Université Bordeaux I
Sciences Technologies

U.F.R. Mathématiques et informatique

Master Thesis

On Realizable Classes

Thesis Advisor
Prof. Boas Erez

Candidate
Andrea Siviero

Academic Year 2009–2010

Acknowledgement

My thanks are due to the University of Bordeaux I and the University of Padova and to the Algant collective for having given me the opportunity to grow and study in a constructive context, to Prof. Erez for his time and patience all along this year and to Prof. Agboola for all the references on Quantitative problems and his knowledge on the subject.

I would also thank my family for their constant presence and love, and all my friends which are far from here, but next to my heart.

I'm also heartily thankful to my friends here in Bordeaux for having made me feel at home and for all the moments spent side by side during this year.

Contents

Chapter 0

Introduction

0.1 Statement of the problem and known results

The Problem of realizable classes is one of the main questions which arose around the so called normal integral basis problem. In particular we consider K a number field (of characteristic zero) with ring of integers O_K and N/K a Galois extension of K (with ring of integers O_N) with Galois group isomorphic to a finite group Γ. The problem of realizable classes emerges from the important property that the ring of integers O_N is a locally free $O_K[\Gamma]$-module (this is the assertion of famous Noether's criterion which will be recalled in the next chapter, for a definition of locally free module look at the Appendix) and in particular it defines a class (O_N) in the class group $Cl(O_K[\Gamma])$ of locally free $O_K[\Gamma]$-modules.
If we consider a given group Γ and we denote by $R(O_K[\Gamma])$ the set of all classes in $Cl(O_K[\Gamma])$ corresponding to the ring of integers of a Galois extension N/K with Galois group isomorphic to Γ, we shall call this set $R(O_K[\Gamma])$ the set of realizable classes. The problem of realizable classes arises from the desire to characterize this set and to investigate his structure inside $Cl(O_K[\Gamma])$.

If we consider $K = \mathbb{Q}$ the problem of realisable classes is perfectly solved by the famous Taylor's Theorem ([Tay81]) proving Fröhlich's conjecture, which says that, if Γ has no sympletic characters, then $R(\mathbb{Z}\Gamma) = 1$ or in other words every tame extension $N/\mathbb{Q}$ has a normal integral basis. More generally, if Γ has such characters, then the elements of $R(\mathbb{Z}[\Gamma])$ have order at most two in $Cl(\mathbb{Z}[\Gamma])$.

The problem of main interest nowadays is to characterize $R(O_K[\Gamma])$ for an arbitrary base field K. The first step in this direction was taken by Leon R. McCulloh, which in [McC83] described $R(O_K[\Gamma])$ in an explicit way for elementary abelian groups Γ and which, after some years, determined $R(O_K[\Gamma])$ in a less evident form for any abelian group ([McC87]); proving in particular the "subgroup nature" of the set of realizable classes.
For nonabelian groups instead, we can say that the problem is still open since we have only some partial and incomplete results, which are presented in the next section.

0.2 General non abelian case

In this section, we shall try to give a general and comprehensive overview of all the results present nowadays in the open problem of Realizable Classes in the non abelian context.
Starting from the fact that a general non abelian result doesn't exist so far, after a general introduction, we'll explain the two principal approaches used to resolve the problem in particular non abelian cases, which will be listed afterwards.
Let's give an explanation of the common situation present in any non abelian particular work.

0.2.1 General Situation

From Maschke's Theorem, we know that the algebra $K[\Gamma]$ is semisimple (because the characteristic of K is zero), and so inside it we can consider $\mathcal{M}$ a maximal O_K-order, containing $O_K[\Gamma]$.

Recall 0.2.2 (Maximal Orders)**.** *Given an integral domain R with quotient field K, we recall that an R-order Λ in the K-algebra A is a subring of A, with the same unity elements as A, such that Λ is a finitely generated R-submodule in A satisfying the condition $K \cdot \Lambda = A$.*
Every K-algebra contains a R-order and a maximal order is defined as an order which is not properly contained in any other R-order in A. If we consider A a separable K-algebra, there always exists at least one maximal R-order inside it (without the hypothesis on separability, it may happens that no maximal orders exists). For a deeper and wide explanation on these subjects, look at [Rei03].

Since we are considering only tame extensions N over K to satisfy Noether's Criterion, we can use Fröhlich's description (look at the Appendix) of class group and consider the class (O_N) in $Cl(O_K[\Gamma])$. In the same way, just extending scalars $(\mathcal{M} \otimes_{O_K[\Gamma]} O_N)$, we can even consider the class (O_N) in $Cl(\mathcal{M})$.

As we have already defined $R(O_K[\Gamma])$ the set of realizable classes inside $Cl(O_K[\Gamma])$, in the same way, we define $R(\mathcal{M})$ inside $Cl(\mathcal{M})$.

Besides the two already cited results in the abelian case, McCulloh also reached in [McC75] (Prop. 1.2.1) an important conclusion which values with an arbitrary group Γ (abelian or not). This Proposition asserts that in general we have

$$R(O_K[\Gamma]) \subseteq Cl^{\circ}(O_K[\Gamma]), \tag{0.2.1}$$

where this last set, which will be called the augmentation kernel, is defined as the kernel of the map $Cl(O_K[\Gamma]) \longrightarrow Cl(K)$, induced by the augmentation map from $K[\Gamma]$ to K ($\epsilon : K[\Gamma] \longrightarrow K$, sending $\sum c_\gamma \gamma \longrightarrow \sum c_\gamma$). The proof of it is just an application of the functorial property of the class group and of the fact that in a tame extension the trace is surjective.
Exactly in the same way, we have

$$R(\mathcal{M}) \subseteq Cl^{\circ}(\mathcal{M}), \tag{0.2.2}$$

where $Cl^{\circ}(\mathcal{M})$ is the kernel of the analogous map $Cl(\mathcal{M}) \longrightarrow Cl(K)$.

0.2.3 Overview of known results

In order to understand the recent results on the open problem of Realizable Classes in the non abelian case, I reviewed the works principally of B. Sodaïgui and the ones of N. P. Byott and M. Godin.
In all these different articles, we can recognize two principal approaches, which we'll be explained later.
In particular the known results nowadays are:

First Approach - Description of $R(\mathcal{M})$ as a group:

- Metacyclic $\longrightarrow \Gamma = \langle \sigma, \tau \rangle = C_l \rtimes_\mu C_m$, where C_l is a cyclic group of order a prime l, while C_m is a cyclic group of order a natural number m and $\mu : C_m \longrightarrow \mathrm{Aut}(C_l)$ is a faithful $\mathbb{F}_l$-linear representation of C_m inside C_l. With the assumption that $K \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$, where ζ_l is a primitive l-th root of unity, it was proved that if we define $R_1(\mathcal{M}) \subseteq R(\mathcal{M})$ as the set of classes realized by metacyclic extensions N/K of order lm, such that the subextension K_1/K of N/K of degree m is linearly disjoint from $K(\zeta_l)/K$; then $R_1(\mathcal{M})$ forms a subgroup of $Cl^\circ(\mathcal{M})$. This work is an extension and also a correction of a previous work by B. Sodaïgui ([Sod97]). Reference: [SS10].
- Dihedral $\longrightarrow \Gamma = D_4$, the Dihedral group of order 8. With the assumptions that K has an odd class number and that $K \cap \mathbb{Q}(i) = \mathbb{Q}$, where i is such that $i^2 = -1$. Reference: [Sod00b].
- Quaternion $\longrightarrow \Gamma = H_8$, the Quaternion group of order 8. With the assumptions that $K \cap \mathbb{Q}(i) = \mathbb{Q}$, where i is such that $i^2 = -1$. Reference: [Sod99b].
  $\Gamma = H_{4l}$, the generalized quaternion group of order $4l$, with l odd prime number. With the assumption that 2 and l ramified in $K/\mathbb{Q}$; the author gives the description as subgroups of two particular subsets of $R(\mathcal{M})$, called $R_1(\mathcal{M})$ and $R_2(\mathcal{M})$. Reference: [Sod00a].
- Tetrahedral $\longrightarrow \Gamma = A_4$, the alternating Tetrahedral group. With the assumptions that $K \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$, where ζ_3 is a primitive 3-rd root of unity and that K has an odd class number. Reference: [GS03].
- Octahedral $\longrightarrow \Gamma = S_4$, the symmetric octahedral group. With the assumption that K has an odd class number. Reference: [Sod07].

Second Approach - The equality $R(O_K[\Gamma]) = Cl^\circ(O_K[\Gamma])$:

- Dihedral $\longrightarrow \Gamma = D_4$, the Dihedral group of order 8. With the assumption that the ray class group of O_K with modulus $4O_K$ has odd order. Reference: [BS05a].
- Tetrahedral $\longrightarrow \Gamma = A_4$, the alternating Tetrahedral group. Without any assumption. Reference: [BS05b]. We remark that this is the only non abelian case in which the original problem given by McCulloh is solved without any assumption on K.

There are also other more recent works, which begin trying to generalize the results for $R(\mathcal{M})$ reached in [GS03] and [Sod07].

The first one [GS06], written by N. P. Byott, C. Greither and B. Sodaïgui, proves the conjecture that $R(\mathcal{M})$ forms a subgroup in $Cl^{\circ}(\mathcal{M})$ for a particular set of groups Γ. They indeed consider the group Γ of the form $V \rtimes_{\rho} C$, where V is a $\mathbb{F}_2$-vector space of dimension $r \geq 2$, C is a cyclic group of order $2^r - 1$ and ρ is a linear representation of C in V. It's important to underline that this article proves that $R(\mathcal{M})$ forms a subgroup in $Cl^{\circ}(\mathcal{M})$, without giving an equality between them, as done in the previous particular works.
We remark that the group A_4 belongs to this set of groups (remark 2 after Prop. 2.3 in the article) and so in this case we obtain an improvement of the result in [GS03], since we have no assumptions on the base field K.

Following the previous article we finally cite the article [BS08] by C. Bruche and B. Sodaïgui; in this work they prove exactly the same result of the previous one, for all the groups Γ of the form $V \rtimes_{\rho} C$, where V is a $\mathbb{F}_p$-vector space of dimension $r \geq 2$ with p an odd prime number, C is a cyclic group of order $p^r - 1$ and ρ is a linear representation of C in V. To reach this result they need the assumption that the base number field K contains a p-th primitive root of unity ζ_p.
We remark that the group S_3 belongs to this set of groups (remark 2 after Prop. 2.3 in the article) and so in this case we obtain an improvement of the result in [Sod97] for the metacyclic groups S_3.

Remark 0.2.4. *It's useful to notice that the proof of the fact that $R(O_K[\Gamma])$ forms a subgroup in $Cl^{\circ}(O_K[\Gamma])$ implies that $R(\mathcal{M})$ forms a subgroup in $Cl^{\circ}(\mathcal{M})$; indeed the extension of scalars from $O_K[\Gamma]$ to $\mathcal{M}$ induces a surjective morphism $Ex: Cl(O_K[\Gamma]) \longrightarrow Cl(\mathcal{M})$ with $Ex(R(O_K[\Gamma])) = R(\mathcal{M})$.*

0.3 Structure of our work

In our work, after the first Chapter dedicated to the definition of the Galois algebras and to a characterization of them, we shall concentrate, in the second Chapter, on the extensions of our interest: the Tame Galois extensions.

We will enter directly in the heart of the problem in the third Chapter where we shall retrace the solution of the problem in the abelian case. We will present the article by McCulloh [McC87] without any particular improvement, but just with some attempts to clarify some parts and to make the article more clear ("we just put some little glims along the path").

In the last chapter we will consider the non abelian case A_4 in order to explain the two approaches utilized in the non abelian case and make a good comparison between them.

Concluding, the Appendix is dedicated to some algebraic techniques and properties which are fundamental along our work.

0.4 Quantitative Problems and Results

In this section we want to cite some problems and results linked to the concept of Realizable Classes.

One of the first questions which arises studying realizable classes is, given a group Γ and a realizable class c, how are the Galois Γ-extensions distributed among the realizable classes?

A first answer to this question was given by K. C. Foster in his unpublished Ph.D. thesis at the University of Illinois ([Fos]), where he considered the case in which Γ is an elementary abelian l-group for some prime l. If we denote by $N_{disc}(c, X)$ the number of tame Γ-extensions N/K which realize the class c and such that the discriminant of N over $\mathbb{Q}$ is less than X, then Foster gave an asymptotic expression with $X \longrightarrow \infty$ of $N_{disc}(c, X)$ with those particular Γ and he proved that it's independent of c; this implies that the tame Γ-extensions are equidistributed among the realizable classes as $X \longrightarrow \infty$.

This work was retraced some years later by A. Agboola in [Agb], where he was able to extend the result to any arbitrary finite abelian groups Γ with the restriction, not on the discriminant, but on the absolute norm of the product of the primes of K which ramify in N/K, which he called $\mathfrak{D}(N/K)$. In particular denoting with $N_{\mathfrak{D}}(c, X)$ the number of tame Γ-extensions N/K which realize the class c and such that $\mathfrak{D}(N/K) \leq X$ and N/K is unramified at all places dividing $|\Gamma|$, he proved that asymptotically the number $N_{\mathfrak{D}}(c, X)$ is independent of c. He also tried to generalize the result of Foster to all the abelian group, but he didn't succeed and contrarily he obtained results which indicates that probably Foster's equidistribution doesn't exist for any arbitrary abelian group, even if he wasn't able to prove it.

It is interesting to compare Agboola's work with the recent article by M. Wood ([Woo10]). In her work, she determined the probabilities of various local completions of a random Γ-extension of K. She found that if the extensions are counted looking at their conductor they are almost all equidistributed, but if we look instead to the discriminant the general behavior is not so good.

Always belonging to this set of "quantitative" results, we also cite the article by A. C. Kable and D. J. Wright [KW06], which deals with counting the distribution of the Steinitz classes in the class group for quadratic and cubic extensions.

Finally, we also cite the article [Bri84] by J. Brinkhuis; in a more algebraic way he linked the problem of realizable classes to the embedding problem and he also found a sort of restriction to the fact that the realizable classes form a subgroup. As a good (maybe) introduction to this work, we refer to chapter VI of [Frö83].

Chapter 1

Galois Algebras

The aim of this chapter is to define Galois extensions and give a good characterization of them. After a first part dedicated to the definitions and terminology, we shall present the concept of resolvend linked to the one of normal basis. In the last part we will restrict to the abelian situation giving a cohomological interpretation, which will be a prelude to the next chapter.
For clarity, we shall explain separately the extensions of fields and the extensions of rings.

1.1 Notation and Terminology

All along this section we denote by K a field of characteristic zero and by Γ a finite group.
Let N be a commutative K-algebra on which Γ acts on the left by K-algebra automorphisms. We use N^{Γ} to indicate the subfield of fixed elements of N under the action of Γ:

$$N^{\Gamma} = \{x \in N \,|\, \forall\, \gamma \in \Gamma : \gamma.x = x\}.$$

Thanks to the definition, we have $K \subset N^{\Gamma}$. The K-algebra N is a *Galois* Γ*-extension* of K (even called Galois algebra over K with group Γ) when the following properties hold:

- N is a commutative semisimple K-algebra,
- $N^{\Gamma}= K$;
- $[N : K] = |\Gamma|$.

The basic example is a Galois field extension L/K, with $\Gamma = Gal(L/K)$. Another important example is the case when we consider $L = \mathrm{Map}(\Gamma, K)$ with pointwise operation, with K embedded via the constant K-valued functions and with Γ acting in the following way: take $f \in L$ and $\gamma \in \Gamma$, and let $\gamma.f(\sigma) = f(\sigma\gamma)$ for all $\sigma \in \Gamma$.
(For many equivalent definitions of Galois extensions of rings and even the equivalent of the Fundamental Theorem of Galois Theory for the Galois extensions, look at [HR65]. For a usual explanation of Galois field extensions look at [Bou81]).

1.2 Characterization of Galois extensions

There is a canonical way to characterize Galois Γ-extensions of K, in particular they can be considered as a particular subgroup of $\mathrm{Map}(\Gamma, K^c)$, where K^c is the algebraic closure of K.

Let's describe this better. If we take $\Omega = \Omega_K$ the Galois group of K^c/K, we can associate to any (continuous) homomorphism $h : \Omega \longrightarrow \Gamma$ a Galois Γ-extension K_h of K, namely:

$$K_h = \mathrm{Map}_{\Omega}({}^h\Gamma, K^c).$$

K_h is the set of K^c-valued functions on Γ which preserve the action of Ω. We put h on the left of Γ to denote that Ω acts on it by left multiplication via the homomorphism h, while Ω acts on K_h in the following way

$$\forall\, f \in\ K_h,\, \omega \in \Omega \quad (\omega.f)(\gamma) = f\left(h\left(\omega\right)\left(\gamma\right)\right).$$

More precisely, for $f \in K_h$ and for all $\gamma \in \Gamma$, $\omega \in \Omega$ we have:

$$\begin{aligned} f(\omega.\gamma) &= \omega\left(f\left(\gamma\right)\right) \\ f(h(\omega)\gamma) &= \omega\left(f\left(\gamma\right)\right). \end{aligned} \tag{1.2.1}$$

It's easy to see that K_h is a Galois Γ-extension, indeed letting Γ act on K_h by

$$\gamma.f(t) = f(t\gamma) \tag{1.2.2}$$

and considering K embedded in K_h via the constant K-valued functions, we obtain ${K_h}^{\Gamma}= K$ (indeed the fixed points are exactly the constant valued functions). Moreover looking at (1.2.1), we can see that f is determined by its values on a set of coset representatives for $h(\Omega)\backslash\Gamma$ and all these values must be fixed by all the $\omega \in \ker h$.
So if we consider

$$K^h = (K^c)^{ker\, h}$$

it follows that any map in K_h has value in K^h (since $f(\gamma) = \omega.f(\gamma)$), giving $K_h = \mathrm{Map}_{\Omega}({}^h\Gamma, K^h)$. Moreover K_h is isomorphic as K-algebra to the product of $[\Gamma : h(\Omega)]$ copies of K^h, showing that K_h is semisimple. Finally since $[K^h : K] = |h(\Omega)|$ we have $[K_h : K] = |\Gamma|$, proving completely that K_h is a Galois Γ-extension.
We may stress that if h is surjective, then $K_h \cong K^h$ so it's a field; while if h is trivial then K_h is equal to a product of $|\Gamma|$ copies of K.

An isomorphism of Galois Γ-extensions of K is an isomorphism of K-algebras, which preserves the action of Γ. Thanks to this it can be proved that, if we take a Galois Γ-extension of K, then there is an element $h \in \mathrm{Hom}(\Omega, \Gamma)$, such that the Galois extension is isomorphic to K_h (look at Section 1 of Chapter 3 in [Ere]).
Moreover we have $K_h \cong K_{h'}$ if and only if h differs from h' by an inner automorphism of Γ (recall: an inner automorphism is an automorphism $\theta : \Gamma \to \Gamma$, such that $\forall\, x \in \Gamma$, $\theta(x) = axa^{-1}$, given a fixed $a \in \Gamma$).
So we have reached the important following Proposition which characterizes Galois algebras.

Proposition 1.2.0.1. *Let Γ be a finite group. The set of isomorphism classes of Galois Γ-extensions over K is in bijection with the set*

$$Inn(\Gamma) \setminus Hom(\Omega_K, \Gamma)$$

of all continuous homomorphisms from Ω_K to Γ, up to inner automorphisms of Γ.

In particular, when Γ is abelian, we have that all the inner automorphisms are trivial and so we obtain that the set of isomorphism classes of Galois Γ-extensions is a commutative group isomorphic to $\mathrm{Hom}(\Omega_K, \Gamma)$.

1.3 Change of the base field (e.g. localization)

In this subsection, we would understand what happens if we change the base field, in particular if we extend it.

Given N a Galois Γ-extension of K, we consider $\sigma : K \longrightarrow F$ the embedding of K into another field F. Just extending the scalars, we obtain the Galois Γ-extension $F \overset{\sigma}{\otimes}_K N$, where Γ acts via the second factor and the exponent of the tensor products means that we have a structure on F of K-algebra via σ. In this way we easily obtain another Galois Γ-extension, depending only on $\sigma : K \longrightarrow F$.
Let's try to describe it in terms of homomorphisms, using an extension σ to the embedding of the algebraic closure $K^c \longrightarrow F^c$; which induces a homomorphism between the Galois fields of F and K:

$$\tilde{\sigma} : \Omega_F \longrightarrow \Omega_K,$$

with $\Omega_F = \mathrm{Gal}(F^c/F)$.
For $h \in \mathrm{Hom}(\Omega_K, \Gamma)$, we obtain $h\tilde{\sigma} \in \mathrm{Hom}(\Omega_F, \Gamma)$ and a canonical isomorphism of Galois Γ-extensions of F:

$$F_{h\tilde{\sigma}} \cong F \overset{\sigma}{\otimes}_K K_h. \tag{1.3.1}$$

To show it we have to underline several observations, first of all we have:

$$F \overset{\sigma}{\otimes}_K K_h = F \overset{\sigma}{\otimes}_K \mathrm{Map}_{\Omega_K}({}^h\Gamma, K^c) = \mathrm{Map}_{\Omega_K}({}^h\Gamma, F \overset{\sigma}{\otimes}_K K^c).$$

We try now to understand the structure of $F \overset{\sigma}{\otimes}_K K^c$. Thanks to a standard result, we have

$$F \overset{\sigma}{\otimes}_K K^c = \mathrm{Map}_{\Omega_F}(\Sigma, F^c);$$

where Σ represents the set of all possible extensions of σ to embeddings $K^c \longrightarrow F^c$ and the isomorphism is obtained sending $a \otimes b$ to the map $\gamma \longrightarrow a\gamma(b)$. Thanks to our choice of a particular embedding $K^c \longrightarrow F^c$ we have the isomorphism of Ω_F-sets $\Sigma \cong {}^{\tilde{\sigma}}\Omega_K$ (the exponent on the left of Ω_K is always to indicate that the action of Ω_F is via $\tilde{\sigma}$) and, using it in the previous isomorphism, we have:

$$F \overset{\sigma}{\otimes}_K K_h \cong \mathrm{Map}_{\Omega_K}\left({}^h\Gamma, \mathrm{Map}_{\Omega_F}\left({}^{\tilde{\sigma}}\Omega_K, F^c\right)\right);$$

which, applying transitivity of (co)-induction, gives

$$F \overset{\sigma}{\otimes}_K K_h \cong \mathrm{Map}_{\Omega_F}({}^{(h\tilde{\sigma})}\Gamma, F^c) = F_{h\tilde{\sigma}}.$$

In the particular case when $F = K_{\mathfrak{v}}$ is a completion of K we shall use

$$K_{\mathfrak{v}} \overset{\sigma}{\otimes}_K K_h \cong \mathrm{Map}_{\Omega_{K_{\mathfrak{v}}}}({}^{\tilde{\sigma}}\Omega_K, {K_{\mathfrak{v}}}^c). \tag{1.3.2}$$

Nevertheless when F is already a subfield of K^c containing K, we shall use the embedding identity $K^c = F^c$ and if $F = K^c$, then $\Omega_F = 1$ and we will have

$$K^c \otimes_K K_h \cong \mathrm{Map}(\Gamma, K^c). \tag{1.3.3}$$

Finally the canonical K-algebra homomorphism $K_h \longrightarrow F \overset{\sigma}{\otimes}_K K_h$, which sends $a \longrightarrow 1 \otimes a$, becomes, for $K_h \longrightarrow F_{h\tilde{\sigma}}$, $a \longrightarrow \sigma \circ a$, where with σ we denote even the extension of the original σ to the embedding $K^c \longrightarrow F^c$ and $\sigma \circ a$ is the composite with the homomorphism $a : \Gamma \longrightarrow K^c$.

1.4 Resolvends and Normal Bases

Remembering that any Galois Γ-extension can be considered inside $\mathrm{Map}(\Gamma, K^c)$, we now define a very important map on this last set, called *resolvend map*:

$$\begin{array}{rccc} r_\Gamma : & \mathrm{Map}(\Gamma, K^c) & \longrightarrow & K^c\Gamma \\ & a & \longrightarrow & \sum_{\gamma \in \Gamma} a(\gamma)\gamma^{-1}, \end{array} \tag{1.4.1}$$

where $r_\Gamma(a)$ is called *resolvend* associated to a.
Remembering the action of Γ on the domain of the map and letting Γ act on $K^c\Gamma$ trivially on the coefficients belonging to K^c, it's easy to check that the *resolvend map* is a $K^c\Gamma$-modules isomorphism; indeed:

$$\begin{aligned} r_\Gamma(\gamma.a) &= \sum_{\gamma' \in \Gamma} \gamma.a(\gamma')\gamma'^{-1} \\ &= \sum_{\gamma' \in \Gamma} a(\gamma'\gamma)\gamma'^{-1} \\ &= \sum_{\tau \in \Gamma} a(\tau)\gamma\tau^{-1} \\ &= \gamma.r_\Gamma(a). \end{aligned}$$

This is the reason why in the definition of the resolvend map we use γ^{-1}, instead of the easier γ; without considering the inverse we would not obtain a $K^c\Gamma$-modules isomorphism.

Using resolvends, we can find a criterion to understand if a map $a \in \mathrm{Map}(\Gamma, K^c)$ belongs to K_h:

$$\begin{aligned} a \in K_h \quad &\Longleftrightarrow \quad \forall\, \omega \in \Omega,\ \omega.r_{\Gamma}(a) = \sum_{\gamma \in \Gamma} \omega.a(\gamma)\gamma^{-1}, \\ &\Longleftrightarrow \quad \forall\, \omega \in \Omega,\ \omega.r_{\Gamma}(a) = \sum_{\gamma \in \Gamma} a(h(\omega)\gamma)\gamma^{-1}, \\ &\Longleftrightarrow \quad \forall\, \omega \in \Omega,\ \omega.r_{\Gamma}(a) = \left(\sum_{\gamma' \in \Gamma} a\left(\gamma'\right)\gamma'^{-1} \right) h(\omega), \\ &\Longleftrightarrow \quad \forall\, \omega \in \Omega,\ \omega.r_{\Gamma}(a) = r_{\Gamma}(a)h(\omega); \end{aligned} \tag{1.4.2}$$

here Ω acts on $K^c\Gamma$ through its action on the coefficients.

Resolvends are also very important because they give us a criterion to decide if an element is a normal basis generator of Γ-extensions. Remember that an element $a \in K_h$ is a *normal basis generator* of K_h/K if the set $\{\gamma(a) : \gamma \in \Gamma\}$ is a basis of K_h/K, or from another point of view if $K_h = K\Gamma.a$.

Proposition 1.4.0.2. *Given $a \in K_h$, we have*

$$K_h = K\Gamma.a \Longleftrightarrow r_{\Gamma}(a) \in \left(K^c\Gamma\right)^{\times},$$

denoting with $\left(K^c\Gamma\right)^{\times}$ the group of units of $K^c\Gamma$.

Proof. It's not difficult to prove that in general we have the following isomorphism:

$$K^c\Gamma.a \cong K^c \otimes_K K\Gamma.a\ , \tag{1.4.3}$$

moreover from (1.3.3), we have:

$$K^c \otimes_K K_h \cong \mathrm{Map}(\Gamma, K^c).$$

So for $a \in K_h$ we have:

$$\begin{aligned} K_h = K\Gamma.a \quad &\Longleftrightarrow \quad K^c\Gamma.a \cong K^c \otimes_K K_h \cong \mathrm{Map}(\Gamma, K^c), \\ &\Longleftrightarrow \quad (K^c\Gamma)(r_{\Gamma}(a)) = K^c\Gamma, \\ &\Longleftrightarrow \quad r_{\Gamma}(a) \in \left(K^c\Gamma\right)^{\times}. \end{aligned}$$

□

Thanks to this proposition we have an easy criterion to understand if an element in K_h is a *normal basis generator*: an element $a \in K_h$ is a *normal basis generator* if and only if its resolvend is invertible in $K^c\Gamma$.

At this point an existence's question arises: has any Galois Γ-extension a normal basis?

In the case of field extensions, the affirmative answer is assured by the well-known Normal Basis Theorem.

Theorem 1.4.1 (Normal Basis Theorem)**.** *Let N be a Galois finite extension of a field K, with Galois group Γ, then a normal basis of N over K exists. In other words, N is a free $K\Gamma$-module of rank* 1*.*

I refer to [Art55] for a proof with K infinite and to [Bou81] and [Jac64] for a proof with whatever base field K.

In the case of Galois ring extensions instead, we need some particular conditions to obtain a Normal basis; in general it doesn't always exist. For a precise Theorem look at [HR65], whereas for an explicit example of Galois ring extension without a normal basis look at [Ere].

Finally in the case of Galois Γ-extensions for algebras, we're lucky because an analogous Theorem, as the one for the field, exists. For a proof of it look at [Frö64].

1.5 Change of group

In this part we want to analyze the effect of a change of the acting group Γ. In order to do this, we consider the homomorphism of finite group $f : \Gamma \longrightarrow \Gamma'$, which gives us the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Map}(\Gamma, K^c) \arrow[r, "r_\Gamma"] \arrow[d, shift left, "f_*^M"] & K^c\Gamma \arrow[d, shift left, "f_*"] \\
\mathrm{Map}(\Gamma', K^c) \arrow[r, "r_{\Gamma'}"] \arrow[u, shift left, "f_M^*"] & K^c\Gamma' \arrow[u, shift left, "f^*"]
\end{tikzcd} \tag{1.5.1}$$

The two functions between the two Map-sets are defined in the following way:

$$\begin{aligned}
(f_*^M(a))(\gamma') &:= \sum_{\substack{\gamma\in\Gamma \\ f(\gamma)=\gamma'}} a(\gamma), \\
f_M^*(b) &:= b \circ f.
\end{aligned} \tag{1.5.2}$$

The first one is seen easily to be a K^c-module homomorphism, with the important "Frobenius" relation

$$b.f_*^M(a) = f_*^M(f_M^*(b).a)\,, \text{with } a \in \mathrm{Map}(\Gamma, K^c) \text{ and } b \in \mathrm{Map}\left(\Gamma', K^c\right);$$

while the second one is a K^c-algebra homomorphism.
Instead on the right side of the diagram, we define the two functions by K^c-linearity, in the following way :

$$\begin{aligned}
f_*(\gamma) &:= f(\gamma), \\
f^*(\gamma') &:= \sum_{\substack{\gamma\in\Gamma \\ f(\gamma)=\gamma'}} \gamma;
\end{aligned} \tag{1.5.3}$$

The proof of the given formulas and of fact that the initial diagram is commutative is not difficult. Just as an example we show the commutativity of the diagram following the maps f_* and f_*^M. For this we have to show that given $a \in \mathrm{Map}(\Gamma, K^{\,c})$, we have $r_{\Gamma'}\left(f_*^M(a)\right) = f_*\left(r_\Gamma(a)\right)$. Indeed, just using definitions, we have:

$$\begin{aligned} r_{\Gamma'}\left(f_*^M(a)\right) &= \sum_{\gamma' \in \Gamma'} f_*^M(a)(\gamma')\gamma'^{-1}, \\ &= \sum_{\gamma' \in \Gamma'} \sum_{\substack{\gamma \in \Gamma \\ f(\gamma)=\gamma'}} a(\gamma)\gamma'^{-1}, \\ &= \sum_{\gamma \in \Gamma} a(\gamma) f(\gamma^{-1}), \\ &= f_*\left(r_\Gamma(a)\right). \end{aligned}$$

The other proofs are similar.

From a Galois Γ-extension K_h, it's not difficult to obtain a Galois Γ'-extension, given the homomorphism $f : \Gamma \longrightarrow \Gamma'$. Considering $\mathrm{Hom}(\Omega, \Gamma)$ and $\mathrm{Hom}(\Omega, \Gamma')$, we have a map between these two sets induced by f:

$$\begin{array}{cccc} F: & \mathrm{Hom}(\Omega, \Gamma) & \longrightarrow & \mathrm{Hom}(\Omega, \Gamma') \\ & h & \longrightarrow & f \circ h\,, \end{array}$$

which sends $\mathrm{Inn}(\Gamma)$-orbits into $\mathrm{Inn}(\Gamma')$-orbits; giving rise to a Γ'-extension $K_{f \circ h} = \mathrm{Map}_\Omega({}^{f \circ h}\Gamma', K^{\,c})$. Thanks to the fact that we are considering the maps fixed by Ω, it's easy to see that f_*^M, f_M^* of the diagram restrict without any problem to:

$$\begin{tikzcd} K_h \arrow[r, shift left, "f_*^K"] & K_{f \circ h}. \arrow[l, shift left, "f_K^*"] \end{tikzcd} \tag{1.5.4}$$

Looking at the diagram with these restrictions, we have another similar commutative diagram:

$$\begin{tikzcd} K_h \arrow[r, "r_\Gamma"] \arrow[d, shift left, "f_*^K"] & K^{\,c}\Gamma \arrow[d, shift left, "f_*"] \\ K_{f \circ h} \arrow[r, "r_{\Gamma'}"] \arrow[u, shift left, "f_K^*"] & K^{\,c}\Gamma' \arrow[u, shift left, "f^*"] \end{tikzcd} \tag{1.5.5}$$

obtaining the formula

$$r_{\Gamma'}\left(f_*^K(a)\right) = f_*\left(r_\Gamma(a)\right),$$

which, thanks to the fact that f_* is a ring homomorphism, gives us the property that f_*^K preserves normal basis generators. Indeed, given a normal basis generator a for K_h (with the consequence that $r_\Gamma(a)$ is a unit), we obtain, using the previous formula, that $r_{\Gamma'}\left(f_*^K(a)\right)$ is invertible and so $\left(f_*^K(a)\right)$ is a normal basis generator for $K_{f \circ h}$.

In particular using (co)-induction on the functor Map, we have:

$$\mathrm{Map}_\Omega({}^f\Gamma', K_h) = \mathrm{Map}_\Omega\left({}^f\Gamma', \mathrm{Map}_\Omega\left({}^h\Gamma, K^{\,c}\right)\right) = \mathrm{Map}_\Omega({}^{f \circ h}\Gamma', K^{\,c}) = K_{f \circ h}.$$

Recalling the discussion after the definition of K_h, we have that if f is surjective, then

$$K_{f \circ h} \cong (K_h)^{ker f} \tag{1.5.6}$$

and the two maps f_*^K and f_K^* are exactly the trace and the inclusion, respectively.

1.6 Tensor Product of Galois extensions

Considering the direct product $\Gamma \times \Gamma'$, we can make the following identifications:

$$\begin{aligned} K^c\Gamma \otimes_{K^c} K^c\Gamma' &= K^c(\Gamma \times \Gamma') \ \ \big(\text{putting}\ \gamma \otimes \gamma' = (\gamma, \gamma')\big), \\ && (1.6.1) \\ \mathrm{Map}(\Gamma, K^c) \otimes_{K^c} \mathrm{Map}(\Gamma', K^c) &= \mathrm{Map}(\Gamma \times \Gamma', K^c) \ \ \big(\text{putting}\ (a \otimes b)\,(\gamma, \gamma') = a\,(\gamma)\,b\,(\gamma')\big)\,; \\ \\ \mathrm{Hom}(\Omega, \Gamma) \times \mathrm{Hom}(\Omega, \Gamma') &= \mathrm{Hom}(\Omega, \Gamma \times \Gamma') \ \ (\text{defining}\ (h,k)\,(\omega) := (h\,(\omega)\,, k\,(\omega)))\,. \end{aligned}$$

In particular thanks to the last two identifications we have:

$$K_h \otimes_K K_k = K_{(h,k)} \tag{1.6.2}$$

and using the fact that

$$r_\Gamma(a) \otimes r_{\Gamma'}(b) = r_{\Gamma \times \Gamma'}(a \otimes b), \tag{1.6.3}$$

we have that if a and b are normal basis generators of K_h and K_k respectively, then their tensor product is a normal basis generator of $K_{(h,k)}$.

1.7 The Abelian case

In this section we assume Γ abelian, so, as already observed, we have that $\mathrm{Hom}(\Omega, \Gamma)$ is isomorphic to the set of isomorphism classes of Galois Γ-extensions, which in this way is an abelian group with a defined group law. Let's describe it better.

We denote by $m : \Gamma \times \Gamma \longrightarrow \Gamma$ the multiplication homomorphism and so given $h, k \in \mathrm{Hom}(\Omega, \Gamma)$ we have $h \cdot k = m(h, k)$. The map m is trivially surjective and then thanks to (1.6.2) and (1.5.6), we have

$$K_{h \cdot k} \cong (K_h \otimes_K K_k)^{ker(m)}.$$

We shall underline here that $\ker(m) = \{(s, s^{-1})\}$. Following the work done in the previous sections, we have the trace map $m_*^K : K_h \otimes_K K_k \longrightarrow K_{h \cdot k}$. So, taken $a \in K_h$ and $b \in K_k$, following (1.5.5) we have:

$$r_\Gamma\left(m_*^K\,(a \otimes b)\right) = m_*\left(r_{\Gamma \times \Gamma}\,(a \otimes b)\right) = m_*\left(r_\Gamma\,(a) \otimes r_\Gamma\,(b)\right),$$

where the last equality follows from (1.6.3).
Recalling (1.5.3), we have that $m_* : K^c\Gamma \otimes K^c\Gamma\,(= K^c\,(\Gamma \times \Gamma)) \longrightarrow K^c\Gamma$ is just the algebra multiplication $\gamma_1 \otimes \gamma_2 \longrightarrow \gamma_1\gamma_2$, and so from the last equivalence we obtain:

$$r_\Gamma\left(m_*^K\,(a \otimes b)\right) = r_\Gamma(a) r_\Gamma(b); \tag{1.7.1}$$

which tells us that if we take a and b normal basis generators of K_h and K_k, respectively, then we have that $m_*^K(a \otimes b)$ is a normal basis generator of $K_{h \cdot k}$.

1.7.1 Cohomology interpretation in the abelian case

We would now apply cohomology theory of groups, to have a particular description of $\mathrm{Hom}(\Omega, \Gamma)$. We start with the exact sequence of Ω-modules, where Ω acts trivially on Γ:

$$1 \longrightarrow \Gamma \longrightarrow (K^c\Gamma)^\times \longrightarrow (K^c\Gamma)^\times/\Gamma \longrightarrow 1 \tag{1.7.2}$$

and we apply Ω-cohomology so that we have the following exact sequence of Ω-modules:

$$1 \longrightarrow (\Gamma)^\Omega \longrightarrow \Big((K^c\Gamma)^\times\Big)^\Omega \longrightarrow \Big((K^c\Gamma)^\times/\Gamma\Big)^\Omega \longrightarrow \mathrm{H}^1(\Omega, \Gamma) \longrightarrow \mathrm{H}^1(\Omega, (K^c\Gamma)^\times) \longrightarrow \dots \ .$$

Analyzing each terms, we see that:

$$\begin{aligned} (\Gamma)^\Omega &= \Gamma, \\ \Big((K^c\Gamma)^\times\Big)^\Omega &= (K\Gamma)^\times, \\ \Big((K^c\Gamma)^\times/\Gamma\Big)^\Omega &=: \mathcal{H}(K\Gamma), \\ \mathrm{H}^1(\Omega, \Gamma) &= \mathrm{Hom}(\Omega, \Gamma) \ \text{(because } \Omega \text{ acts trivially on } \Gamma\text{)}, \\ \mathrm{H}^1(\Omega, (K^c\Gamma)^\times) &= 1 \ \text{(by Hilbert's Satz 90);} \end{aligned} \tag{1.7.3}$$

obtaining the following exact sequence

$$1 \longrightarrow \Gamma \longrightarrow (K\Gamma)^\times \longrightarrow \mathcal{H}(K\Gamma) \longrightarrow \mathrm{Hom}(\Omega, \Gamma) \longrightarrow 1. \tag{1.7.4}$$

We can even write $\mathcal{H}(K\Gamma) = H(K\Gamma)/\Gamma$, where

$$H(K\Gamma) = \{\gamma \in (K^c\Gamma)^\times | \, \forall \omega \in \Omega, \ \frac{\omega.\gamma}{\gamma} \in \Gamma\}. \tag{1.7.5}$$

Remark 1.7.2 (Hilbert's Satz 90)**.** *Here we used the generalization of Hilbert's Satz* 90 *due to Emmy Noether which states that if N/K is a finite Galois extension of fields with Galois group $\Gamma = Gal(N/K)$, then the first cohomology group is trivial:*

$$H^1(\Gamma, N^\times) = 1.$$

For the original Hilbert's Satz 90 *due to Kummer we refer to chapter* 2 *of [Mil].*

Without using Satz 90, we notice that any element γ in $H(K\Gamma)$ defines a map $\phi_\gamma : \Omega \longrightarrow \Gamma$ in the following way:

$$\phi_\gamma(\omega) = \frac{\omega.\gamma}{\gamma}.$$

In this way we find a group homomorphism $\pi : H(K\Gamma) \longrightarrow \mathrm{Hom}(\Omega, \Gamma)$ which induces easily a map on $\mathcal{H}(K\Gamma)$.
So we can find exactness at the right of the sequence understanding that the coset $\gamma\Gamma$, where $\gamma \in H(K\Gamma)$, lies in the preimage of a homomorphism $h \in \mathrm{Hom}(\Omega, \Gamma)$ if and only if $\frac{\omega.\gamma}{\gamma} = h(\omega)$ for all $\omega \in \Omega$. We know that K_h has a normal basis a and so using Prop. 1.4.0.2 we have that $r_{_\Gamma}(a) \in (K^c\Gamma)^\times$ and $\frac{\omega.r_\Gamma(a)}{r_\Gamma(a)} = h(\omega)$ for all $\omega \in \Omega$, thanks to (1.4.2). Thus taking $\gamma = r_{_\Gamma}(a)$ we prove that the preimage of h is not empty, as wanted.
Moreover we have the important consequence, that we can describe $H(K\Gamma)$ as follows:

$$H(K\Gamma) = \{r_{_\Gamma}(a) |\, K\Gamma.a = K_h \text{ for some } h \in \mathrm{Hom}(\Omega, \Gamma)\}, \tag{1.7.6}$$

in other words $H(K\Gamma)$ is the set of all resolvends of normal basis generators of Galois Γ-extensions K_h/K, with $h \in \mathrm{Hom}(\Omega, \Gamma)$.

1.7.3 Interpretation in terms of characters

Recalling that we consider Γ abelian, in this section we shall give an interpretation of $\mathcal{H}(K\Gamma)$ in terms of character functions.

We denote by $\widehat{\Gamma} = \mathrm{Hom}(\Gamma, K^{c\times})$ the group of characters of Γ. Each character $\chi \in \widehat{\Gamma}$ can be extended by linearity to an algebra homomorphism $\chi : K^c\Gamma \longrightarrow K^c$ and we can make the following identification:

$$K^c\Gamma = \mathrm{Map}(\widehat{\Gamma}, K^c),$$

where any element $\gamma \in K^c\Gamma$ is regarded as a function on $\widehat{\Gamma}$ by putting $\gamma(\chi) = \chi(\gamma)$ for $\chi \in \widehat{\Gamma}$.
We have an action of Ω naturally defined on the group of characters, in particular $\omega.\chi(\gamma) = \omega.(\chi(\omega^{-1}.\gamma))$ for al $\gamma \in \Gamma$; which allows us to view the action of Ω on $K^c\Gamma$ in terms of characters, as follows:

$$\omega.\gamma(\chi) = \omega.(\gamma(\omega^{-1}.\chi)). \tag{1.7.7}$$

If we take instead the multiplicative group $(K^c\Gamma)^\times$, it can be identified, after a $\mathbb{Z}$-linearity extension of homomorphisms, with $\mathrm{Hom}\left(\mathbb{Z}\widehat{\Gamma}, (K^c)^\times\right)$. So, considering the fixed points under the action of Ω, we have $K\Gamma^\times = \mathrm{Hom}_\Omega\left(\mathbb{Z}\widehat{\Gamma}, (K^c)^\times\right)$, and we can have an alternative description of (1.7.2), by applying $\mathrm{Hom}(-, (K^c)^\times)$ to the sequence

$$0 \longrightarrow A_{\widehat{\Gamma}} \longrightarrow \mathbb{Z}\widehat{\Gamma} \xrightarrow{\det} \widehat{\Gamma} \longrightarrow 1, \tag{1.7.8}$$

where $A_{\widehat{\Gamma}}$ is the kernel of the map det: $\mathbb{Z}\widehat{\Gamma} \longrightarrow \widehat{\Gamma}$, defined in the following way:

$$\det\left(\sum_{\chi\in\widehat{\Gamma}} a_\chi\chi\right) = \prod_{\chi\in\widehat{\Gamma}} \chi^{a_\chi} \quad (a_\chi \in \mathbb{Z}).$$

Since $(K^c)^\times$ is divisible (so injective), we obtain another exact sequence

$$1 \longrightarrow \mathrm{Hom}\left(\widehat{\Gamma},(K^c)^\times\right) \longrightarrow \mathrm{Hom}\left(\mathbb{Z}\widehat{\Gamma},(K^c)^\times\right) \longrightarrow \mathrm{Hom}\left(A_{\widehat{\Gamma}},(K^c)^\times\right) \longrightarrow 1. \tag{1.7.9}$$

Now we can make some identifications: first of all from previous facts we have $\mathrm{Hom}\left(\mathbb{Z}\widehat{\Gamma},(K^c)^\times\right) = (K^c\Gamma)^\times$ and then it's well known that $\widehat{\widehat{\Gamma}} = \Gamma$, so we have even $\mathrm{Hom}\left(\widehat{\Gamma},(K^c)^\times\right) = \Gamma$. Thanks to these, we can rewrite the previous exact sequence:

$$\begin{tikzcd}
1 \arrow[r] & \Gamma \arrow[r] \arrow[d, equal] & (K^c\Gamma)^\times \arrow[r] \arrow[d, equal] & (K^c\Gamma)^\times/\Gamma \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathrm{Hom}\left(\widehat{\Gamma},(K^c)^\times\right) \arrow[r] & \mathrm{Hom}\left(\mathbb{Z}\widehat{\Gamma},(K^c)^\times\right) \arrow[r] & \mathrm{Hom}\left(A_{\widehat{\Gamma}},(K^c)^\times\right) \arrow[r] & 1
\end{tikzcd} \quad , \tag{1.7.10}$$

where the third identification derives from the other two. In particular, looking at the fixed points, we underline the following situation:

$$\begin{tikzcd}
(K\Gamma)^\times \arrow[r] \arrow[d, equal] & \mathcal{H}(K\Gamma) \arrow[d, equal] \\
\mathrm{Hom}_\Omega\left(\mathbb{Z}\widehat{\Gamma},(K^c)^\times\right) \arrow[r, "rag"] & \mathrm{Hom}_\Omega\left(A_{\widehat{\Gamma}},(K^c)^\times\right)
\end{tikzcd} \quad ; \tag{1.7.11}$$

where *rag* is just the restriction of homomorphisms to $A_{\widehat{\Gamma}}$. It follows, from the previous equivalence of sets, that if a generates a normal basis of K_h/K, then its resolvend belongs to $(K^c\Gamma)^\times$ and so it's a homomorphism $r_\Gamma(a) : \mathbb{Z}\widehat{\Gamma} \longrightarrow (K^c)^\times$. We denote its restriction to $A_{\widehat{\Gamma}}$ by $\mathcal{R}_\Gamma(a) : A_{\widehat{\Gamma}} \longrightarrow (K^c)^\times$, obtaining:

$$\mathcal{R}_\Gamma(a) = rag\left(r_\Gamma(a)\right) = r_\Gamma(a)\Gamma. \tag{1.7.12}$$

We shall call $\mathcal{R}_\Gamma(a)$ the *reduced resolvend* of a. So with this notation we obtain

$$\mathcal{H}(K\Gamma) = \{\mathcal{R}_\Gamma(a) |\, K\Gamma.a = K_h \text{ for some } h \in \mathrm{Hom}(\Omega,\Gamma)\}. \tag{1.7.13}$$

Remembering that $\gamma.r_\Gamma(a) = r_\Gamma(\gamma.a)$ for any $\gamma \in \Gamma$, we have that the elements of $\mathcal{H}(K\Gamma)$ are in one to one correspondence with the actual normal bases of the various Galois $\Gamma-$algebras K_h/K.

Chapter 2

Tame extensions and integral resolvends

The aim of this chapter is to give an integral interpretation of what done in the final part of the previous chapter for algebraic number fields K and their completion $K_{\mathfrak{v}}$; we will concentrate in particular on Tame Galois extensions. We shall see that strict analogues exist only for unramified extensions of the ring of integers (O and $O_{\mathfrak{v}}$).

2.1 Completion

We take K an algebraic number field, or better a finite extension of $\mathbb{Q}$ contained in the complex number field $\mathbb{C}$ and we denote by K^c the algebraic closure of K. For any prime $\mathfrak{v}$ of K we take the completion $K_{\mathfrak{v}}$ and we have a natural embedding $i_{\mathfrak{v}} : K^c \longrightarrow K_{\mathfrak{v}}^c$, where $K_{\mathfrak{v}}^c$ is the algebraic closure of the completion. Moreover we denote by $\widetilde{i_{\mathfrak{v}}} : \Omega_{\mathfrak{v}} \longrightarrow \Omega$ the corresponding embedding of the Galois groups, respectively of $K_{\mathfrak{v}}^c/K_{\mathfrak{v}}$ and of K^c/K.
If we take $h \in \mathrm{Hom}(\Omega, \Gamma)$, then $h_{\mathfrak{v}} = h \circ \widetilde{i_{\mathfrak{v}}} \in \mathrm{Hom}(\Omega_{\mathfrak{v}}, \Gamma)$ and so from (1.3.1) we have

$$(K_{\mathfrak{v}})_{h_{\mathfrak{v}}} \cong K_{\mathfrak{v}} \otimes_K K_h; \tag{2.1.1}$$

moreover considering $i_{\mathfrak{v}}$ as an inclusion, we have that $K_h \subseteq (K_{\mathfrak{v}})_{h_{\mathfrak{v}}}$.

2.2 Tame Galois Γ-extensions

Let Ω^t (resp. $\Omega_{\mathfrak{v}}^t$) denote the Galois group of the maximal tame extension K^t/K (resp. $K_{\mathfrak{v}}^t/K_{\mathfrak{v}}$) in K^c (resp. in $K_{\mathfrak{v}}^c$); clearly $\widetilde{i_{\mathfrak{v}}}$ restricts to $\widetilde{i_{\mathfrak{v}}} : \Omega_{\mathfrak{v}}^t \longrightarrow \Omega^t$.
A Galois Γ-extension K_h/K is called tame when h factors through the quotient map $\Omega \twoheadrightarrow \Omega^t$ or in other words when we have the following commutative diagram:

$$\begin{tikzcd}
\Omega \arrow[rr, "h"] \arrow[dr, two heads, "\text{quot.}"'] & & \Gamma \\
& \Omega^t \arrow[ur] &
\end{tikzcd} \tag{2.2.1}$$

Remark 2.2.1. *We can underline that, looking at the diagram, K_h/K is tame $\Longleftrightarrow$ $K^h \subseteq K^t$. Indeed we have K_h/K tame $\Longleftrightarrow$ $Gal(K^c, K^t) \subseteq ker(h) \Longleftrightarrow K^h \subseteq K^t$.*
This means that if we consider $Hom(\Omega^t, \Gamma)$ as a subset of $Hom(\Omega, \Gamma)$, then K_h/K is tame if and only if $h \in Hom(\Omega^t, \Gamma)$; in which case we also say h is tame.

The same can be done for $K_\mathfrak{v}$ and we have h tame if and only if $h_\mathfrak{v}$ tame for all primes $\mathfrak{v}$ of K (for $\mathfrak{v}$ infinite we take $K^t_\mathfrak{v} = K^c_\mathfrak{v}$).
For Γ abelian, we call $\mathcal{H}^t(K\Gamma)\,(= H^t(K\Gamma)/\Gamma)$ the preimage of $\mathrm{Hom}(\Omega^t, \Gamma)$ under the connecting homomorphism $\mathcal{H}(K\Gamma) \longrightarrow \mathrm{Hom}(\Omega, \Gamma)$ explained above (the same for $K_\mathfrak{v}$).
So we have the following commutative diagram, where the vertical maps are induced by the suppressed $i_\mathfrak{v}$:

$$\begin{tikzcd}
1 \arrow[r] & \Gamma \arrow[r] & (K\Gamma)^\times \arrow[r, "rag"] \arrow[d] & \mathcal{H}^t(K\Gamma) \arrow[r] \arrow[d] & \mathrm{Hom}(\Omega^t, \Gamma) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \Gamma \arrow[r] & (K_\mathfrak{v}\Gamma)^\times \arrow[r, "rag"] & \mathcal{H}^t(K_\mathfrak{v}\Gamma) \arrow[r] & \mathrm{Hom}(\Omega^t_\mathfrak{v}, \Gamma) \arrow[r] & 1.
\end{tikzcd} \tag{2.2.2}$$

Exactly the same, done for the maximal tame extension, can be remade for the maximal unramified extension $K^{nr}_\mathfrak{v}/K_\mathfrak{v}$ in $K^c_\mathfrak{v}$ with Galois group denoted by $\Omega^{nr}_\mathfrak{v}$. So we also call $\mathcal{H}^{nr}(K_\mathfrak{v}\Gamma)\,(= H^{nr}(K_\mathfrak{v}\Gamma)/\Gamma)$ the preimage of $\mathrm{Hom}(\Omega^{nr}_\mathfrak{v}, \Gamma)$ as above.

2.3 Integral vision

We denote by O, O^t, O^c, and O^h the ring of integers in K, K^t, K^c, and K^h, respectively. The integral closure O_h of O in K_h is

$$O_h = \mathrm{Map}_\Omega({}^h\Gamma, O^c).$$

As done with K_h, we can see O_h as $[\Gamma : h(\Omega)]$ copies of O^h.
Exactly the same for $O_\mathfrak{v}$, $O^c_\mathfrak{v}$, $O^{h_\mathfrak{v}}_\mathfrak{v}$ and $(O_\mathfrak{v})_{h_\mathfrak{v}} = \mathrm{Map}_{\Omega_\mathfrak{v}}({}^{h_\mathfrak{v}}\Gamma, O^c_\mathfrak{v})$, where for infinite $\mathfrak{v}$ we take $O_\mathfrak{v} = K_\mathfrak{v}$.

In the rest of the subsection we denote by $\mathfrak{v}$ a finite prime of K and also by $\mathfrak{v}$ the additive valuation normalized associated. Trying to find an integral analogous of some previous relations we find (thanks to Section 1.3 and thanks to [Ser79] Chap. 2, Prop. 4)

$$O_\mathfrak{v} \otimes_O O^c \cong \mathrm{Map}_{\Omega_\mathfrak{v}}(\Omega, O^c_\mathfrak{v}) \tag{2.3.1}$$

and always following the proof in 1.3 we obtain

$$(O_\mathfrak{v})_{h_\mathfrak{v}} \cong O_\mathfrak{v} \otimes_O O_h. \tag{2.3.2}$$

The fundamental theorem to start from, in the study of integral Galois module structure, is Noether's Criterion:

Theorem 2.3.1 (Noether's Criterion)**.** *The extension $(K_\mathfrak{v})_{h_\mathfrak{v}}/K_\mathfrak{v}$ is tame if and only if it has a normal integral basis (N.I.B.); i.e., if and only if $(O_\mathfrak{v})_{h_\mathfrak{v}} = (O_\mathfrak{v}\Gamma).a_\mathfrak{v}$ for some $a_\mathfrak{v} \in (O_\mathfrak{v})_{h_\mathfrak{v}}$.*

For different proofs of this theorem, look in [Ere] (Chap. 3.4); while a particular proof for the unramified case will be given in the next Chapter.

2.4 Trace Map - Duality

The usual trace defined on $\mathrm{Map}(\Gamma, K^c)$ is well known and so for any $h \in \mathrm{Hom}(\Omega, \Gamma)$, thanks to a restriction on K_h, we have a trace map defined on the set K_h in the usual way:

$$\begin{array}{rccc} \mathrm{Tr}: & K_h & \longrightarrow & K \\ & a & \longrightarrow & \mathrm{Tr}(a) = \sum_{\gamma \in \Gamma} a(\gamma) \ ; \end{array} \tag{2.4.1}$$

satisfying trivially the relation $\mathrm{Tr}(\gamma'.\, a) = \mathrm{Tr}(a)$, for any $a \in K_h$ and $\gamma' \in \Gamma$.
Associated to it, we have a nondegenerate bilinear form $(a, b) \longrightarrow \mathrm{Tr}(ab)$, which gives the definition of dual lattice and discriminant for Galois algebras, as usual. If we take M, an O-lattice in K_h, we have

$$\begin{aligned} M^* &= \{b \in K_h |\, \mathrm{Tr}(bM) \subseteq O\}, \\ \delta(O_h/O) &= [O_h^* : O_h]_O, \end{aligned} \tag{2.4.2}$$

where $[\,:\,]_O$ is the O-module index. It's not hard to prove that $O_h^* = \mathrm{Map}\left({}^h\Gamma, (O^h)^*\right)$, in other words a product of $[\Gamma : h(\Omega)]$ copies of $(O^h)^*$, given

$$\delta(O_h/O) = \delta(O^h/O)^{[\Gamma:h(\Omega)]} \tag{2.4.3}$$

where $(O^h)^*$ and $\delta(O^h/O)$ have the usual meaning in K_h/K. So in particular we have that $O_h = O_h^*$ if and only if $h_{\mathfrak{v}}$ is unramified for all finite primes $\mathfrak{v}$.

2.5 Resolvends and integral properties

In this subsection we assume that Γ is abelian. So the canonical involution $\gamma \longrightarrow \gamma^{-1}$ in Γ, induces a canonical involution $h \longrightarrow h^{-1}$ on $\mathrm{Hom}(\Omega, \Gamma)$ and involutions on the K^c-algebras $\mathrm{Map}(\Gamma, K^c)$ and $K^c\Gamma$ which we shall denote by $[-1]$.
Thus we have the commutative diagram

$$\begin{tikzcd} \Omega \arrow[rr, "h"] \arrow[dr, "h^{-1}"'] & & \Gamma \arrow[dl, "{[-1]}"] \\ & \Gamma & \end{tikzcd} \tag{2.5.1}$$

,

which gives us the following results:

$$\begin{aligned} (K_h)^{[-1]} &= K_{h^{-1}}, \\ r_\Gamma(a^{[-1]}) &= r_\Gamma(a)^{[-1]} \quad \text{for}\, a \in \mathrm{Map}(\Gamma, K^c). \end{aligned} \tag{2.5.2}$$

We arrive so at the deeper following result:

Proposition 2.5.0.1. **(a)** *For any $a, b \in Map(\Gamma, K^c)$ we have*

$$r_\Gamma(a)r_\Gamma(b)^{[-1]} = \sum_{\gamma \in \Gamma} Tr\left((\gamma(a))\, b\right)\gamma^{-1}.$$

(b) *If $K_h = K\Gamma.a$. Let $b \in K_h$ satisfying $Tr(\gamma(a)b) = \delta_{\gamma,1}$ then*

$$r_\Gamma(a)^{-1} = r_\Gamma(b)^{[-1]},$$

(c) $(O\Gamma.a)^* = O\Gamma.b$,

(d) $[(O\Gamma.a)^* : O\Gamma.a]_O = [O\Gamma : O\Gamma r_\Gamma(a) r_\Gamma(a)^{[-1]}]_O$.

Proof. **(a)** We compute $r_\Gamma(a)r_\Gamma(b)^{[-1]} = \sum_{\sigma,\tau} \sigma(a)\tau(b)\sigma^{-1}\tau$. Let $\gamma^{-1} = \sigma^{-1}\tau$ so

$$\begin{aligned} r_\Gamma(a)r_\Gamma(b)^{[-1]} &= \sum_{\tau,\gamma \in \Gamma} \tau\gamma(a)\tau(b)\gamma^{-1}\ , \\ &= \sum_{\gamma \in \Gamma} \left(\sum_\tau \tau\left(\gamma(a)b\right)\right)\gamma^{-1}\ , \\ &= \sum_{\gamma \in \Gamma} \mathrm{Tr}\left(\gamma(a)b\right)\gamma^{-1}. \end{aligned}$$

(b) The existence of such an element b follows from the separability property which says that the trace is surjective. From $\mathrm{Tr}\left(\gamma(a)b\right) = \delta_{\gamma,1}$ we have

$$\mathrm{Tr}(\sigma(a)\tau(b)) = \mathrm{Tr}(\tau^{-1}\sigma(a)b) = \delta_{\sigma,\tau},$$

and so the proof follows from the formula of the previous point.

(c) This follows from the existence of the element b with the property in point (b).

(d) From the previous point we have

$$\begin{aligned} [(O\Gamma.a)^* : O\Gamma.a]_O &= [O\Gamma.b : O\Gamma.a]_O \\ &= [O\Gamma r_\Gamma(b) : O\Gamma r_\Gamma(a)]_O \\ &= [O\Gamma : O\Gamma r_\Gamma(a) r_\Gamma(b)^{-1}]_O \\ &= [O\Gamma : O\Gamma r_\Gamma(a) r_\Gamma(a)^{[-1]}]_O, \end{aligned}$$

where in the first equality we used point (c), in the second equality the fact that r_Γ is an isomorphism and in the last one we applied point (b).

□

Moreover we have the following important Theorem, which characterizes the normal integral basis generators of unramified extensions thanks to their resolvends.

Theorem 2.5.1 (Condition on resolvend to be N.I.B. generator)**.**

$$r_\Gamma(a) \in (O^c\Gamma)^\times \Longleftrightarrow O_h = O\Gamma \cdot a \ \ \textit{and} \ \ \delta(O_h/O) = (1). \tag{2.5.3}$$

Proof. For both sides we have $a \in O_h$ and consequently $(O\Gamma \cdot a)^* \supseteq O_h^* \supseteq O_h \supseteq O\Gamma \cdot a$. But, then

$$\begin{aligned} r_\Gamma(a) \in (O^c\Gamma)^\times \ &\Longleftrightarrow \ r_\Gamma(a) r_\Gamma(a)^{[-1]} \in (O\Gamma)^\times \\ &\Longleftrightarrow \ (O\Gamma.a)^* = (O\Gamma.a) \\ &\Longleftrightarrow \ O_h = O\Gamma.a \ \text{ and } [O_h^* : O_h] = (1), \end{aligned}$$

where in the second equality we used Proposition 2.5.0.1 and in the last one the inclusion written at the beginning of the proof. □

2.6 Cohomological integral analogue

In this section we try to do the same thing done in the general non integral case, applying $\Omega_{\mathfrak{v}}$-cohomology to the following exact sequence:

$$1 \longrightarrow \Gamma \longrightarrow (O_{\mathfrak{v}}^c\Gamma)^\times \longrightarrow (O_{\mathfrak{v}}^c\Gamma)^\times/\Gamma \longrightarrow 1. \tag{2.6.1}$$

In this case we obtain

$$1 \longrightarrow \Gamma \longrightarrow (O_{\mathfrak{v}}\Gamma)^\times \longrightarrow \mathcal{H}(O_{\mathfrak{v}}\Gamma) \longrightarrow \mathrm{Hom}(\Omega_{\mathfrak{v}}^{nr}, \Gamma) \longrightarrow 1, \tag{2.6.2}$$

where

$$\mathcal{H}(O_{\mathfrak{v}}\Gamma) = \left((O_{\mathfrak{v}}^c\Gamma)^\times/\Gamma\right)^{\Omega_{\mathfrak{v}}} = H(O_{\mathfrak{v}}\Gamma)/\Gamma,$$

and

$$H(O_{\mathfrak{v}}\Gamma) = (O_{\mathfrak{v}}^c\Gamma)^\times \cap H(K_{\mathfrak{v}}\Gamma).$$

The exactness on the right of the sequence (2.6.2) essentially only depends on the fact that we are considering a tame extension (so we have a normal integral basis) and from the local version of Theorem 2.5.1.

Moreover, as in the general case, we have the following two analogous consequences:

$$\mathcal{H}(O_{\mathfrak{v}}\Gamma) = \{\mathcal{R}_\Gamma(a_{\mathfrak{v}}) \,|\, O_{\mathfrak{v}}\Gamma.a_{\mathfrak{v}} = (O_{\mathfrak{v}})_{h_{\mathfrak{v}}}, \text{ for some } h_{\mathfrak{v}} \in \mathrm{Hom}(\Omega_{\mathfrak{v}}^{nr}, \Gamma)\}, \tag{2.6.3}$$

and

$$\mathcal{H}^{nr}(K_{\mathfrak{v}}\Gamma) = \mathcal{H}(O_{\mathfrak{v}}\Gamma) \cdot rag\left((K_{\mathfrak{v}}\Gamma)^\times\right), \text{ or } H^{nr}(K_{\mathfrak{v}}\Gamma) = H(O_{\mathfrak{v}}\Gamma)(K_{\mathfrak{v}}\Gamma)^\times. \tag{2.6.4}$$

Finally we try to give an analogous of (1.7.11). For any integral ideal $\mathfrak{m}$ of O, let

$$U_{\mathfrak{m}}(O_{\mathfrak{v}}^c) = (1 + \mathfrak{m}O_{\mathfrak{v}}^c) \cap (O_{\mathfrak{v}}^c)^\times;$$

in particular if $\mathfrak{m}$ and $\mathfrak{v}$ are relatively prime we have $U_{\mathfrak{m}}(O_{\mathfrak{v}}^c) = (O_{\mathfrak{v}}^c)^\times$. If $\mathfrak{m}$ is principal generated by e we denote $U_{\mathfrak{m}}(O_{\mathfrak{v}}^c)$ just as $U_e(O_{\mathfrak{v}}^c)$.

We prove here a Lemma which will be useful for the next important Theorem.

Lemma 2.6.1. *If* $y^e \in U_{e^2}(O^c_{\mathfrak{v}})$*, then* $\frac{y^e-1}{e(y-1)} \in O^c_{\mathfrak{v}}$.

Proof. If $y = 1$ we interpret the fraction as 1 and so there's no problem because $1 \in O^c_{\mathfrak{v}}$, while if $\mathfrak{v}(e) = 0$ the proof is trivial because $\mathfrak{v}(y^e - 1) \geq \mathfrak{v}(y - 1)$; thus, assuming $y \neq 1$ and $\mathfrak{v}(e) > 0$, we have to show that $\mathfrak{v}\left(\frac{y^e-1}{e(y-1)}\right) \geq 0$.
From hypothesis, we have $y^e \in U_{e^2}(O^c_{\mathfrak{v}})$ and so $\mathfrak{v}(y^e - 1) \geq 2\mathfrak{v}(e)$; so

$$\mathfrak{v}\left(\frac{y^e-1}{e(y-1)}\right) \geq \mathfrak{v}(e) - \mathfrak{v}(y-1).$$

If $\mathfrak{v}(e) - \mathfrak{v}(y-1) \geq 0$, we are done. If not, then $\mathfrak{v}(y-1) \geq \mathfrak{v}(e)$ so $\mathfrak{v}\left((y-1)^2\right) > \mathfrak{v}\left(e\left(y-1\right)\right)$, and since

$$y^e - 1 = \sum_{r=1}^{e} \binom{e}{r} (y-1)^r \equiv e(y-1) \qquad \left(\mathrm{mod}(y-1)^2 O^c_{\mathfrak{v}}\right)$$

we conclude $\mathfrak{v}\left(\frac{y^e-1}{e(y-1)}\right) = 0$ and again we are done. □

We can give now the Theorem which gives us the analogous of (1.7.11).

Theorem 2.6.2. *Suppose* Γ *is abelian.*

(a) *If* $|\Gamma|$ *divides* $\mathfrak{m}$*, then*

$$Hom_{\Omega_{\mathfrak{v}}}\left(\mathbb{Z}\widehat{\Gamma}, U_{\mathfrak{m}}(O^c_{\mathfrak{v}})\right) \subseteq (O_{\mathfrak{v}}\Gamma)^{\times} \subseteq Hom_{\Omega_{\mathfrak{v}}}\left(\mathbb{Z}\widehat{\Gamma}, (O^c_{\mathfrak{v}})^{\times}\right)$$

(b) *If* $\mathfrak{m}$ *is divisible both by* $|\Gamma|$ *and* m^2*, where* m *is the exponent of* Γ*, then*

$$Hom_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}}, U_{\mathfrak{m}}(O^c_{\mathfrak{v}})\right) \subseteq \mathcal{H}(O_{\mathfrak{v}}\Gamma) \subseteq Hom_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}}, (O^c_{\mathfrak{v}})^{\times}\right).$$

In particular, if $\mathfrak{v}$ *is relatively prime to* $|\Gamma|$*, then*

$$O_{\mathfrak{v}}\Gamma^{\times} = Hom_{\Omega_{\mathfrak{v}}}\left(\mathbb{Z}\widehat{\Gamma}, (O^c_{\mathfrak{v}})^{\times}\right),$$

and

$$\mathcal{H}(O_{\mathfrak{v}}\Gamma) = Hom_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}}, (O^c_{\mathfrak{v}})^{\times}\right).$$

Proof. **(a)** We know that the maximal $O^c_{\mathfrak{v}}$-order of $K^c_{\mathfrak{v}}\Gamma$ is $\mathrm{Map}(\widehat{\Gamma}, O^c_{\mathfrak{v}})$ and that $|\Gamma| \cdot \mathrm{Map}(\widehat{\Gamma}, O^c_{\mathfrak{v}}) \subseteq O^c_{\mathfrak{v}}\Gamma$. So if $|\Gamma|$ divides $\mathfrak{m}$ we have the assertion.

(b) From the previous section about the non integral part (1.7.10) it follows that $(O_{\mathfrak{v}}^c\Gamma)^\times \subseteq \mathrm{Hom}\left(\mathbb{Z}\widehat{\Gamma}, (O_{\mathfrak{v}}^c)^\times\right)$ and $(O_{\mathfrak{v}}^c\Gamma)^\times/\Gamma \subseteq \mathrm{Hom}\left(A_{\widehat{\Gamma}}, (O_{\mathfrak{v}}^c)^\times\right)$, so $\mathcal{H}(O_{\mathfrak{v}}\Gamma) \subseteq \mathrm{Hom}_{\Omega_{\mathfrak{v}}}(A_{\widehat{\Gamma}}, (O_{\mathfrak{v}}^c)^\times)$. If $\mathfrak{v}$ and $|\Gamma|$ are relatively prime ($\mathfrak{v}(|\Gamma|) = 0$) then we have equality in the previous inclusion from point (a), so to prove (b) we only need to consider the case $\mathfrak{v}(|\Gamma|) > 0$. We are so interested in prove the first inclusion of (b).

Let $g \in \mathrm{Hom}_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}}, U_{\mathfrak{m}}(O_{\mathfrak{v}}^c)\right) \subseteq \mathrm{Hom}_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}}, (K)^\times\right) = \mathcal{H}(K_{\mathfrak{v}}\Gamma) = \left((K_{\mathfrak{v}}^c\Gamma)^\times/\Gamma\right)^{\Omega_{\mathfrak{v}}}$. So $g = f\Gamma$ for some $f \in (K_{\mathfrak{v}}^c\Gamma)^\times$ and now it sufficient to prove that $f \in O_{\mathfrak{v}}^c\Gamma$, since we can apply the same argument to $g^{-1} = f^{-1}\Gamma$ to get $f \in (O_{\mathfrak{v}}^c\Gamma)^\times$. Let $f = \sum_{\gamma\in\Gamma} a(\gamma)\gamma^{-1}$, we shall prove that $a(\gamma) \in O_{\mathfrak{v}}^c$.

Let $\phi_1, \ldots, \phi_k$ a basis for the abelian group $\widehat{\Gamma}$, each one with order e_i, respectively for $i = 1, \ldots, k$. So any element $\chi \in \widehat{\Gamma}$ can be represented in the following unique way

$$\chi = \prod_{i=1}^{k} \phi_i^{r_i(\chi)}, \quad \text{where} \quad 0 \le r_i(\chi) < e_i.$$

Hence, trivially (review the definition of $A_{\widehat{\Gamma}}$), $A_{\widehat{\Gamma}}$ contains the elements (actually they form a basis for $A_{\widehat{\Gamma}}$)

$$\{e_i\phi_i | i = 1, \ldots, k\} \cup \{d(\chi) | \chi \in \widehat{\Gamma}\}$$

with

$$d(\chi) = \chi - \sum_{i=1}^{k} r_i(\chi)\phi_i.$$

By Fourier inversion, for $\gamma \in \Gamma$,

$$a(\gamma) = |\Gamma|^{-1} \sum_{\chi\in\widehat{\Gamma}} f(\chi)\chi(\gamma) = |\Gamma|^{-1} \sum_{\chi\in\widehat{\Gamma}} (f\cdot\gamma)(\chi),$$

where the multiplication $f \cdot \gamma \in (K_{\mathfrak{v}}^c\Gamma)^\times$. We note that $f \cdot \gamma$ lies in the coset $f\Gamma = g$, so changing f by $f \cdot \gamma$, we see that it suffices to show $a(1) \in O_{\mathfrak{v}}^c$, where

$$a(1) = |\Gamma|^{-1} \sum_{\chi\in\widehat{\Gamma}} f(\chi).$$

Now, for every $\chi \in \widehat{\Gamma}$, we have $f(\chi) \in (O_{\mathfrak{v}}^c)^\times$. Indeed if m is the exponent of Γ, then $m\chi \in A_{\widehat{\Gamma}}$, so, using the definition of g and the equality $f\Gamma = g$, we have the result claimed just above

$$f(\chi)^m = f(m\chi) = g(m\chi) \in U_{\mathfrak{m}}(O_{\mathfrak{v}}^c) \subseteq (O_{\mathfrak{v}}^c)^\times.$$

By the definition of $d(\chi)$ we have now

$$f(\chi) = f(d(\chi)) \prod_{i=1}^{k} f(\phi_i)^{r_i(\chi)}$$

and since $d(\chi) \in A_{\widehat{\Gamma}}$, $f\left(d\left(\chi\right)\right) = g\left(d\left(\chi\right)\right) \in U_{\mathfrak{m}}(O_{\mathfrak{v}}^c)$. Hence,

$$f(\chi) \equiv \prod_{i=1}^{k} f(\phi_i)^{r_i(\chi)} \pmod{\mathfrak{m}O_{\mathfrak{v}}^c},$$

and so by the definition of $a(1)$ we obtain

$$|\Gamma| \cdot a(1) \equiv \sum_{\chi \in \widehat{\Gamma}} \prod_{i=1}^{k} y_i^{r_i(\chi)} \pmod{\mathfrak{m}O_{\mathfrak{v}}^c},$$

where $y_i = f(\phi_i)$.
Now, χ run over $\widehat{\Gamma}$, so the k-tuple $\left(r_1\left(\chi\right), \ldots, r_k\left(\chi\right)\right)$ runs over all k-tuples of integer $(r_1, \ldots, r_k)$ with $0 \leq r_i < e_i$. Hence, since we have that $|\Gamma| = e_1 \cdots e_k$ and $|\Gamma|$ divides $\mathfrak{m}$, we obtain

$$a(1) = |\Gamma|^{-1} \prod_{i=1}^{k} \left(\sum_{r_i=0}^{e_i-1} y_i^{r_i} \right) = \prod_{i=1}^{k} \frac{y_i^{e_i} - 1}{e_i(y_i - 1)}, \quad (\mathrm{mod} O_{\mathfrak{v}}^c);$$

where if $y_i = 1$ put the corresponding factor equal to 1.
So now, we only need to show that $\frac{y_i^{e_i}-1}{e_i(y_i-1)} \in O_{\mathfrak{v}}^c$.
Before applying the previous Lemma which gives us the final proof, we notice that $e_i\phi_i \in A_{\widehat{\Gamma}}$, so

$$y_i^{e_i} = f(\phi_i)^{e_i} = g(e_i\phi_i) \in U_{\mathfrak{m}}(O_{\mathfrak{v}}^c) \subseteqq U_{e_i^2}(O_{\mathfrak{v}}^c),$$

since from definition and hypothesis we have that e_i divides m and m^2 divides $\mathfrak{m}$. Now applying the Lemma everything is proved.

□

Chapter 3

McCulloh's result in the Abelian situation - Unramified case

In this chapter and in the following one, we will retrace the proof given by McCulloh in [McC87] for realizable classes with the group Γ abelian. First of all we shall concentrate on the unramified case and the in the following chapter we will consider the general tame case, which is more difficult to solve and understand.
The basic tools used in these chapters are contained in the section A.4 of the Appendix, where the concept of class of a tame Γ-extension is introduced.

All along this chapter we shall consider just the unramified situation, without considering the general tame case. Indeed if we restrict our attention to the unramified extensions, then the work is easier and lightened by the absence of a component depending on the Stickelberger map, which we are going to define in the first section of the next chapter.

During this chapter and the following one, given a prime $\mathfrak{v}$ of K, we choose and fix a generator $\pi\,(=\pi_{\mathfrak{v}})$ of the maximal ideal $\mathfrak{p}$ of $O_{\mathfrak{v}}$. We denote by q the finite order of the residue class field $O_{\mathfrak{v}}/\mathfrak{p}$ and p its characteristic. As before we use $\mathfrak{v}$ to denote even the additive valuation $\mathfrak{v} : (K_{\mathfrak{v}}^{c})^{\times} \longrightarrow \mathbb{Q}$ normalized with respect to $K_{\mathfrak{v}}$, so that $\mathfrak{v}(\pi) = 1$.

3.1 Unramified local resolvends

In this section, we try to well describe the unramified local resolvends, which will be fundamental to understand the shape of the realisable classes.

It's better to start recalling some basic notions about the Galois group of unramified extensions.

Maximal Unramified extensions and structure of $\Omega_{\mathfrak{v}}^{nr}$: As well known to understand unramified extensions, we've just to look at the residue field extensions. We know by hypothesis that $O_{\mathfrak{v}}/\mathfrak{p}$ is of finite order $q = p^{r}$ (where p is the characteristic of the field) and so, by finite fields theory, any extension is a finite field of order q^{n}, obtained adding a primitive $(q^{n}-1)$-th primitive root of unity. Thanks to this, we can pass to the original unramified extension of fields which is again obtained adding a primitive root of unity as for residue fields extensions. Thanks to the fact that we are considering an unramified extension, the Galois Group of the field extension is equal to the Galois Group of the residue field extension (remembering that the Galois Group of the residue field extension is isomorphic to the quotient between the Decomposition group and the Inertia group and that we are considering a local and unramified situation, so the Decomposition Group is equal to the Galois Group of the field extension and the Inertia Group is trivial). In this case, always using finite fields theory, we have a cyclic Galois Group, generated by the Frobenius map $\phi : x \longrightarrow x^q$ and so, thanks to this consideration, it follows that $K_{\mathfrak{v}}^{nr}$ is obtained from $K_{\mathfrak{v}}$ adding all roots of unity with order coprime with p and its Galois Group $\Omega_{\mathfrak{v}}^{nr}$ is a procyclic group generated by $\phi\,(=\phi_{\mathfrak{v}})$ (for a detailed explanation of these considerations, look at [Art67] and at [FT91], pag.135-136). Of course from finite fields considerations, all $(q-1)$-th roots of unity lie in $K_{\mathfrak{v}}$.

We recall now, without proving it, the famous Nakayama's Lemma, which will be useful in the next Proposition.

Lemma 3.1.1 (Nakayama's Lemma)**.** *Let Λ be a (not necessarily commutative) ring. If $M = L + IM$, where M is a finitely generated Λ-module, $L \subset M$ is a submodule and I an ideal contained in any maximal ideal ($I \in rad(\Lambda)$); then $M = L$.*

Thanks to the previous Lemma, we can prove now the following Proposition, which is a particular case of the already cited Noether Criterion.

Proposition 3.1.1.1. *Let $h_{\mathfrak{v}} \in Hom(\Omega_{\mathfrak{v}}^{nr}, \Gamma)$. Then $(O_{\mathfrak{v}})_{h_{\mathfrak{v}}}/O_{\mathfrak{v}}$ has a normal integral basis.*

Proof. Like in previous proof, we always consider the local case, without writing $\mathfrak{v}$ anytime. The field extension K^h/K is unramified and so, as we've seen in the explanation about unramified extensions, Gal(K^h/K) is isomorphic to the Galois group of the residue field extension $\overline{K}^h/\overline{K}$. Now any lifting to O^h of a field basis of $\overline{K}^h/\overline{K}$ is an integral basis. If we denote by $\beta \in O^h$ the lifting of the normal basis generator $\overline{\beta}$, we have that the set $\{\gamma(\beta)\}_{\gamma\in\Gamma}$ is linearly independent over O (to see it consider any linear combination giving a linear dependence relation among the $\gamma(\beta)$'s and using the quotient map to the residue field, prove that any coefficient is zero) and it generates O^h over O, by Nakayama's Lemma. Indeed if M is the O-submodule of O^h generated by the $\gamma(\beta)$'s, we have $O^h = M + \mathfrak{v}O^h$ and so $O^h = M$. Letting $b : \Gamma \longrightarrow O^c$ be defined as in the previous proof by

$$b(t) = \begin{cases} \tau(\beta) & \text{if } t = h(\tau), \\ 0 & \text{if } t \notin h(\Omega^t), \end{cases}$$

it's not hard to check that b generates a normal integral basis of O_h/O. □

After this general introduction to the unramified context, we can finally enunciate the Theorem which describes the unramified local resolvends.

Theorem 3.1.2. *Let $h_{\mathfrak{v}} \in Hom(\Omega_{\mathfrak{v}}^{nr}, \Gamma)$. If $a_{\mathfrak{v}}$ is a N.I.B. generator of $(O_{\mathfrak{v}})_{h_{\mathfrak{v}}}/O_{\mathfrak{v}}$, then*

$$\mathcal{R}_\Gamma(a_{\mathfrak{v}}) = u_{\mathfrak{v}}$$

where $u_{\mathfrak{v}} \in \mathcal{H}(O_{\mathfrak{v}}\Gamma)$.
Conversely, let $u_{\mathfrak{v}} \in \mathcal{H}(O_{\mathfrak{v}}\Gamma)$ *and let* $h_{\mathfrak{v}}$ *be the image of* $u_{\mathfrak{v}}$ *under the connecting homomorphism* $\mathcal{H}(O_{\mathfrak{v}}\Gamma) \longrightarrow Hom(\Omega_{\mathfrak{v}}^{nr}, \Gamma)$. *Then* $(O_{\mathfrak{v}})_{h_{\mathfrak{v}}}/O_{\mathfrak{v}}$ *has a N.I.B. generator* $a_{\mathfrak{v}}$ *for which* $\mathcal{R}_{\Gamma}(a_{\mathfrak{v}}) = u_{\mathfrak{v}}$.

Proof. It is just another way of saying that $\mathcal{H}(O_{\mathfrak{v}}\Gamma)$ is the set of all reduced resolvends of local normal integral basis generators (look at (2.6.3)). □

3.2 Characterization of realizable classes

In this section we will be able to give the desired characterization of the set of realizable classes in the unramified case, that is to say the set $R_{nr}(O\Gamma)$ of classes in $Cl(O\Gamma)$ of form (O_h) for some unramified Γ-extension K_h/K. We refer to A.4 for the definition of the idele $J(K\Gamma)$ and the basic notions on the idea of class of an unramified (in general tame) Γ-extension.

We shall use the previous section to decompose a representative $c \in J(K\Gamma)$ of such a class in the form

$$rag(c) = \lambda\left(\mathcal{R}_{\Gamma}(b)\right) u\,, \tag{3.2.1}$$

where u is an idele with components $u_{\mathfrak{v}}$, λ is a principal idele map and $\mathcal{R}_{\Gamma}(b) \in \mathcal{H}(K\Gamma)$.
The characterization will say that if a class in $Cl(O\Gamma)$ has a representative c for which $rag(c)$ has a decomposition like the previous one, then the class is realizable.

3.2.1 Definition of the ideles involved in the unramified case

In this section we define the ideles which will be involved thereafter for the unramified case.
Let $\mathcal{H}(\mathbb{A}(K\Gamma))$, $\mathcal{H}^t(\mathbb{A}(K\Gamma))$ and $\mathcal{H}^{nr}(\mathbb{A}(K\Gamma))$, respectively, be the restricted direct product of the $\mathcal{H}(K_{\mathfrak{v}}\Gamma)$, $\mathcal{H}^t(K_{\mathfrak{v}}\Gamma)$ and $\mathcal{H}^{nr}(K_{\mathfrak{v}}\Gamma)$ with respect to the subgroups $\mathcal{H}(O_{\mathfrak{v}}\Gamma)$. We can define, componentwise, the following map:

$$rag : J(K\Gamma) \longrightarrow \mathcal{H}(\mathbb{A}(K\Gamma))\,; \tag{3.2.2}$$

which is well defined since, by Theorem 2.6.2, we have $rag(O_{\mathfrak{v}}\Gamma)^{\times} \subseteq \mathcal{H}(O_{\mathfrak{v}}\Gamma)$ for all $\mathfrak{v}$.

For completeness we also define the unit idele group $\mathcal{H}(\mathbb{A}(O\Gamma)) = \prod_{\mathfrak{v}} \mathcal{H}(O_{\mathfrak{v}}\Gamma)$, which allows us to write $rag(U(O\Gamma)) \subseteq \mathcal{H}(\mathbb{A}(O\Gamma))$.

Moreover we define the useful principal idele map

$$\lambda : \mathcal{H}(K\Gamma) \longrightarrow \mathcal{H}(\mathbb{A}(K\Gamma))\,, \tag{3.2.3}$$

which arises from the componentwise inclusions $\mathcal{H}(K\Gamma) \subseteq \mathcal{H}(K_{\mathfrak{v}}\Gamma)$ given by the inclusions $i_{\mathfrak{v}} : K^c \longrightarrow K_{\mathfrak{v}}^c$. This is again well defined: if $\mathcal{R}_{\Gamma}(a) \in \mathcal{H}(K\Gamma)$ where $K\Gamma.a = K_h$, then for all but a finite number of prime $\mathfrak{v}$, $h_{\mathfrak{v}}$ is unramified and $O_{\mathfrak{v}}\Gamma.a = (O_{\mathfrak{v}})_{h_{\mathfrak{v}}}$, so that, by (2.6.3), $\mathcal{R}_{\Gamma}(a) \in \mathcal{H}(O_{\mathfrak{v}}\Gamma)$.

From (2.2.2) it follows that the following diagram commutes:

$$\begin{tikzcd}
\mathcal{H}(K\Gamma) \arrow[d, "\lambda"] & & K\Gamma^{\times} \arrow[ll, hook', "rag"'] \arrow[d, "\lambda"] \\
\mathcal{H}\left(\mathbb{A}\left(K\Gamma\right)\right) & & J(K\Gamma). \arrow[ll, hook', "rag"']
\end{tikzcd} \tag{3.2.4}$$

Clearly,

$$\lambda\left(\mathcal{H}^{t}\left(K\Gamma\right)\right) = \lambda\left(\mathcal{H}\left(K\Gamma\right)\right) \cap \mathcal{H}^{t}\left(\mathbb{A}\left(K\Gamma\right)\right), \tag{3.2.5}$$

$$\lambda\left(\mathcal{H}^{nr}\left(K\Gamma\right)\right) = \lambda\left(\mathcal{H}\left(K\Gamma\right)\right) \cap \mathcal{H}^{nr}\left(\mathbb{A}\left(K\Gamma\right)\right). \tag{3.2.6}$$

3.2.2 Decomposition of unramified global resolvends

We are now ready to get a decomposition of unramified global resolvends, using the results achieved in the previous local part; in particular we have the following important Theorem.

Theorem 3.2.3. *Let $h \in Hom(\Omega, \Gamma)$ and suppose $K\Gamma.b = K_h$ (b is a normal basis generator). Then h is unramified if and only if there are elements $c \in J(K\Gamma)$ and $u \in \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)$ such that*

$$\lambda\left(\mathcal{R}_{\Gamma}\left(b\right)\right) = \left(rag\left(c\right)\right)^{-1} u.$$

Moreover, if so, then $j(c) = (O_h) \in Cl(O\Gamma)$.

Proof. ($\Longrightarrow$) We suppose that h is unramified. Exactly as in (A.4.0.1) $b \in K_h$ is a normal basis generator and for all $\mathfrak{v}$ we have $a_{\mathfrak{v}} \in (O_{\mathfrak{v}})_{h_{\mathfrak{v}}}$, such that

$$(O_{\mathfrak{v}})_{h_{\mathfrak{v}}} = O_{\mathfrak{v}}\Gamma.a_{\mathfrak{v}},$$

and $c = (c_{\mathfrak{v}})_{\mathfrak{v}} \in J(K\Gamma)$ such that

$$a_{\mathfrak{v}} = c_{\mathfrak{v}}.b;$$

so by (A.4.3), $\mathcal{R}_{\Gamma}(a_{\mathfrak{v}}) = (rag(c_{\mathfrak{v}}))\mathcal{R}_{\Gamma}(b)$.
Now we can use Theorem 3.1.2 which tells us that

$$\mathcal{R}_{\Gamma}(a_{\mathfrak{v}}) = u_{\mathfrak{v}}$$

where $u_{\mathfrak{v}} \in \mathcal{H}(O_{\mathfrak{v}}\Gamma)$. In this way $u = (u_{\mathfrak{v}})_{\mathfrak{v}} \in \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)$ and we have

$$u = \left(rag\left(c\right)\right)\lambda\left(\mathcal{R}_{\Gamma}\left(b\right)\right),$$

as we wanted to show.

($\Longleftarrow$) Conversely, suppose

$$\lambda\left(\mathcal{R}_{\Gamma}\left(b\right)\right) = \left(rag\left(c\right)\right)^{-1} u,$$

where $c \in J(K\Gamma)$ and $u \in \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)$. By (2.6.4), we have $\left(rag\left(c\right)\right)^{-1} \in \mathcal{H}^{nr}\left(\mathbb{A}\left(K\Gamma\right)\right)$ and $u \in \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right) \subseteq \mathcal{H}^{nr}\left(\mathbb{A}\left(K\Gamma\right)\right)$. Thus we obtain

$$\lambda\left(\mathcal{R}_{\Gamma}\left(b\right)\right) \in \lambda\left(\mathcal{H}\left(K\Gamma\right)\right) \cap \mathcal{H}^{nr}\left(\mathbb{A}\left(K\Gamma\right)\right) = \lambda\left(\mathcal{H}^{nr}\left(K\Gamma\right)\right),$$

which tells that h is unramified.

Moreover, locally we have for any $\mathfrak{v}$

$$\mathcal{R}_{\Gamma}(b) = (rag\,(c_{\mathfrak{v}}))^{-1}\, u_{\mathfrak{v}} \in \mathcal{H}^{nr}\,(K_{\mathfrak{v}}\Gamma)\,.$$

So, by (2.2.2), $\mathcal{R}_{\Gamma}(b)$ and $u_{\mathfrak{v}}$ have the same image $h_{\mathfrak{v}}$ in $\mathrm{Hom}(\Omega_{\mathfrak{v}}^{nr}, \Gamma)$, and so by Theorem 3.1.2, $u_{\mathfrak{v}} = \mathcal{R}_{\Gamma}(a_{\mathfrak{v}})$ where $O_{\mathfrak{v}}\Gamma.a_{\mathfrak{v}} = (O_{\mathfrak{v}})_{h_{\mathfrak{v}}}$. Hence, recalling the remark made after (A.4.3), we have $j(c) = (O_h)$ in $Cl(O\Gamma)$. □

3.2.4 The Realizable classes form a subgroup

In this section we arrive to the most important result which says that the realizable classes form a subgroup in the unramified abelian case.

We start by defining the important set of realizable classes obtained by unramified extensions

$$R_{nr}(O\Gamma) = \{(O_h) |\, h \in \mathrm{Hom}(\Omega_K^{nr}, \Gamma)\}.$$

We can also define

$$\mathbb{R}_{nr}(O\Gamma) = j^{-1}\,(R_{nr}\,(O\Gamma))\,, \tag{3.2.7}$$

where $j : J(K\Gamma) \longrightarrow Cl(O\Gamma)$ is the usual quotient map.

Here we have the important Theorem, which gives us the result we are looking for in the unramified case.

Theorem 3.2.5 (Unramified case)**.** *Let* $c \in J(K\Gamma)$*. Then*

$$c \in \mathbb{R}_{nr}(O\Gamma) \Longleftrightarrow rag(c) \in \lambda\,(\mathcal{H}\,(K\Gamma))\,\mathcal{H}\,(\mathbb{A}\,(O\Gamma))\,.$$

Proof. ($\Longrightarrow$) We take $h \in \mathrm{Hom}(\Omega^{nr}, \Gamma)$ and suppose that $(O_h) = j(c)$. By the Normal basis Theorem, we take b such that $K\Gamma.b = K_h$. Then using Theorem 3.2.3, we find $c' \in J(K\Gamma)$ and $u \in \mathcal{H}\,(\mathbb{A}\,(O\Gamma))$ with $j(c') = j(c)$ and $\lambda\,(\mathcal{R}_{\Gamma}\,(b)) = (rag\,(c'))^{-1}\,u$.
Then bringing $rag(c')$ to the other side, we obtain $rag(c') \in \lambda\,(\mathcal{H}\,(K\Gamma))\,\mathcal{H}\,(\mathbb{A}\,(O\Gamma))$.
Since $j(c) = j(c')$, we have $c^{-1}c' \in \lambda(K\Gamma^{\times})U(O\Gamma)$, so we deduce that

$$rag(c^{-1}c') \in \lambda\,(\mathcal{H}\,(K\Gamma))\,\mathcal{H}\,(\mathbb{A}\,(O\Gamma))\,,$$

obtaining the first implication.

($\Longleftarrow$) If we suppose that $rag(c) \in \lambda\,(\mathcal{H}\,(K\Gamma))\,\mathcal{H}\,(\mathbb{A}\,(O\Gamma))$, then

$$rag(c) = \lambda\,(\mathcal{R}_{\Gamma}\,(b))^{-1}\,u,$$

where $K\Gamma.b = K_h$ for some $h \in \mathrm{Hom}(\Omega, \Gamma)$ and $u \in \mathcal{H}\,(\mathbb{A}\,(O\Gamma))$. Using Theorem 3.2.3, we conclude that h is unramified and $j(c) = (O_h)$. □

We give an alternative formulation of the previous Theorem, using the following map

$$Cl(O\Gamma) = \frac{J(K\Gamma)}{\lambda(K\Gamma^{\times})U(O\Gamma)} \xrightarrow{\qquad Rag \qquad} \frac{\mathcal{H}(\mathbb{A}(K\Gamma))}{\lambda(\mathcal{H}(K\Gamma))\mathcal{H}(\mathbb{A}(O\Gamma))} \quad , \tag{3.2.8}$$

where Rag is induced by $rag : J(K\Gamma) \longrightarrow \mathcal{H}(\mathbb{A}(K\Gamma))$. Indeed from Theorem 3.2.5, we have the following Corollary.

Corollary 3.2.6. *In same hypothesis as before:*

$$R_{nr}(O\Gamma) = ker(Rag).$$

In particular, $R_{nr}(O\Gamma)$ is a subgroup of $Cl(O\Gamma)$.

From (2.2.2), we observe that the kernel of $rag : J(K\Gamma) \longrightarrow \mathcal{H}(\mathbb{A}(K\Gamma))$ is $\prod_{\mathfrak{v}} \Gamma \subseteq U(O\Gamma)$ and so we have

$$\begin{aligned} Cl(O\Gamma) = \frac{J(K\Gamma)}{\lambda(K\Gamma^{\times})U(O\Gamma)} &\cong \frac{rag\, J(K\Gamma)}{\lambda(rag\, K\Gamma^{\times})\, rag\, U(O\Gamma)}, \\ &\subseteq \frac{\mathcal{H}(\mathbb{A}(K\Gamma))}{\lambda(rag\, K\Gamma^{\times})\, rag\, U(O\Gamma)}. \end{aligned}$$

So we can give an explicit description of the set of realizable classes realized by unramified extensions.

Corollary 3.2.7. *Under the previous isomorphism, we have*

$$R_{nr}(O\Gamma) \cong \frac{rag\, J(K\Gamma) \cap \lambda(\mathcal{H}(K\Gamma))\,\mathcal{H}(\mathbb{A}(O\Gamma))}{\lambda(rag\, K\Gamma^{\times}) rag\, U(O\Gamma)}.$$

Chapter 4

McCulloh's result in the Abelian situation - Tame case

In this chapter, as already announced, we will consider McCulloh's proof for the more general and complex tame case. We will see that some parts are exactly equal to the unramified situation, even if in this case we have to introduce a new tool which is fundamental to get the final result: the Stickelberger map.

4.1 The Stickelberger map and its transpose

We start here introducing the so called Stickelberger map, an important tool which is fundamental to produce reduced resolvends of local normal integral basis generator in the tame situation and describe their prime factorization. After its definition, we shall try to discover different properties of the Stilckelberger map and we will see how this map is linked to the set of reduced resolvends.

For Γ abelian, we define a $\mathbb{Q}$-bilinear map

$$\langle\, , \rangle : \mathbb{Q}\widehat{\Gamma} \times \mathbb{Q}\Gamma \longrightarrow \mathbb{Q} \tag{4.1.1}$$

as follows on basis elements. Given $\chi \in \widehat{\Gamma}$, $\gamma \in \Gamma$, we know that $\chi(\gamma)$ is a root of unity because Γ is a finite group and we define $\langle \chi, \gamma \rangle$ as the unique rational number characterized by

$$\chi(\gamma) = e^{2\pi i \langle \chi, \gamma \rangle}, \;\; 0 \leq \langle \chi, \gamma \rangle < 1. \tag{4.1.2}$$

The *Stickelberger map*

$$\Theta = \Theta_{\Gamma} : \mathbb{Q}\widehat{\Gamma} \longrightarrow \mathbb{Q}\Gamma \tag{4.1.3}$$

is the $\mathbb{Q}$-linear transformation defined for $\alpha \in \mathbb{Q}\widehat{\Gamma}$ by

$$\Theta(\alpha) = \sum_{\gamma \in \Gamma} \langle \alpha, \gamma \rangle \gamma. \tag{4.1.4}$$

The *Stickelberger module* is the set

$$S = S_{\Gamma} = \Theta(\mathbb{Z}\widehat{\Gamma}) \cap \mathbb{Z}\Gamma, \tag{4.1.5}$$

which is well characterized by the following Proposition.

Proposition 4.1.0.1. *For $\alpha \in \mathbb{Z}\widehat{\Gamma}$,*

$$\Theta(\alpha) \in \mathbb{Z}\Gamma \Longleftrightarrow \alpha \in A_{\widehat{\Gamma}}.$$

In particular, Θ defines, by restriction, a $\mathbb{Z}$-homomorphism

$$\Theta_{\Gamma} : A_{\widehat{\Gamma}} \longrightarrow \mathbb{Z}\Gamma,$$

whose image is the Stickelberger module

$$S_{\Gamma} = \Theta_{\Gamma}(A_{\widehat{\Gamma}}).$$

Proof. We recall that $\det(\sum_{\chi} a_{\chi}\chi) = \prod \chi^{a_{\chi}}$ and so if $\alpha \in \mathbb{Z}\widehat{\Gamma}$ and $\gamma \in \Gamma$, by bilinearity of the Stickelberger map we have

$$(\det(\alpha))(\gamma) = e^{2\pi i \langle \alpha, \gamma \rangle},$$

indeed if $\alpha = \sum_{\chi} a_{\chi}\chi$, $a_{\chi} \in \mathbb{Z}$, then $(\det(\alpha))(\gamma) = \prod_{\chi} \chi(\gamma)^{a_{\chi}} = e^{2\pi i \sum_{\chi} \langle \chi, \gamma \rangle a_{\chi}}$ and by bilinearity,

$$\sum_{\chi} a_{\chi} \langle \chi, \gamma \rangle = \langle \sum_{\chi} a_{\chi}\chi, \gamma \rangle = \langle \alpha, \gamma \rangle.$$

Hence

$$\Theta(\alpha) \in \mathbb{Z}\Gamma \Longleftrightarrow \forall \gamma, \langle \alpha, \gamma \rangle \in \mathbb{Z},$$

which means

$$\Theta(\alpha) \in \mathbb{Z}\Gamma \Longleftrightarrow \forall \gamma, (\det(\alpha))(\gamma) = 1 \Longleftrightarrow \alpha \in \ker(\det) = A_{\widehat{\Gamma}}.$$

The last assertion of the Proposition now is trivial. □

Now we're going to play with the different possible Ω-actions on Γ, in order to find a particular action of Ω on Γ such that $\Theta : \mathbb{Q}\widehat{\Gamma} \longrightarrow \mathbb{Q}\Gamma$ preserves Ω-action.
If we denote by m the exponent of Γ, then $(\mathbb{Z}/m\mathbb{Z})^{\times}$ acts (canonically) as the group of automorphisms of the group of m-th roots of unity μ_m and it also acts (canonically) as a group of automorphisms of any group of exponent m, in particular Γ and $\widehat{\Gamma}$.
Let

$$\kappa : \Omega \longrightarrow (\mathbb{Z}/m\mathbb{Z})^{\times}$$

be the *"m-th cyclotomic character"* of Ω, obtained restricting the action of Ω to μ_m; in other words

$$\omega.\zeta = \zeta^{\kappa(\omega)}$$

for all $\zeta \in \mu_m$, $\omega \in \Omega$. We underline that if $\mu_m \subseteq K$ then the map κ is trivial, because any m-th root of unity is fixed by Ω in this case.
We denote by $\Gamma(n)$, for any $n \in \mathbb{Z}$, the group Γ considered as an Ω-module via $\kappa^n : \Omega \longrightarrow (\mathbb{Z}/m\mathbb{Z})^{\times}$, that is to say that Ω acts on Γ in the following way:

$$\omega.\gamma = \gamma^{\kappa^n(\omega)} \quad \text{for} \quad \gamma \in \Gamma, \ \omega \in \Omega.$$

Thus $\Gamma(0)$ denotes Γ with the trivial action of Ω, instead if we consider $\Gamma(-1)$ we have

$$\omega.\gamma = \gamma^{\kappa(\omega^{-1})} \quad \text{for} \quad \gamma \in \Gamma, \ \omega \in \Omega.$$

By the previous remark, if $\mu_m \subseteq K$ then we have $\Gamma(n) = \Gamma(0)$ for all n.

Remark 4.1.1. *If we view Γ as a group of characters of $\widehat{\Gamma}$, it has a natural Ω-action given by $(\omega.\gamma)(\chi) = \omega.\left(\gamma\left(\chi\right)\right)$ for $\gamma \in \Gamma$, $\chi \in \widehat{\Gamma}$ and $\omega \in \Omega$. Since $\gamma(\chi)$ is an m-th root of unity we have that $\omega.\gamma = \gamma^{\kappa(\omega)}$ and so we can identify Γ with $\Gamma(1)$ and thanks to this, we have*

$$K\widehat{\Gamma} \cong Map_{\Omega}\left(\Gamma\left(1\right), K^{c}\right).$$

Proposition 4.1.1.1. *The linear transformation $\Theta_{_\Gamma} : \mathbb{Q}\widehat{\Gamma} \longrightarrow \mathbb{Q}\Gamma(-1)$ preserves the action of Ω.*

Proof. Given $\omega \in \Omega$, $\chi \in \widehat{\Gamma}$ and $\gamma \in \Gamma(-1)$ we have

$$(\omega.\chi)(\gamma) = \omega.\left(\chi\left(\gamma\right)\right) = \chi(\gamma)^{\kappa(\omega)} = \chi(\gamma^{\kappa(\omega)}) = \chi(\omega^{-1}.\gamma),$$

obtaining $\langle \omega.\chi, \gamma\rangle = \langle \chi, \omega^{-1}.\gamma\rangle$. Then

$$\Theta(\omega.\chi) = \sum_{\gamma\in\Gamma} \langle \omega.\chi, \gamma\rangle\gamma = \sum_{\gamma\in\Gamma} \langle \chi, \omega^{-1}.\gamma\rangle\gamma = \sum_{\gamma\in\Gamma} \langle \chi, \gamma\rangle(\omega.\gamma) = \omega.\left(\Theta\left(\chi\right)\right).$$

□

Thanks to Prop. 4.1.0.1 and Prop. 4.1.1.1 we can consider the transpose map

$$\Theta^{t} = \Theta^{t}_{_\Gamma} : \mathrm{Hom}\left(\mathbb{Z}\Gamma(-1), (K^{c})^{\times}\right) \longrightarrow \mathrm{Hom}\left(A_{\widehat{\Gamma}}, (K^{c})^{\times}\right),$$

where $\Theta^{t}(f) = f \circ \Theta$. If Ω acts on homomorphisms as usual by $(\omega.f)(\chi) = \omega.\left(f\left(\omega^{-1}.\chi\right)\right)$, we see that the transpose map is an Ω-homomorphism; so by restriction we obtain the useful homomorphism

$$\Theta^{t} : \mathrm{Hom}_{\Omega}\left(\mathbb{Z}\Gamma\left(-1\right), (K^{c})^{\times}\right) \longrightarrow \mathrm{Hom}_{\Omega}\left(A_{\widehat{\Gamma}}, (K^{c})^{\times}\right) = \mathcal{H}(K\Gamma), \tag{4.1.6}$$

which connects the Stickelberger map with resolvends.

The domain of the transpose map $\mathrm{Hom}_{\Omega}\left(\mathbb{Z}\Gamma\left(-1\right), (K^{c})^{\times}\right)$ is identified with the group of units of the K-algebra $\mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), K^{c}\right)$, which is not canonically isomorphic to $\mathrm{Map}_{\Omega}\left(\Gamma\left(+1\right), K^{c}\right)$. Indeed a function in $\mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), K^{c}\right)$ is determined by its values on a set of Ω-orbit representatives $\Gamma' \subseteq \Gamma(-1)$ and with the only request that the value at such a representative $\gamma' \in \Gamma'$ is fixed by the stabilizer of γ'. Now for any $\chi \in \widehat{\Gamma}$ and $\gamma \in \Gamma(-1)$, we have $\chi(\omega.\gamma) = \chi(\gamma^{\kappa(\omega)^{-1}}) = \omega^{-1}.\left(\chi\left(\gamma\right)\right)$, so ω fixes γ' if and only if it fixes $\chi(\gamma')$ for all $\chi \in \widehat{\Gamma}$ and so the values $\chi(\gamma')$'s are fixed by the stabilizer as required. For $\gamma \in \Gamma$, let $K(\gamma)$ denote the field obtained from K by adjoining $\chi(\gamma)$ for all $\chi \in \widehat{\Gamma}$. Then, evaluating at the elements of Γ', we obtain

$$\mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), K^{c}\right) \cong \prod_{\gamma'\in\Gamma'} K(\gamma'). \tag{4.1.7}$$

Moreover $\Gamma(-1)$ and $\Gamma(+1)$ have the same Ω-orbits and the same stabilizers, since $\gamma = \omega.\gamma'$ in $\Gamma(-1) \iff \gamma' = \omega.\gamma$ in $\Gamma(+1)$. Thus we can apply exactly the same argument as before, to obtain

$$\mathrm{Map}_{\Omega}\left(\Gamma\left(+1\right), K^{c}\right) \cong \prod_{\gamma'\in\Gamma'} K(\gamma'). \tag{4.1.8}$$

As a consequence, we have

$$\mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), K^{c}\right) \cong \mathrm{Map}_{\Omega}\left(\Gamma\left(+1\right), K^{c}\right) \cong K\widehat{\Gamma},$$

where the isomorphism depends on the choice of the set of orbit representatives Γ' (so it is not canonical).

We denote by $O(\gamma)$ the ring of integers in $K(\gamma)$ and by Λ the maximal O-order of the K-algebra $\mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), K^{c}\right)$; which is $\mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), O^{c}\right)$. So, using the previous isomorphism, we obtain:

$$\begin{aligned} \mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), O^{c}\right) &= \Lambda \cong \prod_{\gamma' \in \Gamma'} O(\gamma'), \\ \mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), K^{c}\right) &= K\Lambda \cong \prod_{\gamma' \in \Gamma'} K(\gamma'), \\ \mathrm{Map}\left(\Gamma\left(-1\right), O^{c}\right) &= O^{c}\Lambda, \\ \mathrm{Map}\left(\Gamma\left(-1\right), K^{c}\right) &= K^{c}\Lambda. \end{aligned} \tag{4.1.9}$$

In this way we can abbreviate (4.1.6) to give

$$\Theta^{t} : K\Lambda^{\times} \longrightarrow \mathcal{H}(K\Gamma). \tag{4.1.10}$$

Localization. Regarding $i_{\mathfrak{v}} : K \longrightarrow K_{\mathfrak{v}}^{c}$ as an inclusion, $\widehat{\Gamma}$ as $\mathrm{Hom}\left(\Gamma, (K_{\mathfrak{v}}^{c})^{\times}\right)$ and the cyclotomic character $\kappa_{\mathfrak{v}}$ just as the restriction of κ to $\Omega_{\mathfrak{v}} \subseteq \Omega$; we can now give a local interpretation of the previous result. Indeed locally we can consider $\Lambda_{\mathfrak{v}} = \mathrm{Map}_{\Omega_{\mathfrak{v}}}(\Gamma(-1), O_{\mathfrak{v}}^{c})$, which is just the completion $O_{\mathfrak{v}} \otimes_{O} \Lambda$, since

$$\begin{aligned} O_{\mathfrak{v}} \otimes_{O} \mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), O^{c}\right) &= \mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), O_{\mathfrak{v}} \otimes_{O} O^{c}\right) \\ &= \mathrm{Map}_{\Omega}\left(\Gamma\left(-1\right), \mathrm{Map}_{\Omega_{\mathfrak{v}}}\left(\Omega, O_{\mathfrak{v}}^{c}\right)\right) \\ &= \mathrm{Map}_{\Omega_{\mathfrak{v}}}\left(\Gamma\left(-1\right), O_{\mathfrak{v}}^{c}\right); \end{aligned}$$

where in the first equality we just used the property of the tensor product, in the second we used the already known equality $O_{\mathfrak{v}} \otimes O^{c} \cong O_{\mathfrak{v}}^{c}$ and in the last one we applied coinduction.
Using exactly the same arguments as before, we obtain the local homomorphism

$$\Theta^{t} : \left(K_{\mathfrak{v}}\Lambda_{\mathfrak{v}}\right)^{\times} \longrightarrow \mathcal{H}(K_{\mathfrak{v}}\Gamma),$$

now we just observe that $K_{\mathfrak{v}}\Lambda_{\mathfrak{v}} = K_{\mathfrak{v}}\Lambda$ and then we have the following commutative diagram

$$\begin{tikzcd} K\Lambda^{\times} \arrow[r, "\Theta^{t}"] \arrow[d] & \mathcal{H}(K\Gamma) \arrow[d] \\ (K_{\mathfrak{v}}\Lambda)^{\times} \arrow[r, "\Theta^{t}"] & \mathcal{H}(K_{\mathfrak{v}}\Gamma), \end{tikzcd} \tag{4.1.11}$$

where the vertical maps are inclusions induced by the inclusion $i_{\mathfrak{v}}$ and the commutativity is easily proved considering the vertices as Hom groups.

4.2 Decomposition of tame local resolvends

In this section, using the results reached in the previous part, we try to obtain a decomposition of tame local resolvends, useful to understand the shape of the set of realizable classes.

As done for the unramified case, we need now to recall, in an explicit way, some well known notions about the Galois Group of tame extensions.

Maximal Tame extensions and structure of $\Omega_{\mathfrak{v}}^t$: As well explained in [Ere], the Maximal Tame extension is obtained by the compositum of all split tame extensions. In particular $K_{\mathfrak{v}}^t$ is obtained from $K_{\mathfrak{v}}^{nr}$, adjoining the values $\pi^{\frac{1}{n}}$ with n prime to p (we choose a coherent set of radicals $\pi^{\frac{1}{n}}$, such that $\left(\pi^{\frac{1}{mn}}\right)^n = \pi^{\frac{1}{m}}$ for all $m,\ n$). Always considering $i_{\mathfrak{v}}$ as an inclusion of $K^c \subseteq K_{\mathfrak{v}}^c$, for each n, we have in $K_{\mathfrak{v}}^c$ a distinguished primitive n-th root of unity ζ_n $\left(\text{which is } i_{\mathfrak{v}}\left(e^{\frac{2\pi i}{n}}\right)\right)$. From this we obtain that $\Omega_{\mathfrak{v}}^t/\Omega_{\mathfrak{v}}^{nr}$ is a procyclic group generated by σ $(= \sigma_{\mathfrak{v}})$, where

$$\sigma(\pi^{\frac{1}{n}}) = \zeta_n \pi^{\frac{1}{n}} \text{ for } \ (n,\, p) = 1.$$

Now lifting ϕ from $\Omega_{\mathfrak{v}}^{nr}$ to $\Omega_{\mathfrak{v}}^t$, fixing all the different $\pi^{\frac{1}{n}}$ for $(n, p) = 1$, we have that $\Omega_{\mathfrak{v}}^t$ is generated by σ and ϕ; with the identity $\phi\sigma\phi^{-1} = \sigma^q$. This last identity easily follows, looking at the value of σ and ϕ on the various $\pi^{\frac{1}{n}}$ and ζ_n for $(n, p) = 1$.
If we pass to the abelianization $\Omega_{\mathfrak{v}}^{t\ ab}$ $\left(= \Omega_{\mathfrak{v}}^t/[\Omega_{\mathfrak{v}}^t, \Omega_{\mathfrak{v}}^t]\right)$, we have, from the last equality, that σ^{q-1} is the commutator of σ and ϕ and so $\Omega_{\mathfrak{v}}^{t\ ab}$ is the direct product of the cyclic group of order $(q-1)$ generated by $\overline{\sigma}$ with the procyclic group generated by $\overline{\phi}$; where $\overline{\sigma}$ and $\overline{\phi}$ are the images of σ and ϕ in the abelianization. This is the group of interest for us since we are considering Γ abelian and so $\text{Hom}(\Omega_{\mathfrak{v}}^t, \Gamma) = \text{Hom}(\Omega_{\mathfrak{v}}^{t\ ab}, \Gamma)$.

Now we can proceed in our investigation of the tame local resolvends' decomposition. Using the map evaluation at σ, we have

$$\begin{array}{ccc} \text{Hom}(\Omega_{\mathfrak{v}}^t, \Gamma) & \longrightarrow & \Gamma \\ h & \longrightarrow & h(\sigma) \ , \end{array}$$

whose Kernel is, thanks to the previous consideration, $\text{Hom}(\Omega_{\mathfrak{v}}^{nr}, \Gamma)$.
Thanks to the fact that we are considering the abelianization, we have that σ is of order $(q-1)$ and so $h(\sigma) \in \Gamma_{(q-1)}$, the subgroup of Γ of elements of order dividing $q-1$. Hence we have

$$\mathcal{H}^t(K_{\mathfrak{v}}\Gamma)/\mathcal{H}^{nr}(K_{\mathfrak{v}}\Gamma) \cong \text{Hom}(\Omega_{\mathfrak{v}}^t, \Gamma)/\text{Hom}(\Omega_{\mathfrak{v}}^{nr}, \Gamma) \cong \Gamma_{(q-1)},$$

where the first isomorphism is canonical, arising from the surjection $\mathcal{H}(K_{\mathfrak{v}}\Gamma) \longrightarrow \text{Hom}(\Omega_{\mathfrak{v}}, \Gamma)$; instead the second one depends on the distinguished generator σ which depends on $i_{\mathfrak{v}}$.

The decomposition Theorem that we will prove, we shall give even a section of the map $\mathcal{H}^t(K_{\mathfrak{v}}\Gamma) \longrightarrow \Gamma_{(q-1)}$; depending on the distinguished prime elements π of $O_{\mathfrak{v}}$. The section is the following: for each $\gamma \in \Gamma_{(q-1)}$, we define $f_{\mathfrak{v},\gamma} \in (K_{\mathfrak{v}}\Lambda)^{\times} = \text{Hom}_{\Omega_{\mathfrak{v}}}\left(\mathbb{Z}\Gamma\,(-1)\,, (K_{\mathfrak{v}}^c)^{\times}\right)$ in the following way

$$f_{\mathfrak{v},\gamma}(\tau) = \begin{cases} \pi_{\mathfrak{v}} & \text{if } \tau = \gamma \neq 1, \\ 1 & \text{otherwise} \end{cases} \quad \text{for any } \tau \in \Gamma.$$

To check the $\Omega_{\mathfrak{v}}$-invariance of $f_{\mathfrak{v},\gamma}$ is enough to notice that $K_{\mathfrak{v}}$ contains the $(q-1)$-roots of unity so that any element of order dividing $(q-1)$ is fixed by $\Omega_{\mathfrak{v}}$ as is $\pi_{\mathfrak{v}}$, the prime element. Recalling that

$$\Theta^t : (K_{\mathfrak{v}}\Lambda)^{\times} = \mathrm{Hom}_{\Omega_{\mathfrak{v}}}\left(\mathbb{Z}\Gamma\,(-1)\,, (K_{\mathfrak{v}}^c)^{\times}\right) \longrightarrow \mathcal{H}(K_{\mathfrak{v}}\Gamma),$$

since $f_{\mathfrak{v},\gamma} \in (K_{\mathfrak{v}}\Lambda)^{\times}$, then $\Theta^t(f_{\mathfrak{v},\gamma}) \in \mathcal{H}(K_{\mathfrak{v}}\Gamma)$. The map $\gamma \longrightarrow \Theta^t(f_{\mathfrak{v},\gamma})$ will give us the desired section.

Lemma 4.2.1. *Given $f_{\mathfrak{v},\gamma} \in (K_{\mathfrak{v}}\Lambda)^{\times}$ defined as above, for any $\alpha \in A_{\widehat{\Gamma}}$, we have*

$$\left(\Theta^t\left(f_{\mathfrak{v},\gamma}\right)\right)(\alpha) = \pi^{\langle\alpha,\gamma\rangle}.$$

Proof. It is just an easy computation:

$$\left(\Theta^t\left(f_{\gamma}\right)\right)(\alpha) = f_{\gamma}\left(\Theta\left(\alpha\right)\right) = f_{\gamma}\left(\sum_{\tau\in\Gamma}\langle\alpha,\tau\rangle\tau\right) = \prod_{\tau\in\Gamma} f_{\gamma}(\tau)^{\langle\alpha,\tau\rangle} = \pi^{\langle\alpha,\gamma\rangle},$$

where in the last equality we used the definition of $f_{\gamma}(\tau)$. □

Proposition 4.2.1.1. *Let $\gamma \in \Gamma_{(q-1)}$ with order e and let $h_{\mathfrak{v}} \in$ Hom$(\Omega_{\mathfrak{v}}^t, \Gamma)$ be defined by $h_{\mathfrak{v}}(\sigma_{\mathfrak{v}}) = \gamma$, $h_{\mathfrak{v}}(\phi_{\mathfrak{v}}) = 1$. Then $K_{\mathfrak{v}}^{h_{\mathfrak{v}}} = K_{\mathfrak{v}}(\pi^{\frac{1}{e}})$ and $\Theta^t(f_{\mathfrak{v},\gamma}) = \mathcal{R}_{\Gamma}(b_{\mathfrak{v}})$ where $b_{\mathfrak{v}}$ generates a normal integral basis of $(O_{\mathfrak{v}})_{h_{\mathfrak{v}}}/O_{\mathfrak{v}}$. In particular, $\Theta^t(f_{\mathfrak{v},\gamma}) \in \mathcal{H}^t(K_{\mathfrak{v}}\Gamma)$ and $\Theta^t(f_{\mathfrak{v},\gamma}) \longrightarrow \gamma$ under the map $\mathcal{H}^t(K_{\mathfrak{v}}\Gamma) \longrightarrow \Gamma_{(q-1)}$.*

Proof. In the proof we'll always refer to the local situation even if not explicitly, so we will write h, K, Ω^t, f_{γ} to indicate $h_{\mathfrak{v}}$, $K_{\mathfrak{v}}$, $\Omega_{\mathfrak{v}}^t$, $f_{\mathfrak{v},\gamma}$ etc..

The case $\gamma = 1$ is easy, indeed in this case $h = 1$ and so $K^h = K$ and $O_h(= \mathrm{Map}(\Gamma, O))$ has a trivial normal integral basis generator b where $b(\tau) = 0$ if $\tau \neq 1$ and $b(1) = 1$. But then $r_{\Gamma}(b) = 1$ like $\Theta^t(f_{\gamma})$, since $f_{\gamma} = 1$.

Now we analyze the case with γ of order $e > 1$. First of all, $\ker(h)$ is generated by σ^e and ϕ thanks to their definition. So we can see that $K^h = K(\pi^{\frac{1}{e}})$ indeed $\pi^{\frac{1}{e}}$ is fixed by both the generators and if we look at the order we have

$$[\Omega^t : \ker(h)] = e = [K(\pi^{\frac{1}{e}}), K].$$

Moreover we easily find a normal integral basis generator for O^h/O, which is the element

$$\beta = \frac{1}{e}\sum_{r=0}^{e-1}\pi^{\frac{r}{e}} \in O^h,$$

since $(p, e) = 1$. To see that it's a normal integral basis generator we compute $\sigma^i(\beta)$ for $i = 0, ..., e-1$:

$$\sigma^i(\beta) = \frac{1}{e}\sum_{r=0}^{e-1}\zeta_e^{ri}\pi^{\frac{r}{e}},$$

and we have
$$\sum_{i=0}^{e-1}\sigma^i(\beta)\zeta_e^{-ki}=\frac{1}{e}\sum_{r=0}^{e-1}\pi^{\frac{r}{e}}\sum_{i=0}^{e-1}\zeta_e^{(r-k)i}=\pi^{\frac{k}{e}}\text{ for }k=0,...,e-1;$$

where in the last equality we used orthogonality of roots of unity. But $\zeta_e\in O$, since e divides $(q-1)$ and the $\pi^{\frac{k}{e}}$'s form an integral basis since O^h/O is totally ramified. Hence, it's easy to see that the element $b\in O_h$ defined by

$$b(t)=\begin{cases}\tau(\beta) & \text{if } t=h(\tau),\ \tau\in\Omega^t\\ 0 & \text{if } t\notin h(\Omega^t)\end{cases}$$

generates a normal integral basis of O_h/O. Moreover, since $h(\Omega^t)=\langle\gamma\rangle$,

$$r_\Gamma(b)=\sum_{i=0}^{e-1}b(\gamma^i)\gamma^{-i}=\sum_{i=0}^{e-1}\sigma^i(\beta)\gamma^{-i},$$

just from definition. If we take $\chi\in\widehat{\Gamma}$, from the order of γ, it follows that $\langle\chi,\gamma\rangle=\frac{k}{e}$, $0\leq k<e$. So we have $\chi(\gamma)=\zeta_e^k$ and

$$r_\Gamma(b)(\chi)=\sum_{i=0}^{e-1}\sigma^i(\beta)\zeta_e^{-ki}=\pi^{\frac{k}{e}}=\pi^{\langle\chi,\gamma\rangle},$$

which says that for any $\alpha\in A_{\widehat{\Gamma}}$, $\mathcal{R}_\Gamma(b)(\alpha)=\pi^{\langle\alpha,\gamma\rangle}$. Thus, using Lemma 4.2.1, it follows that $\mathcal{R}_\Gamma(b)=\Theta^t(f_\gamma)$ (since $\Theta^t(f_\gamma)\in\text{Hom}\left(A_{\widehat{\Gamma}},(K^c)^\times\right)$ and so it's just defined from its values on $A_{\widehat{\Gamma}}$) . The two last remarks of the Proposition are now easy because the connecting homomorphism $\mathcal{H}(K\Gamma)\longrightarrow\text{Hom}(\Omega,\Gamma)$ sends $\mathcal{R}_\Gamma(b)\longrightarrow h\in\text{Hom}(\Omega^t,\Gamma)$ and because $h(\sigma)=\gamma\in\Gamma_{(q-1)}$. (We underline that f_γ and $\mathcal{R}_\Gamma(b)$ depend only on the choice of π, whereas $r_\Gamma(b)$ depends also on the choice of the radicals $\pi^{\frac{1}{n}}$.) □

We can finally enunciate the Theorem which gives us the desired Decomposition of tame local resolvends.
Now any tame extension of $K_\mathfrak{v}$ with ramification index e is contained in the composite of $K_\mathfrak{v}(\pi^{\frac{1}{e}})$ with an unramified extension. The decomposition in the following Theorem is a reflection of this fact.

Theorem 4.2.2. *Let $h_\mathfrak{v}\in$ Hom$(\Omega^t_\mathfrak{v},\Gamma)$. If $a_\mathfrak{v}$ is a N.I.B. generator of $(O_\mathfrak{v})_{h_\mathfrak{v}}/O_\mathfrak{v}$, then*

$$\mathcal{R}_\Gamma(a_\mathfrak{v})=\Theta^t(f_{\mathfrak{v},\gamma})u_\mathfrak{v}$$

where $h_\mathfrak{v}(\sigma_\mathfrak{v})=\gamma\in\Gamma_{(q-1)}$ and $u_\mathfrak{v}\in\mathcal{H}(O_\mathfrak{v}\Gamma)$. Conversely, let $\gamma\in\Gamma_{(q-1)}$ and $u_\mathfrak{v}\in\mathcal{H}(O_\mathfrak{v}\Gamma)$, and let $h_\mathfrak{v}$ be the image of $\Theta^t(f_{\mathfrak{v},\gamma})u_\mathfrak{v}$ under the connecting homomorphism $\mathcal{H}^t(K_\mathfrak{v}\Gamma)\longrightarrow$ Hom$(\Omega^t_\mathfrak{v},\Gamma)$. Then $h_\mathfrak{v}(\sigma_\mathfrak{v})=\gamma$ and $(O_\mathfrak{v})_{h_\mathfrak{v}}/O_\mathfrak{v}$ has a N.I.B. generator $a_\mathfrak{v}$ for which $\mathcal{R}_\Gamma(a_\mathfrak{v})=\Theta^t(f_{\mathfrak{v},\gamma})u_\mathfrak{v}$.

Proof. Again in the proof we shall omit the subscript $\mathfrak{v}$. Let $h\in\text{Hom}(\Omega^t,\Gamma)$, since Γ is abelian, we can decompose h uniquely as a product $h=h_1h_2$ where h_1, $h_2\in\text{Hom}(\Omega^t,\Gamma)$ with $h_1(\phi)=$

$1 = h_2(\sigma)$ so that $h(\sigma) = h_1(\sigma)$ and $h(\phi) = h_2(\phi)$. Particularly we have that h_2 is unramified. By Noether's Criterion, both in the tame and in the unramified case, we can find a_1 and a_2 N.I.B. generators for O_{h_1} and O_{h_2}, respectively, over O.
First of all we shall prove that

$$r_\Gamma(a_1)r_\Gamma(a_2) = r_\Gamma(a') \tag{4.2.1}$$

where a' is a N.I.B. generator for O_h/O.

We observe that under the isomorphism $\mathrm{Gal}(K^h/K) \cong h(\Omega)$, the inertia group is isomorphic to $\langle h(\sigma)\rangle$, with order e; then

$$\delta(O^h/O) = N_{K^h/K}(\mathcal{D}) = (\mathfrak{p}^{e-1})^f = \mathfrak{p}^{\frac{(e-1)|h(\Omega)|}{e}},$$

where in the first equality we used the usual formula linking the discriminant and the different, in the second and in the last one we used the tame property and the usual property of norm in the ramified case. Similar formulas exist for h_1 and h_2, so from (2.4.3) it follows that

$$\begin{gathered}\delta(O_h/O) = \mathfrak{p}^{\frac{(e-1)|\Gamma|}{e}} = \delta(O_{h_1}/O),\\ \delta(O_{h_2}/O) = (1) \quad \text{(because unramified).}\end{gathered} \tag{4.2.2}$$

Let $a' = m_*(a_1 \otimes a_2)$, then clearly $a' \in O_h$ and by formula on resolvends we have $r_\Gamma(a') = r_\Gamma(a_1)\, r_\Gamma(a_2)$, so it only remains to show that it's a N.I.B. generator. Clearly

$$r_\Gamma(a')r_\Gamma(a')^{[-1]} = \left(r_\Gamma\,(a_1)\, r_\Gamma\,(a_1)^{[-1]}\right)\left(r_\Gamma\,(a_2)\, r_\Gamma\,(a_2)^{[-1]}\right).$$

Hence by (2.5.0.1), first of all we have $O\Gamma = O\Gamma\, r_\Gamma(a_2)\, r_\Gamma(a_2)^{[-1]}$ since h_2 is unramified, and thus

$$\begin{aligned}[(O\Gamma.a')^* : O\Gamma.a']_O &= [O\Gamma : O\Gamma r_\Gamma(a_1) r_\Gamma(a_1)^{[-1]}]_O\\ &= \delta(O_{h_1}/O) = \delta(O_h/O).\end{aligned}$$

Since $(O\Gamma.a')^* \supseteq O_h^* \supseteq O_h \supseteq O\Gamma.a'$, it follows that $O\Gamma.a' = O_h$, as we wanted to prove.

($\Longrightarrow$) Now, let a be any N.I.B. generator of O_h/O, and let $\gamma = h(\sigma)$. Then since $h_1(\sigma) = \gamma$ and $h_1(\phi) = 1$, by Prop. 4.2.1.1 we may choose a_1 such that $\mathcal{R}_\Gamma(a_1) = \Theta^t(f_\gamma)$. Moreover, $a = w.a'$ where $w \in O\Gamma^\times$, so

$$r_\Gamma(a) = w\, r_\Gamma(a_1)\, r_\Gamma(a_2) = r_\Gamma(a_1)r_\Gamma(w.a_2),$$

so

$$\mathcal{R}_\Gamma(a) = \mathcal{R}_\Gamma(a_1)\,\mathcal{R}_\Gamma(w \cdot a_2) = \Theta^t(f_\gamma)\, u$$

where $u = \mathcal{R}_\Gamma(w.a_2) \in \mathcal{H}(O\Gamma)$, proving the first assertion of the Theorem.

($\Longleftarrow$) Conversely, let $\gamma \in \Gamma_{(q-1)}$ and $u \in \mathcal{H}(O\Gamma)$. By Prop. 4.2.1.1, $\Theta^t(f_\gamma) = \mathcal{R}_\Gamma(a_1)$ where $O\Gamma.a_1 = O_{h_1}$ with h_1 defined by $h_1(\sigma) = \gamma$, $h_1(\phi) = 1$. Of course h_1 is the image of $r_\Gamma(a_1)$ under $\mathcal{H}^t(K\Gamma) \longrightarrow \mathrm{Hom}(\Omega^t, \Gamma)$. Moreover by (2.6.3), $u = \mathcal{R}_\Gamma(a_2)$ where $O\Gamma.a_2 = O_{h_2}$ for some $h_2 \in \mathrm{Hom}(\Omega^{nr}, \Gamma)$. Of course then h_2 is the image in $\mathrm{Hom}(\Omega^t, \Gamma)$ of $\mathcal{R}_\Gamma(a_2)$ and $h_2(\sigma) = 1$.

Hence, by multiplicativity, if h is the image under $\mathcal{H}^t(K\Gamma) \longrightarrow \mathrm{Hom}(\Omega^t,\Gamma)$ of $\Theta^t(f_\gamma)\,u$, then $h = h_1\,h_2$. Since $h_1(\phi) = 1 = h_2(\sigma)$ we have $h(\sigma) = h_1(\sigma) = \gamma$ and we may apply (4.2.1) obtaining $\Theta^t(f_\gamma)u = \mathcal{R}_\Gamma(a_1)\mathcal{R}_\Gamma(a_2) = \mathcal{R}_\Gamma(a)$ where a generates a N.I.B. of O_h/O. □

Let $F_\mathfrak{v}$ $\left(\subseteq (K_\mathfrak{v}\Lambda)^\times\right)$ be the set of all $f_{\mathfrak{v},\gamma}$ for $\gamma \in \Gamma_{(q-1)}$. Since the order of the group of those roots of unity in $K_\mathfrak{v}$ with order prime to $\mathfrak{v}$ is $(q-1)$, we have

$$\gamma \in \Gamma_{(q-1)} \Longleftrightarrow \mathfrak{v}(|\gamma|) = 0 \text{ and } K_\mathfrak{v}(\gamma) = K_\mathfrak{v},$$

so we obtain

$$F_\mathfrak{v} = \{f_{\mathfrak{v},\gamma} | \mathfrak{v}(|\gamma|) = 0, K_\mathfrak{v}(\gamma) = K_\mathfrak{v}\},$$

where $|\gamma|$ denotes the order of γ (for infinite $\mathfrak{v}$, we put $F_\mathfrak{v} = \{f_{\mathfrak{v},1}\} = \{1\}$).

4.3 Characterization of realizable classes

Following the analogous section in the previous chapter, now we will be able to give the desired characterization of the set of realizable classes, that is to say the set $R(O\Gamma)$ of classes in $Cl(O\Gamma)$ of form (O_h) for some tame Γ-extension K_h/K. For the basic notions used in the section, we always refer to A.4.

We shall use the previous section's decomposition of the tame local resolvends to decompose a representative $c \in J(K\Gamma)$ of such a class in the form

$$rag(c) = \lambda\left(\mathcal{R}_\Gamma(b)\right)\Theta^t(f)\,u\,,$$

where f and u are ideles with components $f_\mathfrak{v}$ and $u_\mathfrak{v}$ respectively, λ is a principal idele map and $\mathcal{R}_\Gamma(b) \in \mathcal{H}(K\Gamma)$.
The characterization will say that if a class in $Cl(O\Gamma)$ has a representative c for which $rag(c)$ has a decomposition like the previous one with f an arbitrary idele in $K\Lambda$, then the class is realizable.

We easily link this situation to the unramified one looking at (3.2.1), we remark here that now in our decomposition we need a now component $\Theta^t(f)$, given by the Stickelberger map.

4.3.1 Definition of the ideles involved in the tame case

To work in the tame case, we have to add some new ideles to the set of ideles defined in the subsection 3.2.1.

Let $J(K\Lambda)$ be the restricted direct product of the $(K_\mathfrak{v}\Lambda)^\times$ with respect to the subgroups $\Lambda_\mathfrak{v}^\times$, for all primes $\mathfrak{v}$ (actually the infinite prime has no role and could be omitted from now on).
Thanks to this, we can define, componentwise, the following map:

$$\Theta^t : J(K\Lambda) \longrightarrow \mathcal{H}\left(\mathbb{A}\left(K\Gamma\right)\right), \tag{4.3.1}$$

which is well defined, since we have

$$\Lambda_{\mathfrak{v}}^{\times} = \mathrm{Hom}_{\Omega_{\mathfrak{v}}}\left(\mathbb{Z}\Gamma\,(-1)\,,(O_{\mathfrak{v}}^{c})^{\times}\right)$$

which, thanks to Theorem 2.6.2, says that whenever $\mathfrak{v}(|\Gamma|) = 0$ (so except a finite number of cases) we get

$$\Theta^{t}(\Lambda_{\mathfrak{v}}^{\times}) \subseteq \mathrm{Hom}_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}},\,(O_{\mathfrak{v}}^{c})^{\times}\right).$$

We also define the unit idele group $U(\Lambda) = \prod_{\mathfrak{v}}(\Lambda_{\mathfrak{v}})^{\times}$ and we can remark that in general we have not $\Theta^{t}\left(U(\Lambda)\right) \subseteq \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)$.

Moreover we define the useful principal idele map

$$\lambda : K\Lambda^{\times} \longrightarrow J(K\Lambda), \tag{4.3.2}$$

which arises from the componentwise inclusions $K\Lambda^{\times} \subseteq (K_{\mathfrak{v}}\Lambda)^{\times}$ given by the inclusions $i_{\mathfrak{v}} : K^{c} \longrightarrow K_{\mathfrak{v}}^{c}$ (it's not difficult to prove that it's well defined).

From (4.1.11) it follows that the following diagram commutes:

$$\begin{tikzcd} K\Lambda^{\times} \arrow[r, "\Theta^{t}"] \arrow[d, "\lambda"] & \mathcal{H}(K\Gamma) \arrow[d, "\lambda"] \\ J(K\Lambda) \arrow[r, "\Theta^{t}"] & \mathcal{H}\left(\mathbb{A}\left(K\Gamma\right)\right) \end{tikzcd} \quad . \tag{4.3.3}$$

4.3.2 Decomposition of tame global resolvends

We define $F \subseteq J(K\Lambda)$ in the following way

$$f \in F \Longleftrightarrow f \in J(K\Lambda) \ \text{ and } \ f_{\mathfrak{v}} \in F_{\mathfrak{v}} \ \text{ for all } \ \mathfrak{v}. \tag{4.3.4}$$

Now given $f_{\mathfrak{v}} \in F_{\mathfrak{v}}$, we have $f_{\mathfrak{v}} \neq 1 \Longrightarrow f_{\mathfrak{v}} \notin \Lambda_{\mathfrak{v}}^{\times}$, so it follows that if $f \in F$, then $f_{\mathfrak{v}} = 1$ for almost all $\mathfrak{v}$. We will consider the elements of $F_{\mathfrak{v}}$ themselves as ideles embedded in F via the map $(K_{\mathfrak{v}}\Lambda)^{\times} \longrightarrow J(K\Lambda)$.
The nontrivial elements of $F_{\mathfrak{v}}$ will be called the *prime F-elements* lying over $\mathfrak{v}$. Thus from the previous remark, the elements of F are finite products of prime F-elements lying over distinct primes $\mathfrak{v}$ of K. From Proposition 4.2.1.1 it follows that

$$\Theta^{t}(f) \in \mathcal{H}^{t}\left(\mathbb{A}\left(K\Gamma\right)\right) \quad \text{for all} \quad f \in F. \tag{4.3.5}$$

We can state now the tame analogous of Theorem 3.2.3 which gives the useful decomposition of a tame global resolvend; for the proof we use some facts present in A.4. We underline once again that also in the global situation, a new component, depending on the Stickelberger map, arises in the decomposition of tame resolvends and it distinguishes the tame case from the unramified one.

Theorem 4.3.3. *Let $h \in$ Hom(Ω, Γ) and suppose $K\Gamma.b = K_h$ (b is a normal basis generator). Then h is tame if and only if there are elements $c \in J(K\Gamma)$, $f \in F$, and $u \in \mathcal{H}(\mathbb{A}(O\Gamma))$ such that*

$$\lambda(\mathcal{R}_\Gamma(b)) = (rag(c))^{-1}\,\Theta^t(f)u.$$

Moreover, if so, then $j(c) = (O_h) \in Cl(O\Gamma)$ and f is unique.
In particular, $f = (f_\mathfrak{v})_\mathfrak{v}$, where for each finite $\mathfrak{v}$, $f_\mathfrak{v} = f_{\mathfrak{v},\gamma}$, with $\gamma = h_\mathfrak{v}(\sigma_\mathfrak{v})$; so $f_\mathfrak{v} \neq 1$ if and only if $h_\mathfrak{v}$ is ramified and $f = 1$ if and only if h is unramified.

Proof. ($\Longrightarrow$) We suppose that h is tame. Exactly as in (A.4.0.1) $b \in K_h$ is a normal basis generator and for all $\mathfrak{v}$ we have $a_\mathfrak{v} \in (O_\mathfrak{v})_{h_\mathfrak{v}}$, such that

$$(O_\mathfrak{v})_{h_\mathfrak{v}} = O_\mathfrak{v}\Gamma.a_\mathfrak{v},$$

and $c = (c_\mathfrak{v})_\mathfrak{v} \in J(K\Gamma)$ such that

$$a_\mathfrak{v} = c_\mathfrak{v}.b;$$

so by (A.4.3), $\mathcal{R}_\Gamma(a_\mathfrak{v}) = (rag(c_\mathfrak{v}))\mathcal{R}_\Gamma(b)$.
Now we can use the decomposition of tame local resolvends given in Theorem 4.2.2 which tells us that

$$\mathcal{R}_\Gamma(a_\mathfrak{v}) = \Theta^t(f_\mathfrak{v})u_\mathfrak{v}$$

where $f_\mathfrak{v} = f_{\mathfrak{v},\gamma} \in F_\mathfrak{v}$ with $h_\mathfrak{v}(\sigma_\mathfrak{v}) = \gamma \in \Gamma_{(q-1)}$ and $u_\mathfrak{v} \in \mathcal{H}(O_\mathfrak{v}\Gamma)$. In particular if $\mathfrak{v}$ is unramified, so for all but finitely many primes, we have $f_\mathfrak{v} = 1$; which tell us that $f = (f_\mathfrak{v})_\mathfrak{v} \in F$. Moreover $u = (u_\mathfrak{v})_\mathfrak{v} \in \mathcal{H}(\mathbb{A}(O\Gamma))$ and we have

$$\Theta^t(f)\,u = (rag(c))\,\lambda(\mathcal{R}_\Gamma(b)),$$

as we wanted to show.

($\Longleftarrow$) Conversely, suppose

$$\lambda(\mathcal{R}_\Gamma(b)) = (rag(c))^{-1}\,\Theta^t(f)\,u,$$

where $c \in J(K\Gamma)$, $f \in F$, and $u \in \mathcal{H}(\mathbb{A}(O\Gamma))$. By (4.3.5) we have $\Theta^t(f) \in \mathcal{H}^t(\mathbb{A}(K\Gamma))$, while by (2.6.4) we have $(rag(c))^{-1} \in \mathcal{H}^{nr}(\mathbb{A}(K\Gamma)) \subseteq \mathcal{H}^t(\mathbb{A}(K\Gamma))$ and $u \in \mathcal{H}(\mathbb{A}(O\Gamma)) \subseteq \mathcal{H}^t(\mathbb{A}(K\Gamma))$. Thus we obtain

$$\lambda(\mathcal{R}_\Gamma(b)) \in \lambda(\mathcal{H}(K\Gamma)) \cap \mathcal{H}^t(\mathbb{A}(K\Gamma)) = \lambda\left(\mathcal{H}^t(K\Gamma)\right),$$

which tells that h is tame.

Moreover, locally we have for any $\mathfrak{v}$

$$\mathcal{R}_\Gamma(b) = (rag(c_\mathfrak{v}))^{-1}\,\Theta^t(f_\mathfrak{v})u_\mathfrak{v} \in \mathcal{H}^t(K_\mathfrak{v}\Gamma).$$

Thus, by (2.2.2), $\mathcal{R}_\Gamma(b)$ and $\Theta^t(f_\mathfrak{v})u_\mathfrak{v}$ have the same image $h_\mathfrak{v}$ in Hom$(\Omega^t_\mathfrak{v}, \Gamma)$, and so by Theorem 4.2.2, $\Theta^t(f_\mathfrak{v})\,u_\mathfrak{v} = \mathcal{R}_\Gamma(a_\mathfrak{v})$ where $O_\mathfrak{v}\Gamma.a_\mathfrak{v} = (O_\mathfrak{v})_{h_\mathfrak{v}}$ and $f_\mathfrak{v} = f_{\mathfrak{v},\gamma}$ with $\gamma = h_\mathfrak{v}(\sigma_\mathfrak{v})$. Hence f is uniquely determined by h. Moreover, recalling the remark made after (A.4.3), we have $j(c) = (O_h)$ in $Cl(O\Gamma)$. □

4.3.4 Towards the main Theorem: The Modified Ray Class Group

Let $\mathfrak{m}$ be an integral ideal of O and recall that for each of these ideals we have defined $U_{\mathfrak{m}}(O_{\mathfrak{v}}^c) = (1 + \mathfrak{m}O_{\mathfrak{v}}^c) \cap (O_{\mathfrak{v}}^c)^{\times}$.
For each $\mathfrak{v}$ we denote by $U_{\mathfrak{m}}^{'}(\Lambda_{\mathfrak{v}})$ the subgroup of $g_{\mathfrak{v}} \in (K_{\mathfrak{v}}\Lambda)^{\times} = \mathrm{Map}_{\Omega_{\mathfrak{v}}}\left(\Gamma(-1), (K_{\mathfrak{v}}^c)^{\times}\right)$ satisfying the following condition

$$g_{\mathfrak{v}} \in U_{\mathfrak{m}}^{'}(\Lambda_{\mathfrak{v}}) \Longleftrightarrow g_{\mathfrak{v}}(\gamma) \in U_{\mathfrak{m}}(O_{\mathfrak{v}}^c) \ \text{ for } \ \gamma \in \Gamma,\ \gamma \neq 1. \tag{4.3.6}$$

Let the value on 1 be arbitrary. We define the idelic analogues

$$\mathbb{U}_{\mathfrak{m}}^{'}(\Lambda) = \left(\prod_{\mathfrak{v}} U_{\mathfrak{m}}^{'}(\Lambda_{\mathfrak{v}})\right) \cap J(K\Lambda).$$

Proposition 4.3.4.1. *If* $\mathfrak{m}$ *is divisible by* $|\Gamma|$ *and* m^2 *(where* m *is the exponent of* Γ*), then*

$$\Theta^t\left(\mathbb{U}_{\mathfrak{m}}^{'}(\Lambda)\right) \subseteq \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right).$$

Proof. With these hypothesis, by (2.6.2), we have $\mathrm{Hom}_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}}, U_{\mathfrak{m}}\left(O_{\mathfrak{v}}^c\right)\right) \subseteq \mathcal{H}(O_{\mathfrak{v}}\Gamma)$, so it suffices to show that for each $\mathfrak{v}$ we have

$$\Theta^t\left(U_{\mathfrak{m}}^{'}\left(\Lambda_{\mathfrak{v}}\right)\right) \subseteq \mathrm{Hom}_{\Omega_{\mathfrak{v}}}\left(A_{\widehat{\Gamma}}, U_{\mathfrak{m}}\left(O_{\mathfrak{v}}^c\right)\right).$$

Now everything is easy because, given $g_{\mathfrak{v}} \in U_{\mathfrak{m}}^{'}(\Lambda_{\mathfrak{v}})$ and $\alpha \in A_{\widehat{\Gamma}}$, we have

$$\left(\Theta^t\left(g_{\mathfrak{v}}\right)\right)(\alpha) = g_{\mathfrak{v}}\left(\Theta\left(\alpha\right)\right) = \prod_{\gamma \in \Gamma} g_{\mathfrak{v}}(\gamma)^{\langle \alpha, \gamma \rangle}.$$

Since $\langle \alpha, 1 \rangle = 0$ the value in 1 gives no complications, so the right side does not depend on $g_{\mathfrak{v}}(1)$ and it lies in $U_{\mathfrak{m}}(O_{\mathfrak{v}}^c)$. □

We can now define the *modified ray class group* mod $\mathfrak{m}$ of Λ, in the following way

$$Cl_{\mathfrak{m}}^{'}(\Lambda) = J(K\Lambda)/\lambda(K\Lambda^{\times})\mathbb{U}_{\mathfrak{m}}^{'}(\Lambda),$$

where the elements will be called *modified ray classes* mod $\mathfrak{m}$ of Λ.

We shall give now a characterization of the modified ray class in terms of the field components of $K\Lambda$.
Following (4.1.9) we have that the algebra $K\Lambda$ can be decompose in its field components in the following way

$$K\Lambda = \prod_{H} K(H),$$

where $H \in \Omega \setminus \Gamma(-1)$ are the Ω-orbits and $K(H) = \mathrm{Map}_{\Omega}(H, K^c)$. The projection map $K\Lambda \longrightarrow K(H)$ is given by restriction of functions from $\Gamma(-1)$ to H and thanks to the evaluation at $t \in H$ we have the isomorphism

$$K(H) = \mathrm{Map}_{\Omega}(H, K^c) \cong (K^c)^{\Omega_{K(t)}} = K(t);$$

with $\Omega_{K(t)}$ stabilizer of t in Ω. The isomorphism depends on t and making it running over H, the isomorphism runs over all K-isomorphisms $K(H) \longrightarrow K(t)$.

Passing to the ring of integers, we can define

$$O(H) = \mathrm{Map}_{\Omega}(H, O^c).$$

For each prime $\mathfrak{v}$ we consider the completions $K(H)_{\mathfrak{v}} = K_{\mathfrak{v}} \otimes_K K(H)$ and $O(H)_{\mathfrak{v}} = O_{\mathfrak{v}} \otimes_O O(H)$. In order to give a decomposition of the modified ray class group, we have to decompose each component on the right side of its definition. We start proving that

$$J(K\Lambda) = \prod_H J\left(K\left(H\right)\right),$$

where as usual $J\left(K\left(H\right)\right)$ is the idele group of $K(H)$ (the restricted direct product of the $K(H)_{\mathfrak{v}}^{\times}$ with respect to the $O(H)_{\mathfrak{v}}^{\times}$.)
First of all, localizing, we have

$$K_{\mathfrak{v}}\Lambda = \prod_H K(H)_{\mathfrak{v}}$$

and using coinduction and Section 1.3, we obtain

$$\begin{aligned} K(H)_{\mathfrak{v}} &= K_{\mathfrak{v}} \otimes_K K(H) \\ &= \mathrm{Map}_{\Omega}(H, K_{\mathfrak{v}} \otimes_K K^c) \\ &= \mathrm{Map}_{\Omega}\left(H, \mathrm{Map}_{\Omega_{\mathfrak{v}}}\left(\Omega, K_{\mathfrak{v}}^c\right)\right) \\ &= \mathrm{Map}_{\Omega_{\mathfrak{v}}}(H, K_{\mathfrak{v}}^c), \end{aligned}$$

where again the projection map

$$K_{\mathfrak{v}}\Lambda = \mathrm{Map}_{\Omega_{\mathfrak{v}}}\left(\Gamma\left(-1\right), K_{\mathfrak{v}}^c\right) \longrightarrow K(H)_{\mathfrak{v}} = \mathrm{Map}_{\Omega_{\mathfrak{v}}}(H, K_{\mathfrak{v}}^c),$$

is the restriction of functions from $\Gamma(-1)$ to H.

Remark 4.3.5. *We underline that $K(H)_{\mathfrak{v}}$ is no more a field, but it can be decomposed in field components as done for $K(\Lambda)$, using the set of $\Omega_{\mathfrak{v}}$-orbits $\Omega_{\mathfrak{v}} \setminus H$ which is in bijection with the set of those primes $\mathfrak{w}$ of $K(H)$ lying over $\mathfrak{v}$ of K.*
For $g_{\mathfrak{v}} \in \left(K_{\mathfrak{v}}\Lambda\right)^{\times} = \prod_H K(H)_{\mathfrak{v}}^{\times}$, we write $g_{\mathfrak{v}} = (g_{\mathfrak{v},H})_H$ where $g_{\mathfrak{v},H} \in K(H)_{\mathfrak{v}}^{\times}$.

In the same way, we have

$$\Lambda_{\mathfrak{v}} = \prod_H O(H)_{\mathfrak{v}} \tag{4.3.7}$$

and from the fact that restricted products commute naturally with finite products we have

$$J(K\Lambda) = \prod_H J\left(K\left(H\right)\right).$$

So we denote an element $g \in J(K\Lambda)$ as $g = (g_H)_H$ with any component $g_H \in J(K(H))$ and $J(K(H))$ is naturally embedded in $J(K\Lambda)$.
Moreover,

$$U(\Lambda) = \prod_H U(O(H)) \quad \text{where} \quad U(O(H)) = \prod_{\mathfrak{v}} O(H)_{\mathfrak{v}}^{\times},$$

and passing to the quotient we get

$$J(K\Lambda)/U(\Lambda) = \prod_H J(K(H))/U(O(H)).$$

The factors of the product on the right are identified with the fractional ideals $I(O(H))$ of $K(H)$, thus $J(K\Lambda)/U(\Lambda)$ with the group of *invertible fractional* Λ*-ideals* in $K\Lambda$. For $\mathfrak{a} \in I(\Lambda)$ we write $\mathfrak{a} = (\mathfrak{a}_H)_H \in \prod_H I(O(H))$.

In this context, we consider the image in $I(\Lambda)$ of the prime F-elements. Using the definition of $F_{\mathfrak{v}}$, if $f_{\mathfrak{v},\gamma} \neq 1$ in $F_{\mathfrak{v}}$, then: $\mathfrak{v}$ is finite, $\gamma \neq 1$, $K_{\mathfrak{v}}(\gamma) = K_{\mathfrak{v}}$, $\mathfrak{v}(|\gamma|) = 0$ and $f_{\mathfrak{v},\gamma} \in K(H)_{\mathfrak{v}}^{\times}$, where H is the Ω-orbit of γ, since $f_{\mathfrak{v},\gamma}(\tau) = 1$ for $\tau \notin H$. Since $K_{\mathfrak{v}}(\gamma) = K_{\mathfrak{v}}$, $\mathfrak{v}$ splits completely in $K(\gamma) \cong K(H)$, which means that $\Omega_{\mathfrak{v}}$ fixes γ; so in our notation

$$K(H)_{\mathfrak{v}} = \mathrm{Map}_{\Omega_{\mathfrak{v}}}(H, K_{\mathfrak{v}}^c) = \mathrm{Map}(H, K_{\mathfrak{v}}).$$

The primes of $K(H)$ lying over $\mathfrak{v}$ then correspond naturally to the elements of H. Moreover for $\tau \in H$, $f_{\mathfrak{v},\gamma}(\tau) = 1$ if $\tau \neq \gamma$ and $f_{\mathfrak{v},\gamma}(\gamma) = \pi_{\mathfrak{v}}$, so clearly the image of $f_{\mathfrak{v},\gamma}$ in $I(O(H))$ is the prime ideal corresponding to $\gamma \in H$, giving the following Proposition.

Proposition 4.3.5.1. *The images in $I(\Lambda)$ of the prime F-elements lying over $\mathfrak{v}$ are the invertible prime ideals of Λ arising from the prime ideals of relative degree one over $\mathfrak{v}$ in those components $K(H)/K$ for which $H \neq 1$ and $\mathfrak{v}(|\gamma|) = 0$ for $\gamma \in H$.*

We can now obtain the decomposition we're looking for, indeed by (4.3.6) and (4.3.7) we have

$$U_{\mathfrak{m}}^{'}(\Lambda_{\mathfrak{v}}) = K(1)_{\mathfrak{v}}^{\times} \times \prod_{H \neq 1} U_{\mathfrak{m}}^{'}(O(H)_{\mathfrak{v}})$$

where we define $U_{\mathfrak{m}}^{'}(O(H)_{\mathfrak{v}}) = \mathrm{Map}_{\Omega_{\mathfrak{v}}}(H, U_{\mathfrak{m}}(O_{\mathfrak{v}}^c))$, so making the product over all primes $\mathfrak{v}$ we have

$$\mathbb{U}_{\mathfrak{m}}^{'}(\Lambda) = J(K(1)) \times \prod_{H \neq 1} \mathbb{U}_{\mathfrak{m}}(O(H))$$

where $\mathbb{U}_{\mathfrak{m}}(O(H)) = \prod_{\mathfrak{v}} U_{\mathfrak{m}}^{'}(O(H)_{\mathfrak{v}})$. From the decomposition of $K\Lambda$ we have

$$\lambda(K\Lambda^{\times}) = \prod_H \lambda\left(K(H)^{\times}\right)$$

and hence we obtain the desired decomposition

$$Cl_{\mathfrak{m}}^{'}(\Lambda) \cong \prod_{H \neq 1} Cl_{\mathfrak{m}}(O(H)),$$

where $Cl_{\mathfrak{m}}(O(H))$ is the ray class group mod $\mathfrak{m}$ of the component $K(H)$,

$$Cl_{\mathfrak{m}}(O(H)) = \frac{J(K(H))}{\lambda\left(K(H)^{\times}\right)\mathbb{U}_{\mathfrak{m}}(O(H))}.$$

Thus we can now formulate the following Proposition.

Proposition 4.3.5.2. *Let $g \in \mathbb{J}(K\Lambda)$ and let V be a finite set of primes of K. Then the modified ray class mod $\mathfrak{m}$ of g contains an element $f \in F$, such that $f_{\mathfrak{v}} = 1$ for all $\mathfrak{v} \in V$.*
Moreover f can be chosen so that $f_H \neq 1$ for each $H \neq 1$. In particular each class in $Cl'_{\mathfrak{m}}(\Lambda)$ contains infinitely many elements of F and they can be chosen with support disjoint from any preassigned finite set of primes V.

Proof. Let $g = (g_H)_H$ with $g_H \in J(K(H))$. By the generalized Dirichlet Theorem for primes in arithmetic progression, each ray class mod $\mathfrak{m}$ contains infinitely many prime ideals of relative degree one in $K(H)/K$. By the previous Proposition, if $H \neq 1$ and $\mathfrak{v}(|\gamma|) = 0$ for $\gamma \in H$, then these prime ideals are the images of prime F-elements. So, for each $H \neq 1$, we may choose a prime F-element, called $f_H \neq 1$, in the ray class mod $\mathfrak{m}$ of $K(H)$ represented by g_H in such a way that the f_H lies over distinct primes of K not belonging to V.
Then $g_H f_H^{-1} \in \lambda\left(K(H)^{\times}\right)\mathbb{U}_{\mathfrak{m}}(O(H))$, so letting $f_1 = 1$ we can define $f = (f_H)_H$ and we obtain $f \in F$ and $gf^{-1} \in \lambda(K\Lambda^{\times})\mathbb{U}'_{\mathfrak{m}}(\Lambda)$ as wanted. □

4.3.6 The Realizable classes form a subgroup

We are ready now to reach the analogous result for the tame case of section 3.2.4, in particular we shall describe the shape of the set of realizable classes $R(O\Gamma)$ in $Cl(O\Gamma)$ realized by tame extensions, which is defined as:

$$R(O\Gamma) = \{(O_h) |\, h \in \mathrm{Hom}(\Omega_K^t, \Gamma)\}.$$

Passing to the idelic context, we can also define

$$\mathbb{R}(O\Gamma) = j^{-1}(R(O\Gamma)), \tag{4.3.8}$$

where $j : J(K\Gamma) \longrightarrow Cl(O\Gamma)$ is the usual quotient map.

In the easy case we have $R(\mathbb{Z}\Gamma) = 1$ and so $\mathbb{R}(\mathbb{Z}\Gamma) = \lambda(\mathbb{Q}\Gamma^{\times})U(\mathbb{Z}\Gamma)$.

Here we have the important Theorem corresponding to the unramified result present in Theorem 3.2.5, which gives us the result we are looking for; also in the tame case we have an analogous characterization of the idelic version of the set of realizable classes even if this time we have a component depending on the Stickelberger map.

Theorem 4.3.7 (Tame case)**.** *Let $c \in J(K\Gamma)$. Then*

$$c \in \mathbb{R}(O\Gamma) \iff rag(c) \in \lambda(\mathcal{H}(K\Gamma))\,\mathcal{H}(\mathbb{A}(O\Gamma))\,\Theta^t(J(K\Lambda)).$$

Moreover, if $c \in \mathbb{R}(O\Gamma)$, then there is an $h \in Hom(\Omega^t, \Gamma)$ with $j(c) = (O_h)$ such that

(a) *K_h is a field,*

(b) *the only subfield of K_h unramified over K is K itself,*

(c) *the discriminant $\delta(O_h/O)$ is relatively prime to any preassigned ideal of O.*

Proof. ($\Longrightarrow$) We take $h \in \operatorname{Hom}(\Omega^t, \Gamma)$ and suppose that $(O_h) = j(c)$. By the Normal basis Theorem, we take b such that $K\Gamma.b = K_h$. Then using Theorem 4.3.3, we find $c' \in J(K\Gamma)$, $f \in F$, and $u \in \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)$ with $j(c') = j(c)$ and $\lambda\left(\mathcal{R}_{\Gamma}\left(b\right)\right) = \left(rag\left(c'\right)\right)^{-1}\Theta^t(f)u$.
Then bringing $rag(c')$ to the other side, we obtain $rag(c') \in \lambda\left(\mathcal{H}\left(K\Gamma\right)\right)\mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)\Theta^t\left(J\left(K\Lambda\right)\right)$.
Since $j(c) = j(c')$, we have $c^{-1}c' \in \lambda(K\Gamma^{\times})U(O\Gamma)$, so we deduce that

$$rag(c^{-1}c') \in \lambda\left(\mathcal{H}\left(K\Gamma\right)\right)\mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right),$$

obtaining the first implication.

($\Longleftarrow$) In the general ramified case, let $\mathfrak{m}$ be an ideal of O divisible by $|\Gamma|$ and m^2. By the previous Proposition and the definition of the modified ray class group, $g \equiv f \bmod \lambda(K\Lambda^{\times})\mathbb{U}'_{\mathfrak{m}}(\Lambda)$, for some $f \in F$ with support disjoint from any preassigned finite set of primes and $f_{_H} \neq 1$ for all Ω-orbits $H \neq 1$ of $\Gamma(-1)$. In anyway, by (4.1.10), we have $\Theta^t(K\Lambda^{\times}) \subseteq \mathcal{H}(K\Gamma)$ and, by Proposition 4.3.4.1, $\Theta^t\left(\mathbb{U}'_{\mathfrak{m}}\left(\Lambda\right)\right) \subseteq \mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)$ so $\Theta^t(g) \equiv \Theta^t(f) \bmod \lambda\left(\mathcal{H}\left(K\Gamma\right)\right)\mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)$ and so, changing b, h and u as necessary, we may assume $g = f$. So applying now Theorem 4.3.3, we conclude that h is tame and $j(c) = cl(O_h)$, as we wanted to show.

(c) To prove this part, is enough to observe that h is ramified only at primes $\mathfrak{v}$ for which $f_{\mathfrak{v}} \neq 1$.

(a) Now let consider Σ a proper subgroup of Γ, $\overline{\Gamma} = \Gamma/\Sigma$, and $\overline{h} : \Omega \longrightarrow \overline{\Gamma}$ the composite of h with the quotient map $\Gamma \longrightarrow \overline{\Gamma}$.
We show now that $\overline{h}$ is ramified. From the definition of $\Gamma(-1)$ it follows that if $\gamma \in \Gamma(-1)$ and $\omega \in \Omega$, then γ and γ^{ω} generate the same subgroup of Γ. From the fact that $\overline{\Gamma}$ is not trivial, there is a Ω-orbit H of $\Gamma(-1)$ all elements of which have nontrivial image in $\overline{\Gamma}$. But $f_{_H} \neq 1$, so in particular there is a prime $\mathfrak{v}$ such that $f_{_{\mathfrak{v},H}} \neq 1$, i.e., $f_{_\mathfrak{v}} = f_{_{\mathfrak{v},\gamma}}$ for some $\gamma \in H$. So by the uniqueness of f in (4.3.3), $h_{\mathfrak{v}}(\sigma_{\mathfrak{v}}) = \gamma \in H$; hence $\overline{h_{\mathfrak{v}}}(\sigma_{\mathfrak{v}}) \neq 1$, which says that $\overline{h_{\mathfrak{v}}}$ is ramified and so $\overline{h}$ is ramified.
To show that K_h is a field, we have to prove that $h(\Omega) = \Gamma$, so by contradiction we consider the non trivial quotient $\overline{\Gamma} = \Gamma/h(\Omega)$ which gives $\overline{h} = 1$, so $\overline{h}$ unramified which is a contradiction. So $h(\Omega)$ cannot be a proper subgroup of Γ.

(b) Finally, every subfield of K_h over K is the fixed field $(K_h)^{\Sigma}$ of some subgroup Σ of Γ. Again we consider the quotient $\overline{\Gamma} = \Gamma/\Sigma$ and the quotient map $\overline{h}$. By the discussion on the change of the acting group, $(K_h)^{\Sigma} \cong K_{\overline{h}}$ and so if $\Sigma \neq \Gamma$, then $(K_h)^{\Sigma}$ is ramified over K, proving (b) and completing the proof. □

Remark 4.3.8. *By (c) if we consider $|\Gamma|$ as an ideal, we find h' such that $j(c) = (O_{h'})$ and*

$\delta(O_h/O)$ relatively prime to $|\Gamma|$; or in other words h' is domestic. So any realisable class is even given by a domestic extension.

We give an alternative formulation of the previous Theorem, using the following commutative diagram

$$\begin{tikzcd}
Cl(O\Gamma) = \frac{J(K\Gamma)}{\lambda(K\Gamma^{\times})U(O\Gamma)} \arrow[r, "Rag"] \arrow[dr, "Rag'"] & \frac{\mathcal{H}(\mathbb{A}(K\Gamma))}{\lambda(\mathcal{H}(K\Gamma))\mathcal{H}(\mathbb{A}(O\Gamma))} \arrow[d, "p"] \\
 & \frac{\mathcal{H}(\mathbb{A}(K\Gamma))}{\lambda(\mathcal{H}(K\Gamma))\mathcal{H}(\mathbb{A}(O\Gamma))\Theta^t(J(K\Lambda))},
\end{tikzcd} \tag{4.3.9}$$

where Rag was already defined in the previous chapter, while p is just a quotient map and $Rag' = p \circ Rag$. Thus, from Theorem 4.3.7, we have the following Corollary.

Corollary 4.3.9. *In same hypothesis as before:*

$$R(O\Gamma) = ker(Rag').$$

In particular, $R(O\Gamma)$ is a subgroup of $Cl(O\Gamma)$.

In the same way as done for the unramified case, we can also give an explicit description of the set of realizable classes.

Corollary 4.3.10. *In the general tame case, we have*

$$R(O\Gamma) \cong \frac{rag\,J(K\Gamma) \cap \lambda\left(\mathcal{H}\left(K\Gamma\right)\right)\mathcal{H}\left(\mathbb{A}\left(O\Gamma\right)\right)\Theta^t\left(J\left(K\Lambda\right)\right)}{\lambda(rag\,K\Gamma^{\times})rag\,U(O\Gamma)}.$$

4.4 Link between the Stickelberger module here defined and Stickelberger's Theorem

After the important result reached in the previous part which well describes the behavior of the set of realizable classes, we would now to underline the link between the Stickelberger map defined at the beginning of this chapter and the classical Stickelberger Theorem.

The famous Stickelberger Theorem is well known by basic Galois module theory and it says that the classgroup of the cyclotomic extension $\mathbb{Q}(q)$ (the splitting field over $\mathbb{Q}$ of the polynomial $x^q - 1$) is annihilated by a particular element $\theta \in \mathbb{Z}[\mathrm{Gal}\,(\mathbb{Q}(q)/\mathbb{Q})]$ (for a precise statement and proof of this Theorem we refer to Chapter 1 in [Ere]).

One would know why we called Θ_{Γ} the Stickelberger map and S_{Γ} the Stickelberger module. The reason of these names is well explained in Section 7 in [McC87] and it arises by some annihilation results depending on Θ_{Γ} and S_{Γ}, generally defined on the quotient $Cl(O\Gamma)/R(O\Gamma)$.
Without going into details, in this section we try to give an overview of the annihilation results

reached by McCulloh.

In the first part, using the pairing

$$\begin{array}{rccc} [\ ,\ ]_{\Gamma}: & \mathrm{Hom}_{\Omega}(\mathbb{Z}\widehat{\Gamma}, \mathbb{Z}\Gamma(-1)) \times J(K\Lambda) & \longrightarrow & J(K\Gamma) \\ & (\Phi, \gamma) & \longrightarrow & \Phi^t(\gamma) \end{array}$$

and defining the module $\mathcal{S} = (\mathrm{End}_{\Gamma}(\mathbb{Z}\Gamma(-1)) \circ \Theta_{\Gamma}) \cap \mathrm{Hom}_{\Gamma}\left(\mathbb{Z}\widehat{\Gamma}\mathbb{Z}\Gamma(-1)\right)$, it's proved the first general annihilation result which says that

$$[\mathcal{S}, J(K\Lambda)]_{\Gamma} \subseteq R(O\Gamma).$$

Starting from this general result and passing from $J(K\Lambda)$ to $J(K\Gamma)$, McCulloh arrived to a generalization of the classical relations, already cited, on the ideal classgroup of $\mathbb{Q}(q)$.

In particular the intermediate step is to consider E a commutative ring of endomorphisms of Γ over which $\widehat{\Gamma}$ is cyclic.
Thanks to the pairings

$$\begin{array}{rccc} [\ ,\ ]_{E}: & \mathbb{Z}\Gamma(-1) \times J(K\Lambda) & \longrightarrow & J(K\Gamma) \\ \{\ ,\ \}_{E}: & \mathbb{Z}E \times J(K\Gamma) & \longrightarrow & J(K\Gamma)\ , \end{array}$$

McCulloh showed that

$$[S_{\Gamma}, J(K\Lambda)]_{E} \subseteq R(O\Gamma)$$

and

$$\{S_{E}, J(K\Gamma)]_{E} \subseteq R(O\Gamma),$$

where $S_E \subseteq \mathbb{Z}E$ is the unique submodule such that $S_E s_1 = S_{\Gamma}$ (with s_1 the element such that $\Gamma = Es_1$).
Using $C = E^{\times}$ and considering $K[\mu_E]$ a particular quotient algebra of $K\Gamma$, McCulloh defined a Stickelberger ideal S_C in $\mathbb{Z}(C)$ such that

$$Cl(O[\mu_E])^{S_C} \subseteq R(O[\mu_E]),$$

where $O[\mu_E]$ and $R(O[\mu_E])$ are the images of $O\Gamma$ and $R(O\Gamma)$ in $K(\mu_E)$ and $Cl(O[\mu_E])$, respectively.

This is the result which generalizes Stickelberger's Theorem, indeed if $K = \mathbb{Q}$ and Γ is cyclic of order q, then $K[\mu_E] = \mathbb{Q}(q)$ and $R(\mathbb{Z}[\mu_E]) = (1)$ since $R(\mathbb{Z}\Gamma) = 1$, giving the classical annihilation result on cyclotomic extensions.

Chapter 5

The case of A_4

In this chapter, we will explain the two approaches, preluded in the introduction, used to solve the non abelian case applied to the group $\Gamma = A_4$. For the description of the group A_4 and of all its elements as x and y, we remand to the Appendix A.2.
We shall try to sectionize what follows in different steps, in order to have the possibility to underline the common elements in the two approaches and to give a pleasant presentation.

Looking at the Appendix, where a good algebraic background can be found, in our presentation we shall focus on the case of $\Gamma = A_4$, the alternating tetrahedral group of order 12; treated with the first approach in [GS03] and with the second one in [BS05b]. We consider this particular case because it is one of the only two groups treated with both the approaches and because it is the only one for which a clear result about the set of realizable classes is given *without any restriction on the base field* ([BS05b]).

From the Introduction we already know that

$$R(\mathcal{M}) \subseteq Cl^{\circ}(\mathcal{M})$$

and that

$$R(O_K[\Gamma]) \subseteq Cl^{\circ}(O_K[\Gamma]).$$

The already cited work [GS03], following the first approach, makes use of the maximal order $\mathcal{M}$ and, with some assumptions on the base field K, it arrives to prove the reverse inclusion for $R(\mathcal{M})$; in particular it proves the following Theorem.

Theorem 5.0.1. *Let K a number field not containing ω (a primitive 3-rd root of unity) and with odd class number. Then we have*

$$R(\mathcal{M}) = Cl^{\circ}(\mathcal{M}) \cong Cl\left(K(\omega)\right) \times Cl(K).$$

Found the Wedderburn's decomposition in simple components of the semisimple algebra $K[\Gamma]$, the main idea of this approach is to use the Hom-description given by Fröhlich, through the different irreducible characters of Γ, to find a representative class in $Cl(\mathcal{M})$ and then to prove that the set

$R(\mathcal{M})$ is the subgroup $Cl^{\circ}(\mathcal{M})$, via the concept of Steinitz class which will be later recalled.

Even if the main problem proposed by McCulloh consists in describing $R(O_K[\Gamma])$, we can read $R(\mathcal{M})$ as a "good approximation" of the desired set. So the lack of this first approach is that we will not arrive to solve the original given problem, even if we reach a good approximation (and so a vivid hope to obtain it even in the required form) of it.

An answer to the description of $R(O_K[\Gamma])$ is given some years later in [BS05b], where without any assumption on the base field K is proved that $Cl^{\circ}(O_K[\Gamma]) \subseteq R(O_K[\Gamma])$. Thus the main Theorem of the Chapter is the following.

Theorem 5.0.2. *Given a number field K and $\Gamma = A_4$, then $R(O_K[\Gamma]) = Cl^{\circ}(O_K[\Gamma])$.*

Remark 5.0.3. *As an obvious Corollary, we have that the set of realizable classes for the alternating group A_4 forms a subgroup in $Cl(O_K[\Gamma])$.*

5.1 $K[A_4]$, $Cl(\mathcal{M})$, $Cl^{\circ}(O_K[A_4])$ and the ray class group

We recall here some results already presented in the Appendix which are fundamental for our presentation.

We already know the Wedderburn decomposition of $K[A_4]$ (look at the Appendix A.3) and we can write it in a compact way using K' defined as

$$K' = \begin{cases} K \times K & \text{if } \omega \in K, \\ \\ K(\omega) & \text{if } \omega \notin K; \end{cases}$$

where ω is the usual 3-rd root of unity.
Indeed using K', we have

$$K[A_4] \cong K \times K' \times M_3(K)$$

and we obtain

$$Cl(\mathcal{M}) \cong Cl(K) \times Cl(K') \times Cl(K).$$

As well explained in the Appendix, using the modified Hom-description we can identify the representing homomorphism f with the set of values it assumes on the irreducible characters over K. Since the irreducible characters over K depend on whether ω belongs to K or not, we can write

$$\mathrm{Hom}^{\circ}_{\Omega_K}\left(R_{A_4}, J\left(\mathbb{Q}^c\right)\right) = J(K') \times J(K)$$

and

$$\mathrm{Hom}^{\circ}_{\Omega_K}(R_{A_4}, (\mathbb{Q}^c)^{\times}) = K'^{\times} \times K^{\times}.$$

Thus, regarding $\mathrm{Det}^{\circ}\left(U\left(O_K[A_4]\right)\right)$ as a subgroup of $J(K') \times J(K)$, the Hom-description of the augmentation kernel becomes

$$Cl^{\circ}(O_K[A_4]) \cong \frac{J(K') \times J(K)}{\left(K'^{\times} \times K^{\times}\right) \mathrm{Det}^{\circ}\left(U\left(O_K[A_4]\right)\right)}. \tag{5.1.1}$$

Given a nonzero ideal $\mathfrak{a}$ in O_K, recall the definition of the ray class group $Cl_{\mathfrak{a}}(O_K)$:

$$Cl_{\mathfrak{a}}(O_K) = \frac{J(K)}{K^{\times}U_{\mathfrak{a}}(O_K)},$$

where

$$U_{\mathfrak{a}}(O_K) = \{u \in U(O_K) \mid u \equiv 1 (mod^{\star}\mathfrak{a})\}.$$

We can extend this notion to the integral closure $O_{K'}$ of O_K in K'. Indeed if $\omega \notin K$ we just apply the definition; while if $\omega \in K$, we have that any nonzero ideal $\mathfrak{a}$ in $O_{K'}$ is the product $\mathfrak{a}_1\mathfrak{a}_2$ of two nonzero ideals $\mathfrak{a}_1$, $\mathfrak{a}_2$ in O_K and we put

$$Cl_{\mathfrak{a}}(O_{K'}) = Cl_{\mathfrak{a}_1}(O_K) \times Cl_{\mathfrak{a}_2}(O_K).$$

We can now use the ray class group to obtain a surjection into the augmentation kernel, as well explained by the following Proposition.

Proposition 5.1.0.1. *The natural map $J(K') \times J(K) \longrightarrow Cl^{\circ}(O_K[\Gamma])$ given by (5.1.1), induces a surjection*

$$Cl_{\mathfrak{a}}(O_{K'}) \times Cl_8(O_K) \longrightarrow Cl^{\circ}(O_K[\Gamma]), \tag{5.1.2}$$

where $\mathfrak{a}$ is an ideal of $O_{K'}$ divisible only by primes of O_K above 2 and 3 and where the subscript 8 denotes the principal ideal $8O_K$.

Proof. For a proof we refer to [BS05b]. □

5.2 The Embedding Problem

In the solution of the problem, using the fact that $A_4 = C_3 \rtimes \Delta$ and by means of the already cited results in the abelian case (applied to C_3), we will always start taking a cyclic extension E/K of order 3 and then we would embed it in a tetrahedral extension N/K. In order to get it, we have to solve an embedding problem and the following important Lemma will help us in this direction.

Lemma 5.2.1 (Immersion Problem)**.** *Let K be a number field, E/K a cyclic extension of degree 3 and $E(\sqrt{b})/E$ a quadratic extension of E. Then the following are equivalent:*

(i) *The Galois closure of $E(\sqrt{b})/K$ is a tetrahedral extension N/K,*

(ii) *$N_{E/K}(b)$ is a square in K;*

If (ii) is satisfied, then we can take $N = E(\sqrt{b}, \sqrt{\sigma(b)})$ (where σ is the generator of the cyclic Galois group of degree 3).

Proof. For a proof of it, look at [Mar90] pag. 365. □

Remark 5.2.2. *The situation in the Lemma is well represented by the following diagram:*

$$\begin{tikzcd}
& N = E\left(\sqrt{b}, \sqrt{\sigma(b)}\right) \arrow[dl, dash, "2"'] \arrow[dr, dash] & \\
L = E\left(\sqrt{b}\right) \arrow[dr, dash, "2"'] & & L' = E\left(\sqrt{\sigma(b)}\right) \arrow[dl, dash] \\
& E \arrow[d, dash, "3"', "\langle\sigma\rangle"] & \\
& K &
\end{tikzcd} \tag{5.2.1}$$

5.3 Fröhlich's Hom-description and irreducible characters for A_4

Once we have the irreducible characters over the field K, one can apply Fröhlich's Hom-description (look at the Appendix A.5) to calculate a representative $f \in \mathrm{Hom}_{\Omega_K}(R_{A_4}, J(\mathbb{Q}^c))$ of the class corresponding to the given extension, by its values on the irreducible characters over K.

In particular if $\omega \in K$ the $f \in \mathrm{Hom}_{\Omega_K}(R_{A_4}, J(\mathbb{Q}^c))$ can be identified with its set of values

$$\left(f(\chi_0), f(\chi_1), f(\chi_1^2), f(\chi_2)\right) \in J(K)^4,$$

while if $\omega \notin K$ then we associate to f the triple

$$(f(\chi_0), f(\chi_1), f(\chi_2)) \in J(K) \times J\left(K(\omega)\right) \times J(K).$$

If we want to find a representative $f \in \mathrm{Hom}^{\circ}_{\Omega_K}(R_{A_4}, J(\mathbb{Q}^c))$ the computation is the same even if we don't consider $f(\chi_0)$ since it's equal to 1 by assumption (look at the Appendix A.5.10).

So considering N/K a tame tetrahedral extension with normal basis generator α and local normal integral basis generator $\alpha_{\mathfrak{v}}$, it's better to give a look at each computation considering each irreducible character. We don't write explicitly $f(\chi_1^2)$ since it's analogous to the computation for $f(\chi_1)$.
In the computations we make use of the cyclic subextension E/K fixed by Δ with normal integral basis c. Moreover we consider the biquadratic extension N/E with normal basis generator η and local normal integral basis generator $\eta_{\mathfrak{v}}$.

Trivial character χ_0

Thanks to the fact that χ_0 is 1-dimensional and trivial, we have $(\alpha_{\mathfrak{v}}|\chi_0) = \mathrm{Tr}_{N_{\mathfrak{v}}/K_{\mathfrak{v}}}(\alpha_{\mathfrak{v}})$ and $(\alpha|\chi_0) = \mathrm{Tr}_{N/K}(\alpha)$, where Tr is the usual trace map. In both cases we have that the value of the trace map is a unit (thanks to the basis properties), so taking $\alpha_{\mathfrak{v}}\left(\mathrm{Tr}_{N_{\mathfrak{v}}/K_{\mathfrak{v}}}(\alpha_{\mathfrak{v}})\right)^{-1}$ and

$\alpha\left(\mathrm{Tr}_{N/K}(\alpha)\right)^{-1}$ if necessary, we can assume that α and $\alpha_{\mathfrak{v}}$ are such that the trace assumes value 1, giving

$$f(\chi_0) = (1).$$

One dimensional non trivial character χ_1

If we consider χ_1 we can restrict it to C_3 and obtain a non trivial character denoted by $\overline{\chi_1}$ (non trivial because the kernel of χ_1 is Δ). Thanks to the fact that we are considering a 1-dimensional character, we use the property of the Fröhlich-Lagrange resolvent to restrict to the extension E/K in the following way

$$\begin{aligned} (\alpha_{\mathfrak{v}}|\chi_1)_{N/K} &= (\mathrm{Tr}_{N_{\mathfrak{v}}/E_{\mathfrak{v}}}(\alpha_{\mathfrak{v}})|\overline{\chi_1})_{E/K}, && (5.3.1)\\ (\alpha|\chi_1)_{N/K} &= (\mathrm{Tr}_{N/E}(\alpha)|\overline{\chi_1})_{E/K}. && (5.3.2)\end{aligned}$$

We stress that the two new elements, obtained considering the trace map over N/E, are still basis generators for the $O_{K,\,\mathfrak{v}[C_3]}$-module $O_{E,\,\mathfrak{v}}$ and the $K[C_3]$-module E (it comes from the first chapter on Galois Algebra).
In this way we have

$$f(\chi_1) = \left(\frac{\left(\mathrm{Tr}_{N_{\mathfrak{v}}/E_{\mathfrak{v}}}(\alpha_{\mathfrak{v}})|\overline{\chi_1}\right)_{E/K}}{\left(\mathrm{Tr}_{N/E}(\alpha)|\overline{\chi_1}\right)_{E/K}}\right).$$

Three dimensional character χ_2

To determine $f(\chi_2)$ we use the fact that $\chi_2 = \mathrm{Ind}_{\Delta}^{A_4}\phi$, where ϕ is the non trivial character of Δ which fixes x. Indeed there is a result of Fröhlich (look at [Frö75], Theorem 12, pag.165) which solves this situation.
Fröhlich's formula says that there are λ and $\lambda_{\mathfrak{v}}$, invertible elements in the rings $K[\Delta]$ and $O_{K,\,\mathfrak{v}}[\Delta]$, such that

$$\begin{aligned} (\alpha|\chi_2)\phi(\lambda) &= \mathcal{N}_{E/K}\left((\eta|\phi)_{N/E}\right) e(E/K), && (5.3.3)\\ (\alpha_{\mathfrak{v}}|\chi_2)\phi(\lambda_{\mathfrak{v}}) &= \mathcal{N}_{E/K}\left((\eta_{\mathfrak{v}}|\phi)_{N/E}\right) e(E_{\mathfrak{v}}/K_{\mathfrak{v}}), && (5.3.4)\end{aligned}$$

where ϕ is extended by linearity to $K[\Delta]$ and $K_{\mathfrak{v}}[\Delta]$, while $e(E/K)$ is the square root of the discriminant of a basis of E over K and $e(E_{\mathfrak{v}}/K_{\mathfrak{v}})^2 O_{K,\,\mathfrak{v}}$ is the discriminant of $E_{\mathfrak{v}}/K_{\mathfrak{v}}$. $\mathcal{N}_{E/K}\left((\eta|\phi)_{N/E}\right)$ denotes the product $\prod_{\gamma\in\,\mathrm{Gal}(E/K)}\gamma\left((\eta|\gamma^{-1}\phi)_{N/E}\right)$; since in our situation ϕ assumes only values $\{\pm 1\}$, $\gamma^{-1}\phi = \phi$ and $\mathcal{N}_{E/K}$ is exactly the usual norm $\mathrm{N}_{E/K}$:

$$\mathcal{N}_{E/K}\left((\eta|\phi)_{N/E}\right) = \mathrm{N}_{E/K}\left((\eta|\phi)_{N/E}\right) = \prod_{\gamma\in\,\mathrm{Gal}(E/K)} \gamma\left((\eta|\phi)_{N/E}\right).$$

Thus we obtain the following Lemma.

Lemma 5.3.1. *We consider the cyclic extension E/K with normal basis generator c embedded in the tetrahedral extension N/K with normal basis generator α and local normal integral basis* *generator $\alpha_{\mathfrak{v}}$. We also take the biquadratic extension N/E with normal basis generator η and local normal integral basis generator $\eta_{\mathfrak{v}}$. Then using the notation given above, we have that*

$$f(\chi_2) = \left(\frac{e(E_{\mathfrak{v}}/K_{\mathfrak{v}})}{e(E/K)} N_{E/K} \left(\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}} \right) \frac{\phi(\lambda)}{\phi(\lambda_{\mathfrak{v}})} \right).$$

where ϕ is extended by linearity to $K[\Delta]$ and $K_{\mathfrak{v}}[\Delta]$, while $e(E/K)$ is the square root of the discriminant of a basis of E over K and $e(E_{\mathfrak{v}}/K_{\mathfrak{v}})^2 O_{K,\mathfrak{v}}$ is the discriminant of $E_{\mathfrak{v}}/K_{\mathfrak{v}}$.

In particular as a basis of E over K we can take the set $\{\sigma^i(c)\}_{0\leq i\leq 2}$ (the element σ, as denoted in the appendix, is the generator of the cyclic group of order 3 or in other words of the Galois group of E/K, this is a base since c is a normal basis generator for E/K) and reading the proof of Fröhlich's formula we understand that λ is the determinant of the matrix (λ_{ij}) over $K[\Delta]$ given by

$$\sigma^i(c)\eta = \sum_{j=0}^{2} \lambda_{ij}\sigma^j(\alpha) \quad \text{for} \quad 0 \leq i \leq 2. \tag{5.3.5}$$

An analogous thing can be done for $\lambda_{\mathfrak{v}}$.

Remark 5.3.2. *The element $e(E/K)$ is a global element belonging to $K^{\times}$, so in the Hom-description it can even be ignored.*

Remark 5.3.3 (Simplification in the case over the maximal order $\mathcal{M}$)**.** *Since $\phi(\lambda)$ and $\phi(\lambda_{\mathfrak{v}})$ are units, the maps sending the 1-dimensional characters to 1 and χ_2 to the value $\phi(\lambda)$ (resp. $\phi(\lambda_{\mathfrak{v}})$) are in $Hom_{\Omega_K}(R_{A_4}, K^{c\times})$ (resp. $Hom_{\Omega_K}(R_{A_4}, U(K^c))$); thus we can "erase" them in the Hom-description with the maximal order $\mathcal{M}$ and obtain*

$$f(\chi_2) = \left(\frac{e(E_{\mathfrak{v}}/K_{\mathfrak{v}})}{e(E/K)} N_{E/K} \left(\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}} \right) \right).$$

5.4 First Approach

We are now ready to enter deeply in the heart of the first approach and from now one, in this section, we shall consider only the case of K *not containing ω*. First of all let's describe the use of the Steinitz classes which are of fundamental importance in the first approach treating with the maximal order $\mathcal{M}$. With the assumption on K and ω, the situation is the following:

$$\begin{tikzcd}
& N \arrow[dl, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash, "3"'] & & K(\omega) \arrow[dl, dash, "2"] \\
& K &
\end{tikzcd} \tag{5.4.1}$$

5.4.1 Components of the class $\mathcal{M} \otimes_{O_K[A_4]} O_N$ and Steinitz class

Using the description of f given in the previous section, we are ready now to understand the components c_i with $0 \leq i \leq 2$ of the class $\mathcal{M} \otimes_{O_K[A_4]} O_N$ in the three components of $Cl(\mathcal{M})$.

If we consider the cyclic (of degree 2) Galois Group $S = \langle s \rangle$ of $K(\omega)/K$, where $s(\omega) = \omega^2$ and $s^2(\omega) = \omega$, taking the Stickelberger element $\theta := s^{-2} + 2s^{-1}$ (which is equal to $s^2 + 2s$, since $s^{-1} = s$) and using [Sod88] (Theorem 2.2(1)), we have

$$\left(\left(\mathrm{Tr}_{N/E}(\alpha), \overline{\chi_1}\right)_{E/K}\right)^3 O_{K(\omega)} = \left(I(\overline{\chi_1})\right)^3 \theta\left(J\left(\overline{\chi_1}\right)\right),$$

where $I(\overline{\chi_1})$ is a fractional ideal of $O_{K(\omega)}$, and $J(\overline{\chi_1})$ is a square free integral ideal of $O_{K(\omega)}$, uniquely determined by $\mathrm{Tr}_{N/E}(\alpha)$, such that $J(\overline{\chi_1})$ is relatively coprime with $s\left(J(\overline{\chi_1})\right)$.

Recall 5.4.2 (Steinitz class). *If we have N/K an extension of number fields of degree n, we have that O_N is a torsion free O_K-module of rank n and in particular $O_N \cong O_K^{n-1} \oplus I$, where I is an ideal of O_K (for this result look at Theorem* 1.2.19 *in [Coh00]).*
The class of I in $Cl(K)$ is defined as the Steinitz class of N/K or of O_N and it's denoted by $Cl_K(O_N)$.
The structure of O_N as an O_K-module is determined up to isomorphism by its rank and its Steinitz class (Theorem 13 *pag.*95 *in [FT91]).*

We use now Steinitz classes in the following Proposition to determine the components c_i defined above.

Proposition 5.4.2.1. *Following the previous notation, we have*

(i) *c_0 is the trivial class in $Cl(K)$.*

(ii) *c_1 is the class of $\left(I(\overline{\chi_1})\right)^{-1}$ (or of O_E) in $Cl\left(K(\omega)\right)$.*

(iii) *$c_2 = Cl_K(O_E)N_{E/K}\left(Cl_E(O_L)\right)$ in $Cl(K)$, where L/E is a quadratic subextension of N/E.*

Proof. **(i)** This first result is trivial from the fact that $f(\chi_0) = (1)$.

(ii) From the discussion on the value of $f(\chi_1)$, we understand that $f(\chi_1) = f(\overline{\chi_1})$, indeed $f(\chi_1) = \left(\frac{\left(\mathrm{Tr}_{N_{\mathfrak{v}}/E_{\mathfrak{v}}}(\alpha_{\mathfrak{v}})|\overline{\chi_1}\right)_{E/K}}{\left(\mathrm{Tr}_{N/E}(\alpha)|\overline{\chi_1}\right)_{E/K}}\right)$ and the two trace values are still basis generators, giving the equality with $f(\overline{\chi_1})$.
From this fact, we reduce to study the extension E/K, which is cyclic of degree 3 and tame (since N/K is so). From the fact that the cyclic group C_3 is abelian and that K doesn't contain ω, we have that all the irreducible representations over K are one dimensional and, as done before, if we consider $\mathcal{M}'$ the O_K-maximal order in $K[C_3]$ (where C_3 is the cyclic group of order 3) we obtain

$$Cl(\mathcal{M}') \cong Cl(K) \times Cl\left(K(\omega)\right) \cong Cl(O_K[C_3]);$$

where the last isomorphism is given by the fact that we are considering an abelian group. Applying the Hom-description here, we have that the class of $\mathcal{M}' \otimes_{O_K[C_3]} O_E$ is represented by the map f which sends the trivial characters of C_3 to 1 and $\overline{\chi_1}$ to $f(\chi_1)$. Looking in [Sod88] (Theorem 2.3), we have that the component of the class of $\mathcal{M}' \otimes_{O_K[C_3]} O_E$ in $Cl\,(K(\omega))$ is the class of $(I(\overline{\chi_1}))^{-1}$, as we wanted to show.

(iii) If we consider $\mathcal{M}_2$ the maximal O_E-order in $E[\Delta]$, we can act as before to find a representative of the class of $\mathcal{M}_2 \otimes_{O_{E[\Delta]}} O_N$ in $Cl(\mathcal{M}_2)$. Since we have four 1-dimensional representations over E, the class group is written in simple components as

$$Cl(\mathcal{M}_2) \cong Cl(E)^4$$

and the representative f_2 of the class desired, sends the trivial character to 1 and for any other characters ϕ of Δ is defined componentwise as $(f_2(\phi))_{\mathfrak{v}} = \frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}}$. Considering ϕ the character which induces χ_2, if we take L/E the quadratic subextension fixed by $\mathrm{Ker}(\phi)$, we denote by $\overline{\phi}$ the restriction of ϕ to $\mathrm{Gal}(L/E)$.
As already done before, we can restrict to L/E, obtaining

$$\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}} = \frac{\left(\mathrm{Tr}_{N_{\mathfrak{v}}/L_{\mathfrak{v}}}(\eta_{\mathfrak{v}})|\overline{\phi}\right)_{L/E}}{\left(\mathrm{Tr}_{N/L}(\eta)|\overline{\phi}\right)_{L/E}}.$$

Looking at [Sod99a] (pag. $52-53$), we see that the class in $Cl(E)$ of the content of the idele with components the elements on the right of the previous formula is exactly $Cl_E(O_L)$.

We consider now the terms $\frac{e(E_{\mathfrak{v}}/K_{\mathfrak{v}})}{e(E/K)}$ and we denote by H the ideal of O_K which is the content of the idele with these components. Since $e(E_{\mathfrak{v}}/K_{\mathfrak{v}})^2 O_{K,\mathfrak{v}}$ is the discriminant of $E_{\mathfrak{v}}/K_{\mathfrak{v}}$ (the local discriminant), if we denote by $\Delta(E/K)$ the discriminant of E/K, then we have

$$I^2 = \frac{\Delta(E/K)}{e(E/K)^2}.$$

As $d := e(E/K)^2$ is the discriminant of a basis of E/K, we have, from a result of Artin (look in the next section for reference and a good explanation), that $Cl_K(O_E) = Cl\left(\sqrt{\frac{\Delta(E/K)}{d}}\right) = Cl(H)$.

Putting all together, we obtain now that

$$f(\chi_2) = \left(\frac{e(E_{\mathfrak{v}}/K_{\mathfrak{v}})}{e(E/K)} \mathrm{N}_{E/K}\left(\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}}\right)\right) = Cl_K(O_E)\mathrm{N}_{E/K}\left(Cl_E(O_L)\right),$$

as we wanted to show.

□

5.4.3 The structure of the Realizable classes over the maximal order

This is the final step which leads to the proof of the fact that $R(\mathcal{M})$ is a subgroup of $Cl^{\circ}(\mathcal{M})$, proving in particular that $R(\mathcal{M})$ is the whole $Cl^{\circ}(\mathcal{M})$. While we have already talked of the proof of the first inclusion ($\subseteq$) in the Introduction (like a reference we always consider [McC75]), the other inclusion ($\supseteq$) will take the whole effort in our proof.

Anticipation of the proof of the inclusion ($\supseteq$). In order to have an easier explanation and also to visualize the skeleton of the method utilized in this kind of problem, we will divide the second part of the proof of this inclusion in three smaller problems: an Immersion Problem, use of the Artin's result and use of Class Field Theory.

The Immersion Problem regards the fact that, after the first part of the proof, we'll have a cyclic extension of number fields E/K of degree 3 and we would find an extension N/E such that N/K is a tetrahedral extension.

During the proof, we shall make use of the Steinitz class of an extension L/E and in particular we would compute it. To succeed, using the discriminant $\Delta(L/E)$ of the extension L/E, we'll apply the famous Artin's result, which will be recalled later.

Finally in the computation of the discriminant, we would control the ramification in the extension L/E and to get it we shall apply a general result of Class Field Theory.

Before of the main result, let's recall the important results by Artin which will be used in the proof.

Proposition 5.4.3.1 (Artin's Result)**.** *Given an extension of number fields L/E, we have*

$$Cl_E(O_L) \cong Cl\left(\sqrt{\frac{\Delta(L/E)}{d}}\right),$$

where $\Delta(L/E)$ is the discriminant of L/E and d is the discriminant of a basis of L/E.

Proof. For the original proof of it look at [Art50]. □

We enter now in detail in the main result over the maximal order, giving the proof of Theorem 5.0.1. From the isomorphism $Cl(\mathcal{M}) \cong Cl(K) \times Cl\left(K\left(\omega\right)\right) \times Cl(K)$, it follows that $Cl^{\circ}(\mathcal{M}) \cong Cl\left(K(\omega)\right) \times Cl(K)$.

Proof of Theorem 5.0.1. As already remarked, we have only to prove that $Cl\left(K(\omega)\right) \times Cl(K) \subseteq R(\mathcal{M})$.
So given $(x_1, x_2) \in Cl\left(K(\omega)\right) \times Cl(K)$, we want to construct a tame tetrahedral extension N/K such that the components of the class of $\mathcal{M} \otimes_{O_K[A_4]} O_N$ are (x_1, x_2).

We start from the first components $x_1 \in Cl\left(K(\omega)\right)$. If we consider the Stickelberger ideal $\mathcal{S} = \frac{1}{3}\theta\mathbb{Z}[S] \cap \mathbb{Z}[S]$, where S is the already defined cyclic Galois Group of $K(\omega)/K$, then we have

that $\mathcal{S} = \mathbb{Z}[S]$, since $\frac{1}{3}\theta(2s - s^2) = 1$.
Following [Sod88] (Theorem 2.4, with $l = 3$ and N substituted by E), $R(\mathcal{M}')$ can be identified with $Cl\,(K(\omega))$, so there exists a tame cyclic extension E/K of degree 3, such that the class of $\mathcal{M}' \otimes_{O_{K[S]}} O_E$ in $Cl\,(K(\omega))$ is x_1. Moreover E/K can be chosen such that it ramifies at least over one place.

We focus now on the second component x_2 and we'll separate under the small three problems already citated.
Let $c \in Cl(K)$ such that

$$x_2 = c\,Cl_K(O_E).$$

Here we use the fact that the class number of K is odd, indeed if it's so, we find $c' \in Cl(K)$ such that $c = (c')^2$. From Theorem 10.1 in [Was96], $\mathrm{N}_{E/K} : Cl(E) \longrightarrow Cl(K)$ is surjective, since E/K is ramified; so there is $C \in Cl(E)$ such that $\mathrm{N}_{E/K}(C) = c'$.

Immersion Problem. Once we have the cyclic (abelian) extension E/K of degree 3, we want now to find an extension N/E such that N/K is the tame tetrahedral extension we are looking for. To solve this problem, we would use the already recalled Lemma 5.2.1, which says that if we find an element $b \in E$ such that $\mathrm{N}_{E/K}(b)$ is a square in K, then E is embeddable in the tame tetrahedral extension $N = E\left(\sqrt{b}, \sqrt{\sigma(b)}\right)$.

Class Field Theory. In order to find such an element b, we'll make use of a Class Field Theory result. If we consider $Cl_4(O_E)$, the modified ray class group modulo $4O_E$, just by definition we have the canonical surjection from $Cl_4(O_E) \longrightarrow Cl(E)$, which let us to find a fractional ideal I of O_E so that $Cl(I^{-1}) = C$; then thanks to the Tchebotarev density Theorem in ray classgroups (look at [Neu86], Theorem 6.4) we get $m \in E^\times$ and a prime ideal $\mathcal{B}$ of O_E such that:

- $\mathcal{B} \cap O_K$ splits completely in E/K,
- $mO_E = I^2\mathcal{B}$,
- $m \equiv 1 \bmod 4O_E$.

Applying σ we have $\sigma(m)O_E = \sigma(I)^2\sigma(\mathcal{B})$ and so

$$(m\sigma(m))\,O_E = (I\sigma(I))^2\,\mathcal{B}\sigma(\mathcal{B}).$$

If we call $b := m\sigma(m)$, it's not a square in E (since $\mathcal{B}$ and $\sigma(\mathcal{B})$ are distinct) and we can consider the quadratic extension $L = E(\sqrt{b})/E$. This is exactly the element we were looking for, indeed its norm over K is a square since $\mathrm{N}_{E/K}(b) = \mathrm{N}_{E/K}(m\sigma(m)) = \left(\mathrm{N}_{E/K}(m)\right)^2$, letting us to embed E/K in the tame tetrahedral extension $N = E\left(\sqrt{b}, \sqrt{\sigma(b)}\right)$.

Artin's result. Moreover the decomposition laws in the extension $E(\sqrt{b})/E$ are well known (look at section 39 in [Hec81]) and the only primes which ramify are $\mathcal{B}$ and $\sigma(\mathcal{B})$. Thus we have

$\Delta(L/E) = \mathcal{B}\sigma(\mathcal{B})$ and, thanks to the already cited result of Artin [Art50], we obtain $Cl_E(O_L) = Cl(\sqrt{\Delta(L/E)}) = Cl\,(I\sigma(I))^{-1}$, which assures that

$$Cl_E(O_L) = C\sigma(C).$$

In conclusion, calculating the norms we get

$$\mathrm{N}_{E/K}\left(Cl_E(O_L)\right) = \mathrm{N}_{E/K}\left(C\sigma(C)\right) = \mathrm{N}_{E/K}(C^2) = c'^2 = c,$$

which yields

$$x_2 = Cl_K(O_E)\,c = Cl_K(O_E)\mathrm{N}_{E/K}\left(Cl_E(O_L)\right).$$

After all, by Proposition 5.4.2.1, we see that the components of the class of O_N (where N is the constructed number field) in $Cl\left(K(\omega)\right) \times Cl(K)$ are exactly (x_1, x_2); completing the proof of the Theorem.

5.5 Refinement: Main Theorem

After the presentation of the approach which leads to describe $R(\mathcal{M})$, in this section all our efforts shall regard the proof of the inclusion $R(O_K[\Gamma]) \supseteq Cl^\circ(O_K[\Gamma])$. In other words, given an element in $Cl^\circ(O_K[\Gamma])$, we would find a tame tetrahedral extension N/K such that the corresponding class is exactly the considered element.
We recall that from now on we don't make any assumption on the base field K as done over the maximal order, in particular ω can belong or not to K.

5.5.1 Construction of the tame tetrahedral extension N/K

From the Hom-description, any element in $Cl^\circ(O_K[\Gamma])$ is represented by the pair of ideles $(c_1, c_2) \in J(K') \times J(K)$ and thanks to Proposition 5.1.0.1 we can multiply c_1 (resp. c_2) by elements in the set $K'^\times U_{\mathfrak{a}}(O_{K'})$ (resp. $K^\times U_8(O_K)$) without any change.
So beginning with the given pair (c_1, c_2), we shall construct a tame tetrahedral extension N/K, which shall represent the given class.
The first intermediate step to take is to link the given pair with a cyclic extension E/K of degree 3.

Existence of a suitable cyclic subextension E/K and its resolvents

Following the description of A_4 given in the previous chapter, we have that the quotient A_4/Δ is the cyclic group C_3 of order 3. Moreover, for the cyclic group C_3, the modified Hom-description gives

$$Cl^\circ(O_K[C_3]) \cong \frac{J(K')}{K'^\times \mathrm{Det}^\circ\left(U\left(O_K[C_3]\right)\right)}.$$

Thanks to the fact that the cyclic group is abelian (so we can use the results of McCulloh) and the fact that the Stickelberger ideal in $\mathbb{Z}[\mathrm{Aut}(C_3)]$ is the whole $\mathbb{Z}[\mathrm{Aut}(C_3)]$, we have that $R(O_K[C_3]) = Cl^\circ(O_K[C_3])$. Thus, using Theorem 5.1 in [McC83], we can find a tame cyclic extension E/K, ramified in at least one place, for which the class $(O_E) \in Cl^\circ(O_K[C_3])$ is represented exactly by the given $c_1 \in J(K')$. From now on the cyclic extension E/K will be fixed.

We will now use the Hom-description modified for the augmentation kernel to give a representative for the class (O_E) in terms of resolvents. To do it we need to choose a normal basis generator c'' and some local normal integral basis generators ${c'}_{\mathfrak{v}}$ for the extension E/K.

Since E/K is tame (so the ring of integers is locally free), for any place $\mathfrak{v}$ we take a local normal integral basis generator $c_{\mathfrak{v}} \in O_{E,\,\mathfrak{v}}$.

For each place not above 2, we want to modify $c_{\mathfrak{v}}$ in order to have the trace equal to 1. To do it it'sufficient to take ${c'}_{\mathfrak{v}} = c_{\mathfrak{v}} \left(\mathrm{Tr}_{E_{\mathfrak{v}}/K_{\mathfrak{v}}}(c_{\mathfrak{v}})\right)^{-1}$, indeed it remains a local normal integral basis generator but with local trace equal to 1 (thanks to the linear properties of the trace map):

$$O_{E,\,\mathfrak{v}} = O_{K,\,\mathfrak{v}}[C_3]{c'}_{\mathfrak{v}} \;\text{ and }\; \mathrm{Tr}_{E_{\mathfrak{v}}/K_{\mathfrak{v}}}({c'}_{\mathfrak{v}}) = 1.$$

For all the places over 2 (they are a finite number) instead, we consider an element $c' \in E$ closed to $c_{\mathfrak{v}}$, such that c' is a local normal integral basis generator at these places (it can be found since we only require a finite number of conditions to solve). If we set $c'' = c' \left(\mathrm{Tr}_{E/K}(c')\right)^{-1}$ and ${c'}_{\mathfrak{v}} = c''$ for al these finite $\mathfrak{v}$ over 2 we still have

$$O_{E,\,\mathfrak{v}} = O_{K,\,\mathfrak{v}}[C_3]{c'}_{\mathfrak{v}} \;\text{ and }\; \mathrm{Tr}_{E_{\mathfrak{v}}/K_{\mathfrak{v}}}({c'}_{\mathfrak{v}}) = 1,$$

while in the global sense we obtain (since a linearly independent set of elements in the local field is still linearly independent passing to the global field)

$$E = K[C_3]c'' \;\text{ and }\; \mathrm{Tr}_{E/K}(c'') = 1;$$

as wanted.

We can now express the representative in terms of the resolvents, distinguishing the two possible situations which depend on the "position" of ω respect to K. Following the modified Hom-description, the class (O_E) is then represented in $Cl^{\circ}(O_K[C_3])$ by the idele $c_1' \in J(K')$ given by

$$c_1' = \begin{cases} \left(\frac{(({c'}_{\mathfrak{v}}|\chi_1))_{\mathfrak{v}}}{(c''|\chi_1)}, \frac{\left(({c'}_{\mathfrak{v}}|\chi_1^2)\right)_{\mathfrak{v}}}{(c''|\chi_1^2)} \right) & \text{if } \omega \in K, \\ \left(\frac{(({c'}_{\mathfrak{v}}|\chi_1))_{\mathfrak{v}}}{(c''|\chi_1)} \right) & \text{if } \omega \notin K; \end{cases} \tag{5.5.1}$$

where χ_1 and χ_1^2 are the two nontrivial characters of dimension 1 over K; indeed we can recall that, depending on whether ω belongs or not to K, we have two or only one nontrivial 1-dimensional character over K.

If we are able to prove that instead of the given c_1 we can take this particular c_1', we shall have that, from the definitions set above, all the components for the place over 2 are trivial (equal to 1). The following Proposition will help us in this direction.

Proposition 5.5.1.1. *Given the pair (c_1, c_2) and the idele c_1' defined as above, there exists an idele $c_2' \in J(K)$, such that the pair (c_1', c_2') represents the same class in $Cl^{\circ}(O_K[\Gamma])$ as (c_1, c_2).*

Proof. Since (O_E) is represented by both c_1 and c_1', using the modified Hom-description in the case of the cyclic group C_3, we obtain

$$c_1^{-1}c_1' = k\left(\mathrm{Det}(\alpha_{\mathfrak{v}})\right)_{\mathfrak{v}},$$

with $k \in {K'}^{\times}$ and $\alpha_{\mathfrak{v}} \in O_{K,\mathfrak{v}}[C_3]^{\times}$ such that $\mathrm{Det}(\alpha_{\mathfrak{v}})(\chi_0) = 1$. If we lift any local element $\alpha_{\mathfrak{v}}$ from the cyclic situation to the general Γ situation, we have

$$\alpha_{\mathfrak{v}} = a_{0\mathfrak{v}} + a_{1\mathfrak{v}}\sigma + a_{2\mathfrak{v}}\sigma^2 \in O_{K_{\mathfrak{v}}}[\Gamma]^{\times};$$

where with σ we denote even the lift of the generator of the cyclic group C_3. Then the determinant applied to this element with the 1-dimensional characters remains the same and we find $\epsilon \in J(K)$ such that

$$(c_1^{-1}c_1', \epsilon) = (k, 1)\mathrm{Det}\left((\alpha_{\mathfrak{v}})_{\mathfrak{v}}\right) \in ({K'}^{\times} \times K^{\times})\mathrm{Det}^{\circ}\left(U(O_K[\Gamma])\right) \subset J(K') \times J(K).$$

Thus we can multiply (c_1, c_2) by this last pair without any change, obtaining the equality inside class group

$$(c_1, c_2) = (c_1, c_2)(c_1^{-1}c_2', \epsilon) = (c_1', c_2\epsilon) = (c_1', c_2'),$$

which gives us the proof. □

Thus from now on we can assume that c_1 *is represented by* (5.5.1), in particular we have all the components $c_{1\mathfrak{v}}$ relative to the places over 2 equal to 1.

Once we have the cyclic extension E/K, we would embed it in a tame tetrahedral extension N/K, using the embedding result given by Lemma 5.2.1.

Embedding of E/K in a tame tetrahedral extension N/K

Exactly as we have already done, we would use Lemma 5.2.1 in the previous section to embed E/K in a tame tetrahedral extension N/K. In order to succeed we need an element $n \in E$ which is not a square but such that its norm over K is a square in K. Once we have it, then $N = E\left(\sqrt{n}, \sqrt{\sigma(n)}\right)$ will be the extension of K required. Before finding explicitly the element n, we go on assuming we have this extension N/K and we will see what we will require from the definition of n.

If we consider the extension $N = E\left(\sqrt{n}, \sqrt{\sigma(n)}\right)$, we find the second component in the Hom-description, computing the representative homomorphism on the character χ_2. The value $f(\chi_2)$ is given by Lemma 5.3.1 and, thanks to the remark immediately after it, we have

$$f(\chi_2) = e(E_{\mathfrak{v}}/K_{\mathfrak{v}})\mathrm{N}_{E/K}\left(\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}}\right)\frac{\phi(\lambda)}{\phi(\lambda_{\mathfrak{v}})}; \tag{5.5.2}$$

where we use the same notation of the Lemma.

Remark 5.5.2. *Up to now we haven't use any congruence condition to develop the problem, but at this moment we see from the formula above the presence of a so called "tension" between the different elements involved, indeed we have that the elements λ and $\lambda_{\mathfrak{v}}$ are linked to the normal basis generators and to the local normal integral ones of the different extensions considered.*

We proceed now making some remarks about the element $e(E_{\mathfrak{v}}/K_{\mathfrak{v}})$. From its definition we immediately observe that the content of the idele $\left(e(E_{\mathfrak{v}}/K_{\mathfrak{v}})^2\right)_{\mathfrak{v}}$ is the discriminant ideal $\Delta(E/K)$. Now the discriminant ideal $\Delta(E/K)$ is a square of an ideal $\sqrt{\Delta(E/K)}$ of O_K; this follows from the fact that the order of E/K is 3 and from the well-known result on the valuation of the different (look at [Ser79], Prop. 4 chap. 4).

Thus we can rewrite (5.5.2) as

$$f(\chi_2) = \sqrt{\Delta(E/K)}\,\mathrm{N}_{E/K}\left(\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}}\right)\frac{\phi(\lambda)}{\phi(\lambda_{\mathfrak{v}})}. \tag{5.5.3}$$

Since to solve the problem we would obtain $f(\chi_2) = c_2$, we are lead, by the "morphology" of the previous equation, to write $\frac{\sqrt{\Delta(E/K)}}{c_2}$ as the norm of a class. In order to do it we recall that if an extension E/K contains no unramified subextensions, then the norm map $Cl(E) \longrightarrow Cl(K)$ is surjective ([Was96] Theorem 10.1) and, generalizing this results to the ray class group, we also get a surjection between $Cl_8(O_E)$ and $Cl_8(O_K)$. Since E/K in our case is ramified at some place of K, then we can take $\mathfrak{b}$ a ray class in $Cl_8(O_E)$ such that $\left(\mathrm{N}_{E/K}(\mathfrak{b})\right) = \left(\sqrt{\Delta(E/K)}\right)(c_2)^{-1}$ in $Cl_8(O_K)$; where with (c_2) we denote the class related to the idele c_2.

To link the extension N/K and this class $\mathfrak{b}$, we make use now of the Tchebotarev density Theorem for ray class groups, which gives us the following Lemma.

Lemma 5.5.3. *We can find two ideals $\mathfrak{q}_1$, $\mathfrak{q}_2$ of O_E, such that*

- *they are totally split over K and above different ideals in O_K,*
- *$\mathfrak{q}_1$ is in the same class $\mathfrak{b}$ of $Cl_8(O_E)$,*
- *$\mathfrak{q}_2$ is in the same class as $\mathfrak{q}_1^{-1-\sigma}$ in $Cl_{64}(O_E)$.*

The first condition of the Lemma gives us the element n which we were looking for to obtain the tetrahedral extension N/K. Indeed, using even the third condition, we have

$$\mathfrak{q}_1^{1+\sigma}\mathfrak{q}_2 = mO_E,$$

with $m \equiv 1(\mathrm{mod}^\star 64O_E)$ and if we put $n := m\sigma(m)$, we easily see that its norm over K is the square of $\mathrm{N}_{E/K}(m)$ and it's not a square in E since

$$nO_E = (\mathfrak{q}_1^{1+\sigma}\mathfrak{q}_2)^{1+\sigma} = (\mathfrak{q}_1^{\sigma})^2\mathfrak{q}_1^{1+\sigma^2}\mathfrak{q}_2^{1+\sigma} \tag{5.5.4}$$

and $\mathfrak{q}_1$, $\mathfrak{q}_1^{\sigma^2}$, $\mathfrak{q}_2$, $\mathfrak{q}_1^{\sigma}$ are distinct prime ideals in O_E (because $\mathfrak{q}_1, \mathfrak{q}_2$ are totally split over K and above different ideals in O_K).

The second condition of the Lemma instead gives us the linking with the class $\mathfrak{b}$, indeed we have

$$\left(\mathrm{N}_{E/K}(\mathfrak{q}_1)\right) = \left(\sqrt{\Delta(E/K)}\right)(c_2)^{-1}. \tag{5.5.5}$$

Remark 5.5.4. *From the ramification Theory in a biquadratic extension and from the fact that*

$$n \equiv 1(mod^{\star} 64 O_E),$$

it follows that the tetrahedral extension N/K is tamely ramified and that all places of E over 2 split completely in N.

In order to prove that the extension N/K is exactly the one needed to prove the main Theorem, we have to analyze the resolvents for N/K; but to get it, first of all we need them for N/E.
This is the very clever and technical part of the solution, we find explicitly the basis generator η and $\eta_{\mathfrak{v}}$, in order to have a "good" result computing

$$\mathrm{N}_{E/K}\left(\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}}\right).$$

More precisely we will show the following Lemma.

Lemma 5.5.5. *The idele of E given by*

$$\frac{\left((\eta_{\mathfrak{v}}|\phi)_{N/E}\right)_{\mathfrak{v}}}{(\eta|\phi)_{N/E}}$$

has content $(\mathfrak{q}_1^{\sigma})^{-1}$.

5.5.6 The extension N/E and its resolvents

The biquadratic extension N/E, as explained above from the immersion problem, has the Galois group which is isomorphic to the group Δ of order 4 ($\cong C_2 \times C_2$, where C_2 is the cyclic group of order 2).
We have the following easy Proposition on the structure of the group algebra $K[\Delta]$.

Proposition 5.5.6.1. *The group algebra $K[\Delta]$ contains the following idempotent elements which are orthogonal in pairs:*

$$\begin{aligned}
e_0 &= \frac{1}{4}(1+x+y+xy),\\
e_1 &= \frac{1}{4}(1+x-y-xy),\\
e_2 &= \frac{1}{4}(1-x+y-xy),\\
e_3 &= \frac{1}{4}(1-x-y+xy).
\end{aligned}$$

Moreover the element

$$\eta = \frac{1}{4}\left(1+\sqrt{n}\right)\left(1+\sqrt{\sigma(n)}\right)$$

is a normal basis generator for the extension N/E.

Proof. We just verify that $e_0^2 = e_0$ and that $e_0 \cdot e_1 = 0$, the other controls are exactly analogous. Just using the fact that $x^2 = y^2 = 1$ and $xy = yx$, we have

$$\begin{aligned} e_0 \cdot e_0 &= \frac{1}{16}(4 + 4x + 4y + 4xy) = e_0, \\ e_0 \cdot e_1 &= \frac{1}{16}(1 + x + y + xy + x + x^2 + xy + x^2y - y - yx - y^2 - xy^2 - xy - x^2y - xy^2 - x^2y^2) \\ &= 0. \end{aligned}$$

Assuming that x (resp. y) corresponds to the element of $\mathrm{Gal}(N/E)$ fixing $\sqrt{n}$ $\left(\text{resp. } \sqrt{\sigma(n)}\right)$, we calculate how the idempotents act on η:

$$\begin{aligned} e_0\eta &= \frac{1}{4}, \\ e_1\eta &= \frac{1}{4}\sqrt{n}, \\ e_2\eta &= \frac{1}{4}\sqrt{\sigma(n)}, \\ e_3\eta &= \frac{1}{4}\sqrt{n\sigma(n)}. \end{aligned}$$

From that, the second assertion of the Proposition easily follows. □

We will now get from η a set of local normal integral basis generators for any place $\mathfrak{v}$, in order to calculate the resolvents of the extension N/E which are of our interest.

For all places above 2 we have no problems, because, since $n \equiv \sigma(n) \equiv 1(\mathrm{mod}^\star 4O_E)$ by the last remark in the previous section, η is also a local normal integral basis generator for all the places above 2.

For all the other places of E we will specify case by case the local normal integral basis generator. From (5.5.4) we also get

$$\begin{aligned} \sigma(n)O_E &= (\mathfrak{q}_1^{\sigma^2})^2\mathfrak{q}_1^{\sigma+1}\mathfrak{q}_2^{\sigma+\sigma^2}, \\ n\sigma(n)O_E &= (\mathfrak{q}_1^{1+\sigma+\sigma^2})^2\mathfrak{q}_1^{\sigma+\sigma^2}\mathfrak{q}_2^{1+\sigma^2}. \end{aligned} \tag{5.5.6}$$

Thus we obtain the following precise result.

Proposition 5.5.6.2. *For each place $\mathfrak{v}$, fix a uniformizer $\pi(\mathfrak{v})$ of $O_{E,\mathfrak{v}}$, and define*

$$\begin{aligned} \eta_{\mathfrak{q}_1} &= (e_0 + e_1 + e_2 + \pi(\mathfrak{q}_1)^{-1}e_3)\eta, \\ \eta_{\mathfrak{q}_1^\sigma} &= (e_0 + \pi(\mathfrak{q}_1^\sigma)^{-1}e_1 + e_2 + \pi(\mathfrak{q}_1^\sigma)^{-1}e_3)\eta, \\ \eta_{\mathfrak{q}_1^{\sigma^2}} &= (e_0 + e_1 + \pi(\mathfrak{q}_1^{\sigma^2})^{-1}e_2 + \pi(\mathfrak{q}_1^{\sigma^2})^{-1}e_3)\eta, \\ \eta_{\mathfrak{q}_2^\sigma} &= (e_0 + e_1 + e_2 + \pi(\mathfrak{q}_2^\sigma)^{-1}e_3)\eta, \\ \eta_{\mathfrak{v}} &= \eta \ \ \textit{for } \mathfrak{v} \neq \mathfrak{q}_1,\, \mathfrak{q}_1^\sigma,\, \mathfrak{q}_1^{\sigma^2},\, \mathfrak{q}_2^\sigma. \end{aligned}$$

Then we have

$$O_{N,\mathfrak{v}} = O_{E,\mathfrak{v}}[\Delta]\eta_{\mathfrak{v}} \ ,$$

for all the places $\mathfrak{v}$.

We can now compute the resolvents associated to the character ϕ of Δ. Thanks to the fact that the character is 1-dimensional, as explained in the Appendix (A.5.3), we have to compute an usual Lagrange resolvent. Thus we have

$$\begin{aligned}(\eta|\phi)_{N/E} &= \sum_{\delta\in\Delta}\delta(\eta)\phi(\delta^{-1})\\ &= \eta + x(\eta) - y(\eta) - xy(\eta)\\ &= 4e_1\eta\\ &= \sqrt{n},\end{aligned}$$

and locally, in the same way, we get $(\eta_{\mathfrak{v}}|\phi)_{N/E} = 4e_1\eta_{\mathfrak{v}}$, which gives

$$\begin{aligned}(\eta_{\mathfrak{v}}|\phi)_{N/E} &= \sqrt{n} \text{ for all } \mathfrak{v} \neq \mathfrak{q}_1^{\sigma},\\ (\eta_{\mathfrak{q}_1^{\sigma}}|\phi)_{N/E} &= \pi(\mathfrak{q}_1^{\sigma})^{-1}\sqrt{n}.\end{aligned}$$

Thus as a corollary of these computations about the resolvents in N/E, we get the proof of Lemma 5.5.5.

As already done for η and c, it remains now to choose α and $\alpha_{\mathfrak{v}}$, such that they coincide on the places above 2 and such that they allow us to close the circle and prove the main Theorem.

5.5.7 Places not above 2

First of all we set the values $\alpha_{\mathfrak{v}}$ for all the *places not above* 2.
If we consider $\alpha'_{\mathfrak{v}}$ any local normal integral basis generator for the extension N/K, we can use the trace map from N to E to get a local normal integral basis generator for E/K. For the extension E/K we have already considered as local normal integral basis generator the element $c_{\mathfrak{v}}$, so these two elements differ for a unit; explicitly

$$c_{\mathfrak{v}} = k_{\mathfrak{v}}\mathrm{Tr}_{N_{\mathfrak{v}}/E_{\mathfrak{v}}}(\alpha'_{\mathfrak{v}})$$

with $k_{\mathfrak{v}} \in O_{K,\mathfrak{v}}[C_3]^{\times}$, which can be lift to the element $\overline{k_{\mathfrak{v}}} \in O_{K,\mathfrak{v}}[\Gamma]^{\times}$.
Setting $k'_{\mathfrak{v}} = \overline{k_{\mathfrak{v}}}e_0 + (1-e_0) \in O_{K,\mathfrak{v}}[\Gamma]^{\times}$ and $\alpha_{\mathfrak{v}} = k'_{\mathfrak{v}}\alpha'_{\mathfrak{v}}$, we still have a local normal integral basis generator $\alpha_{\mathfrak{v}}$ and we can easily compute the trace from $N_{\mathfrak{v}}$ to $E_{\mathfrak{v}}$:

$$\begin{aligned}\mathrm{Tr}_{N_{\mathfrak{v}}/E_{\mathfrak{v}}}(\alpha_{\mathfrak{v}}) &= (1+x+y+xy)(k'_{\mathfrak{v}}\alpha'_{\mathfrak{v}})\\ &= 4e_0\left(\overline{k_{\mathfrak{v}}}e_0 + (1-e_0)\right)\alpha'_{\mathfrak{v}}\\ &= (4e_0\overline{k_{\mathfrak{v}}}e_0 + 4e_0 - 4e_0)\alpha'_{\mathfrak{v}}\\ &= k_{\mathfrak{v}}\mathrm{Tr}_{N_{\mathfrak{v}}/E_{\mathfrak{v}}}(\alpha'_{\mathfrak{v}})\\ &= c_{\mathfrak{v}}. \qquad (5.5.7)\end{aligned}$$

From this and using the fact that $c_{\mathfrak{v}}$ has trace 1, we deduce that

$$\mathrm{Tr}_{N_{\mathfrak{v}}/K_{\mathfrak{v}}}(\alpha_{\mathfrak{v}}) = \mathrm{Tr}_{E_{\mathfrak{v}}/K_{\mathfrak{v}}}(c_{\mathfrak{v}}) = 1.$$

We can concentrate now on the places above 2.

5.5.8 Places above 2

First of all we start remarking that, since any place above 2 splits completely in N/E, we have $N_2 \cong E_2^4$ as Galois algebras over K_2 and in particular the isomorphism is given by

$$z \longrightarrow (z, y(z), x(z), yx(z))\,.$$

Thanks to this isomorphism, we identify $O_{N,\,2}$ with $O_{E,\,2}^4$ and we have

$$\begin{aligned} y(z_1,z_2,z_3,z_4) &= (z_2,z_1,z_4,z_3),\\ x(z_1,z_2,z_3,z_4) &= (z_3,z_4,z_1,z_2),\\ \sigma(z_1,z_2,z_3,z_4) &= (\sigma(z_1),\sigma(z_4),\sigma(z_2),\sigma(z_3))\,. \end{aligned} \tag{5.5.8}$$

Now considering the elements β' and α' in N_2 defined as follows

$$\beta' = (1,0,0,0), \quad \alpha' = c\beta' = (c,0,0,0),$$

we have that they are local normal integral basis generators for N/E and N/K respectively at all places above 2 (indeed looking at the action of the element in Γ we understand that they generate a normal basis) and moreover $\mathrm{Tr}_{N/E}(\beta') = 1$ (since computing the trace we get $(1,1,1,1) = 1$).

We now want to get from this local elements an element $\alpha \in N$ which is a local normal integral basis generator for N/K at all places above 2; to do it we shall use the already quoted Nakayama's Lemma.

If we take an element $\beta \in N$, so that

$$\beta \equiv \beta' (\mathrm{mod} 8 O_{N_2}), \quad \mathrm{Tr}_{N/E}(\beta) = 1,$$

and an element $\alpha = c\beta$; then we get

$$O_{K,\,2}[\Gamma]\alpha + 8O_{N,\,2} = O_{K,\,2}[\Gamma]\alpha' + 8O_{N,\,2} = O_{N,\,2}.$$

Applying now the Nakayama's Lemma we obtain that α is a local normal integral basis generator at all places above 2, since the Lemma says that $O_{N,\,2} = O_{K,\,2}[\Gamma]\alpha$. In the same way one can verify that β at these places is a local normal integral basis generator for N/E.

Moreover we have that the trace takes value 1 since

$$\mathrm{Tr}_{N/K}(\alpha) = \mathrm{Tr}_{E/K}\left(\mathrm{Tr}_{N/E}(\alpha)\right) = \mathrm{Tr}_{E/K}\left(c\,\mathrm{Tr}_{N/E}(\beta)\right) = \mathrm{Tr}_{E/K}(c) = 1.$$

Finally we consider this α as the normal basis generator for N/K we need (it's a normal basis generator, since it's a local one at the places above 2). For all the places $\mathfrak{v}$ above 2 we consider

$$\alpha_{\mathfrak{v}} = \alpha, \quad \lambda_{\mathfrak{v}} = \lambda, \quad e(E_{\mathfrak{v}}/K_{\mathfrak{v}}) = e(E/K),$$

where λ and $e(E/K)$ are defined by (5.3.1). In these places we have $\alpha_{\mathfrak{v}}$ local normal integral basis generator and $c_{\mathfrak{v}} = c$.

5.5.9 Investigation of λ

If we consider the normal integral basis generator α set above and the local ones $\alpha_{\mathfrak{v}}$, we have the following Proposition on the element λ defined by (5.3.5).

Proposition 5.5.9.1. *The element λ defined by (5.3.5) satisfies the following congruence*

$$\lambda \equiv 1(mod\ 8O_{K,2}[\Delta]).$$

Proof. Both η and β' are local normal integral basis generator for N/E above 2 and so they differ by a unit $\mu' \in O_{E,2}[\Delta]^{\times}$, obtaining

$$\beta' = \mu'\eta.$$

Since we have that $n \equiv 1(\text{mod}^{\star}\, 64O_E)$, we can find an element $f \in O_{E,2}$ with $f \equiv 1(\text{mod } 32O_{E,2})$ and $f^2 = n$. Using the previous isomorphism $O_{N,2} \cong O_{E,2}^4$, we can write

$$\begin{aligned} \sqrt{n} &= (f, -f, f, -f), \\ \sqrt{\sigma(n)} &= (\sigma(f), \sigma(f), -\sigma(f), -\sigma(f)) \,. \end{aligned}$$

Thus using the computation we have done in the proof of Prop. 5.5.6.1, we get

$$\begin{aligned} e_0\eta &= \frac{1}{4}(1,1,1,1), \\ e_1\eta &= \frac{1}{4}(f,-f,f,-f), \\ e_2\eta &= \frac{1}{4}\left(\sigma(f), \sigma(f), -\sigma(f), -\sigma(f)\right), \\ e_3\eta &= \frac{1}{4}\left(f\sigma(f), -f\sigma(f), -f\sigma(f), f\sigma(f)\right). \end{aligned}$$

If we consider $\beta' = (1,0,0,0)$, then we can write it as

$$\beta' = e_0\eta + \frac{e_1\eta}{f} + \frac{e_2\eta}{\sigma(f)} + \frac{e_3\eta}{f\sigma(f)}$$

and, since $f \equiv \sigma(f) \equiv 1(\text{mod } 32O_{E,2})$, we obtain

$$\mu' = e_0 + \frac{e_1}{f} + \frac{e_2}{\sigma(f)} + \frac{e_3}{f\sigma(f)} \equiv 1(\text{mod } 8O_{E,2}[\Delta]).$$

We know that $\beta \equiv \beta'(\text{mod}8O_{N,2})$ and so from $\beta' = \mu'\eta$ we get

$$\beta \equiv \eta(\text{mod } 8O_{N,2}).$$

Since $\sigma(\beta) \equiv \sigma(\beta') = \beta' \equiv \beta(\text{mod } 8O_{N,2})$, we have from the equality $\alpha = c\beta$ that

$$\sigma^j(c)\beta \equiv \sigma^j(c)\sigma^j(\beta) = \sigma^j(\alpha)(\text{mod } 8O_{N,2}) \quad \text{for } 0 \le j \le 2$$

and consequently

$$\sigma^j(c)\eta \equiv \sigma^j(\alpha)(\text{mod } 8O_{N,2}) \quad \text{for } 0 \le j \le 2.$$

So the matrix which defines λ is congruent to the identity modulo $8O_{K,2}[\Delta]$ and hence its determinant λ is congruent to $1(\text{mod } 8O_{K,2}[\Delta])$; as we wanted to prove. □

5.5.10 From the resolvents' quotients to the new idele y'

In order to obtain the proof of the main Theorem we now prove the following Lemma using formula (5.5.3).

Lemma 5.5.11. *The idele $c_2' = f(\chi_2) = \frac{\left((\alpha_{\mathfrak{v}}|\chi_2)_{N/K}\right)_{\mathfrak{v}}}{(\alpha|\chi_2)_{N/K}} \in J(K)$ determines the same class in $Cl_8(O_K)$ as c_2.*

Proof. By Proposition 5.5.9.1 we have that $\frac{\phi(\lambda)}{(\phi(\lambda_{\mathfrak{v}}))_{\mathfrak{v}}} \in K^{\times} U_8(O_K)$, so we can "erase" this factor in (5.5.3). Moreover from Lemma 5.5.5 we have

$$\mathrm{N}_{E/K}\left(\frac{\left((\eta_{\mathfrak{v}}|\phi)_{N/E}\right)_{\mathfrak{v}}}{(\eta|\phi)_{N/E}}\right) = \mathrm{N}_{E/K}\left((\mathfrak{q}_1^{-1})^{\sigma}\right) = \mathrm{N}_{E/K}\left(\mathfrak{q}_1^{-1}\right).$$

So concluding c_2' determines in $Cl_8(O_K)$ the same class of $\mathrm{N}_{E/K}(\mathfrak{q}_1)^{-1}\sqrt{\Delta(E/K)}$, which by (5.5.5) is exactly the class determined by c_2. □

Remark 5.5.12 (Places above 2)**.** *We understand here the reason why we have always distinguished the places above 2. In order to prove that $\frac{\phi(\lambda)}{(\phi(\lambda_{\mathfrak{v}}))_{\mathfrak{v}}} \in K^{\times} U_8(O_K)$, the only places $\mathfrak{v}$ which can give some "problems" are the places above 2, this follows from the definition of $U_8(O_K)$ and in particular from the need for a specific investigation of the places above the only prime divisor of 8, which is 2.*

5.5.13 Proof of the main Theorem

We can now use all the results we achieved in order to exhibit the inclusion requested by the proof of the main Theorem. In particular we want to show that the class (O_N) (where N/K is the extension constructed above) in $Cl^{\circ}(O_K[\Gamma])$ is the same of the class represented by the given pair $(c_1, c_2) \in J(K') \times J(K)$.

First of all we have

$$\begin{aligned}(\alpha|\chi_0)_{N/K} &= \mathrm{Tr}_{N/K}(\alpha) = 1,\\ (\alpha_{\mathfrak{v}}|\chi_0)_{N/K} &= \mathrm{Tr}_{N_{\mathfrak{v}}/K_{\mathfrak{v}}}(\alpha_{\mathfrak{v}}) = 1 \text{ for all } \mathfrak{v};\end{aligned}$$

so we can use the normal basis generator α and the local normal integral basis generators $\alpha_{\mathfrak{v}}$ in computing the quotients of resolvents which give the class (O_N).
In particular the class (O_N) is represented by the couple (c_1', c_2'), where c_1' comes from the resolvents with the non trivial 1-dimensional characters; while c_2' is defined by Lemma 5.5.11.
Remembering that in function of the "position" of ω respect to K we have one 1-dimensional character χ_1 (if $\omega \notin K$) or two 1-dimensional characters χ_1 and χ_1^2 (if $\omega \in K$), we can compute the resolvents, restricting ourself on the extension E/K, in the following way:

$$\begin{aligned}(\alpha|\chi_1^i)_{N/K} &= (\mathrm{Tr}_{N/E}(\alpha)|\overline{\chi_1^i})_{E/K} = (c''|\overline{\chi_1^i})_{E/K},\\ (\alpha_{\mathfrak{v}}|\chi_1^i)_{N/K} &= (\mathrm{Tr}_{N_{\mathfrak{v}}/E_{\mathfrak{v}}}(\alpha_{\mathfrak{v}})|\overline{\chi_1^i})_{E/K} = (c'_{\mathfrak{v}}|\overline{\chi_1^i})_{E/K},\end{aligned}$$

where $i = 1, 2$ and $\overline{\chi_1^i}$ means the restriction of the character to E/K.
So it follows that c_1' is given by (5.5.1) and we have $c_1' = c_1$ by the result of Proposition 5.5.1.1.

Thus we have that the class (O_N) is represented by the couple (c_1, c_2'). But we know that c_2 and c_2' are in the same class in $Cl_8(O_K)$ by Lemma 5.5.11 and so we have the desired result that (c_1, c_2') and (c_1, c_2) represent the same class in $Cl^\circ(O_K[\Gamma])$, proving the inclusion $Cl^\circ(O_K[\Gamma]) \subseteq R(O_K[\Gamma])$.

5.6 Conclusion and final comparison between the two approaches

As a conclusion of this chapter and even of the whole work, we can retrace and underline the similarities and the differences between the two approaches.

First of all we have seen that, in both the two works, we start linking to the abelian case of C_3. This comes from the structure of the group A_4 which has the cyclic group as a direct factor. The abelian case C_3 is "comfortable" thanks to the cited works by McCulloh which erase any doubt in an abelian situation.

Thus given the cyclic extension E/K, we would then embed it in a tetrahedral extension whose class represents the given element in $Cl(O_K)$.
The embedding of E/K is not so difficult using Lemma 5.2.1, but the arduousness comes when we want to look at the component in the Hom-description which derives from the 3-dimensional character χ_2.
In particular we get the formula

$$f(\chi_2) = \left(\frac{e(E_{\mathfrak{v}}/K_{\mathfrak{v}})}{e(E/K)} \mathrm{N}_{E/K} \left(\frac{(\eta_{\mathfrak{v}}|\phi)_{N/E}}{(\eta|\phi)_{N/E}} \right) \frac{\phi(\lambda)}{\phi(\lambda_{\mathfrak{v}})} \right).$$

It's exactly here that the main difference between the two approaches arises when we try to treat and handle this formula.

In the case over the maximal order $\mathcal{M}$ we have already remarked that the formula simplifies because we can ignore the term with λ and $\lambda_{\mathfrak{v}}$. So, after this simplification, the use of the Steinitz classes, with some assumption on the base field K, leads to the solution of the problem, giving us the desired tetrahedral extension.

Contrarily in the refinement of the previous result, we have no more a simplification on the previous formula and we need to consider also the factors depending on λ and $\lambda_{\mathfrak{v}}$. In order to do it, we have seen that in this approach we need to find particular normal basis generators and normal integral basis generators for the different extensions involved. Once we have it, using the modified ray class group, the conclusion is not so far.

5.7 Open questions

Had we more time, we would have liked to tackle the following problems:

The first question which arises after this chapter is: *how can we deduce from the result $R(O_K A_4) = Cl^\circ(O_K A_4)$ in [BS05b] the equality $R(\mathcal{M}) = Cl^\circ(\mathcal{M})$, reached in [GS03]*?

As we have seen in the case of A_4, we get that the set of realizable classes coincides exactly with the augmentation kernel; while in his work [McC87], McCulloh proved that $R(O_K\Gamma) = \ker(Rag')$ for Γ abelian and in general he proved, in an unpublished work, that $R(O_K\Gamma) \subseteq \ker(Rag')$ for any group Γ (not necessarily abelian). *It would be interesting to link the sets $Cl^\circ(O_K\Gamma)$ and ker(Rag')* in order to know when we have an equality between them. For example in the case of $\Gamma = A_4$, it's possible to prove that $Cl^\circ(O_K A_4) = \ker(Rag')$.

It would be also inspiring to understand just the existence of a solution to the problem of finding an extension which gives the given class, before discovering it explicitly as done in the case of A_4.

Another desire which arises after our work is to know how the tame extensions are distributed among the realizable classes. In order to answer this question, we have already cited the quantitative results in the Introduction which go in this direction, but *is it also possible to give a strictly algebraic interpretation and answer to this question*?

The further step after this work, would be *to reach a sort of general and axiomatic context* under which we have the proof of the fact that the set of realizable classes forms a subgroup (we can observe that the works [GS06] and [BS08] cited in section 0.2.3 of the Introduction, under some points of view, go in this direction). For example, it would be interesting to find a result on $R(O_K\Gamma)$ analogous to the one reached for A_4, when we consider the set of groups treated in [BS08], namely $\Gamma = (\mathbb{F}_p)^r \rtimes C_{p^r-1}$.

In this final section, we can also mention some recent results on Steinitz Classes, reached by A. Cobbe. As done for the set of realizable classes, using Steinitz classes, one can also define $R_t(K,\Gamma)$ as the set of classes which are Steinitz classes of a tamely ramified Γ-extension of K. It is conjectured that this set is always a group, while this is not true in the wildly ramified case. A. Cobbe, in his work [Cob10] and in his preprints available at his website, proved the conjecture for a large set of groups Γ.
Using the augmentation map defined in the introduction, it is possible to link the set of realizable classes of our interest with the set of realizable Steinitz classes and *it would be inspiring to catch some information for our work from these recent results on Steinitz classes.*

Finally, to solve the case of A_4 we always used field extensions, *how can the problem (and also the solution) change if we consider Galois algebras and not only fields*?

Appendix A

Algebraic Techniques

In this appendix we recall some algebraic techniques and definitions which are useful along our work. In particular we shall explain the fundamental Hom-description of the class group given by Fröhlich.

A.1 Locally free modules

All our efforts start from the fact that given a tame Galois extension N/K, the ring of integers O_N is a locally free $O_K[\Gamma]$-module; where Γ is the Galois group of the extension. Let's recall better the definition of locally free module.

Definition A.1.1 (Locally free module)**.** *Given a ring R and an R-order $\mathfrak{U}$, a* locally free *$\mathfrak{U}$-module X is a finitely generated $\mathfrak{U}$-module so that the $\mathfrak{U}_{\mathfrak{v}}$-module $X_{\mathfrak{v}}$ is free, for all prime divisors $\mathfrak{v}$ of R.*

So in our case the fact that O_N is a locally free $O_K[\Gamma]$-module means that, for any place $\mathfrak{v}$ of K it exists an element $\alpha_{\mathfrak{v}} \in O_N$ such that

$$O_{N_{\mathfrak{v}}} = O_{K_{\mathfrak{v}}}[\Gamma]\alpha_{\mathfrak{v}}.$$

The element $\alpha_{\mathfrak{v}}$ is called a local normal integral basis generator and this condition holds for any tame extension thanks to the already cited Noether's Criterion.

A.2 Presentation of the group Γ and its characters

The starting point for all our work is to find the irreducible representations of the group Γ and its characters over a not algebrically closed field K (the so called rationality question).

When we are looking for irreducible representations over $\mathbb{C}$, everything is simpler and well explained in the first section of [Ser77]. The situation becomes harder when we pass to the field K. After a general overview of the basic results over $\mathbb{C}$, we will try to give an idea of the passage to K, which will be of fundamental importance for the following sections.
After this general explanation, we shall give some non abelian examples, following the cases treated

by B. Sodaïgui in the articles cited in the Introduction.

For the definitions of linear representations, irreducible representations and characters we refer to the already cited work of Serre; here we just recall the basic tools to discover the number of irreducible representations of Γ over $\mathbb{C}$ and its characters' table.

Given a group Γ of order g, we have a number of irreducible representations over $\mathbb{C}$ equal to the number of conjugacy classes of Γ and in particular we have the formula

$$\sum n_i^2 = g,$$

where n_i is the dimension of the different irreducible representations, which allows us to discover the dimension of the different irreducible representations over $\mathbb{C}$.
A characters is associated to any of these representations and, defined the scalar product in the set of characters

$$(\phi|\psi) = \frac{1}{g}\sum_{\gamma\in\Gamma}\phi(\gamma)\overline{\psi(\gamma)},$$

we have that a representation V with character ϕ is irreducible if and only if $(\phi|\phi) = 1$; while given two characters χ and χ' of two non isomorphic irreducible representations, we have the orthogonality relation $(\chi|\chi') = 0$.
While in an abelian group all the irreducible representations are 1-dimensional, in a non abelian case the situation is more complicated but easily solvable thanks to the previous results. Let's give a look to some examples of irreducible representations over $\mathbb{C}$.

D_{2n} with focus on D_4

This group is the group of rotations and reflections of the plane which preserve a regular polygon with $2n$ vertices. In particular we have $2n$ rotations (r^k with $0 \leq k \leq 2n-1$ and r the rotation of angle π/n) and $2n$ reflections, telling us that the order of the group is $4n$. Given any reflection s, any element can be uniquely written either as r^k with $0 \leq k \leq 2n-1$ or as sr^k with $0 \leq k \leq 2n-1$; where s and r are linked by the relation $srs = r^{-1}$.
For any of this group we have 4 one dimensional representations, obtained letting ±1 corresponding to r and s in all possible ways, and $n-1$ representations of dimension 2.

In the particular case of D_4 (the group of rotations and reflections of the plane preserving a square), we have 5 conjugacy classes and so, after the always present four 1-dimensional representations, we have the following 2-dimensional representation

$$r \longrightarrow \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad sr \longrightarrow \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

So for D_4 we have 5 characters, represented in the following table:

	1	r	r^2	s	sr
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	-1	1	1	-1
χ_3	1	-1	1	-1	1
χ_4	2	0	-2	0	0

The Alternating Group A_4

The alternating group A_4 is the group of all even permutations of a set of four elements $\{a, b, c, d\}$. It can even be considered as the group of rotations in $\mathbb{R}^3$ which stabilize a regular tetrahedron with barycenter the origin.
It contains 12 elements which are:

- the identity element 1,
- 3 elements of order 2: $x = (ab)(cd)$, $y = (ac)(bd)$, $z = (ad)(bc)$,
- 8 elements of order 3: $\sigma = (abc)$, $(acb), \dots,$ (bcd).

If we consider the cyclic subgroup $C_3 = \{1, \sigma, \sigma^2\}$ and the normal subgroup $\Delta = \{1, x, y, z\}$, we have the relations

$$\sigma x \sigma^{-1} = z, \;\; \sigma z \sigma^{-1} = y \;\text{ and }\; \sigma y \sigma^{-1} = x,$$

with $C_3 \cap \Delta = 1$. In particular A_4 is the semidirect product of these two sets,

$$A_4 = \Delta \rtimes C_3.$$

In this group we have 4 conjugacy classes, which are: $\{1\}, \{x, y, z\}, \{\sigma, \sigma x, \sigma y, \sigma z\}, \{\sigma^2, \sigma^2 x, \sigma^2 y, \sigma^2 z\}$; so an equal number of irreducible characters over $\mathbb{C}$. Thanks to the equivalence on the dimensions $12 = n_1^2 + n_2^2 + n_3^2 + n_4^2$, we easily see that we have three 1-dimensional irreducible representations and one 3-dimensional representation over $\mathbb{C}$.
The three 1-dimensional characters χ_0, χ_1, ${\chi_1}'$ derive from the characters of the cyclic C_3 and they are defined by $\chi(\delta \cdot \sigma^k) = \chi(\sigma^k)$. While we can easily understand the character of the 3-dimensional irreducible representation, just using the orthogonal relations on characters.
We give here the characters table:

	1	x	σ	σ^2
χ_0	1	1	1	1
χ_1	1	1	ω	ω^2
${\chi_1}'$	1	1	ω^2	ω
χ_2	3	-1	0	0

where with ω we denote the primitive 3-rd root of unity $e^{\frac{2\pi i}{3}}$.
It's not difficult to prove that the 3-dimensional representation is induced by any non trivial 1-dimensional representation of Δ (for example by ϕ defined as $\phi(1) = \phi(x) = 1$ and $\phi(y) = \phi(z) = -1$), giving $\chi_2 = \mathrm{Ind}_{\Delta}^{A_4} \phi$.

The Symmetric Group S_4

The symmetric group S_4 is the group of all permutations of a set of 4 elements $\{a, b, c, d\}$. It can even be considered as the group of all rigid motions which stabilize a regular tetrahedron.
This groups contains 24 elements, divided into 5 conjugacy classes, which are:

- the identity element 1,
- 6 transpositions: (ab), (ac), (ad), (bc), (bd), (cd),
- 3 elements in A_4 of order 2: $x = (ab)(cd)$, $y = (ac)(bd)$, $z = (ad)(bc)$,
- 8 elements of order 3: (abc), $(acb), \dots$, (bcd),
- 6 elements of order 4: $(abcd)$, $(abdc)$, $(acbd)$, $(acdb)$, $(adbc)$, $(adcb)$.

If we consider the subgroup $H = \{1, x, y, z\}$ and the normal subgroup L of permutations leaving fixed the element d, we can see S_4 as the semidirect product of these two sets:

$$S_4 = L \rtimes H.$$

Each representation of L extends to S_4 just letting the character act trivially on the elements of H ($\chi(l \cdot h) = \chi(l)$); obtaining in this way two 1-dimensional representations and a 2-dimensional one. After that, thanks to the usual formula connecting the order of the group and the dimensions of the irreducible representations, we see that we need two other 3-dimensional representations. One 3-dimensional irreducible representation is the standard representation of S_4, which is the permutation representations of S_4 on $\mathbb{C}^4$ quotient by the trivial subrepresentation; while the other 3-dimensional representation is given by this last one tensor the non trivial representation of dimension one.

Remark A.2.1. *The values of the characters of S_4 are all integers, it's important to note that it can be proved that for any symmetric group we have this property on the characters of irreducible representations.*

We can give now the characters' table of S_4:

	1	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
χ_0	1	1	1	1	1
ϵ	1	-1	1	1	-1
θ	2	0	2	-1	0
ϕ	3	1	-1	0	-1
$\epsilon\phi$	3	-1	-1	0	1

Remark A.2.2. *Since any character has values in an algebraic extension of $\mathbb{Q}$, we can consider any representation over $\mathbb{Q}^c$ instead that over $\mathbb{C}$.*

Once we have the irreducible representations over $\mathbb{C}$ (or over $\mathbb{Q}^c$) of a group Γ, a question arises: how can we deduce from them, the irreducible representations over a not necessarily algebrically closed field K? For the answer we have to look at the Galois group $\mathrm{Gal}(\mathbb{Q}^c/K)$, in particular any orbit of it gives an irreducible character over K (as a reference we can consider section §74 in [CR87]).

So for example, regarding A_4 with the assumption that K is linearly disjoint from $\mathbb{Q}(\omega)$; we have three irreducible characters over K:

- χ_0 the trivial character;
- χ_1 the character of degree 1, which is defined by $\chi_1(\sigma) = \omega$ and $\chi_1(x) = 1$ (so with kernel=Δ);
- χ_2 the character of degree 2, which is defined by: $\chi_2(\sigma) = 0$ and $\chi_2(x) = -1$. It is induced, as explained in the case over $\mathbb{C}$, by a nontrivial character ϕ of Δ: $\chi_2 = \mathrm{Ind}_{\Delta}^{A_4}\phi$.

Remark A.2.3. *In the case that K contains the root of unity ω, we still have the two nontrivial 1-dimensional characters χ_1 and χ_1^2, together with χ_0 and the 3-dimensional one.*

A.3 The semisimple algebra $K[\Gamma]$

Once we know the characters' table of the group we're treating, we would know the structure of the group algebra $K[\Gamma]$ (recall that any element of the group algebra is of the form $\sum_{\gamma\in\Gamma} a_\gamma\gamma$, where $a_\gamma \in K$).
The first important result that we invoke is the famous Maschke's Theorem:

Theorem A.3.1 (Maschke's Theorem)**.** *Given K a field of characteristic not dividing the order $|\Gamma|$, we have that the group algebra associated $K[\Gamma]$ is semisimple.*

For a proof of this result we remand to pag. 43 of Vol. 1 in [CR87].

As a corollary of it we have that $K[\Gamma]$ is a product of matrix algebras over division ring of finite degree over K.
Moreover, when we take K algebraically closed, we have

$$K[\Gamma] \approxeq \prod_{i=1}^{h} \mathrm{M}_{n_i}(K),$$

where h is the number of irreducible representations and n_i is the dimension of each representation.

In our general case, we have that K is of characteristic zero, ensuring us the semisemplicity of the group algebra; but it's not in general algebraically closed, complicating seriously the description of the simple components.

The main result in a not necessarily algebraically closed case makes use of the Schur's Index and can be found in section 74 of [CR87] with a resume at pag. 330 of the same book.

It says that for any K (not necessarily algebraically closed), the group algebra associated to Γ has the following Wedderburn's decomposition:

$$K[\Gamma] \cong \prod_{i=1}^{h} \mathrm{M}_{n_i}(D_i),$$

where D_i is a skewfield (or in other word a division ring) with center $K(\chi_i)$, which is the extension of K obtained by adding to K the values of the correspondent character χ_i; moreover the dimension of D_i over $K(\chi_i)$ is equal to the square of the Schur index m_i^2 relative to K and the dimension of the matrix group n_i is linked with the Schur index thanks to the formula $m_i n_i = \chi_i(1)$.

Remark A.3.2. *We remark that in the* 1*-dimensional case we have* $\chi_i(1) = 1$ *and so necessarily* $m_i = n_i = 1$*. While when a character is realizable over* K*, then the Schur index is equal to* 1 *(indeed the Schur index over* K *is even defined as the smallest positive integer* m *such that there exists an extension* L *of* K *of degree* m *so that the character* χ_i *can be realized over* L*), so in this case we have* n_i *equal to the dimension of the correspondent representation and the respective simple component in the group algebra is* $M_{n_i}(K)$*.*

We can now apply all these considerations to the non abelian groups considered in the previous section. Looking just at the characters' table and thinking about the transposition of characters over a field (not necessarily algebrically closed) K, we obtain the following group algebra decomposition, for any K of characteristic zero:

- $D_4 \longrightarrow$ All the irreducible representations are realizable over K, so we have

$$K[D_4] \cong K^4 \times \mathrm{M}_2(K);$$

- $A_4 \longrightarrow$ Given ω a primitive 3-rd root of unity, if K doesn't contain ω, the non trivial 1-dimensional representation has values in $K(\omega)$, while the 3-dimensional one is realizable over K, so we have

$$K[A_4] \cong K \times K(\omega) \times \mathrm{M}_3(K),$$

  while if K contains ω we have

$$K[A_4] \cong K \times K \times K \times \mathrm{M}_3(K);$$

- $S_4 \longrightarrow$ For any symmetric group, as already remarked, all the irreducible representations are realizable over K; so we have

$$K[S_4] \cong K \times K \times \mathrm{M}_2(K) \times \mathrm{M}_3(K) \times \mathrm{M}_3(K).$$

A.4 The class of a tame Γ-extension

In this section we use the notation of the first three chapters. Thanks to Noether's criterion, we know that if K_h/K is tame, then O_h is locally free as an $O\Gamma$-module and it determines a class (O_h) in the locally free class group $Cl(O\Gamma)$. The aim of this section is to describe (O_h) in the idelic form developed by Fröhlich.

Assuming Γ abelian for simplicity, we define

$$Cl(O\Gamma) = \frac{J(K\Gamma)}{\lambda(K\Gamma^{\times})U(O\Gamma)}, \tag{A.4.1}$$

where $J(K\Gamma)$, the *idele group* of $K\Gamma$, is the restricted product of the groups $(K_{\mathfrak{v}}\Gamma)^{\times}$ with respect to the subgroups $(O_{\mathfrak{v}}\Gamma)^{\times}$ for all primes $\mathfrak{v}$ of K; $U(O\Gamma)$, the group of *unit ideles*, is $\prod_{\mathfrak{v}}(O_{\mathfrak{v}}\Gamma)^{\times}$; and $\lambda(K\Gamma^{\times})$, the group of *principal ideles*, is the image of $K\Gamma^{\times}$ under the canonical embedding $\lambda : K\Gamma^{\times} \longrightarrow J(K\Gamma)$. We also denote by j the canonical quotient map

$$j : J(K\Gamma) \longrightarrow Cl(O\Gamma). \tag{A.4.2}$$

In the following Proposition we are able to define (O_h).

Proposition A.4.0.1. *Let $b \in K_h$ a normal basis generator and, for all $\mathfrak{v}$, $a_{\mathfrak{v}} \in (O_{\mathfrak{v}})_{h_{\mathfrak{v}}}$ be given such that*

$$K_h = K\Gamma.b \quad \textit{and} \quad (O_{\mathfrak{v}})_{h_{\mathfrak{v}}} = O_{\mathfrak{v}}\Gamma.a_{\mathfrak{v}} \quad \textit{for all} \mathfrak{v}.$$

For each $\mathfrak{v}$, let $c_{\mathfrak{v}}$ be the unique element of $(K_{\mathfrak{v}}\Gamma)^{\times}$ such that $\big($in $(K_{\mathfrak{v}})_{h_{\mathfrak{v}}}\big)$

$$a_{\mathfrak{v}} = c_{\mathfrak{v}} \cdot b.$$

Then $c = (c_{\mathfrak{v}})_{\mathfrak{v}} \in J(K\Gamma)$ and $j(c)$ in $Cl(O\Gamma)$ depends only on $O_{\mathfrak{v}}$ and not on the choice of b and of the $a_{\mathfrak{v}}$; we denote $j(c)$ by (O_h).

Proof. The existence and uniqueness of $c_{\mathfrak{v}}$ are immediate from the fact that

$$(K_{\mathfrak{v}})_{h_{\mathfrak{v}}} = K_{\mathfrak{v}}\Gamma.b = K_{\mathfrak{v}}\Gamma.a_{\mathfrak{v}},$$

so we find a unique $c = (c_{\mathfrak{v}})_{\mathfrak{v}} \in \prod_{\mathfrak{v}}(K_{\mathfrak{v}}\Gamma)^{\times}$ with the property request. Moreover it belongs to $J(K\Gamma)$ because O_h and $O\Gamma \cdot b$ can differ at only finitely many primes $\mathfrak{v}$, so for all primes but a finite set we have

$$(O_{\mathfrak{v}})_{h_{\mathfrak{v}}} = O_{\mathfrak{v}}\Gamma.b = O_{\mathfrak{v}}\Gamma.a_{\mathfrak{v}},$$

by (2.3.2), so $c_{\mathfrak{v}} \in (O_{\mathfrak{v}}\Gamma)^{\times}$ for almost all $\mathfrak{v}$.
Finally changing b or $a_{\mathfrak{v}}$ we only change c by principal or unit idele, respectively, leaving in this way the class $j(c)$ of c in $Cl(O\Gamma)$ unchanged. □

We can rewrite the previous Proposition in terms of resolvends, obtaining

$$r_{\Gamma}(a_{\mathfrak{v}}) = c_{\mathfrak{v}} r_{\Gamma}(b) \quad \text{in} \quad H(K_{\mathfrak{v}}\Gamma),$$

whence

$$\mathcal{R}_{\Gamma}(a_{\mathfrak{v}}) = rag(c_{\mathfrak{v}})\mathcal{R}_{\Gamma}(b) \quad \text{in} \quad \mathcal{H}(K_{\mathfrak{v}}\Gamma). \tag{A.4.3}$$

The previous equality (A.4.3) is the characteristic equation of (O_h) for the following reason. If $rag(c'_{\mathfrak{v}}) = rag(c_{\mathfrak{v}})$ for all primes $\mathfrak{v}$, then $c'_{\mathfrak{v}} = c_{\mathfrak{v}} s_{\mathfrak{v}}$ where $s_{\mathfrak{v}} \in \Gamma$ for all $\mathfrak{v}$. Hence $(s_{\mathfrak{v}})_{\mathfrak{v}} \in U(O\Gamma)$ and $(c'_{\mathfrak{v}})$ determines the same class in $Cl(O\Gamma)$ as $(c_{\mathfrak{v}})_{\mathfrak{v}}$.

A.5 Hom-description

Following [Frö83], we will give an analogous definition of the class group $Cl(\mathfrak{U})$ of an order $\mathfrak{U}$ in $K[\Gamma]$, which is fundamental for all our work.

Given a finite group Γ, its additive group of virtual characters R_Γ (linear combinations of the irreducible complex characters of Γ) is an Ω_K-module (recall that $\Omega_K = \mathrm{Gal}(K^c/K)$), under the action:

$$\chi^\omega(\gamma) = (\chi(\gamma))^\omega, \quad \omega \in \Omega_K.$$

Now let $J(\mathbb{Q}^c)$ the idele group of $\mathbb{Q}^c$, it's not difficult to see that it exists a number field F containing K, which is Galois over $\mathbb{Q}$ and such that

$$\mathrm{Hom}_{\Omega_K}(R_\Gamma, J(\mathbb{Q}^c)) = \mathrm{Hom}_{\Omega_K}(R_\Gamma, J(F)) = \mathrm{Hom}_{\mathrm{Gal}_{(F/K)}}(R_\Gamma, J(F)),$$

which is the group of *Galois equivariant homomorphisms*; the base group of our definition of class group.

We proceed now to give a generalization of the notion of determinant. Let A be a commutative K-algebra then we have a natural action of Ω_K on the tensor product $\mathbb{Q}^c \otimes_K A$ via the action on the first factor.

Given a representation

$$T : \Gamma \longrightarrow \mathrm{GL}_n\mathbb{Q}^c,$$

we extend it to a homomorphism of algebras

$$T : A\Gamma \longrightarrow \mathrm{M}_n(\mathbb{Q}^c \otimes_K A);$$

which, restricting it to the invertible elements, becomes

$$T : A\Gamma^\times \longrightarrow \mathrm{GL}_n(\mathbb{Q}^c \otimes_K A).$$

Thanks to the following commutative diagram

$$\begin{tikzcd}
A\Gamma^\times \arrow[r, "T"] \arrow[dr, "\mathrm{Det}_\chi"'] & \mathrm{GL}_n(\mathbb{Q}^c \otimes_k A) \arrow[d, "\det"] \\
& (\mathbb{Q}^c \otimes_K A)^\times
\end{tikzcd} \tag{A.5.1}$$

,

where det is the usual determinant; we define a new determinant

$$\mathrm{Det}_\chi : A\Gamma^\times \longrightarrow (\mathbb{Q}^c \otimes_K A)^\times,$$

depending only on the character of the representation χ (because the determinant remains the same in a class of conjugated elements).

If we even consider another representation with character θ, we have

$$\mathrm{Det}_{\chi+\theta}(a) = \mathrm{Det}_\chi(a) \cdot \mathrm{Det}_\theta(a)$$

and by letting

$$\mathrm{Det}_{\chi-\theta}(a) = \mathrm{Det}_{\chi}(a) \cdot (\mathrm{Det}_{\theta}(a))^{-1},$$

we can extend the map $\chi \longrightarrow \mathrm{Det}_{\chi}(a)$ to the homomorphism

$$\begin{array}{rccc} \mathrm{Det}(a): & R_{\Gamma} & \longrightarrow & (\mathbb{Q}^c \otimes_K A)^{\times} \\ & \chi & \longrightarrow & \mathrm{Det}(a)(\chi) = \mathrm{Det}_{\chi}(a)\ ; \end{array} \tag{A.5.2}$$

called the *generalized determinant* of $a \in A\Gamma^{\times}$.

If χ is the character of a representation T, then $\chi^{\omega^{-1}}$ is that of the representation $T^{\omega^{-1}}$, where $T^{\omega^{-1}}(\gamma) = \omega^{-1}(T(\gamma))$; then, given $a \in A\Gamma^{\times}$, we have

$$\begin{aligned} \left(\mathrm{Det}_{\chi^{\omega^{-1}}}(a)\right)^{\omega} &= \omega\left(\mathrm{Det}\left(\sum_{\gamma\in\Gamma} a_{\gamma}\omega^{-1}(T(\gamma))\right)\right) \\ &= \mathrm{Det}\left(\omega\left(\sum_{\gamma\in\Gamma} a_{\gamma}\omega^{-1}(T(\gamma))\right)\right) \\ &= \mathrm{Det}\left(\sum_{\gamma\in\Gamma} a_{\gamma}T(\gamma)\right) \\ &= \mathrm{Det}_{\chi}(a). \end{aligned}$$

This easy result allows us to define the homomorphism

$$\begin{array}{rccc} \mathrm{Det}: & (A\Gamma)^{\times} & \longrightarrow & \mathrm{Hom}_{\Omega_K}\left(R_{\Gamma}, (\mathbb{Q}^c \otimes_K A)^{\times}\right) \\ & a & \longrightarrow & \mathrm{Det}(a)\ . \end{array} \tag{A.5.3}$$

If we take $A = K_{\mathfrak{v}}$ and in $K_{\mathfrak{v}}\Gamma$ the order $\mathfrak{U}_{\mathfrak{v}}$ (when $\mathfrak{v}$ is infinite, consider $\mathfrak{U}_{\mathfrak{v}} = K_{\mathfrak{v}}\Gamma$), then we have $\mathbb{Q}^c \otimes_K K_{\mathfrak{v}} = (\mathbb{Q}^c)_{\mathfrak{v}}$ and considering $U_{\mathfrak{v}}(\mathbb{Q}^c)$ the group of units of the ring of integers in $(\mathbb{Q}^c)_{\mathfrak{v}}$, just by restriction we obtain

$$\mathrm{Det}: \mathfrak{U}_{\mathfrak{v}}^{\times} \longrightarrow \mathrm{Hom}_{\Omega_K}\left(R_{\Gamma}, U_{\mathfrak{v}}(\mathbb{Q}^c)\right),$$

as $\mathrm{Det}_{\chi}(a)$ is clearly a unit for $a \in \mathfrak{U}_{\mathfrak{v}}^{\times}$.

Making product over all primes $\mathfrak{v}$ we define

$$U(\mathfrak{U}) = \prod_{\mathfrak{v}} \mathfrak{U}_{\mathfrak{v}}^{\times}$$

and in the same way

$$U(\mathbb{Q}^c) = \prod_{\mathfrak{v}} U_{\mathfrak{v}}(\mathbb{Q}^c).$$

So going over the product we have the homomorphism

$$\mathrm{Det}: U(\mathfrak{U}) \longrightarrow \mathrm{Hom}_{\Omega_K}\left(R_{\Gamma}, U(\mathbb{Q}^c)\right) \subset \mathrm{Hom}_{\Omega_K}\left(R_{\Gamma}, J(\mathbb{Q}^c)\right),$$

whose image we denote by $\mathrm{Det}\,(U\,(\mathfrak{U}))$.

Now we can give the desired Hom-description of the class group, indeed in [Frö83], starting from the original definition of the class group of an order given through the Grothendieck group $\mathcal{K}_0(\mathfrak{U})$, is proved the following Theorem.

Theorem A.5.1 (Hom-description)**.** **(i)** *Let X be a locally free rank one $\mathfrak{U}$-module. So we can choose a free generator v of $V = X \otimes_{O_K} K$ over $K\Gamma$ and for any prime $\mathfrak{v}$ in K a free generator $x_{\mathfrak{v}}$ of the local $X_{\mathfrak{v}}$ over $\mathfrak{U}_{\mathfrak{v}}$. Then they are both generator of $V_{\mathfrak{v}}$ over $K_{\mathfrak{v}}\Gamma$ and so*

$$x_{\mathfrak{v}} = v\lambda_{\mathfrak{v}}, \quad \lambda_{\mathfrak{v}} \in (K_{\mathfrak{v}}\Gamma)^{\times}.$$

Define for any $\mathfrak{v}$ and for any character χ

$$f_{\mathfrak{v}}(\chi) = f(\chi)_{\mathfrak{v}} = Det_{\chi}(\lambda_{\mathfrak{v}}).$$

Then $f_{\mathfrak{v}} \in Hom_{\Omega_K}(R_{\Gamma}, {(\mathbb{Q}^c)_{\mathfrak{v}}}^{\times})$, so

$$f \in Hom_{\Omega_K}(R_{\Gamma}, J(\mathbb{Q}^c))$$

and its class (f) modulo $Hom_{\Omega_K}(R\Gamma, (\mathbb{Q}^c)^{\times})Det(U(\mathfrak{U})$ only depends on the isomorphism class of X.

(ii) *There is a unique isomorphism*

$$Cl(\mathfrak{U}) \cong \frac{Hom_{\Omega_K}(R_{\Gamma}, J(\mathbb{Q}^c))}{Hom_{\Omega_K}(R_{\Gamma}, (\mathbb{Q}^c)^{\times})Det(U(\mathfrak{U}))}$$

so that for any locally free rank one module X, the class (X) maps onto the corresponding class (f) as constructed above.

Without going into details, we can take this last isomorphism as definition of the class group of an order.

Remark A.5.2 (Hom-description for a maximal order)**.** *As explained by Fröhlich in [Frö83] (Interpretation 1 after Prop. 2.1), in the case of a maximal order $\mathcal{M}$, the Hom-description becomes:*

$$Cl(\mathcal{M}) \cong \frac{Hom_{\Omega_K}(R_{\Gamma}, J(\mathbb{Q}^c))}{Hom_{\Omega_K}(R_{\Gamma}, (\mathbb{Q}^c)^{\times})Hom_{\Omega_K}(R_{\Gamma}, U(\mathbb{Q}^c))}.$$

A.5.3 Resolvents

We introduce here the notion of resolvent, which is one of the main ingredient in the non abelian approaches, trying to investigate its main properties and its importance in the Hom-description given above.

Given a Galois extension of fields N/K, with Galois group Γ, we consider A a commutative K-algebra. Then extending scalars we have that $N \otimes_K A$ is free of rank one over $A[\Gamma]$, with Γ acting via N. Given $a \in N \otimes_K A$ free generator, we have that the element $\sum_{\gamma \in \Gamma} \gamma(a)\gamma^{-1}$ belongs to $((N \otimes_K A)\,\Gamma)^{\times}$ (for the proof look at [Frö83]).
Let a be in $N \otimes_K A$ (not necessarily free generator), we define the resolvent of a by

$$(a|\chi) = \mathrm{Det}_{\chi}\left(\sum_{\gamma \in \Gamma} \gamma(a)\gamma^{-1}\right) = \mathrm{Det}\left(\sum_{\gamma \in \Gamma} \gamma(a)T(\gamma)^{-1}\right);$$

where T is the representation with character associated χ. By the result claimed above, we have that if a is a free generator of $N \otimes_K A$ over $A[\Gamma]$, then $(a|\chi) \in (K^c \otimes_K A)^\times$ and so the map $\chi \longrightarrow (a|\chi)$ lies in $\mathrm{Hom}_{\Omega_N}\left(R_\Gamma, (K^c \otimes_K A)^\times\right)$.

Remark A.5.4. *When we are in the abelian case, any representation is* 1*-dimensional, and so the resolvent here defined becomes the usual Lagrange resolvent*

$$(a|\chi) = \sum_{\gamma\in\Gamma} \gamma(a)\chi(\gamma^{-1}).$$

If we assume that the Galois extension N/K is tame, then by Noether Criterion we have that O_N is locally free over $O_K[\Gamma]$ ($O_{N,\mathfrak{v}} = O_N \otimes_{O_K} O_{K,\mathfrak{v}}$ is free of rank one over $O_{K,\mathfrak{v}}[\Gamma]$, for all prime divisors $\mathfrak{v}$), and thus defines a class $(O_N)_{O_K[\Gamma]} \in Cl(O_K[\Gamma])$.
Thanks to the notion of resolvent, we can now find a representative function of this class, following the Hom-description. Indeed in [Frö83] we can find the following Theorem.

Theorem A.5.5. *Let a be a free generator of N over $K[\Gamma]$ and, for each prime divisor $\mathfrak{v}$ of K, let $\alpha_\mathfrak{v}$ be a free generator of $O_{N,\mathfrak{v}}$ over $O_{K,\mathfrak{v}}[\Gamma]$. For $\chi \in R_\Gamma$, define $(\alpha|\chi) \in \prod_\mathfrak{v}(\mathbb{Q}^c_\mathfrak{v})^\times$ by*

$$(\alpha|\chi)_\mathfrak{v} = (\alpha_\mathfrak{v}|\chi).$$

Then $(\alpha|\chi) \in J(\mathbb{Q}^c)$ and the map

$$\chi \longrightarrow \frac{(\alpha|\chi)}{(a|\chi)}$$

is a representative of $(O_N)_{O_K[\Gamma]}$.

A.5.6 The structure of $Cl(\mathcal{M})$

Thanks to the structure of the group algebra $K[\Gamma]$, we can now investigate the shape of the class group $Cl(\mathcal{M})$. To discover its structure, we shall make use of some results presented in [Rei03].

First of all we recall the definition of the Eichler condition relative to a Dedekind domain R with field of quotients K. In the definition, with the notion of "non-R" prime of K we denote a prime of K which doesn't derive from an ideal of R; when K is a number field it means the infinite primes of K.

Definition A.5.7. *The central simple K-algebra A satisfies the* Eichler Condition relative to *R, if either*

- *K is an algebraic number field and $(A : K) \neq 4$ if A ramifies at every "non-R" prime of K, or*

- *K is a function field and some "non-R" prime of K does not ramify in A*

When A doesn't satisfy the Eichler condition, it's called a totally definite quaternion algebra.
The Eichler condition for a separable algebra becomes:

Definition A.5.8. *Given an R-order Λ in a separable K-algebra A. For each simple components A_i of A, let R_i denote the integral closure of R in the center of A_i. A satisfies the Eichler condition relative to R if for each i, A_i satisfies it relative to R_i.*

Considering a central simple K-algebra A, we recall even the definition of $Cl_A R$, the modified ray class group mod$S$; where S denotes the set of all infinite primes of K ramified in A.
It's just a modified definition of the original class group of R: given $P_A(R) = \{R\alpha : \alpha \in K^\times \text{ and } \alpha_\mathfrak{p} > 0 \, \text{for each } \mathfrak{p} \in S\}$, we define the modified ray class group as

$$Cl_A R = \frac{\{\text{multiplicative group of } R\text{-ideals in } K\}}{P_A(R)};$$

it's not difficult to remark that the modified ray class group coincides with $Cl(R)$ when the set S is empty.

A general result of Jacobinski (look at [Rei03] pag.344) allows to understand the structure of $Cl(\Lambda)$; which, in the particular case of a maximal order $\mathcal{M}$ in a separable K-algebra A satisfying the Eichler condition, is deductible just considering the central simple components.

The central simple situation is now easy thanks to a result of Swan ([Rei03] pag.313), for any maximal order $\mathcal{M}$ in a central simple K-algebra A (K field of quotients of the Dedekind domain R) we have

$$Cl(\mathcal{M}) \cong Cl_A R,$$

where $Cl_A R$ denotes the modified ray class group mod$S$.

Thanks to all these considerations is now easy to describe $Cl(\mathcal{M})$ for the previous non abelian groups. Let's give a look:

- $K[D_4] \cong K^4 \times \mathrm{M}_2(K) \longrightarrow Cl(\mathcal{M}) \cong Cl(K)^5$;
- $K[A_4] \cong K \times K(\omega) \times \mathrm{M}_3(K) \longrightarrow Cl(\mathcal{M}) \cong Cl(K) \times Cl\left(K\left(\omega\right)\right) \times Cl(K)$ in the first case, while $K[A_4] \cong K \times K \times K \times \mathrm{M}_3(K) \longrightarrow Cl(\mathcal{M}) \cong Cl(K)^4$ in the second one;
- $K[S_4] \cong K \times K \times \mathrm{M}_2(K) \times \mathrm{M}_3(K) \times \mathrm{M}_3(K) \longrightarrow Cl(\mathcal{M}) \cong Cl(K)^5$.

Remark A.5.9. *The Eichler condition is satisfied in any of these situations, just observing the dimension of the simple components over their center.*
We have also to observe that there are examples of non abelian groups, for which the Eichler condition is not satisfied; for some examples look at [Rei03].

A.5.10 The Hom-description of $Cl^\circ(O_K[\Gamma])$

Using the already presented Hom-description, we will now give a particular Hom-description of $Cl^\circ(O_K[\Gamma])$ in order to well investigate it.

The analogue Hom-description for the augmentation kernel arises from the following Proposition, where with χ_0 we denote the trivial character.

Proposition A.5.10.1. *Given $f \in Hom_{\Omega_K}(R_\Gamma, J(K))$, if $f(\chi_0) = 1$ then $(f) \in Cl^\circ(O_K[\Gamma])$. Conversely any class in $Cl^\circ(O_K[\Gamma])$ can be written as (f) with $f(\chi_0) = 1$.*

Proof. The augmentation map is exactly the linear extension of the trivial character χ_0 of Γ and so the induced homomorphism

$$\epsilon_\star : Cl(O_K[\Gamma]) \longrightarrow Cl(O_K) \cong \frac{J(K)}{K^\times U(O_K)}$$

is given by $\epsilon_\star((f)) = (f(\chi_0))$. Thus the class (f) lies in the kernel $Cl^\circ(O_K[\Gamma])$ of the induced homomorphism if and only if the content of the idele $f(\chi_0) \in J(K)$ is a principal ideal of O_K.
So if $f(\chi_0) = 1$ it is easily a principal ideal and then $(f) \in Cl^\circ(O_K[\Gamma])$.
To prove the other inclusion instead we take $(f) \in Cl^\circ(O_K[\Gamma])$ and we have $f(\chi_0) = b \in J(K)$ where $b = ku$ with $k \in K^\times$ and $u \in U(O_K)$. Now we can define $\widehat{b} \in \mathrm{Hom}_{\Omega_K}(R_\Gamma, J(K))$ as $\widehat{b}(\chi) = b^{\chi(1)}$ and exactly in the same way we define $\widehat{k}$ and $\widehat{u}$. In this way we have that $\widehat{k} \in \mathrm{Hom}_{\Omega_K}\left(R_\Gamma, K^\times\right)$ and $\widehat{u} = \mathrm{Det}(u)$ since $u \in U(O_K)$. Thus we have $\widehat{b} = \widehat{k}\widehat{u} = \widehat{k}\mathrm{Det}(u) \in \mathrm{Hom}_{\Omega_K}\left(R_\Gamma, K^\times\right)\mathrm{Det}\left(U(O_K)\right)$ and $\widehat{b}(\chi_0) = b$.
If we consider $f' = \widehat{b}^{-1}f$ then f and f' define the same class and in particular $f'(\chi_0) = \frac{f(\chi_0)}{\widehat{b}(\chi_0)} = 1$, as we wanted to prove. □

The Proposition explains the following Hom-description of the augmentation kernel, in particular

$$Cl^\circ(O_K[\Gamma]) \cong \frac{\mathrm{Hom}^\circ_{\Omega_K}\left(R_\Gamma, J\left(\mathbb{Q}^c\right)\right)}{\mathrm{Hom}^\circ_{\Omega_K}(R_\Gamma, (\mathbb{Q}^c)^\times)\mathrm{Det}^\circ\left(U\left(O_K[\Gamma]\right)\right)} \quad ,$$

where with the exponent ∘ we denote the fact that we consider only homomorphisms f acting trivially on the character χ_0 (the trivial one). Indeed this assertion comes from the previous Proposition and from the fact that it can be proved as in the Proposition that

$$\mathrm{Hom}^\circ_{\Omega_K}\left(R_\Gamma, J\left(\mathbb{Q}^c\right)\right) \cap \mathrm{Hom}_{\Omega_K}(R_\Gamma, K^\times)\mathrm{Det}\left(U(O_K[\Gamma])\right) = \mathrm{Hom}^\circ_{\Omega_K}(R_\Gamma, (\mathbb{Q}^c)^\times)\mathrm{Det}^\circ\left(U\left(O_K[\Gamma]\right)\right).$$

Given the Γ-extension N/K, the class (O_N) in $Cl^\circ(O_K[\Gamma])$ is always described as quotient of resolvents as in A.5.5, even if we have to take the normal basis generator a and the local one $\alpha_\mathfrak{v}$ such that $\mathrm{Tr}_{N/K}(a) = 1$ and $\mathrm{Tr}_{N_\mathfrak{v}/K_\mathfrak{v}}(\alpha_\mathfrak{v}) = 1$ for all $\mathfrak{v}$ (this indeed is the condition to have $f(\chi_0) = 1$, just looking at the remark A.5.4).

Bibliography

[Agb] A. Agboola, *On counting rings of integers as Galois modules*, Preliminaty version of November 25, 2008.

[Art50] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, Colloque International CNRS **24** (1950), 19–20.

[Art55] ______, *Galois Theory*, number 2 ed., Notre Dame Mathematical Lectures, 1955.

[Art67] ______, *Algebraic Numbers and Algebraic Functions*, AMS Chelsea Publishing, 1967.

[Bou81] N. Bourbaki, *Algèbre, chap.4-7*, Masson, Paris, 1981.

[Bri84] J. Brinkhuis, *Galois modules and embedding problems*, J. Reine Angew. Math. **346** (1984), 141–165.

[BS05a] N. P. Byott and B. Sodaïgui, *Galois module structure for dihedral extensions of degree 8: Realizable classes over the group ring*, Journal of Number Theory **112** (2005), 1–19.

[BS05b] ______, *Realizable Galois module classes for tetrahedral extensions*, Compositio Math. **141** (2005), 573–582.

[BS08] C. Bruche and B. Sodaïgui, *On realizable Galois module classes and Steinitz classes of nonabelian extensions*, Journal of Number Theory **128** (2008), 954–978.

[Cob10] A. Cobbe, *Steinitz classes of tamely ramified galois extensions of algebraic number fields*, Journal of Number Theory **130** (2010), 1129–1154.

[Coh00] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer-Verlag New York, Inc., 2000.

[CR87] C. W. Curtis and I. Reiner, *Methods of representation theory, with applications to finite groups and orders*, John Wiley and Sons, 1987.

[Ere] B. Erez, *Galois modules in arithmetic*, Book in preparation.

[Fos] K. Foster, *An equal-distribution result for Galois module structure*, Ph.D. Thesis, University of Illinois at Urbana-Champaign (1987).

[Frö64] A. Fröhlich, *Galois algebra and their homomorphisms*, J.Reine Angew.Math. **216** (1964), 1–11.

[Frö75] ______, *Galois module structure*, Algebraic Number Fields (A. Fröhlich, ed.), Proceedings of the Durham Symposium, Academic Press, London, 1977, 1975, pp. 133–191.

[Frö83] ______, *Galois Module Structure of Algebraic Integers*, Springer-Verlag Berlin Heidelberg New York Tokyo, 1983.

[FT91] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge University Press, 1991.

[GS03] M. Godin and B. Sodaïgui, *Realizable classes of tetrahedral extensions*, Journal of Number Theory **98** (2003), 320–328.

[GS06] N. P. Byott, C. Greither and B. Sodaïgui, *Classes réalisables d'extensions non abéliennes*, J Reine Angew. Math. **601** (2006), 1–27.

[Hec81] E. Hecke, *Lectures on the theory of algebraic numbers*, Springer, New York, 1981.

[HR65] S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois Theory and Cohomology of commutative rings*, Mem. Amer. Math. Soc. **52** (1965).

[Jac64] N. Jacobson, *Lectures in Abstract Algebra, Theory of fields and Galois Theory*, vol. 3, D.Van Nostrand Company, Inc., 1964.

[KW06] A. C. Kable and D. J. Wright, *Uniform distribution of the Steinitz invariants of quadratic and cubic extensions*, Compositio Math. **142** (2006), 84–100.

[Mar90] J. Martinet, *Discriminants and permutation groups*, Number Theory (Richard A. Molin, ed.), Walter de Gruyter, Berlin - New York, 1990, pp. 359–385.

[McC75] L. R. McCulloh, *A Stickelberger condition on Galois module structure for Kummer extension of prime degree*, Algebraic Number Fields (A. Fröhlich, ed.), Proceedings of the Durham Symposium, Academic Press, London, 1977, 1975, pp. 561–588.

[McC83] ______, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), 102–134.

[McC87] ______, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987), 259–306.

[Mil] J. S. Milne, *Class field theory*, Available at his website.

[Neu86] J. Neukirch, *Class Field Theory*, Springer, Berlin, 1986.

[Rei03] I. Reiner, *Maximal Orders*, Oxford University Press Inc., New York, 2003.

[Ser77] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag New York Berlin Heidelberg, 1977.

[Ser79] ———, *Local Fields*, Springer-Verlag New York Inc., 1979.

[Sod88] B. Sodaïgui, *Structure galoisienne relative des anneaux d'entiers*, Journal of Number Theory **28 (2)** (1988), 189–204.

[Sod97] ———, *Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger*, Journal of Number Theory **65** (1997), 87–95.

[Sod99a] ———, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de* 2 *et problème de plongement*, Illinois J. Math. **43(1)** (1999), 47–60.

[Sod99b] ———, *"Galois Module Structure" des extensions quaternioniennes de degré 8*, Journal of Algebra **213** (1999), 549–556.

[Sod00a] ———, *Realizable classes of quaternion extensions of degree 4l*, Journal of Number Theory **80** (2000), 304–315.

[Sod00b] ———, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, Journal of Algebra **223** (2000), 367–378.

[Sod07] ———, *Relative Galois module structure of octahedral extensions*, Journal of Algebra **312** (2007), 590–601.

[SS10] F. Sbeity and B. Sodaïgui, *Classes réalisables d'extensions métacycliques de degré lm*, Journal of Number Theory **130** (2010), 1818–1834.

[Tay81] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41–79.

[Was96] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, Berlin, 1996.

[Woo10] M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compositio Math. **146** (2010), 102–128.

To Elena and her cheerful presence

“Roads? Where we’re going we don’t need roads!”