi]$ is lcm of c and Φ. By definition of Φ, we have that $[c, \Phi] \leq \Phi$, hence $c \mid \Phi$. □

Now, we will prove the theorem 37:

Let $\delta = \mu^{\Phi(\delta)}$ for some $\mu \in K$. Then $\sigma(\delta) = \sigma(\mu)^{\Phi(\delta)}$. Hence, we have that $s_Q^{r_\sigma(Q)} \equiv \sigma(\mu)^{\Phi(\delta)} \mod Q$.

On the other hand, we have that $\sigma(\mu) \equiv n \mod Q$ for some n, since Q has $f_{Q/q} = 1$(absolute degree 1). So, $s_Q^{r_\sigma(Q)} \equiv n^{\Phi(\delta)} \mod Q$ and $\mod q$.

Claim: $(\Phi(\delta), b) \mid g$

Let $d = (\Phi(\delta), b)$, then $\Phi(delta) = dc$ and $b = dt$. We also have that $b|q-1$, then $q-1 = dl$. Now we have that $s_Q^{r_\sigma(Q)lt} \equiv n^{tl} \equiv 1 \mod q$. $r_\sigma(Q)lt =$ multiple of $q-1$, which is a multiple of d. But $d \nmid lt$, so $d \mid r_\sigma(Q)$.

We proved that for all $Q \in \mathcal{P}(\mathcal{C}, b)$ there exists $\beta_Q \in \mathbb{Z}$ such that $\sigma(\delta) \equiv \beta_Q^g \mod Q$. This implies that $\sigma(\delta^2) \equiv \beta_Q^{2g} \mod Q$.

Define $c = (2g, b)$. By the last proposition, $\sigma(\delta) = \gamma^g$ or $\sigma(\delta) = \gamma^{g/2}$ if $\sigma(\delta) > 0$. Also $\sigma(\delta^2) = \gamma'^c$ if c is odd, and $\sigma(\delta^2) = \gamma'^{c/2}$ if c is even.

1. If b is odd, then $g = c$ and divides $(\Phi(\delta), b) = (\Phi(\delta^2, b))$. It implies that $g = (\Phi(\delta), b)$.

2. If b is even and $\sigma(\delta) > 0$, then $g \mid 2(\Phi(\delta), b)$. Then $g = (\Phi(\delta), b)$ or $g = 2(\Phi(\delta), b)$.

3. In all cases, $c = (2g, b)$ divides $2\Phi(\delta^2) = 4\Phi(|\delta|)$. Therefore, $c = g(2, b/g) \mid 4(\varphi(|\delta|), b)$.

□

Now we can find more annihilators for some ideal class of $(Cl(K))_p$

Proposition 39. *Let p^n be an exponent of $(Cl(K))_p$. Suppose that for all $\sigma \in G = Gal(K/\mathbb{Q})$ there exists integer c_σ, non-divisible by p, such that*

$$\sigma(\delta) \equiv \delta^{c_\sigma} \mod E^{p^n} \tag{2.4}$$

Let $\mathcal{C} \in (Cl(K)_p)$ and denote $\sum_{\sigma \in G} c_\sigma \sigma^{-1} \in \mathbb{Z}[G]$ by ω, then:

1. *If p is odd, then $(\Phi(\delta), p^n)\omega$ annihilates $\mathcal{C}$*

2. *If $p = 2$, $2(\Phi(|\delta|), 2^n)\omega$ annihilates $\mathcal{C}$.*

Proof. Let $Q \in \mathcal{P}(\mathcal{C}, p^n)$ and $q, s, r_\sigma(Q) = r_\sigma$ as before. We have that $\lambda = \sum_{\sigma \in G} r_\sigma \sigma^{-1}$ annihilates $\mathcal{C}$.

On the other hand, we have that $s^d \equiv \delta \mod Q$ for some $d \in \mathbb{Z}_+^*$.

Fixed $\sigma \in G$. By hypothesis, we have that $\sigma(\delta) = \epsilon_\sigma \delta^{c_\sigma}$ for some $\epsilon_\sigma \in E^{p^n}$.

Now, $s^{r_\sigma} \equiv \sigma(\delta) \equiv \delta^{c_\sigma}\epsilon_\sigma^{p^n} \equiv s^{dc_\sigma + p^n t} \mod Q$. Hence $s^{r_\sigma - (dc_\sigma + p^n t)} \equiv 1 \mod Q$. s is primitive root by choice, so $q-1 | r_\sigma - (dc_\sigma + p^n t)$ or $r_\sigma = dc_\sigma + p^n t$.

We know that $p^n | q-1$, then $r_\sigma \equiv dc_\sigma \mod q$ and also $\mod p^n$. Therefore $\lambda \equiv d(Q) \sum_{\sigma \in G} c_\sigma \mod p^n$

Since $\mathcal{C}^{p^n} = \mathcal{C}^\lambda = 1$, we have that $g_0 \sum_{\sigma\in G} c_\sigma \sigma^{-1}$ annihilates $\mathcal{C}$, where $g_0 = (p^n, d(Q))$.

Look at g_0. We know $r_\sigma \equiv dc_\sigma \mod p^n$. We need to have c_σ prime to p^n. So g_0 is also the gcd of (r_Q, p^n). So g from the last theorem is exact g_0.

Now, we apply the last theorem for (1). For (2), we observe that $|\delta|$ satisfies (2.4) whenever $p = 2$. □

2.3 Annihilators of the p-part of the Ideal Class Group

We have obtained of ideal class, but we want annihilators for $(Cl(K))_p$.

Given $\chi : G \to \mathbb{Z}_l^\times$ a representation of G. We can associate χ to $e_\chi = \frac{1}{|G|}\sum \chi(\sigma)\sigma^{-1}$.

e_χ has the following properties:

1. $e_\chi^2 = e_\chi$

2. $1 = \sum e_\chi$

3. $e_\chi \sigma = \chi(\sigma) e_\chi$

Proposition 40. *Suppose that $p \nmid [K:\mathbb{Q}]$. Let p^k be an exponent of $(W)_p$, $\chi : G \to \mathbb{Z}_p^\times$ a non-trivial p-adic valued Dirichlet character, $e_\chi = \frac{1}{|G|}\sum_{g \in G} \chi(\sigma)\sigma^{-1} \in \mathbb{Z}_p[G]$ the corresponding idempotent and p^t the exact exponent of the χ-component $e_\chi(W)_p$ of $(W)_p$. Then, there exists $\delta \in C$ such that $p^{t+1} \nmid \Phi(\delta)$ and such that $\sigma(\delta) \equiv \delta^{\chi(a)} \mod E^{p^k}$ for all $\sigma \in G$.*

Proof. For $k = 0$, the result is trivial.

$(W)_p \cong E/E^{p^k}C$, so we have $e_\chi(W)_p \cong e_\chi(E/E^{p^k}C) \cong \frac{e_\chi(E/E^{p^k})}{e_\chi(E^{p^k}C/E^{p^k})}$.

By the isomorphism, $\eta \in E$ such that $\eta C \in e_\chi(W)_p$ are the same η such that $\eta E^{p^k} \in e_\chi(E/E^{p^k})$. For these η, we have $\eta^{p^t c} \in C$, for some c prime to p and $\sigma(\eta) \equiv \eta^{\chi(\sigma)} \mod E^{p^k}$.

Claim: $\exists$ η such that $\eta \notin E^p$

Proof: Suppose that all $\eta \in E^{p^k}$. Then, $e_\chi(E/E^{p^k}) \subset E^p/E^{p^k} = (E/E^{p^k})^p$. It implies that

$$e_\chi(E/E^{p^k}) \subset e_\chi(E/E^{p^k})^p \subset ... \subset e_\chi(E/E^{p^k})^{p^k} = 1$$

Therefore $e_\chi(E/E^{p^k}) = 1$. Thus, since $j \geq k$

$$e_\chi(E/E^{p^k}) \cong e_\chi(\tfrac{(E/E^{p^k})}{(E/E^{p^j})^{p^k}}) \cong \tfrac{e_\chi(E/E^{p^j})}{e_\chi(E/E^{p^j})^{p^k}}$$

we have $e_\chi(E/E^{p^j}) = 1 \forall j \geq 1$.

Let $\hat{E}$ be the inverse limit $\varprojlim(E/E^{p^j})$. For above equality $e_\chi(\hat{E}) = 1$.

Now we need a lemma

Lemma 41. *There exists $\epsilon \in E$ such that the subgroup $\{\epsilon^\lambda | \lambda \in \mathbb{Z}[G]\}$ has a finite index in E*

Proof of the lemma: Consider $\sigma_k \in G$ for all $0 \leq k \leq r = |G| - 1$ and $\epsilon \in E$. We will prove that $\det[ln(\sigma_i\sigma_j(\epsilon)] \neq 0$.

Determinant is a polynomial function. We will consider $f(X_1, ..., X_r) = det(X_{p(i,j)})$ where $p(i,j)$ is defined by $\sigma_i\sigma_j = \sigma_{p(i,j)}$ and $X_0 = -X_1 - ... - X_r$.

$f(1, ..., 1) = |G|^{|G|-2}$, so f is not identically to 0.

Now, consider $\epsilon_1, ..., \epsilon_r$ be a fundamental system of units and define $g(y_1, ..., y_r) = f(\sum_{j=1}^r ln(\sigma_1(\epsilon_j)y_1 ... \sum_{j=1}^r ln|\sigma_r(\epsilon_j)|y_j)$. That's the same to look for all $\epsilon = \epsilon_1^{y_1}...\epsilon_r^{y_r}$ where $y_i \in \mathbb{Z}$.

Now, suppose that g is 0 for all this $(y_i) \in \mathbb{Z}^r$. So, if we fix $w \in \mathbb{Z}^{r-1}$, then $g(y, w)$ will have infinite solutions. Therefore, g is the polynomial 0.

However, we $f \neq 0$ and $ln|\sigma_i(\epsilon_j)$ is invertible($\det[ln(\sigma_i(e_j)] \neq 0$. □

For this ϵ, consider the function $\varphi : \mathbb{Z}_p \to \hat{E}$ defined by $\lambda \mapsto \epsilon^\lambda$.

The $ker(\varphi)$ is generated by e_{χ_0} But $e_\chi \in ker(\varphi)$, then $\chi = \chi_0$. Contradiction!

So, there is η such that $\eta \notin E^p$. Let c be a prime to p, such that $\delta = \eta^{p^t c} \in C$.

Claim: δ satisfies the conditions of proposition.

$p \nmid \varPhi(\eta) \Rightarrow p^{t+1} \nmid \varPhi(\delta)$ and $\delta \equiv \delta^{\chi(\sigma)} \mod E^{p^k}$. Furthermore, χ forces p be odd.

□

Theorem 42. *Let p be a prime such that $p \nmid [K : \mathbb{Q}]$, $\chi : G \to \mathbb{Z}_p^x$ be a non-trivial p-adic valued Dirichlet character, e_χ the corresponding idempotent. If p^a is the exact exponent of $e_\chi(W)_p$, then p^a annihilates $e_\chi(Cl(K))_p$.*

Proof. First, note that the conditions on χ force p to be odd. For each $\sigma \in G$, there is an integer c_σ such that $c_\sigma \equiv \chi(\sigma) \mod p^n$. Then, $\sum_{\sigma \in G} c_\sigma \sigma^{-1} \equiv |G| e_\chi \mod p^n$. (1)

By the last proposition, there is $\delta \in C$ such that $p^{a+1} \nmid \varPhi(\delta)$ and $\sigma(\delta) \equiv \delta^{\chi(\sigma)} \equiv \delta^{c_\sigma} \mod E^{p^n}$

Let $\mathcal{C} \in (Cl(K))_p$. We have seen that $(\varPhi(\delta), p^n) \sum_{\sigma \in G} c_\sigma \sigma^{-1}$ annihilates $\mathcal{C}$. Now, observe that $(\varPhi(\delta), p^n) \mid p^a$. Therefore, $p^a \sum_{\sigma \in G} c_\sigma \sigma^{-1}$ annihilates $\mathcal{C}$.

Multiplying (1) by p^a, we have that $p^a \sum_{\sigma \in G} c_\sigma \sigma^{-1} \equiv p^a |G| e_\chi \mod p^n$. However, $p \nmid |G|$, so $p^a e_\chi$ annihilates $\mathcal{C}$. As we have taken any $\mathcal{C}$, we have p^a annihilates $e_\chi(Cl(K))_p$. □

Corollary 43. *Let p be an odd prime. If $K \subset \mathbb{Q}(\zeta_b) \cap \mathbb{R}$, then every annihilator of $(W)_p$ (in $\mathbb{Z}[G]$) is also annihilator of $(Cl(K))_p$.*

Proof. Let $\sum_{\sigma \in G} c_\sigma \sigma^{-1}$ be an annihilator of $(W)_p$. χ any non-trivial p-adic valued Dirichlet character of G.

We have that $(\sum_{\sigma \in G} c_\sigma \sigma) e_\chi = \sum_{\sigma \in G} c_\sigma \chi(\sigma) e_\chi$. Therefore, $\sum_{\sigma \in G} c_\sigma \chi(\sigma)$ annihilates $e_\chi(W)_p$.

If $p^{a(x)}$ is the order of this group, then $\sum_{\sigma \in G} c_\sigma \chi(\sigma) \equiv 0 \mod p^{a(x)}$

$K \subset \mathbb{Q}(\zeta_b)$, we have that $\sum_\chi e_\chi = 1$, where χ runs over all p-adic-valued Dirichlet characters.

We can write $\sum_{\sigma \in G} c_\sigma \sigma = \sum_{\sigma \in G} c_\sigma \sigma \sum_\chi e_\chi = \sum_\chi \sum_{\sigma \in G} c_\sigma \chi(\sigma) e_\sigma$.

By last theorem, $\sum_{\sigma \in G} c_\sigma \chi(\sigma)$ annihilates $e_\chi(W)_p$, then $\sum_{\sigma \in G} c_\sigma \chi(\sigma) e_\sigma$ annihilates $(Cl(K))_p$ for all χ. Therefore $\sum_{\sigma \in G} c_\sigma \sigma$ is an annihilator of $(Cl(K))_p$. □

Now, we need to prove Thaine's theorem:

To prove it we will extend the idea from the last proof to character with more than one dimension.

Proposition 44. *Let $p \nmid [K : \mathbb{Q}]$, and $p^n > 4$ be an exponent of $(Cl(F))_p$ and $(W)_p$. Then, $2p^{a_\rho}$ annihilates $(Cl(K))_p$.*

Proof. Let $\mathcal{C} \in (Cl(K))_p$. We have that $\mathcal{P}(\mathcal{C}, p^n)$ is nonempty. Now we consider Q, q, s, r_σ as before.

Define $\varphi_Q : C/C \cap E^{p^n} \to \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G]$ by $\delta \to \sum_{\sigma \in G} r_\sigma \sigma^{-1}$.

We have already seen that $\mathcal{C}^{\varphi_Q(\delta)} = 1$ for all $\delta \in .C/C \cap E^{p^n}$

Now, we can written $\mathbb{Z}_p[G] = \oplus_\rho e_\rho \mathbb{Z}_p$, where e_ρ are the idempotents of $\mathbb{Z}_p$. It is possible, because we already know that $\oplus e_\rho \mathbb{F}_p$ correspond to the above decomposition by theorem 27.

Let ρ be an irreducible non-trivial character of G into F_p. We can restrict φ_Q to $\varphi_Q^\rho : e_\rho(C/C \cap E^{p^n}) \to e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G]$.

The proposition 40 follows true in general case.So, let $p^a = p^{a_\rho}$ be the exact exponent of $e_\rho(W)_p$. Exists $\delta \in e_\rho(C/C \cap E^{p^n})$ such that $p^{a+1} \nmid \Phi(\delta)$.

For such δ, it follows from Theorem 37 that $g(\delta, \mathcal{C}, p^n, id)$ divides $2p^a$. Hence, there exist $Q \in P(\mathcal{C}, p^n)$ such that

$$\varphi_Q^\rho(\delta) \not\equiv 0 \mod p^{a+1}, \text{ if } p \text{ is odd}$$
$$\varphi_Q \not\equiv 0 \mod 2^{a+2}, \text{ if } p = 2$$

For this Q we define a' be a minimal such that $\varphi_Q^\rho(\delta) \not\equiv 0 \mod p^{a'+1}$. Therefore $p^{-a'}\varphi_Q^\rho(\delta)$ is non-zero in $e_\rho \mathbb{F}_p[G]$.

$e_\rho \mathbb{F}_p$ is irreducible, so $p^{-a'}\varphi_Q^\rho(\delta)$ generate it as $\mathbb{F}_p[G]$ module.

We know that $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with maximal ideal $p\mathbb{Z}/p^n\mathbb{Z}$ and residue field $\mathbb{F}_p$. The $\mathbb{Z}/p^n\mathbb{Z}$- module $e_\rho(\mathbb{Z}/p\mathbb{Z})[G]$ has the elements $p^{-a}\varphi_Q^\rho(\delta)\sigma$, $\sigma \in G$. Since $p^{-a'}\varphi_Q^\rho(\delta)$ generate it as $\mathbb{F}_p[G]$ module, the image of $p^{-a}\varphi_Q^\rho(\delta)\sigma$ in $e_\rho \mathbb{F}_p[G]$ form a basis of this $\mathbb{F}_p$-vector space.

We need a lemma from commutative algebra:

Lemma 45. *Let x_i be elements of M whose images in M/mM form a basis of this vector space. Then x_i generate M.*

Proof: See [17], proposition 2.8.

Applying to our situation, we have that $p^{-a}\varphi_Q^\rho(\delta)(\mathbb{Z}/p^n\mathbb{Z})[G] = e_\rho(\mathbb{Z}/p^n\mathbb{Z})[G]$.

It implies that $2p^a e_\rho(\mathbb{Z}/p^n\mathbb{Z}) \subset p^{a'}\varphi_Q^\rho(\delta)e_\rho(\mathbb{Z}/p^n\mathbb{Z}) \subset Image(\varphi_Q^\rho)$.

Therefore, $2p^a e_\rho(\mathbb{Z}/p^n\mathbb{Z})$ annihilates $\mathcal{C}$. Since $\mathcal{C}$ is arbitrary, we have that $2p^{a_\rho}e_\rho$ annihilates $(Cl(K))_p$. □

Now we can prove Thaine's Theorem

Theorem 46. *Let K be a real abelian field and E its unit group, C its group of circular units, $Cl(K)$ its class field group. Define $W = E/C$. Let $(W)_p$ and $(Cl(K))_p$ be the p-sylow subgroups of these groups. If $\theta \in \mathbb{Z}[Gal(K/\mathbb{Q})]$ is such that θ annihilates $(W)_p$ then 2θ annihilates $(Cl(K))_p$.*

Proof. Let $\theta \in \mathbb{Z}_p[G]$ be an annihilator of $(W)_p$. Let ρ be a irreducible character $G \to \mathbb{F}_p$ and e_ρ the idempotent associated to ρ.

We have that θe_ρ annihilates $e_\rho(W)_p$. Let p^b be a maximal power of p dividing θe_ρ. We use the same argument of the last proposition, to prove $\theta e_\rho(\mathbb{Z}/p^n\mathbb{Z})[G] = p^b e_\rho[G]$.

In particular, exists γ such that $\theta e_\rho \gamma = p^b e_\rho$. Therefore, p^b annihilates $e_\rho(W)_p$. It implies that $b \geq a_\rho$, and $p^{a_\rho} \mid \theta e_\rho$, where p^{a_ρ} is the exact exponent of $(W)_p$, hence $2\theta e_\rho$ annihilates $(Cl(K))_p$.

$2\theta = \sum_\rho 2\theta e_\rho$, thus we have that 2θ annihilates $(Cl(K))_p$.

□

Chapter 3

Generalization of Thaine's Method

3.1 Notation and main theorem

In this chapter, we will fix the notation that will be used in the others chapters and state the main theorem of this thesis.

Given any number field E, we denote by $\mathcal{O}_E$ its ring of integers.

Fix K a number field and F an abelian extension of K containing the Hilbert class Field of K denoted by K_H. We write $G = Gal(F/K)$.

So, we have the following diagram:

$$\begin{tikzcd}
F \arrow[d, dash] \\
K_H \arrow[d, dash] \\
K \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

For any prime q of K, we define:

$$K(q) \text{ the ray class field of } K \text{ modulo } q.$$

$$F(q) = \text{composition of } K(q) \text{ and } F$$
$$\mathcal{E}(q) = \{u \in \mathcal{O}_{F(q)}^{\times} | N_{F(q)/F}(u) = 1\}.$$
$$w(q) = \text{the order of } \mathcal{O}_K^{\times} \text{ in } (\mathcal{O}_K/q)^{\times}$$
$$\tilde{q} = \text{product of prime above } q.$$
$$\mathcal{C}(q) = \{\epsilon \in \mathcal{O}_F^{\times} | \exists u \in \mathcal{E}(q) s.t. u \equiv \epsilon^{w(q)} (\mod \tilde{q})\}$$

We define $\mathcal{L}$ the set of primes of K of absolute degree 1 which split completely in F. Define $\mathcal{C}$ the group of special units of F/K to be

$$\mathcal{C} = \{\epsilon \in \mathcal{O}_F^{\times} | \epsilon \in \mathcal{C}(q) \quad for \quad all \quad but \quad finitely \quad many \quad q\}$$

We know that $\mathcal{O}_F^{\times}$ is finitely-generated, then $\mathcal{C}$ is also finitely-generated. Moreover, note that $\mathcal{C}(q)$ is stable under G, therefore $\mathcal{C}$ is also stable.

Fix $N \in \mathbb{N}$. We define

1. a $G-module$ V of $\mathcal{O}_F^{\times}/(\mathcal{O}_F^{\times})^N$

2. a $G-module$ map $\alpha : V \to (\mathbb{Z}/\mathbb{N}\mathbb{Z})[G]$ which is trivial on $\mathcal{O}_K^{\times} \cap V$

3. $G-module$ quotient A of $Cl(F)/NCl(F)$, where $Cl(F)$ is the ideal class group of F. We identify A with $Gal(H_A/F)$, where H_A is the subfield of the Hilbert Class Field of F, F_H.

Define $H' = H_A \cap F(\mu_N, (ker\alpha)^{1/N}, (\mathcal{O}_K^{\times})^{1/N})$ and $A' = Gal(H_A/H') \subset A$.

The **main result** of this thesis is the following.

MAIN THEOREM: *Let N, V, α, A and $\mathcal{C}$ as above. If $4 \nmid N$ or $\mu_4 \subset F$, then $\alpha(\mathcal{C} \cap V)$ annihilates A'. In general, $2\alpha(\mathcal{C} \cap V)$ annihilates A'*

We also define:

1. $F_1 = F(\mu_{Nm(F)})$, where $m(F)$ is the number of roots of unity in F.

2. $F_2 = F_1((\ker\alpha)^{1/N})$

3. $F_3 = F_2((\mathcal{O}_K^{\times})^{1/N})$

$$H_i = H_A \cap F_i$$

Therefore, each H_i is a subfield of H_A and F_i. Furthermore, H_A is a subfield of the Hilbert Class Field of F, so each H_i is abelian over F and unramified. Moreover, $H' \subset H_3$.

Note that if $\mathcal{I} \subset \mathbb{Z}[G]$ annihilates $Gal(H_3/F)$ then $\mathcal{I}$ annihilates A/A'. Furthermore by our main theorem $\mathcal{I}\alpha(\mathcal{C} \cap V)$ (or $2\mathcal{I}\alpha(\mathcal{C} \cap V)$) annihilates A.

3.2 Kummer Theory and useful lemmas

In this chapter, we will use Kummer Theory. For this purpose, we will do a quick review of Kummer Theory.

Definition 29. Let G be a finite group and M a $G - module$. The 0^{th} cohomology of the $G - module\ M$, which is denoted by M^G or $H^0(G, M)$ is the set

$$H^0(G, M) = \{m \in M | m^\sigma = m \forall \sigma \in G\}$$

Given an exact sequence of $G - modules$

$$0 \to N \to M \to L \to 0$$

It is easy to see that $G - invariants$ imply the following exact sequence

$$0 \to N^G \to M^G \to L^G$$

Definition 30. Let M be a $G - module$. The group of $1 - cochain$ is defined by

$$C^1(G, M) = \{maps \quad f : G \to M\}$$

The group of $1 - cocycles$ is defined by

$$Z^1(G, M) = \{f \in C^1(G, M) | f_{\sigma\tau} = f_\sigma^\tau + f_\tau\}$$

The group of 1-coboundaries is defined by

$$B^1(G, M) = \{f \in C^1(G, M) | \quad \exists m \in M \quad s.t. \quad f_\sigma = m^\sigma - m \forall \sigma \in G\}$$

Definition 31. The 1^{st} cohomology group of the $G - module\ M$ is the quotient group

$$H^1(G, M) = \frac{Z^1(G,M)}{B^1(G,M)}$$

Suppose that G acts trivially on M, then $H^0(G, M) = M$ and $H^1(G, M) = Hom(G, M)$

Proposition 47. *(Hilbert's 90 Theorem) Let L/T be any finite Galois extension of fields. Then $H^1(Gal(L/T), L^\times) = 0$.*

Proof. Suppose $f : Gal(L/T) \to L^\times$ is $1 - cocycle$. For any $c \in L$, consider $b = \sum_{\sigma \in Gal(L/T)} f(\sigma)\sigma(c)$.

If b is 0 for all c, then the elements will be linearly depend, but we know from Artin's theorem that is not true.[See 18].

Therefore, $\tau(b) = \sum_{\sigma \in Gal(L/T)} \tau(f(\sigma))\tau\sigma(c) = \sum_{\tau\sigma} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(c) = f(\sigma)^{-1}(b)$.

Thus, f is a coboundary. □

Theorem 48. *Let L/T be a finite Galois extension with Galois Group H and suppose that $\mu_n \subset T$. Then, $(T^\times \cap (L^\times)^n)/(T^\times)^n \cong Hom(H, \mu_n)$.*

Proof. We have the following exact sequence:

$$0 \to \mu_n \to L^\times \to (L^\times)^n \to 0$$

It gives the long exact sequence

$$0 \to \mu^H \to (L^\times)^H \to ((L^\times)^n)^H \to H^1(H, \mu_n) \to H^1(H, L^\times) \to ...$$

By the last proposition, $H^1(H, L^\times) = 0$. Moreover, H acts trivially on μ_n, so $H^1(H, \mu_n) = Hom(H, \mu_n)$ Therefore, we can rewrite the sequence as

$$0 \to \mu_n \to T^\times \to T^\times \cap (L^\times)^n \to Hom(H, \mu_n) \to 0$$

Thus, we have the isomorphism $\frac{T^\times \cap (L^\times)^n}{(T^\times)^n} \cong Hom(H, \mu_n)$ □

Definition 32. A finite Galois extension L/T is callled $n - Kummer$ extension when T contains an $n - primitive$ root of unity and $Gal(L/T)$ is abelian with exponent n.

Definition 33. Let G_1 and G_2 be an abelian groups. A bilinear pairing is a map $B : G_1 \times G_2 \to C$, where C is another abelian group, such that

$$B(g_1 g_1', g_2) = B(g_1, g_2)B(g_1', g_2)$$
$$B(g_1, g_2 g_2') = B(g_1, g_2)B(g_1.g_2')$$

The pairing is said to be non-degenerate when for any $g_1 \neq 1 \in G_1$ there exist $g_2 \in G_2$ such that $B(g_1, g_2) \neq 1$.

Proposition 49. *Suppose $B : G_1 \times G_2 \to \mu_n$ a bilinear pairing with order of n divisible by the exponent of G_1 and G_2. If G_1 or G_2 is finite, then $G_1 \cong Hom(G_2, C = \mu_n)$, $G_2 \cong Hom(G_1, \mu_n)$ and $G_1 \cong G_2$.*

Proof. Define $G_1 \to Hom(G_2, \mu_n)$ as $g_1 \to B(g_1, -)$. Since B é is non-degenerate, we have it is injective.

Suppose that G_2 is finite, then $|G_1| \leq |Hom(G_2, \mu_n)| = |G_2|$.

We can reapply the argument replacing G_1 with G_2. Therefore, $|G_1| = |G_2|$ and $G_1 \cong Hom(G_2, \mu_n)$

□

In particular, we want to take T/L a $n - Kummer$ extension, $G_1 = Gal(T/L)$ and $G_2 = \frac{L^\times \cap (T^\times)^n}{(L^\times)^n}$. G_1 and G_2 form a non-degenerate bilinear pairing. This pair is called a **Kummer pairing** and is defined by $B(\sigma, \overline{a}) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$, where $\bar{a}$ is the class of a in G_2 and $\sqrt[n]{a}$ is any n-th root of a in T.

Theorem 50. *The Kummer pairing as defined above is well-defined, bilinear and nondegenerate.*

Proof. If $\overline{a} = \overline{a'}$, then $a = a'h^n$. $B(\sigma, \overline{a}) = \frac{\sigma(\zeta \sqrt[n]{a})}{\zeta \sqrt[n]{a}} = \frac{\zeta \sqrt[n]{a'}h}{\zeta \sqrt[n]{a'}h} = \frac{\zeta\sigma(\sqrt[n]{a'})f}{\zeta \sqrt[n]{a'}f} = \frac{\sigma(\sqrt[n]{a'})}{\sqrt[n]{a'}}$.

Therefore the Kummer Pairing is well defined.

Linearity in the first coordinate:

$B(\sigma\tau, \overline{a}) = \frac{\sigma\tau(a)}{\sqrt[n]{a}} = \frac{\sigma\tau(\sqrt[n]{a})}{\tau(\sqrt[n]{a})} \frac{\tau(\sqrt[n]{a})}{\sqrt[n]{a}}$

Since, our galois group is abelian, we have $\frac{\sigma\tau(a)}{\tau(\sqrt[n]{a})} = \tau(\frac{\sigma(a)}{\sqrt[n]{a}}) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$, since $\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \in L$.

Linearity in the second coordinate:

$B(\sigma, \overline{ab}) = \frac{\sigma(ab)}{\sqrt[n]{ab}} = \frac{\sigma(a)}{\sqrt[n]{a}} \frac{\sigma(b)}{\sqrt[n]{b}}$.

Non-degenerate

Suppose $\sigma \in Gal(T/L)$ is such that $B(\sigma, \overline{a}) = 1$ for all $\overline{a}$. This means that σ fixes all a, therefore $\sigma = Id$.

Suppose that there is $\overline{a}$ such that $B(\sigma, \overline{a}) = 1 \forall \sigma \in Gal(T/L)$. Therefore, $\sqrt[n]{a}a$ is fixed by $Gal(T/L)$. $\sqrt[n]{a} \in L$. □

Corollary 51. *Let T, L and H as in the theorem 2. Then $H \cong Hom(\frac{T^\times \cap (L^\times)^n}{(T^\times)^n}, \mu_n)$*

Theorem 52. *Let $n > 1$, and let L be a field containing a primitive $n - th$ root of unity. Fix an algebraic closure of $\overline{L}$ of L. There exists a one-to-one, order preserving correspondence between $n - Kummer$ extension T/L contained in $\overline{L}$ and the finite subgroups of $L^\times/(L^\times)^n$. The correspondence maps T/L to $\frac{L^\times \cap T^{\times n}}{L^{\times n}}$, and maps $A \subset L^\times/L^{\times n}$ to $L[\sqrt[n]{a}]$. Moreover, when T/L and A correspond each other, then $Gal(T/L)$ and A related by the Kummer Pairing.*

Proof. Let $f(A) = L[\sqrt[n]{a}]$, where A is subgroup of $L^\times/L^{\times n}$ and $a \in A$, and $g(T/L) = L^\times \cap T^{\times n}/L^{\times n}$ but $g(f(A)) = A$ by the last theorem.

We know that any T/L is of the form $f(A)$ for some A. Therefore $f(g(K/F)) = f(g(f(A))) = f(A) = T/L$ □

Now, we will prove some useful lemmas using the fixed notation. These lemmas are useful because we can use annihilators of $Gal(H_1/F)$, $Gal(H_2/H_1)$ and $Gal(H_3/H_2)$ to find an annihilator of $Gal(H_3/F)$. Recall $G = Gal(K/F)$

Lemma 53. *1. For all $\sigma \in G$, $(\sigma - 1)Gal(H_1/F) = 0$.*

2. $m(F)Gal(H_3/H_1) = 0$

Proof. 1. We have the following exact sequence $0 \to Gal(H_1/F) \to Gal(H_1/K) \to Gal(F/K) \to 0$.

F_1 is abelian over K, therefore H_1 is also abelian over K. Hence G acts trivially on $Gal(H_1/F)$

2. Define $L = H_3(\mu_{Nm(F)}) = H_3F_1$. Then, $L \subset F_3 \subset F_1((F^\times)^{1/N})$.

Using Kummer Theory, we have that $Gal(L/F_1) \cong Hom(W, \mu_n)$, where W is some subgroup of $\frac{F^\times}{F^\times \cap (F_1^\times)^N}$

On the other hand, L is abelian over F, so $Gal(F_1/F)$ acts trivially on $Gal(L/F_1)$.

From the isomorphism and the action, $Gal(L/F_1) \cong Hom(W, \mu_n)^{Gal(F_1/F)} = Hom(W, \mu_n \cap \mu_F)$. Therefore, $m(F)Gal(L/F_1) = 0$.

By Galois Theory, we have $Gal(L/F_1) \cong Gal(H_3/H_1)$ So we have proved (2).

□

Let $\chi : G \to (\mathbb{Z}/m(F)\mathbb{Z})^{\times}$ denote the character giving the action of G on μ_F. For any divisor d of $m(F)$, define an involution γ of $(\mathbb{Z}/d\mathbb{Z})[G]$ by $\gamma(\sigma) = \chi(\sigma)\sigma^{-1}$.

Lemma 54. *Let $\mathcal{A}$ be the annihilator in $(\mathbb{Z}/N\mathbb{Z})[G]$ of $\frac{\ker\alpha}{\mu_F\cap\ker\alpha}$. Then, $\gamma(\mathcal{A} \mod (m(F), N))$ annihilates $Gal(H_2/H_1)$*

Proof. Again, we use Kummer Theory to obtain that $Gal(F_2/F_1) \cong Hom(X, \mu_N)$, where X is a quotient of $\ker(\alpha)/(\mu_f \cap (\ker(\alpha)))$.

We also know that there is a natural surjection of $Gal(F_2/F_1) \to Gal(H_2/H_1)$. Therefore, $Gal(H_2/H_1) \cong Hom(Y, \mu_N)$, for some submodule Y of X.

By the last lemma, $m(F)Gal(H_2/H_1) = 0$, then $Gal(H_2/H_1) \cong Hom(Y, \mu_F\cap \mu_F)$.

Now, take $r \in \mathcal{A}$. Then, $r = \sum r_\sigma \sigma$. By definition of $\mathcal{A}$, r annihilates Y. The isomorphism implies that $\sum \chi(\sigma) r_\sigma \sigma^{-1} = \gamma(r \mod (m(F), N))$. □

Lemma 55. *1. For all $\sigma \in G$, $(\sigma - \chi(\sigma))Gal(H_3/H_2) = 0$*

2. If $\mathcal{O}_K^{\times}$ is finite or $\mathcal{O}_K^{\times}(\mathcal{O}_F^{\times})^N/(\mathcal{O}_F^{\times})^N \subset V$, then $H_3 = H_2$.

Proof. 1. The same argument used before gives $Gal(H_3/H_2) \cong Hom(Y, \mu_F)$, where Y is a some quotient of $\mathcal{O}_K^{\times}$.

Now, G acts trivially on Y and G acts on $Gal(H_3/H_1)$ via χ. Therefore, we have (1).

2. If $\mathcal{O}_K^{\times}$ is finite, then $(\mathcal{O}_K^{\times})^{1/N} \subset F_1$. Therefore, $F_2 = F_3$

Since α is trivial on V, hence it is trivial on $\mathcal{O}_K^{\times}(\mathcal{O}_F^{\times})^N/(\mathcal{O}_F^{\times})^N$. Therefore $(\mathcal{O}_K^{\times})^{1/N} \subset F_2$

In both cases, $H_3 = H_2$.

□

3.3 Cyclotomic Units and Cyclotomic Fields

In this chapter, we will use the main theorem of this thesis and the result from previous chapter to obtain theorem related with Thaine's theorem.

Let $F = \mathbb{Q}(\mu_m)^+$ the maximal real subfield of the field of m^{th} roots of units. Define the group $\mathcal{E}'_{cycl}$ of cyclotomic numbers of F to be the group generated by $\{(1-\zeta)(1-\zeta^{-1}) | \zeta \in \mu_m, \zeta \neq 1\}$, and define the cyclotomic units by

$$\mathcal{E}_{cycli} = \mathcal{E}'_{cycl} \cap \mathcal{O}_F^\times$$

Theorem 56. *$\mathcal{E}_{cycl} \subset \mathcal{C}$.*

Proof. From Class Field Theory, for any odd prime q such that $q \equiv \pm 1(\mod m)$ splits completely.

We know that the ray class group of the field E for $\overline{m}$($\overline{m}$ is a non-zero principal ideal of E) is $\mathcal{I}_E(\overline{m})/\mathcal{P}_{E,\overline{m}}$, where $\mathcal{I}_{E,\overline{m}} = \{\overline{a} \in \mathcal{I}_{E,\overline{m}} | ord_t a = 0 \forall t \mid \overline{m}\}$ and $\mathcal{P}_E = \{principal \quad ideals \quad in \quad \mathcal{I}_E\}$.

Now, the ray class group for $\mathbb{Q}$ and q is $R_{\mathbb{Q},\overline{q}} \cong (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. Therefore the Ray Class field is $\mathbb{Q}(\mu_q)^+$. According to the notation already established $F(q) = F\mathbb{Q}(\mu_q)^+$

Let ζ be any m-th root of unity. We define $\epsilon = (1-\zeta)(1-\zeta^{-1})$. $\epsilon \in \mathcal{E}_{cycli}$ by definition.

Define $u = (1-\zeta\zeta_q^{-1})(1-\zeta\zeta_q)(1-\zeta^{-1}\zeta_q^{-1})(1-\zeta^{-1}\zeta_q)$.

$N_{F(q)/F}(u) = (1-\zeta^q)(1-\zeta^{-q})/(1-\zeta)(1-\zeta^{-1}) = 1$. Therefore u is a global unit in $F(q)$

On the other hand, $q \equiv (1-\zeta^2)(1-\zeta^{-2}) = \epsilon^2$ modulus any prime above q.

Now, by definitions, $\mathcal{E}_{cycl} \subset \mathcal{C}$. □

The next theorem is related to Thaine's theorem.

Theorem 57. *Let $F = \mathbb{Q}(\mu_m)^+$. If $\alpha : \mathcal{O}_L \to \mathbb{Z}[Gal(F/\mathbb{Q})]$ is any $Gal(F/\mathbb{Q})-$equivariant map then $4\alpha(\mathcal{E}_{cycl})$ annihilates the ideal class group of F.*

Proof. To apply result from the last section, take $K = \mathbb{Q}$, arbitrary N, $V = \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^N$, $A = Cl(F)/NCl(F)$.

$\alpha_N : \mathcal{O}_F^\times \to \mathbb{Z}/(N\mathbb{Z})[Gal(F/\mathbb{Q})]$ the map induced by α.

Since $K = \mathbb{Q}$, $\mathcal{O}_K^\times = \pm 1$. $m(F) = 2$ since F is real. Furthermore, by last theorem, $\mathcal{E}_{cycl} \subset \mathcal{C}$.

Claim: $H_1 = F$. It means that F_1 does not have non-trivial everywhere-unramified extension of F.

Proof: Recall that $F_1 = \mathbb{Q}(\mu_n)$ with n divisible by m. Since $H_1 = F_1 \cap H_A$, we need to show that F there is no non-trivial everywhere unramified extension in F_1.

First, note that $Gal(F_1/F) \cong \{a \in (\mathbb{Z}/n\mathbb{Z})^\times | a \equiv \pm 1 \mod m\}$.

Remember from Algebraic Number Theory that the order of inertia group is the ramification degree and that primes ramify completely over the field fixed by inertia group.

Therefore, for each p prime, we have the inertia group of p in F_1/F is $\{a \in (\mathbb{Z}/n\mathbb{Z}^\times) | a \equiv \pm 1 mod(m),\ a \equiv 1 \mod (n/p^t)\}$ where t is the exactly power that divides n. Applying the Chinese remainder theorem and the fact that abelian group are products of cyclic groups, we have that inertia groups generate $Gal(F_1/F)$. Any subfield L, $F \subset L \subset F_1$ is ramified because this field corresponds to some subgroup that is contained or has subgroup contained in inertia group of some p.

We know from previous lemmas that $m(F)Gal(H_3/H_1) = 0$, therefore $2Gal(H_3/F) = 0$.

Note that if $J \in \mathbb{Z}[G]$ annihilates $Gal(H_3/F)$, then J annihilates A/A'.

Now, $V \cap \mathcal{C} = \mathcal{E}_{cycli}$. By our main theorem, $4\alpha(\mathcal{E}_{cyclic})$ annihilates $Cl(F)/NCl(F)$. Since N is arbitrary, we have the result.

□

3.4 Specializations of the main theorem

In this section, we will prove two theorems that can be more useful in practice. For example, in [19] these two theorems are used.

Fix a rational prime p and let E be an intermediate number field, $K \subset E \subset F$ with $H = Gal(F/E)$ of order prime to p.

Let $\rho : H \to GL_k(\mathbb{Z}_p)$ be an irreducible representation.

Let M be a $\mathbb{Z}[H]-$ module and $\hat{M} = \varprojlim M/p^n M$ the p-adic completion of M. We define $M^\rho = e_\rho \hat{M}$, the ρ-eigenspace, where $e_\rho \in \mathbb{Z}[H]$ is the idempotent $\frac{1}{|H|} \sum Tr(\rho(\sigma^{-1}))\sigma$. Moreover, we write $\check{\rho} = \rho(\sigma^{-1})$.

If $\mu_p \subset F$, we will write ω for the $\mathbb{Z}_p^\times$ valued character giving the action of H on μ_p.

Remember that for any ring R, the augmentation ideal of $R[G]$ is the ideal generated by $\{\sigma - 1|\sigma \in G\}$. Or equivalently it is the kernel of $R[G] \to R$ with $\sum rg \to \sum r$ by proposition 23.

Theorem 58. *Suppose p is a rational prime, ρ a non-trivial irreducible $\mathbb{Z}_p$-representation of H, and W a submodule of $(\mathcal{O}_F^\times)^\rho$ such that $(\mathcal{O}_F^\times)^\rho/W$ has no $\mathbb{Z}_p$-torsion. Suppose $1 \leq n \leq \infty$ and either $p \neq 2$, or $n = 1$, or $\mu_4 \subset F$.*

Let $\alpha : W \to (\mathbb{Z}_p/p^n\mathbb{Z}_p)[G]^\rho$ be any $G - module$ map. Then

1. *$m(F)\alpha(\mathcal{C}^\rho \cap W)$ annihilates $Cl(F)^\rho/p^nCl(F)^\rho$*
2. *If $\mu_p \subset F$, $\mathcal{O}_K^\times$ is finite, and $\rho \neq \check{\rho} \otimes \omega$, then $\alpha(\mathcal{C}^\rho \cap W)$ annihilates $Cl(F)^\rho/p^nCl(F)$.*
3. *If $\mu_p \subset F$, $\rho \neq \omega$, and $\rho \neq \check{\rho}\otimes\omega$, then $\alpha(\mathcal{C}^\rho\cap W)$ annihilates $Cl(F)^\rho/p^nCl(F)^\rho$.*
4. *If $p = 2$, $n \geq 2$ and $\mu_4 \subset F$, then the first three assertion hold with $\alpha(\mathcal{C}^\rho \cap W)$ replaced by $2\alpha(\mathcal{C}^\rho \cap W)$.*

Proof. We will separate the proof in cases:

1. n finite and either $p \neq 2$, or $n = 1$, or $\mu_4 \subset F$ and fix $N = p^n$.

   By hypothesis, $(\mathcal{O}_F^\times)^\rho/W$ is torsion-free. So, W/W^N injects into $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^N$.

   We would like to apply lemmas from section 2, hence we set $V = W/W^N$, $\alpha_N : V \to (\mathbb{Z}/N\mathbb{Z})[G]$ the induced map and $A = (Cl(F))^\rho/NCl(F)^\rho$.

   Since, $\rho \neq 1$ and ρ is $\mathbb{Z}_p-$representation, $e_\rho = \frac{1}{|H|}\sum \chi(\sigma^{-1})\sigma$. Now, note that $\frac{1}{|H|}\sum \chi(\sigma^{-1}) = 0$.

   Therefore $(\mathbb{Z}/N\mathbb{Z})[G]^\rho$ is contained in the augmentation ideal, thus it is contained in the ideal generated by $\{\sigma - 1|\sigma \in G\}$.

   Applying lemma 53, $(\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_1/F) = 0$ and $m(F)Gal(H_3/H_1) = 0$. Therefore, $m(F)(\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_3/F) = 0$.

   Now, combining the main theorem with last sentence, we have $m(F)(\mathbb{Z}/N\mathbb{Z})[G]^\rho\alpha(\mathcal{C}^\rho\cap W)A = 0$.

   On the other hand, $(\mathbb{Z}/N\mathbb{Z})[G]^\rho A = A^\rho = A$ since ρ is idempotent.

   Thus, we have (1)

2. Now suppose in addition that $\mu_p \subset F$. Let χ be the $(\mathbb{Z}/m(F)\mathbb{Z})$ character of the action of G on μ_F. This character is related to ω by $\chi|_H \equiv \omega(\mod (m(F)\mathbb{Z}_p))$

   If $\rho \neq \omega$ or if $\mathcal{O}_K^\times$ is finite, then, we have $(\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_3/H_2) = 0$.

   If, in addition, $\rho \neq \check{\rho} \otimes \omega$, then $(\mathbb{Z}/N\mathbb{Z})[G]^{\rho\otimes\omega}$ annihilates V. Applying lemma 54, $\gamma(((\mathbb{Z}/N'\mathbb{Z})[G]^\rho$ annihilates $Gal(H_2/H_1)$, where $N' = gcd(N, m(F))$. We also have that $\gamma((\mathbb{Z}/N'\mathbb{Z})[G]^{\check{\rho}\otimes\omega}) = (\mathbb{Z}/N'\mathbb{Z})[G]^\rho$. Hence, $(\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_2/H_1) = 0$.

   Therefore, we have $(\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_1/F) = (\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_3/H_2) = (\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_2/H_1) = 0$. And since, $((\mathbb{Z}/N\mathbb{Z})[G]^\rho)^3 = \mathbb{Z}/N\mathbb{Z}[G]^\rho$, $(\mathbb{Z}/N\mathbb{Z})[G]^\rho Gal(H_3/F) = 0$.

   So, by our main theorem, $\alpha(\mathcal{C}^\rho \cap W)A = \alpha(\mathcal{C}^\rho \cap W)(\mathbb{Z}/N\mathbb{Z})[G]^\rho A = 0$.

3. If $n = \infty$, the result is immediate since $Cl(F)^\rho$ is finite.

4. If $p = 2, n \geq 2, \mu_4 \not\subseteq F$ is proved exactly the same way using the factor of 2 in our main theorem.

□

Let S be a finite set of rational primes. We define $M_S = \varprojlim M/nM$, where n are the integers divisible only by primes in S.

In particular, if M is a finite abelian group, then M_S is the product over $p \in S$ of the $p - Sylow$ subgroups of M. Also, $\mathbb{Z}_S = \prod_{p \in S} \mathbb{Z}_p$.

Lemma 59. *Fix a set S of rational primes and let W be a $Z_S[G] - module$ which contains a cyclic $\mathbb{Z}_S$ submodule of finite index. Let $\alpha : W \to \mathbb{Z}_S[G]$ be any $G - homomorphism$ and for any positive integer N let $\alpha_N : W/NW \to (\mathbb{Z}_S/N\mathbb{Z}_S)[G]$ be the inducted map. Then for every N, $\alpha(W)$ annihilates $(ker\alpha_N)/W_{tors}$, where W_{tors} denotes the $\mathbb{Z}$-torsion in W.*

Proof. Fix $w \in W$ and $n \in \mathbb{Z}^*$ such that $nW \subset \mathbb{Z}_S[G]w$. Also fix N a positive integer. Choose $x \in W$ and $y \in \alpha^{-1}(N\mathbb{Z}_S[G])$

We want to show that $\alpha(x)y \in W_{tors} + NW$.

We can find f and $g \in \mathbb{Z}_S[G]$ such that $nx = fw$ and $ny = gw$. Then $n\alpha(x)ny = \alpha(nx)gw = \alpha(fw)gw = \alpha(gw)fw = n\alpha(y)nx$. Thus, $\alpha(x)y -$

$\alpha(y)x \in W_{tors}$.

Therefore $\alpha(x)y \in W_{tors} + \alpha(y)W \subset W_{tors} + NW$. □

Fix a finite set S of rational primes and write J for the augmentation ideal of $\mathbb{Z}_S[G]$. We have already defined γ the involution of $(\mathbb{Z}_S/m(F)\mathbb{Z}_S)[G]$, then for any ideal $\mathcal{I}$ of $\mathbb{Z}_S[G]$ containing $m(F)\mathbb{Z}_S[G]$ we write $\gamma(\mathcal{I})$ for the lift of $\gamma(\mathcal{I}mod(m(F)))$ from $(\mathbb{Z}_S/m(F)\mathbb{Z}_S)$ to $\mathbb{Z}_S[G]$.

Theorem 60. *Suppose W is a $G-submodule$ of $(\mathcal{O}_F^\times)_S$ such that*

(a) W contains a submodule of finite index which is cyclic over $\mathbb{Z}_S[G]$

(b) $(\mathcal{O}_F^\times)_S/W$ has no $\mathbb{Z}$-torsion, and

(c) $(\mathcal{O}_K^\times)_S \subset W$ and $\alpha : W \to \mathbb{Z}_S[G]$ is a $G-homomorphism$ which is trivial on $(\mathcal{O}_K^\times)_S$. Then,

1. *If $2 \notin S$ or $\mu_4 \in F$, then $J\gamma(\alpha(W) + m(F)\mathbb{Z}_S[G])\alpha(\mathcal{C}_S \cap W)$ annihilates $Cl(F)_S$.*

2. *In general, $2J\gamma(\alpha(W) + m(F)\mathbb{Z}_S[G])\alpha(\mathcal{C}_S \cap W)$ annihilates $Cl(F)_S$.*

Proof. 1. Set N a positive integer such that N is divisible only by prime in S. By (b), $W \cap (\mathcal{O}_F^\times)_S^N = W^N$. To apply result from section 2, consider $V = W/W^N \subset \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^N, \alpha_N : V \to (\mathbb{Z}_S/N\mathbb{Z}_S)[G]$ and $A = Cl(F)_S/NCl(F)_S$.

J annihilates $Gal(H_1/F)$ since J is generated by $\{\sigma - 1 | \sigma \in G\}$.

Lemma 55 shows that $H_2 = H_3$. Combining lemma 59 with Lemma 54, we obtain $\gamma(\alpha(W) \mod (m(F), N))$ annihilates $Gal(H_2/H_1)$.

If $2 \notin S$ or $\mu_4 \subset F$, applying our main theorem, we have

$$J\gamma(\alpha(W) + m(F)\mathbb{Z}_S[G])\alpha(\mathcal{C}_S \cap W)Cl(F)_S \subset NCl(F)_S$$

Now, we choose $N = |Cl(F)|$ to obtain (1).

(2) is proved the exact same way using the factor 2 from theorem.

□

Corollary 61. *Let W and α be as in last theorem. Let B any subquotient of $Cl(F)_S$ satisfying $JB = B$. Then:*

1. *If $\mu_4 \subset F$ or $2 \notin S$ then $\gamma(\alpha(W) + m(F)\mathbb{Z}_S[G])\alpha(\mathcal{C}_S \cap W)$ annihilates B.*

2. *In general, $2\gamma(\alpha(W) + m(F)\mathbb{Z}_S[G])\alpha(\mathcal{C}_S \cap W)$ annihilates B.*

Proof. Direct from the theorem 60. □

3.5 Proof of Main Theorem

The proof of the main theorem will be a consequence of two other theorems.

For any finite extension M of F we define

$$\mathcal{E} = \{u \in \mathcal{O}_M^\times | N_{M/F}(u) = 1\}$$

This first theorem was almost done in the first section of previous chapter.

We will need the following lemma:

Lemma 62. *If any prime p is totally tamely ramified in M/F, then Gal(M/F) is cyclic*

Proof. Since p is totally ramified its decomposition group is isomorphic to its inertia group and isomorphic to $Gal(M/F)$.

Now, we need to remember some definitions and properties of ramification groups:

The ramification groups of G relative to p for our case are:

$$G_i = \{s \in Gal(M/F)| \quad s(x) \equiv x \quad mod \quad p^{i+1}\}$$

G_0 is the inertia group and G_1 is trivial since p is tamely ramified. From local field theory, G_0/G_1 is always cyclic, but since G_1 is trivial, we have that G_0 is cyclic.

□

Remember the fixed notation in the beginning of the chapter. $G = Gal(K/F)$.

Theorem 63. *Let q be a prime of K that splits completely in F. Let M be a finite extension of F, abelian over K, such that in M/F all primes above q are* *totally tamely ramified and no others primes ramify. Write q_M for the product of all primes of M above q, and let $\mathcal{A}$ be the annihilator in $(\mathbb{Z}/(N(q)-1)\mathbb{Z})[G]$ of the cokernel of the reduction map*

$$\varphi' : \mathcal{E}(M) \to (\mathcal{O}_M/q_M)^\times$$

Define $w = (N(q)-1)/[M : F]$ Then $\mathcal{A} \subset w(\mathbb{Z}/(N(q)-1)\mathbb{Z})[G]$ and for every prime $\overline{q}$ above q, $w^{-1}\mathcal{A}$ annihilates the ideal class of $\overline{q}$ in $Cl(F)/[M : F]Cl(F)$.

Remark: 3. Remember that tamely ramified means that the ramification index is prime to the residue field characteristic.

Also, $cokernel\varphi' = \frac{(\mathcal{O}_M/q_M)^\times}{Image \quad of \quad reduction \quad map}$

Proof. All primes of F above q totally ramify in M/F, so G acts on $(\mathcal{O}_M/q_M)^\times$ and on the set of primes of M above q.

1. Primes above q in K are $\overline{q}^\sigma$ for all $\sigma \in G$.

2. Primes above $\overline{q}$ in M are $[q]^\sigma$ for all $\sigma \in G$

Fix any prime $\overline{q}$ above q. Choose an element $\pi \in M$ such that π has order 1 at $[q]$. It means that $\pi = [q]y$. We define

$$\varphi : Gal(M/F) \to (\mathcal{O}_m/[q])$$
$$g \mapsto \frac{\pi^g}{\pi}$$

As $\overline{q}$ totally tamely ramifies in M/F, then φ is injective.

Now, take $\tau \in Gal(M/F)$ such that τ generates $Gal(M/F)$.(It is possible due to the last lemma). Therefore, $\frac{\pi^\tau}{\pi}$ has order $[M : F]$ in $(\mathcal{O}_M/[q])^\times$.

Choose $u \in (\mathcal{O}_M/q_M)^\times$ such that

$$\begin{cases} u^w \equiv \frac{\pi^\tau}{\pi}, & \mod \quad [q] \\ u \equiv 1, \quad \mod \quad [q]^\sigma & \forall \sigma \neq 1 \end{cases}$$

Note that it implies that order of u is $N(q)-1$.

Since $\mathcal{A}$ annihilates the cokernel of reduction map, then exist $\theta \in \mathcal{A}$ such that

$$u^\theta \equiv \epsilon \mod q_M \tag{3.1}$$

for some $\epsilon \in \mathcal{E}(M)$.

By Hilbert Theorem 90 there exists $\alpha \in M^{\times}$ such that $\frac{\alpha^{\tau}}{\alpha} = \epsilon$. So, $\langle \alpha^{\tau} \rangle = \langle \alpha \rangle$. Since only primes above q ramify in M/F we have that

$$\langle \alpha \rangle = I\mathcal{O}_M \prod a_{\sigma}[q]^{\sigma}.$$

where I is an ideal prime to q. Applying $N_{M/F}$, we have that

$$N_{M/F}(\alpha) = I^{[M:K]}\overline{q}^{\sum a_{\sigma}\sigma} \text{ and}$$
$$\overline{q}^{\sum a_{\sigma}\sigma} = 0 \text{ in } Cl(F)/[M:F]Cl(F)$$

$a_{\sigma} = ord_{[q]^{\sigma}}(\alpha)$. For any $\sigma \in G$, we can extend σ to $\overline{\sigma} \in Gal(M/K)$.

$ord_{[q]^{\sigma}}\pi = 1$, so we can write $\alpha = \beta(\pi^{\overline{\sigma}})^{a_{\sigma}}$, where β is a unit at $[q]^{\sigma}$.

τ belongs to inertia group of $[q]^{\sigma}$, then $\beta^{\tau} \equiv \beta \mod [q]^{\sigma}$. Therefore we have

$$\epsilon = \frac{\alpha^{\tau}}{\alpha} = \frac{\beta^{\tau}\pi^{\overline{\sigma}a_{\sigma}}}{\beta\pi^{\overline{\sigma}a_{\sigma}}} \equiv (\frac{\pi^{\tau}}{\pi})^{a_{\sigma}\sigma} \mod [q]^{\sigma} \tag{3.2}$$

Using the conditions of u, we obtain

$$\epsilon \equiv u^{[w\sum a_{\sigma}\sigma]} \mod q_m \tag{3.3}$$

On the other hand, we can use (3.1) and the fact that annihilator of u in $\mathbb{Z}[G]$ is $(N(q)-1)\mathbb{Z}[G]$ to obtain:

$$\theta \equiv w\sum a_{\sigma}\sigma \mod (N(q)-1) \tag{3.4}$$

Therefore, $\mathcal{A} \subset w(\mathbb{Z}/N(q)-1\mathbb{Z})$.

Since $\overline{q}^{\sum a_{\sigma}\sigma} = 0$ in $Cl(F)/[M:F]Cl(F)$ and (3.4) we have that $w^{-1}A$ annihilates $\overline{q}$ in $Cl(F)/[M:F]Cl(F)$. □

Again, remember the definition from first section.

Now define

$$H'' = H_A \cap F(\mu_N, V^{1/N}, (\mathcal{O}_K^{\times})^{1/N}) \supseteq H'$$

Also, $A'' = Gal(H_A/H'') \subset A' = Gal(H_A/H') \subset A$.

For the next theorem, we will need a definition from Commutative Algebra.

Definition 34. A $R-module$ M is injective if given $R-modules$ X and Y, $f: X \to Y$ an injective module homomorphism and $g: X \to M$ is an arbitrary module homomorphism, then there is $h : Y \to M$ such that $h \circ f = g$.

Theorem 64. *Fix N, V and A as in the first section of this chapter.*

Suppose $\alpha : V \to (\mathbb{Z}/N\mathbb{Z})[G]$ is a $G - module$ trivial on $[\mathcal{O}_K^\times(\mathcal{O}_F^\times \cap (F(\mu_N)^\times)^N)] \cap V$. Then there is a $\mathbb{Z}[G]$-generator C_0 of A'/A'' such that for any $C \in A'$ which projects to C_0 modulo A'', there are infinitely many primes $\overline{q}$ of F of absolute degree one satisfying

1. *$[q] = C$, where $[q]$ is the projection of the ideal class $\overline{q}$ on A*
2. *$N|(N(q) - 1)/w(q)$*
3. *There is a map $\varphi : (\mathcal{O}_F/q\mathcal{O}_F) \to (\mathbb{Z}/(N(q) - 1)\mathbb{Z})[G]$ such that the following diagram commutes:*

$$\begin{tikzcd}
V \arrow[r, "\alpha"] \arrow[d] & (\mathbb{Z}/N\mathbb{Z}[G]) \\
(\mathcal{O}_F/q\mathcal{O}_F)^\times \otimes (\mathbb{Z}/N\mathbb{Z}[G]) \arrow[ur, "\tilde{\varphi}"'] &
\end{tikzcd}$$

Proof. Define the following tower of fields:

$$\begin{tikzcd}
F'' = F'(V^{1/N}) \arrow[d, dash] \\
F' = F(\mu_N, (\ker\alpha)^{1/N}, (\mathcal{O}_K^\times)^{1/N}) \arrow[d, dash] \\
F(\mu_N) \arrow[d, dash] \\
F
\end{tikzcd}$$

Define $G_N = Gal(F(\mu_N)/K)$. Applying Kummer theory, we obtain $Gal(F''/F') \cong Hom(B, \mu_N)$ as G_N modules, where

$$\begin{aligned}
B &= V/(ker(\alpha))[\mathcal{O}_K^\times(\mathcal{O}_F^\times \cap (F(\mu_N)^\times)^N)] \cap V) \\
&= V/Ker(\alpha) \\
&\cong Image(\alpha) \subset (\mathbb{Z}/N\mathbb{Z})[G]
\end{aligned}$$

It implies that $Gal(F''/F')$ is cyclic over $(\mathbb{Z}/N\mathbb{Z})[G_N]$

Since $Gal(F''/F')$ is cyclic over G_N we can take γ a generator of $Gal(F''/F')$.

Now, note that $Gal(F''/F')$ maps subjectively to $Gal(H''/H')$, then if we restrict γ to H'' we obtain C_0 such that C_0 generates $Gal(H''/H') = A'/A''$ over G_N. The action of G_N on A factors through to G, then C_0 generates A'/A'' over G.

Let C be any element of A' such that the class of C in A'/A'' is C_0. Let β be an element of $Gal(F''H_A/H)$ such that

$$\begin{cases} \beta\mid_{F''}=\gamma \\ \beta\mid_{H_A}=C \end{cases}$$

The choice of this β is possible because $\gamma|_{H''} = C_0 = C|_{H''}$.

Now, let $\overline{q}$ be any prime of inertia degree one, not dividing N, whose Frobenius lies in the conjugacy class of β. The Chebotarev density theorem guarantees the existence of this element. $q = K \cap \overline{q}$

Claim: $\overline{q}$ satisfies 1,2 and 3.

Proof:

1) $[q]$ is the Frobenius of $\overline{q}$ in $Gal(H_A/F) = A$. But $\overline{q}$ by construction is in the same conjugacy of β, therefore $[q] = \beta|_{H_A} = C$.

2) $\beta|_{F''} = \gamma \Rightarrow \beta|_{F'} = 1$. Therefore, q splits completely in F'/K.

q does not divide N, so q splits completely in $K(\mu_N)/K$. Therefore, $N||(\mathcal{O}_K/q)^\times = N(q) - 1$.

Since q splits completely in $K((\mathcal{O}_K^\times)^{1/n})$, then the reduction map of $\mathcal{O}_K^\times$ to $(\mathcal{O}_K/q)^\times$ is contained in $((\mathcal{O}_K/q)^\times)^N$. Therefore, $N|(\mathcal{N}(q) - 1)/w(q)$.

3) Let ψ be the map from V to $(\mathcal{O}_F/q\mathcal{O}_F)^\times \otimes (\mathbb{Z}/N\mathbb{Z})$. Let $z \in V$,

$z \in \ker(\psi) \iff z$ is an $N-th$ power modulo $\overline{q}^\sigma$ for all $\sigma \in G$.

On other hand, z is $N-th$ power modulo $\overline{q}^\sigma$ for all $\sigma \in G \iff \overline{q}^\sigma$ splits completely in $F(z^{1/N})/F$.

But, $\overline{q}^\sigma$ splits completely in $F(z^{1/N})/F$ for all $\sigma \in G \iff \overline{q}$ splits completely in $F'(z^{1/n}) \iff \gamma^\sigma$ is trivial on $F'(z^{1/N})$ for all $\sigma \in G_N$

But γ fixes F', so γ^σ is trivial on $F'(z^{1/N})$ for all $\sigma \in G_N \iff z^{1/N} \in F'$.

By definition of F', $z^{1/n} \in F' \iff z \in Ker(\alpha)$.

Since, $(\mathbb{Z}/N\mathbb{Z})[G]$ is injective over itself, there is a map $\tilde{\varphi} : (\mathcal{O}_F/q\mathcal{O}_F)^\times \otimes (\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})[G]$ such that $\alpha = \tilde{\varphi} \circ \psi$.

$$\begin{tikzcd}
V \arrow[r, "\alpha"] \arrow[d] & (\mathbb{Z}/N\mathbb{Z}[G]) \\
(\mathcal{O}_F/q\mathcal{O}_F)^\times \otimes (\mathbb{Z}/N\mathbb{Z}[G]) \arrow[ur, "\tilde{\varphi}"'] &
\end{tikzcd}$$

We need to lift $\tilde{\varphi}$ to $\varphi : (\mathcal{O}_F/q\mathcal{O}_F)^\times \to (\mathbb{Z}/(N(q)-1)\mathbb{Z})$.

$(\mathcal{O}_F/q\mathcal{O}_F)^\times$ is free of rank one over $(\mathbb{Z}/(N(q)-1)\mathbb{Z})$(u defined in theorem 63 is an example of generator). Then, we can do this lift.

□

Lemma 65. *Suppose N is a prime power, then*

1. *If $4 \nmid N$ or $\mu_N \subset F$, then $F^\times \cap (F(\mu_N)^\times)^N = (F^\times)^N$*
2. *If $4 \mid N$ or $\mu_4 \not\subset F$, then $[F^\times \cap (F(\mu_N)^\times)^N : (F^\times)^N] \leq 2$.*

Proof. Define $G_N = Gal(F(\mu_N)/F)$.

We have the following exact sequence:

$$0 \to \mu_N \to F(\mu_N)^\times \xrightarrow{N} (F(\mu_N)^\times)^N \to 0.$$

It gives the long exact sequence

$$0 \to \mu^{G_N} \to F(\mu_N)^{G_N} \to ((F(\mu_N)^\times)^N)^{G_N} \to H^1(G_N, \mu_N) \to H^1(G_N, F(\mu_N)^\times) \to 0$$

We can rewrite as

$$0 \to \mu_N^{G_N} \to F^\times \to F^\times \cap (F(\mu_N)^\times)^N/(F^\times)^N \to H^1(G_N, \mu_N)$$

Therefore, we have the following isomorphism:

$$(F^\times \cap (F(\mu_N)^\times)^N)/(F^\times)^N \cong H^1(Gal(F(\mu_N)/F), \mu_N) \cong H^1(X, \mathbb{Z}/N\mathbb{Z})$$

where $X \subset (\mathbb{Z}/N\mathbb{Z})^\times$.

1. If $4 \nmid N$ or $\mu_4 \subset F$, then X is cyclic. It is due to the fact that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for p odd. In this case, $H^1(X, \mathbb{Z}/N\mathbb{Z}) = 0$

2. If $4 \mid N$ or $\mu_4 \not\subseteq F$, there are two possible cases due to $(\mathbb{Z}/2^N\mathbb{Z})$. X cyclic or not

   If X is cyclic, then $|H^1(X, \mathbb{Z}/N\mathbb{Z})| \leq 2$ If X is not cyclic, $X = \{\pm 1\} \times Y$ with $Y \subset 1 + 4(\mathbb{Z}/N\mathbb{Z})$. Now, by inflation-restriction sequence, we have

$$0 \to H^1(\{\pm 1\}, (\mathbb{Z}/N\mathbb{Z})^Y) \to H^1(X, \mathbb{Z}/N\mathbb{Z}) \to H^1(Y, \mathbb{Z}/N\mathbb{Z}) = 0$$

□

Using the same notation of the first section of this chapter. Now we can prove our main theorem:

Theorem 66. *Let N, V, α, A and $\mathcal{C}$ as described in the first section. If $4 \nmid N$ or $\mu_4 \subset F$, then $\alpha(\mathcal{C} \cap V)$ annihilates A'. In general, $2\alpha(\mathcal{C} \cap V)$ annihilates A'*

Proof. Without loss of generality we will assume that N is a prime power. We can do it because the general case follows by splitting N, V, α and A into their p-primary parts.

Define

$$\alpha' = \begin{cases} \alpha \quad if \quad 4 \nmid N \quad or \quad \mu_4 \subset F \\ \qquad\qquad 2\alpha, \quad otherwise \end{cases}$$

α is trivial on $\mathcal{O}_K^\times \cap V$. The last lemma applied to $[\mathcal{O}_K^\times(\mathcal{O}_F^\times \cap (F(\mu_N)^\times)^N)]$ gives us that α' is trivial on $[\mathcal{O}_K^\times(\mathcal{O}_F^\times \cap (F(\mu_N)^\times)^N)] \cap V$.

It means that α satisfies the last theorem. Therefore we can choose C the $\mathbb{Z}[G]$-generator of A'/A'' as in the last theorem and can choose $\overline{q}$ of F of absolute degree one satisfying the last theorem and such that $\mathcal{C} \subset \mathcal{C}(q)$, where $q = \overline{q} \cap K$.

The Hilbert Class Field of K is contained in F, then any extension $F' \supseteq F$ is ramified over K. Now, let be $F(q) = K(q)F$. $F(q)/F$ is totally, tamely ramified at all primes of F above q and unramified everywhere else and $[F(q) : F] = \frac{N(q)-1}{w(q)}$

Now, we will apply the last theorem with $M = F(q)$.

Let φ be the map that satisfies the last theorem and define

$$\Phi : \mathcal{O}_{F(q)}^\times \to (\mathcal{O}_{F(q)}/\tilde{q})^\times \cong (\mathcal{O}_F/q\mathcal{O}_F)^\times \xrightarrow{\varphi} (\mathbb{Z}/(N(q)-1)\mathbb{Z})$$

Note that $(\mathcal{O}_{F(q)}/\overline{q})^{\times} \cong (\mathcal{O}_F/q\mathcal{O}_F)^{\times}$ because q has absolute degree 1.

Again, define $\mathcal{A}$ the annihilator in $(\mathbb{Z}/(N(q)-1)\mathbb{Z})[G]$ of the cokernel of the map $\mathcal{E}(q) \to (\mathcal{O}_{F(q)}/\tilde{q})^{\times}$.

$(\mathcal{O}_F/q\mathcal{O}_F)^{\times}$ is free-rank one over $(\mathbb{Z}/(N(q)-1)\mathbb{Z})$, therefore $\Phi(\mathcal{E}(q)) \subset A$.

On the other hand, $\Phi(\mathcal{C}^{w(q)}) \subset \Phi(\mathcal{E}(q))$. So, $w(q)\Phi(\mathcal{C}) \subset \mathcal{A}$. Applying theorem 63, $\Phi(\mathcal{C})$ annihilates the class of $\overline{q}$ in $Cl(F)/([N(q)-1]/w(q))\mathbb{Z}$.

Theorem 64 implies that $N \mid \frac{N(q)-1}{w(q)}$, so $\Phi(\mathcal{C})$ annihilates the class of $\overline{q}$ in $Cl(F)/NCl(F)$. Thus $\Phi(\mathcal{C})$ annihilates $[q] = C$ in A and by theorem 64 $\alpha'(\mathcal{C} \cap V)$ annihilates C in A.

It holds for every C in C_0. C_0 is an A'' coset contained in A'. Since C_0 generates A'/A'' over G, then the elements of this coset generate A' over G. Therefore $\alpha'(\mathcal{C} \cap V)$ annihilates A'.

□

3.6 Iwasawa Theory

This section is very technical, so we will give a sketch of the proofs and indicate where to find every details.

For this section we will need to fix some notation.

Fix p a rational prime and K a number field. Let $K_\infty = \cup K_n$ be an abelian extension containing the Hilbert Class Field of K such that $Gal(K_\infty/K) \cong \mathbb{Z}_p^d \times H$ and $Gal(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^d \times H$, where H is a finite group with order prime to p and d is a positive integer.

For each n, let A_n denote the $p-primary$ part of the ideal class group of K_n, $\mathcal{E}_n$ the group of global units of K_n, and $\mathcal{C}_n$ the group of special units of K_n/K.

$$\hat{\mathcal{E}}_n = \varprojlim_m (\mathcal{E}_n/(\mathcal{E}_n)^{p^m}).$$
$$\hat{\mathcal{C}} = \varprojlim_m (\mathcal{C}_n/\mathcal{C}_n^{p^m})$$

Also, $A_\infty = \varprojlim_n A_n$ and $\mathcal{E}_\infty = \varprojlim_n \hat{\mathcal{E}}_n$ (inverse limits with respect to the norm maps) and $\mathcal{C}_\infty\{(u_n) \in \mathcal{E}_\infty| \quad u_n \in \hat{\mathcal{C}}_n \forall n\}$

Write Λ for the Iwasawa algebra

$$\Lambda = \mathbb{Z}_p[[Gal(K_\infty/K)]] = \varprojlim \mathbb{Z}_p[Gal(K_n/K)]$$

Before we begin with statements about that relates Iwasawa Theory with our theorems, we will review concepts from Group Cohomology.

The group of *n-cochains* is the abelian group $C^n(G,A) := Maps(G^n, A)$ of maps of sets $f : G^n \to A$ under pointwise addition.

The $n-th$ coboundary map $d^n : C^n(G,A) \to C^{n+1}(G,A)$ is the homomorphism of the abelian group defined by

$d^n(f)(g_0,...,g_n) := g_0 f(g_1,...,g_n) - f(g_0g_1, g_2,...,g_1) + f(g_0, g_1g_2,...,g_n)... + (-1)^n f(g_0,...,g_{n-2}, g_{n-1}g_n) + (-1)^{n+1} f(g_0,...,g_{n-1})$.

The group $C(G,A)$ contains subgroups of $n-cocycles$ and $n-boundaries$ defined by

$$Z^n(G,A) := \ker d^n \text{ and } B^n(G,A) := Imd^{n-1}$$

Definition 35. The nth cohomology group of G with coeficients in A is the abelian group

$$H^n(G,A) := Z^n(G,A)/B^n(G,A)$$

Definition 36. The $i-th$ homology group $H_i(G,A)$ of a group G with coefficients in a $G-module$ A is defined to be the i-th homology group $H_i(G,A) = \ker d_i / Im(d_{i+1})$ in the complex

$$... \to \mathbb{Z}[G^3] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_2} \mathbb{Z}[G^2] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_1} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_0} 0$$

where $d_i = (g_0,...,g_i) = \sum_{j=0}^{i} (-1)(g_0,...,g_{j-1}, g_{j+1},...,g_i)$

Definition 37. The norm of element in $\mathbb{Z}[G]$ is $N_G = \sum g$. It induces a morphism $\hat{N}_G : A_G \to A^G$ where $A_G = A/I_G A$ with I_G the augmentation ideal of G.

We define $\hat{H}_0(G,A) = \ker \hat{N}_G$ and $\hat{H}^0 = coker \hat{N}_G$.

Definition 38. Let G be a finite group and A a $G-module$. For any $i \in \mathbb{Z}$, we define the ith Tate cohomology group by

$$\hat{H}^i(G,A) = \begin{cases} H_{-i-1}(G,A) & if \quad i \leq -2 \\ \hat{H}_0(G,A), & if \quad i = -1 \\ \hat{H}^0(G,A) & if \quad i = 0 \\ H^i(G,A) & if \quad i \geq 1 \end{cases}$$

Theorem 67. *Let $K_\infty = \cup K_n$ be as above. Fix an irreducible $\mathbb{Z}_p$-representation $\rho \neq 1$ of H and suppose that there are integers r and s such that for all pairs of integers $m \geq n$, $p^r \hat{H}^0(Gal(K_m/K_n), \mathcal{E}_m^\rho) = 0$ and $p^s \hat{H}^{-1}(Gal(K_m/K_n), \mathcal{E}_m^\rho) = 0$. Suppose in addition at least one of the following conditions is satisfied:*

1. *$\mu_p \nsubseteq K_\infty$; or*
2. *$\mu_p \subset K_\infty, \rho \neq \check{\rho} \otimes \omega$, and either $\rho \neq \omega$ or $\mathcal{O}_K^\times$ is finite; or*
3. *the number $m_p(K_\infty)$ of p-power roots of unity in K_∞ is finite*

Define t by $t = r$ if (1) or (2) holds, and otherwise $p^t = p^r m_p(K_\infty)$. If $\alpha : \mathcal{E}_\infty^\rho \to \Lambda^\rho$ is any $\Lambda - module$ map, then $p^t \alpha(\mathcal{C}_\infty^\rho)$ annihilates A_∞^ρ

Proof. Let n be large enough so that K_n contains the Hilbert Class Field of K.

Define J_n be the ideal generated by $\{\gamma - 1 | \gamma \in Gal(K_\infty/K_n)\}$. Therefore, $\lambda/J_n \cong \mathbb{Z}_p[G(K_\infty/K_n)]^\rho$

From α, we can define an equivariant $Gal(K_n/K){-}map$ $\alpha_n : \mathcal{E}_\infty^\rho / J_n \mathcal{E}_\infty^\rho \to \mathbb{Z}_p[Gal(K_n/K)]^\rho$.

There is a natural projection from $\mathcal{E}_\infty$ to $\hat{\mathcal{E}}_n$ that induces a map $\pi : \mathcal{E}_\infty^\rho / J_n \mathcal{E}_\infty^\rho \to \mathcal{E}_n^\rho$.

The map π fits into an exact sequence

$$0 \to \varprojlim_m \hat{H}^{-1}(Gal(K_m/K_n, \mathcal{E}_\infty^\rho)) \to \mathcal{E}_\infty^\rho / J_n \mathcal{E}_\infty^\rho \xrightarrow{\pi} \mathcal{E}_n^\rho \to \varprojlim_m \hat{H}_0(Gal(K_m/K_n), \mathcal{E}_m^\rho) \to 0.$$

p^s kills kernel of π and p^r annihilates cokernel of π. Thus $p^r \alpha_n$ induces a well-defined map from $\mathcal{E}_n^\rho$ to $\mathbb{Z}_p[Gal(K_n/K)]^\rho$.

Therefore Theorem 58 implies that $p^t \alpha_n(\mathcal{C}_n^\rho)$ annihilates A_n^ρ.

Since, it holds for all n large enough, we have $p^t \alpha(\mathcal{C}_\infty^\rho)$ annihilates A_∞^ρ.

□

Corollary 68. *Suppose $Gal(K_\infty/K_0) \cong \mathbb{Z}_p$, $rank_{\Lambda^\rho} \mathcal{E}_\infty^\rho > 0$ and ρ and K_n/K satisfy the conditions of the last theorem. Define $\mathcal{A}$ as the annihilator in Λ of $\mathcal{E}_\infty^\rho / \mathcal{C}_\infty^\rho$. Then there is an integer k such that $p^k \mathcal{A}$ annihilates A_∞^ρ.*

Sketch of proof: $\mathcal{E}_\infty^\rho$ is finitely generated Λ^ρ-module.

$$\Lambda^{\rho} \cong (\mathbb{Z}_p[H]^{\rho})[[Gal(K_\infty/K_0)]] \cong \mathcal{O}[[T]]$$

where $\mathcal{O}$ is the ring of integers of the unramified extension of $\mathbb{Q}_p$ of degree $\dim(\rho)$.

On the other hand, by the structure theorem for $\mathcal{O}[[T]]$-modules, since $rank_{\Lambda^{\rho}}\mathcal{E}_\infty^{\rho} > 0$, there is a map: $\alpha : \mathcal{E}_\infty^{\rho} \to \Lambda^{\rho}$ with finite cokernel.

Now, the last theorem implies that $p^t\alpha(\mathcal{C}_\infty^{\rho})$ annihilates A_∞^{ρ}.

Choose j such that p^j annihilates the cokernel of α. Therefore $p^j\mathcal{A} \subset \mathcal{A}\alpha(\mathcal{E}_\infty^{\rho}) \subset \alpha(\mathcal{C}_\infty^{\rho})$. This concludes that $p^{t+j}\mathcal{A}$ annihilates A_∞^{ρ}. □

The next proposition is a variant of a theorem due to Iwasawa.

Proposition 69. *Suppose $Gal(K_\infty/K_0) \cong \mathbb{Z}_p$. Let ρ be an irreducible representation of H such that for every prime $\mathfrak{p}$ of K which ramified in K_∞/K_0, the restriction of ρ to the decomposition group of $\mathfrak{p}$ in H is non-trivial. Then $\#\hat{H}^0(Gal(K_m/K_n), \mathcal{E}_m^{\rho})$ and $\#\hat{H}^{-1}(Gal(K_m/K_n), \mathcal{E}_m^{\rho})$ are bounded independently of m and n.*

Proof. Let $S = \{primes \quad \mathfrak{p} \quad of \quad K| \quad \mathfrak{p} \quad ramifies \quad in \quad K_\infty/K_0\}$.

Let $\mathcal{E}'_m$ be the group of $S - units$ of K_m, i.e. elements of K_m which are units at all primes not lying above primes of S.

For each $\mathfrak{p} \in S$, we have the following exact sequence

$$0 \to \mathcal{E}_m \to \mathcal{E}'_m \to \bigoplus_{\mathfrak{p}\in S} R_m(\mathfrak{p})$$

where $R_m(\mathfrak{p})$ is the free abelian group generated by primes $\tilde{\mathfrak{p}}$ above $\mathfrak{p}$ in K_m and the map $\mathcal{E}'_m \to \bigoplus_{\mathfrak{p}\in S} R_m(\mathfrak{p})$ sends $u \to \sum ord_{\tilde{\mathfrak{p}}}(u)\tilde{\mathfrak{p}}$.

Denote by $DH_{\mathfrak{p}}$ the decomposition group of $\mathfrak{p}$ in H. $DH_{\mathfrak{p}}$ acts trivially on $R_m(\mathfrak{p})$. On the other hand, $\rho\mid_{DH_{\mathfrak{p}}}$ is non-trivial, thus $R_m(\mathfrak{p})^{\rho} = 0$.

Since $R_m(\mathfrak{p})^{\rho} = 0$ for every $\mathfrak{p}$, we have $\mathcal{E}_m^{\rho} = (\mathcal{E}'_m)^{\rho}$.

It is possible to prove that $\#\hat{H}^{-1}(Gal(K_m/K_n), \mathcal{E}'_m)$ is bounded independently of m, n. See for example [12].

Since

$$\hat{H}^{-1}(Gal(K_m/K_n), \mathcal{E}_m^{\rho}) = \hat{H}^{-1}(Gal(K_m/K_n), (\mathcal{E}'_m)^{\rho}) =$$
$$\hat{H}^{-1}(Gal(K_m/K_n), \mathcal{E}_m)^{\rho}$$

we have that $\hat{H}^{-1}(Gal(K_m/K_n), \mathcal{E}_m)^{\rho}$ is bounded.

$\mathbb{Z}_p$ has no element of order 2, then every infinite place of K_0 splits completely in K_∞.

Now, we will not prove, but from [12] we know that for any m, n, $\mathcal{E}_m^\rho$ contains a subgroup of finite index which is free over $\mathbb{Z}_p[Gal(K_m/K_n)]$. From it follows that the Herbrand quotient

$$\#\hat{H}^0(Gal(K_m/K_n), \mathcal{E}_m^\rho)/\hat{H}^{-1}(Gal(K_m/K_n), \mathcal{E}_m^\rho) = 1$$

. So, $\#\hat{H}^0(Gal(K_m/K_n), \mathcal{E}_m^\rho)$ is bounded independently of m and n. □

Define $\mathcal{U}_n$ for the local 1-units of K_n above p, i.e., the local units of $K_n \otimes K_p$ congruent to 1 modulo primes above p and $\mathcal{U} = \varprojlim_n \mathcal{U}_n$.

Now we will give a theorem with weaker hypothesis than theorem 67.

Theorem 70. *Supppose that the decomposition group of p has finite index in $Gal(K_\infty/K)$. Fix an irreducible representation ρ of H whose restriction to the decomposition group of p in H is non-trivial. Let $\alpha : \mathcal{U}_\infty^\rho \to \Lambda^\rho$ be any $\Lambda - module$ map.*

1. *If $m_p(K_\infty)$ is finite, then $m_p(K_\infty)\alpha(\mathcal{C}_\infty^\rho)$ annihilates A_∞^ρ*
2. *If $\mu_p \subset K_\infty, \mathcal{O}_K^\times$ is finite, and $\rho \neq \check{\rho} \otimes \omega$, then $\alpha(\mathbb{C}_\infty^\rho)$ annihilates A_∞^ρ*
3. *If $\mu_p \subset K_\infty, \rho \neq \omega$ and $\rho \neq \check{\rho} \otimes \omega$, then $\alpha(\mathcal{C}_\infty^\rho)$ annihilates A_∞^ρ.*

Proof. Choose n be large enough such that $Gal(K_\infty/K_n)$ is contained in the decomposition group of p and K_n contains the Hilbert Class Field of K.

Let J_n be the ideal generated by $\{\gamma - 1 | \gamma \in Gal(K_\infty/K_n)\}$.

Using [14] and [13] is possible to prove that $\mathcal{U}_\infty^\rho / J_n \mathcal{U}_\infty^\rho \cong \mathcal{U}_n^\rho$.

α induces $\alpha_n : \mathcal{U}_\infty^\rho / J_n \mathcal{U}_\infty^\rho \cong \mathcal{U}_n^\rho \to \lambda^\rho / J_n \Lambda^\rho \cong \mathbb{Z}_p[Gal(K_n/K)]^\rho$.

Now, we want to apply theorem 58. Therefore, we restrict α_n to $\mathcal{E}_n^\rho$. We obtain

1. If (1) is satisfied then $m_p(K_\infty)\alpha_n(\mathcal{C}_n^\rho)$ annihilates A_n^ρ
2. or (3) are satisfied, then $\alpha(\mathcal{C}_n^\rho)$ annihilates A_n^ρ.

Since (1),(2),(3) are for n large enough, then the theorem follows. □

Bibliography

[1] Thaine, Francisco. ”On the ideal class groups of real abelian number fields.” *Annals of mathematics* 128.1 (1988): 1-18.

[2] Rubin, Karl. ”Global units and ideal class groups.” *Inventiones mathematicae* 89.3 (1987): 511-526.

[3] Neukirch, Jürgen. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[4] Marcus, Daniel A. *Number fields*. Vol. 8. New York: Springer, 1977.

[5] Lettl, Günter. ”A note on Thaine’s circular units.” *Journal of Number Theory* 35.2 (1990): 224-226.

[6] Cassels, John William Scott, and Albrecht Frölich. *Algebraic number theory: proceedings of an instructional conference*. Academic Pr, 1967.

[7] Guillot, Pierre. *A Gentle Course in Local Class Field Theory: Local Number Fields, Brauer Groups, Galois Cohomology*. Cambridge University Press, 2018.

[8] Serre, Jean-Pierre. *Local fields*. Vol. 67. Springer Science & Business Media, 2013.

[9] Reiner, Irving, and Charles Whittlesey Curtis. *Methods of representation theory with applications to finite groups and orders*. Wiley, 1990.

[10] Milies, César Polcino, Sudarshan K. Sehgal, and Sudarshan Sehgal. *An introduction to group rings*. Vol. 1. Springer Science & Business Media, 2002.

[11] Iwasawa, Kenkichi. *"On Z_p-extensions of algebraic number fields."* Annals of Mathematics (1973): 246-326.

[12] Iwasawa, Kenkichi. *"On cohomology groups of units for Z p-extensions."* American Journal of Mathematics 105.1 (1983): 189-200.

[13] Wintenberger, Jean-Pierre. *"Structure galoisienne de limites projectives d'unités locales."* Compositio Mathematica 42.1 (1980): 89-103.

[14] Tate, John Torrence. *Les conjectures de Stark sur les fonctions L d'Artin en s: notes d'un cours à Orsay*. Birkhäuser, 1984.

[15] Childress, Nancy. *Class field theory*. Springer Science & Business Media, 2008.

[16] Sinnott, Warren. *On the Stickelberger ideal and the circular units of an abelian field.* Inventiones mathematicae 62.2 (1980): 181-234.

[17] Atiyah, Michael F., and Ian G. Macdonald. *"Introduction to commutative algebra"* Addison." (1969).

[18] Morandi, Patrick. *Fields and Galois theory*. Vol. 167. Springer Science & Business Media, 2012.