UNIVERSIDADE FEDERAL DO
RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA

Cláudio da Silva Velasque

On the ideal class groups of real abelian number fields

Rio de Janeiro

2019

On the ideal class groups of real abelian number fields

Cláudio da Silva Velasque

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.

Orientador: Aftab Pande

Rio de Janeiro

2019

CIP - Catalogação na Publicação

```
         Velasque, Cláudio
V434o       On the ideal class groups of real abelian number
         fields / Cláudio Velasque. -- Rio de Janeiro, 2019.
            50 f.

            Orientador: Aftab Pande.
            Dissertação (mestrado) - Universidade Federal do
         Rio de Janeiro, Instituto de Matemática, Programa
         de Pós-Graduação em Matemática, 2019.

            1. Teoria algébrica dos números. 2. Corpos
         ciclotômicos. I. Pande, Aftab, orient. II. Título.
```

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos
pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

On the ideal class groups of real abelian number fields

Cláudio da Silva Velasque

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.

Aprovada por:

Prof. Dr. Aftab Pande - IM/UFRJ, (Presidente)

Prof. Dr. Amílcar Pacheco - IM/UFRJ

Prof. Dr. Luis Lomelí - IM/PUCV

Prof. Dr. Younes Nikdelan - IME/UERJ (Suplente)

Prof. Dr. Seyed Hamid Hassanzadeh Hafshejani - IM/UFRJ (Suplente)

Rio de Janeiro

2019

"Number Theory, among the mathematical disciplines, occupies an idealized position, similar to the one that mathematics holds among the sciences. Under no obligation to serve needs that do not originate within itself, it is essentially autonomous in setting its goals, and thus manages to protect its undisturbed harmony. The possibility of formulating its basic problems simply, the peculiar clarity of its statements, the arcane touch in its laws, be they discovered or undiscovered, merely divined; last but not least, the charm of its particularly satisfactory ways of reasoning - all these features have at all times attracted to number theory a community of dedicated followers. "

Jurgen Neukirch

Acknowledgements

Prima facea, I am grateful to God for the good health and well being that were necessary to complete this work.

I would like to express my sincere gratitude to my advisor Prof. Aftab Pande for the continuous support of my M.Sc study, for his patience, motivation, and immense knowledge.

Besides my advisor, I would like to thank my colleagues, Ricardo Torso and André Lelis, for the valuable suggestions and help during the study.

I am also grateful to the CPNq for the financial support.

Finally, I must express my very profound gratitude to my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Abstract

The purpose of this thesis is to give a proof of a theorem of F. Thaine [Tha] about annihilators of class groups of real abelian number fields. An improvement of R. Kucera [Kuc] is also treated.

First, we summarize some basic facts, including Algebraic Number Theory. In the first chapter, we develop Global Class Field Theory ,according to N. Childress' book [Chi]. In the second chapter, we give a proof of Thaine's theorem for odd primes. The third chapter gives an extension of R. Kucera of Thaine's theorem for $p = 2$. Finally, an outline of the proof of Catalan's Conjecture shows an application of the main result of this thesis. The last chapter is based on an article of T. Metsankyla[Met].

Keywords: Thaine's theorem, annihilators, real number field, ideal class groups.

Resumo

O propósito desta dissertação é provar um teorema de F. Thaine [Tha] sobre anuladores de grupos de classes de corpos numéricos abelianos reais. Um aperfeiçoamento de R. Kucera [Kuc] também é tratado.

Primeiramente, nos sumarizamos alguns fatos básicos, incluindo a teoria dos números algébricos. No primeiro capítulos, nos desenvolvemos a teoria dos corpos de classe globais, seguindo o livro da N. Childress [Chi]. No segundo capítulo, nos provamos o teorema de Thaine para primos ímpares. No terceiro capítulo é dada a extenção de R. Kucera do teorema de Thaine para $p = 2$. Finalmente, um resumo da prova da conjectura de Catalan mostra uma aplicação do principal resultado desta dissertação. O último capítulo é baseado em um artigo de T. Metsankyla[Met].

Palavras-clave: Theorema de Thaine, anuladores, corpos numéricos reais, grupos de classes ideais.

Contents

Basic Results 1

0.1 Algebraic Number Theory 1

0.2 Inverse Limits 4

0.3 Semisimple Rings 5

0.4 Group Rings and Maschke's Theorem 6

0.5 Group Representations and Characters 7

1 Class Field Theory 8

1.1 Universal Norm Index Inequality 8

1.2 Cyclic Norm Index Equality 9

1.3 Artin Reciprocity 12

1.4 The Existence Theorem 14

2 Thaine's Theorem for odd primes 16

2.1 Factorization of certain principal ideals 16

2.2 Ideal classes and units. A local-global theorem 18

2.3 A relation between the ideal class group and the units of F 22

2.4 Annihilators of ideal classes of prime order to $[F : \mathbb{Q}]$ 26

3 The case $p = 2$ 28

3.1 Reduction to cyclic fields 28

3.2 Circular numbers of an abelian field 29

3.3 Cyclic fields 29

3.4 An auxiliary field 30

3.5 Annihilating the ideal class group 32

4 An application: Catalan's Conjecture 34

4.1 An outline of the proof 34

4.2 Annihilators 36

4.3 A contradiction 37

Bibliography **39**

Basic Results

0.1 Algebraic Number Theory

A number field is a finite algebraic extension of $\mathbb{Q}$. If F is a number field, denote the ring of algebraic integers of F by $\mathcal{O}_F$. It is well-known that $\mathcal{O}_F$ is a Dedekind domain, so that any ideal of $\mathcal{O}_F$ has a unique factorization into a product of prime ideals. A fractional ideal of F is a non-zero finitely generated $\mathcal{O}_F$-submodule of F, which forms a group $\mathcal{I}_F$ under multiplication. The principal fractional ideals of F form a normal subgroup of $\mathcal{I}_F$, denoted $\mathcal{P}_F$. The quotient group $\mathcal{C}_F = \mathcal{I}_F/\mathcal{P}_F$ is called the ideal class group of F. It is a finite group. Its order is the class number of F, denoted h_F.

The ideal classes in $\mathcal{O}_F$ are generated as a group by prime ideals $\mathfrak{p}$ with norm $N(\mathfrak{p}) \leq B_K$, where

$$B_K = \prod_{\sigma: F \hookrightarrow \mathbb{C}} \sum_{i=1}^{n} |\sigma(e_i)|$$

for some choice of $\mathbb{Z}$-basis $\{e_1, \cdots, e_n\}$ of $\mathcal{O}_F$. As an example, we will show that $\mathbb{Q}(\sqrt{-5})$ has only two ideal classes. Let $\{e_1, e_2\} = \{1, \sqrt{-5}\}$. Since

$$B_K = (|e_1| + |e_2|)(|\overline{e_1}| + |\overline{e_2}|) = (1 + \sqrt{-5})^2 \approx 10.4,$$

we have that $\mathcal{C}_{\mathbb{Q}(\sqrt{-5})}$ is generated by primes $\mathfrak{p}$ with $N(\mathfrak{p}) \leq 10$. Then $\mathfrak{p}$ divides $(2), (3), (5)$, or (7). These primes decompose as

$$(2) = \mathfrak{p}_2^2,\ (3) = \mathfrak{p}_3\mathfrak{p}_3^{'},\ (5) = (\sqrt{-5})^2,\ (7) = \mathfrak{p}_7\mathfrak{p}_7^{'}.$$

In $\mathcal{C}_{\mathbb{Q}(\sqrt{-5})}$ principal ideals become trivial, so

$$[\mathfrak{p}_2^2] = 1,\ [\mathfrak{p}_3][\mathfrak{p}_3^{'}] = 1,\ [\mathfrak{p}_7][\mathfrak{p}_7^{'}] = 1.$$

Thus $\mathcal{C}_{\mathbb{Q}(\sqrt{-5})}$ is generated by $\mathfrak{p}_2$, either prime ideal of norm 3, and either prime ideal of norm 7. Since $(1+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3$ and $(3+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_7$, we have that $[\mathfrak{p}_3]$ and $[\mathfrak{p}_7]$ both equal $[\mathfrak{p}_2]^{-1}$. Thus $\mathcal{C}_{\mathbb{Q}(\sqrt{-5})} = \langle[\mathfrak{p}_2]\rangle$. Since $\mathfrak{p}_2$ is not principal and its square is principal, $[\mathfrak{p}_2]$ has order 2 and thus $\mathcal{C}_{\mathbb{Q}(\sqrt{-5})} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Given a finite extension K/F of number fields, let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_F$. Using unique factorization of ideals in $\mathcal{O}_K$, we have

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

where the $\mathfrak{P}_j$ are distinct prime ideals of $\mathcal{O}_K$, g and e_j are positive integers. We call $e_j = e(\mathfrak{P}_j/\mathfrak{p})$ the ramification index of $\mathfrak{P}_j/\mathfrak{p}$. If K/F is a Galois extension, then the Galois group permutes the $\mathfrak{P}_j$ transitively, so that $e_1 = \cdots = e_g = e$, say.

Since every non-zero prime ideal is maximal in a Dedekind domain, the quotients $\mathbb{F}_{\mathfrak{P}_j} = \mathcal{O}_K/\mathfrak{P}_j$ and $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_F/\mathfrak{p}$ are fields, called residue fields. We may view $\mathbb{F}_{\mathfrak{p}}$ as a subfield of $\mathbb{F}_{\mathfrak{P}_j}$. The inertia degree is

$$f(\mathfrak{P}_j/\mathfrak{p}) = [\mathbb{F}_{\mathfrak{P}_j} : \mathbb{F}_{\mathfrak{p}}].$$

If K/F is a Galois extension, then $f(\mathfrak{P}_1/\mathfrak{p}) = \cdots = f(\mathfrak{P}_g/\mathfrak{p}) = f$, say.

In general, we have $\displaystyle\sum_{j=1}^{g} e(\mathfrak{P}_j/\mathfrak{p}) f(\mathfrak{P}_j/\mathfrak{p}) = [K : F]$.

If K/F is a finite extension of number fields, we say that the prime $\mathfrak{p}$ is unramified if $e(\mathfrak{P}_j/\mathfrak{p}) = 1, \forall j$, $\mathfrak{p}$ is totally ramified if there is a unique prime $\mathfrak{P}$ above $\mathfrak{p}$ with $e(\mathfrak{P}/\mathfrak{p}) = [K : F]$, $\mathfrak{p}$ remains inert if $\mathfrak{p}\mathcal{O}_K$ is prime in $\mathcal{O}_K$, and $\mathfrak{p}$ splits completely if $g = [K : F]$.

Theorem 0.1. *(Dedekind-Kummer): Let K/F be an extension of number fields and suppose $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. Let $f(X) = Irr_F(\alpha, X)$, and let $\mathfrak{p}$ be a prime ideal of F. Put $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_F/\mathfrak{p}$, and denote the image of $f(X)$ in $\mathbb{F}_{\mathfrak{p}}[X]$ by $\overline{f(X)}$. If $\overline{f(X)} = \overline{p_1(X)}^{e_1} \cdots \overline{p_g(X)}^{e_g}$, where the $\overline{p_j(X)}$ are distinct monic irreducible polynomials in $\mathbb{F}_{\mathfrak{p}}[X]$, then $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, with the $\mathfrak{P}_j$ distinct prime ideals of $\mathcal{O}_K$.*

Let $\{v_1, ..., v_n\}$ be a F-basis of K, define the discriminant of this basis as

$$d(v_1, ..., v_n) = \det[\sigma_i(v_j)]^2,$$

where $\sigma_1, ..., \sigma_n : K \hookrightarrow F^{\text{Alg}}$ are F-monomorphisms. Note that different F-bases for K need not have the same discriminant. Hence the discriminant of the extension must be defined in terms of all possible basis for K.

Suppose M is a non-zero $\mathcal{O}_F$-submodule of K and M contains an F-basis for K. We let d(M) be the $\mathcal{O}_F$-module generated by all $d(v_1, ..., v_n)$ where $\{v_1, ..., v_n\} \subset$ M varies through the F-basis for K contained in M. The discriminant of the extension K/F is $d_{K/F} = d(\mathcal{O}_K)$, where $\mathcal{O}_K$ is considered as a finitely generated $\mathcal{O}_F$-module. This makes $d_{K/F}$ an ideal of $\mathcal{O}_F$. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, we have that $\mathfrak{p}$ is ramified in K/F if and only if $\mathfrak{p}|d_{K/F}$.

Let $\mathfrak{p}$ and $\mathfrak{P}$ be prime ideals of $\mathcal{O}_F$ and $\mathcal{O}_K$,respectively, such that $\mathfrak{P}|\mathfrak{p}\mathcal{O}_K$. Define the norm of $\mathfrak{P}$ as $N_{K/F}\mathfrak{P} = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$. Now extend $N_{K/F}$ to fractional ideals of K multiplicatively, i.e.,

$$N_{K/F}(\mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_g^{a_g}) = N_{K/F}(\mathfrak{P}_1)^{a_1} \cdots N_{K/F}(\mathfrak{P}_g)^{a_g}.$$

Note that if K/F is Galois, then $N_{K/F}(\mathfrak{A})\mathcal{O}_K = \prod_{\sigma \in \mathrm{Gal(K/F)}} \sigma(\mathfrak{A})$. If $F \subseteq E \subseteq K$ are number fields, then $N_{K/F} = N_{E/F} \circ N_{K/E}$.

Supposing K/F Galois, we can define the decomposition group

$$Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G; \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Note that $Z(\mathfrak{P}/\mathfrak{p})$ acts on $\mathbb{F}_{\mathfrak{P}}$, and fixes the subfield $\mathbb{F}_{\mathfrak{p}}$ elementwise, so there is a natural homomorphism of groups

$$Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

Theorem 0.2. *Let K/F be Galois and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$.*
(i) G acts transitively on the set of prime ideals $\mathfrak{P}$ of $\mathcal{O}_F$ that divide $\mathfrak{p}\mathcal{O}_K$ whence

$$[G : Z(\mathfrak{P}/\mathfrak{p})] = g.$$

Also, if $\mathfrak{P}_1$,$\mathfrak{P}_2$ are prime ideals of $\mathcal{O}_K$ above $\mathfrak{p}$, then $Z(\mathfrak{P}_1/\mathfrak{p})$ and $Z(\mathfrak{P}_2/\mathfrak{p})$ are G-conjugate;
(ii)$N\mathfrak{p} = \#\mathbb{F}_{\mathfrak{p}}$, $N\mathfrak{P} = \#\mathbb{F}_{\mathfrak{P}}$, and Gal$(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is cyclic, generated by the Frobenius automorphism $\varphi_{\mathfrak{p}} : x \mapsto x^{N\mathfrak{p}}$;
(iii) The homomorphism $Z(\mathfrak{P}/\mathfrak{p}) \to$ Gal$(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is surjective; its kernel is called the inertia subgroup, denoted $T(\mathfrak{P}/\mathfrak{p})$. Note that [$Z(\mathfrak{P}/\mathfrak{p})$:$T(\mathfrak{P}/\mathfrak{p})$] $= f$ and
$\#T(\mathfrak{P}/\mathfrak{p}) = e$.

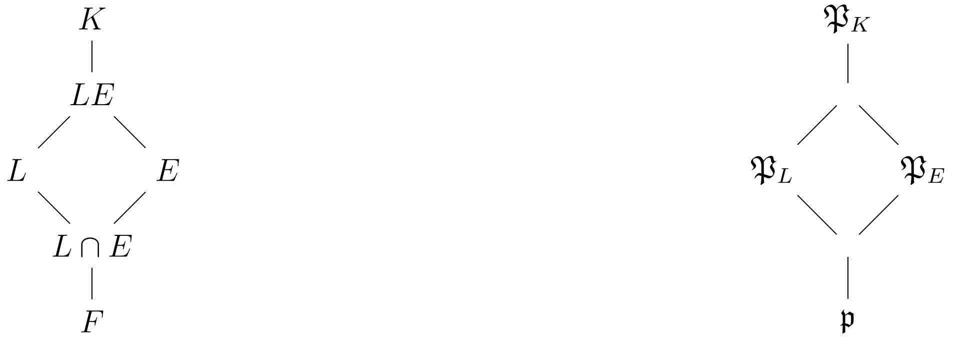
Theorem 0.3. *Let K^Z =Inv$(Z(\mathfrak{P}/\mathfrak{p})) = \{x \in K;\ \sigma(x) = x,\ \forall\sigma \in Z(\mathfrak{P}/\mathfrak{p})\}$ and K^T =Inv$(T(\mathfrak{P}/\mathfrak{p}))$. If K/F is abelian, then $\mathfrak{p}$ splits completely in K^Z/F. The primes above $\mathfrak{p}$ remain inert in K^T/K^Z and ramify totally in K/K^T.*

Proposition 0.4. *Let K_1 and K_2 be two extensions of a number field F. If a prime ideal $\mathfrak{p}$ of F splits completely in both K_1 and K_2, then $\mathfrak{p}$ splits completely in K_1K_2.*

If $e(\mathfrak{P}/\mathfrak{p}) = 1$, then $Z(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, hence $\exists!\ \sigma\ \in Z(\mathfrak{P}/\mathfrak{p})$ that corresponds to $\varphi_{\mathfrak{p}}$ under the natural isomorphism. This element σ is called the Frobenius element at $\mathfrak{P}$.

Proposition 0.5. *Let K/F be Galois, $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ unramified in K/F and $\mathfrak{P}$ prime ideal of $\mathcal{O}_K$ above $\mathfrak{p}$. Then the Frobenius element at $\mathfrak{P}$ is the unique element $\sigma \in Gal(K/F)$ that satisfies $\sigma(\alpha) \equiv \alpha^{N\mathfrak{p}} \mod \mathfrak{P}, \forall \alpha \in \mathcal{O}_F$. If K/F is abelian, then the Frobenius element does not depend on the choice of $\mathfrak{P}$.*

Theorem 0.6. *(Consistency Property): Let $F \subseteq L \subseteq K, F \subseteq E \subseteq K$ be number fields and suppose K/F is Galois. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ that is unramified in K/F and let $\mathfrak{P}_K$ be a prime ideal of $\mathcal{O}_K$ that divides $\mathfrak{p}$. Let $\mathfrak{P}_L = L \cap \mathfrak{P}_K, \mathfrak{P}_E = E \cap \mathfrak{P}_K$. Then $\left(\dfrac{\mathfrak{P}_K}{K/E}\right)\Big|_L = \left(\dfrac{\mathfrak{P}_L}{L/F}\right)^f$, where $f = f(\mathfrak{P}_E/\mathfrak{p})$.*



Proposition 0.7. *The prime p splits completely in $\mathbb{Q}(\zeta_m)$ if and only if $p \equiv 1 \mod m$.*

Theorem 0.8. *(Dirichlet Unit Theorem) Denote $\mathcal{O}_F^\times$ by $\mathcal{U}_F$. Let F be a number field and let r_1 and r_2 represent the number of real embeddings and the number of conjugate pairs of imaginary embeddings of F, respectively. Then $\exists\ \varepsilon_1, \cdots, \varepsilon_{r_1+r_2-1} \in \mathcal{U}_F$ such that*

$$\mathcal{U}_F \cong \mathcal{W}_F \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_{r_1+r_2-1} \rangle,$$

where $\mathcal{W}_F$ is the group of roots of unity in F. The ε_j are called a fundamental system of units of F.

For the proofs, see [Mar].

0.2 Inverse Limits

A sequence $(E_n, \varphi_n)_{n \geq 0}$ of sets and maps $\varphi_n : E_{n+1} \to E_n$ is called an inverse system. A set E together with maps $\psi_n : E \to E_n$ such that $\psi_n = \varphi_n \circ \psi_{n+1}$ is called an inverse limit of the sequence $(E_n, \varphi_n)_{n \geq 0}$ if the following condition is satisfied: For each set X and maps $f_n : X \to E_n$ satisfying $f_n = \varphi_n \circ f_{n+1}$ there is a unique factorization f of f_n through the set E: $f_n = \psi_n \circ f : X \to E \to E_n$.

Theorem 0.9. *For every inverse system $(E_n, \varphi_n)_{n\geq 0}$ of sets, there is a inverse limit $E = \varprojlim E_n \subset \prod\limits_{n\geq 0} E_n$ with maps ψ_n given by restriction of projections. Moreover, if (D, Ψ_n) is another inverse system of the same sequence, there is a unique bijection $f : D \to E$ such that $\Psi_n = \psi_n \circ f$.*

Corollary 0.10. *When all the maps φ_n are surjective, then the inverse limit $(E, (\psi))$ also has surjective projections ψ_n, and in particular, the set E is not empty.*

Example: The ring of p-adic integers $\mathbb{Z}_p = \varprojlim \mathbb{Z}/(p^n\mathbb{Z})$.
For proofs, see [Rob] pag 29.

0.3 Semisimple Rings

A ring R is said to be semisimple if it is a direct sum of a finite number of minimal right ideals.
Example: Let $M_n(D)$ denote the full ring of $n\times n$ matrices over a division ring D. Set

$$L_1 = \begin{bmatrix} D & 0 & \cdots & 0 \\ D & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ D & 0 & \cdots & 0 \end{bmatrix}, \cdots, L_n = \begin{bmatrix} 0 & 0 & \cdots & D \\ 0 & 0 & \cdots & D \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & D \end{bmatrix}.$$

We have that L_i is a minimal right ideal of $M_n(D)$ and $M_n(D) = L_1 \oplus \cdots \oplus L_n$. Thus $M_n(D)$ is semisimple.

Theorem 0.11. *A ring R is semisimple if and only if every right ideal I of R is of the form $I = eR$, where $e \in R$ is an idempotent(i.e. $e^2 = e$).*

Theorem 0.12. *Let $R = \oplus_{i=1}^N I_i$ be a decomposition of a semisimple ring as a direct sum of minimal right ideals. Then there exists a set $\{e_1, \cdots, e_N\}$ of idempotents of R such that*
(i) If $i \neq j$, then $e_i.e_j = 0$;
(ii) $1 = e_1 + \cdots + e_N$;
(iii) e_i cannot be written as a sum of two other orthogonal idempotents.
Conversely, if there exists a set of idempotents $\{e_1, \cdots, e_N\}$ satisfying the conditions above, then the right ideals $I_i = e_i.R$ are minimal and $R = \oplus_{i=1}^N I_i$.

Theorem 0.13. *Let $\overline{R} = R/I$, where I is a two-sided ideal of R contained in $Rad(R)$. Assume either* *(i) R is right artinian;*

(ii) R is an R_1-algebra, finitely generated as R_1-module, where R_1 is a commutative complete local noetherian ring.

Then each decomposition of R into indecomposable right ideals e_iR, yields a decomposition $\overline{R} = \overline{e_1}\overline{R} \oplus \cdots \oplus \overline{e_n}\overline{R}$ into indecomposable right ideals $\overline{e_i}\overline{R}$.

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

Furthermore, for $1 \le i, j \le n$, we have $e_iR \cong e_jR \Leftrightarrow \overline{e_i}\overline{R} \cong \overline{e_j}\overline{R}$.

Proof. See [CR], pag 125. □

0.4 Group Rings and Maschke's Theorem

Let G be a group (not necessarily finite) and R a ring. We denote by $R[G]$ the set of all formal linear combinations of the form

$$\alpha = \sum_{g \in G} a_g g,$$

where $a_g \in R$ and $a_g = 0$ almost everywhere. We define the sum of two elements in $R[G]$ componentwise

$$\{\sum_{g \in G} a_g g\} + \{\sum_{g \in G} b_g g\} = \sum_{g \in G} \{a_g + b_g\} g.$$

Also, given two elements $\alpha = \sum a_g g$ and $\beta = \sum b_g g$ in $R[G]$ we define their product by

$$\alpha\beta = \sum_{u \in G} c_u u, \text{ where } c_u = \sum_{gh=u} a_g b_h.$$

It is easy to verify that, with the operations above, $R[G]$ is a ring, which has unity, namely, the element $1 = \sum u_g.g$ where the coefficient corresponding to the unit element of the group is equal to 1 and $u_g = 0$ otherwise.

We can also define a product of elements in $R[G]$ by elements $\lambda \in R$ as

$$\lambda\{\sum a_g.g\} = \sum \{\lambda a_g\} g.$$

The set $R[G]$, with the operations above, is called the group ring of G over R.

The homomorphism $\varepsilon : R[G] \to R$ given by $\varepsilon(\sum a_g g) = \sum a_g$ is called the augmentation mapping of $R[G]$ and its kernel is called the augmentation ideal of $R[G]$.

Theorem 0.14. *(Maschke) The group ring $R[G]$ is semisimple if and only if the following conditions hold*
(i) R is a semisimple ring;
(ii) G is finite;
(iii) $\#G$ is invertible in R.

Corollary 0.15. *Let G be a finite group and let F be a field. Then $F[G]$ is semisimple if and only if char(F) $\nmid \#G$.*

For the proofs, see [MS] chapter 3.

0.5 Group Representations and Characters

A representation of a group G is a homomorphism $\varphi : G \rightarrow$GL(V) for some finite dimensional vector space V over a field F. A subspace $W \subseteq V$ is G-invariant if, for all $g \in G$ and $w \in W$, one has $\varphi(g)w \in W$. If the only G-invariant subspaces of V are $\{0\}$ and V, we say that φ is irreducible.
Example: The function $\varphi : \mathbb{Z}/(4\mathbb{Z}) \rightarrow \mathbb{C}$ given by $\varphi(m) = i^m$ is a representation

The character ρ of G afforded by the representation φ is the mapping $\rho : G \rightarrow F$ given by $\rho(g) =$Tr$(\varphi(g))$. If φ is irreducible, then the character ρ is called an irreducible character.

Theorem 0.16. *The elements $e_\rho = (\#G)^{-1} \sum_{g \in G} \rho(1)\rho(g^{-1})g$, where ρ is any irreducible character, have the following relations:*
(A) $e_\rho^2 = e_\rho$;
(B) $e_{\rho_1} e_{\rho_2} = 0$ if $\rho_1 \neq \rho_2$;
(C) $1 = \sum_\rho e_\rho$;
(D) If M is a module over $F[G]$, then we may write $M = \bigoplus_\rho e_\rho M$.

Chapter 1

Class Field Theory

1.1 Universal Norm Index Inequality

Let F be a number field. If an element $\alpha \in F$ satisfies $\sigma(\alpha) > 0$ for every real embedding σ of F, we say that α is totally positive, and write $\alpha \gg 0$. Let $\mathfrak{m}$ be a non-zero integral ideal of $\mathcal{O}_F$. Define

$$\begin{aligned} \mathcal{I}_F(\mathfrak{m}) =& \{\mathfrak{a} \in \mathcal{I}_F; \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0, \forall \mathfrak{p} \mid \mathfrak{m}\} \\ \mathcal{P}^+_{F,\mathfrak{m}} =& \{\langle \frac{\alpha}{\beta} \rangle : \frac{\alpha}{\beta} \gg 0;\ \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m};\ \alpha \equiv \beta \mod \mathfrak{m}\}. \end{aligned}$$

The strict ray class group of F for $\mathfrak{m}$, is

$$\mathcal{R}^+_{F,\mathfrak{m}} = \mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}}.$$

Example: Let $F = \mathbb{Q}$, $\mathfrak{m} = m\mathbb{Z}$, where $m \geq 1$. If $\langle r \rangle \in \mathcal{I}_F(\mathfrak{m})$, then we may suppose $r \geq 1$ and $r = a/b$, where $(a, m) = (b, m) = 1$. The map

$$\begin{aligned} \mathcal{I}_F(\mathfrak{m}) &\longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \\ \langle r \rangle &\longmapsto ab^{-1} \mod m \end{aligned}$$

has kernel $\{\langle r \rangle : r > 0, r = a/b, (a, m) = (b, m) = 1, a \equiv b \mod \mathfrak{m}\} = \mathcal{P}^+_{\mathbb{Q},\mathfrak{m}}$. Hence $\mathcal{R}^+_{\mathbb{Q},\mathfrak{m}} = (\mathbb{Z}/m\mathbb{Z})^\times$, for $\mathfrak{m} = m\mathbb{Z}$.

Proposition 1.1. *$\mathcal{R}^+_{F,\mathfrak{m}}$ is a finite group.*

If $\mathcal{S}$ is a set of prime ideals of $\mathcal{O}_F$, and

$$\lim_{s \to 1_+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})} = \delta, \text{ exists},$$

then we say that $\mathcal{S}$ has Dirichlet density $\delta = \delta_F(\mathcal{S})$.

Proposition 1.2. *Let K/F be Galois, and let $\mathcal{S}_{K/F} = \{$ Prime ideals $\mathfrak{p}$ that split completely in $K/F\}$. Then $\delta_F(\mathcal{S}_{K/F}) = \frac{1}{[K:F]}$.*

Let $\mathcal{S}, \mathcal{T}$ be two sets of prime ideals of $\mathcal{O}_F$. We write $\mathcal{S} \approx \mathcal{T}$ to mean $\delta_F(\mathcal{S} \setminus \mathcal{T}) = \delta_F(\mathcal{T} \setminus \mathcal{S}) = 0$.

If $\mathfrak{m}$ is a non-zero integral ideal of $\mathcal{O}_F$, and $\mathcal{H}$ satisfies $\mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$, then we say K is the class field of F over $\mathcal{H}$ if K/F is Galois and $\mathcal{S}_{K/F} \approx \{$ Prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$; $\mathfrak{p} \subset \mathcal{H}\}$.

Example: For $F = \mathbb{Q}$ and $\mathfrak{m} = m\mathbb{Z}$, we have

$$\begin{aligned}\{p\mathbb{Z} : p\mathbb{Z} \in \mathcal{P}^+_{\mathbb{Q},\mathfrak{m}}\} &= \{p\mathbb{Z} : p \equiv 1 \mod m,\ p > 0\} \\ &= \{p\mathbb{Z} : p\mathbb{Z} \text{ splits completely in } \mathbb{Q}(\zeta_m)/\mathbb{Q}\} \\ &= \mathcal{S}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\end{aligned}$$

Thus $\mathbb{Q}(\zeta_m)$ is the class field over $\mathbb{Q}$ of $\mathcal{P}^+_{\mathbb{Q},\mathfrak{m}}$.

Theorem 1.3. *If the class field K of $\mathcal{H}$ exists, then it is unique.*

Theorem 1.4. *Suppose K/F is Galois, $\mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$, and $\exists\ \mathcal{T} \subseteq \{$ Prime ideals $\mathfrak{p}$ that split completely in $K/F\}$ with $\mathcal{S}_{K/F} \approx \mathcal{T}$. Then $[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \leq [K : F]$.*

Define $\mathcal{N}_{K/F}(\mathfrak{m}) = N_{K/F}(\mathcal{I}_K) \cap \mathcal{I}_F(\mathfrak{m})$.

Theorem 1.5. *(Universal Norm Index Inequality) Let K/F be Galois and $\mathcal{H} = \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})$. Then $[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \leq [K : F]$.*

Proof. If $\mathfrak{p} \in \mathcal{S}_{K/F}$ and $\mathfrak{P}|\mathfrak{p}$, where $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_K$. Then $N_{K/F}\mathfrak{P} = \mathfrak{p}$. Hence $\mathcal{S}_{K/F} \setminus \{$ Prime ideals $\mathfrak{p}$ of $\mathcal{O}_F; \mathfrak{p}|\mathfrak{m}\} \subseteq \mathcal{N}_{K/F}(\mathfrak{m}) \subseteq \mathcal{H}$. By the previous theorem, $[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \leq [K : F]$. □

1.2 Cyclic Norm Index Equality

Let F be a number field. An absolute value on F is a mapping $\|.\| : F \to [0, \infty)$ that satisfies $\|0\| = 0$, whose restriction to $F^\times$ is a homomorphism of multiplicative groups $F^\times \to \mathbb{R}^\times_+$, and that satisfies $\|1 + x\| \leq c$ whenever $\|x\| \leq 1$, for some $c \geq 1$. An absolute value induces a metric topology on F via fundamental systems of neighbourhoods of the form

$$\{x \in F : \|x - a\| < \varepsilon\}, \varepsilon > 0.$$

We say that two absolute values are equivalent if they induce the same topology.

A place of F is an equivalence class of non-trivial absolute values on F. Denote the set of places of F by V_F. By Ostrowski's Theorem, each of the places of F falls into one of the following categories:

(1) Places that contain one of the $\mathfrak{p}$-adic absolute values given by $\|\alpha\|_\mathfrak{p} = N\mathfrak{p}^{-\mathrm{ord}_\mathfrak{p}(\alpha)}$, for $\mathfrak{p}$ a prime ideal of $\mathcal{O}_F$. These are the finite places of F.

(2) Places that contain one of the absolute values $\|\alpha\|_\sigma = |\sigma(\alpha)|_\mathbb{R}$, for some real embedding $\sigma : F \hookrightarrow \mathbb{R}$. These are the finite real places of F.

(3) Places that contain one of the absolute values $\|\alpha\|_\sigma = |\sigma(\alpha)|_\mathbb{C}^2$, for some imaginary embedding $\sigma : F \hookrightarrow \mathbb{C}$. These are the infinite imaginary places of F.

The completion of a number field F with respect to the absolute value $|.|$ is

$$\{\text{Cauchy sequences in } F\}/\{\text{Null sequences in } F\}$$

If $|.| = |.|_\mathfrak{p}$ for some $\mathfrak{p}$ prime ideal of $\mathcal{O}_F$, then denote the completion of F by $F_\mathfrak{p}$. If $|.| = |.|_\sigma$ for some $\sigma : F \hookrightarrow \mathbb{C}$, then the completion of F is isomorphic either to $\mathbb{R}$ or $\mathbb{C}$, according as $\sigma(F) \subset \mathbb{R}$ or not.

Let $\mathcal{O}_\mathfrak{p} = \{x \in F_\mathfrak{p}; |x|_\mathfrak{p} \leq 1\}$ be the ring of $\mathfrak{p}$-adic integers. It has a unique maximal ideal $\mathcal{P}_\mathfrak{p} = \{x \in F_\mathfrak{p}; |x|_\mathfrak{p} < 1\}$, we also have $\mathcal{P}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ and

$$\mathcal{O}_\mathfrak{p}/\mathcal{P}_\mathfrak{p} \cong \mathcal{O}_F/\mathfrak{p}$$

Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ and view π as an element of $F_\mathfrak{p}$. Observe that $\mathcal{P}_\mathfrak{p} = \langle \pi \rangle$, we say that π is an uniformizer for $F_\mathfrak{p}$. Every $x \in F_\mathfrak{p}$ may be written as $x = \varepsilon\pi^t$, where $t \in \mathbb{Z}$ and $\varepsilon \in \mathcal{O}_\mathfrak{p}^\times$.

An idèle is an element $\mathbf{a} = (\cdots, a_v, \cdots) \in \prod_{v \in V_F} F_v^\times$ such that $\|a_v\|_v \neq 1$ only for finitely many places. They form a multiplicative group, denoted J_F. Let $\mathcal{E}_F = \prod_{v \in V_F} \mathcal{U}_v$, clearly a subgroup of J_F. We may give $\mathcal{E}_F$ the product topology, where each $\mathcal{U}_v$ has its metric topology.
Example: $J_\mathbb{Q} = \mathbb{Q}^\times \times \mathbb{R} \times \prod_p \mathbb{Z}_p^\times$.

We want to put a topology on J_F that will make it a locally compact topological group. To do so, we require $\mathbf{a}\mathcal{E}_F$ to be an open subset of J_F, $\forall\ \mathbf{a} \in J_F$, and also require that the map $\mathcal{E}_F \mapsto \mathbf{a}\mathcal{E}_F$ be a multiplicative homeomorphism $\forall \mathbf{a} \in J_F$.

Proposition 1.6. *A basis of open sets for J_F is given by*

$$\{\boldsymbol{a}A : \boldsymbol{a} \in J_F, \text{and } A \text{ is an open subset of } \mathcal{E}_F\}.$$

Proposition 1.7. *J_F with this topology is a locally compact topological group.*

Proposition 1.8. $J_F/\mathcal{E}_F \cong \mathcal{I}_F$.

We may view $\alpha \in F^\times$ as an idèle $(..., \iota_v(\alpha), ...)$, where $\iota_v : F \hookrightarrow F_v$ is an embedding of F into its completion at v. This gives an embedding, called the diagonal embedding,

$$\iota : F \hookrightarrow J_F, \text{ where } \iota(\alpha) = (..., \iota_v(\alpha), ...).$$

Usually we shall identify α and $\iota(\alpha)$, writing $F^\times$ when we really mean $\iota(F^\times)$.

Proposition 1.9. $J_F/(F^\times\mathcal{E}_F) \cong \mathcal{I}_F/\mathcal{P}_F$.

Proposition 1.10. *Let* $\mathfrak{m}$ *be a non-zero integral ideal of* $\mathcal{O}_F$*, and define*
$J^+_{F,\mathfrak{m}} = \{\boldsymbol{a} \in J_F : a_v > 0 \textit{ for all real } v, \textit{and } a_v \equiv 1 \;(\mod \mathfrak{p}_v^{ord_v(\mathfrak{m})}), \forall \mathfrak{p}_v|\mathfrak{m}\}$
$\mathcal{E}^+_{F,\mathfrak{m}} = J^+_{F,\mathfrak{m}} \cap \mathcal{E}_F$.
Then $J_F/(F^\times\mathcal{E}^+_{F,\mathfrak{m}}) = \mathcal{R}^+_{F,\mathfrak{m}}$

Corollary 1.11. *The set of subgroups* $\mathcal{H}$ *of* J_F*, with* $F^\times\mathcal{E}^+_{F,\mathfrak{m}} \subseteq \mathcal{H}$ *for some* $\mathfrak{m}$*, corresponds to the set of open subgroups of* J_F *that contain* $F^\times$.

Define $N_{K/F} : J_K \to J_F$ by $N_{K/F}(..., a_w, ...) = (..., \prod_{w|v} N_{K_w/F_v}(a_w), ...)$.

Let G be a finite cyclic group, say $G = \langle\sigma\rangle$, and let A be a $\mathbb{Z}[G]$-module. Define $s(G) = 1 + \sigma + \cdots + \sigma^{n-1}$, where $n = \#G$. Considering the map $\sigma - 1$ on A, we have $\ker(\sigma - 1) = \{a \in A : \sigma(a) = a\} = A^G$. Note that $s(G)A \subseteq A^G$ and $(\sigma - 1) \subseteq \ker s(G)$.

We define

$$\mathcal{Q}_G(A) = [A^G : s(G)A]/[\ker s(G) : (\sigma - 1)A],$$

when these indices are finite. The number $\mathcal{Q}_G(A)$ is called the Herbrand quotient of A for the group G.
Example: Let $G = \langle\sigma\rangle$ be cyclic of order n and let $A = \mathbb{Z}$, with G acting trivially on A. Then $A^G = \mathbb{Z}$ and $s(G)A = n\mathbb{Z}$. Also, $\ker s(G) = \{0\} = (\sigma - 1)A$. We get $\mathcal{Q}_G(A) = [\mathbb{Z} : n\mathbb{Z}] = n$.

Let K/F be a Galois extension of number fields, $\sigma \in G =$Gal(K/F), and $\mathbf{a} = (\cdots, a_w, \cdots) \in J_K$. For a place w of K, define the place σw by

$$\|\alpha\|_{\sigma w} = \|\sigma^{-1}(\alpha)\|_w,$$

Note that $\tau(\sigma w) = (\tau\sigma)w$. We have that G transitively permutes the places of K above some place of F, and $(K, \|.\|_w)$ is isomorphic to $(K, \|.\|_{\sigma w})$ via σ. Thus σ induces an isomorphism between the completions that we also denote by σ:

$$\sigma : K_w \xrightarrow{\cong} K_{\sigma w}.$$

We may now define for each $v \in V_F$

$$\sigma(\cdots, a_w, \cdots)_{w|v} = (\cdots, b_w, \cdots)_{w|v}, \text{where } b_w = \sigma(a_{\sigma^{-1}w})$$

This gives an action of σ on J_K with $J_K^G = J_F$. If G is cyclic, then $N_{K/F}(\mathbf{a}) = \prod_{\sigma\in G} \sigma(\mathbf{a})$.

Lemma 1.12. *Let $C_K = J_K/K^\times$, and $C_F = J_F/F^\times$. The embedding $J_F \hookrightarrow J_K$ induces an embedding $C_F \hookrightarrow C_K$. Furthermore, $C_K^G = C_F$.*

Proposition 1.13. $\mathcal{Q}_G(C_K) = [K : F]$.

Proposition 1.14. *For an abelian extension K/F of number fields, let $\mathcal{H} = F^\times N_{K/F}J_K$. Then*
(i) $\mathcal{H}$ is open in J_F, and $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq \mathcal{H}$, for some $\mathfrak{m}$ divisible only by the primes that ramify in K/F,
(ii) $J_F/\mathcal{H} \cong \mathcal{I}_F(\mathfrak{m})/(\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m}))$

Theorem 1.15. *(Cyclic Norm Index Equality) If K/F is a cyclic extension of number fields, and $\mathfrak{m}$ is an integral ideal of $\mathcal{O}_F$ that is divisible by sufficiently high power of every ramified prime in K/F, then*

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})] = [K : F].$$

Proof. By Proposition 1.13,

$$[C_K^G : s(G)C_K] = [K : F][\ker_{C_K} s(G) : (\sigma - 1)C_K].$$

But also $[C_K^G : s(G)C_K] = [C_F : N_{K/F}C_K] = [J_F/F^\times : N_{K/F}J_K/(F^\times N_{K/F}J_K)] = [J_F : F^\times N_{K/F}J_K] = [\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})]$, whenever $\mathfrak{m}$ satisfies $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F}J_K$. Thus $[K : F] \leq [\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})]$.

On the other hand, the Universal Norm Index Inequality gives $[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})] \leq [K : F]$. □

1.3 Artin Reciprocity

Let K/F be a Galois extension of number fields with abelian Galois group G. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ that is unramified in K/F. Then the decomposition group $G_\mathfrak{p} = Z(\mathfrak{p})$ must be cyclic with a canonical generator $\sigma_\mathfrak{p} = \left(\frac{\mathfrak{p}}{K/F}\right)$, the Artin automorphism.

Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_F$ that is divisible by all primes that ramify in the extension K/F and no others. The map $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$ induces a homomorphism $\mathcal{A} = \mathcal{A}_{K/F} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow G$ given by $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}} = \left(\dfrac{\mathfrak{a}}{K/F}\right)$ where, for $\mathfrak{a} = \prod\limits_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} \in \mathcal{I}_F(\mathfrak{m})$, we set $\sigma_{\mathfrak{a}} = \prod\limits_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_{\mathfrak{p}}}$. The map $\mathcal{A}$ is called the Artin map and $\left(\dfrac{\mathfrak{a}}{K/F}\right)$ is the Artin symbol.
Example: Let $F = \mathbb{Q}$, and $K = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m^{th} root of unity. Let $p\mathbb{Z}$ be a prime of $\mathbb{Z}$, where $(p, m) = 1$. Then $\left(\dfrac{p\mathbb{Z}}{K/F}\right) = \sigma_p : \zeta_m \mapsto \zeta_m^p$. If $a \in \mathbb{Z}_+$, say $a = p_1^{e_1} \cdots p_r^{e_r}$ with $(p_j, m) = 1$, then

$$\left(\frac{a\mathbb{Z}}{K/F}\right) = \prod_{j=1}^{r} \sigma_{p_j}^{e_j} = \sigma_a : \zeta_m \mapsto \zeta_m^a.$$

Theorem 1.16. *(Artin Reciprocity) Let K/F be an abelian extension of number fields, let G =Gal(K/F), and assume $\mathfrak{m}$ is an ideal of $\mathcal{O}_F$, divisible by all the ramifying primes. Then*
(i) $\mathcal{A} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow G$ is surjective,
(ii) The ideal $\mathfrak{m}$ can be chosen so that it is divisible only by the ramified primes and satisfies $\mathcal{P}^+_{F,\mathfrak{m}} \subseteq ker(\mathcal{A})$,
(iii) $\mathcal{N}_{K/F}(\mathfrak{m}) \subseteq ker(\mathcal{A})$.

Choosing $\mathfrak{m}$ as in (ii), we have a well-defined epimorphism $\mathcal{I}_F(\mathfrak{m})/(\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})) \longrightarrow G$. Since $\#\left(\mathcal{I}_F(\mathfrak{m})/(\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m}))\right) \leq [K : F] = \#G$ by the Universal Norm Index Inequality, in fact we have

$$\mathcal{I}_F(\mathfrak{m})/(\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})) \cong G$$

Proposition 1.17. *Let K/F be an abelian extension of number fields. If $\mathfrak{m}$ is an ideal of $\mathcal{O}_F$ such that $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq N_{K/F}\mathcal{E}_K$, then $\mathfrak{m}$ satisfies Artin Reciprocity.*

Proposition 1.18. *(Completeness Theorem) Let K/F be an abelian extension of number fields. If the ideal $\mathfrak{m}$ of $\mathcal{O}_F$ satisfies Artin Reciprocity, then K is the class field over F of $\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})$.*

A proof of the next result can be found in [Sch], chapter 15.

Theorem 1.19. *(Chebotarev Density) Let K/F be an Galois extension of number fields with Gal$(K/F) = G$. Let $\sigma \in G, [\sigma]_G = \{\tau\sigma\tau^{-1} : \tau \in G\}$. Define*

$$\mathcal{S}_\sigma = \{\textit{unramified primes } \mathfrak{p} \textit{ of } \mathcal{O}_F : \left(\frac{\mathfrak{P}}{K/F}\right) \in [\sigma]_G \textit{ for } \mathfrak{P}|\mathfrak{p}\mathcal{O}_K\}.$$

Then $\delta_F(\mathcal{S}_\sigma) = \dfrac{\#[\sigma]_G}{[K/F]}$.

If $\mathfrak{m}$ satisfies $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F}J_K$, then we have

$$\begin{aligned} \mathcal{I}_F(\mathfrak{m})/(\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})) &\cong G, \text{by Artin Reciprocity;} \\ J_F/(F^\times N_{K/F}J_K) &\cong \mathcal{I}_F(\mathfrak{m})/(\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})), \text{by Proposition 1.14;} \\ J_F &\twoheadrightarrow J_F/(F^\times N_{K/F}J_K), \text{by the canonical surjection.} \end{aligned}$$

Let $\rho_{K/F} : J_F \to G$ be the composition of the above functions. It is surjective with kernel $F^\times N_{K/F}J_K$. We say K is the class field over F of $F^\times N_{K/F}J_K$ and we call $\rho_{K/F}$ the idèlic Artin map.

1.4 The Existence Theorem

Theorem 1.20. *(Ordering Theorem) Let*

$$\Phi : \{\textit{finite abelian extensions } K \textit{ of } F\} \longrightarrow \{\textit{open subgroups } \mathcal{H} \textit{ of } J_F \textit{ that contain } F^\times\}$$

be given by $\Phi(K) = F^\times N_{K/F}J_K$. *Then:*

$$K_1 \subseteq K_2 \Longleftrightarrow \Phi(K_2) \subseteq \Phi(K_1).$$

Corollary 1.21. *Suppose K is the class field to the open subgroup $\mathcal{H}$ of J_F, where $F^\times \subseteq \mathcal{H}$, and let $\mathcal{H}_1 \supseteq \mathcal{H}$ be an open subgroup of J_F. Then $\mathcal{H}_1$ has a class field over F.*

Proposition 1.22. *(Reduction Lemma) Let K/F be a cyclic extension of number fields and suppose $\mathcal{H}$ is an open subgroup of J_F that contains $F^\times$. If $N^{-1}_{K/F}(\mathcal{H})$ has a class field over K, then $\mathcal{H}$ has a class field over F.*

Let n be a positive integer. An abelian group G is said to have exponent n if $g^n = 1$, $\forall g \in G$. Similarly, an abelian extension K/F is said to have exponent n if the abelian group $\mathrm{Gal}(K/F)$ has exponent n.

Let F be an number field. Let $\mathcal{S}$ be a finite set of places of F and assume {infinite places of F} $= \mathcal{S}_\infty \subseteq \mathcal{S}$. Define

$$\begin{gathered} J_{F,\mathcal{S}} = \prod_{v\in\mathcal{S}} F_v^\times \times \prod_{v\notin\mathcal{S}} \mathcal{U}_v \\ F_\mathcal{S} = J_{F,\mathcal{S}} \cap F^\times. \end{gathered}$$

Lemma 1.23. *There is a finite set of places $\mathcal{S} \supseteq \mathcal{S}_\infty$ such that $J_F = F^\times J_{F,\mathcal{S}}$.*

Theorem 1.24. *Let F be a number field that contains all the n^{th} roots of unity. Let $\mathcal{S}$ be a finite set of places of F containing $\mathcal{S}_\infty$, the places v such that $\mathfrak{p}_v|n$, and sufficiently many finite places so that $J_F = F^\times J_{F,\mathcal{S}}$. Let*

$$B = \prod_{v\in\mathcal{S}}(F_v^\times)^n \times \prod_{v\notin\mathcal{S}}\mathcal{U}_v.$$

Then $F^\times B$ has class field $F(F_{\mathcal{S}}^{1/n})$ over F.

Theorem 1.25. *(Existence Theorem) Let F be a number field. Let $\mathcal{H}$ be an open subgroup of J_F with $F^\times \subseteq \mathcal{H}$. Then there is a finite abelian extension K of F such that $\mathcal{H} = F^\times N_{K/F}J_K$*

Proof. Suppose that $J_F/\mathcal{H}$ has exponent n. Assume that F contains the n^{th} roots of unity. Find a set $\mathcal{S}$ as in Lemma 1.24, then enlarge it further to contain all v such that $\mathcal{U}_v \nsubseteq \mathcal{H}$. For this enlarged $\mathcal{S}$, we get $B \subseteq \mathcal{H}$. By Theorem 1.25, $F^\times B$ has a class field and $\mathcal{H} = \mathcal{H}F^\times \supseteq F^\times B$. By Corollary 1.22, $\mathcal{H}$ has a class field too.

In the general case, consider the extension $F(\zeta_n)/F$. We can find a tower of intermediate fields:

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = F(\zeta_n),$$

such that each $\text{Gal}(F_{i+1}/F_i)$ is cyclic. Let $\mathcal{H}_i = N^{-1}_{F_i/F}\mathcal{H}$. Note that $\mathcal{H}_i = N^{-1}_{F_i/F_{i-1}}\mathcal{H}_{i-1}$. We know that $\mathcal{H}_t$ has a class field. Applying the Reduction Lemma to the cyclic extension F_t/F_{t-1}, we conclude that $\mathcal{H}_{t-1}$ has a class field too. Continuing in a finite number of steps, we get that $\mathcal{H}_0$ has a class field. □

Theorem 1.26. *(Kronecker-Weber) Every finite abelian extension F of $\mathbb{Q}$ satisfies $F \subseteq \mathbb{Q}(\zeta)$ for some root of unity ζ.*

Proof. F is the class field of $\mathbb{Q}^\times N_{F/\mathbb{Q}}J_F$. By Corollary 1.11, $\mathbb{Q}^\times\mathcal{E}^+_{\mathbb{Q},m\mathbb{Z}} \subseteq \mathbb{Q}^\times N_{F/\mathbb{Q}}J_F$, for some $m \in \mathbb{Z}$. We know that $\mathbb{Q}(\zeta_m)$ is the class field of $\mathbb{Q}^\times\mathcal{E}^+_{\mathbb{Q},m\mathbb{Z}}$. By the Ordering Theorem,

$$F = \Phi^{-1}(\mathbb{Q}^\times N_{F/\mathbb{Q}}J_F) \subseteq \Phi^{-1}(\mathbb{Q}^\times\mathcal{E}^+_{\mathbb{Q},m\mathbb{Z}}) = \mathbb{Q}(\zeta_m).$$

□

Proposition 1.27. *Let F be a number field. $F_1 = \Phi^{-1}(F^\times\mathcal{E}_F)$ is the maximal unramified abelian extension of F(It is called the Hilbert Class Field of F) and Gal$(F_1/F) \simeq \mathcal{C}_F$ via the Artin map.*

Chapter 2

Thaine's Theorem for odd primes

2.1 Factorization of certain principal ideals

Let $F \neq \mathbb{Q}$ be a real abelian number field and ζ_m a primitive m-th root of unity, where m is the least positive integer such that $F \subseteq \mathbb{Q}(\zeta_m)$ (We call m the conductor of the field F). Let $G = \mathrm{Gal}(F/\mathbb{Q})$. For $j \geq 1$ we define

$$C_j(X) = \left\{ f(X) = \pm \prod_{i=1}^{j} \prod_{k=1}^{m-1} (X^i - \zeta_m^k)^{a_{ik}} : a_{ik} \in \mathbb{Z}, f(X) \in F(X), f(1) \in \mathcal{U}_F \right\},$$

where X is an indeterminate.

Let $C = \cup_{j=1}^{\infty} C_j(1)$ be the group of cyclotomic units. Since $\mathcal{U}_F$ is a noetherian $\mathbb{Z}$-module, there exists $l \geq 1$ such that $C = C_l(1)$.

Proposition 2.1. *We have that $\#W < \infty$, where $W = \mathcal{U}_F/C$.*

Proof. Sinnott[Sin] showed that a subgroup of the cyclotomic units has finite index in the full group of units. It was shown by G. Lettl[Let] that these two groups coincide. □

In this section q is an odd prime greater than l, that splits completely in F, ζ_q is a primitive q-th root of unity, and $K = F(\zeta_q)$.

Proposition 2.2. $f(X) \in C_l(X) \Rightarrow N_{K/F}(f(\zeta_q)) = 1.$

Proof. $f(X) \in F(X) \Rightarrow f(\zeta_q) \in F(\zeta_q) = K$. By Galois Theory, $\mathrm{Gal}(K/F) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{mq})/\mathbb{Q}(\zeta_m))$.

$$\begin{tikzcd}
 & & \mathbb{Q}(\zeta_{mq}) \arrow[dll, dash] \arrow[ddr, dash] & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash] & & K \arrow[dl, dash] \arrow[dr, dash] & \\
 & F \arrow[dr, dash] & & \mathbb{Q}(\zeta_q) \arrow[dl, dash] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

Then

$$\begin{aligned}
N_{K/F}(f(\zeta_q)) =& \prod_{j=1}^{l}\prod_{k=1}^{m-1} N_{\mathbb{Q}(\zeta_{mq})/\mathbb{Q}(\zeta_m)}(\zeta_q^j - \zeta_m^k)^{a_{jk}} \\
=& \prod_{j=1}^{l}\prod_{k=1}^{m-1}(\prod_{i=1}^{q-1}(\zeta_q^i - \zeta_m^k))^{a_{jk}} \\
=& \prod_{j=1}^{l}\prod_{k=1}^{m-1}(\frac{1-\zeta_m^{qk}}{1-\zeta_m^k})^{a_{jk}} = f(1)^{\sigma_q - 1},
\end{aligned}$$

where $\left(\dfrac{q}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right) = \sigma_q : \zeta_m \mapsto \zeta_m^q$. Since q splits completely in F, $\sigma_q\Big|_F = \left(\dfrac{q}{F/\mathbb{Q}}\right)$=id; hence $N_{K/F}(f(\zeta_q)) = 1$. □

Let $\mathfrak{Q}$ be a prime ideal of F above q and $\mathfrak{B}$ the only prime ideal of K above $\mathfrak{Q}$. Choose an integer s such that $\langle s \rangle = (\mathbb{Z}/(q\mathbb{Z}))^\times$ (We call s a primitive root modulo q). Let $\tau \in \mathrm{Gal}(K/F)$, such that $\tau(\zeta_q) = \zeta_q^s$. Then $\langle \tau \rangle = \mathrm{Gal}(K/F)$. Let $H = \mathrm{Gal}(K/\mathbb{Q}(\zeta_q))$.

Proposition 2.3. *If $f(X) \in C_l(X)$, then there exists $\alpha \in K^\times$ such that $\tau(\alpha) = f(\zeta_q)\alpha$. For any such α,*

$$(\alpha) = D \prod_{\sigma \in H} \sigma^{-1}(\mathfrak{B})^{r_\sigma},$$

where D is the lift of an ideal of F and the r_σ are integers such that

$$s^{r_\sigma} \equiv f(1)^\sigma \mod \mathfrak{Q}.$$

Proof. From Hilbert's Theorem 90 and from Proposition 2.2, we conclude that if $f(X) \in C_l(X)$, then there exists $\alpha \in K^\times$ such that $\tau(\alpha) = f(\zeta_q)\alpha$.

We have the following prime ideal decompositions:

$$\begin{aligned} q\mathcal{O}_F &= \prod_{\sigma\in G} \sigma(\mathfrak{Q}), \\ (\zeta_q-1)\mathcal{O}_K &= \prod_{\sigma\in H} \sigma(\mathfrak{B}), \\ \mathfrak{Q}\mathcal{O}_K &= \mathfrak{B}^{q-1}, \\ q\mathcal{O}_K &= \prod_{\sigma\in H} \sigma(\mathfrak{B})^{q-1}. \end{aligned}$$

Then

$$(\alpha) = D\prod_{\sigma\in H} \sigma^{-1}(\mathfrak{B})^{r_\sigma},$$

where D is the lift of an ideal of F relatively prime to q and the r_σ are integers.

Let $\sigma \in H$ and α, r_σ be as above, define $\gamma = \alpha/(\zeta_q-1)^{r_\sigma}$. Then $\text{ord}_{\sigma^{-1}(\mathfrak{B})}(\gamma) = 0$, which implies that there exists $\lambda, \mu \in \mathcal{O}_K$, non-divisible by $\sigma^{-1}(\mathfrak{B})$, such that $\gamma = \lambda/\mu$. Since $\#T(\sigma^{-1}(\mathfrak{B})/\sigma^{-1}(\mathfrak{Q})) = q-1 = \#\text{Gal}(K/F) = \#\langle\tau\rangle$, we have that $\tau \in T(\sigma^{-1}(\mathfrak{B})/\sigma^{-1}(\mathfrak{Q}))$. Then $\tau(\lambda) \equiv \lambda$ and $\tau(\mu) \equiv \mu \mod \sigma^{-1}(\mathfrak{B})$. Hence $\tau(\gamma) \equiv \gamma \not\equiv 0 \mod \sigma^{-1}(\mathfrak{B})$.

If $\tau(\alpha) = f(\zeta_q)\alpha$, then $((\zeta_q^s-1)/(\zeta_q-1))^{r_\sigma}\tau(\gamma) = f(\zeta_q)\gamma$. On the other hand, $0 < d < p \Rightarrow (\zeta_q^d-1)/(\zeta_q-1)$ is an unit $\Rightarrow (\zeta_q^d-1) = (\zeta_q-1) = \prod \sigma^{-1}(\mathfrak{B}) \Rightarrow \zeta_q^d \equiv 1 \mod \sigma^{-1}(\mathfrak{B}) \Rightarrow s \equiv \sum_{i=0}^{s-1}\zeta_q^i = (\zeta_q^s-1)/(\zeta_q-1) \mod \sigma^{-1}(\mathfrak{B}) \Rightarrow s^{r_\sigma} \equiv ((\zeta_q^s-1)/(\zeta_q-1))^{r_\sigma} \mod \sigma^{-1}(\mathfrak{B})$. Therefore

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

This implies that $s^{r_\sigma} \equiv f(1) \mod \sigma^{-1}(\mathfrak{B})$, hence $s^{r_\sigma} \equiv \sigma(f(1)) \mod \mathfrak{B}$ and also mod $\mathfrak{Q}$, since $f(1) \in K$. □

Taking norms we conclude that

$$(N_{K/F}(\alpha)) = D^{q-1}\prod_{\sigma\in G} \sigma^{-1}(\mathfrak{Q})^{r_\sigma},$$

for some ideal D of F.

2.2 Ideal classes and units. A local-global theorem

Fix an embedding of F into $\mathbb{R}$, and define $|x| = \sup\{x, -x\}$. Given an ideal class $\mathcal{C}$ of F and a positive integer b, we define $P(\mathcal{C}, b)$ as the set of all prime ideals $\mathfrak{Q} \in \mathcal{C}$ above odd primes $q > l$, splitting completely in F and such that $q \equiv 1 \bmod b$.

Let $\delta \in C$, $\mathcal{C}$ an ideal class and b a positive integer. From Proposition 2.3 we conclude that for all $\mathfrak{Q} \in P(\mathcal{C}, b)$ there exists a non-zero ideal $\mathcal{R}_{\mathfrak{Q}}$ of F such that $\mathcal{R}_{\mathfrak{Q}}^b \prod\limits_{\sigma \in G} \sigma^{-1}(\mathfrak{Q})^{r_\sigma(\mathfrak{Q})}$ is a principal ideal, where the integers $r_\sigma(\mathfrak{Q})$ satisfy $s_{\mathfrak{Q}}^{r_\sigma(\mathfrak{Q})} \equiv \sigma(\delta) \mod \mathfrak{Q}$.

Suppose that $P(\mathcal{C}, b)$ is non-empty. Let $\sigma \in G$ be fixed. We define the number $g = g(\delta, \mathcal{C}, b, \sigma)$ as the greatest common divisor of b and of all the $r_\sigma(\mathfrak{Q})$ such that $\mathfrak{Q} \in P(\mathcal{C}, b)$.

Proposition 2.4. *$P(\mathcal{C}, b) \neq \emptyset \Rightarrow \forall \mathfrak{Q} \in P(\mathcal{C}, b)\ \exists\ \beta_{\mathfrak{Q}} \in \mathbb{Z}$ such that $\sigma(\delta) \equiv \beta_{\mathfrak{Q}}^g \mod \mathfrak{Q}$.*

Proposition 2.5. *Let F be any real number field.*
(A) If $P(\mathcal{C}, b) \neq \emptyset$, then it is an infinity set;
(B) If F is abelian and the order of $\mathcal{C}$ is prime to $[F : \mathbb{Q}]$, then $P(\mathcal{C}, b) \neq \emptyset$;
(C) If $F \subseteq \mathbb{Q}(\zeta_{p^r})$ and $b = p^n$ with p prime and r, n positive integers, then $P(\mathcal{C}, b) \neq \emptyset$;

Proof. Let F_1 be the Hilbert Class Field of F. We know that $\mathrm{Gal}(F_1/F) \simeq \mathcal{C}_F$ via the Artin map. Let $\varphi \in \mathrm{Gal}(F_1/F)$ corresponding to $\mathcal{C}$. Suppose $P(\mathcal{C}, b) \neq \emptyset$ and let $\mathfrak{Q} \in P(\mathcal{C}, b)$, then $\varphi = \left(\dfrac{\mathfrak{Q}}{F_1/F}\right)$. Since $q \equiv 1 \mod b$, we have that q splits completely in $\mathbb{Q}(\zeta_b)$, then q splits completely in $F(\zeta_b)$, hence the same is true for $\mathfrak{Q}$. Let $J = F_1 \cap F(\zeta_b)$. Then $\varphi\Big|_J = \left(\dfrac{\mathfrak{Q}}{F_1/F}\right)\Big|_J = \left(\dfrac{\mathfrak{Q}}{J/F}\right)$ =id.

$$\begin{tikzcd}
& F_1(\zeta_b) \arrow[dl, dash] \arrow[dr, dash] & \\
F(\zeta_b) \arrow[dr, dash] & & F_1 \arrow[dl, dash] \\
& J \arrow[d, dash] & \\
& F &
\end{tikzcd}$$

By Galois Theory, $\mathrm{Gal}(F_1/J) \simeq \mathrm{Gal}(F_1(\zeta_b)/F(\zeta_b))$. Then we can extend φ to an automorphism $\Phi \in \mathrm{Gal}(F_1(\zeta_b)/F(\zeta_b))$. By the Chebotarev Density Theorem,

$$\delta_{F(\zeta_b)}(\mathcal{S}_\Phi) = \frac{1}{[F_1(\zeta_b) : F(\zeta_b)]}.$$

Since $\delta_{F(\zeta_b)}(\mathfrak{p} \in \mathcal{S}_\Phi; f(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})) > 1) = 0$, we have that $\delta_{F(\zeta_b)}(\mathfrak{p} \in \mathcal{S}_\Phi; f(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})) = 1) > 0$, then the set $\{\mathfrak{p} \in \mathcal{S}_\Phi; f(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})) = 1 = e(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})), \mathfrak{p}$ does not divide $2\}$ is infinite. For any $\mathfrak{p}$ in the above set, we can use the Consistency Property of the Artin map to get $\left(\frac{\mathfrak{Q}}{F_1/F}\right) = \left(\frac{\mathfrak{p}}{F_1(\zeta_b)/F(\zeta_b)}\right)\Bigg|_{F_1} = \varphi$, where $\mathfrak{Q} = \mathfrak{p} \cap \mathcal{O}_K$. Hence $\mathfrak{Q} \in \mathcal{C}$. If $f(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})) = 1 = e(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z}))$, then $f(\mathfrak{Q}/(\mathfrak{Q} \cap \mathbb{Z})) = 1 = e(\mathfrak{Q}/(\mathfrak{Q} \cap \mathbb{Z}))$ and the prime $q \in \mathbb{Z}$ above $\mathfrak{Q}$ splits completely in $\mathbb{Q}(\zeta_b)$, then $\mathfrak{Q} \in P(\mathcal{C}, b)$. Therefore $P(\mathcal{C}, b)$ is an infinite set.

Let F be a real abelian number field. By Galois Theory (See Proposition 3.20 of [Mil]), Gal$(F(\zeta_b)/\mathbb{Q})$ is isomorphic to a subgroup of Gal$(F/\mathbb{Q})\times$Gal$(\mathbb{Q}(\zeta_b)/\mathbb{Q})$, which implies that J is abelian over $\mathbb{Q}$ and unramified over F. Suppose a prime p divides $[J : F]$ but does not divide $[F : \mathbb{Q}]$. Let $J^{(p)}$ be the subfield fixed by the p-Sylow subgroup of Ga(J/F), which is also the p-Sylow subgroup of Gal$(J/\mathbb{Q})$, because

$p \nmid [F : \mathbb{Q}]$. By the structure Theorem of abelian groups, Gal$(J/\mathbb{Q})$ =Gal$(J/J^{(p)}) \times H$. By Galois Theory, Gal$(J^H/\mathbb{Q}) \simeq$ Gal$(J/\mathbb{Q})/H \simeq$ Gal$(J/J^{(p)}) = p-$group.

Let q be any rational prime. Since $J/J^{(p)}$ is unramified everywhere, we have that $T(J/q)\cap$Gal$(J/J^{(p)})$ =id, then $p \nmid e(J/q)$. Hence $p \nmid e(J^H/q)$, which implies that $e(J^H/q) = 1$, because $T(J^H/q)$ is a subgroup of a p-group. Then J^H is unramified p-extension of $\mathbb{Q}$, contradiction. Then gcd(ord($\mathcal{C}$) , $[F : \mathbb{Q}]) = 1 \Rightarrow$ gcd(ord($\mathcal{C}$) , $[J : \mathbb{Q}]$)=1. Since ord($\mathcal{C}$)=ord(φ), we must have $\varphi\Big|_J$ =id; thus $P(\mathcal{C}, b) \neq \emptyset$.

If $F \subseteq \mathbb{Q}(\zeta_{p^r})$ and $b = p^n$, then $F(\zeta_b) \subseteq \mathbb{Q}(\zeta_{p^{r+n}})$. Since p is totally ramified in $\mathbb{Q}(\zeta_{p^r})$, we have the same in J. Then J is totally ramified and unramified over F, therefore $J = F$, $\varphi\Big|_J$ =id. This proves (c). □

Proposition 2.6. *Let F be any number field. Let γ be a positive element of $\mathcal{O}_F$, and $c > 0$ a divisor of b. Suppose that $P(\mathcal{C}, b) \neq \emptyset$ and that for all, except possibly a finite set, prime ideals $\mathfrak{Q} \in P(\mathcal{C}, b)$ there exists $\beta_{\mathfrak{Q}} \in \mathcal{O}_K$ such that $\gamma \equiv \beta_{\mathfrak{Q}}^c \mod \mathfrak{Q}$. 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 $\nu = \sqrt[c]{\gamma}$ be the positive c-th root of γ and let L be the Galois closure of $F(\nu)/F$, i.e. the intersection of all Galois extensions of F that contains $F(\nu)$. Let $p(X)$ be the irreducible polynomial of ν over F, then $p(X)|X^c - \gamma$ and L is the splitting field of $p(X)$ over F. Hence $L = F(\nu, \zeta_e)$ for some $e|c$.

Suppose $L \subseteq F_1(\zeta_b)$. By Galois Theory, Gal$(F_1(\zeta_b)/F)$ is isomorphic to a subgroup of Gal$(F_1/F)\times$Gal$(\mathbb{Q}(\zeta_b)/\mathbb{Q})$, which implies that $F_1(\zeta_b)/F$ is abelian, then L/F and $F(\nu)/F$ are abelian. Hence $L = F(\nu)$, $\zeta_e \in F(\nu) \subseteq \mathbb{R}$, $\zeta_e = \pm 1$. Therefore $p(X) = X - \nu$ if c is odd and $p(X) = X^2 - \nu^2$ if c is even. In the first case take $\beta = \nu$; in the other case take $\beta = \nu^2$.

We will prove that $L \subseteq F_1(\zeta_b)$. Let $M = LF_1(\zeta_b)$ and $\varphi \in$Gal(F_1/F) corresponding to $\mathcal{C}$. Since $P(\mathcal{C}, b) \neq \emptyset$, we have that $\varphi\Big|_J$ =id. By Galois Theory, Gal$(F_1/J) \simeq$ Gal$(F_1(\zeta_b)/F(\zeta_b)) \simeq$ Gal$(M/L(\zeta_b))$, so we can extend φ to an automorphism $\Phi \in$Gal$(M/L(\zeta_b))$.

$$\begin{tikzcd}
 & & & M \arrow[dl, dash] \arrow[dr, dash] & & \\
 & & L(\zeta_b) \arrow[dl, dash] \arrow[dr, dash] & & F_1(\zeta_b) \arrow[dl, dash] \arrow[dr, dash] & \\
 & L \arrow[dl, dash] \arrow[dr, dash] & & F(\zeta_b) \arrow[dl, dash] \arrow[dr, dash] & & F_1 \arrow[dl, dash] \\
F(\nu) \arrow[dr, dash] & & F(\zeta_e) \arrow[dl, dash] & & J \arrow[dlll, dash] & \\
 & F & & & &
\end{tikzcd}$$

Let $f \in \Phi G$, where $G =$ Gal$(M/F_1(\zeta_b))$. By the Chebotarev Density Theorem, the set $\{\mathfrak{p} \in \mathcal{S}_f; f(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})) = 1 = e(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})), \mathfrak{p}$ does not divide $2\}$ is infinite. Fix $\mathfrak{p}$ in the above set. Let $\mathfrak{P}|\mathfrak{p}\mathcal{O}_M$ be such that $\left(\dfrac{\mathfrak{P}}{M/F(\zeta_b)}\right) = f$.

$$\begin{tikzcd}
 & M \arrow[d, dash] & \\
 & F_1(\zeta_b) \arrow[dl, dash] \arrow[dr, dash] & \\
F(\zeta_b) \arrow[dr, dash] & & F_1 \arrow[dl, dash] \\
 & J \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

By the Consistency Property and the fact that F_1/F is abelian, $\left(\dfrac{\mathfrak{Q}}{F_1/F}\right) = \left(\dfrac{\mathfrak{P}}{M/F(\zeta_b)}\right)\Bigg|_{F_1} = f\Bigg|_{F_1} = \varphi$, where $\mathfrak{Q} = \mathfrak{p} \cap \mathcal{O}_F$. Hence $\mathfrak{Q} \in \mathcal{C}$. If $f(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})) = 1 = e(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z}))$, then $f(\mathfrak{Q}/(\mathfrak{Q} \cap \mathbb{Z})) = 1 = e(\mathfrak{Q}/(\mathfrak{Q} \cap \mathbb{Z}))$ and the prime $q \in \mathbb{Z}$ above $\mathfrak{Q}$ splits completely in $\mathbb{Q}(\zeta_b)$, then $\mathfrak{Q} \in P(\mathcal{C}, b)$ and we can choose $\mathfrak{p}$ so as to avoid the finitely many exceptions and such that $\mathfrak{Q}$ does not divide γ.

Any such $\mathfrak{Q}$ splits completely in L, because $p(X)$, reduced mod $\mathfrak{Q}$, splits completely over the field $\mathcal{O}_F/\mathfrak{Q}$ $(p(X) \mid X^c - \gamma, X^c - \gamma \equiv X^c - \beta_{\mathfrak{Q}}^c$ mod $\mathfrak{Q}$ and $\mathcal{O}_F/\mathfrak{Q}$ contains the c-th roots of unity since $c \mid b$ and $b \mid (q-1) = |(\mathcal{O}_F/\mathfrak{Q})^\times|)$ and because $\mathfrak{Q}$ does not divide the discriminant of ν over F.By the Dedekind-Kummer Theorem, $\mathfrak{Q}$ splits completely over L.

$$\begin{tikzcd}
 & M \arrow[d, dash] & \\
 & L(\zeta_b) \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & F(\zeta_b) \arrow[dl, dash] \\
 & F(\zeta_e) \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

By the Consistency Property, $f\Bigg|_L = \left(\dfrac{\mathfrak{P}}{M/F(\zeta_b)}\right)\Bigg|_L = \left(\dfrac{\mathfrak{P} \cap L}{L/F}\right)$=id, because $(\mathfrak{P} \cap L)|\mathfrak{Q}\mathcal{O}_L$. Then $\Phi G \subseteq$ Gal(M/L), hence $\Phi \in$Gal(M/L) and $G \subseteq$Gal(M/L). By Galois Theory, $L \subseteq F_1(\zeta_b)$.

□

For each unit $\varepsilon \neq \pm 1$ of $\mathcal{O}_F$ we define $\phi(\varepsilon)$ as the greatest integer k such that

$\varepsilon = \mu^k$ for some $\mu \in F$. We have $\phi(\sigma(\varepsilon)) = \phi(\varepsilon), \forall \sigma \in G$. Let (c, d)=gcd(c, d) for any $c, d \in \mathbb{Z}$.

Lemma 2.7. *Let $\delta \in \mathcal{U}_F - \{\pm 1\}$. If $\delta = \beta^c$ with $\beta \in K$, then $c|\phi(\delta)$.*

Proof. Let $\mu \in F$ such that $\delta = \mu^\phi$. Let $d = (c, \phi)$, m=lcm(c, ϕ), and $x, y \in \mathbb{Z}$ such that $xc + y\phi = d$. Observe that $m = c\phi/d$, then $(\mu^x \beta^y)^m = (\mu^\phi)^{xc/d}(\beta^c)^{y\phi/d} = \delta^{(xc+y\phi)/d} = \delta$. Hence $m \leq \phi$, therefore $c|\phi$. □

Theorem 2.8. *Let $\delta \in C - \{\pm 1\}$. Suppose $P(\mathcal{C}, b) \neq \emptyset$, then*
(i) If b is odd, then $g = (\phi(\delta), b)$.
(ii) If b is even and $\sigma(\delta) > 0$, then $g = (\phi(\delta), b)$ or $g = 2(\phi(\delta), b)$.
(iii) 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. Let $d = (\phi(\delta), b)$, $\phi(\delta) = md, b = Md$, and $q - 1 = tb$. Let $\delta = \mu^{\phi(\delta)}$, with $\mu \in K$. $\mathfrak{Q} \in P(\mathcal{C}, b) \Rightarrow \exists n$ such that $\sigma(\mu) \equiv n \bmod \mathfrak{Q}$ (since $\frac{\mathcal{O}_F}{\mathfrak{Q}} \simeq \frac{\mathbb{Z}}{q\mathbb{Z}}$) $\Rightarrow s_{\mathfrak{Q}}^{r_\sigma(\mathfrak{Q})} \equiv \sigma(\mu)^{\phi(\delta)} \equiv n^{\phi(\delta)} \bmod \mathfrak{Q} \Rightarrow s_{\mathfrak{Q}}^{r_\sigma(\mathfrak{Q})} \equiv n^{\phi(\delta)} \bmod q \Rightarrow s_{\mathfrak{Q}}^{r_\sigma(\mathfrak{Q})Mt} \equiv n^{\phi(\delta)Mt} \equiv (n^{tb})^m \equiv 1 \bmod q \Rightarrow \exists k \in \mathbb{N}$ such that $r_\sigma(\mathfrak{Q})Mt = k(q-1) = ktMd \Rightarrow d|r_\sigma(\mathfrak{Q})$. Therefore $(\phi(\delta), b)$ divides g in any case.

By Proposition 2.4, $\forall \mathfrak{Q} \in P(\mathcal{C}, b)$ $\exists \beta_{\mathfrak{Q}} \in \mathbb{Z}$ such that $\sigma(\delta) \equiv \beta_{\mathfrak{Q}}^g$ mod$\mathfrak{Q}$; hence $\sigma(\delta^2) \equiv \beta_{\mathfrak{Q}}^{2g}$ mod$\mathfrak{Q}$. Let $c = (2g, b)$; since $P(\mathcal{C}, b) \neq \emptyset$, we have by Proposition 2.6 that $\sigma(\delta) = \gamma^g$ or $\sigma(\delta) = \gamma^{g/2}$ if $\sigma(\delta) > 0$ and that $\sigma(\delta^2) = \eta^c$ if c is odd and $\sigma(\delta^2) = \eta^{c/2}$ if c is even, for some $\gamma, \eta \in K$. By the Lemma 2.7 we conclude that:
(i) if b is odd, then $g = c$ divides $(\phi(\delta^2), b) = (\phi(\delta), b)$. Therefore $g = (\phi(\delta), b)$.
(ii) If b is even and $\sigma(\delta) > 0$, then $g|2(\phi(\delta), b)$. Therefore $g = (\phi(\delta), b)$ or $g = 2(\phi(\delta), b)$.
(iii) In all cases, c divides $2\phi(\delta^2) = 4\phi(|\delta|)$; hence $c|4(\phi(|\delta|), b)$. □

2.3 A relation between the ideal class group and the units of F

Let p be an odd prime. Denote the p-Sylow subgroup of a group H by $(H)_p$.

Proposition 2.9. *Let $\delta \in C$ and let p^n be an exponent of $(\mathcal{C}_F)_p$. If $\mathcal{C} \in (\mathcal{C}_F)_p$, $\mathfrak{Q} \in P(\mathcal{C}, p^n)$, then $\lambda = \lambda_{\mathfrak{Q}} = \sum_{\sigma \in G} r_\sigma(\mathfrak{Q})\sigma^{-1}$ annihilates $\mathcal{C}$, where the r_σ are the integers of Proposition 2.3.*

Proof. By Proposition 2.3, there exists an ideal class $D_{\mathfrak{Q}}$ such that $D_{\mathfrak{Q}}^{p^n} \prod_{\sigma \in G} \sigma^{-1}(\mathcal{C})^{r_\sigma} = 1$. Since all conjugates of $\mathcal{C}$ belong to $(\mathcal{C}_F)_p$, we have that $D_{\mathfrak{Q}}^{p^n} \in (\mathcal{C}_F)_p$. Then $D_{\mathfrak{Q}} \in (\mathcal{C}_F)_p$ and $D_{\mathfrak{Q}}^{p^n} = 1$. Therefore $\mathcal{C}^\lambda = 1$. □

Proposition 2.10. *Let p^n be an exponent of $(\mathcal{C}_F)_p$. Suppose that $\delta \in C$ is such that for all $\sigma \in G$ there exists an integer c_σ, non-divisible by p, such that*

$$\sigma(\delta) \equiv \delta^{c_\sigma} \mod (\mathcal{U}_F^{p^n}).$$

Let $\mathcal{C} \in (\mathcal{C}_F)_p$ be such that $P(\mathcal{C}, p^n) \neq \emptyset$ and denote $\sum_{\sigma \in G} c_\sigma \sigma^{-1} \in \mathbb{Z}[G]$ by ω. Then $(\phi(\delta), p^n)\omega$ annihilates $\mathcal{C}$.

Proof. Let $\mathfrak{Q} \in P(\mathcal{C}, p^n)$ and let $q, s, r_\sigma, \sigma \in G$, be as in Proposition 2.9. Then $\lambda_{\mathfrak{Q}} = \sum_{\sigma \in G} r_\sigma(\mathfrak{Q})\sigma^{-1}$ annihilates $\mathcal{C}$. Let $d = d(\mathfrak{Q})$ be a positive integer such that $\delta \equiv s^d$ mod $\mathfrak{Q}$ (Recall that $\frac{\mathcal{O}_K}{\mathfrak{Q}} \simeq \frac{\mathbb{Z}}{q\mathbb{Z}}$). By hypothesis, $\exists \varepsilon_\sigma \in \mathcal{U}_F$ such that $\sigma(\delta) = \delta^{c_\sigma}\varepsilon_\sigma^{p^n}$. Let t be a positive integer such that $\varepsilon_\sigma \equiv s^t$ mod $\mathfrak{Q}$. Then $s^{r_\sigma} \equiv \sigma(\delta) \equiv \delta^{c_\sigma}\varepsilon_\sigma^{p^n} \equiv s^{dc_\sigma + p^n t}$ mod $\mathfrak{Q}$. Hence $s^{r_\sigma} \equiv s^{dc_\sigma + p^n t}$ mod q.

Suppose $r_\sigma < dc_\sigma + p^n t$. If q divides $s^{r_\sigma}(1 - s^{dc_\sigma + p^n t - r_\sigma})$, then $s^{dc_\sigma + p^n t - r_\sigma} \equiv 1$ mod q. Since ord (s mod q)=q-1, we have that $dc_\sigma + p^n t \equiv r_\sigma$ mod $q-1$ and also mod p^n, because $p^n | q-1$. Then $\mathcal{C}^{d\omega} = \mathcal{C}^\lambda = 1$, which implies that $\text{ord}_{\mathcal{C}_F}\mathcal{C}^\omega | g_0$, where g_0 is the greatest common divisor of p^n and all the $d(\mathfrak{Q}), \mathfrak{Q} \in P(\mathcal{C}, p^n)$, so $g_0\omega$ annihilates $\mathcal{C}$.

Given $\sigma \in G$, we have that $r_\sigma = mp^n + dc_\sigma$. If $(p, c_\sigma) = 1$, then $\text{ord}_p(r_\sigma)$=min$(n, \text{ord}_p(d))$, hence $g_0 = g(\delta, \mathcal{C}, p^n, \sigma)$. By Theorem 2.8, $g_0 = (\phi(\delta), p^n)$ when p is odd. □

Lemma 2.11. *$\exists \varepsilon \in \mathcal{U}_F$ such that $[\mathcal{U}_F : \{\varepsilon^\lambda, \lambda \in \mathbb{Z}[G]\}] < \infty$.*

Proof. It is enough to show that

$$\det[\ln|\sigma_i\sigma_j(\varepsilon)|]_{1 \le i,j \le r} \neq 0,$$

for some $\varepsilon \in \mathcal{U}_F$, where $G = \{\sigma_0 = \text{id}, \sigma_1, \cdots, \sigma_r\}, r = \#G - 1$. Consider the polynomial

$$f(X_1, \cdots, X_r) = \det[X_{p(i,j)}]_{1 \le i,j \le r},$$

where the integers $p(i,j), 0 \le p(i,j) \le r$, are defined by $\sigma_i\sigma_j = \sigma_{p(i,j)}$ and $X_0 = -X_1 - \cdots - X_r$. Let $\varepsilon_1, \cdots, \varepsilon_r$ be a fundamental system of units of F. If we had $f(\ln|\sigma_1(\varepsilon)|, \cdots, \ln|\sigma_r(\varepsilon)|) = 0$ for all $\varepsilon = \varepsilon_1^{y_1} \cdots \varepsilon_r^{y_r}$, with $y_i \in \mathbb{Z}$, then the polynomial

$$g(Y_1, \cdots, Y_r) = f\left(\sum_{j=1}^{r} \ln|\sigma_1(\varepsilon_j)|.Y_j, \cdots, \sum_{j=1}^{r} \ln|\sigma_r(\varepsilon_j)|.Y_j\right)$$

would be identically zero (since $g(\mathbb{Z}^r) = \{0\}$ and a nonzero polynomial has a finite number of zeros).

On the other hand, let $[a_{ij}]_{1\leq i,j\leq r}$ be the inverse matrix of $[\ln|\sigma_i(\varepsilon_j)|]_{1\leq i,j\leq r}$. Define $Z_i = \sum_{j=1}^r a_{ij}$. We have that $\sum_{j=1}^r \ln|\sigma_i(\varepsilon_j)|.Z_j = \sum_{j=1}^r \ln|\sigma_i(\varepsilon_j)|.\sum_{k=1}^r a_{jk} = \sum_{k=1}^r\sum_{j=1}^r \ln|\sigma_i(\varepsilon_j)|.a_{jk} = \sum_{k=1}^r I_{ik} = 1$. Then $g(Z_1, \cdots, Z_r) = f(1, \cdots, 1) = \pm\#G^{\#G-2} \neq 0$. A contradiction. □

Proposition 2.12. *Suppose that $p \nmid [F : \mathbb{Q}]$. Let p^k be an exponent of $(W)_p$, $\chi : G \to \mathbb{Z}_p^\times$ a non-trivial Dirichlet character, $e_\chi = \dfrac{1}{\#G}\displaystyle\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1} \in \mathbb{Z}_p[G]$ the corresponding idempotent and p^a the exact exponent of the χ-component $e_\chi(W)_p$ of $(W)_p$. Then there exists $\delta \in C$ such that $p^{a+1} \nmid \phi(\delta)$ and such that*

$$\sigma(\delta) \equiv \delta^{\chi(\sigma)} \mod \mathcal{U}_F^{p^k},\ \forall\sigma \in G.$$

Remark: Raising a number to a p-adic exponent means, when we are working modulo p^kth power, we should take an integer congruent to the exponent mod p^k.

Proof. The affirmation is trivial if $k = 0$; assume $k \geq 1$. Since $(W)_p \simeq \mathcal{U}_F/C\mathcal{U}_F^{p^k}$, we have

$$e_\chi(W)_p \simeq e_\chi(\mathcal{U}_F/C\mathcal{U}_F^{p^k}) \simeq \frac{e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k})}{e_\chi(\mathcal{U}_F^{p^k}C/\mathcal{U}_F^{p^k})};$$

so the elements $\eta \in \mathcal{U}_F$ such that $\eta C \in e_\chi(W)_p$ are the same as the elements $\eta \in \mathcal{U}_F$ such that $\eta\mathcal{U}_F^{p^k} \in e_\chi(e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k}))$. Therefore, for such η, we have $\eta^{p^a c} \in C$, for some c prime to p, and

$$\sigma(\eta) \equiv \eta^{\chi(\sigma)} \bmod \mathcal{U}_F^{p^k}.$$

We affirm that there exists some η as above such that $\eta \notin \mathcal{U}_F^{p^k}$. In fact, otherwise we would have

$$e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k}) \subseteq \mathcal{U}_F^p/\mathcal{U}_F^{p^k} \subseteq (\mathcal{U}_F/\mathcal{U}_F^{p^k})^p,$$

which implies that

$$e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k}) \subseteq e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k})^p \subseteq \cdots \subseteq e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k})^{p^k} = 1.$$

That is, $e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k}) = 1$. Then, since for $j \geq k$

$$e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^k}) \simeq e_\chi\left(\frac{\mathcal{U}_F/\mathcal{U}_F^{p^j}}{(\mathcal{U}_F/\mathcal{U}_F^{p^j})^{p^k}}\right) \simeq \frac{e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^j})}{e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^j})^{p^k}},$$

we must have that $e_\chi(\mathcal{U}_F/\mathcal{U}_F^{p^j}) = 1$ for all $j \geq 1$. Let $\widehat{\mathcal{U}_F} = \varprojlim\ \mathcal{U}_F/\mathcal{U}_F^{p^j}$. For the above equality, $e_\chi(\widehat{\mathcal{U}_F}) = 1$.

By Lemma 2.11, there exists a unit $\varepsilon \in \mathcal{U}_F$ such that the group $\{\varepsilon^{\lambda} : \lambda \in \mathbb{Z}_p[G]\}$ of $\widehat{\mathcal{U}_F}$ has finite index in this group. For such ε, consider the function $\lambda \mapsto \varepsilon^{\lambda}$ from $\mathbb{Z}_p[G]$ to $\widehat{\mathcal{U}_F}$. From what we have show, its kernel is the ideal of $\mathbb{Z}_p[G]$ generated by $e_{\chi_0}(\chi_0$ the trivial character). Since this kernel contains e_χ, we must have $\chi = \chi_0$, a contradiction.

Therefore there exists some $\eta \in \mathcal{U}_F$ as claimed. Let c be prime to p, such that $\delta = \eta^{p^a c} \in C$; then δ satisfies the conditions of the proposition. Note that $p^{a+1} \nmid \phi(\delta)$ since $p \nmid \phi(\eta)$. □

Theorem 2.13. *Let p be a prime such that $p \nmid [K : \mathbb{Q}], \chi : G \to \mathbb{Z}_p^{\times}$ a non-trivial Dirichlet character, $e_\chi \in \mathbb{Z}[G]$ the corresponding idempotent. If p^a is the exact exponent of $e_\chi(W)_p$, then p^a annihilates $e_\chi(\mathcal{C}_F)_p$.*

Proof. Let p^n be an exponent of both $(W)_p$ and $(\mathcal{C}_F)_p$. For each $\sigma \in G$, let c_σ be an integer such that $c_\sigma \equiv \chi(\sigma)$ mod p^n. Then $\sum\limits_{\sigma \in G} c_\sigma \sigma^{-1} \equiv (\#G)e_\chi \ \mathrm{mod} p^n$.By Proposition 2.12, $\exists \delta \in C$ such that $p^{a+1} \nmid \phi(\delta)$ and such that $\sigma(\delta) \equiv \delta^{\chi(\sigma)} \equiv \delta^{c_\sigma} \mathrm{mod}\ \mathcal{U}_K^{p^n}, \forall \sigma \in G$.

Let $\mathcal{C} \in (\mathcal{C}_F)_p$. By Proposition 2.5(b), $P(\mathcal{C}, b) \neq \emptyset$. By Proposition 2.10, $(\phi(\delta), p^n) \sum\limits_{\sigma \in G} c_\sigma \sigma^{-1}$ annihilates $\mathcal{C}$. If $p^{a+1} \nmid \phi(\delta)$, then $(\phi(\delta), p^n) \mid p^a$, then $p^a \sum\limits_{\sigma \in G} c_\sigma \sigma^{-1}$ annihilates $\mathcal{C}$. Since $p \nmid \#G$, we have that there exists $d \in \mathbb{Z}$ such that $d\#G \equiv 1 \mathrm{mod}$ p^n. Then $p^a d \sum\limits_{\sigma \in G} c_\sigma \sigma^{-1} \equiv p^a e_\chi \mathrm{mod}\ p^n$. Therefore p^a annihilates $e_\chi(\mathcal{C}_F)_p$. □

Corollary 2.14. *If $F \subseteq \mathbb{Q}(\zeta_p) \cap \mathbb{R}$, then every annihilator (in $\mathbb{Z}[G]$) of $(W)_p$ also annihilates $(\mathcal{C}_F)_p$.*

Proof. Let $\sum\limits_{\sigma \in G} b_\sigma \sigma \in \mathbb{Z}[G]$ be an annihilator of $(W)_p$. Let χ be a non-trivial p-adic-valued Dirichlet character of G. Since $(\sum\limits_{\sigma \in G} b_\sigma \sigma) e_\chi = \sum\limits_{\sigma \in G} b_\sigma \chi(\sigma) e_\chi$, we have that $\sum\limits_{\sigma \in G} b_\sigma \chi(\sigma)$ annihilates $e_\chi(W)_p$. Then $p^{a(\chi)} \mid \sum\limits_{\sigma \in G} b_\sigma \chi(\sigma)$, where $p^{a(\chi)}$ is the exact exponent of $e_\chi(W)_p$. By Theorem 2.13, $p^{a(\chi)}$ annihilates $e_\chi(\mathcal{C}_F)_p$, so every multiple of it does the same.

Since $F \subseteq \mathbb{Q}(\zeta_p)$, we have that $\sum_\chi e_\chi = 1$, where χ runs over all p-adic-valued Dirichlet characters of G. Then $\sum\limits_{\sigma \in G} b_\sigma \sigma = \sum\limits_{\sigma \in G} b_\sigma \sigma \sum\limits_{\chi} e_\chi = \sum\limits_{\chi} \sum\limits_{\sigma \in G} b_\sigma \chi(\sigma) e_\chi$. Therefore $\sum\limits_{\sigma \in G} b_\sigma \sigma$ annihilates $(\mathcal{C}_F)_p$. □

2.4 Annihilators of ideal classes of prime order to $[F:\mathbb{Q}]$

In order to simplify notation, we identify elements of a given abelian group with its class modulo a subgroup.

Proposition 2.15. *Let ρ be any irreducible character of Δ with values in $\mathbb{F}_p$ and let e_ρ be the idempotent of $\mathbb{Z}[\Delta]$ associated to ρ, i. e.*

$$e_\rho = (\#G)^{-1} \sum_{g\in\Delta} \rho(1)\rho(g^{-1})g.$$

Then $p^a e_\rho$ annihilates $(\mathcal{C}_F)_p$, where p^a is the exact exponent of $e_\rho(W)_p$.

Proof. Let p^n be an exponent of both $(\mathcal{C}_F)_p$ and $(W)_p$. Let $\mathcal{C} \in (\mathcal{C}_F)_p$. By Proposition 2.5(B), we know that $P(\mathcal{C}, p^n)$ is non-empty.

For each $\mathfrak{Q} \in P(\mathcal{C}, p^n)$ choose a primitive root s modulo q (the rational prime below $\mathfrak{Q}$) and define a function

$$\begin{aligned} \varphi_{\mathfrak{Q}} : \frac{C}{C \cap \mathcal{U}_F^{p^n}} &\longrightarrow \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G] \\ \delta &\longmapsto \sum_{\sigma\in G} r_\sigma \sigma^{-1} \end{aligned}$$

where the r_σ are integers such that $s^{r_\sigma} \equiv \sigma(\delta) \bmod \mathfrak{Q}$. The $\varphi_{\mathfrak{Q}}$ are well-defined homomorphisms of $\mathbb{Z}_p[G]$-modules. By Proposition 2.9, we have that $\mathcal{C}^{\varphi_{\mathfrak{Q}}(\delta)} = 1$ for all $\delta \in \frac{C}{C\cap\mathcal{U}_F^{p^n}}$.

Since $p \nmid \#G$, we may decompose (via Maschke's Theorem)

$$\mathbb{F}_p[G] = \bigoplus_\rho e_\rho \mathbb{F}_p[G],$$

Where ρ runs through the irreducible (over $\mathbb{F}_p$) characters of G with values in $\mathbb{F}_p$.There is a corresponding decomposition (via Theorem 0.13)

$$\mathbb{Z}_p[G] = \bigoplus_\rho e_\rho \mathbb{Z}_p[G],$$

Let ρ be any non-trivial irreducible character of G with values in $\mathbb{F}_p$; since the $\varphi_{\mathfrak{Q}}$ are homomorphisms of $\mathbb{Z}_p[G]$-modules, we have the restriction

$$\varphi_{\mathfrak{Q}}^\rho : e_\rho \frac{C}{C\cap\mathcal{U}_F^{p^n}} \longrightarrow e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G].$$

Let $p^a = p^{a_\rho}$ be the exact exponent of $e_\rho(W)_p$. By the same proof of Proposition 2.12, there exists $\delta \in e_\rho \frac{C}{C \cap \mathcal{U}_F^{p^n}}$ such that $p^{a+1} \nmid \phi(|\delta|)$. For such δ, it follows from Theorem 2.8 that $g(\delta, \mathcal{C}, p^n,$ id$)=$ $(\phi(\delta), b)$ divides p^a. Hence, there exists $\mathfrak{Q} \in P(\mathcal{C}, p^n)$ such that $\varphi^\rho_{\mathfrak{Q}}(\delta) \not\equiv 0 \bmod p^{a+1}$.

For $\mathfrak{Q}$ as above let a_0 be minimal such that $\varphi^\rho_{\mathfrak{Q}}(\delta) \not\equiv 0 \bmod p^{a_0+1}$, so that $a_0 \leq a$. Then $p^{-a_0}\varphi^\rho_{\mathfrak{Q}}(\delta)$ is non-zero in $e_\rho \mathbb{F}_p[G]$. Since this is irreducible ([Was] Proposition 15.5), we have that

$$p^{-a_0}\varphi^\rho_{\mathfrak{Q}}(\delta)\mathbb{F}_p[G] = \ e_\rho \mathbb{F}_p[G].$$

Now, $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ is a local ring with maximal ideal $\frac{p\mathbb{Z}}{p^n\mathbb{Z}}$ and residue field $\mathbb{F}_p$. The $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$-module $e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G]$ has the elements $p^{-a_0}\varphi^\rho_{\mathfrak{Q}}(\delta)\sigma, \sigma \in G$, whose images in $e_\rho \mathbb{F}_p[G]$ form, by the above equality, a basis of this $\mathbb{F}_p$-vector space. By an application of Nakayama's Lemma (see [AM], Proposition 2.8) we have that these elements generate $e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G]$; that is

$$p^{-a_0}\varphi^\rho_{\mathfrak{Q}}(\delta)\frac{\mathbb{Z}}{p^n\mathbb{Z}}[G] = \ e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G].$$

This implies that

$$p^a e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G] \subseteq \ p^{a_0} e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G] \subseteq \ \text{image}(\varphi^\rho_{\mathfrak{Q}}) = \ \{\text{id}\}.$$

Therefore we have that $p^a e_\rho$ annihilates $(\mathcal{C}_F)_p$. □

Theorem 2.16. *(Thaine) If p is an odd prime and $p \nmid [F:\mathbb{Q}]$, then*

$$Ann_{\mathbb{Z}[G]}((W)_p) \subseteq Ann_{\mathbb{Z}[G]}((\mathcal{C}_F)_p).$$

Proof. Let $\theta \in \mathbb{Z}_p[G]$ be an annihilator of $(W)_p$; then for any character ρ, we have that θe_ρ annihilates $e_\rho(W)_p$. Let p^b be the maximal power of p dividing θe_ρ. As in the proof of Proposition 2.15, we find that

$$\theta e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G] = p^b e_\rho \frac{\mathbb{Z}}{p^n\mathbb{Z}}[G].$$

In particular, there exists ϑ such that $\theta e_\rho \vartheta = p^b e_\rho$. Therefore p^b annihilates $e_\rho(W)_p$, so that $b \geq a_\rho$. This proves that $p^{a_\rho} | \theta e_\rho$; hence θe_ρ annihilates $(\mathcal{C}_F)_p$. Finally, since θ is the sum, over the irreducible ρ, of θe_ρ we have that θ annihilates $(\mathcal{C}_F)_p$.

□

Remark: The statement of the above Theorem is a consequent of a conjecture of G. Gras[Gra], stating that $(W)_p$ and $(\mathcal{C}_F)_p$ have isomorphic composition series as $\mathbb{Z}_p[G]$-modules. This conjecture was shown by R. Greenberg[Gre] to follow from the Main Conjecture of Iwasawa Theory, which was proved, for odd primes, by B. Mazur and A. Wiles[MW].

Chapter 3

The case $p = 2$

It is not possible to prove Thaine's Theorem for $p = 2$ by a modification of the method of chapter 2. The problem consists in the fact that a fundamental unit of F can be a square in the 2-Hilbert class field of F. For example, one of the two abelian cubic fields ramified only at 19 and 37 has class number 12 and its 2-Hilbert class field is obtained by adjoining the square roots of both (totally positive) fundamental units.

3.1 Reduction to cyclic fields

Let F be a real abelian number field of odd degree $d = [F : \mathbb{Q}]$ and let $G =$Gal$(F/\mathbb{Q})$ be its Galois group. Let us choose and fix a character $\chi : G \to \mathbb{Z}_2[\zeta_d]$. Let

$$X(\chi) = \{\tau \circ \chi | \tau \in \mathrm{Gal}(\mathbb{Q}_2(\zeta_d)/\mathbb{Q}_2\}$$

be the Galois orbit of χ and let

$$e_\chi = \frac{1}{d} \sum_{\psi \in X(\chi)} \sum_{\sigma \in G} \psi(\sigma)\sigma^{-1} \in \mathbb{Z}_2[G]$$

be the corresponding idempotent.

Lemma 3.1. *Let $\theta \in e_\chi \mathbb{Z}_2[G]$ satisfy $\theta \notin 2e_\chi \mathbb{Z}_2[G]$. Then there is $\vartheta \in e_\chi \mathbb{Z}_2[G]$ such that $\theta\vartheta = e_\chi$.*

Proof. Since $e_\chi^2 = e_\chi$, we have $\theta = e_\chi \theta$ and so $\theta \notin 2\mathbb{Z}_2[G]$. Hence the reduction $\overline{\theta} \in e_\chi \mathbb{F}_2[G]$ of θ is nonzero. Then $\sigma\overline{\theta}, \sigma \in G$, generate $e_\chi \mathbb{F}_2[G]$ over $\mathbb{Z}_2$. By an application of Nakayama's Lemma (see [AM] Proposition 2.8), we have that $\sigma\theta, \sigma \in G$, generate $e_\chi \mathbb{Z}_2[G]$ over $\mathbb{Z}_2$, so there is $\alpha \in \mathbb{Z}_2[G]$ such that $\alpha\theta = e_\chi$. Then $\vartheta = e_\chi \alpha$ satisfies the stated properties. □

Since e_χ form a complete system of orthogonal idempotents, it is enough to show for each character χ that

$$\mathrm{Ann}_{\mathbb{Z}_2[G]}(e_\chi(\mathcal{U}_F/C)_2) \subseteq \mathrm{Ann}_{\mathbb{Z}_2[G]}(e_\chi(\mathcal{C}_F)_2) \tag{3.1}$$

Having fixed the character χ, let F_χ be the corresponding cyclic subfield of F, i.e. $\mathrm{Gal}(F/F_\chi) = \ker \chi$. Let C_{F_χ} be the group of circular units of F_χ. Then we have

Lemma 3.2. *The following $\mathbb{Z}[G]$-modules are isomorphic*

$$e_\chi(\mathcal{U}_F/C)_2) \cong e_\chi(\mathcal{U}_{F_\chi}/C_{F_\chi})_2), \qquad e_\chi(\mathcal{C}_F)_2 \cong e_\chi(\mathcal{C}_{F_\chi})_2$$

Lemma 3.2 gives the following equivalent form of (3.1),

$$\mathrm{Ann}_{\mathbb{Z}_2[G]}(e_\chi(\mathcal{U}_{F_\chi}/C_{F_\chi})_2) \subseteq \mathrm{Ann}_{\mathbb{Z}_2[G]}(e_\chi(\mathcal{C}_{F_\chi})_2), \tag{3.2}$$

If χ is the trivial character, then (3.2) is obvious since $\mathcal{C}_{\mathbb{Q}}$ is trivial. Hence we need to prove (3.2) for any nontrivial character χ on G. This means to prove (3.1) just in the special case $F = F_\chi \neq \mathbb{Q}$ being cyclic and χ being any injective character on G.

3.2 Circular numbers of an abelian field

For a positive integer m let

$$\eta_{F,m} = N_{\mathbb{Q}(\zeta_m)/F\cap\mathbb{Q}(\zeta_m)}(1 - \zeta_m).$$

We define the group D of circular number of F as the $\mathbb{Z}[G]$-submodule of the multiplicative group $F^\times$ generated by -1 and by all $\eta_{F,m}$, where $m > 1$ divides the conductor of F. Then the group C of cyclotomic units of F can be show to be equal to $D \cap \mathcal{U}_F$ (see [Let]). We have the following explicit set of generators of C: it is the $\mathbb{Z}[G]$-submodule of $\mathcal{U}_F$ generated by -1, by all $\eta_{F,m}$, where $m|\mathrm{cond}F$ and m is not a prime power, and by all $\eta_{F,m}^{1-\sigma}$, where a prime power $m|\mathrm{cond}F$ and $\sigma \in G$.

3.3 Cyclic fields

Let F be a cyclic number field of odd degree $d > 1$. We fix a generator $\nu \in G$ and an injective character $\chi : G \to \mathbb{Z}_2[\zeta_d]$. Let m=cond F and let us fix a positive integer n large enough to satisfy $2^n \nmid \#\mathcal{C}_F$ and $2^n \nmid 4\#\mathcal{U}_F/C$.

Lemma 3.3. *The $\mathbb{Z}_2[G]$-module $e_\chi(\mathcal{CU}_F^{2^n}/\mathcal{U}_F^{2^n})$ is cyclic. If m is not a prime power, then this module is generated by the image of $\eta_{F,m}$, while if m is a prime power, then it is generated by the image of $\eta_{F,m}^{1-\nu}$.*

Corollary 3.4. *The $\mathbb{Z}_2[G]$-module $e_\chi(\mathcal{CU}_F^{2^n}/\mathcal{U}_F^{2^n})$ is generated by the image of $\eta_{F,m}^e$, where $e = \sum_{\sigma\in G}(1-\sigma)$.*

Proof. If m is not a prime power, then $N_{F/\mathbb{Q}}(\eta_{F,m}) = 1$ and so $\eta_{F.m}^e = \eta_{F,m}^d$. Since d is odd, the image of $\eta_{F,m}^d$ generates the image of $\eta_{F,m}$ in the module.

If m is a power of a prime p, then $N_{F/\mathbb{Q}}(\eta_{F,m}) = p$ and so $\eta_{F.m}^e = \eta_{F,m}^d p^{-1}$, which is a unit because e belongs to the augmentation ideal of $\mathbb{Z}[G]$. Since $(\eta_{F.m}^e)^{1-\nu} = \eta_{F,m}^{d(1-\nu)}$ and d is odd, we get the statement. □

3.4 An auxiliary field

Let us fix a prime number $q \equiv 1 \bmod 2^n$ such that q splits completely in F. Since q is unramified in $F/\mathbb{Q}$ and totally ramified in $\mathbb{Q}(\zeta_q+\zeta_q^{-1})/\mathbb{Q}$, the fields F and $\mathbb{Q}(\zeta_q+\zeta_q^{-1})$ are linearly disjoint. By Galois Theory,

$$\mathrm{Gal}(F(\zeta_q+\zeta_q^{-1})/\mathbb{Q}(\zeta_q+\zeta_q^{-1})) \cong \mathrm{Gal}(F/\mathbb{Q})$$

and $e = \sum_{\sigma\in G}(1-\sigma)$ can be applied to nonzero numbers in $F(\zeta_q+\zeta_q^{-1})$. Let $\delta = N_{\mathbb{Q}(\zeta_{mq})/F(\zeta_q+\zeta_q^{-1})}(\zeta_q-\zeta_m)$.

Since q does not divide m, this is a cyclotomic unit in $F(\zeta_q+\zeta_q^{-1})$. Let us denote $L = \mathbb{Q}(\zeta_m+\zeta_m^{-1}, \zeta_q+\zeta_q^{-1})$. A computation gives

$$N_{\mathbb{Q}(\zeta_{mq})/L}(\zeta_q-\zeta_m) = \beta^2,$$

where $\beta = \zeta_m(\zeta_m^{-1}-\zeta_q)(\zeta_m^{-1}-\zeta_q^{-1})$. Since β is real and fixed by the automorphism of $\mathbb{Q}(\zeta_{mq})$ determined by $\zeta_m \mapsto \zeta_m, \zeta_q \mapsto \zeta_q^{-1}$, we have $\beta \in L$. Hence $\delta = \kappa^2$, where

$$\kappa = N_{L/F(\zeta_q+\zeta_q^{-1})}(\beta).$$

$$\begin{tikzcd}
& & \mathbb{Q}(\zeta_{mq}) \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash] & & L \arrow[dl, dash] \arrow[dr, dash] & & F(\zeta_q) \arrow[dl, dash] \\
& \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \arrow[dr, dash] & & F(\zeta_q + \zeta_q^{-1}) \arrow[dl, dash] \arrow[dr, dash] & \\
& & F \arrow[dr, dash] & & \mathbb{Q}(\zeta_q + \zeta_q^{-1}) \arrow[dl, dash] \\
& & & \mathbb{Q} &
\end{tikzcd}$$

The norm relations satisfied by cyclotomic units give

$$N_{F(\zeta_q+\zeta_q^{-1})/F}(\delta) = N_{\mathbb{Q}(\zeta_{mq})/F}(\zeta_q - \zeta_m) = N_{\mathbb{Q}(\zeta_{mq})/F}(1 - \zeta_q^{-1}\zeta_m) = 1$$

because F is real and q splits completely in F. Hence $N_{F(\zeta_q+\zeta_q^{-1})/F}(\kappa) = \pm 1$ and

$$N_{F(\zeta_q+\zeta_q^{-1})/F}(\kappa^e) = 1. \tag{3.3}$$

Let $\mathfrak{B}$ be a prime ideal of $F(\zeta_q + \zeta_q^{-1})$ above q and $\mathfrak{Q}$ be the prime ideal of F below $\mathfrak{B}$. Hence $\prod_{\sigma \in G} \mathfrak{B}^\sigma$ is the principal ideal of $F(\zeta_q + \zeta_q^{-1})$ generated by $(1 - \zeta_q)(1 - \zeta_q^{-1})$. Since

$$\delta \equiv N_{\mathbb{Q}(\zeta_{mq})/F(\zeta_q+\zeta_q^{-1})}(1 - \zeta_m) = N_{\mathbb{Q}(\zeta_m)/F}(1 - \zeta_m)^2 \mod (1 - \zeta_q)(1 - \zeta_q^{-1}),$$

we have

$$\kappa^2 = \delta \equiv \eta_{F,m}^2 \mod \prod_{\sigma \in G} \mathfrak{B}^\sigma. \tag{3.4}$$

Let us fix a generator τ of $\mathrm{Gal}(F(\zeta_q + \zeta_q^{-1})/F)$. By Hilbert's Theorem 90 and (3.3), there exists a nonzero $\alpha \in F(\zeta_q + \zeta_q^{-1})$ such that $\alpha^{\tau - 1} = \kappa^e$. Since κ^e is a unit, the principal ideal (α) is fixed by τ and so there is an ideal I of F coprime with the conjugates of $\mathfrak{Q}$, whose lift (I) to $F(\zeta_q + \zeta_q^{-1})$ satisfies

$$(\alpha) = (I) \prod_{\sigma \in G} (\mathfrak{B}^{\sigma^{-1}})^{r_\sigma}$$

for suitable $r_\sigma \in \mathbb{Z}$, because $F(\zeta_q + \zeta_q^{-1})/F$ is unramified outside of the primes above q. Taking norms gives the following equality of ideals of F

$$(N_{F(\zeta_q+\zeta_q^{-1})/F}(\alpha)) = I^{\frac{(q-1)}{2}} \prod_{\sigma \in G} (\mathfrak{Q}^{\sigma^{-1}})^{r_\sigma}. \tag{3.5}$$

Since $2^{n-1} | \frac{q-1}{2}$ and $2^n > \#(\mathcal{C}_F)_2$, we have that the image of $\prod_{\sigma\in G}(\mathfrak{Q}^{\sigma^{-1}})^{r_\sigma}$ in $\mathcal{C}_F/(\mathcal{C}_F)^{2^{n-1}} \cong (\mathcal{C}_F)_2$ is trivial.

The fixed generator τ of $\mathrm{Gal}(F(\zeta_q+\zeta_q^{-1})/F)$ gives a positive integer s such that $(\zeta_q+\zeta_q^{-1})^\tau = \zeta_q^s+\zeta_q^{-s}$.

For any $\sigma \in G$, the quotient $\dfrac{\alpha}{((1-\zeta_q)(1-\zeta_q^{-1}))^{r_\sigma}}$ is coprime with $\mathfrak{B}^{\sigma^{-1}}$. Since the extension $F(\zeta_q+\zeta_q^{-1})/F$ is totally ramified at primes above q, the action of τ is trivial modulo $\mathfrak{B}^{\sigma^{-1}}$, so

$$\begin{aligned}\frac{\alpha}{((1-\zeta_q)(1-\zeta_q^{-1}))^{r_\sigma}} &\equiv \frac{\alpha^\tau}{((1-\zeta_q)(1-\zeta_q^{-1}))^{r_\sigma\tau}} = \frac{\alpha\kappa^e}{((1-\zeta_q^s)(1-\zeta_q^{-s}))^{r_\sigma}}\\ &\equiv \frac{\alpha\kappa^e}{((1-\zeta_q)(1-\zeta_q))^{r_\sigma}} s^{-2r_\sigma} \mod \mathfrak{B}^{\sigma^{-1}}.\end{aligned}$$

Cancelling by $\dfrac{\alpha}{((1-\zeta_q)(1-\zeta_q^{-1}))^{r_\sigma}}$ gives $s^{2r_\sigma} \equiv \kappa^e \mod \mathfrak{B}^{\sigma^{-1}}$, and by (3.4) we get

$$s^{4r_\sigma} \equiv \kappa^{2e} \equiv \eta_{F,m}^{2e} \mod \mathfrak{B}^{\sigma^{-1}},$$

which means

$$s^{4r_\sigma} \equiv \eta_{F,m}^{2e} \mod \mathfrak{Q}^{\sigma^{-1}} \tag{3.6}$$

as both sides belong to F.

3.5 Annihilating the ideal class group

Let us choose a class in $e_\chi(\mathcal{U}_F/C\mathcal{U}_F^{2^n})$ of maximal order 2^a and let us take any $\varepsilon \in \mathcal{U}_F$ belonging to this class. Let us fix $\overline{e}_\chi \in \mathbb{Z}[G]$ such that $\overline{e}_\chi - e_\chi \in 2^n\mathbb{Z}_2[G]$. If $a > 0$, then neither $\varepsilon^{\overline{e}_\chi}$ nor $-\varepsilon^{\overline{e}_\chi}$ is a square in F. Since

$$2^a \le \#e_\chi(\mathcal{U}_F/C\mathcal{U}_F^{2^n}) \le \#(\mathcal{U}_F/C)_2 < 2^{n-2},$$

we have $n \ge a+3$.

By Corollary 3.4, there are $\rho \in \mathbb{Z}[G]$ and $\varepsilon_1 \in \mathcal{U}_F$ such that

$$\varepsilon^{2^a\overline{e}_\chi} = \eta_{F,m}^{e\overline{e}_\chi\rho}\varepsilon_1^{2^n}$$

Since $\pm\varepsilon_1^{\overline{e}_\chi}$ is not a square in $\mathcal{U}_F$ and n is large enough, we get that neither $\eta^{e\overline{e}_\chi\rho}$ nor $-\eta^{e\overline{e}_\chi\rho}$ is a 2^{a+1}th power in $\mathcal{U}_F$.

Let us choose and fix $\mathcal{C} \in e_\chi(\mathcal{C}_F)_2$. By Proposition 2.6, there are infinitely many primes ideals $\mathfrak{Q} \in \mathcal{C}$ of absolute degree 1, lying over primes ideals $q \equiv 1 \mod 2^n$ such that $\eta_{F,m}^{e\overline{e}_\chi\rho}$ is not a 2^{a+2}th power modulo $\mathfrak{Q}$. For this q and $\mathfrak{Q}$ we can use the results of section 3.4.

Since -1 is not a 2^{n-1}th power modulo $\mathfrak{Q}$, we have that $\eta_{F,m}^{2e}$ is not a 2^{a+3}th power modulo $\mathfrak{Q}$ and (3.6) for σ gives that s^{4r_1} is not a 2^{a+3}th power modulo $\mathfrak{Q}$. Hence $2^{a+3} \nmid 4r_1$, which means $2^{a+1} \nmid r_1$.

Let us concentrate on $\pi = \sum_{\sigma \in G} r_\sigma \sigma^{-1} \in \mathbb{Z}[G]$. Let

$$b = \max\{j \in \mathbb{Z} | 2^{-j}\pi \in \mathbb{Z}[G]\} \geq 0.$$

As $2^{a+1} \nmid r_1$, we have $b \leq a$. Lemma 3.1 for $\theta = 2^{-b}\pi$ gives $\vartheta \in \mathbb{Z}_2[G]$ such that $\theta\vartheta = e_\chi$, so $\pi\vartheta = 2^b e_\chi$. Since we have obtained in (3.5) that the image of $\mathfrak{Q}^\pi$ in $(\mathcal{C}_F)_2$ is trivial, we have that

$$\mathcal{C}^{2^b e_\chi} = \mathcal{C}^{\pi\vartheta} = 1 \tag{3.7}$$

in $(\mathcal{C}_F)_2$.

Let $\beta \in \mathbb{Z}_2[G]$ be any annihilator of $e_\chi(\mathcal{U}_F/C)_2$. Since $2^n \nmid 4\#\mathcal{U}_F/C$, we have that $e_\chi(\mathcal{U}_F/C)_2 \cong e_\chi(\mathcal{U}_F/C\mathcal{U}_F^{2^n})$, so β is an annihilator of $e_\chi(\mathcal{U}_F/C\mathcal{U}_F^{2^n})$. Let

$$c = \max\{j \in \mathbb{Z} | 2^{-j} e_\chi \beta \in \mathbb{Z}_2[G]\} \geq 0.$$

Lemma 3.1 for $\theta = 2^{-c} e_\chi \beta$ gives $\Theta \in \mathbb{Z}_2[G]$ such that $\theta\Theta = e_\chi$, and so we have $e_\chi \beta \Theta = 2^c e_\chi$. Then 2^c is an annihilator of $e_\chi(\mathcal{U}_F/C\mathcal{U}_F^{2^n})$. Since 2^c annihilates also the class of ε, which is of order 2^a in $e_\chi(\mathcal{U}_F/C\mathcal{U}_F^{2^n})$, we have $c \geq a$, so $c \geq b$. Then (3.7) gives $\mathcal{C}^{\beta\Theta} = \mathcal{C}^{2^c e_\chi} = 1$ in $(\mathcal{C}_F)_2$, which implies $\mathcal{C}^\beta = \mathcal{C}^{\beta e_\chi} = \mathcal{C}^{\beta\Theta\theta} = 1$ in $(\mathcal{C}_F)_2$. This proves Theorem 2.16 for $p = 2$.

Chapter 4

An application: Catalan's Conjecture

4.1 An outline of the proof

Catalan's conjecture predicts that 8 and 9 are the only consecutive perfect powers, i. e. that there are no solutions of the diophantine equation

$$x^p - y^q = 1 \qquad (x > 0, y > 0, \qquad p, q \text{ different primes})$$

other then $x^p = 3^2, y^q = 2^3$.

The case of $q = 2$ was solved in 1850 by V.A. Lebesgue [Leb]. For $p = 2$, Chao Ko [Ko] gave a proof in 1964. So we can consider p and q odd primes.

Rewrite the diophantine equation as

$$(x-1)\frac{x^p - 1}{x - 1} = y^q.$$

By considering the identity $x^p = ((x-1)+1)^p$, we find that there are two possibilities for the gcd of the two factors on the left hand side: it is either 1 or p. This leads to case I and case II of the problem, respectively.

In case I, when the gcd equals 1, we obtain the equations

$$x - 1 = a^q, \qquad \frac{x^p - 1}{x - 1} = b^q, \qquad y = ab$$

where a and b are coprime and not divisible by p. In 1960, J.W.S. Cassels [Cas] showed that these equations yield a contradiction.

This means that we are left with case II. In particular, one of the two numbers $x-1$ and $\frac{x^p-1}{x-1}$ contains p just in the first power. But this number cannot be $x-1$, since in that case $x^p - 1$ would only be divisible by p^2. Then we have the equations

$$x - 1 = p^{q-1}a^q, \qquad \frac{x^p - 1}{x - 1} = pb^q, \qquad y = pab, \tag{4.1}$$

where again a and b are coprime and p does not divide b (but p may divide a). Analogous equations follow from the factorization of x^p into the product of $y+1$ and $\dfrac{y^q+1}{y+1}$. In particular, y is divisible by p and x is divisible by q.

Combining equation (4.1) with the observation

$$p = \prod_{k=1}^{p-1}(1-\zeta_p^k),$$

we obtain the equation

$$\prod_{k=1}^{p-1}\frac{x-\zeta_p^k}{1-\zeta_p^k} = b^q.$$

Write $x-\zeta_p^k = (x-1)+(1-\zeta_p^k)$ and notice that $x-1$ was found to be divisible by p. It follows that the quotients $\dfrac{x-\zeta_p^k}{1-\zeta_p^k}$ are in $\mathbb{Z}[\zeta_p]$. The principal ideals $\left\langle\dfrac{x-\zeta_p^k}{1-\zeta_p^k}\right\rangle$ are pairwise coprime. Hence each of them is a q-th power of some ideal. In particular,

$$\left\langle\frac{x-\zeta_p}{1-\zeta_p}\right\rangle = J^q,$$

where J is a nonzero ideal of $\mathbb{Z}[\zeta_p]$. The same is true for the complex conjugate ideal, and multiplying these ideals we get

$$\left\langle\frac{(x-\zeta_p)(x-\zeta_p^{-1})}{(1-\zeta_p)(1-\zeta_p^{-1})}\right\rangle = (J\overline{J})^q \tag{4.2}$$

an equation between real ideals. In particular, the ideal class of $J\overline{J}$ has order q or 1 in $\mathcal{C}_F$, where $F=\mathbb{Q}(\zeta_p)\cap\mathbb{R}$. Then $J\overline{J}\in(\mathcal{U}_F)_q$.

In order to use Thaine's theorem we need to enlarge the group of cyclotomic units defined in chapter 2. Consider the units

$$\frac{\sin(l\pi/p)}{\sin(\pi/p)} = \frac{\zeta_p^{l/2}-\zeta_p^{-l/2}}{\zeta_p^{1/2}-\zeta_p^{-1/2}} \qquad (l=2,\cdots,m),\ \text{where } m=\frac{p-1}{2}.$$

Together with -1 these units generate a subgroup of $\mathcal{U}_F$ of finite index. Denote it by U. We have that $[U:C]=2^{m-1}$ (cf. [Let]). This difference does not matter here (since q is odd) and will be ignored in the sequel.

Let G=Gal$(F/\mathbb{Q})=\{\sigma_1,\cdots,\sigma_m\}$ and consider $\theta\in\mathbb{Z}[G]$ annihilator of $\mathcal{U}_F/C$, so that $\mathcal{U}_F^\theta\subseteq C$. Then Thaine's theorem implies (as will be shown in the next section) that θ annihilates $(\mathcal{C}_F)_q$. By (4.2), it follows that

$$\left(\frac{(x-\zeta_p)(x-\zeta_p^{-1})}{(1-\zeta_p)(1-\zeta_p^{-1})}\right)^\theta = \varepsilon\gamma^q \tag{4.3}$$

where $\varepsilon \in \mathcal{U}_F$ and $\gamma \in F^\times$. Since γ is unknown anyway, it is sufficient to consider ε, and the units related to it, up to a factor which is a qth power in $F^\times$. Since $\varepsilon^\theta \in C$, the unit ε in (4.3) can itself be assumed to be in C (We will prove this step in the next section).

A trivial but important choice for θ above is the norm map $N = \sum_c \sigma_c$ or an integral multiple of it. Indeed, the norm of any unit is ±1. For a suitable $r \in \mathbb{Z}$, we have $((1-\zeta_p)(1-\zeta_p^{-1}))^{\theta - rN} \in U$, and (4.3) then implies that

$$((x-\zeta_p)(x-\zeta_p^{-1}))^{\theta - rN} \in \eta (F^\times)^q, \qquad \eta \in C, \tag{4.4}$$

Since $x \equiv 0 \bmod q^2$, we find that $\eta \equiv 1 \bmod q^2$ (η up to a qth power). The cyclotomic units satisfying this condition are called q-primary, they constitute a subgroup of C denoted by C_q.

Let $\vartheta \in \mathbb{Z}[G]$ be a annihilator of C_q. It follows from (4.4) that

$$((x-\zeta_p)(x-\zeta_p^{-1}))^{\theta\vartheta - rN} \in (F^\times)^q \tag{4.5}$$

Now we consider P. Mihailescu's [Mih] key theorem in his proof of case II,

Theorem 4.1. *Assume that $\theta = \sum_{c=1}^m n_c \sigma_c \in \mathbb{Z}[G]$ and $((x-\zeta_p)(x-\zeta_p^{-1}))^\theta \in (F^\times)^q$. If $\sum_{c=1}^m n_c \equiv 0 \mod q$, then each n_c is divisible by q.*

By Theorem 4.1, $\theta\vartheta - rN = q\omega$, where $\omega \in \mathbb{Z}[G]$.

Turning now to the group $\mathcal{U}_F$ we find that every unit $\varepsilon \in \mathcal{U}_F$ satisfies the condition

$$\varepsilon^{\theta\vartheta} = \varepsilon^{rN + q\omega} = \varepsilon^{rN} = 1.$$

Recalling that $\varepsilon^\theta \in C$, this suggests that ϑ in fact annihilates more of C than C_q, in this way forcing C_q to be equal to C(We will prove it in the next section). Thus we have that all cyclotomic units should be q-primary. We will see in the last section that it is impossible.

4.2 Annihilators

As stated in the first section, it is sufficient to replace a unit $\varepsilon \in \mathcal{U}_F$ by its coset $\varepsilon\mathcal{U}_F^q$ in the group $\mathcal{U}_F/\mathcal{U}_F^q$. When a map $\theta = \sum_c n_c\sigma_c \in \mathbb{Z}[G]$ operates on the latter group, it is not the coefficients n_c that matter but just their residues modulo q. Thus $\theta = \sum_c n_c\sigma_c \in \mathbb{F}_q[G]$ and the group $\mathcal{U}_F/\mathcal{U}_F^q$ becomes a cyclic module over the ring $R = \mathbb{F}_q[G]$.

Define

$$A_1 = \mathrm{Ann}(\mathcal{U}_F/C\mathcal{U}_F^q), \qquad A_2 = \mathrm{Ann}(C\mathcal{U}_F^q/C_q\mathcal{U}_F^q), \qquad A_3 = \mathrm{Ann}(C_q\mathcal{U}_F^q/\mathcal{U}_F^q).$$

These are ideals of R annihilating cyclic R-modules.

Every cyclic R-module M is (non-canonically) isomorphic to $R/\mathrm{Ann}(M)$. This isomorphism plus some information about the ideals of R enables one to conclude that the ideals A_1, A_2, A_3 are pairwise coprime and

$$A_1A_2A_3 = \mathrm{Ann}(\mathcal{U}_F/\mathcal{U}_F^q) = RN,$$

the principal ideal generated by the norm. Here the second equality follows from the cyclicity of $\mathcal{U}_F/\mathcal{U}_F^q$.

Every ideal I of R is idempotent, thus an element of I can always be written as a product of any number of elements of I. This is a convenient property of annihilators.

Let us show that every $\theta \in A_1$ annihilates $(\mathcal{C}_F)_q$. Write $\theta = \theta_1 \cdots \theta_z$, where $\theta_j \in A_1$ and $z = \mathrm{ord}_q\#(\mathcal{U}_F/C)_q$. By the definition of A_1, we have $\mathcal{U}_F^{\theta_j} \subseteq C\mathcal{U}_F^q$ and so $\mathcal{U}_F^{\theta} \subseteq C\mathcal{U}_F^{q^z}$. Now let $\varepsilon C \in (\mathcal{U}_F/C)_q$. Then $\varepsilon^{\theta} = \eta\varepsilon_1^{q^z}$ with $\eta \in C, \varepsilon_1 \in \mathcal{U}_F, \varepsilon_1 C \in (\mathcal{U}_F/C)_q$. It follows that $\varepsilon^{\theta}C = (\varepsilon_1 C)^{q^z} = C$. Consequently, θ annihilates the group $(\mathcal{U}_F/C)_q$, and the assertion is a consequence of Thaine's theorem.

Look at the equation (4.3) for $\theta \in A_1$. Write $\theta = \theta_1\theta_2$ with θ_1, θ_2 in A_1. Then the second hand side of (4.3) assumes the form

$$(\varepsilon_1\gamma_1^q)^{\theta_2} = \varepsilon_1^{\theta_2}(\gamma_1^{\theta_2})^q = \varepsilon_2\gamma_2^q,$$

where $\varepsilon_1 \in \mathcal{U}_F, \varepsilon_2 \in C$, and $\gamma_1, \gamma_2 \in F^{\times}$. Hence the unit ε in (4.3) can be chosen from C as claimed.

Once the reasoning outlined in the first section is carried through in a precise form, the relation corresponding to (4.5) says that

$$((x-\zeta)(x-\zeta^{-1}))^{\theta_1\theta_3 - rN} \in (F^{\times})^q$$

for any $\theta_1 \in A_1$ and $\theta_3 \in A_3$, where $r \in \mathbb{F}_q$ is so chosen that the map $\theta_1\theta_3 - rN = \sum_c n_c\sigma_c$ satisfies the condition $\sum_c n_c = 0$. Theorem 4.1 then tells us that $\theta_1\theta_3 - rN = 0$. Consequently, $A_1A_3 \subseteq RN$. Noting that $RN = A_1A_2A_3$ and A_1, A_2, A_3 are pairwise coprime, we deduce that $A_2 = \langle 1 \rangle$. Then $C = C_q$.

4.3 A contradiction

The equality $C = C_q$ means that every cyclotomic unit in F, when regarded modulo q^2, is the qth power of some nonzero integer of F.

We will need the notion of cyclotomic units in the whole field $\mathbb{Q}(\zeta_p)$. In this field, these units make up a subgroup C_0 of $\mathbb{Z}[\zeta_p]^\times$ generated by C and ζ_p. Since $\zeta_p = \zeta_p^{dq}$, where d is the inverse modulo p of q, we now have that all units in C_0 are qth powers modulo q^2.

In particular, so is the unit $1+\zeta_p^q = \dfrac{1-\zeta_p^{2q}}{1-\zeta_p^q}$. This gives us a congruence of the form $1+\zeta_p^q \equiv \eta^q \bmod q^2$. A well-know property of binomial coefficients then implies that $(1+\zeta_p)^q \equiv \eta^q \bmod q$. By means of the Rule of Lifting the Exponent we therefore obtain

$$(1+\zeta_p)^q \equiv 1+\zeta_p^q \bmod q^2.$$

Hence the polynomial

$$f(T) = \frac{1}{q}((1+T)^q - 1 - T^q) \in \mathbb{Z}[T]$$

has ζ_p as a zero modulo q, and also its conjugates $\zeta_p^k, k = 1, \cdots, p-1$. Consider $f(T)$ as a polynomial over the field $\mathbb{Z}[\zeta_p]/\mathfrak{Q}$, where $\mathfrak{Q}$ is a prime ideal factor of $< q >$. Since this polynomial has $p-1$ distinct zeros, its degree $q-1$ is at least $p-1$. The primes p and q are assumed different, so that we must have $q > p$. But p and q can be interchanged, so the above inequality cannot be true.

For more details, see [Met] or [Sch].

Bibliography

[AM] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, westview press (2016).

[Cas] J.W.S. Cassels, On the equation $a^x - b^y = 1$, II, Proc. Cambridge Philos. Soc. 56 (1960), 97-103.

[Chi] N. Childress, Class Field Theory, Universitext, Springer-Verlag, New York (2009).

[CR] C. Curtis and I. Reiner, Methods of representation theory, volume 1, John Wiley and Sons, Inc., New York (1981).

[Gra] G. Gras, Classes d'ideaux des corps abeliens et nombres de Bernoulli generalises, Ann. Inst. Fourier 27 (1977), 1-66.

[Gre] R. Greenberg, On p-dic L-fuctions and cyclotomic fields II. Nagoya Math. J. 67 (1977) 139-158.

[Ko] C. Ko, On the Diophantine equation $x^2 = y^n + 1, xy \neq 0$, Sci. Sinica (Notes) 14 (1964), 457-460.

[Kuc] R. Kucera, On a theorem of Thaine. Journal of Number Theory 173 (2017), 416-424.

[Leb] V.A. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, Nouv. Ann. Math. 9 (1850), 178-181.

[Let] G. Lettl, A note on Thaine's circular units. Journal of Number Theory 35 (1990), 224-226 .

[Mar] D. A. Marcus, Number Fields, Universitex, Springer-Verlag, New York.

[Met] T. Metsankyla, Catalan's conjecture: Another old diophantine problem solved. Bulletin of the AMS 41 (2003), 43-57.

[Mih] P. Mihailescu, Primary cyclotomic units and a proof of Catalan's conjecture, J. reine angew. Mathematik 572 (2004), 167-195.

[Mil] J. S. Milne, Fields and Galois Theory. (2015).

[MS] C. P. Milles and S. K. Sehgal, An Introduction to Group Rings, Springer (2002).

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$. Invent. Math. 76 (1984) 179-330.

[Rob] A. M. Robert, A Course in p-adic analysis, GTM, Springer-Verlag, New York (2000).

[Sch] R. Schoof, Catalan's conjecture, Universitext, Springer-Verlag, New York (2008).

[Sin] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. 62 (1980), 181-234.

[Tha] F. Thaine, On the ideal class groups of real abelian number fields. Annals of math. 128 (1986), 1-18.

[Was] L. C. Washington, Introduction to Cyclotomic Fields, GTM, Springer-Verlag, New York (1997).