Class invariants for tame Galois algebras

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof.mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 26 juni 2013
klokke 08:45 uur

door

Andrea Siviero
geboren te Rovigo, Italië
in 1986

Samenstelling van de promotiecommissie

Promotores

prof.dr. B. Erez (Université Bordeaux I)

prof.dr. P. Stevenhagen

Copromotor

dr. B. de Smit

Overige leden

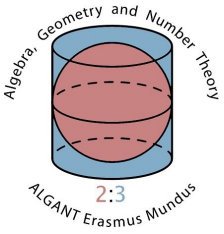
prof.dr. A. Agboola (UC, Santa Barbara)

dr. N. Byott (University of Exeter)

prof.dr. P. Cassou-Noguès (Université Bordeaux I)

prof.dr. H.W. Lenstra, Jr.

This work was funded by ALGANT-Doc Erasmus Action and was carried out at Universiteit Leiden and Université Bordeaux I



Universiteit Leiden

Cover picture courtesy of Nicola di Pietro (Glimpse of the Dolomites - Cadore, in the Italian region of Veneto)

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Andrea SIVIERO

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ: Mathématiques Pures

Class invariants for tame Galois algebras

Directeurs de recherche: Bart DE SMIT et Boas EREZ

Soutenue le: 26 Juin 2013 à Leiden

Après l'avis favorable de la commission d'examen formée de:

M AGBOOLA, Adebisi	Professeur	UC, Santa Barbara	Rapporteur
M BYOTT, Nigel	Docteur	University of Exeter	Rapporteur
M CASSOU-NOGUÈS, Philippe	Professeur	Université Bordeaux I	Examinateur
M DE SMIT, Bart	Docteur	Universiteit Leiden	Directeur
M EREZ, Boas	Professeur	Université Bordeaux I	Directeur
M LENSTRA, Hendrik W., Jr.	Professeur	Universiteit Leiden	Examinateur
M STEVENHAGEN, Peter	Professeur	Universiteit Leiden	Examinateur

Class invariants for tame Galois Algebras

ABSTRACT (short version)

Let K be a number field with ring of integers O_K and let G be a finite group.
By a result of E. Noether, the ring of integers of a tame Galois extension of K with Galois group G is a locally free $O_K[G]$-module of rank 1.
Thus, to any tame Galois extension L/K with Galois group G we can associate a class $[O_L]$ in the locally free class group $\mathrm{Cl}(O_K[G])$. The set of all classes in $\mathrm{Cl}(O_K[G])$ which can be obtained in this way is called the set of realizable classes and is denoted by $R(O_K[G])$.
In this dissertation we study different problems related to $R(O_K[G])$.
The first part focuses on the following question: is $R(O_K[G])$ a subgroup of $\mathrm{Cl}(O_K[G])$? When the group G is abelian, L. McCulloh proved that $R(O_K[G])$ coincides with the so-called Stickelberger subgroup $\mathrm{St}(O_K[G])$ of $\mathrm{Cl}(O_K[G])$. In Chapter 2, we give a detailed presentation of unpublished work by L. McCulloh that extends the definition of $\mathrm{St}(O_K[G])$ to the non-abelian case and shows that the inclusion $R(O_K[G]) \subseteq \mathrm{St}(O_K[G])$ holds (the opposite inclusion is still not known in the non-abelian case).
Then, just using its definition and Stickelberger's classical theorem, we prove in Chapter 3 that $\mathrm{St}(O_K[G])$ is trivial if $K = \mathbb{Q}$ and G is either cyclic of order p or dihedral of order $2p$, where p is an odd prime number. This, together with McCulloh's results, allows us to have a new proof of the triviality of $R(O_K[G])$ in the cases just considered.
The main original results are contained in the second part of this thesis. In Chapter 4, we prove that $\mathrm{St}(O_K[G])$ has good functorial behavior under restriction of the base field. This has the interesting consequence that, if N/L is a tame Galois extension with Galois group G, and $\mathrm{St}(O_K[G])$ is known to be trivial for some subfield K of L, then O_N is stably free as an $O_K[G]$-module.
In the last chapter, we prove an equidistribution result for Galois module classes amongst tame Galois extensions of K with Galois group G in which a given prime $\mathfrak{p}$ of K is totally split.

Keywords: Galois module structure, tame Galois extensions, locally free modules, reduced norm, realizable classes, locally free class group, Stickelberger's Theorem.

Klasse-invarianten voor tamme Galoisalgebra's

SAMENVATTING (beknopte versie)

Zij K een getallenlichaam met ring van gehelen O_K en zij G een eindige groep. Een resultaat van E. Noether zegt dat de ring van gehelen van een tamme G-Galoisuitbreiding van K een lokaal vrij $O_K[G]$-moduul van rang 1 is.
Hieruit volgt dat we aan elke tamme G-Galoisuitbreiding van K een klasse kunnen toekennen in de lokaal vrije klassegroep $\mathrm{Cl}(O_K[G])$. De verzameling van alle klassen in $\mathrm{Cl}(O_K[G])$ die afkomstig zijn van de ring van gehelen van een tamme G-Galoisuitbreiding van K wordt de verzameling van realiseerbare klassen genoemd en wordt genoteerd als $R(O_K[G])$.
In dit proefschrift bestuderen we verschillende problemen gerelateerd aan $R(O_K[G])$. Allereerst het volgende probleem: is $R(O_K[G])$ een ondergroep van $\mathrm{Cl}(O_K[G])$? Voor abelse G bewees L. McCulloh dat $R(O_K[G])$ overeenkomt met de zogenaamde Stickelberger-ondergroep $\mathrm{St}(O_K[G])$ van $\mathrm{Cl}(O_K[G])$. In hoofdstuk 2, wij geven een gedetailleerde presentatie van de gedeeltelijk ongepubliceerde resultaten van L. McCulloh die de definitie van $\mathrm{St}(O_K[G])$ uitbreiden tot het niet-abelse geval, en een inclusie $R(O_K[G]) \subseteq \mathrm{St}(O_K[G])$ bewijzen (of de omgekeerde inclusie ook altijd geldt, is voor niet-abelse G nog steeds niet bekend.)
Vervolgens bewijzen we in hoofdstuk 3, gebruikmakend van de definitie en de klassieke Stelling van Stickelberger, dat $\mathrm{St}(O_K[G])$ triviaal is als $K = \mathbb{Q}$ en G een cyclische groep van orde p is of een dihedrale groep van orde $2p$, waarbij $p \geq 3$ priem is. Dit resultaat, samen met resultaten van McCulloh, staat ons toe om een nieuw bewijs te geven voor de trivialiteit van $R(O_K[G])$ in bovenstaande gevallen.
De belangrijkste originele resultaten zijn bevat in het tweede deel van dit proefschrift. In hoofdstuk 4, bewijzen we dat $\mathrm{St}(O_K[G])$ zich functorieel goed gedraagt ten opzichte van het beperken van het grondlichaam. Dit geeft het interessante gevolg dat als N/L een tamme Galoisuitbreiding met groep G is, en als $\mathrm{St}(O_K[G])$ triviaal is voor een deellichaam K van L, de ring O_N stabiel vrij is als $O_K[G]$-moduul.
In het laatste hoofdstuk bewijzen we een resultaat over de verdeling van Galoismoduulklassen afkomstig van tamme Galoisuitbreidingen van K met Galoisgroep G met de beperking dat een gegeven priem $\mathfrak{p}$ van K volledig splitst.

Steekwoorden: Galoismoduulstructuur, tamme Galoisuitbreidingen, lokaal vrije modulen, gereduceerde norm, realiseerbare klassen, lokaal vrije klassegroep, Stelling van Stickelberger.

Invariants de classe pour algèbres galoisiennes modérément ramifiées

RÉSUMÉ (version brève)

Soient K un corps de nombres d'anneau des entiers O_K et G un groupe fini.
Grâce à un résultat de E. Noether, l'anneau des entiers d'une extension galoisienne de K modérément ramifiée, de groupe de Galois G, est un $O_K[G]$-module localement libre de rang 1.
Donc, à chaque extension galoisienne L/K modérément ramifiée, de groupe de Galois G, on peut associer une classe $[O_L]$ dans le groupe des classes des modules localement libres $\mathrm{Cl}(O_K[G])$. L'ensemble des classes de $\mathrm{Cl}(O_K[G])$ qui peuvent être obtenues de cette façon est appelé ensemble des classes réalisables et on le note $R(O_K[G])$.
Dans cette thèse, on étudie différents problèmes liés à $R(O_K[G])$.
Dans la première partie, nous nous focalisons sur la question suivante: $R(O_K[G])$ est-il un sous-groupe de $\mathrm{Cl}(O_K[G])$? Si G est abélien, L. McCulloh a prouvé que $R(O_K[G])$ coïncide avec le soi-disant sous-groupe de Stickelberger $\mathrm{St}(O_K[G])$ dans $\mathrm{Cl}(O_K[G])$. Dans le Chapitre 2, nous donnons une présentation détaillée d'un travail non publié de L. McCulloh qui étend la définition de $\mathrm{St}(O_K[G])$ au cas non-abélien et montre l'inclusion $R(O_K[G]) \subseteq \mathrm{St}(O_K[G])$ (l'inclusion opposée n'est pas encore connue dans le cas non-abélien).
Puis, en utilisant sa définition et le Théorème de Stickelberger classique, nous montrons dans le Chapitre 3 que $\mathrm{St}(O_K[G])$ est trivial si $K = \mathbb{Q}$ et G est soit un groupe cyclique d'ordre p soit un groupe diédral d'ordre $2p$, avec p premier impair. Ceci, lié aux résultats de McCulloh, nous donne une nouvelle preuve de la trivialité de $R(O_K[G])$ dans les cas considérés.
Les résultats originaux les plus importants sont contenus dans la deuxième partie de cette thèse. Dans le Chapitre 4 nous montrons la fonctorialité de $\mathrm{St}(O_K[G])$ par rapport au changement du corps de base. Ceci implique que si N/L est une extension galoisienne modérément ramifiée, de groupe de Galois G, et $\mathrm{St}(O_K[G])$ est connu être trivial pour un certain sous-corps K de L, alors O_N est un $O_K[G]$-module stablement libre.
Dans le dernier chapitre, nous montrons un résultat concernant la distribution des classes réalisables parmi les extensions galoisiennes de K modérément ramifiées, de groupe de Galois G, dans lesquelles un idéal premier de K donné est totalement décomposé.

Mots-clés: structure des modules galoisiens, extensions galoisiennes modérément ramifiées, modules localement libres, norme réduite, classes réalisables, groupe des classes des modules localement libres, Théorème de Stickelberger.

Universiteit Leiden
Mathematisch Instituut
Postbus 9512
2300 RA Leiden
NEDERLAND

Université Bordeaux I
Institut des Mathématiques de Bordeaux
351, cours de la Libération
F 33405 TALENCE cedex
FRANCE

Contents

Nomenclature

K	Algebraic number field
O_K	Ring of integers of K
G	Finite group
G^{ab}	Abelianization of G
$\mathrm{Irr}(G)$	Set of irreducible characters of G
R_G	Ring of $\mathbb{Z}$-linear combinations of elements in $\mathrm{Irr}(G)$
$\mathcal{A}_G$	Augmentation kernel
$\tilde{\chi}$	Complex conjugate of the character χ
$\{q\}$	Fractional part of q
$\lfloor q \rfloor$	Integral part of q
$[f]$	Class with representative f
$Z(A)$	Center of A
$\bar{s}$	Conjugacy class of s
$\bar{G}$	Set of conjugacy classes of G
rn	Reduced norm
$K_{\mathfrak{p}}$	Completion of K with respect to its place $\mathfrak{p}$
K^{c} (resp. $K_{\mathfrak{p}}^{\mathrm{c}}$)	An algebraic closure of K (resp. $K_{\mathfrak{p}}$)
K^{nr}	Maximal extension of K unramified at finite places
$K_{\mathfrak{p}}^{\mathrm{nr}}$	Maximal unramified extension of $K_{\mathfrak{p}}$, if $\mathfrak{p}$ is finite
	$K_{\mathfrak{p}}^{\mathrm{nr}} = K_{\mathfrak{p}}^{\mathrm{c}}$, if $\mathfrak{p}$ is infinite
K^{t}	Maximal tame extension of K
$K_{\mathfrak{p}}^{\mathrm{t}}$	Maximal tame extension of $K_{\mathfrak{p}}$, if $\mathfrak{p}$ is finite
	$K_{\mathfrak{p}}^{\mathrm{t}} = K_{\mathfrak{p}}^{\mathrm{c}}$, if $\mathfrak{p}$ is infinite
$O_{K,\mathfrak{p}}$	Completion of O_K with respect to $\mathfrak{p}$, if $\mathfrak{p}$ is finite
	$O_{K,\mathfrak{p}} = K_{\mathfrak{p}}$, if $\mathfrak{p}$ is infinite
O_K^{c} (resp. $O_{K,\mathfrak{p}}^{\mathrm{c}}$)	Integral closure of O_K (resp. $O_{K,\mathfrak{p}}$) in K^{c} (resp. $K_{\mathfrak{p}}^{\mathrm{c}}$)
Ω_K (resp. $\Omega_{K_{\mathfrak{p}}}$)	Absolute Galois group of K (resp. $K_{\mathfrak{p}}$)
Ω_K^{nr} (resp. $\Omega_{\mathfrak{p}}^{\mathrm{nr}}$)	$\mathrm{Gal}(K^{\mathrm{nr}}/K)$ (resp. $\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{nr}}/K_{\mathfrak{p}})$)
Ω_K^{t} (resp. $\Omega_{\mathfrak{p}}^{\mathrm{t}}$)	$\mathrm{Gal}(K^{\mathrm{t}}/K)$ (resp. $\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{t}}/K_{\mathfrak{p}})$)

$J(K)$	Group of idèles of K (including infinite places)
$U(O_K)$	$\prod_{\mathfrak{p}} O_{K,\mathfrak{p}}^{\times}$
$J(K^{\mathrm{c}})$	$\varinjlim J(L)$, as L runs over all fin. Galois ext. of K in K^{c}
$K[G]$ (resp. $K_{\mathfrak{p}}[G]$)	Group ring of G over K (resp. $K_{\mathfrak{p}}$)
$K^{\mathrm{c}}[G]$ (resp. $K_{\mathfrak{p}}^{\mathrm{c}}[G]$)	Group ring of G over K^{c} (resp. $K_{\mathfrak{p}}^{\mathrm{c}}$)
$O_K[G]$ (resp. $O_{K,\mathfrak{p}}[G]$)	Group ring of G over O_K (resp. $O_{K,\mathfrak{p}}$)
$J(K[G])$	Group of idèles of $K[G]$ (including infinite places)
$U(O_K[G])$	$\prod_{\mathfrak{p}} O_{K,\mathfrak{p}}[G]^{\times}$,
$A_G(K)$	Set of isomorphism classes of G-Galois K-algebras
$A_G^{\mathrm{t}}(K)$	Set of isom. classes of tame G-Galois K-algebras
$A_G'(K)$	Set of isom. classes of G-Galois K-alg. unram. at $\mathfrak{p}\big\|\|G\|$
$F_G(K)$	Set of isom. classes of G-Galois field ext. of K
$F_G^{\mathrm{t}}(K)$	Set of isom. classes of tame G-Galois field ext. of K
$F_G'(K)$	Set of isom. cl. of G-Galois field K-ext. unram. at $\mathfrak{p}\big\|\|G\|$
$\mathrm{Cl}(O_K)$	Ideal class group of K
$\mathrm{Cl}(O_K[G])$	Locally free class group of $O_K[G]$
$R_{\mathrm{t}}(O_K, G)$	Set of Steinitz classes given by tame G-Galois K-alg.
$R_A(O_K[G])$	Set of classes realized by tame G-Galois K-alg.
$R_F(O_K[G])$	Set of classes realized by tame G-Galois field ext. of K
$R_{\mathrm{nr}}(O_K[G])$	Set of classes realized by unramified G-Galois K-alg.
$H(K[G])$	$\{\alpha \in K^{\mathrm{c}}[G]^{\times} \mid \alpha^{-1} \cdot \alpha^{\omega} \in G,\ \forall \omega \in \Omega_K\}$
$\mathcal{H}(K[G])$	$H(K[G])/G$
$H(K_{\mathfrak{p}}[G])$	$\left\{\alpha \in K_{\mathfrak{p}}^{\mathrm{c}}[G]^{\times} \mid \alpha^{-1} \cdot \alpha^{\omega} \in G,\ \forall \omega \in \Omega_{K_{\mathfrak{p}}}\right\}$
$\mathcal{H}(K_{\mathfrak{p}}[G])$	$H(K_{\mathfrak{p}}[G])/G$
$H(O_{K,\mathfrak{p}}[G])$	$\left\{\alpha \in O_{K,\mathfrak{p}}^{\mathrm{c}}[G]^{\times} \mid \alpha^{-1} \cdot \alpha^{\omega} \in G,\ \forall \omega \in \Omega_{K_{\mathfrak{p}}}\right\}$
$\mathcal{H}(O_{K,\mathfrak{p}}[G])$	$H(O_{K,\mathfrak{p}}[G])/G$
$\left(K\bar{\Lambda}\right)^{\times}$	$\mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\bar{G}(-1)], (K^{\mathrm{c}})^{\times}\right)$
$\bar{\Lambda}^{\times}$	$\mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\bar{G}(-1)], (O_K{}^{\mathrm{c}})^{\times}\right)$
$J(K\bar{\Lambda})$	Restricted direct product of $\left(K\bar{\Lambda}\right)^{\times}$ w.r.t. $\bar{\Lambda}^{\times}$
$\mathrm{MCl}(O_K[G])$	$\dfrac{\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, J(K^{\mathrm{c}}))}{(\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}) \cdot \prod_{\mathfrak{p}} \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G])))}$

Acknowledgements

A first thank to the institutions who financially supported my research during these three years. I gratefully acknowledge the Universiteit Leiden, the Université Bordeaux I and the ALGANT project.

This dissertation could not have been written without my two supervisors. I am grateful to Boas Erez for having suggested me the research project of my thesis three years ago and having taught me how to paddle my own canoe, and to Bart de Smit for all the insightful mathematical discussions we had in Leiden and for his care of having a final version of this manuscript as correct and clear as possible.

I thank Nigel Byott for having accepted to review my thesis and for the careful and detailed corrections he sent me. I also thank Adebisi Agboola, not just for having reviewed this dissertation with plenty of useful suggestions, but also for the fantastic hospitality he gave me during my short stay in Santa Barbara and for all the e-mails he sent me (without any delay) replying to every doubt and question on my research subject I had. It has been a honor to have them as reviewers of my thesis.

I would also like to thank Hendrik W. Lenstra and Peter Stevenhagen, who had the infliction of reading this manuscript and provided me with plenty of insightful comments and suggestions.
A special thank goes to Philippe Cassou-Noguès for his help during my stay in Bordeaux, for his constant support, for his humility and for his ability to convey joy all around him. He is an example to me.
I am also indebted to the rest of my defense committee, that I thank for being present in this important occasion.
Among all the other professors that I met during these three years I would like to heartily thank: Bas Edixhoven, Qing Liu, Lenny Taelman and Ronald van Luijk. I am particularly grateful to Yuri Bilu for his friendship and for having been the best teacher I ever had.

I am grateful to all the ALGANT staff, with a particular thank to Virginie and Christopher. My thank goes also to the administrative staff at the Mathematisch Instituut in Leiden and at the IMB in Bordeaux. In particular I am indebted to Pauline, Christine, Ida, Karine, Catherine, who made French bureaucracy seem easier than it actually is. A special thank to Marilyne, for her cheerfulness and cooking tips.

Let me now spend some words to thank all my colleagues. First of all I thank Luca Caputo and Alessandro Cobbe for their suggestions and for the unforgettable week we shared in Morocco. Then I am grateful to Giovanni Rosso for his visit in Bordeaux and the night I spent at his place in Paris.
I thank all the PhD students in Leiden: Alberto and Samuele for our friendships and the warm hospitality they gave during my stays in Leiden; Michiel for the Dutch translations, for every mathematical suggestion and for our runnings all around the Netherlands; Dino and Jacopo who also were condemned to have me as a flatmate for one year; Ariyan for all the funny jokes and situations we had together; Diego for our soccer discussions; Liu, his wife Bo and Weidong for having introduced me to the Chinese culture with plenty of delicious dinners; Krysztof, Tanos and all the others.
I also heartly thank my officemate in Bordeaux Sophie for the time we spent together and all the other PhD students in Bordeaux: Clément (for the French corrections and the course we taught together), Florence, Nicolas, Aurélien, Pierre, Bruno, Samuel, Guhan, Wen and all the others.
I extend my heartfelt thanks to Dajano and Nicola, with a special thank to the last one for having lent me his computer when mine "had drunk too much beer" in a crucial point of the write up of this dissertation.

I am heartily grateful to Alberto, Giovanni and Nicola who started with me our adventure in Bordeaux four years ago. In particular I would like to thank Giovanni and Nicola who lived with me for three years and are like a sort of second family for me, thank you!

I will never forget this delightful last year in Bordeaux thanks to: Alessio, Dario, Anthony, Agostino and Aurélie. Thanks for your presence!

I also thank all my friends in Italy: Anna and Michele, Alberto and Silvia, Filippo and Silvia, Giulia, Giorgio, Luca, Cristina and Pierpaolo, Carlo and Elisa. Every e-mail and phone call we had, made me feel less far from home and kept me company during these years.

Last but not least, a heartfelt thank to my family for their constant support and encouragement. *Anche se lontani fisicamente, siamo sempre stati vicini nel cuore.*

My greatest thank goes to my future wife Elena, for her love, patience, support and for having been able to bear my absence from home during the last long four years... "Roads? Where we are going we do not need roads!"

To Lorenza and Giulietta

Chapter 0

Introduction

Throughout this dissertation we will study properties of the structure of rings of integers in Galois extensions, when seen as Galois modules.
Let K be an algebraic number field and let L/K be a finite Galois extension with Galois group G (abbreviated as G-Galois extension in the sequel). The question which gives rise to the main subject of this thesis is: when does there exist a normal integral basis generator for L over K, i.e. an element $a \in O_L$ such that $\{s \cdot a\}_{s \in G}$, the set of translates of a by the elements of G, forms an O_K-basis of O_L? Or in another equivalent form, does there exist an element $a \in O_L$ such that $O_L = O_K[G] \cdot a$?
This question goes under the name of Normal Integral Basis Problem (NIBP). Note that, from the Normal Basis Theorem (see [23]), we know that for any G-Galois extension L/K, there exists an element $b \in L$ such that $L = K[G] \cdot b$ (such an element b is called normal basis generator of L/K).

When the base field K equals $\mathbb{Q}$ and the group G is abelian, the NIBP is completely solved by the Hilbert–Speiser Theorem. From the Kronecker–Weber Theorem we know that any abelian G-Galois extension $L/\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$ and we define the conductor of L to be the smallest natural number r such that $L \subseteq \mathbb{Q}(\zeta_r)$. Then the Hilbert–Speiser theorem says that a finite abelian extension $L/\mathbb{Q}$ has a normal integral basis if and only if its conductor is square-free, or equivalently if $L/\mathbb{Q}$ is tamely ramified (i.e. for any prime (p) of $\mathbb{Z}$, its ramification index in L is coprime to p, or equivalently the trace map from O_L to $\mathbb{Z}$ is surjective).
It is shown in [21] that the field $\mathbb{Q}$ is the only field with this property, i.e. such that any finite abelian tame Galois extension over it has a normal integral basis.

It is clear that, if a G-Galois extension L/K has a normal integral basis, then for any prime ideal $\mathfrak{p}$ of O_K also $O_{L,\mathfrak{p}} := O_{K_\mathfrak{p}} \otimes_{O_K} O_L$ (where $K_\mathfrak{p}$ is the completion of K with respect to the topology induced by $\mathfrak{p}$) has a normal integral basis, i.e. there exists $a_\mathfrak{p} \in O_{L,\mathfrak{p}}$ such that $O_{L,\mathfrak{p}} = O_{K_\mathfrak{p}}[G] \cdot a_\mathfrak{p}$. We call an $O_K[G]$-module with this property locally free of rank 1 (see §1.1 for a precise definition).
For local extensions, tameness is a necessary and sufficient condition for the existence of a normal integral basis (as it was globally over $\mathbb{Q}$ by the Hilbert–Speiser Theorem), as Noether's Criterion explains.

Theorem 0.0.1 (Noether's Criterion)**.** *Let L/K be a finite G-Galois extension. Then L/K is tamely ramified if and only if O_L is a locally free $O_K[G]$-module of rank* 1*.*

We understand from this that, over a general number field K, the right framework to study the normal integral basis problem is given by tame extensions.
So restricting our attention to tame G-Galois extensions over K, we can see the NIBP as a question about when a locally free $O_K[G]$-module is actually free.
The main way of approaching such a question is to translate it in terms of a computation inside a particular classgroup that will be denoted by $\mathrm{Cl}(O_K[G])$. The precise definition of this group will be given in Chapter 1.
The idea behind its definition is analogous to the one leading to the definition of the classical classgroup $\mathrm{Cl}(O_K)$, which can be considered for the moment as a prototype of $\mathrm{Cl}(O_K[G])$ (it will coincide with it in the case $G = 1$). The classgroup $\mathrm{Cl}(O_K)$ measures how far O_K is from being a principal ideal domain; more precisely any ideal $\mathfrak{p}$ of O_K is clearly O_K-locally free (since $O_{K_\mathfrak{p}}$ is a principal ideal domain) and its class in $\mathrm{Cl}(O_K)$ is trivial if and only if $\mathfrak{p}$ is O_K-free.
With this in mind, basic K-theory will lead to a rigorous definition (§1.3) of the locally free classgroup $\mathrm{Cl}(O_K[G])$; where, if G is abelian, the class $[M]$ of a locally free $O_K[G]$-module M is trivial if and only if M is free (when G is not abelian a slightly modified version of this holds, see §1.3 and §1.4). As we will see, $\mathrm{Cl}(O_K[G])$ is a finite abelian group.
Thus to any tame G-Galois extension L/K we can associate the class of its ring of integers $[O_L]$ in $\mathrm{Cl}(O_K[G])$. Noether's Criterion holds in general for G-Galois algebras over K (see §1.9 for a precise definition), which are a generalization of the notion of G-Galois field extensions over K. Hence, as for field extensions, to any tame G-Galois K-algebra we can associate a class in $\mathrm{Cl}(O_K[G])$.
It is well-known that the set of isomorphism classes of G-Galois K-algebras is in bijection with $H^1(\Omega_K, G)$ (see [35, §5] for a precise definition), the first cohomology set of the absolute Galois group Ω_K with coefficients in G (where Ω_K acts trivially

on G). Hence we can consider the following morphism of pointed sets:

$$\begin{aligned} \mathcal{R} : H^1(\Omega_K^{\mathrm{t}}, G) &\longrightarrow \mathrm{Cl}(O_K[G]) \\ [L] &\longmapsto [O_L], \end{aligned}$$

where Ω_K^{t} denotes the Galois group of the maximal tame extension over K. In terms of this map, the NIBP reduces to the study of the kernel of $\mathcal{R}$ (i.e. the inverse image of the trivial class in $\mathrm{Cl}(O_K[G])$). Note that, for any finite group G, the set $H^1(\Omega_K^{\mathrm{t}}, G)$ is defined as the pointed set $\mathrm{Hom}\,(\Omega_K^{\mathrm{t}}, G)\,/\mathrm{Inn}(G)$ (where $\mathrm{Hom}\,(\Omega_K^{\mathrm{t}}, G)$ is the set of continuous homomorphisms from Ω_K^{t} to G and $\mathrm{Inn}(G)$ is the set of inner automorphisms of G), so in particular, if G is abelian, $H^1(\Omega_K^{\mathrm{t}}, G)$ is equal to the group $\mathrm{Hom}\,(\Omega_K^{\mathrm{t}}, G)$.

The map $\mathcal{R}$ also allows us to define a new set, which is the main subject of this thesis: the set of realizable classes.
The set of realizable classes, denoted by $R(O_K[G])$, is defined as the image of $\mathcal{R}$, i.e. it is composed by all the classes in $\mathrm{Cl}(O_K[G])$ which can be obtained from the rings of integers of tame G-Galois K-algebras.

From what we have seen above, if G is abelian and K equals $\mathbb{Q}$, the set $R(\mathbb{Z}[G])$ is trivial. In all the other cases this set is quite difficult to study and describe. For example, over a general number field K and given a finite group G, a natural question is still open in general:

Question 1. *Is $R(O_K[G])$ a subgroup of $\mathrm{Cl}(O_K[G])$?*

Firstly note that $\mathcal{R}$, when not trivial, is not a priori a group homomorphism. Indeed, if G is not abelian, the domain is just a pointed set, but even if G is abelian, it is not difficult to find an example which explains why $\mathcal{R}$ is not a group homomorphism. For a deeper explanation of this fact, see Appendix.

Remark 0.0.2. *We could restrict the map $\mathcal{R}$ to the set of isomorphism classes of G-Galois field extensions of K, i.e. to the set of classes in $H^1(\Omega_K^{\mathrm{t}}, G)$ represented by surjective homomorphisms. The image of this restriction will be denoted by $R_F(O_K[G])$ and we will see that in many cases, with this restriction, we do not lose any realizable class, i.e. $R_F(O_K[G]) = R(O_K[G])$. When we shall want to distinguish between the two sets of realizable classes, we will denote $R(O_K[G])$ by $R_A(O_K[G])$.*

When the base field is $\mathbb{Q}$ and G is abelian we have already seen that $R(\mathbb{Z}[G]) = 1$. Thanks to a result by Taylor ([43]), proving a conjecture of Fröhlich, the same

holds if $K = \mathbb{Q}$ and G is a non-abelian group with no symplectic characters. More generally he proved that any element in $R(\mathbb{Z}[G])$ has order at most 2 in $\mathrm{Cl}(\mathbb{Z}[G])$.

Remark 0.0.3. *Note that we could also restrict our attention to $R_F(\mathbb{Z}[G])$ in the statement of Taylor's general result, even if, in this case, one has to take care of the inverse Galois problem. Indeed, given a finite group G, before investigating the structure of the set $R_F(\mathbb{Z}[G])$, one has to be sure that there exists at least a G-Galois field extension of $\mathbb{Q}$. The study of this question goes under the name of inverse Galois problem and, for a general non-abelian group G, is still one of the main open problems in number theory.*

Over a general number field K, when G is abelian, a positive answer to Question 1 is given by Leon McCulloh in [28].
Given a finite group G, he introduced a subgroup $\mathrm{St}(O_K[G])$ of $\mathrm{Cl}(O_K[G])$ (the notation used here differs from the original one by McCulloh), defined in terms of some Stickelberger maps (see Chapter 2), and he proved the following result.

Theorem 0.0.4. *Let G be a finite abelian group, then*

$$R_F(O_K[G]) = R_A(O_K[G]) = \mathrm{St}(O_K[G]).$$

In particular $R_A(O_K[G])$ is a subgroup of $\mathrm{Cl}(O_K[G])$.

When G is non-abelian, he managed to prove the following inclusion (this is an unpublished result announced in a talk given in Oberwolfach in February 2002 - a detailed proof of it will be the main subject of Chapter 2).

Theorem 0.0.5. *For any finite group G,*

$$R(O_K[G]) \subseteq \mathrm{St}(O_K[G]).$$

The proof of the reverse inclusion still remains an open problem.

When G is non-abelian and $K \neq \mathbb{Q}$, determining if $R(O_K[G])$ forms a subgroup is in general an open problem.
Nevertheless, with an approach different from McCulloh's that starts from the inclusion $R(O_K[G]) \subseteq \mathrm{Cl}^\circ(O_K[G])$ (where $\mathrm{Cl}^\circ(O_K[G])$ is the kernel of the augmentation map from $\mathrm{Cl}(O_K[G])$ to $\mathrm{Cl}(O_K)$, see §3.1), some non-abelian results have been achieved. In particular, it has been proved that $R(O_K[G]) = \mathrm{Cl}^\circ(O_K[G])$ in the following cases: $G = D_8$, the dihedral group of order 8, with the assumption

that the ray class group modulo $4O_K$ of O_K has odd order (see [10]); and $G = A_4$, without any restriction on K (see [11]).
Recently in [9], Nigel P. Byott and Bouchaib Sodaïgui, under the assumption that K contains a root of unity of prime order p, showed that $R(O_K[G])$ is a subgroup of $\mathrm{Cl}(O_K[G])$, when G is the semidirect product $V \rtimes C$ of an elementary abelian group V of order p^r by any non-trivial cyclic group C which acts faithfully on V and makes V into an irreducible $\mathbb{F}_p[C]$-module (where $\mathbb{F}_p$ is the finite field with p elements). This last result contains as a corollary the main result of [11].
In the non-abelian context, more has been done in describing a weaker form of $R(O_K[G])$. If $\mathcal{M}$ denotes a maximal order in $K[G]$ containing $O_K[G]$, then, as done for $R(O_K[G])$, we can define $R(\mathcal{M})$ to be the subset in $\mathrm{Cl}(\mathcal{M})$ of classes $[\mathcal{M} \otimes_{O_K[G]} O_L]$, where L is a tame G-Galois algebra over K. The two sets $R(\mathcal{M})$ and $R(O_K[G])$ are linked by the extension of scalars $\mathrm{Ex} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(\mathcal{M})$ and in fact one has $R(\mathcal{M}) = \mathrm{Ex}(R(O_K[G]))$.
A complete list, as far as we are aware, of works investigating the structure of $R(\mathcal{M})$ follows: [37] with $G = H_8$; [39] with $G = D_4$; [20] with $G = A_4$; [8] with $G = V \rtimes_\rho C$, where V is a vector space of dimension r over the finite field with 2 elements $\mathbb{F}_2$, C is a cyclic group of order $2^r - 1$ and ρ is a faithful representation of C in V; [40] with $G = S_4$; [6] with $G = V \rtimes_\rho C$, where V is a vector space of dimension r over the finite field with p elements $\mathbb{F}_p$, C is a cyclic group of order $p^r - 1$ and ρ a faithful representation of C in V; [38] with $G = H_{4l}$ and [32] with $G = C_l \rtimes C_m$ (where C_l and C_m are cyclic groups of order l and m respectively; this article also improves another previous similar work [36]). Note that [6] and [8] are improved by [9].

Apart from studying the structure of $R(O_K[G])$, more has been done on realizable classes and, as an example of them, we cite the work by Adebisi Agboola [1] (which improves a previous result by K. Foster [16]).
Given G abelian, once one knows the description of $R(O_K[G])$ in terms of the Stickelberger group $\mathrm{St}(O_K[G])$, one may wonder if the G-module structures of rings of integers of G-Galois K-algebras are equidistributed among the set of realizable classes. Agboola managed to prove that the asymptotic number (with a slight restriction) of tame G-Galois extensions over K which realize a class $c \in R(O_K[G])$, counted by the absolute norm of the product of ramified primes, does not depend on the given class c (for details see Chapter 5).

Some motivations to study realizable classes are given, as noted in [1], by the fact for example that they arise in looking for an explicit analog of known Adams–Riemann–Roch Theorems for $\mathrm{Cl}(O_K[G])$ (see [2, §4]).

Moreover realizable classes are useful to deduce some results on another related open subject in number theory: the problem of Steinitz classes. Given L a G-Galois K-algebra, we know that $O_L \cong O_K^{[L:K]-1} \oplus I$ as O_K-modules, where I is a fractional ideal of O_K. The associated class $[I]$ in $\mathrm{Cl}(O_K)$ is called the Steinitz class of L/K. Analogously to the set of realizable classes, the collection of all classes in $\mathrm{Cl}(O_K)$ which can be obtained as Steinitz classes of tame G-Galois field extensions of K defines the set of Steinitz classes denoted by $R_{\mathrm{t}}(O_K, G)$. The set of realizable classes and the set of Steinitz classes are linked by the restriction map $\mathrm{res}^G_{\{1\}} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_K)$ (see §1.8.1), indeed under this map $\mathrm{res}^G_{\{1\}}(R(O_K[G])) = R_{\mathrm{t}}(O_K, G)$.

In this thesis, we shall investigate some questions on the problem of realizable classes with particular regard to the Stickelberger subgroup $\mathrm{St}(O_K[G])$, introduced by McCulloh, and we will study some new problems related to the equidistribution result of Agboola.

We shall start in Chapter 1 with some preliminary notions and prerequisites on the locally free classgroup $\mathrm{Cl}(O_K[G])$, giving a good reference for people interested in the subject.

Chapter 2 will be devoted to McCulloh's results, in particular we shall give the unpublished proof (by McCulloh) of the inclusion $R(O_K[G]) \subseteq \mathrm{St}(O_K[G])$ in the non-abelian case (Theorem 0.0.5). The chapter will finish with a sketch of the proof of the equality given in Theorem 0.0.4, of which the original version is contained in [28].

Chapter 3 will contain the first new results. After a general comparison of the Stickelberger group $\mathrm{St}(O_K[G])$ and $\mathrm{Cl}^\circ(O_K[G])$ (see above), we will explicitly compute, just using its definition, $\mathrm{St}(\mathbb{Z}[G])$ in the cases $G = C_p$, a cyclic group of prime order p, and $G = D_p$, a dihedral group of order $2p$ (with p an odd prime). In particular we shall prove the following theorem.

Theorem 0.0.6. *Let p be an odd prime number. If $G = C_2$, a cyclic group of order 2, or $G = C_p$, a cyclic group of order p or $G = D_p$, the dihedral group of order $2p$, then* $\mathrm{St}(\mathbb{Z}[G]) = 1$.

In Chapter 4 we shall study the behavior of $\mathrm{St}(O_K[G])$ under the change of base field K. Namely, if L is a number field containing K, there is a restriction map $\mathcal{N}_{L/K} : \mathrm{Cl}(O_L[G]) \longrightarrow \mathrm{Cl}(O_K[G])$ (see §1.8.3). We shall prove the following result.

Theorem 0.0.7. *For every finite group G,*

$$\mathcal{N}_{L/K}(\mathrm{St}(O_L[G])) \subseteq \mathrm{St}(O_K[G]).$$

This will have some nice consequences, such as a new proof of a result of Taylor, contained in [43], which says that the ring of integers of an abelian G-Galois tame extension over K is free over $\mathbb{Z}[G]$.

In the last chapter, restricting ourselves to the abelian case, we will start the investigation of the connections between the work of Agboola [1] and the work of M. M. Wood [47]. Given G a finite abelian group, in [1], Agboola studied the distribution of the G-Galois algebras over a number field K with respect to the group of realizable classes, while Wood, in [47], studied the distribution of local behaviors in abelian G-Galois field extensions. The main result of the chapter will consist of a description of $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, the set of realizable classes given by tame G-Galois K-algebras totally split at a given finite prime $\mathfrak{p}$ of K. After introducing the group $\mathrm{St}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, a modified version of the original Stickelberger subgroup $\mathrm{St}(O_K[G])$, we shall prove the following result.

Theorem 0.0.8. *Let G be a finite abelian group. Then*

$$R_{\mathrm{ts},\mathfrak{p}}(O_K[G]) = \mathrm{St}_{\mathrm{ts},\mathfrak{p}}(O_K[G]).$$

In the second part of the chapter we will adapt the equidistribution results contained in [1] to $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$. Namely, let us consider $A'_G(K)$ the set of isomorphism classes of G-Galois K-algebras unramified at the primes dividing $|G|$. Moreover, given $L \in A'_G(K)$, let us denote by $D(L/K)$ the absolute norm of the product of primes of O_K that ramify in L. Then, given $c \in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, let us define

$$\mathrm{Pr}_{\mathrm{ts},\mathfrak{p}}(c) := \lim_{X\to\infty} \frac{\sharp\{[L] \in A'_G(K) |\, L_{\mathfrak{p}} \text{ tot. split at } \mathfrak{p},\, [O_L] = c,\, D(L/K) \leq X\}}{\sharp\{[L] \in A'_G(K) |\, D(L/K) \leq X\}}.$$

In the last chapter we shall prove the following result.

Theorem 0.0.9. *Given $c \in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, the limit $\mathrm{Pr}_{\mathrm{ts},\mathfrak{p}}(c)$ exists and it does not depend on the given realizable class c.*

The chapter will end by highlighting the connections between [1] and [47] with regard to the totally split situation. In particular we shall prove that, with regard to the totally split case, the events considered by Agboola and Wood, respectively, are independent if and only if $R_{\mathrm{ts},\mathfrak{p}}(O_K[G]) = R(O_K[G])$.

0.1 Notations

Let K be a number field and O_K its ring of integers. Given a place $\mathfrak{p}$ of K, we denote by $K_\mathfrak{p}$ its completion with respect to the metric defined by $\mathfrak{p}$: if $\mathfrak{p}$ is a finite place, then $K_\mathfrak{p}$ is a non-archimedean field which is a finite extension of $\mathbb{Q}_p$ (where p is the characteristic of $O_K/\mathfrak{p}$); if $\mathfrak{p}$ is an infinite place, then $K_\mathfrak{p}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$.
We choose an algebraic closure K^c (resp. $K_\mathfrak{p}^c$) of K (resp. $K_\mathfrak{p}$) and, for each (finite or infinite) prime $\mathfrak{p}$ of K, we fix an embedding $\widehat{i_\mathfrak{p}} : K^c \longrightarrow K_\mathfrak{p}^c$. Let Ω_K (resp. $\Omega_{K\mathfrak{p}}$) denote the Galois group of K^c/K (resp. $K_\mathfrak{p}^c/K_\mathfrak{p}$). When no confusion arises, to simplify the notation, we will just write Ω (resp. $\Omega_\mathfrak{p}$). We denote by $i_\mathfrak{p}$ the corresponding embedding of $\Omega_\mathfrak{p}$ into Ω.
The symbol Ω^{nr} (resp. $\Omega_\mathfrak{p}^{nr}$) will denote the Galois group of the maximal unramified (at finite places) extension K^{nr}/K (resp. $K_\mathfrak{p}^{nr}/K_\mathfrak{p}$) in K^c (resp. $K_\mathfrak{p}^c$) and Ω^t (resp. $\Omega_\mathfrak{p}^t$) will be the Galois group of the maximal tame extension K^t/K (resp. $K_\mathfrak{p}^t/K_\mathfrak{p}$) in K^c (resp. $K_\mathfrak{p}^c$). At the infinite places we take $K_\mathfrak{p}^{nr} = K_\mathfrak{p}^t = K_\mathfrak{p}^c$.
If $\mathfrak{p}$ is a finite place, let $O_{K,\mathfrak{p}}$ be the completion of O_K with respect to $\mathfrak{p}$ (which also coincides with the ring of integers of the completion $K_\mathfrak{p}$) and $O_{K,\mathfrak{p}}^c$ the integral closure of O_K in $K_\mathfrak{p}^c$. If $\mathfrak{p}$ is an infinite place, we define $O_{K,\mathfrak{p}}$ to be $K_\mathfrak{p}$.

Let $J(K)$ denote the group of idèles of K, i.e. the restricted direct product of $\{K_\mathfrak{p}^\times\}_\mathfrak{p}$ with respect to $\{O_{K,\mathfrak{p}}^\times\}_\mathfrak{p}$, where $\mathfrak{p}$ runs through the places of K (both finite and infinite). We consider $K^\times$ diagonally embedded in $J(K)$ and $U(O_K)$ will denote the product $\prod_\mathfrak{p} O_{K,\mathfrak{p}}^\times$. Similarly, given a finite group G, the idèle group $J(K[G])$ is the restricted direct product of the unit groups of group rings $\{K_\mathfrak{p}[G]^\times\}_\mathfrak{p}$ with respect to $\{O_{K,\mathfrak{p}}[G]^\times\}_\mathfrak{p}$, where $\mathfrak{p}$ runs through the places of K.
The notation $J(K^c)$ (resp. $U(O_K^c)$) will denote the direct limit of the idèle groups $J(L)$ (resp. $U(O_L)$), as L runs over all finite Galois extensions of K inside K^c.

When we consider a representative for a class in a class group, we use the brackets $[-]$ to denote its class (e.g. $[O_L]$ denotes the class in $\mathrm{Cl}(O_K[G])$ corresponding to the ring of integers O_L of a tame G-Galois algebra L/K).

Throughout this dissertation, G will denote a finite group, G^{ab} its abelianization and $\bar{G}$ its set of conjugacy classes. Given $s \in G$, we denote by $\bar{s}$ its conjugacy class.
The set of irreducible complex characters of G will be denoted by $\mathrm{Irr}(G)$ (occasionally by $\widehat{G}$). The symbol R_G will denote the ring of virtual characters of G, i.e.

the ring of $\mathbb{Z}$-linear combinations of elements in $\mathrm{Irr}(G)$. The complex conjugate of a character χ will be denoted by $\tilde{\chi}$.

If Y is a group acting on the left on a set X, we denote the action of $y \in Y$ on $x \in X$ by the symbol x^y (occasionally by $y \cdot x$); note in particular that $(x^y)^z = x^{zy}$. If Y is a group acting on two groups H and H', we denote by $\mathrm{Hom}_Y(H, H')$ the set of all group homomorphisms from H to H' fixed by the action of Y; in other words, let $f \in \mathrm{Hom}(H, H')$ (group homomorphisms), then $f \in \mathrm{Hom}_Y(H, H')$ if and only if $f(h^y) = (f(h))^y$, for all $y \in Y$ and $h \in H$.

If we choose an embedding of K^{c} in $\mathbb{C}$, then the values of the irreducible characters of G are in K^{c} and we get that the absolute Galois group Ω naturally acts on the left on $\mathrm{Irr}(G)$ by $\chi^\omega(s) = \chi(s)^\omega$, for all $\omega \in \Omega$ and $s \in G$. We extend this action by linearity to R_G. When we have an Ω-action on a set, we can always consider a $\Omega_{\mathfrak{p}}$-action on the same set, via the embedding $i_{\mathfrak{p}}$.

All these notations and further ones that we will encounter in this thesis are listed in the Nomenclature page.

Chapter 1

Prerequisites

In this chapter we will recall some general results linked to the notion of locally free class group. Throughout this chapter, unless otherwise stated, let R be a Dedekind domain with quotient field an algebraic number field K.

Definition 1.0.1 (Finite dimensional separable algebra)**.** *Let L be a field. A finite dimensional separable L-algebra B is a finite dimensional semisimple L-algebra such that the center of each simple component of B is a separable field extension of L.*

As proved in [30, Theorem 7.18], the following result holds.

Theorem 1.0.2. *Let B be a finite dimensional L-algebra. The following are equivalent:*

- *B is a finite dimensional separable L-algebra;*
- *There exists a finite separable field extension E/L such that*

$$E \otimes_L B \cong \prod_{i=1}^{s} \mathrm{M}_{n_i}(E),$$

  as E-algebras, where $\mathrm{M}_{n_i}(E)$ is the E-algebra of $n_i \times n_i$ matrices over E and s is a natural number;

- *For every field $F \supseteq L$, $F \otimes_L B$ is semisimple.*

Thus, from now on, given our algebraic number field K, let us consider a finite dimensional separable K-algebra A.

Definition 1.0.3 (Order)**.** *Let S be a Dedekind domain with field of fractions L. An S-order in a finite dimensional separable L-algebra B is a subring Γ of B such that:*

- *S is contained in the center of Γ;*
- *Γ is finitely generated as S-module;*
- *$L \cdot \Gamma = B$.*

Thus, from now on, given our K-algebra A, let us take an R-order Λ in A.

Definition 1.0.4 (Λ-lattice)**.** *A Λ-lattice M is a left Λ-module which is finitely generated and projective as R-module.*

All these definitions are taken from [14, §23].

We shall start this chapter by introducing the definition of locally free module.

1.1 Locally free modules

Given a maximal ideal $\mathfrak{p}$ of R, let us denote by $R_{\mathfrak{p}}$ its *completion* with respect to the metric induced by $\mathfrak{p}$. We then define

$$\Lambda_{\mathfrak{p}} := R_{\mathfrak{p}} \otimes_R \Lambda.$$

Analogously given a Λ-lattice M, let us define $M_{\mathfrak{p}} := R_{\mathfrak{p}} \otimes_R M$.

Definition 1.1.1 (Locally free Λ-lattice)**.** *Let $n \in \mathbb{Z}_{\geq 0}$. A Λ-lattice M is said to be locally free of rank n (or locally free of constant rank n) if*

$$M_{\mathfrak{p}} \cong \Lambda_{\mathfrak{p}}^n, \text{ as } \Lambda_{\mathfrak{p}}-\text{modules},$$

for each maximal ideal $\mathfrak{p}$ of R. We then define $\mathrm{rk}(M) := n$.

Example 1.1.2. *In this thesis we will frequently consider G-Galois field extensions L/K, with G a finite group. Then the group ring $K[G]$ is clearly a finite dimensional separable K-algebra and if we consider $R = O_K$ (the ring of integers of K), then $O_K[G]$ is an O_K-order and O_L is an $O_K[G]$-lattice.*
Moreover, when the G-Galois field extension L/K is tame, Noether's Criterion (see Chapter 0) states that O_L is a locally free $O_K[G]$-module of rank 1.

Note that in our definition of locally free Λ-lattices of rank n we could consider $R_{(\mathfrak{p})}$ (resp. $\Lambda_{(\mathfrak{p})} := R_{(\mathfrak{p})} \otimes_R \Lambda$ and $M_{(\mathfrak{p})} := R_{(\mathfrak{p})} \otimes_R M$), where $R_{(\mathfrak{p})}$ is the localization of R with respect to a maximal ideal $\mathfrak{p}$ of R, instead of $R_{\mathfrak{p}}$ (resp. $\Lambda_{\mathfrak{p}}$ and $M_{\mathfrak{p}}$). Replacing completions by localizations gives an equivalent version of Definition 1.1.1, due to the following result contained in [14, Proposition 30.17].

Proposition 1.1.3. *Let $\mathfrak{p}$ be a maximal ideal of R and let M and N be two Λ-lattices. Then*

$$M_{\mathfrak{p}} \cong N_{\mathfrak{p}} \text{ as } \Lambda_{\mathfrak{p}}\text{-modules} \iff M_{(\mathfrak{p})} \cong N_{(\mathfrak{p})} \text{ as } \Lambda_{(\mathfrak{p})}\text{-modules.}$$

Remark 1.1.4. *The same definition of locally free Λ-lattices applies even when K is just the fraction field of a Dedekind domain R (we do not need the fact that K is assumed to be an algebraic number field). In fact, the results in section 1.2 and 1.3 also hold in this more general setting.*

1.2 Link with projective modules

The locally free notion is strictly connected to the definition of projective modules, as we shall explain in this section.

Proposition 1.2.1. *Let Λ be an R-order and M a Λ-lattice. If M is a locally free Λ-lattice of rank n then M is a finitely generated projective Λ-module.*

Proof. Since, for every maximal ideal $\mathfrak{p}$ of R, the lattice $M_{\mathfrak{p}}$ is free as a $\Lambda_{\mathfrak{p}}$-module (and the same is true considering localizations), we deduce that, for all maximal ideals $\mathfrak{p}$, the functor $\mathrm{Hom}_{\Lambda_{(\mathfrak{p})}}(M_{(\mathfrak{p})}, -)$ from the category of $\Lambda_{(\mathfrak{p})}$-modules to the category of $R_{(\mathfrak{p})}$-module is exact. This implies, since M is finitely presented, that $\mathrm{Hom}_{\Lambda}(M, -) \otimes_R R_{(\mathfrak{p})}$ is exact for all $\mathfrak{p}$. It follows that the functor $\mathrm{Hom}_{\Lambda}(M, -)$ from the category of Λ-modules to the category of R-modules is also exact. Therefore M is projective as a Λ-module. □

The reverse implication is not in general true. Nevertheless when Λ is a group ring $R[G]$ (with G a finite group and R satisfying an extra hypothesis detailed below), for every finitely generated projective Λ-module M there exists an $n \in \mathbb{Z}_{\geq 0}$, such that M is a locally free Λ-lattice of rank n. Before giving the precise result let us recall the following lemma contained in [33, Exercise 16.4].

Lemma 1.2.2. *Let G be a finite group. Suppose that for every prime number p dividing the order of the group $|G|$ there exists a maximal ideal $\mathfrak{p}$ of R with $R/\mathfrak{p}$ of characteristic p. Then if M is a projective $R[G]$-module this implies that $K \otimes_R M$ is a free $K[G]$-module.*

Thanks to this lemma, we can now prove the following result.

Proposition 1.2.3. *Let Λ be the group ring $R[G]$, with G a finite group and R satisfying the hypothesis of Lemma 1.2.2. Then every finitely generated projective Λ-module M is a locally free Λ-module of rank n, for some $n \in \mathbb{Z}_{\geq 0}$.*

Proof. In [41] Richard G. Swan showed that, given a maximal ideal $\mathfrak{p}$ of R and two projective $R_{\mathfrak{p}}[G]$-modules M and M' (where G is a finite group), then, if $K_{\mathfrak{p}} \otimes M$ is isomorphic to $K_{\mathfrak{p}} \otimes M'$, this implies that $M \cong M'$. Thus combining this result with Lemma 1.2.2, the proof follows. □

Example 1.2.4. *Of course, the ring of integers O_K satisfies the conditions of Proposition 1.2.3. So, if $\Lambda = O_K[G]$, an $O_K[G]$-lattice is projective if and only if there exists an $n \in \mathbb{Z}_{\geq 0}$, such that M is a locally free $O_K[G]$-lattice of rank n.*

1.3 Genus and locally free class group

We say that two Λ-lattices M and N are in the same genus (or are locally isomorphic) and we denote it by $M \vee N$ (or $N \in g(M)$), if

$$M_{\mathfrak{p}} \cong N_{\mathfrak{p}}, \ \forall\, \mathfrak{p} \text{ maximal ideal of } R,$$

as $\Lambda_{\mathfrak{p}}$-modules. A Λ-lattice in $g(\Lambda)$ is usually called a *locally free left Λ-ideal* in A.

Again, by Proposition 1.1.3, it is irrelevant if in the previous definition we use localizations instead of completions.
Our definition implies that, if M and N are in the same genus, then also for $\mathfrak{p} = 0$ (i.e. for all prime ideals of R) we have $M_0 = KM \cong KN = N_0$. This follows from the fact that for every maximal ideal $\mathfrak{p}$ we have $KM \cong KM_{(\mathfrak{p})}$ (resp. $KN \cong KN_{(\mathfrak{p})}$).

Definition 1.3.1 (Maximal order)**.** *A maximal order Γ in A is an R-order such that, for all R-orders Γ' with $\Gamma \subseteq \Gamma'$, we have $\Gamma = \Gamma'$.*

Remark 1.3.2. *In general checking that two Λ-lattices M and N are in the same genus reduces to checking local isomorphism at a finite set of maximal ideals. More precisely, if*

$$S(\Lambda) := \{\mathfrak{p} \mid \Lambda_{\mathfrak{p}} \text{ is not a maximal } R_{\mathfrak{p}}\text{-order in } A_{\mathfrak{p}}\}$$

is not empty, for having $M \vee N$ it is sufficient that $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ for all $\mathfrak{p} \in S(\Lambda)$. This follows from the fact that if $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ for at least one maximal ideal, then $KM \cong KN$, which implies that $KM_{\mathfrak{p}} \cong KN_{\mathfrak{p}}$ for all maximal ideals. Now, when $\Lambda_{\mathfrak{p}}$ is a maximal $R_{\mathfrak{p}}$-order in $A_{\mathfrak{p}}$, if $KM_{\mathfrak{p}} \cong KN_{\mathfrak{p}}$ as $A_{\mathfrak{p}}$-modules then $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ as $\Lambda_{\mathfrak{p}}$-modules ([14, Exercise 26.11]).
If Λ is maximal, the genus of M is given by the isomorphism class of KM.
In some cases $S(\Lambda)$ can be determined explicitly, e.g. if $\Lambda = R[G]$, with G a finite group, then $S(R[G]) = \{\mathfrak{p} \mid \mathfrak{p} \text{ contains } |G|\}$ (this follows from [14, Proposition 27.1] which explains that if Λ' is a maximal order in $K[G]$ then $R[G] \subseteq \Lambda' \subseteq |G|^{-1}R[G]$).

An application of a Lemma by Roiter ([14, 31.6]) gives us a first indication on the direct sum of Λ-lattices in the same genus: if L, M, N are Λ-lattices in the same genus, then there exists $L' \in g(M)$ such that

$$M \oplus N \cong L \oplus L'. \tag{1.1}$$

In the same vein we have also the following property ([15, Proposition 49.3]): given two Λ-lattices M and N, if $M \vee N^r$, with r a natural number, then $M \cong N^{r-1} \oplus M'$ with $M' \vee N$.

In order to define the locally free class group for a general order Λ we have to focus our investigation on the elements in $g(\Lambda)$.

Given a Λ-lattice M in $g(\Lambda)$, since $KM \cong A$, up to an isomorphism, we can consider $M \subset A$. For every maximal ideal $\mathfrak{p}$ of R we have $M_{\mathfrak{p}} \cong \Lambda_{\mathfrak{p}}$ and so, considering this isomorphism as the restriction of an element in $\mathrm{Aut}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}) \cong A_{\mathfrak{p}}^{\times}$, we can write

$$M_{\mathfrak{p}} = \Lambda_{\mathfrak{p}} \cdot \alpha_{\mathfrak{p}} \quad \text{with } \alpha_{\mathfrak{p}} \in A_{\mathfrak{p}}^{\times}, \forall\, \mathfrak{p} \text{ maximal ideal of } R.$$

Moreover, given $m \neq 0$ in $M \subset A$, then $\Lambda \cdot m$ and M differ at only finitely many places, as do Λ and $\Lambda \cdot m$; hereby $M_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$ a.e. and so $\alpha_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}}^{\times}$ a.e. (actually we

can take $\alpha_{\mathfrak{p}} = 1$ a.e.).

Definition 1.3.3. *We define the group $J^*(A)$ as the group of elements $\{x = (x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} A_{\mathfrak{p}}^{\times} : x_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}}^{\times}$ a.e.$\}$, where the product is taken over all maximal ideals $\mathfrak{p}$ of R. Moreover $U^*(\Lambda)$ denotes the set of elements $x = (x_{\mathfrak{p}})_{\mathfrak{p}}$ in $J^*(A)$ with $x_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}}^{\times}$ for every maximal ideal $\mathfrak{p}$ of R.*

Remark 1.3.4. *$J^*(A)$ does not depend on the choice of Λ, i.e. if we take another R-order Λ' spanning A over K, we have that $\Lambda_{\mathfrak{p}} = \Lambda'_{\mathfrak{p}}$ a.e. and so they give the same group $J^*(A)$.*

Thus to every Λ-lattice M in $g(\Lambda)$ we can associate an element $\alpha \in J^*(A)$. Conversely, given $\alpha \in J^*(A)$, we can recover the Λ-lattice M as

$$M = I(\alpha) := \bigcap_{\mathfrak{p}\,\max} \{A \cap \Lambda_{\mathfrak{p}} \cdot \alpha_{\mathfrak{p}}\}$$

which is evidently in $g(\Lambda)$.
So considering $I(\alpha)$ and $I(\beta)$, two Λ-lattices in the genus of Λ, we observe that

$$I(\alpha) \cong I(\beta) \Leftrightarrow I(\alpha) = I(\beta) \cdot a \text{ with } a \in A^{\times} \Leftrightarrow \Lambda_{\mathfrak{p}} \cdot \alpha_{\mathfrak{p}} = \Lambda_{\mathfrak{p}} \cdot \beta_{\mathfrak{p}} \cdot i_{\mathfrak{p}}(a)\ \forall\ \mathfrak{p} \text{ max. ideal},$$

where $i_{\mathfrak{p}}$ embeds A into $A_{\mathfrak{p}}$. This shows that

$$\begin{aligned} I(\alpha) \cong I(\beta) &\iff \alpha_{\mathfrak{p}} = u_{\mathfrak{p}} \cdot \beta_{\mathfrak{p}} \cdot i_{\mathfrak{p}}(a) \text{ with } u_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}}^{\times},\ \forall\, \mathfrak{p} \text{ maximal ideal} \\ &\iff \alpha = u \cdot \beta \cdot a \text{ where } u \in U^*(\Lambda) \text{ and } a \in A^{\times}. \end{aligned}$$

We are now ready to define $\mathrm{Cl}(\Lambda)$ the locally free class group associated to the R-order Λ.
We can reformulate our formula (1.1) in terms of idèles: given $\alpha, \beta \in J^*(A)$ we have from [14, 31.19]:

$$I(\alpha) \oplus I(\beta) \cong \Lambda \oplus I(\alpha\beta). \tag{1.2}$$

It would be nice to define a group law on the isomorphism classes of Λ-lattices in $g(\Lambda)$ as $[I(\alpha)] + [I(\beta)] = [I(\alpha\beta)]$ (where the symbol $[-]$ denotes an isomorphism class), reflecting the group structure of $J^*(A)$, but unfortunately, for some particular Λ's (see [42] for an explicit example),

$$\Lambda \oplus I(\gamma) \cong \Lambda \oplus I(\gamma') \not\Rightarrow I(\gamma) \cong I(\gamma')$$

and so the addition would not be well defined in these cases.
To avoid these "cancellation problems" we have to introduce the notion of *stably isomorphic* Λ-lattices: we say that M and N, two Λ-lattices, are stably isomorphic if there exists a natural number k such that

$$M \oplus \Lambda^k \cong N \oplus \Lambda^k. \tag{1.3}$$

Note that this definition does not imply that $M \cong N$ as already noted before. Just in some special cases this notion is equivalent to the notion of isomorphic Λ-lattices; the next section will develop this topic in detail.

Remark 1.3.5. *The Bass Cancellation Theorem ([15, 41.20]) allows us to restrict our previous definition to $k = 1$, since it proves the following implication*

$$M \oplus \Lambda^k \cong N \oplus \Lambda^k \Rightarrow M \oplus \Lambda \cong N \oplus \Lambda.$$

If now $[M]_s$ denotes the stable isomorphism class of M, we define

$$\mathrm{Cl}(\Lambda) := \{[M]_s : M \in g(\Lambda)\} \tag{1.4}$$

and we call it the *locally free class group* of Λ. Now, on this set, using (1.1), we have a well defined group law given by

$$[M_1]_s + [M_2]_s = [M_3]_s, \tag{1.5}$$

where, $M_3 \in g(\Lambda)$ such that $M_1 \oplus M_2 \cong \Lambda \oplus M_3$.
This addition law is well defined since if we take another representative M_1' of $[M_1]_s$ (resp. M_2' of $[M_2]_s$) and M_3' is such that $M_1' \oplus M_2' \cong \Lambda \oplus M_3'$, we have that there exists a natural number k such that $M_1 \oplus \Lambda^k \cong M_1' \oplus \Lambda^k$ (resp. $M_2 \oplus \Lambda^k \cong M_2' \oplus \Lambda^k$). Therefore

$$M_3 \oplus \Lambda^{(2k+1)} \cong M_1 \oplus \Lambda^k \oplus M_2 \oplus \Lambda^k \cong M_1' \oplus \Lambda^k \oplus M_2' \oplus \Lambda^k \cong M_3' \oplus \Lambda^{(2k+1)}$$

which proves that $[M_3]_s = [M_3']_s$. This operation is clearly commutative and associative, with unit $[\Lambda]_s$ and $[I(\alpha^{-1})]_s$ inverse element of $[I(\alpha)]_s$.

From (1.2), we see that we have a surjective group homomorphism from $J^*(A)$ to $\mathrm{Cl}(\Lambda)$, which sends $\alpha \in J^*(A)$ to $[I(\alpha)]_s \in \mathrm{Cl}(\Lambda)$.

Since K is a global field, the Jordan-Zassenhaus Theorem (see [30, Theorem 26.4]) tells us that the number of isomorphism classes of Λ-lattices in $g(\Lambda)$ is finite, so a fortiori $\mathrm{Cl}(\Lambda)$ is finite.

Example. *If $\Lambda = R$, then the locally free class group $\mathrm{Cl}(R)$ is exactly the ideal class group of R.*

1.4 Cancellation law

We have already seen that, given two Λ-lattices M and N such that $M \oplus \Lambda^k \cong N \oplus \Lambda^k$, for a natural number k, then this does not generally imply $M \cong N$. In this section we will recall some results which explain when two lattices which are stably isomorphic are also isomorphic. We call this property locally free cancellation and in this case we say that Λ has locally free cancellation.

With our assumption on K to be an algebraic number field, a sufficient condition to have locally free cancellation is that A (as at the beginning of the chapter) satisfies the Eichler condition. We define this condition just in the case when R is the ring of integers of K, which is actually the original case considered by Eichler; the generalization due to Swan to every K-algebra A with K global field can be found in [15, §51A].

Definition 1.4.1 (Totally definite quaternion algebra)**.** *A simple K-algebra B is totally definite quaternion if its center $Z(B)$ is a totally real number field and for every embedding $Z(B) \hookrightarrow \mathbb{R}$ the scalar extension $B \otimes_{Z(B)} \mathbb{R}$ is the Hamilton quaternion algebra.*

Definition 1.4.2 (Eichler's condition, when K is a number field)**.** *A K-algebra A satisfies the Eichler condition when none of the simple components of A is a totally definite quaternion algebra.*

When $A = K[G]$, which will be our case in the sequel, [15, Theorem 51.3] lists all the groups G for which A does not satisfy the Eichler condition. In particular when G is abelian or of odd order the Eichler condition is always satisfied.

Using this definition we have the following fundamental result.

Theorem 1.4.3 (Jacobinski Cancellation Theorem)**.** *If A, as defined at the beginning of the chapter, satisfies the Eichler condition, then every O_K-order Λ in A has locally free cancellation.*

Proof. See [15, 51.24]. □

Note that the same result is true if we replace O_K with a Dedekind domain R with field of fractions a global field K.

The Eichler condition is actually just a sufficient condition to have locally free cancellation, indeed for example when $\Lambda = \mathbb{Z}[G]$, various authors such as J. Martinet and R. G. Swan investigated the groups G for which the locally free cancellation holds for the integral group ring even if the Eichler condition does not. For details see [15, §51C].

Remark 1.4.4. *If Λ is an order with locally free cancellation, we deduce that $\mathrm{Cl}(\Lambda)$, as previously defined, consists now of the isomorphism classes of Λ-lattices in $g(\Lambda)$ and we have that $[M]_s = 1$ if and only if M is Λ-free.*

Remark 1.4.5. *If R is a d.v.r. then locally free cancellation always holds ([15, Exercise 39.1]).*

1.5 Other (equivalent) definitions of the locally free class group

In the literature we also find other definitions of $\mathrm{Cl}(\Lambda)$ through the Grothendieck group $K_0(\Lambda)$ of projective Λ-modules. We shall see in this section that they all coincide with our previous one.

Definition 1.5.1 (The Grothendieck group of projective modules)**.** *The Grothendieck group $K_0(\Lambda)$ of projective Λ-modules is defined as the abelian group with generators the isomorphism classes $[M]$ of finitely generated projective Λ-modules under the relation $[M] + [N] = [M \oplus N]$.*

By the definition of projective module, we immediately understand that every element $x \in K_0(\Lambda)$ can be written as $[F] - [X]$, where F is a free Λ-module and X a finitely generated projective Λ-module.

Remark 1.5.2. *When Λ is equal to $O_K[G]$, by Example 1.2.4, the Grothendieck group $K_0(O_K[G])$ can be defined as the abelian group with generators the isomorphism classes $[M]$ of locally free $O_K[G]$-lattices with the sum defined as before.*

The next proposition shows that we can also define the locally free class group $\mathrm{Cl}(\Lambda)$ as the kernel of the following map

$$\begin{aligned} \psi : K_0(\Lambda) &\longrightarrow \prod_{\mathfrak{p}\,\max} K_0(\Lambda_{\mathfrak{p}}), \\ [M] &\longmapsto \prod_{\mathfrak{p}\,\max} [M_{\mathfrak{p}}]. \end{aligned}$$

Proposition 1.5.3. *Let $\phi : \mathrm{Cl}(\Lambda) \longrightarrow K_0(\Lambda)$ be the group homomorphism sending $[M]_s \in \mathrm{Cl}(\Lambda)$ to $[\Lambda] - [M] \in K_0(\Lambda)$. Then the following sequence is exact*

$$0 \longrightarrow \mathrm{Cl}(\Lambda) \xrightarrow{\phi} K_0(\Lambda) \xrightarrow{\psi} \textstyle\prod_{\mathfrak{p}\,\max} K_0(\Lambda_{\mathfrak{p}}).$$

Proof. Since $[M] = [N]$ in the Grothendieck group if and only if M is stably isomorphic to N (see [15, Proposition 38.22]), we see that ϕ is injective. Moreover we also understand that an element $x \in K_0(\Lambda)$, written as before $([F] - [X])$, is in the kernel of ψ if and only if $F_{\mathfrak{p}}$ is stably isomorphic to $X_{\mathfrak{p}}$, which, by Remark 1.4.5, is equivalent to say that $F_{\mathfrak{p}} \cong X_{\mathfrak{p}}$ for every $\mathfrak{p}$ (or in other words $X \in g(F)$). Moreover if F is free of rank k, by the property below (1.1), we have that $[X] = [\Lambda]^{k-1} + [M]$ and $x = [\Lambda] - [M]$, where $M \in g(\Lambda)$. Thus, looking at the definition of $\mathrm{Cl}(\Lambda)$ (see 1.4), this shows that $x \in K_0(\Lambda)$ is in the kernel of ψ if and only if it is in the image of ϕ, concluding the proof. □

Other equivalent definitions of the locally free class group $\mathrm{Cl}(\Lambda)$ exist, considering the following Grothendieck group.

Definition 1.5.4. *The Grothendieck group $K_0^{\mathrm{LF}}(\Lambda)$ is defined as the abelian group with generators the isomorphism classes $[M]$ of locally free Λ-lattices of constant rank, under the relation $[M] + [N] = [M \oplus N]$.*

Remark 1.5.5. *Note that if $\Lambda = O_K[G]$, then by Section 1.2, the Grothendieck group $K_0(\Lambda)$ coincides with $K_0^{\mathrm{LF}}(\Lambda)$.*

When $A = K[G]$, with G a finite group, and Λ is an R-order in A, another way of defining $\mathrm{Cl}(\Lambda)$, used for example by Fröhlich in his works (see for example [17, §2]), is through the surjective homomorphism $\mathrm{rk}_\Lambda : K_0^{\mathrm{LF}}(\Lambda) \longrightarrow \mathbb{Z}$, defined extending linearly the map sending $[M] \mapsto \mathrm{rk}(M)$ (see Definition 1.1.1). Using this homomorphism, $\mathrm{Cl}(\Lambda)$ is defined as its kernel ($\mathrm{Cl}(\Lambda) := \mathrm{Ker}(\mathrm{rk}_\Lambda)$).
As before we can see every element x in $K_0^{\mathrm{LF}}(\Lambda)$ as $[F] - [X]$, where F is a free Λ-module of rank k and X a locally free Λ-lattice of constant rank. Then

$x \in \mathrm{Ker}(\mathrm{rk}_\Lambda)$ if and only if X is of constant rank k, or in other words $X \in g(\Lambda^k)$. Then, as seen before, we can write $[X] = [\Lambda]^{k-1} + [M]$, with $M \in g(\Lambda)$, which proves the equivalence of this definition with the previous one.

Equivalently, always considering Λ an R-order in $A = K[G]$, the locally free class group $\mathrm{Cl}(\Lambda)$ can also be defined as the cokernel of the homomorphism

$$\mathbb{Z} \longrightarrow K_0^{\mathrm{LF}}(\Lambda),$$

obtained extending the map which sends a natural number n to the class $[\Lambda^n]$ (see for example [19, §2]).

Remark 1.5.6. *If the group G is abelian, then the locally free class group $\mathrm{Cl}(O_K[G])$ is isomorphic to the Picard group $\mathrm{Pic}(O_K[G])$ (see [4, Part 4, Corollary 3.8]).*

1.6 Idelic representation of $\mathrm{Cl}(\Lambda)$

In this section we recall the idelic representation of $\mathrm{Cl}(\Lambda)$ presented by A. Fröhlich in [17]. As in the original paper, except for 1.6.2, we restrict our study to the case R equal to O_K. We recall from the beginning that A is assumed to be a finite dimensional separable (and so semisimple) K-algebra and that Λ is an R-order in A.

Moreover from now on we also need to add the infinite places of K to our definition of the idelic group $J^*(A)$, in particular we shall need the following definition.

Definition 1.6.1. *Let us define $\Lambda_\mathfrak{p}$ to be equal to $A_\mathfrak{p}$ at the infinite places $\mathfrak{p}$ of K. Then the idelic group $J(A)$ is defined as the set of elements $(x_\mathfrak{p})_p$ belonging to the product over all places of K (also infinite) $\prod_\mathfrak{p} A_\mathfrak{p}^\times$, such that $x_\mathfrak{p} \in \Lambda_\mathfrak{p}^\times$ almost everywhere.*
The group $U(\Lambda)$ is now defined as the set of elements $x = (x_\mathfrak{p})_\mathfrak{p}$ in $J(A)$ with $x_\mathfrak{p} \in \Lambda_\mathfrak{p}^\times$ for every place $\mathfrak{p}$ of K.

Given an element $\alpha \in J^*(A)$ we embed it in $J(A)$ imposing $\alpha_\mathfrak{p} = 1$ at every infinite place.

The main role in the idelic description of $\mathrm{Cl}(\Lambda)$ is played by the reduced norm map on A.

1.6.2 Reduced norm

Note that all the definitions and results contained in this subsection hold for every field K (not necessarily an algebraic number field). Let us denote by d the dimension of A as a K-algebra.

Given an element a in A and chosen a basis of A, we can define the characteristic polynomial of a over K, denoted by $\mathrm{chp}_{A/K}(a)$, as the characteristic polynomial of the matrix associated to the K-linear transformation $m_a : A \longrightarrow A$, which sends x to ax. If T_a is the associated $d \times d$ matrix, then $\mathrm{chp}_{A/K}(a) := \det(X\mathbb{1}_d - T_a)$. The trace of a over K, denoted by $\mathrm{Tr}_{A/K}(a)$, and the norm of a over K, denoted by $\mathrm{N}_{A/K}(a)$, are defined as the following coefficients of the characteristic polynomial:

$$\mathrm{chp}_{A/K}(a) = X^d - \mathrm{Tr}_{A/K}(a)X^{d-1} + \cdots + (-1)^d \mathrm{N}_{A/K}(a).$$

If we consider the simple algebra $A = M_n(K)$ and we take a matrix $a \in A$, we immediately realize that

$$\begin{aligned} \mathrm{Tr}_{A/K}(a) &= n(\mathrm{Tr}(a)) \\ \mathrm{N}_{A/K}(a) &= (\det(a))^n, \end{aligned}$$

where $\mathrm{Tr}(a)$ (resp. $\det(a)$) is the usual trace (resp. determinant) of the matrix a. This suggests that it would be useful to have some tools which generalize the previous relations to a general finite dimensional separable K-algebra, with instead of the trace and determinant of the matrix a a "modified version" of the trace and norm maps. This is the main motivation which leads to the notions of reduced trace and reduced norm.

Definitions and properties

From the definition of A and Theorem 1.0.2, there exists E, a finite separable field extension of K, such that E splits A, i.e. such that

$$E \otimes_K A \cong \prod_{i=1}^{s} \mathrm{M}_{n_i}(E);$$

where this isomorphism of E-algebras, that we call h, sends $1 \otimes a$ to the product $\prod_{i=1}^{s} T_{a_i}$, with $T_{a_i} \in \mathrm{M}_{n_i}(E)$, for $1 \leq i \leq s$.
The reduced characteristic polynomial of a over K, denoted by $\mathrm{rchp}_{A/K}(a)$, is then

defined as the following polynomial of degree $m := \sum n_i$

$$\mathrm{rchp}_{A/K}(a) := \prod_{i=1}^{s} \mathrm{chp}(T_{a_i}) = \prod_{i=1}^{s} \det(X\mathbb{1}_{n_i} - T_{a_i}). \tag{1.6}$$

It can be proved that $\mathrm{rchp}_{A/K}(a) \in K[X]$ and that this definition does not depend on the choice of E and of the isomorphism h (see [30, Chapter 2, §9]).
For the proof it is sufficient to consider the case where A is a central simple K-algebra. In this situation there exists E as above with an isomorphism $h : E \otimes_K A \longrightarrow \mathrm{M}_n(E)$, where n^2 is the dimension of A over K. Then in this case every other isomorphism $h' : E \otimes_K A \longrightarrow \mathrm{M}_n(E)$ is related to h by an inner automorphism, i.e. for every $u \in E \otimes_K A$ we have $h(u) = th'(u)t^{-1}$ with $t \in \mathrm{M}_n(E)$, and consequently the characteristic polynomial remains the same. Moreover it does not depend on the choice of the field extension E, since if we consider another field extension E' with the property above we find a field F such that both E and E' embed inside it; F is again a splitting field and, considering the original characteristic polynomials "inside" F, we see that they are actually the same. Finally $\mathrm{rchp}_{A/K}(a) \in K[X]$ in this case since we can choose E to be Galois over K with Galois group G and show that s fixes $\mathrm{rchp}_{A/K}(a)$ for every $s \in G$.

Since $(\mathrm{chp}(T_{a_i}))^{n_i} = \mathrm{chp}_{\mathrm{M}_{n_i}(E)/E}(T_{a_i})$ for every i and since $E \otimes_K A \cong \prod_{i=1}^{s} \mathrm{M}_{n_i}(E)$, we deduce that

$$\prod_{i=1}^{s} (\mathrm{chp}(T_{a_i}))^{n_i} = \prod_{i=1}^{s} \mathrm{chp}_{M_{n_i}(E)/E} T_{a_i} = \mathrm{chp}_{E\otimes_K A/E}(1 \otimes a) = \mathrm{chp}_{A/K}(a), \tag{1.7}$$

which allows us to understand that $\mathrm{rchp}_{A/K}$ and $\mathrm{chp}_{A/K}$ have the same irreducible factors.

We can then write

$$\mathrm{rchp}_{A/K}(a) = X^m - (\mathrm{rt}_{A/K}(a))X^{m-1} + \cdots + (-1)^m \mathrm{rn}_{A/K}(a),$$

where the *reduced trace* of a is defined as $\mathrm{rt}_{A/K}(a)$ and the *reduced norm* of a as $\mathrm{rn}_{A/K}(a)$.

The reduced trace behaves as the usual one, namely it is a K-linear map from A to K and

$$\mathrm{rt}_{A/K}(ab) = \mathrm{rt}_{A/K}(ba).$$

While for the reduced norm we have the following formulas:

$$\begin{aligned} \mathrm{rn}_{A/K}(ab) &= \mathrm{rn}_{A/K}(a)\mathrm{rn}_{A/K}(b) \\ \mathrm{rn}_{A/K}(ka) &= k^m \mathrm{rn}_{A/K}(a), \end{aligned}$$

for every $k \in K$.

If A is a separable simple K-algebra with center L (so L separable over K), let $\dim_L A = u^2$ and $\dim_K L = v$, then E can be chosen such that $E \otimes_K A \cong \prod_{i=1}^{v} \mathrm{M}_u(E)$ and for every $a \in A$, from (1.6) and (1.7), we obtain

$$\begin{aligned} \mathrm{chp}_{A/K}(a) &= (\mathrm{rchp}_{A/K}(a))^u \\ \mathrm{Tr}_{A/K}(a) &= m(\mathrm{rt}_{A/K}(a)) \\ \mathrm{N}_{A/K}(a) &= (\mathrm{rn}_{A/K}(a))^u. \end{aligned}$$

If A is a separable K-algebra (so semisimple) we can decompose it in simple algebras as $A = A_1 \times \cdots \times A_t$, where each simple algebra A_i has center K_i a field extension of K and $\dim_{K_i} A_i = m_i^2$. If $a \in A$ is equal to $(a_1, \ldots, a_n)$, extending the previous formulas to this situation, we have

$$\begin{aligned} \mathrm{Tr}_{A/K}(a) &= \sum_{i=1}^{t} m_i \cdot \mathrm{rt}_{A_i/K}(a_i) \\ \mathrm{N}_{A/K}(a) &= \prod_{i=1}^{t} (\mathrm{rn}_{A_i/K}(a_i))^{m_i} \end{aligned}$$

and moreover $\mathrm{rt}_{A/K} = \sum_{i=1}^{t} \mathrm{rt}_{A_i/K}$ and $\mathrm{rn}_{A/K} = \prod_{i=1}^{t} \mathrm{rn}_{A_i/K}$.

Example 1.6.3. *Let $A = K[G]$, with K of characteristic 0 and G abelian, then the reduced norm (resp. reduced trace) coincides with the usual norm (resp. trace). Indeed $A \cong \prod_{i=1}^{s} K_i$, where each K_i is a cyclotomic extension. Then it is easy to see that*

$$\mathrm{rn}_{A/K}(a) = \prod_{i=1}^{s} \mathrm{rn}_{K_i/K}(a_i) = \prod_{i=1}^{s} \mathrm{N}_{K_i/K}(a_i) = \mathrm{N}_{A/K}(a),$$

where $a = \prod a_i$. Analogously for the trace.

Other examples on explicit computations of reduced traces and norms can be found in [14, §7D].

Remark 1.6.4. *As already noted at the beginning of the section, the reduced norm map can be defined for every field K (not necessarily an algebraic number field).*

In this general context, one of the main reason to use $\mathrm{rt}_{A/K}$ *instead of the usual trace map is that, when* A *is a separable simple* K*-algebra of dimension* m^2 *over its center, it allows us to have a non-degenerate bilinear form from* $A \times A$ *to* K *even if* $\mathrm{char}(K)$ *divides* m *(which does not hold for the usual trace). This result can be extended to every finite dimensional separable* K*-algebra. For details on that see [14, §7D].*

The image and kernel of the reduced norm map

We see from [14, §7D] that, when we consider A a central simple K-algebra, the image and the kernel of the reduced norm map are well known.
Namely as regards the image, in the local case we have the following theorem.

Theorem 1.6.5. *Let* $\mathfrak{p}$ *be a finite place of* K *and* A *a central simple* $K_\mathfrak{p}$*-algebra, then* $\mathrm{rn}_{A/K_\mathfrak{p}}(A^\times) = K_\mathfrak{p}^\times$.

Globally, the result is a bit more delicate and in order to explain it we have to define the subgroup $K_+^\times$ in $K^\times$. This is defined as the set of elements $x \in K^\times$ such that $x_\mathfrak{p} > 0$ at each real prime $\mathfrak{p}$ of K ramified in A. For an infinite prime $\mathfrak{p}$ to be ramified in A means that $A_\mathfrak{p}$ is a central simple $\mathbb{R}$-algebra such that $A_\mathfrak{p} \cong \mathrm{M}_n(\mathbb{H})$, where $\mathbb{H}$ is the skewfield of real quaternions (remember that every central simple $\mathbb{R}$-algebra has to be of the form $\mathrm{M}_n(\mathbb{R})$ or $\mathrm{M}_n(\mathbb{H})$, since $\mathbb{R}$ and $\mathbb{H}$ are the only finite dimensional skewfields with center $\mathbb{R}$). Note that this definition even if not explicit in the notation depends on the algebra A and not just on K. Then in the global case we have the following result.

Theorem 1.6.6 (Hasse–Schilling–Mass Norm Theorem)**.** *Let* A *be a central simple* K*-algebra. Then* $\mathrm{rn}_{A/K}(A^\times) = K_+^\times$.

This result also holds for K a global field (not necessarily an algebraic number field).

Remaining in the case of A a central simple K-algebra, both Nakayama and Matsushima, for the local case, both Wang and Platonov, for the global one, proved that the kernel of $\mathrm{rn}_{A/K} : A^\times \to K^\times$ is equal to the commutator subgroup $[A^\times, A^\times]$. For details and proofs see [14, §7D] and [30, §33].

Extending now these results to the more general case of A a separable K-algebra, with K a global field, we can consider its decomposition in simple components

$$A \cong A_1 \times \cdots \times A_n$$

where each A_i is a simple algebra with center K_i. Then we can consider rn_{A_i/K_i} : $A_i^\times \to K_i^\times$, which combine to yield the reduced norm $\mathrm{rn}_{A/Z(A)} : A^\times \to Z(A)^\times$, where $Z(A)$ is the center of the algebra A and $Z(A)^\times = \prod K_i^\times$.
Using the previous results, we have that for A a separable K-algebra

$$\mathrm{rn}_{A/Z(A)}(A^\times) = Z(A)_+^\times$$
$$\mathrm{Ker}(\mathrm{rn}_{A/Z(A)}) = [A^\times, A^\times],$$

where $Z(A)_+^\times = \prod K_{i,+}^\times$ and $K_{i,+}^\times$ is analogously defined as for $K_+^\times$ with respect now to the simple component A_i.

Locally for every finite place $\mathfrak{p}$, if we consider $A_\mathfrak{p}$, we have that $\mathrm{rn}_{A_\mathfrak{p}/Z(A_\mathfrak{p})}$ is surjective on $Z(A_\mathfrak{p})^\times$ with kernel the commutator subgroup, while $\mathrm{rn}_{A_\mathfrak{p}/Z(A_\mathfrak{p})}(\Lambda_\mathfrak{p}^\times) \subseteq Z(\Lambda_\mathfrak{p})^\times$, with equality when $\Lambda_\mathfrak{p}$ is a maximal order.
Hence we can consider an idelic version of the reduced norm

$$\mathrm{rn}_{J(A)/J(Z(A))} : J(A) \to J(Z(A)),$$

where now the kernel, denoted by $J(A)'$, is equal to the closure in $J(A)$ of $J(A) \cap \prod_\mathfrak{p}[A_\mathfrak{p}^\times, A_\mathfrak{p}^\times]$ (which coincides with the commutator subgroup of $J(A)$, see [15, Exercise 51.1]); while the image is given by $J(Z(A))_+ = \prod J(K_i)_+$ (subgroup of idèles positive at the real primes ramifying in A), by the behavior of the reduced norm at the infinite real primes.

We conclude this section with a remark which will be useful in the sequel.

Remark 1.6.7. *Given $\mathcal{M}$ a maximal R-order in A,*

$$\mathrm{rn}_{A/Z(A)}(U(\mathcal{M})) = U(\mathcal{O})_+,$$

where $\mathcal{O}$ is the maximal order of $Z(A)$. Note that $\mathcal{O}$ is isomorphic to $\prod O_{K_i}$, with O_{K_i} the ring of integers of K_i for every i (as above the K_i's are the centers of the simple components), and $U(\mathcal{M})$ and $U(\mathcal{O})$ are special cases of $U(\Lambda)$ defined in Definition 1.6.1. Now $U(\mathcal{O})_+$ denotes $U(\mathcal{O}) \cap J(Z(A))_+$. The proof is based on the fact cited before that $\mathrm{rn}_{A_\mathfrak{p}/Z(A)_\mathfrak{p}}(\Lambda_\mathfrak{p}^\times) = Z(\Lambda_\mathfrak{p})^\times$ when $\Lambda_\mathfrak{p}$ is a maximal order. For details we refer to [17].

1.6.8 Idelic description

Let $J(A)'$ be defined as the commutator subgroup $[J(A), J(A)]$. In [17], Fröhlich showed that

$$\mathrm{Cl}(\Lambda) \cong \frac{J(A)}{J(A)' \cdot A^{\times} \cdot U(\Lambda)}, \tag{1.8}$$

where the isomorphism sends $[I(\alpha)] \mapsto \alpha$ (see Section 1.3).
If we denote the reduced norm from A to $Z(A)$ just by rn, applying it to the right-hand quotient above and using the fact that $\mathrm{rn}(J(A)) = J(Z(A))_+$ (resp. $\mathrm{rn}(A^{\times}) = Z(A)_+^{\times}$), we get the isomorphism

$$\mathrm{Cl}(\Lambda) \cong \frac{J(Z(A))_+}{Z(A)_+^{\times} \cdot \mathrm{rn}(U(\Lambda))},$$

which, thanks to the equality $J(Z(A)) = J(Z(A))_+ \cdot Z(A)^{\times}$, yields

$$\mathrm{Cl}(\Lambda) \cong \frac{J(Z(A))}{Z(A)^{\times} \cdot \mathrm{rn}(U(\Lambda))}. \tag{1.9}$$

When the K-algebra A is commutative, since $J(A)' = 1$, (1.8) simplifies to

$$\mathrm{Cl}(\Lambda) \cong \frac{J(A)}{A^{\times} \cdot U(\Lambda)}.$$

When $\mathcal{M}$ is a maximal order in A, we know that $\mathrm{rn}(U(\mathcal{M})) = U(\mathcal{O})_+$, where $\mathcal{O}$ is the maximal order of $Z(A)$, so (1.9) reduces to

$$\mathrm{Cl}(\mathcal{M}) \cong \frac{J(Z(A))}{Z(A)^{\times} \cdot U(\mathcal{O})_+}.$$

Remark 1.6.9. *The idelic representation can be actually deduced by a more general work of Wall [44], where he gave an idelic description of* $\mathrm{Cl}(\Lambda)$ *with* Λ *an* R*-order, where* R *now is a general Dedekind domain.*

Remark 1.6.10. *There is also a way of writing the previous isomorphism without considering the infinite primes, i.e. using the group* $J^*(A)$ *defined in Definition 1.3.3. For details on that, see [15, page 226].*

1.6.11 Explicit idelic description for $A = K[G]$

We now assume that $A = K[G]$ and $\Lambda = R[G]$. In this case, given an $R[G]$-lattice M in the genus of $R[G]$, we are able to give an explicit way to find the

representative $\alpha \in J(K[G])$ of the class associated to M.

Proposition 1.6.12. *Let b be a free generator of KM over $K[G]$ and $a_{\mathfrak{p}}$ a free generator of $M_{\mathfrak{p}}$ over $R_{\mathfrak{p}}[G]$, for every maximal ideal $\mathfrak{p}$. Let us define $c_{\mathfrak{p}} \in K_{\mathfrak{p}}[G]^{\times}$ such that $a_{\mathfrak{p}} = c_{\mathfrak{p}} \cdot b$, for every maximal ideal $\mathfrak{p}$. At the infinite place let us take $c_{\mathfrak{p}} = 1$.*
Then the class of M in $\mathrm{Cl}(R[G])$ is given by the class of representative $c := (c_{\mathfrak{p}})_{\mathfrak{p}}$ in $J(K[G])/\left(J(K[G])' \cdot K[G]^{\times} \cdot U(R[G])\right)$.

Proof. Referring to Section 1.3, let us consider M in $K[G]$ via an embedding i which sends b to 1. Then, for every maximal ideal $\mathfrak{p}$, if $i_{\mathfrak{p}} : M_{\mathfrak{p}} \longrightarrow K_{\mathfrak{p}}[G]$ denotes the completion at $\mathfrak{p}$ of i, since $i_{\mathfrak{p}}(a_{\mathfrak{p}}) = c_{\mathfrak{p}}$, we deduce that $i_{\mathfrak{p}}(M_{\mathfrak{p}}) = R_{\mathfrak{p}}[G] \cdot c_{\mathfrak{p}}$.
Let $c^* := (c_{\mathfrak{p}})_{\mathfrak{p}<\infty} \in J(K[G])^*$. In Section 1.3 we defined $I(c^*)$ as $\bigcap_{\mathfrak{p}<\infty}(K[G] \cap R_{\mathfrak{p}}[G] \cdot c_{\mathfrak{p}})$. Then, from the previous relation, we get

$$I(c^*) = \bigcap_{\mathfrak{p}<\infty} (K[G] \cap R_{\mathfrak{p}}[G] \cdot c_{\mathfrak{p}}) = \bigcap_{\mathfrak{p}<\infty} (K[G] \cap i_{\mathfrak{p}}(M_{\mathfrak{p}})) = i(M),$$

as we wanted to prove to show our claim. □

Remark 1.6.13. *Note that a representative of the class of M in terms of the isomorphism (1.9) is obtained applying the reduced norm* rn *to the idelic element $(c_{\mathfrak{p}})_{\mathfrak{p}}$ found in the previous proposition.*

1.7 Hom representation of $\mathrm{Cl}(\Lambda)$

Let K be as above and let G be a finite group.

The idelic description just seen in the previous section, despite its easiness and elegance, turns out not always to be so convenient in its applications to concrete computations of class groups. Also for this reason, when A is equal to $K[G]$, Fröhlich in [18] gave another description in terms of homomorphism groups involving complex irreducible characters, which are common arithmetic invariants often appearing in number theory. This description is better known as the Hom-description.

For the rest of the section we restrict our attention to the case $A = K[G]$.

1.7.1 The Det map

Given a finite group G, we denote by R_G its associated ring of virtual characters, i.e. the $\mathbb{Z}$-linear combinations of characters in $\mathrm{Irr}(G)$.
Moreover we consider E a Galois field extension of K such that the irreducible complex representations of G are defined over E. Let G_E denote the Galois group $\mathrm{Gal}(E/K)$. Then G_E acts naturally on the left on $\mathrm{Irr}(G)$ via $\chi^\omega(s) = \chi(s)^\omega$, for all $\omega \in G_E$, $\chi \in \mathrm{Irr}(G)$ and $s \in G$. This action linearly extends to the ring R_G, which therefore can be considered as a left G_E-module.
Moreover the group G_E acts on the left on $\mathrm{Hom}(R_G, E^\times)$ by conjugation: $f^\omega(\alpha) = (f(\alpha^\omega))^{\omega^{-1}}$, where $f \in \mathrm{Hom}(R_G, E^\times)$, $\omega \in G_E$ and $\alpha \in R_G$. We recall from the Introduction that $\mathrm{Hom}_{G_E}(R_G, E^\times)$ denotes the set of fixed elements in $\mathrm{Hom}(R_G, E^\times)$ under the left action of G_E (i.e. the set of elements $f \in \mathrm{Hom}(R_G, E^\times)$, such that $(f(\alpha))^\omega = f(\alpha^\omega)$, for all $\omega \in G_E$ and $\alpha \in R_G$).

Given $\chi \in \mathrm{Irr}(G)$, we can consider an associated representation $T_\chi : G \longrightarrow \mathrm{GL}_n(E)$ and its K-linear extension, always denoted by T_χ, which sends $K[G]$ to $\mathrm{M}_n(E)$ (i.e. the group of n-square matrices over E). To every character χ we can associate the map $\det_\chi$, an extended version of the usual determinant map, via the following diagram

$$\begin{array}{ccc} K[G] & \xrightarrow{T_\chi} & \mathrm{M}_n(E) \\ & \searrow^{\det_\chi} & \downarrow{\scriptstyle \det} \\ & & E \end{array}$$

where det is the usual determinant of a matrix. If T'_χ is another associated representation, then for every $s \in G$, there exists a square matrix D, such that $T_\chi(s) = D^{-1}T'_\chi(s)D$; hence we understand that this definition does not depend on the choice of the representation associated to the character χ ($\det(T_\chi(x)) = \det(T'_\chi(x))$ for every $x \in K[G]$).
It is clear that $\det_\chi$ sends a unit $x \in K[G]^\times$ to $E^\times$. Moreover we can easily see that $\det_\chi(x \cdot x') = \det_\chi(x)\det_\chi(x')$, proving that $\det_\chi$ is actually a group homomorphism from $K[G]^\times$ to $E^\times$.

Since $T_{\chi+\chi'}(x) = \left(\begin{array}{c|c} T_\chi(x) & 0 \\ \hline 0 & T_{\chi'}(x) \end{array}\right)$, we have $\det_{\chi+\chi'}(x) = \det_\chi(x)\det_{\chi'}(x)$, thus we can finally define a group homomorphism $\mathrm{Det} : K[G]^\times \longrightarrow \mathrm{Hom}(R_G, E^\times)$, which maps x to the linear extension of the homomorphism sending $\chi \mapsto \det_\chi(x)$.
If we consider now the G_E-action on the characters of G we see that T_{χ^ω} can be chosen so that $T_{\chi^\omega}(x) = T_\chi(x)^\omega$ and thus we deduce that, for all $\omega \in G_E$ and $x \in K[G]^\times$, we have $\det_{\chi^\omega}(x) = \det_\chi(x)^\omega$ which finally explains why we can

consider the Det map as follows:

$$\begin{aligned} \mathrm{Det} : K[G]^\times &\longrightarrow \mathrm{Hom}_{G_E}(R_G, E^\times) \\ x &\longmapsto (\chi \mapsto \det_\chi(x)). \end{aligned}$$

A "local" analog can be easily obtained substituting K with its completion $K_\mathfrak{p}$, with $\mathfrak{p}$ a prime of K (finite or not). Then we have that T_χ sends $K_\mathfrak{p}[G]$ to $\mathrm{M}_n(E_\mathfrak{p})$, where as usual $E_\mathfrak{p} := E \otimes_K K_\mathfrak{p}$. Considering G_E acting on the left on $E_\mathfrak{p}$ via its action on the first component, for every $\mathfrak{p}$ we also have

$$\mathrm{Det} : K_\mathfrak{p}[G]^\times \longrightarrow \mathrm{Hom}_{G_E}(R_G, E_\mathfrak{p}^\times).$$

One may wonder what happens if we restrict the Det-map to $R[G]$ (resp. $R_\mathfrak{p}[G]$). The key point now is that if we restrict our attention to the local case $R_\mathfrak{p}[G]$, with $\mathfrak{p}$ a finite maximal ideal, every $K_\mathfrak{p}$-representation is equivalent to an $R_\mathfrak{p}$-representation ([14, Corollary 16.14]) and so for every $x \in R_\mathfrak{p}[G]$ we can consider $T_\chi(x) \in \mathrm{M}_n(S_\mathfrak{p})$, where S is the integral closure of R in E (e.g. if $R = O_K$ then $S = O_E$). Or better it is sufficient to note that the image of $R_\mathfrak{p}[G]$ under T_χ is an $R_\mathfrak{p}$-order in $\mathrm{M}_n(E_\mathfrak{p})$, so the determinant of elements in $T_\chi(R_\mathfrak{p}[G])$ must be integral over $R_\mathfrak{p}$, and therefore contained in $S_\mathfrak{p}$. Note that this is no longer true for R not a d.v.r.. So for every maximal ideal $\mathfrak{p}$, we have

$$\mathrm{Det} : R_\mathfrak{p}[G]^\times \longrightarrow \mathrm{Hom}_{G_E}(R_G, S_\mathfrak{p}^\times). \tag{1.10}$$

Remark 1.7.2. *At the beginning of the section we chose a Galois field extension E/K, nevertheless everything remains the same if we consider another field extension E'/K, with the only requirement being that it is Galois and contains all the values of the irreducible complex characters of G. A method to avoid the choice of E is to consider a given algebraic closure K^c of K and everything can be rewritten replacing E with K^c, G_E with Ω_K (the absolute Galois group of K) and $S_\mathfrak{p}$ with the integral closure of $O_{K_\mathfrak{p}}$. This simplifies the choice at the beginning but it introduces an infinite extension which is somewhat harder to be used in practice.*

Remark 1.7.3. *We also have an analogous homomorphism to (1.10) if we replace $R_\mathfrak{p}[G]^\times$ by $\Lambda_\mathfrak{p}$, where Λ is an R-order contained in $A = K[G]$. Namely*

$$\mathrm{Det} : \Lambda_\mathfrak{p}^\times \longrightarrow \mathrm{Hom}_{G_E}(R_G, S_\mathfrak{p}^\times).$$

1.7.4 Hom description

The Det-map just defined and the reduced norm are almost the same, indeed they are equal up to an isomorphism, as explained by the following theorem (the proof given here is taken from [15, Proposition 52.9]).

Theorem 1.7.5. *Let E be an extension of K defined as at the beginning of 1.7.1. There is an isomorphism $f : Z(K[G])^\times \longrightarrow \mathrm{Hom}_{G_E}(R_G, E^\times)$, such that the following diagram commutes*

$$\begin{array}{ccc} K[G]^\times & & \\ \Big\downarrow{\scriptstyle \mathrm{rn}} & \searrow^{\mathrm{Det}} & \\ Z(K[G])^\times & \xrightarrow{f} & \mathrm{Hom}_{G_E}(R_G, E^\times). \end{array}$$

Proof. To understand the proof we have to recall some well-known facts on the Wedderburn's decomposition of the group algebra $K[G]$. First the number of simple components is equal to the number of characters of irreducible K-representations of G, which in turn are in bijection with the orbits of the irreducible complex characters under the action of G_E ([22, Chapter 10]). Moreover, let $\chi_1, \ldots, \chi_t$ be a set of representatives of the irreducible complex characters under the action of G_E, then we have the Wedderburn's decomposition:

$$K[G] \cong \prod_{i=1}^{t} A_i,$$

where each A_i is a simple algebra with center $K(\chi_i)$, i.e. the field extension of K obtained adding the values of the character χ_i ([15, §75]). Hereby the center $Z(K[G]) \cong \prod_{i=1}^{t} K(\chi_i)$.

We can now proceed to the proof of the statement, starting with the definition of the isomorphism f. Given an element $c = \prod_{i=1}^{t} c_i \in Z(K[G])$ we define $f(c) = f_c \in \mathrm{Hom}_{G_E}(R_G, E^\times)$ as the product $\prod_{i=1}^{t} f_{c_i}$, where each f_{c_i} is defined on each character χ as

$$f_{c_i}(\chi) = \begin{cases} c_i^\omega & \text{if } \chi = \chi_i^\omega \text{ for some } \omega \in G_E, \\ 1 & \text{otherwise.} \end{cases}$$

Then in general for an element $\sum \alpha_\chi \chi \in R_G$, $f_c(\sum \alpha_\chi \chi) = \prod f_c(\chi)^{\alpha_\chi}$. The injectivity of f is given computing the values of f_c at the representatives χ_i, while for the

surjectivity it is sufficient to underline that every element $g \in \mathrm{Hom}_{G_E}(R_G, E^\times)$ is determined by the values it assumes on the representative χ_i and that $g(\chi_i)$ belongs to $K(\chi_i)$.

For the commutativity of the diagram, it is sufficient to show it on a single character $\chi \in \mathrm{Irr}(G)$, since then by linearity we can extend it on R_G . Let us assume that $\chi = \chi_i^\omega$, for an $\omega \in G_E$, we would like to prove that, for every $a \in K[G]^\times$, $f(\mathrm{rn}(a))(\chi) = \mathrm{Det}(a)(\chi)$.
Our field extension E, by definition, is a splitting field for each simple component (i.e. for every simple component $E \otimes_K A_i \cong \mathrm{M}_{n_i}(E)$, for some $n_i \in \mathbb{N}$), so from the definition of the reduced norm map we have $\mathrm{rn}(a) = \prod_{i=1}^t \det(T_{\chi_i}(a)) = \prod_{i=1}^t \det_{\chi_i}(a)$, where T_{χ_i} is a representation associated to χ_i. Hereby applying f, we get

$$f(\mathrm{rn}(a))(\chi) = \prod_{i=1}^{t} f_{\det_{\chi_i}(a)}(\chi) = \prod_{i=1}^{t} f_{\det_{\chi_i}(a)}(\chi_i^\omega) = \det_{\chi_i}(a)^\omega.$$

At the same time by definition we have $\mathrm{Det}(a)(\chi) = \det_{\chi_i^\omega}(a)$. But as explained in the previous subsection $\det_{\chi_i^\omega}(a) = \det_{\chi_i}(a)^\omega$, which gives our claim. □

The isomorphism f induces the isomorphism $J(Z(K[G])) \longrightarrow \mathrm{Hom}_{G_E}(R_G, J(E))$. Thus, applying it to the idelic formula (1.9) and using the commutativity of the previous diagram, we get the Hom-formula for the class group:

$$\mathrm{Cl}(R[G]) \cong \frac{\mathrm{Hom}_{G_E}(R_G, J(E))}{\mathrm{Hom}_{G_E}(R_G, E^\times) \cdot \mathrm{Det}(U(R[G]))},$$

where, by (1.10), $\mathrm{Det}(U(R[G]))$ is contained in $\mathrm{Hom}_{G_E}(R_G, U(S))$, with $U(S) = \prod_{\mathfrak{p}} S_{\mathfrak{p}}^\times$ (remember that for the infinite primes $R_{\mathfrak{p}} = K_{\mathfrak{p}}$ and $S_{\mathfrak{p}} = E_{\mathfrak{p}}$).

Explicitly the Hom-description is given in the following way: given M a locally free left Λ-ideal and considering it as $I(\alpha)$, with $\alpha := (\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in J(K[G])$, the function $f \in \mathrm{Hom}_{G_E}(R_G, J(E))$ representing the class of M is clearly defined by linearity at each $\mathfrak{p}$ as

$$f(\chi)_{\mathfrak{p}} = \det_\chi(\alpha_{\mathfrak{p}}),$$

$\forall\, \chi \in \mathrm{Irr}(G)$. Remember that in Section 1.6.11, we gave an explicit method to find α.

Remark 1.7.6. *If instead of the finite field extension E/K we consider the algebraic closure K^{c}, with absolute Galois group denoted by Ω_K, the Hom-formula*

becomes:

$$\mathrm{Cl}(R[G]) \cong \frac{\mathrm{Hom}_{\Omega_K}(R_G, J(K^c))}{\mathrm{Hom}_{\Omega_K}(R_G, (K^c)^\times) \cdot \mathrm{Det}(U(R[G]))}, \tag{1.11}$$

where $J(K^c)$ is given by the direct limit of $J(F)$, as F runs over all finite Galois extensions of K inside K^c.

Remark 1.7.7. *If we replace $R[G]$ by a generic R-order Λ contained in $K[G]$, we also have*

$$\mathrm{Cl}(\Lambda) \cong \frac{\mathrm{Hom}_{G_E}(R_G, J(E))}{\mathrm{Hom}_{G_E}(R_G, E^\times) \cdot \mathrm{Det}(U(\Lambda))}.$$

Remark 1.7.8. *If $\mathcal{M}$ is a maximal order contained in $K[G]$, we have*

$$\mathrm{Det}(U(\mathcal{M})) = \mathrm{Hom}^+_{G_E}(R_G, U(O_E));$$

where now $\mathrm{Hom}^+_{G_E}(R_G, U(O_E))$ denotes the set of homomorphisms which are positive for every symplectic character of G at every idelic component corresponding to infinite real prime ideals of K. A symplectic character is a complex character such that the associated representation $T : G \longrightarrow \mathrm{GL}_{2m}(\mathbb{C})$ factors through $\mathrm{GL}_m(\mathbb{H})$, where $\mathbb{H}$ is the skew-field of real quaternions.
The previous formula is a direct consequence of Remark 1.6.7 and Theorem 1.7.5, using the fact that the symplectic characters correspond exactly to the simple components of $\mathbb{R}[G]$ isomorphic to $\mathrm{M}_n(\mathbb{H})$.
Hereby the Hom-formula for a maximal order simplifies to

$$\mathrm{Cl}(\mathcal{M}) \cong \frac{\mathrm{Hom}_{G_E}(R_G, J(E))}{\mathrm{Hom}_{G_E}(R_G, E^\times) \cdot \mathrm{Hom}^+_{G_E}(R_G, U(O_E))}.$$

1.8 Functorial properties of $\mathrm{Cl}(R[G])$

One of the main advantages of the Hom-description is given by the fact that it allows one to readily express some functorial properties of $\mathrm{Cl}(R[G])$. In this section we state these properties without giving any proof, for details see [18].

For two different algebras A and A' (not necessarily equal to $K[G]$) containing the R-orders Λ and Λ' respectively, a homomorphism of orders $h : \Lambda \to \Lambda'$ easily induces a homomorphism between class groups $\mathrm{Cl}(\Lambda) \to \mathrm{Cl}(\Lambda')$, sending the class $[M]$ to the class $[\Lambda' \otimes_\Lambda M]$.
This property is valid in general, while when we restrict our attention to the special case $A = K[G]$ we have some further functorial properties under the change of the group G or of the field K.

We shall use the notation of the previous section and in particular we recall that E is defined to be a finite Galois extension of K containing the values of the irreducible complex characters of G.

1.8.1 Change of the group

Restriction. Given $H \leq G$, every $R[G]$-module can be considered as an $R[H]$-module, via restriction of scalars. Since $R[G]$ is $R[H]$-free of rank $[G : H]$, every locally free $R[G]$-module is locally free when considered as an $R[H]$-module. This yields a natural restriction map

$$\mathrm{res}^G_H : \mathrm{Cl}(R[G]) \longrightarrow \mathrm{Cl}(R[H]).$$

On the rings of virtual characters we have the induced map $\mathrm{ind}^G_H : R_H \longrightarrow R_G$ which in turn defines a map $r : \mathrm{Hom}(R_G, -) \longrightarrow \mathrm{Hom}(R_H, -)$.
Under the isomorphisms given by the Hom-description, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Cl}(R[G]) & \xrightarrow{\cong} & \mathrm{Hom}_{G_E}(R_G, J(E))/(\mathrm{Hom}_{G_E}(R_G, E^\times) \cdot \mathrm{Det}(U(R[G]))) \\ {\scriptstyle \mathrm{res}^G_H}\downarrow & & \downarrow{\scriptstyle r} \\ \mathrm{Cl}(R[H]) & \xrightarrow{\cong} & \mathrm{Hom}_{G_E}(R_H, J(E))/(\mathrm{Hom}_{G_E}(R_H, E^\times) \cdot \mathrm{Det}(U(R[H]))). \end{array}$$

Example 1.8.2. *Given a group G, let us consider the trivial group $\{1\}$. The only character of $\{1\}$ is the trivial one χ_0 and moreover $\mathrm{ind}^G_{\{1\}}(\chi_0) = \rho_G$, where ρ_G is the character of the regular representation of G defined as $\rho_G := \sum_{\chi \in \mathrm{Irr}(G)} \chi$. Then, given a class $c \in \mathrm{Cl}(R[G])$ represented by $f \in \mathrm{Hom}_{G_E}(R_G, J(E))$, the class $\mathrm{res}^G_{\{1\}}(c)$ is represented by the homomorphism which sends χ_0 to $f(\rho_G)$.*

Induction. Given $H \leq G$ and M a locally free $R[H]$-module, then the tensor product $R[G] \otimes_{R[H]} M$ yields a locally free $R[G]$-module (this is a special case of the general situation described in the introduction of this section). This induces a natural induction map

$$\mathrm{ind}^G_H : \mathrm{Cl}(R[H]) \longrightarrow \mathrm{Cl}(R[G]).$$

Restricting the characters of G to H, gives a restriction map on virtual characters $\mathrm{res}^G_H : R_G \longrightarrow R_H$, which in turn defines a map $i : \mathrm{Hom}(R_H, -) \longrightarrow \mathrm{Hom}(R_G, -)$.
Under the isomorphisms given by the Hom-description, the following diagram

commutes:

$$\begin{array}{ccc} \mathrm{Cl}(R[H]) & \xrightarrow{\cong} & \mathrm{Hom}_{G_E}(R_H, J(E))/(\mathrm{Hom}_{G_E}(R_H, E^\times)\cdot \mathrm{Det}(U(R[H]))) \\ {\scriptstyle \mathrm{ind}_H^G}\downarrow & & \downarrow{\scriptstyle i} \\ \mathrm{Cl}(R[G]) & \xrightarrow{\cong} & \mathrm{Hom}_{G_E}(R_G, J(E))/(\mathrm{Hom}_{G_E}(R_G, E^\times)\cdot \mathrm{Det}(U(R[G]))). \end{array}$$

1.8.3 Change of the base field

Let us consider a finite group G and a finite field extension L/K. Let R' be the integral closure of R in L. Moreover we now choose as E a field extension of L containing all the values of the irreducible complex characters of G such that E/K is Galois. We denote by G'_E the Galois group $\mathrm{Gal}(E/L)$, while G_E will denote as usual $\mathrm{Gal}(E/K)$.

Restriction. Since R' is a projective R-module, we deduce that $R'[G]$ is $R[G]$-projective, then every projective $R'[G]$-module, once considered as an $R[G]$-module, is still projective. This induces a homomorphism $K_0(R'[G]) \longrightarrow K_0(R[G])$ which commutes with completion and in turn gives a map

$$\mathrm{res}_{L/K} : \mathrm{Cl}(R'[G]) \longrightarrow \mathrm{Cl}(R[G]).$$

On the set of homomorphisms of characters we can define a "norm map"

$$\mathcal{N}_{L/K} : \mathrm{Hom}_{G'_E}(R_G, J(E)) \longrightarrow \mathrm{Hom}_{G_E}(R_G, J(E))$$

defined as $\mathcal{N}_{L/K}(f)(\chi) := \prod_{\sigma \in G_E/G'_E} f(\chi^\sigma)^{\sigma^{-1}}$.
Under the isomorphisms given by the Hom-description, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Cl}(R'[G]) & \xrightarrow{\cong} & \mathrm{Hom}_{G'_E}(R_G, J(E))/(\mathrm{Hom}_{G'_E}(R_G, E^\times)\cdot \mathrm{Det}(U(R'[G]))) \\ {\scriptstyle \mathrm{res}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathcal{N}_{L/K}} \\ \mathrm{Cl}(R[G]) & \xrightarrow{\cong} & \mathrm{Hom}_{G_E}(R_G, J(E))/(\mathrm{Hom}_{G_E}(R_G, E^\times)\cdot \mathrm{Det}(U(R[G]))). \end{array}$$

Induction. Given M a locally free $R[G]$-module, then if we consider the tensor product $R' \otimes_R M$ we get a locally free $R'[G]$-module; this gives an induction map

$$\mathrm{ind}_{L/K} : \mathrm{Cl}(R[G]) \longrightarrow \mathrm{Cl}(R'[G]).$$

We also have a canonical injection $i' : \mathrm{Hom}_{G_E}(R_G, J(E)) \longrightarrow \mathrm{Hom}_{G'_E}(R_G, J(E))$. Under the isomorphisms given by the Hom-description, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Cl}(R[G]) & \xrightarrow{\cong} & \mathrm{Hom}_{G_E}(R_G, J(E))/(\mathrm{Hom}_{G_E}(R_G, E^\times) \cdot \mathrm{Det}(U(R[G]))) \\ {\scriptstyle \mathrm{ind}_{L/K}}\downarrow & & \downarrow{\scriptstyle i'} \\ \mathrm{Cl}(R'[G]) & \xrightarrow{\cong} & \mathrm{Hom}_{G'_E}(R_G, J(E))/(\mathrm{Hom}_{G'_E}(R_G, E^\times) \cdot \mathrm{Det}(U(R'[G]))). \end{array}$$

1.9 G-Galois K-algebras

In this section we recall some well-known results on Galois algebras, which will be frequently used in what follows.

Given G a finite group, a finite dimensional K-algebra L (dimension denoted by $[L : K]$), on which G acts on the left as a group of automorphisms, is called G-Galois K-algebra (or G-Galois algebra over K) if:

- L is a commutative finite dimensional separable K-algebra (i.e. isomorphic to a finite direct product of finite algebraic field extensions of K),
- $[L : K] = |G|$,
- $L^G = K$ (fixed elements coincide with the elements of the base field).

A morphism (resp. isomorphism) of G-Galois K-algebras is a morphism (resp. isomorphism) of K-algebras preserving the G-action. Considering these morphisms, we can then look at the category of G-Galois K-algebras.

We define a G-torsor Ω-set (remember that $\Omega = \Omega_K := \mathrm{Gal}(K^c/K)$) as a finite set X with continuous left Ω-action and with right G-action, respecting the relation $\omega \cdot_\Omega (x \cdot_G s) = (\omega \cdot_\Omega x) \cdot_G s$, for all $\omega \in \Omega$, $x \in X$ and $s \in G$, and such that it is a G-torsor, i.e. under the action of G there exists a unique orbit and for some element $x \in X$ (and so for all) the stabilizer is trivial (see also [35, §5.2], where a G-torsor Ω-set is called *espace principal homogène*).

It is well known that there is an anti-equivalence between the category of G-Galois K-algebras and the category of G-torsor Ω-sets (with Ω, G-equivariant functions).

This anti-equivalence sends a G-Galois algebra L/K to the set $\mathrm{Hom}_K(L, K^c)$, on which Ω acts on the left through its natural action on K^c and G on the right

via its action on L. Under this anti-equivalence G-Galois field extensions over K correspond to finite sets with a transitive Ω-action.

If we consider the set of isomorphism classes of G-Galois K-algebras, this is in bijection with the first cohomology set $H^1(\Omega, G)$ (see [35, Proposition 33]). Since Ω acts trivially on G, by the definition of the cohomology sets, $H^1(\Omega, G)$ is given by the quotient $\mathrm{Hom}\,(\Omega, G)\,/\mathrm{Inn}(G)$, where $\mathrm{Inn}(G)$ denotes the set of inner automorphisms of G. Note that, if G is not abelian, this is just a pointed set, while, if G is abelian, $H^1(\Omega, G)$ is a group.
This bijection sends $[h] \in H^1(\Omega, G)$, with representative $h \in \mathrm{Hom}\,(\Omega, G)$, to the G-Galois K-algebra

$$K_h := \mathrm{Map}_{\,\Omega}\left({}^hG, K^{\mathrm{c}}\right),$$

where ${}^hG$ denotes the set G with a possibly non-trivial left Ω-action via the homomorphism h (i.e. $\omega \cdot s = h(\omega)s$, for all $\omega \in \Omega$ and $s \in G$) and $\mathrm{Map}_{\,\Omega}\left({}^hG, K^{\mathrm{c}}\right)$ denotes the algebra of maps $a \in \mathrm{Map}\left({}^hG, K^{\mathrm{c}}\right)$ such that $\omega \cdot (a(s)) = a(\omega \cdot s)$, for all $\omega \in \Omega$ and $s \in G$. The left action of G on K_h is given by the formula $s \cdot a(s') := a(s's)$, for $a \in \mathrm{Map}_{\,\Omega}\left({}^hG, K^{\mathrm{c}}\right)$ and $\forall\, s,\, s' \in G$.
Under this bijection classes of G-Galois field extensions over K correspond to the elements in $H^1(\Omega,\, G)$ represented by surjective homomorphisms in $\mathrm{Hom}(\Omega,\, G)$.

Remark 1.9.1. *If the group G is abelian, then $H^1(\Omega, G) = \mathrm{Hom}\,(\Omega, G)$ and the set of isomorphism classes of G-Galois K-algebras inherits the structure of abelian group. Given $h_1,\, h_2 \in \mathrm{Hom}\,(\Omega, G)$ the product h_1h_2 corresponds to the algebra $K_{h_1h_2}$. The following isomorphism holds*

$$K_{h_1h_2} \cong (K_{h_1} \otimes_K K_{h_2})^{\mathrm{Ker}(m)},$$

where $m : G \times G \longrightarrow G$ is the multiplication homomorphism. Note that this is an isomorphism of G-Galois K-algebras, where on the right G acts as $(1, g)$ (or equivalently as $(g, 1)$). See [28, page 268] for a proof of this fact.

From now on we consider every G-Galois K-algebra, up to isomorphism, as being some K_h, where $h \in \mathrm{Hom}(\Omega,\, G)$. It is evident that an element $a \in K_h$ is determined by the values it assumes on a set of coset representatives of $h(\Omega)\backslash G$, and these values can be chosen arbitrarily with the only restriction that they have to belong to $(K^{\mathrm{c}})^{\mathrm{Ker}(h)}$. This implies that the following isomorphism of K-algebras holds

$$K_h \cong \prod_{i=1}^{[G:h(\Omega)]} K^h, \tag{1.12}$$

where $K^h := (K^c)^{\mathrm{Ker}(h)}$ (this also explains why a surjective h corresponds to a G-Galois field extension over K).

Remark 1.9.2. *Every G-Galois K-algebra is, up to an isomorphism of G-Galois K-algebras, contained in the K^c-algebra* $\mathrm{Map}\,(G, K^c)$.

With this notation the integral closure of O_K inside K_h is given by

$$O_{K_h} := \mathrm{Map}_{\,\Omega}\left({}^hG, O_K^c\right),$$

which is in turn isomorphic to a product of $[G : h(\Omega)]$ copies of O_{K^h} (the ring of integers of the field extension K^h/K).

Remember that in the Notations section we defined $\Omega_\mathfrak{p}$ as $\mathrm{Gal}(K_\mathfrak{p}^c/K_\mathfrak{p})$ and there you can also find the definitions of Ω^t (resp. $\Omega_\mathfrak{p}^t$) and Ω^{nr} (resp. $\Omega_\mathfrak{p}^{nr}$).
Locally, for every place $\mathfrak{p}$ of K, if $h_\mathfrak{p} = h \circ i_\mathfrak{p} \in \mathrm{Hom}(\Omega_\mathfrak{p}, G)$, we have

$$K_{h,\mathfrak{p}} := K_\mathfrak{p} \otimes_K K_h \cong (K_\mathfrak{p})_{h_\mathfrak{p}} = \mathrm{Map}_{\,\Omega_\mathfrak{p}}\left({}^{h_\mathfrak{p}}G, K_\mathfrak{p}^c\right). \tag{1.13}$$

If we regard $\mathrm{Hom}(\Omega_\mathfrak{p}^t, G)$ as a subset of $\mathrm{Hom}(\Omega_\mathfrak{p}, G)$, we say that $(K_\mathfrak{p})_{h_\mathfrak{p}}$ is tame if and only if $h_\mathfrak{p} \in \mathrm{Hom}(\Omega_\mathfrak{p}^t, G)$. Globally K_h is tame if and only if it is tame for all primes $\mathfrak{p}$, or equivalently $h \in \mathrm{Hom}(\Omega^t, G)$.
The definition of unramified algebras is the same with Ω^t (resp. $\Omega_\mathfrak{p}^t$) replaced by Ω^{nr} (resp. $\Omega_\mathfrak{p}^{nr}$). Note that with the term unramified we mean unramified just at the finite places.

Chapter 2

Realizable classes and Stickelberger subgroups

From now on m will denote the exponent of G (i.e. the least common multiple of the orders of the elements of G).

This chapter is devoted to the exposition of McCulloh's results on the problem of realizable classes. Referring to his main work on the subject [28] and to some unpublished notes on two talks given by McCulloh in Oberwolfach in 2002 and in Luminy in 2011, we will introduce $\mathrm{St}(O_K[G])$ a particular subgroup of $\mathrm{Cl}(O_K[G])$, defined through the use of a Stickelberger map. Then we shall give the unpublished proof of the following result (this corresponds to Theorem 0.0.5 in the Introduction).

Theorem A. *For every number field K and finite group G, we have*

$$R_A(O_K[G]) \subseteq \mathrm{St}(O_K[G]).$$

The description and the notation used for the subgroup $\mathrm{St}(O_K[G])$ do not reflect McCulloh's original choice, but they are rather inspired from some later informal notes by A. Agboola. I am heartily thankful to A. Agboola for his notes, which I used to clarify many points of this chapter.

In the last section of the chapter we restrict our attention to the abelian case and we will explain the proof of the following theorem, which is the main result contained in [28] (this is a more precise version of Theorem 0.0.4 in the Introduction).

Theorem B. *For every number field K and finite* ***abelian*** *group G, we have*

$$R_A(O_K[G]) = \mathrm{St}(O_K[G]).$$

Moreover $R_F(O_K[G]) = R_A(O_K[G])$ and every class can be obtained from a G-Galois field extension K_h/K unramified at a preassigned finite set of finite primes of K.

2.1 Resolvends

One of the main tools used by McCulloh in his works is the notion of resolvend, which, following McCulloh, we spell with the letter "d" on purpose. Roughly speaking it is similar to the Fourier transform, that allows us to attach to any element in a G-Galois K-algebra an element in $K^c[G]$. We will see how some properties of the resolvend map are closely connected to the notions of normal bases in Galois algebra extensions.
The word "resolvend" is similar to "resolvent". In fact these two objects are closely related and indeed one can obtain the second from the first using the characters of G.

Let us recall that Ω denotes the absolute Galois group $\Omega_K := \mathrm{Gal}(K^c/K)$.

As we have already seen in §1.9, any G-Galois K-algebra can be viewed, up to isomorphism, as $K_h := \mathrm{Map}_{\Omega}\left({}^hG, K^c\right)$, where $h \in \mathrm{Hom}(\Omega, G)$. In particular any G-Galois K-algebra may be viewed as lying in the K^c-algebra $\mathrm{Map}\,(G, K^c)$ (Remark 1.9.2). The resolvend map is then defined as follows

$$\begin{array}{rcl} r_G : \mathrm{Map}\,(G, K^c) & \longrightarrow & K^c[G] \\ a & \longmapsto & \displaystyle\sum_{s\in G} a(s)s^{-1}. \end{array}$$

We underline the two following properties:

($P1$) r_G is a $K^c[G]$-module isomorphism (but not an isomorphism of algebras since it does not preserve multiplication);

($P2$) given $a \in \mathrm{Map}\,(G, K^c)$ and Ω acting on the left on $K^c[G]$ via its action on the coefficients in K^c, we see that $a \in K_h \iff r_G(a)^\omega = r_G(a)h(\omega)$, $\forall\, \omega \in \Omega$.

We recall that an element $a \in K_h$ is called a normal basis generator (NBG) of K_h over K if the set $\{s \cdot a\}_{s \in G}$ forms a K-basis of K_h. Such a basis is called a normal basis. Analogously, an element of K_h is called a normal integral basis generator (NIBG) of K_h over K if it is a normal basis generator for O_{K_h} over O_K. The first property connecting resolvends with these notions is the following.

Proposition 2.1.1 (NBG)**.** *For every $a \in K_h$, we have*

$$a \text{ is a normal basis generator of } K_h \text{ over } K \iff r_G(a) \in K^c[G]^\times.$$

Proof. [28, Proposition 1.8]. □

Following the notation used by McCulloh in his work, we introduce the following definitions:

$$\begin{aligned} H(K[G]) &:= \left\{\alpha \in K^c[G]^\times \,|\, \alpha^{-1} \cdot \alpha^\omega \in G,\ \forall \omega \in \Omega\right\}, \\ \mathcal{H}(K[G]) &:= H(K[G])/G = \{\alpha \cdot G \,|\, \alpha \in H(K[G])\} = \left(K^c[G]^\times/G\right)^\Omega. \end{aligned}$$

Pay attention that $\mathcal{H}(K[G])$ is just a left coset space.

Corollary 2.1.2. $H(K[G]) = \{r_G(a) \,|\, a \text{ NBG of } K_h/K \text{ for } h \in \mathrm{Hom}(\Omega, G)\}$.

Proof. ($\subseteq$) Given $\alpha \in H(K[G])$, since the resolvend map is an isomorphism of $K^c[G]$-modules we have that there exists $a' \in \mathrm{Map}(G, K^c)$ such that $\alpha = r_G(a')$. Thanks to the fact that for any $\omega \in \Omega$, the element $r_G(a')^{-1} \cdot r_G(a')^\omega$ belongs to G, we can consider a homomorphism $h' \in \mathrm{Hom}(\Omega, G)$ defined as $h'(\omega) := r_G(a')^{-1} \cdot r_G(a')^\omega$. The proof that h' is an homomorphism follows from the fact that Ω acts on the left on $K^c[G]^\times$, indeed

$$\begin{aligned} h'(\omega_1\omega_2) &= \alpha^{-1} \cdot (\omega_1\omega_2 \cdot \alpha) \\ &= \alpha^{-1} \cdot (\omega_1 \cdot (\omega_2 \cdot \alpha)) \\ &= \alpha^{-1} \cdot \left(\omega_1 \cdot \left(\alpha \cdot \alpha^{-1} \cdot (\omega_2 \cdot \alpha)\right)\right) \\ &= \alpha^{-1} \cdot (\omega_1 \cdot \alpha) \cdot \left(\omega_1 \cdot \left(\alpha^{-1} \cdot (\omega_2 \cdot \alpha)\right)\right) \\ &= \alpha^{-1} \cdot (\omega_1 \cdot \alpha) \cdot \alpha^{-1} \cdot (\omega_2 \cdot \alpha) \\ &= h'(\omega_1)h'(\omega_2), \end{aligned}$$

where we used the property that $\alpha^{-1} \cdot (\omega_2 \cdot \alpha) \in G$ and so it is fixed under the action of Ω.
We immediately see that $a' \in K_{h'}$ and that it is a normal basis generator of it by

Proposition 2.1.1.
($\supseteq$) Just use (P2). □

Thus we have just proved that $H(K[G])$ coincides with the set of resolvends of normal basis generators for G-Galois algebras over K and we easily deduce that $\mathcal{H}(K[G])$ is in bijection with the set of normal bases for G-Galois K-algebras, since we take the quotient by G.
If we consider the quotient map $\mathrm{rag} : K^c[G]^\times \longrightarrow K^c[G]^\times/G$, we can write

$$\mathcal{H}(K[G]) = \{\mathrm{rag}(r_G(a)) |\, a \text{ NBG of } K_h/K \text{ for } h \in \mathrm{Hom}(\Omega, G)\}\,. \tag{2.1}$$

Proposition 2.1.3. *There is an exact sequence of pointed sets (groups if G is abelian)*

$$1 \longrightarrow G \longrightarrow K[G]^\times \xrightarrow{\mathrm{rag}} \mathcal{H}(K[G]) \longrightarrow H^1(\Omega, G) \longrightarrow 1.$$

Proof. As in the abelian case treated in [28], we consider the following exact sequence of pointed sets:

$$1 \longrightarrow G \longrightarrow K^c[G]^\times \xrightarrow{\mathrm{rag}} K^c[G]^\times/G \longrightarrow 1\ . \tag{2.2}$$

Applying (non-abelian) Ω-cohomology (see [35, Chapter 1, §5]), we get in turn the following exact sequence of pointed sets:

$$1 \longrightarrow G \longrightarrow K[G]^\times \xrightarrow{\mathrm{rag}} \mathcal{H}(K[G]) \longrightarrow H^1(\Omega, G) \longrightarrow 1. \tag{2.3}$$

The surjectivity on the right follows from the fact that any G-Galois K-algebra has a normal basis generator and (2.1). □

Remark 2.1.4. *Let A, B, C be three pointed sets with distinguished elements a_0, b_0, c_0, respectively. Recall that the following sequence of pointed sets*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

(with maps preserving the distinguished elements) is called exact if the image of f is equal to the inverse image under g of the distinguished element of C, i.e.

$$f(A) = g^{-1}(c_0).$$

Analogously, we also have a local notion of the sets just defined. For each finite place $\mathfrak{p}$ of K:

$$\begin{aligned} H(K_{\mathfrak{p}}[G]) &:= \left\{\alpha \in K_{\mathfrak{p}}^{c}[G]^{\times} \,|\, \alpha^{-1} \cdot \alpha^{\omega} \in G,\ \forall \omega \in \Omega_{\mathfrak{p}}\right\} \\ &= \left\{r_G(a_{\mathfrak{p}}) \,|\, a_{\mathfrak{p}} \text{ NBG of } (K_{\mathfrak{p}})_{h_{\mathfrak{p}}}/K_{\mathfrak{p}} \text{ for } h_{\mathfrak{p}} \in \mathrm{Hom}(\Omega_{\mathfrak{p}}, G)\right\}, \\ \mathcal{H}(K_{\mathfrak{p}}[G]) &:= H(K_{\mathfrak{p}}[G])/G = \{\alpha \cdot G \,|\, \alpha \in H(K_{\mathfrak{p}}[G])\}. \end{aligned}$$

An integral analog of Proposition 2.1.3 exists just for unramified extensions as explained by the following proposition.

Proposition 2.1.5 (NIBG)**.** *Given $a \in K_h$, such that $K_h = K[G] \cdot a$, we have*

*a is a NIBG of K_h and K_h/K is **unramified** at all fin. $\mathfrak{p} \iff r_G(a) \in O_K^c[G]^{\times}$.*

Proof. The proof consists in slightly adapting the original proof given in [28, (2.11)] to the non-abelian case.
Let us consider the map $[-1] : G \longrightarrow G$ which sends an element $s \in G$ to its inverse s^{-1}. This map induces involutions on $\mathrm{Map}\,(G, K^{c})$ and $K^{c}[G]$, that we denote with the same symbol $[-1]$.
Let $\mathrm{Tr} : \mathrm{Map}\,(G, K^{c}) \longrightarrow K^{c}$ denote the standard trace map defined on $a \in \mathrm{Map}\,(G, K^{c})$ by the formula $\mathrm{Tr}(a) = \sum_{s \in G} a(s)$. By restriction, it induces a trace map $\mathrm{Tr} : K_h \longrightarrow K$. Note that the associated bilinear form, which sends $(a, b) \in K_h \times K_h$ to $\mathrm{Tr}(ab) \in K$, is non-degenerate.
Moreover, given M an O_K-lattice of K_h (i.e. an O_K-submodule of K_h, finitely generated and projective as an O_K-module and such that $K \cdot M = K_h$), its dual lattice M^* is defined as

$$M^* := \{b \in K_h \,|\, \mathrm{Tr}(b \cdot M) \subseteq O_K\}.$$

The discriminant of K_h is then defined as

$$\mathrm{disc}(O_{K_h}/O_K) := [O_{K_h}^* : O_K]_{O_K},$$

where $[- : -]_{O_K}$ denotes the O_K-module index. By definition, the algebra K_h is unramified at all finite places if and only if its discriminant is (1).
For every $a, b \in K_h$, we have the following formula

$$r_G(a) \cdot r_G(b)^{[-1]} = \sum_{s \in G} \mathrm{Tr}(a^s b) s^{-1}, \tag{2.4}$$

where, given an element $s \in G$, the map $a^s \in K_h$ is defined, for every $t \in G$, by the formula $a^s(t) = a(ts)$. The proof of (2.4) follows by an easy computation, that can be found explicitely in [27, (1.6)] (pay attention that the calculation given there is still correct if G is non-abelian).
Moreover, exactly as in [28, (2.11)], we have the following properties:

- there exists a map $b \in K_h$ such that $r_G(a)^{[-1]} = r_G(b)^{-1}$ and $(O_K[G] \cdot a)^* = O_K[G] \cdot b$,
- $[(O_K[G] \cdot a)^* : O_K[G] \cdot a]_{O_K} = \left[O_K[G] : O_K[G] r_G(a) r_G(a)^{[-1]}\right]_{O_K}$.

Then, using the inclusions $O_K[G] \cdot a \subseteq O_{K_h} \subseteq O_{K_h}^* \subseteq (O_K[G] \cdot a)^*$, the conclusion follows exactly as in the abelian case ([28, (2.11)]). □

If we denote by $H^1(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G)$ the elements in $H^1(\Omega_{\mathfrak{p}}, G)$ coming from the homomorphisms h in $\mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G)$, thanks to the local version of the previous proposition, we have a local integral analog of the exact sequence (2.3).

Proposition 2.1.6. *For any finite place $\mathfrak{p}$, there is an exact sequence of pointed sets (groups if G is abelian)*

$$1 \longrightarrow G \longrightarrow O_{K,\mathfrak{p}}[G]^\times \xrightarrow{\mathrm{rag}} \mathcal{H}(O_{K,\mathfrak{p}}[G]) \longrightarrow H^1(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G) \longrightarrow 1, \tag{2.5}$$

Proof. Clear from above and from the fact that any local unramified extension has a NIBG. □

Now, analogously as before, we have

$$\begin{aligned} H(O_{K,\mathfrak{p}}[G]) &:= \left\{\alpha \in O_{K,\mathfrak{p}}^c[G]^\times \,|\, \alpha^{-1} \cdot \alpha^\omega \in G,\ \forall\, \omega \in \Omega_{\mathfrak{p}}\right\} \\ &= \left\{r_G(a_{\mathfrak{p}}) \,|\, a_{\mathfrak{p}} \text{ NIBG for } (K_{\mathfrak{p}})_{h_{\mathfrak{p}}} \text{ where } h_{\mathfrak{p}} \in \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G\right)\right\}, \end{aligned} \tag{2.6}$$

$$\begin{aligned} \mathcal{H}(O_{K,\mathfrak{p}}[G]) &:= H(O_{K,\mathfrak{p}}[G])/G \\ &= \{\alpha \cdot G \,|\, \alpha \in H(O_{K,\mathfrak{p}}[G])\} \\ &= \left\{\mathrm{rag}(r_G(a_{\mathfrak{p}})) \,|\, a_{\mathfrak{p}} \text{ NIBG for } (K_{\mathfrak{p}})_{h_{\mathfrak{p}}} \text{ where } h_{\mathfrak{p}} \in \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G\right)\right\}. \end{aligned}$$

Remark 2.1.7. *If K_h/K is a tame G-Galois extension, we know by Proposition 1.6.12, that its representative in terms of the idelic description is given by the idèle $(c_{\mathfrak{p}})_{\mathfrak{p}}$ defined componentwise by the relation $a_{\mathfrak{p}} = c_{\mathfrak{p}} \cdot b$ (with b considered as*

embedded in the completion at $\mathfrak{p}$), where b and $a_{\mathfrak{p}}$ are normal basis generator and local normal integral basis generator of K_h/K, respectively.
If we apply $\mathrm{rag} \circ r_G$ *to the previous equality, we get*

$$\mathrm{rag}(r_G(a_{\mathfrak{p}})) = \mathrm{rag}(c_{\mathfrak{p}}) \cdot \mathrm{rag}(r_G(b))$$

in $\mathcal{H}(K_{\mathfrak{p}}[G])$. This condition is sufficient to characterize $[O_{K_h}]$, since, as explained in [28, page 277], if $\mathrm{rag}(c'_{\mathfrak{p}}) = \mathrm{rag}(c_{\mathfrak{p}})$ for each $\mathfrak{p}$, then $(c_{\mathfrak{p}})_{\mathfrak{p}}$ and $(c'_{\mathfrak{p}})_{\mathfrak{p}}$ differ by an element $(s_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} G$ and hence represent the same class in $\mathrm{Cl}(O_K[G])$.

Note that at the infinite primes we take $c_{\mathfrak{p}} = 1$ (since at those primes we can take $a_{\mathfrak{p}}$ equal to the embedding of b in the completion) and this is the reason why in what follows these primes play no role.

2.2 Determinants of resolvends

We shall now see how determinants of resolvends may be represented in terms of character maps.

Given an irreducible character χ of G, the map $\det_\chi$ (Chapter 1, Section 1.7.1) is a character of G of degree 1 (or a character of G^{ab}) and it was defined as

$$\det_\chi(s) = \det(T_\chi(s)),$$

where T_χ is a representation associated to χ.
This definition is independent of the choice of the representation T_χ and we can in turn consider the homomorphism $\det : R_G \longrightarrow \widehat{G^{\mathrm{ab}}}$ defined by

$$\det\left(\sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi\right) = \prod_{\chi \in \mathrm{Irr}(G)} (\det_\chi)^{a_\chi}.$$

Let $\mathcal{A}_G$ be the kernel of this map, we shall call it the augmentation kernel. Then we can consider the following short exact sequence of groups:

$$0 \longrightarrow \mathcal{A}_G \longrightarrow R_G \xrightarrow{\det} \widehat{G^{\mathrm{ab}}} \longrightarrow 1. \tag{2.7}$$

Remark 2.2.1. *When the group G is abelian we have an explicit $\mathbb{Z}$-basis of $\mathcal{A}_G$. From the proof of [28, Theorem 2.14], if $\mathrm{Irr}(G)$ has a basis $\chi_1, \ldots, \chi_k$, with χ_i of order e_i, for $i = 1, \ldots, k$ and any $\chi \in \mathrm{Irr}(G)$ is written uniquely as $\chi = \prod_{i=1}^{k} \chi_i^{r_i(\chi)}$,*

where $0 \leq r_i(\chi) < e_i$*; a* $\mathbb{Z}$*-basis of* $\mathcal{A}_G$ *is given by the non-zero elements in the collection* $\{e_i\chi_i |\, i = 1, \ldots, k\} \cup \{\chi - \sum_{i=1}^{k} r_i(\chi)\chi_i |\, \chi \in \mathrm{Irr}(G)\}$.

Going back to the previous short exact sequence and using the fact that $(K^{\mathrm{c}})^{\times}$ is injective, the functor $\mathrm{Hom}(-, (K^{\mathrm{c}})^{\times})$ gives the following short exact sequence

$$1 \longrightarrow \mathrm{Hom}\left(\widehat{G^{\mathrm{ab}}},\, (K^{\mathrm{c}})^{\times}\right) \longrightarrow \mathrm{Hom}\left(R_G,\, (K^{\mathrm{c}})^{\times}\right) \xrightarrow{\mathrm{rag}'} \mathrm{Hom}\left(\mathcal{A}_G,\, (K^{\mathrm{c}})^{\times}\right) \longrightarrow 1 \tag{2.8}$$

where the map rag′ is just the restriction map to the augmentation kernel (this also explains its name).

Extending the definition of the map Det given in Section 1.7.1 to

$$\mathrm{Det} : K^{\mathrm{c}}[G]^{\times} \longrightarrow \mathrm{Hom}\left(R_G, (K^{\mathrm{c}})^{\times}\right)$$

we have now the following proposition.

Proposition 2.2.2. (Global commutative diagram). *There is a commutative* Ω*-diagram (every map preserves the action of* Ω*) of pointed sets with exact rows:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G & \longrightarrow & K^{\mathrm{c}}[G]^{\times} & \xrightarrow{\mathrm{rag}} & K^{\mathrm{c}}[G]^{\times}/G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \widetilde{\mathrm{Det}}} & & \\ 1 & \longrightarrow & G^{\mathrm{ab}} & \longrightarrow & \mathrm{Hom}\left(R_G, (K^{\mathrm{c}})^{\times}\right) & \xrightarrow{\mathrm{rag}'} & \mathrm{Hom}\left(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}\right) & \longrightarrow & 1 \end{array} \tag{2.9}$$

Proof. If $s \in G$, then $\mathrm{Det}(s)(\chi) = \det_{\chi}(s)$ and so Det restricted to G has image $\mathrm{Hom}\left(\widehat{G^{\mathrm{ab}}}, (K^{\mathrm{c}})^{\times}\right) \cong G^{\mathrm{ab}}$ (by duality). Thus Det induces a map $\widetilde{\mathrm{Det}} : K^{\mathrm{c}}[G]^{\times}/G \longrightarrow \mathrm{Hom}\left(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}\right)$, making the diagram commute. □

Remark 2.2.3. *Note that from the definition of the map* Det *and from the canonical isomorphism* $\mathrm{Hom}\left(\widehat{G^{\mathrm{ab}}}, (K^{\mathrm{c}})^{\times}\right) \cong G^{\mathrm{ab}}$*, the map* $\mathrm{Det} : G \longrightarrow G^{\mathrm{ab}}$ *coincides with the natural quotient map* $G \longrightarrow G^{\mathrm{ab}}$ *which sends* $s \in G$ *to its associated coset in* $G/[G, G]$.

Applying (non-abelian) Ω-cohomology we deduce the following proposition.

Proposition 2.2.4. (Global commutative diagram 2). *There is the following commutative diagram of pointed sets with exact rows:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G & \longrightarrow & K[G]^{\times} & \xrightarrow{\mathrm{rag}} & \mathcal{H}(K[G]) & \longrightarrow & H^1(\Omega, G) \longrightarrow 1 \\ & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \widetilde{\mathrm{Det}}} & & \downarrow \\ 1 & \longrightarrow & G^{\mathrm{ab}} & \longrightarrow & \mathrm{Hom}_{\Omega}\left(R_G, (K^{\mathrm{c}})^{\times}\right) & \xrightarrow{\mathrm{rag}'} & \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}\right) & \longrightarrow & \mathrm{Hom}\left(\Omega, G^{\mathrm{ab}}\right) \longrightarrow 1 \end{array}$$

Proof. We just note that exactness at the bottom row follows applying Ω-cohomology to the sequence (2.8).
Indeed $H^1(\Omega, \mathrm{Hom}\left(R_G, (K^c)^\times\right)) = 1$, since $\mathrm{Hom}\left(R_G, (K^c)^\times\right)$ is isomorphic to $Z(K^c[G])^\times$ and $H^1(\Omega, Z(K^c[G])^\times) = 1$, by Hilbert's Satz 90 (see [34, Chapter X, §1]). □

Similarly, for any place $\mathfrak{p}$ of K, we have an analogous diagram.

Proposition 2.2.5. (Local commutative diagram). *The following diagram of pointed sets with exact rows commutes:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G & \longrightarrow & K_{\mathfrak{p}}[G]^\times & \xrightarrow{\mathrm{rag}} & \mathcal{H}(K_{\mathfrak{p}}[G]) & \longrightarrow & H^1(\Omega_{\mathfrak{p}}, G) \longrightarrow 1 \\ & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \widetilde{\mathrm{Det}}} & & \downarrow \\ 1 & \longrightarrow & G^{\mathrm{ab}} & \longrightarrow & \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(R_G, \left(K_{\mathfrak{p}}^c\right)^\times\right) & \xrightarrow{\mathrm{rag}'} & \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, \left(K_{\mathfrak{p}}^c\right)^\times\right) & \longrightarrow & \mathrm{Hom}\left(\Omega_{\mathfrak{p}}, G^{\mathrm{ab}}\right) \longrightarrow 1 \end{array}$$

From Proposition 2.1.6, the integral analog follows.

Proposition 2.2.6. (Local integral commutative diagram) *For any finite place* $\mathfrak{p}$ *of* K*, we have the following commutative diagram:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G & \longrightarrow & O_{K,\mathfrak{p}}[G]^\times & \xrightarrow{\mathrm{rag}} & \mathcal{H}(O_{K,\mathfrak{p}}[G]) & \longrightarrow & H^1(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G) \longrightarrow 1 \\ & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \mathrm{Det}} & & \downarrow{\scriptstyle \widetilde{\mathrm{Det}}} & & \downarrow \\ 1 & \longrightarrow & G^{\mathrm{ab}} & \longrightarrow & \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(R_G, \left(O_{K,\mathfrak{p}}^c\right)^\times\right) & \xrightarrow{\mathrm{rag}'} & \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, \left(O_{K,\mathfrak{p}}^c\right)^\times\right) & \longrightarrow & \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G^{\mathrm{ab}}\right) \longrightarrow 1\,. \end{array}$$

Proof. We just note that exactness at the bottom row follows from the fact that the map $H^1(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G) \longrightarrow \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G^{\mathrm{ab}}\right)$, induced by the natural map from $\mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G\right)$ to $\mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G^{\mathrm{ab}}\right)$, is surjective as one can check using the description of $\Omega_{\mathfrak{p}}^{\mathrm{nr}}$ as a procyclic group (see at the beginning of Section 2.4). □

Therefore we have defined the following maps of pointed sets

$$\widetilde{\mathrm{Det}} : \mathcal{H}(K[G]) \longrightarrow \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, (K^c)^\times\right) \tag{2.10}$$

$$\widetilde{\mathrm{Det}} : \mathcal{H}(K_{\mathfrak{p}}[G]) \longrightarrow \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, \left(K_{\mathfrak{p}}^c\right)^\times\right) \tag{2.11}$$

$$\widetilde{\mathrm{Det}} : \mathcal{H}(O_{K,\mathfrak{p}}[G]) \longrightarrow \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, \left(O_{K,\mathfrak{p}}^c\right)^\times\right) \tag{2.12}$$

and we can actually show that the image of (2.12) is a group. Before giving the proof, let us make the following remark.

Remark 2.2.7. *There is a left action of $O_{K,\mathfrak{p}}[G]^\times$ on $\mathcal{H}(O_{K,\mathfrak{p}}[G])$ defined, via left multiplication, as follows*

$$\begin{aligned} O_{K,\mathfrak{p}}[G]^\times \times \mathcal{H}(O_{K,\mathfrak{p}}[G]) &\longrightarrow \mathcal{H}(O_{K,\mathfrak{p}}[G]) \\ (\lambda, [\alpha]) &\longmapsto [\lambda \cdot \alpha]. \end{aligned}$$

It is easy to see that this action is well defined and that $\lambda \cdot \alpha \in H(O_{K,\mathfrak{p}}[G])$.

Proposition 2.2.8. *The image of (2.12) is a group.*

Proof. From the diagram of Proposition 2.2.6, we have

$$(O_{K,\mathfrak{p}}[G]^\times) \setminus \mathcal{H}(O_{K,\mathfrak{p}}[G]) \cong H^1(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G),$$

where here the symbol $(O_{K,\mathfrak{p}}[G]^\times) \setminus \mathcal{H}(O_{K,\mathfrak{p}}[G])$ denotes the set of orbits of the set $\mathcal{H}(O_{K,\mathfrak{p}}[G])$ under the left action of $O_{K,\mathfrak{p}}[G]^\times$ (see Remark 2.2.7).
Thus, applying the map $\widetilde{\mathrm{Det}}$, we get

$$\mathrm{rag}'(\mathrm{Det}(O_{K,\mathfrak{p}}[G]^\times)) \setminus \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G])) \cong \mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G^{\mathrm{ab}}),$$

since the map $H^1(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G) \longrightarrow \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G^{\mathrm{ab}}\right)$ is surjective. Thus the orbit space $\mathrm{rag}'(\mathrm{Det}(O_{K,\mathfrak{p}}[G]^\times)) \setminus \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$ inherits from $\mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G^{\mathrm{ab}})$ the structure of an abelian group.
From this we can now prove the group structure of $\widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$: given $\widetilde{\mathrm{Det}}(x)$, $\widetilde{\mathrm{Det}}(y) \in \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$, there exist λ in $O_{K,\mathfrak{p}}[G]^\times$ and $z \in \mathcal{H}(O_{K,\mathfrak{p}}[G])$ such that

$$\widetilde{\mathrm{Det}}(x) \cdot \widetilde{\mathrm{Det}}(y) = \mathrm{rag}'(\mathrm{Det}(\lambda)) \cdot \widetilde{\mathrm{Det}}(z),$$

where the products are considered in $\mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, \left(O_{K,\mathfrak{p}}^{\mathrm{c}}\right)^\times\right)$. Moreover

$$\begin{aligned} \widetilde{\mathrm{Det}}(x) \cdot \widetilde{\mathrm{Det}}(y) &= \mathrm{rag}'(\mathrm{Det}(\lambda)) \cdot \widetilde{\mathrm{Det}}(z) \\ &= \widetilde{\mathrm{Det}}(\lambda \cdot z), \end{aligned}$$

which therefore proves, by Remark 2.2.7, that $\widetilde{\mathrm{Det}}(x) \cdot \widetilde{\mathrm{Det}}(y) \in \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$, as we wanted to prove. Analogously, given $x \in \mathcal{H}(O_{K,\mathfrak{p}}[G])$, one can prove that $\widetilde{\mathrm{Det}}(x)^{-1} \in \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$. □

Note that, for every finite place $\mathfrak{p}$ of K, since the reduced norm rn sends $O_{K,\mathfrak{p}}^{\mathrm{c}}[G]^\times$ into $Z(O_{K,\mathfrak{p}}^{\mathrm{c}}[G])^\times$ and thanks to Theorem 1.7.5, we have the following inclusions

$$\widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G])) \subseteq \left(Z(O_{K,\mathfrak{p}}^{\mathrm{c}}[G])^\times / G^{\mathrm{ab}}\right)^{\Omega_{\mathfrak{p}}} \subseteq \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, \left(O_{K,\mathfrak{p}}^{\mathrm{c}}\right)^\times\right). \quad (2.13)$$

When the finite place $\mathfrak{p}$ does not divide $|G|$, then $O_{K,\mathfrak{p}}[G]$ is a maximal order of $K_{\mathfrak{p}}[G]$ and, from Remarks 1.6.7 and 1.7.8,

$$\mathrm{rn}(O_{K,\mathfrak{p}}[G]^{\times}) = Z(O_{K,\mathfrak{p}}[G])^{\times} \cong \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(R_G, \left(O^{\mathrm{c}}_{K,\mathfrak{p}}\right)^{\times}\right).$$

Thus in these cases the inclusions in (2.13) are actually equalities, as one can deduce looking at the diagram of Proposition 2.2.6 and at the proof of Proposition 2.2.8.

When $\mathfrak{p}$ divides $|G|$, we need not have equality, nevertheless, when G is abelian, the following approximation result does hold.

Proposition 2.2.9. *Let G be abelian. If $\mathfrak{m}$ is an integral ideal of O_K divisible by a sufficiently high power of $|G|$, we have*

$$\mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, (1+\mathfrak{m}O^{c}_{K,\mathfrak{p}}) \cap (O^{c}_{K,\mathfrak{p}})^{\times}\right) \subseteq \widetilde{\mathrm{Det}}\left(\mathcal{H}(O_{K,\mathfrak{p}}[G])\right) \subseteq \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^{\times}\right),$$

for each finite place $\mathfrak{p}$ of K.

Proof. See [28, Theorem 2.14] for the original proof by McCulloh. □

Remark 2.2.10. *It is important to note that when G is abelian, the $\widetilde{\mathrm{Det}}$ maps (2.10) and (2.11) are isomorphisms and that $\left(Z(O^{\mathrm{c}}_{K,\mathfrak{p}}[G])^{\times}/G^{\mathrm{ab}}\right)^{\Omega_{\mathfrak{p}}}$ equals the set $\mathcal{H}(O_{K,\mathfrak{p}}[G])$. Thus, we can replace $\widetilde{\mathrm{Det}}\left(\mathcal{H}(O_{K,\mathfrak{p}}[G])\right)$ with $\mathcal{H}(O_{K,\mathfrak{p}}[G])$ in Proposition 2.2.9 (as well as in what follows when G is abelian).*

Now if we write

$$\mathcal{U}(O_K[G]) := \prod_{\mathfrak{p}} \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G])) \subseteq \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right) \tag{2.14}$$

and we define the group

$$\mathrm{MCl}(O_K[G]) := \frac{\mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)}{\mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}\right) \cdot \mathcal{U}(O_K[G])},$$

we see that the map $\mathrm{rag}' : \mathrm{Hom}_{\Omega}\left(R_G, J(K^{\mathrm{c}})\right) \longrightarrow \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)$, induced by the local version of (2.8), yields a group homomorphism

$$\mathrm{Rag} : \frac{\mathrm{Hom}_{\Omega}\left(R_G, J(K^{\mathrm{c}})\right)}{\mathrm{Hom}_{\Omega}\left(R_G, (K^{\mathrm{c}})^{\times}\right) \cdot \mathrm{Det}(U(O_K[G]))} \longrightarrow \frac{\mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)}{\mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}\right) \cdot \mathcal{U}(O_K[G])} \tag{2.15}$$

which, by the Hom-description of $\mathrm{Cl}(O_K[G])$ (see (1.11)), can be written as

$$\mathrm{Rag} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{MCl}(O_K[G]).$$

If we now consider $R_{\mathrm{nr}}(O_K[G])$, the subset of realizable classes given by unramifed (at finite places) G-Galois K-algebras, using the previous results on resolvends and via §1.6.11, we have the following result.

Proposition 2.2.11. *For every finite group G and number field K,*

$$R_{\mathrm{nr}}(O_K[G]) \subseteq \mathrm{Ker}(\mathrm{Rag}).$$

Proof. If K_h/K is an unramified G-Galois K-algebra, we consider $b \in K_h$ a normal basis generator of K_h/K and, for each finite place $\mathfrak{p}$ of K, we choose $a_{\mathfrak{p}} \in O_{K_h,\mathfrak{p}}$ a normal integral basis generator. Considering the idèle $c = (c_{\mathfrak{p}})_{\mathfrak{p}}$ defined componentwise by the relation $\mathrm{rag}(r_G(a_{\mathfrak{p}})) = \mathrm{rag}(c_{\mathfrak{p}}) \cdot \mathrm{rag}(r_G(b))$ (Remark 2.1.7), the element $\mathrm{Det}(c)$ represents the class $[O_{K_h}]$ in terms of the Hom-description (at the infinite primes we take $c_{\mathfrak{p}} = 1$). From the local analog of Proposition 2.2.2,

$$\mathrm{rag}'(\mathrm{Det}(c)) = \widetilde{\mathrm{Det}}(\mathrm{rag}(c)) = \left(\widetilde{\mathrm{Det}}\left(\mathrm{rag}(r_G(a_{\mathfrak{p}}))\right) \cdot \widetilde{\mathrm{Det}}\left(\mathrm{rag}(r_G(b))^{-1}\right)\right)_{\mathfrak{p}}$$

which, by Proposition 2.1.1 and Proposition 2.1.5, gives the proof. □

2.3 The Stickelberger map

In order to describe resolvends of local normal integral basis generators in the ramified case, McCulloh introduced a Stickelberger map $\Theta_G : \mathcal{A}_G \longrightarrow \mathbb{Z}[G]$. It is in particular its transpose $\Theta_G^t : \mathrm{Hom}\left(\mathbb{Z}[G], -\right) \longrightarrow \mathrm{Hom}\left(\mathcal{A}_G, -\right)$, after a necessary adjustment due to the Ω-action, which will be used to give a local decomposition of resolvends. The original definition of the Stickelberger map, when G is abelian, is contained in [28], while its extension to the non-abelian case was presented for the first time by McCulloh in a talk given in Oberwolfach in 2002. Let us start defining the Stickelberger pairing.

We define a $\mathbb{Q}$-pairing $\langle -, - \rangle : \mathbb{Q} \otimes_{\mathbb{Z}} R_G \times \mathbb{Q}[G] \longrightarrow \mathbb{Q}$ as follows:

- ⋆ Characters of degree 1. If χ is a character of degree 1 and $s \in G$, $\langle \chi, s \rangle$ is the rational number defined by

$$\chi(s) = e^{2\pi i \langle \chi, s \rangle},$$

such that $0 \leq \langle \chi, s \rangle < 1$. This was the original definition contained in [28] (in the abelian case every irreducible character is of dimension 1). If G is abelian, this already defines, extending it by $\mathbb{Q}$-bilinearity, a $\mathbb{Q}$-pairing $\langle -, - \rangle : \mathbb{Q} \otimes_{\mathbb{Z}} R_G \times \mathbb{Q}[G] \longrightarrow \mathbb{Q}$.

$\star$ Characters of higher degree. If χ is a character of degree bigger than 1, then we define

$$\langle \chi, s \rangle := \langle \mathrm{res}^G_{\langle s \rangle} \chi, s \rangle,$$

where $\mathrm{res}^G_{\langle s \rangle} \chi$ is the restriction of the character χ to the cyclic group generated by s.

Extending it by $\mathbb{Q}$-bilinearity, we have the required pairing for a generic finite group G.

Thanks to this pairing, the Stickelberger map $\Theta_G : \mathbb{Q} \otimes_{\mathbb{Z}} R_G \longrightarrow \mathbb{Q}[G]$ is defined by $\mathbb{Z}$-linearity as

$$\Theta_G(\chi) := \sum_{s \in G} \langle \chi, s \rangle s.$$

Going back to the definition of $\mathcal{A}_G$, we can now prove the following proposition.

Proposition 2.3.1. *Let $\alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G$, then $\Theta_G(\alpha) \in \mathbb{Z}[G] \Longleftrightarrow \alpha \in \mathcal{A}_G$. So Θ_G induces a homomorphism $\Theta_G : \mathcal{A}_G \longrightarrow \mathbb{Z}[G]$.*

Proof. Given $\alpha := \sum a_\chi \chi \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G$, we have

$$\det(\alpha)(s) = \prod_{\chi \text{ of deg } 1} \chi(s)^{a_\chi} \cdot \prod_{\chi \text{ of deg } >1} \det\left(T_\chi(s)\right)^{a_\chi},$$

with T_χ a representation associated to χ. We know that $\det\left(T_\chi(s)\right) = \prod_{i=1}^n \beta_i^{j_i}$, where β_i are the eigenvalues of $T_\chi(s)$.
In the meanwhile we have $\mathrm{res}^G_{\langle s \rangle} T_\chi = \sum_{i=1}^n j_i \chi_i$, where each χ_i is the irreducible character of $\langle s \rangle$ associated to the eigenvalue β_i ($\beta_i = \chi_i(s)$).
Thus

$$\det\left(T_\chi(s)\right) = e^{2\pi i \langle \mathrm{res}^G_{\langle s \rangle} \chi, s \rangle}$$

and, by bilinearity, we get $\det(\alpha)(s) = e^{2\pi i \langle \alpha, s \rangle}$; which gives

$$\Theta_G(\alpha) \in \mathbb{Z}[G] \Longleftrightarrow \langle \alpha, s \rangle \in \mathbb{Z}, \forall s \in G \Longleftrightarrow \det(\alpha)(s) = 1, \forall s \in G \Longleftrightarrow \alpha \in \mathcal{A}_G.$$

□

Up to now we have not considered the Ω-action. If we let Ω act trivially on G, as at the beginning of the chapter, it is easy to see that the Stickelberger map does not preserve Ω-action. In order to have such an invariant property we have to introduce a non-trivial Ω-action on G.

Definition. *Let m be the exponent of G and μ_m the group of m-th roots of unity. Restricting Ω to $\mathrm{Gal}\left(K\left(\mu_m\right)/K\right)$, we consider the map $\kappa : \Omega \longrightarrow (\mathbb{Z}/m\mathbb{Z})^{\times}$ defined via the formula $\zeta^{\omega} = \zeta^{\kappa(\omega)}$, for $\zeta \in \mu_m$.*
We denote by $G(-1)$ the group G with an Ω-action defined via the inverse of κ:

$$s^{\omega} := s^{\kappa^{-1}(\omega)}.$$

If we take a character χ of degree 1, we have $\chi(s) \in \mu_m$ and, since $\chi^{\omega}(s)$ equals $\chi\left(s\right)^{\omega}$, we get

$$\chi^{\omega}(s) = \chi\left(s\right)^{\omega} = \chi\left(s\right)^{\kappa(\omega)} = \chi(s^{\kappa(\omega)}).$$

By bilinearity, we deduce that, for all $\alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G$ and for all $s \in G$,

$$\langle \alpha^{\omega},\, s\rangle = \langle \alpha,\, s^{\kappa(\omega)}\rangle = \langle \alpha,\, s^{\omega^{-1}}\rangle. \tag{2.16}$$

Applying this to the Stickelberger map, we get

$$\Theta_G(\alpha^{\omega}) = \sum_{s\in G}\langle \alpha^{\omega},\, s\rangle\, s = \sum_{s\in G}\langle \alpha,\, s^{\omega^{-1}}\rangle\, s = \sum_{s\in G}\langle \alpha,\, s\rangle\, s^{\omega};$$

from which we deduce the following proposition.

Proposition 2.3.2. *The map $\Theta_G : \mathbb{Q}\otimes_{\mathbb{Z}} R_G \longrightarrow \mathbb{Q}[G(-1)]$ is an Ω-homomorphism, i.e.*

$$\Theta_G(\alpha^{\omega}) = \Theta_G\left(\alpha\right)^{\omega},$$

$\forall\, \alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G$ and $\omega \in \Omega$.

The pairing $\langle \chi,\, s\rangle$ just depends on the conjugacy class of $s \in G$ (it is the same for all the elements in the same conjugacy class) and hence $\Theta_G(\mathbb{Q} \otimes_{\mathbb{Z}} R_G) \subseteq Z(\mathbb{Q}[G])$, where $Z(\mathbb{Q}[G])$ is the center of the group algebra $\mathbb{Q}[G]$, with basis the conjugacy class sum of G. If we denote by $\bar{G}$ the set of conjugacy classes of G, then the action of Ω via κ^{-1} preserves conjugacy classes and it induces an Ω-action on $Z(\mathbb{Z}[G])$ and on $\mathbb{Z}[\bar{G}]$; we denote these Ω-modules by $Z(\mathbb{Z}[G(-1)])$ and $\mathbb{Z}[\bar{G}(-1)]$, respectively. There is a canonical Ω-module isomorphism i between $\mathbb{Z}[\bar{G}]$ and $Z(\mathbb{Z}[G])$, defined

by linearity as follows:

$$\begin{aligned} i\,:\,\mathbb{Z}[\bar{G}] &\longrightarrow Z(\mathbb{Z}[G]) \\ \bar{s} &\longmapsto i(\bar{s}) := \sum_{t\in\,\bar{s}} t. \end{aligned}$$

Moreover, defining the Stickelberger pairing on the set of conjugacy classes as

$$\langle \chi,\, \bar{s}\rangle := \langle \chi,\, s\rangle,$$

we denote by $\Theta_{\bar{G}}$ the map, defined by $\mathbb{Q}$-bilinearity as:

$$\begin{aligned} \Theta_{\bar{G}}\,:\,\mathbb{Q}\otimes_{\mathbb{Z}} R_G &\longrightarrow \mathbb{Q}[\bar{G}] \\ \chi &\longmapsto \sum_{\bar{s}\in\bar{G}} \langle \chi,\, \bar{s}\rangle \bar{s}. \end{aligned} \tag{2.17}$$

Clearly $i\Theta_{\bar{G}} = \Theta_G$ and $\Theta_{\bar{G}}(\chi) \in \mathbb{Z}[\bar{G}] \Longleftrightarrow \chi \in \mathcal{A}_G$.

Transposing the map $\Theta_{\bar{G}} : \mathcal{A}_G \longrightarrow \mathbb{Z}[\bar{G}(-1)]$, we get the Ω-equivariant homomorphism

$$\Theta^{\mathrm{t}}_{\bar{G}}\,:\,\mathrm{Hom}\left(\mathbb{Z}[\bar{G}(-1), (K^{\mathrm{c}})^{\times}\right) \longrightarrow \mathrm{Hom}\left(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}\right).$$

Hence, if we write

$$\begin{aligned} \left(K\bar{\Lambda}\right)^{\times} &:= \mathrm{Hom}_{\,\Omega}\left(\mathbb{Z}[\bar{G}(-1)], (K^{\mathrm{c}})^{\times}\right), \\ \bar{\Lambda}^{\times} &:= \mathrm{Hom}_{\,\Omega}\left(\mathbb{Z}[\bar{G}(-1)], (O_K^{\mathrm{c}})^{\times}\right); \end{aligned}$$

then $\Theta^{\mathrm{t}}_{\bar{G}}$ induces a homomorphism

$$\Theta^{\mathrm{t}}_{\bar{G}} : \left(K\bar{\Lambda}\right)^{\times} \longrightarrow \mathrm{Hom}_{\,\Omega}\left(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}\right).$$

For any place $\mathfrak{p}$ of K, we get a local analog just replacing K with $K_{\mathfrak{p}}$:

$$\Theta^{\mathrm{t}}_{\bar{G},\,\mathfrak{p}} : \left(K_{\mathfrak{p}}\bar{\Lambda}_{\mathfrak{p}}\right)^{\times} \longrightarrow \mathrm{Hom}_{\,\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, (K_{\mathfrak{p}}^{\mathrm{c}})^{\times}\right).$$

Moreover $\Theta^{\mathrm{t}}_{\bar{G},\,\mathfrak{p}}(\bar{\Lambda}_{\mathfrak{p}}^{\times}) \subseteq \mathrm{Hom}_{\,\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, O_{K,\,\mathfrak{p}}^{\mathrm{c}\,\times}\right)$. Be careful that at the infinite places, since we set $O_{K,\,\mathfrak{p}} = K_{\mathfrak{p}}$, we have $\bar{\Lambda}_{\mathfrak{p}} = K_{\mathfrak{p}}\bar{\Lambda}_{\mathfrak{p}}$.

Hence, if we define the idèle group $J(K\bar{\Lambda})$ as the restricted product of $(K\bar{\Lambda})^{\times}$ with respect to $\bar{\Lambda}^{\times}$, the homomorphisms $\Theta^{\mathrm{t}}_{\bar{G},\,\mathfrak{p}}$ combine to give an idelic transpose

Stickelberger homomorphism:

$$\Theta^{\mathrm{t}}_{\bar{G}} : J(K\bar{\Lambda}) \longrightarrow \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J\left(K^{\mathrm{c}}\right)\right). \tag{2.18}$$

Remark 2.3.3. *Note that $J(K\bar{\Lambda})$ can also be defined as*

$$\mathrm{Hom}_{\Omega}\left(\mathbb{Z}[\bar{G}(-1)], J(K^{\mathrm{c}})\right);$$

for details see [28, Remark 6.22].

Remark 2.3.4. *Note that if G is abelian, we can remove the "bar" from all our notation, since $G = \bar{G}$. In the sequel, if G is abelian, we will adopt this simplification in the notation.*

2.4 Resolvends of local tame extensions

In this section we describe the decomposition of resolvends of normal integral basis generators of local tame extensions which will be the main ingredient of the proof of Theorem A. For this section $\mathfrak{p}$ is a finite place of K.

Notation. For any finite place $\mathfrak{p}$ of K we consider a uniformizer $\pi_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$ and we denote by $q_{\mathfrak{p}}$ the cardinality of the residue field.
Moreover we choose a compatible set of roots of unity $\{\zeta_n\}$ and roots of the uniformizer $\{\pi_{\mathfrak{p}}^{1/n}\}$. The term "compatible" means that the following relations hold: $\zeta_{nr}^n = \zeta_r$ and $\left(\pi_{\mathfrak{p}}^{1/nr}\right)^n = \pi_{\mathfrak{p}}^{1/r}$. Clearly $\pi_{\mathfrak{p}}^{r/n} := \left(\pi_{\mathfrak{p}}^{1/n}\right)^r$.

We denote by $K_{\mathfrak{p}}^{\mathrm{nr}}$ the maximal unramified extension of $K_{\mathfrak{p}}$, it is well known that

$$K_{\mathfrak{p}}^{\mathrm{nr}} = K_{\mathfrak{p}}\left(\{\zeta_n : (n, q_{\mathfrak{p}}) = 1\}\right).$$

Analogously we write $K_{\mathfrak{p}}^{\mathrm{t}}$ for the maximal tamely ramified extension of $K_{\mathfrak{p}}$ and we know that

$$K_{\mathfrak{p}}^{\mathrm{t}} = K_{\mathfrak{p}}\left(\left\{\zeta_n,\, \pi_{\mathfrak{p}}^{1/n} : (n, q_{\mathfrak{p}}) = 1\right\}\right).$$

The Galois group $\Omega_{\mathfrak{p}}^{\mathrm{nr}} := \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{nr}}/K_{\mathfrak{p}})$ is a procyclic group generated by the Frobenius element $\phi_{\mathfrak{p}}$, defined by $\phi_{\mathfrak{p}}(\zeta_n) := \zeta_n^{q_{\mathfrak{p}}}$. This in turn determines a generator $\sigma_{\mathfrak{p}}$ of $\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{t}}/K_{\mathfrak{p}}^{\mathrm{nr}})$, defined as $\sigma_{\mathfrak{p}}(\pi_{\mathfrak{p}}^{1/n}) := \zeta_n \pi_{\mathfrak{p}}^{1/n}$. If we extend $\phi_{\mathfrak{p}}$ to $\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{t}}/K_{\mathfrak{p}})$ fixing $\pi_{\mathfrak{p}}^{1/n}$, one can see that $\Omega_{\mathfrak{p}}^{\mathrm{t}} := \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{t}}/K_{\mathfrak{p}})$ is the profinite group topologically generated by $\sigma_{\mathfrak{p}}$ and $\phi_{\mathfrak{p}}$, subject to the relation $\phi_{\mathfrak{p}} \cdot \sigma_{\mathfrak{p}} \cdot \phi_{\mathfrak{p}}^{-1} = \sigma_{\mathfrak{p}}^{q_{\mathfrak{p}}}$. The set of elements $\sigma_{\mathfrak{p}}^i \phi_{\mathfrak{p}}^j \in \Omega_{\mathfrak{p}}^{\mathrm{t}}$, with i and j natural numbers, forms a dense subgroup of $\Omega_{\mathfrak{p}}^{\mathrm{t}}$.

Thanks to this description, we clearly have the following bijection

$$\begin{array}{rcl} \mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{t}}, G) & \longleftrightarrow & \{(t,u) : t,u \in G \text{ and } t\cdot u\cdot t^{-1} = u^{q_{\mathfrak{p}}}\} \\ h_{\mathfrak{p}} & \longmapsto & (h_{\mathfrak{p}}(\phi_{\mathfrak{p}}), h_{\mathfrak{p}}(\sigma_{\mathfrak{p}}))\,. \end{array}$$

From now on, let $h_{\mathfrak{p}}$ be an element in $\mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{t}}, G)$. We denote by u the element $h_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ and by t the element $h_{\mathfrak{p}}(\phi_{\mathfrak{p}})$. We write e for the order of u and f for the order of t.
Note that if G is abelian then $e|(q_{\mathfrak{p}}-1)$. While in general, for any finite group, we have

$$(e, q_{\mathfrak{p}}) = 1,$$

since $t \in N_G(\langle u\rangle)$ (where $N_G(\langle u\rangle)$ is the normalizer of $\langle u\rangle$ in G) and hence $q_{\mathfrak{p}}$ belongs to $(\mathbb{Z}/e\mathbb{Z})^{\times}$.

Let $h_{\mathfrak{p}}^{\mathrm{nr}}$ and $h_{\mathfrak{p}}^{\mathrm{tr}}$ be two maps in $\mathrm{Map}\left(\Omega_{\mathfrak{p}}^{\mathrm{t}}, G\right)$, defined by:

$$h_{\mathfrak{p}}^{\mathrm{nr}}\left(\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}\right) := t^{j} \tag{2.19}$$

$$h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}\right) := u^{i}. \tag{2.20}$$

Clearly $h_{\mathfrak{p}} = h_{\mathfrak{p}}^{\mathrm{tr}}\cdot h_{\mathfrak{p}}^{\mathrm{nr}}$ and $h_{\mathfrak{p}}^{\mathrm{nr}} \in \mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G)$. Moreover, if we denote by G_{nr} the group G with a non-trivial $\Omega_{\mathfrak{p}}^{\mathrm{t}}$-group action defined as

$$s^{\omega} = h_{\mathfrak{p}}^{\mathrm{nr}}(\omega)\cdot s\cdot h_{\mathfrak{p}}^{\mathrm{nr}}(\omega)^{-1},$$

or better, considering $\omega = \sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}$, as

$$s^{\left(\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}\right)} = t^{j}\cdot s\cdot t^{-j};$$

we can prove the following lemma.

Lemma 2.4.1. *The map $h_{\mathfrak{p}}^{\mathrm{tr}} \in Z^1(\Omega_{\mathfrak{p}}^{\mathrm{t}}, G_{\mathrm{nr}})$, where $Z^1(\Omega_{\mathfrak{p}}^{\mathrm{t}}, G_{\mathrm{nr}})$ represents the set of 1-cocycles of $\Omega_{\mathfrak{p}}^{\mathrm{t}}$ in G_{nr}.*

Proof. Given two elements $\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}$ and $\sigma_{\mathfrak{p}}^{k}\phi_{\mathfrak{p}}^{l}$ in $\Omega_{\mathfrak{p}}^{\mathrm{t}}$, we need to show the equality

$$h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}\cdot\sigma_{\mathfrak{p}}^{k}\phi_{\mathfrak{p}}^{l}\right) = h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}\right)\cdot h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{k}\phi_{\mathfrak{p}}^{l}\right)^{\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}}.$$

Now, using the relation $\phi_{\mathfrak{p}}\cdot\sigma_{\mathfrak{p}}\cdot\phi_{\mathfrak{p}}^{-1} = \sigma_{\mathfrak{p}}^{q_{\mathfrak{p}}}$, it is easy to see that

$$h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}\cdot\sigma_{\mathfrak{p}}^{k}\phi_{\mathfrak{p}}^{l}\right) = h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{i+kq_{\mathfrak{p}}^{j}}\phi_{\mathfrak{p}}^{j+l}\right) = u^{i+kq_{\mathfrak{p}}^{j}}.$$

Moreover $h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}\right)=u^{i}$ and the equality

$$h_{\mathfrak{p}}^{\mathrm{tr}}\left(\sigma_{\mathfrak{p}}^{k}\phi_{\mathfrak{p}}^{l}\right)^{\sigma_{\mathfrak{p}}^{i}\phi_{\mathfrak{p}}^{j}}=t^{j}\cdot u^{k}\cdot t^{-j}=u^{kq_{\mathfrak{p}}^{j}}$$

concludes the proof. □

Let us denote by ${}^{h_{\mathfrak{p}}^{\mathrm{tr}}}G_{\mathrm{nr}}$ the $\Omega_{\mathfrak{p}}^{\mathrm{t}}$-set G with an $\Omega_{\mathfrak{p}}^{\mathrm{t}}$-action defined as

$$s^{\omega}=h_{\mathfrak{p}}^{\mathrm{tr}}(\omega)\cdot h_{\mathfrak{p}}^{\mathrm{nr}}(\omega)\cdot s\cdot h_{\mathfrak{p}}^{\mathrm{nr}}(\omega)^{-1},$$

the easy proof that this action respect the associativity is left to the reader and follows from the fact that $h_{\mathfrak{p}}^{\mathrm{tr}}\in Z^{1}(\Omega_{\mathfrak{p}}^{\mathrm{t}},G_{\mathrm{nr}})$. Pay attention to the fact that we look at ${}^{h_{\mathfrak{p}}^{\mathrm{tr}}}G_{\mathrm{nr}}$ as an $\Omega_{\mathfrak{p}}^{\mathrm{t}}$-set and not as an $\Omega_{\mathfrak{p}}^{\mathrm{t}}$-group.

Then we consider the (Hopf) $K_{\mathfrak{p}}$-algebra

$$(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}:=\mathrm{Map}_{\Omega_{\mathfrak{p}}^{\mathrm{t}}}\left({}^{h_{\mathfrak{p}}^{\mathrm{tr}}}G_{\mathrm{nr}},K_{\mathfrak{p}}^{\mathrm{c}}\right).$$

Here we need to make a clarification: the theory of resolvends that we have seen in the previous sections for G-Galois algebras over K (or $K_{\mathfrak{p}}$) can be generalized to the set of Hopf algebras, as fully done by N. Byott in his paper [7] (the author considered just the abelian case, but what we are going to use is valid in the non-abelian case too). In particular $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}$ is an example of those algebras that the author calls principal homogeneous spaces (p.h.s.) over the algebra $\mathrm{Map}_{\Omega_{\mathfrak{p}}^{t}}\left(G_{\mathrm{nr}},K_{\mathfrak{p}}^{\mathrm{c}}\right)$ (this corresponds to B in [7]). As explained in the cited work, $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}$ can be considered as a $(K_{\mathfrak{p}}^{\mathrm{c}}[G_{\mathrm{nr}}])^{\Omega_{\mathfrak{p}}^{\mathrm{t}}}$-module, where, given $\alpha=\sum_{s\in G_{\mathrm{nr}}}\alpha_{s}s\in(K_{\mathfrak{p}}^{\mathrm{c}}[G_{\mathrm{nr}}])^{\Omega_{\mathfrak{p}}^{\mathrm{t}}}$ and $a\in(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}$,

$$(\alpha\cdot a)(s'):=\sum_{s\in G_{\mathrm{nr}}}\alpha_{s}a(s'\cdot s).$$

The algebra $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}$, considered with such a structure, is free of rank 1 (this follows from the fact that $\mathrm{Map}(G_{\mathrm{nr}},K_{\mathfrak{p}}^{\mathrm{c}})$ is free of rank 1 over $K_{\mathfrak{p}}^{\mathrm{c}}[G_{\mathrm{nr}}]$), i.e. there exists $b\in(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}$ such that $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}=(K_{\mathfrak{p}}^{\mathrm{c}}[G_{\mathrm{nr}}])^{\Omega_{\mathfrak{p}}^{\mathrm{t}}}\cdot b$.

Now if we take its ring of integers $O_{(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}}=\mathrm{Map}_{\Omega_{\mathfrak{p}}^{\mathrm{t}}}\left({}^{h_{\mathfrak{p}}^{\mathrm{tr}}}G_{\mathrm{nr}},O_{K,\mathfrak{p}}^{\mathrm{c}}\right)$, we can consider the element $\beta_{u}:=\dfrac{1}{e}\sum_{i=0}^{e-1}\pi_{\mathfrak{p}}^{i/e}\in O_{K,\mathfrak{p}}^{\mathrm{c}}$ and the map $\varphi_{\mathfrak{p},u}\in\mathrm{Map}(G,O_{K,\mathfrak{p}}^{\mathrm{c}})$ defined as

$$\varphi_{\mathfrak{p},u}(s)=\begin{cases}\sigma_{\mathfrak{p}}^{i}(\beta_{u}) & \text{if } s=u^{i},\\ 0 & \text{otherwise.}\end{cases}\tag{2.21}$$

We can now prove the following results.

Proposition 2.4.2. *(a) The map $\varphi_{\mathfrak{p},u}$ belongs to $O_{(K_\mathfrak{p})_{h_\mathfrak{p}^{\mathrm{tr}}}}$.*

(b) The map $\varphi_{\mathfrak{p},u}$ generates $O_{(K_\mathfrak{p})_{h_\mathfrak{p}^{\mathrm{tr}}}}$ over $(O^{\mathrm{c}}_{K,\mathfrak{p}}[G_{\mathrm{nr}}])^{\Omega^{\mathrm{t}}_\mathfrak{p}}$, i.e.

$$O_{(K_\mathfrak{p})_{h_\mathfrak{p}^{\mathrm{tr}}}} = (O^{\mathrm{c}}_{K,\mathfrak{p}}[G_{\mathrm{nr}}])^{\Omega^{\mathrm{t}}_\mathfrak{p}}.\varphi_{\mathfrak{p},u}.$$

(c) Given $a \in (K_\mathfrak{p})_{h_\mathfrak{p}^{\mathrm{tr}}}$, for any $\omega \in \Omega^{\mathrm{t}}_\mathfrak{p}$,

$$r_G(a)^\omega = h^{\mathrm{nr}}_\mathfrak{p}(\omega)^{-1} \cdot r_G(a) \cdot h_\mathfrak{p}(\omega).$$

Proof. *(a)* For any $\omega = \sigma_\mathfrak{p}^j \phi_\mathfrak{p}^k \in \Omega^{\mathrm{t}}_\mathfrak{p}$, we have

$$\begin{aligned}
\varphi_{\mathfrak{p},u}((u^i)^\omega) &= \varphi_{\mathfrak{p},u}(u^j \cdot t^k \cdot u^i \cdot t^{-k}) \\
&= \varphi_{\mathfrak{p},u}(u^{j+iq_\mathfrak{p}^k}) \\
&= \sigma_\mathfrak{p}^{j+iq_\mathfrak{p}^k}(\beta_u) \\
&= \sigma_\mathfrak{p}^{j+iq_\mathfrak{p}^k}\phi_\mathfrak{p}^k(\beta_u) \\
&= \sigma_\mathfrak{p}^j\phi_\mathfrak{p}^k\sigma_\mathfrak{p}^i(\beta_u) \\
&= \varphi_{\mathfrak{p},u}(u^i)^\omega,
\end{aligned}$$

where we frequently use the relations $t \cdot u \cdot t^{-1} = u^{q_\mathfrak{p}}$ and $\phi_\mathfrak{p} \cdot \sigma_\mathfrak{p} \cdot \phi_\mathfrak{p}^{-1} = \sigma_\mathfrak{p}^{q_\mathfrak{p}}$. If $s \notin \langle u \rangle$, then also s^ω, for $\omega \in \Omega^{\mathrm{t}}_\mathfrak{p}$, is not in $\langle u \rangle$, so clearly $\varphi_{\mathfrak{p},u}(s)^\omega = 0 = \varphi_{\mathfrak{p},u}(s^\omega)$.

(b) The proof of this point generalizes the analogous result in the abelian case contained in [28, page 281] and follows the proof of [7, Lemma 6.6].
Let us consider the cyclic group $\langle u \rangle$ inside ${}^{h_\mathfrak{p}^{\mathrm{tr}}}G_{\mathrm{nr}}$, then the group $\Omega^{\mathrm{t}}_\mathfrak{p}$ acts transitively on it. Now if we consider the algebra $L_u := \mathrm{Map}_{\Omega^t_\mathfrak{p}}\left(\langle u \rangle, K^{\mathrm{c}}_\mathfrak{p}\right)$, this, since the action of $\Omega^{\mathrm{t}}_\mathfrak{p}$ is transitive on $\langle u \rangle$, embeds in a subfield of $K^{\mathrm{t}}_\mathfrak{p}$ via the map which sends $b \in L_u$ to $b(1) \in K^{\mathrm{t}}_\mathfrak{p}$. Since (look at the action of $\Omega^{\mathrm{t}}_\mathfrak{p}$ on ${}^{h_\mathfrak{p}^{\mathrm{tr}}}G_{\mathrm{nr}}$)

$$\begin{aligned}
b(1)^{\sigma_\mathfrak{p}^i} &= b(u^i), \\
b(1)^{\phi_\mathfrak{p}^j} &= b(1),
\end{aligned}$$

we see that L_u coincides with the subfield of $K^{\mathrm{t}}_\mathfrak{p}$ given by the elements fixed by $\phi_\mathfrak{p}$ and $\sigma_\mathfrak{p}^e$, i.e. $K_\mathfrak{p}(\pi_\mathfrak{p}^{1/e})$. Its ring of integers is clearly $O_{K,\mathfrak{p}}[\pi_\mathfrak{p}^{1/e}]$.
Consider now $(O^{\mathrm{c}}_{K,\mathfrak{p}}[\langle u \rangle])^{\Omega^{\mathrm{t}}_\mathfrak{p}}$, where $\langle u \rangle$ is now seen in G_{nr}, and define $\alpha :=$

$\sum_{i=0}^{e-1} \zeta_e^{-ki} u^i$. Since $\sigma_\mathfrak{p}$ acts trivially on G_{nr} and

$$\alpha^{\phi_\mathfrak{p}} = \sum_{i=0}^{e-1} \zeta_e^{-kiq_\mathfrak{p}} u^{q_\mathfrak{p} i} = \sum_{i=0}^{e-1} \zeta_e^{-ki} u^i = \alpha,$$

using the fact that $(e, q_\mathfrak{p}) = 1$, we see that $\alpha \in (O^{\mathrm{c}}_{K,\mathfrak{p}}[\langle u \rangle])^{\Omega^{\mathrm{t}}_\mathfrak{p}}$. Moreover

$$\alpha \cdot \beta_u = \sum_{i=0}^{e-1} \zeta_e^{-ki} u^i \cdot \beta_u = \sum_{i=0}^{e-1} \sigma_\mathfrak{p}^i(\beta_u) \zeta_e^{-ki}$$

and this sum coincides with $\pi_\mathfrak{p}^{k/e}$ (cfr. [28, page 281]). Note that β_u coincides with $\varphi_{\mathfrak{p},u}(1)$.
Hence we have proved that $(O^{\mathrm{c}}_{K,\mathfrak{p}}[\langle u \rangle])^{\Omega^{\mathrm{t}}_\mathfrak{p}} \cdot \beta_u = O_{K,\mathfrak{p}}[\pi_\mathfrak{p}^{1/e}]$, which in turn proves that $(O^{\mathrm{c}}_{K,\mathfrak{p}}[G_{\mathrm{nr}}])^{\Omega^{\mathrm{t}}_\mathfrak{p}} \cdot \varphi_{\mathfrak{p},u} = O_{(K_\mathfrak{p})_{h^{\mathrm{tr}}_\mathfrak{p}}}$.

(c) Remember that $r_G(a) \in K^{\mathrm{c}}_\mathfrak{p}[G]$ and $\Omega^{\mathrm{t}}_\mathfrak{p}$ acts trivially on G. Then we have

$$\begin{aligned}
r_G(a)^\omega &= \sum_{s \in G} a(s^\omega) s^{-1} \\
&= \sum_{s \in G} a(h^{\mathrm{tr}}_\mathfrak{p}(\omega) \cdot h^{\mathrm{nr}}_\mathfrak{p}(\omega) \cdot s \cdot h^{\mathrm{nr}}_\mathfrak{p}(\omega)^{-1}) s^{-1} \\
&= \sum_{\tau \in G} a(\tau) \cdot h^{\mathrm{nr}}_\mathfrak{p}(\omega)^{-1} \cdot \tau^{-1} \cdot h^{\mathrm{tr}}_\mathfrak{p}(\omega) \cdot h^{\mathrm{nr}}_\mathfrak{p}(\omega) \\
&= h^{\mathrm{nr}}_\mathfrak{p}(\omega)^{-1} \cdot r_G(a) \cdot h^{\mathrm{tr}}_\mathfrak{p}(\omega) \cdot h^{\mathrm{nr}}_\mathfrak{p}(\omega) \\
&= h^{\mathrm{nr}}_\mathfrak{p}(\omega)^{-1} \cdot r_G(a) \cdot h_\mathfrak{p}(\omega).
\end{aligned}$$

□

Given a_{nr} a normal integral basis generator of $(K_\mathfrak{p})_{h^{\mathrm{nr}}_\mathfrak{p}} := \mathrm{Map}_{\Omega_\mathfrak{p}}\left({}^{h^{\mathrm{nr}}_\mathfrak{p}}G, K^{\mathrm{c}}_\mathfrak{p}\right)$ and a_{tr} an element in $(K_\mathfrak{p})_{h^{\mathrm{tr}}_\mathfrak{p}}$ such that $O_{(K_\mathfrak{p})_{h^{\mathrm{tr}}_\mathfrak{p}}} = (O^{\mathrm{c}}_{K,\mathfrak{p}}[G_{\mathrm{nr}}])^{\Omega^{\mathrm{t}}_\mathfrak{p}} \cdot a_{\mathrm{tr}}$, we can find an element $a \in (K_\mathfrak{p})_{h_\mathfrak{p}}$ such that

$$r_G(a) = r_G(a_{\mathrm{nr}}) \cdot r_G(a_{\mathrm{tr}}) \in K^{\mathrm{c}}_\mathfrak{p}[G]^\times.$$

The fact that we can find an element $a \in \mathrm{Map}(G, K^{\mathrm{c}}_\mathfrak{p})$ such that its resolvend is equal to the product follows from the fact that the resolved map is an isomorphism.

To prove that a is actually in $(K_\mathfrak{p})_{h_\mathfrak{p}}$ we use (P2), noting that, for any $\omega \in \Omega^{\mathrm{t}}_\mathfrak{p}$,

$$\begin{aligned} r_G(a)^\omega &= r_G(a_{\mathrm{nr}})^\omega \cdot r_G(a_{\mathrm{tr}})^\omega \\ &= r_G(a_{\mathrm{nr}}) \cdot h^{\mathrm{nr}}_\mathfrak{p}(\omega) \cdot h^{\mathrm{nr}}_\mathfrak{p}(\omega)^{-1} \cdot r_G(a_{\mathrm{tr}}) \cdot h_\mathfrak{p}(\omega) \\ &= r_G(a) \cdot h_\mathfrak{p}(\omega), \end{aligned}$$

where on the second line we used point *(c)* of the previous proposition. The fact that $r_G(a) \in K^{\mathrm{c}}_\mathfrak{p}[G]^\times$ proves that a is in particular a normal basis generator of $(K_\mathfrak{p})_{h_\mathfrak{p}}/K_\mathfrak{p}$.
In fact McCulloh proved something more: the element a just found is a normal integral basis generator of $(K_\mathfrak{p})_{h_\mathfrak{p}}/K_\mathfrak{p}$.

Proposition 2.4.3. *Let a_{nr} and a_{tr} be as above. The element $a \in (K_\mathfrak{p})_{h_\mathfrak{p}}$ defined by*

$$r_G(a) = r_G(a_{\mathrm{nr}}) \cdot r_G(a_{\mathrm{tr}})$$

is a normal integral basis generator of $(K_\mathfrak{p})_{h_\mathfrak{p}}/K_\mathfrak{p}$.

Proof. The proof is essentially the same of the one given in the abelian case in [28, Theorem 5.6, page 283]. Since a_{nr} and a_{tr} are normal integral basis generators it is clear that their resolvends have coefficients in $O^{\mathrm{c}}_{K,\mathfrak{p}}$, thus we have $O_{K,\mathfrak{p}}[G] \cdot a \subseteq O_{(K_\mathfrak{p})_{h_\mathfrak{p}}}$. The equality follows, as in the abelian proof, comparing the discriminants of $O_{K,\mathfrak{p}}[G] \cdot a$ and of $O_{(K_\mathfrak{p})_{h_\mathfrak{p}}}$. □

For any finite place $\mathfrak{p}$, let us define

$$\mathcal{C}_{q_\mathfrak{p}} := \{s \in G |\, s^{q_\mathfrak{p}} \in \bar{s}\}.$$

Given $h_\mathfrak{p} \in \mathrm{Hom}(\Omega^{\mathrm{t}}_\mathfrak{p}, G)$, it follows, from the relation $\phi_\mathfrak{p} \cdot \sigma_\mathfrak{p} \cdot \phi_\mathfrak{p}^{-1} = \sigma_\mathfrak{p}^{q_\mathfrak{p}}$, that the element $h_\mathfrak{p}(\sigma_\mathfrak{p})$ belongs to $\mathcal{C}_{q_\mathfrak{p}}$.

Then for any $s \in \mathcal{C}_{q_\mathfrak{p}}$, let us define the map $f_{\mathfrak{p},s} \in \mathrm{Map}_{\Omega_\mathfrak{p}}\left(\bar{G}(-1), (K^{\mathrm{c}}_\mathfrak{p})^\times\right)$ as

$$f_{\mathfrak{p},s}(\bar{t}) = \begin{cases} \pi_\mathfrak{p} & \text{if } \bar{t} = \bar{s} \neq 1, \\ 1 & \text{otherwise.} \end{cases} \tag{2.22}$$

Since $s \in \mathcal{C}_{q_\mathfrak{p}}$, the group $\Omega_\mathfrak{p}$ fixes $\bar{s}$ considered in $\bar{G}(-1)$ and thus we see the $\Omega_\mathfrak{p}$-equivariance of $f_{\mathfrak{p},s}$.

Moreover let us define $F_\mathfrak{p} \subseteq (K_\mathfrak{p}\bar{\Lambda}_\mathfrak{p})^\times$ as the set $\{f_{\mathfrak{p},s}\}_{s \in \mathcal{C}_{q_\mathfrak{p}}}$. These combine to define $F \subseteq J(K\bar{\Lambda})$ as the set of idèles $f \in J(K\bar{\Lambda})$ such that $f_\mathfrak{p} \in F_\mathfrak{p}$ for all

finite $\mathfrak{p}$. We immediately see that, by the definition of $J(K\bar{\Lambda})$, if $f \in F$ then $f_{\mathfrak{p}} = 1$ a.e.. The set $F_{\mathfrak{p}}$ can be considered embedded in F via the natural map $(K_{\mathfrak{p}}\bar{\Lambda}_{\mathfrak{p}})^{\times} \longrightarrow J(K\bar{\Lambda})$ and the non-trivial elements of $F_{\mathfrak{p}}$ once considered in F are called prime F-elements over $\mathfrak{p}$.

We choose T a set of representatives of the orbits of $\bar{G}(-1)$ under the Ω-action and, for any $\bar{t} \in T$, denote by $K(t)$ the field extension over K given by the fixed elements in K^{c} under the stabilizer of $\bar{t}$. Then we have the following Wedderburn decomposition:

$$K\bar{\Lambda} \cong \prod_{\bar{t}\in T} K(t),$$

where, for every $t \in T$, the projection $K\bar{\Lambda} \longrightarrow K(t)$ is given by evaluation of functions in $K\bar{\Lambda}$ at t. For any prime $\mathfrak{p}$ of K, let us denote by $K(t)_{\mathfrak{p}}$ the tensor product $K_{\mathfrak{p}} \otimes_K K(t)$, then analogously, we also have

$$K_{\mathfrak{p}}\bar{\Lambda}_{\mathfrak{p}} \cong \prod_{\bar{t}\in T} K(t)_{\mathfrak{p}},$$

where now, pay attention that every $K(t)_{\mathfrak{p}}$ is not a field but a product of fields. Moreover, if $J(K(t))$ denotes the restricted direct product of $K(t)_{\mathfrak{p}}^{\times}$ with respect to $O_{K(t),\mathfrak{p}}^{\times}$ (where $O_{K(t),\mathfrak{p}} := O_{K,\mathfrak{p}} \otimes_{O_K} O_{K(t)}$), one can prove that

$$J(K\bar{\Lambda}) \cong \prod_{\bar{t}\in T} J(K(t)). \tag{2.23}$$

If $s \in \mathcal{C}_{q_{\mathfrak{p}}}$, we deduce that $(q_{\mathfrak{p}}, |s|) = 1$ and that $\bar{s}$ is fixed by $\Omega_{\mathfrak{p}}$ (and hence $K(s)_{\mathfrak{p}} = K_{\mathfrak{p}}$). Thus (cf. [28, page 288]), we see that the prime F-elements over $\mathfrak{p}$ coincide with the invertible prime ideals $\mathfrak{P} = (\mathfrak{P}_{\bar{t}})_{\bar{t}\in T}$ of Λ, with $\mathfrak{P}_{\bar{s}}$ a prime of degree one over $\mathfrak{p}$ in $K(s)$, for some $\bar{s} \neq 1$ with $v_{\mathfrak{p}}(|s|) = 0$ (where $v_{\mathfrak{p}}$ denotes the valuation associated to $\mathfrak{p}$), and $\mathfrak{P}_{\bar{t}} = O_{K(t)}$, $\forall\, \bar{t} \neq \bar{s}$.

By an easy computation, for any $s \in \mathcal{C}_{q_{\mathfrak{p}}}$ and $\alpha \in \mathcal{A}_G$, we have:

$$\begin{aligned}
\Theta^{\mathrm{t}}_{\bar{G}}(f_{\mathfrak{p},s})(\alpha) &= f_{\mathfrak{p},s}(\Theta_{\bar{G}}(\alpha)) \\
&= f_{\mathfrak{p},s}\left(\sum_{\bar{t}\in\bar{G}} \langle\alpha,\bar{t}\rangle\bar{t}\right) \\
&= \pi_{\mathfrak{p}}^{\langle\alpha,\bar{s}\rangle} \\
&= \pi_{\mathfrak{p}}^{\langle\alpha,s\rangle}.
\end{aligned}$$

In the meanwhile we have the following result.

Proposition 2.4.4. *Let us consider $\varphi_{\mathfrak{p},u}$ as defined in (2.21). For any $\alpha \in \mathcal{A}_G$,*

$$\widetilde{\mathrm{Det}}(\mathrm{rag}(r_G(\varphi_{\mathfrak{p},u})))(\alpha) = \pi_{\mathfrak{p}}^{\langle \alpha, u\rangle}.$$

Proof. Let $\chi \in \mathrm{Irr}(G)$, assume that $\mathrm{res}^G_{\langle u\rangle}(\chi) = \sum_{\psi \in \widehat{\langle u\rangle}} a_\psi \psi$. Then

$$\begin{aligned}\mathrm{Det}(r_G(\varphi_{\mathfrak{p},u}))(\chi) &= \det\left(\sum_{i=0}^{e-1} \sigma_{\mathfrak{p}}^i(\beta_u) T_\chi(u^{-1})\right) \\ &= \prod_{\psi \in \widehat{\langle u\rangle}} \left(\sum_{i=0}^{e-1} \sigma_{\mathfrak{p}}^i(\beta_u)\psi(u^{-1})\right)^{a_\psi}.\end{aligned}$$

Since, as in [28, page 282], we have the relation $\sum_{i=0}^{e-1} \sigma_{\mathfrak{p}}^i(\beta_u)\psi(u^{-1}) = \pi_{\mathfrak{p}}^{\langle \psi, u\rangle}$, we get

$$\prod_{\psi \in \widehat{\langle u\rangle}} \left(\sum_{i=0}^{e-1} \sigma_{\mathfrak{p}}^i(\beta_u)\psi(u^{-1})\right)^{a_\psi} = \pi_{\mathfrak{p}}^{\langle \sum_{\psi \in \langle u\rangle} a_\psi \psi, u\rangle} = \pi_{\mathfrak{p}}^{\langle \chi, u\rangle}.$$

So by linearity, for any $\alpha \in \mathcal{A}_G$,

$$\widetilde{\mathrm{Det}}(\mathrm{rag}(r_G(\varphi_{\mathfrak{p},u})))(\alpha) = \mathrm{rag}'(\mathrm{Det}(r_G(\varphi_{\mathfrak{p},u})))(\alpha) = \mathrm{Det}(r_G(\varphi_{\mathfrak{p},u}))(\alpha) = \pi_{\mathfrak{p}}^{\langle \alpha, u\rangle}.$$

□

Corollary 2.4.5. $\widetilde{\mathrm{Det}}(\mathrm{rag}(r_G(\varphi_{\mathfrak{p},u}))) = \Theta^{\mathrm{t}}_{\bar{G}}(f_{\mathfrak{p},u})$.

Proof. Clear. □

Remark 2.4.6. $\widetilde{\mathrm{Det}}(\mathrm{rag}(r_G(\varphi_{\mathfrak{p},u})))$ *just depends on the conjugacy class of u, since it is easy to check that $r_G(\varphi_{\mathfrak{p},s^{-1}us}) = s^{-1} r_G(\varphi_{\mathfrak{p},u}) s$.*

From now on, let us take $a_{\mathrm{tr}} = \varphi_{\mathfrak{p},u}$.

Proposition 2.4.7. *Let $h_{\mathfrak{p}} \in \mathrm{Hom}_{\Omega}\left(\Omega^{\mathrm{t}}_{\mathfrak{p}}, G\right)$. If $a'_{\mathfrak{p}}$ is a NIBG of $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}}/K_{\mathfrak{p}}$, then*

$$\widetilde{\mathrm{Det}}(\mathrm{rag}(r_G(a'_{\mathfrak{p}}))) = \Theta^{\mathrm{t}}_{\bar{G}}(f_{\mathfrak{p},u}) \cdot w_{\mathfrak{p}},$$

where $u = h_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ and $w_{\mathfrak{p}} \in \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$.

Proof. Given $a'_{\mathfrak{p}}$ a NIBG of $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}}/K_{\mathfrak{p}}$, if we consider $a_{\mathfrak{p}}$ the NIBG defined, as in Proposition 2.4.3 (considering $a_{\mathrm{tr}} = \varphi_{\mathfrak{p},u}$), by the relation $r_G(a_{\mathfrak{p}}) = r_G(a_{\mathrm{nr}}) \cdot r_G(\varphi_{\mathfrak{p},u})$, then there exists an element $d_{\mathfrak{p}} \in O_{K,\mathfrak{p}}[G]^\times$, such that $a'_{\mathfrak{p}} = d_{\mathfrak{p}} \cdot a_{\mathfrak{p}}$. Thus, since $\widetilde{\mathrm{Det}}(\mathrm{rag}(O_{K,\mathfrak{p}}[G]^\times)) \subseteq \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$, using (2.6) and Corollary 2.4.5, we conclude. □

2.5 Proof of Theorem A

We can now define the Stickelberger subgroup $\mathrm{St}(O_K[G])$. Thanks to the definitions given in the previous sections, we have the following group homomorphisms

$$\mathrm{Cl}(O_K[G]) \xrightarrow{\mathrm{Rag}} \mathrm{MCl}(O_K[G]) \xleftarrow{\Theta^{\mathrm{t}}_{\bar{G}}} J(K\bar{\Lambda}),$$

where the map on the right is the natural map given by the composition of $\Theta^{\mathrm{t}}_{\bar{G}} : J(K\bar{\Lambda}) \to \mathrm{Hom}_{\Omega}(\mathcal{A}_G, J(K^{\mathrm{c}}))$ with the quotient map $\mathrm{Hom}_{\Omega}(\mathcal{A}_G, J(K^{\mathrm{c}})) \to \mathrm{MCl}(O_K[G])$ (and we will denote it again by $\Theta^{\mathrm{t}}_{\bar{G}}$).

Definition 2.5.1. *The Stickelberger subgroup* $\mathrm{St}(O_K[G])$ *is defined as*

$$\mathrm{St}(O_K[G]) := \mathrm{Rag}^{-1}(\mathrm{Im}(\Theta^{\mathrm{t}}_{\bar{G}})).$$

Thanks to the previous section, we can now give a proof of Theorem A.

Theorem A. *Given a number field* K *and a finite group* G*,*

$$R_A(O_K[G]) \subseteq \mathrm{St}(O_K[G]).$$

Proof. Let us consider K_h a G-Galois K-algebra tamely ramified, where $h \in \mathrm{Hom}(\Omega^{\mathrm{t}}, G)$. Then as in Propostion 1.6.12, we choose a normal basis generator b and, for any finite place $\mathfrak{p}$, a local normal integral basis generator $a_{\mathfrak{p}}$. Then we know, by Remark 2.1.7, that the class $[O_{K_h}]$ is represented by the idèle $c = (c_{\mathfrak{p}})_{\mathfrak{p}} \in J(K[G])$ defined componentwise by the relation $\mathrm{rag}(r_G(a_{\mathfrak{p}})) = \mathrm{rag}(c_{\mathfrak{p}}) \cdot \mathrm{rag}(r_G(b))$ (where $c_{\mathfrak{p}} = 1$ at the infinite primes).
Applying now the map $\widetilde{\mathrm{Det}}$, by (2.1) and Proposition 2.4.7, for any finite prime $\mathfrak{p}$ we get

$$\widetilde{\mathrm{Det}}(\mathrm{rag})(c_{\mathfrak{p}}) = g^{-1} \cdot \Theta^{\mathrm{t}}_{\bar{G}}(f_{\mathfrak{p},u}) \cdot w_{\mathfrak{p}},$$

with $g = \widetilde{\mathrm{Det}}(\mathrm{rag}(r_G(b))) \in \mathrm{Hom}_{\Omega}(\mathcal{A}_G, (K^{\mathrm{c}})^{\times})$ (note that g does not depend on $\mathfrak{p}$), $w_{\mathfrak{p}} \in \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$ and $f_{\mathfrak{p},u} \in \mathrm{Map}_{\Omega_{\mathfrak{p}}}\left(\bar{G}(-1), (K^{\mathrm{c}}_{\mathfrak{p}})^{\times}\right)$ defined as in (2.22), with $u = h_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$. Note that since K_h/K has to be unramified a.e., $f_{\mathfrak{p},u}$ will be equal to 1 a.e..
If we define $f := (f_{\mathfrak{p},u})_{\mathfrak{p}} \in J(K\bar{\Lambda})$ (with $f_{\mathfrak{p},u} = 1$ at the infinite primes) and $w := \prod_{\mathfrak{p}} w_{\mathfrak{p}} \in \mathcal{U}(O_K[G])$ (with $w_{\mathfrak{p}} = g_{\mathfrak{p}}$ at the infinite primes), we finally get

$$\widetilde{\mathrm{Det}}(\mathrm{rag})(c) = g^{-1} \cdot \Theta^{\mathrm{t}}_{\bar{G}}(f) \cdot w,$$

which concludes the proof. □

2.6 The abelian equality

From now on the group G will be assumed to be abelian.

In this last part of the chapter we will explain the main ideas which led McCulloh to prove the inclusion $\mathrm{St}(O_K[G]) \subseteq R_A(O_K[G])$ in the abelian case and hence Theorem B.

When G is abelian, the main simplifications, with respect to the previous sections, are the following:

- ⋆ The maps Det and $\widetilde{\mathrm{Det}}$ in the diagrams of Proposition 2.2.4 and Proposition 2.2.5 are isomorphisms (Remark 2.2.10). So we will avoid in the notation the use of Det and we have

$$\begin{aligned} K[G]^\times &\cong \mathrm{Hom}_\Omega\left(R_G, (K^c)^\times\right), \\ \mathcal{H}(K[G]) &\cong \mathrm{Hom}_\Omega\left(\mathcal{A}_G, (K^c)^\times\right), \\ \mathcal{H}(O_{K,\mathfrak{p}}[G]) &\subseteq \mathrm{Hom}_{\Omega_\mathfrak{p}}\left(\mathcal{A}_G, (O^c_{K,\mathfrak{p}})^\times\right). \end{aligned}$$

- ⋆ Any irreducible character of G is of dimension 1.
- ⋆ The set of conjugacy classes $\bar{G}$ coincides with G, so in particular $J(K\Lambda) = J(K\bar{\Lambda})$.
- ⋆ In Section 2.4, the set $\mathcal{C}_{q_\mathfrak{p}}$ becomes the set of elements in G of order dividing $q_\mathfrak{p} - 1$.

The proof of Proposition 2.4.7 becomes easier in the abelian situation, in particular we do not need to use the notion of Hopf-algebras, thanks to the fact that $h^{\mathrm{tr}}_\mathfrak{p} \in \mathrm{Hom}\left(\Omega^{\mathrm{t}}_\mathfrak{p}, G\right)$ in this case. Moreover, we also have a reverse statement of that proposition.

Proposition 2.6.1. *Given an element $s \in G$ of order dividing $q_\mathfrak{p} - 1$ and an element $w_\mathfrak{p} \in \mathcal{H}(O_{K,\mathfrak{p}}[G])$, there exists an $h_\mathfrak{p} \in \mathrm{Hom}\left(\Omega^{\mathrm{t}}_\mathfrak{p}, G\right)$, such that $h_\mathfrak{p}(\sigma_\mathfrak{p})$ equals s and $(K_\mathfrak{p})_{h_\mathfrak{p}}/K_\mathfrak{p}$ has a NIBG $a_\mathfrak{p}$ such that* $\mathrm{rag}(r_G(a_\mathfrak{p})) = \Theta^{\mathrm{t}}_{\bar{G}}(f_{\mathfrak{p},s}) \cdot w_\mathfrak{p}$.

Proof. ([28, Theorem 5.6]) The general idea is that for any element $s \in G$ of order dividing $q_{\mathfrak{p}} - 1$ we can always find a totally ramified extension $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}^{\mathrm{tr}}}/K_{\mathfrak{p}}$ such that $h_{\mathfrak{p}}^{\mathrm{tr}}(\sigma_{\mathfrak{p}})$ equals s and $h_{\mathfrak{p}}^{\mathrm{tr}}(\phi_{\mathfrak{p}}) = 1$. In the meanwhile, by (2.6), we can find an unramified $h_{\mathfrak{p}}^{\mathrm{nr}} \in \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G\right)$ with a NIBG $a_{\mathfrak{p}}^{\mathrm{nr}}$ such that $\mathrm{rag}(r_G(a_{\mathfrak{p}}^{\mathrm{nr}})) = w_{\mathfrak{p}}$. A homomorphism $h_{\mathfrak{p}}$ defined as $h_{\mathfrak{p}} = h_{\mathfrak{p}}^{\mathrm{tr}} \cdot h_{\mathfrak{p}}^{\mathrm{nr}}$ will give the extension required. □

The following proposition will be the main ingredient in the proof of Theorem B.

Proposition 2.6.2. *Let K_h/K be a G-Galois K-algebra and take b a normal basis generator. Then K_h/K is tamely ramified if and only if there are $c \in J(K[G])$, $f \in F$ and $w \in \mathcal{U}(O_K[G])$, such that*

$$\mathrm{rag}(c) = \mathrm{rag}(r_G(b))^{-1} \cdot \Theta_G^{\mathrm{t}}(f) \cdot w. \tag{2.24}$$

Moreover c is a representative of the class $[O_{K_h}]$ and f is uniquely determined by the relation $f_{\mathfrak{p}} = f_{\mathfrak{p},s}$ for each finite $\mathfrak{p}$, with $s = h_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$. In particular h is unramified at $\mathfrak{p}$ if and only if $f_{\mathfrak{p}} = 1$ and h is unramified if and only if $f = 1$.

Proof. See [28, page 286]. The main property which allows to prove this result in the abelian case is that, when G is abelian, $\mathcal{H}(K_{\mathfrak{p}}[G]) \cong \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, \left(K_{\mathfrak{p}}^{\mathrm{c}}\right)^{\times}\right)$, for any place $\mathfrak{p}$. □

This would already be sufficient to give the proof of Theorem B, restricting the Stickelberger map from $\mathrm{St}(O_K[G])$ to Θ_G^t to F. But note that F is not a group and so this would not prove that the set of realizable classes, for an abelian group, forms a subgroup of $\mathrm{Cl}(O_K[G])$. Hence in order to give a proof of Theorem B, we need to show that $\Theta_G^{\mathrm{t}}(F) = \Theta_G^{\mathrm{t}}(J(K\Lambda))$ in $\mathrm{MCl}(O_K[G])$ and this will be obtained through the following approximation result.

Let $\mathfrak{m}$ be an integral ideal of O_K. For each finite place $\mathfrak{p}$ of K, we define

$$U'_{\mathfrak{m}}(\Lambda_{\mathfrak{p}}) := \{g_{\mathfrak{p}} \in (K_{\mathfrak{p}}\Lambda)^{\times} \,|\, g_{\mathfrak{p}}(s) \in (1 + \mathfrak{m}O_{K,\mathfrak{p}}^{\mathrm{c}}) \cap (O_{K,\mathfrak{p}}^{\mathrm{c}})^{\times}, \forall\, s \in G,\, s \neq 1\}.$$

The value at $s = 1$ can be arbitrary. If we write

$$U'_{\mathfrak{m}}(\Lambda) := \left(\prod_{\mathfrak{p}} U'_{\mathfrak{m}}(\Lambda_{\mathfrak{p}})\right) \cap J(K\Lambda),$$

then we define the modified ray class group mod $\mathfrak{m}$ of Λ as

$$\mathrm{Cl}'_{\mathfrak{m}}(\Lambda) := \frac{J(K\Lambda)}{(K\Lambda)^{\times} \cdot U'_{\mathfrak{m}}(\Lambda)}. \tag{2.25}$$

The following result holds.

Proposition 2.6.3. *Given an integral ideal $\mathfrak{m}$ of O_K, each class in $\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)$ contains infinitely many elements of F and they can be chosen with support disjoint from any preassigned finite set of finite primes. Moreover $f \in F$ can be chosen so that $f_t \neq 1$ for each $t \in T \setminus \{1\}$, where $f = \prod_{t\in T} f_t$, via the Wedderburn decomposition (2.23).*

Proof. ([28, Proposition 6.14]) This mainly follows considering

$$\mathrm{Cl}'_{\mathfrak{m}}(\Lambda) \cong \prod_{t\in T\setminus\{1\}} \mathrm{Cl}_{\mathfrak{m}}(O_{K(t)}),$$

where $\mathrm{Cl}_{\mathfrak{m}}(O_{K(t)})$ is the ray class group mod $\mathfrak{m}$ of $K(t)$. Indeed, as already seen below (2.23), the prime F-elements over $\mathfrak{p}$ coincide with the invertible prime ideals $\mathfrak{P} = (\mathfrak{P}_t)_{t\in T}$ of Λ, with $\mathfrak{P}_s$ a prime of degree one over $\mathfrak{p}$ in $K(s)$, for some $s \neq 1$ with $v_{\mathfrak{p}}(|s|) = 0$, and $\mathfrak{P}_t = O_{K(t)}$, $\forall\, t \neq s$. Thus, since, for every $t \in T \setminus \{1\}$, each ray class mod $\mathfrak{m}$ of $K(t)$ contains infinitely many prime ideals of degree one in $K(t)/K$, the proof follows. □

Corollary 2.6.4. $\Theta^{\mathrm{t}}_G(F) = \Theta^{\mathrm{t}}_G(J(K\Lambda))$ *in* $\mathrm{MCl}(O_K[G])$.

Proof. Let us consider $\mathfrak{m}$ an integral ideal divisible by a sufficiently high power of $|G|$ (following Proposition 2.2.9). Then, by the previous proposition, given an element $g \in J(K\Lambda)$ there exists an $f \in F$ (which can be chosen with support disjoint from any preassigned finite set of finite primes S), such that

$$g \equiv f \bmod((K\Lambda)^\times \cdot U'_{\mathfrak{m}}(\Lambda)).$$

Thus, applying the map Θ^{t}_G to this relation and using the fact that $\Theta^{\mathrm{t}}_G((K\Lambda)^\times) \subseteq \mathrm{Hom}_\Omega(\mathcal{A}_G, (K^{\mathrm{c}})^\times)$ and $\Theta^{\mathrm{t}}_G(U'_{\mathfrak{m}}(\Lambda)) \subseteq \mathcal{U}(O_K[G])$ (by Proposition 2.2.9), we get

$$\Theta^{\mathrm{t}}_G(g) \equiv \Theta^{\mathrm{t}}_G(f) \bmod \left(\mathrm{Hom}_\Omega\left(\mathcal{A}_G, (K^{\mathrm{c}})^\times\right) \cdot \mathcal{U}(O_K[G])\right).$$

□

Thanks to this, we can now (re)state and prove Theorem B.

Theorem B. *Given a number field K and a finite* ***abelian*** *group G,*

$$R_A(O_K[G]) = \mathrm{St}(O_K[G]).$$

Moreover $R_F(O_K[G]) = R_A(O_K[G])$ and any class can be obtained from a G-Galois field extension K_h/K unramified at a preassigned finite set of finite primes.

Proof. For a precise proof see [28, Theorem 6.17]. Nevertheless the general idea behind the proof should now be clear and the main ingredients are given by: the fact that in the abelian case Det is an isomorphism, Proposition 2.6.2 and Corollary 2.6.4.

The fact that any class can be actually obtained from a G-Galois field extension follows from:

- if K_h/K is not a field, then it contains an unramified non-trivial extension H/K,
- given $K_{h'}/K$ such that the associated (via 2.24) $f \in F$ is so that $f_t \neq 1$, for each $t \in T \setminus \{1\}$ (in terms of (2.23)), then every K-subalgebra of $K_{h'}$ is ramified ([28, page 290]).

Since for any class c we can find an algebra K_h/K realizing c such that the associated $f \in F$ is so that $f_t \neq 1$, for each $t \in T \setminus \{1\}$ (Proposition 2.6.3), we conclude that this has to be a field extension.

The statement on the ramification follows from the fact that the element $f \in F$ in a given modified ray class group can be chosen with support disjoint from any preassigned finite set of primes. □

Corollary 2.6.5. *Given a number field K and a finite **abelian** group G,*

$$R_{\mathrm{nr}}(O_K[G]) = \mathrm{Ker}(\mathrm{Rag}).$$

Proof. This follows from Proposition 2.2.11, Theorem B and the last statement of Proposition 2.6.2. □

Chapter 3

Computing the Stickelberger subgroup

This chapter contains the first new results of this dissertation.

In the first part we shall investigate the relations between the Stickelberger subgroup $\mathrm{St}(O_K[G])$ defined by McCulloh in his works and the subgroup $\mathrm{Cl}^\circ(O_K[G])$, that we have already met in the Introduction.

The second part of this chapter is devoted to the explicit computations of $\mathrm{St}(O_K[G])$, just using its definition, in some particular situations. Namely, we will consider $K = \mathbb{Q}$ and we will develop the cases $G = C_p$ and $G = D_p$, where C_p is a cyclic group of prime order p and D_p the dihedral group of order $2p$, with $p \geq 3$.

3.1 $\mathrm{St}(O_K[G])$ and $\mathrm{Cl}^\circ(O_K[G])$

In this section G is a finite group, not necessarily abelian.

From Theorem A of the previous chapter, we know, that for any number field K and for any finite group G,

$$R_A(O_K[G]) \subseteq \mathrm{St}(O_K[G]),$$

where $\mathrm{St}(O_K[G])$ is a particular subgroup of $\mathrm{Cl}(O_K[G])$, defined in Definition 2.5.1, via a Stickelberger map (see (2.18)) and the map Rag (see (2.15)).

In the meanwhile, we recall that $\mathrm{Cl}^\circ(O_K[G])$ is defined as the kernel of the group homomorphism $\epsilon^\star : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_K)$, induced by the augmentation map $\epsilon : O_K[G] \longrightarrow O_K$ which sends $\sum_{s\in G} a_s s$ to $\sum_{s\in G} a_s$. McCulloh proved the following result.

Proposition 3.1.1. *For every number field K and finite group G,*

$$R_A(O_K[G]) \subseteq \mathrm{Cl}^\circ(O_K[G]).$$

Proof. The original proof is contained in [26] (see also [27]). The general idea is that given L/K a tame G-Galois K-algebra, then

$$\epsilon^\star([O_L]) = O_K \otimes_{O_K[G]} O_L \cong \frac{1}{|G|}\mathrm{Tr}_{L/K}(O_L),$$

where $\mathrm{Tr}_{L/K}$ is the trace map from L to K.
By definition of tame extensions the trace map is surjective, i.e. $\mathrm{Tr}_{L/K}(O_L) = O_K$, hence $\epsilon^\star([O_L])$ is trivial in $\mathrm{Cl}(O_K)$. □

Remark 3.1.2. *In terms of the Hom-description (§1.7.4), we have the following isomorphism*

$$\mathrm{Cl}^\circ(O_K[G]) \cong \frac{\mathrm{Hom}^\circ_\Omega\left(R_G, J(K^c)\right)}{\mathrm{Hom}^\circ_\Omega\left(R_G, (K^c)^\times\right)\cdot \mathrm{Det}^\circ\left(U\left(O_K[G]\right)\right)} \ .$$

The superscript " $\circ$ " means that we are considering the homomorphisms f such that $f(\chi_0) = 1$, where χ_0 is the trivial character of G (see [10]).

Considering the two inclusions just recalled, a natural question arises: what is the link between the two groups $\mathrm{St}(O_K[G])$ and $\mathrm{Cl}^\circ(O_K[G])$? Are they equal?

A first answer to these questions is given by the following result.

Proposition 3.1.3. *Given a number field K and a finite group G,*

$$\mathrm{St}(O_K[G]) \subseteq \mathrm{Cl}^\circ(O_K[G]).$$

Proof. Let us consider a class $c \in \mathrm{St}(O_K[G])$ represented in terms of the Hom-description by $f \in \mathrm{Hom}_\Omega\left(R_G, J(K^c)\right)$. In order to prove that $c \in \mathrm{Cl}^\circ(O_K[G])$, we need to show that $f(\chi_0) \in K^\times \cdot U(O_K)$ (see [10, Proposition 2.1]).
Since for any finite group G, the trivial character χ_0 belongs to $\mathcal{A}_G$, in order to get

$f(\chi_0)$ we can compute the value of $\mathrm{rag}'(f)(\chi_0)$. By the definition of $\mathrm{St}(O_K[G])$, we have

$$\mathrm{rag}'(f) \in \mathrm{Hom}_\Omega\left(\mathcal{A}_G, (K^c)^\times\right) \cdot \mathcal{U}(O_K[G]) \cdot \Theta^t_{\bar{G}}(J(K\bar{\Lambda})),$$

so we can split the computation on χ_0 to any of the three components on the right. Let us compute these values:

⋆ $\mathrm{Hom}_\Omega\left(\mathcal{A}_G, (K^c)^\times\right)$**:** If we take a homomorphism $g \in \mathrm{Hom}_\Omega\left(\mathcal{A}_G, (K^c)^\times\right)$, the fact that g is Ω-equivariant means that, for any $\omega \in \Omega$, we have

$$g\left(\chi\right)^\omega = g(\chi^\omega).$$

Thus when we consider the value $g(\chi_0)$, we have that, for any $\omega \in \Omega$,

$$g\left(\chi_0\right)^\omega = g(\chi_0^\omega) = g(\chi_0)$$

and hence $g(\chi_0) \in K^\times$, since it is fixed by Ω. So we have shown that every element in $\mathrm{Hom}_\Omega\left(\mathcal{A}_G, (K^c)^\times\right)$ evaluated at χ_0 gives a global element in $K^\times$.

⋆ $\mathcal{U}(O_K[G])$**:** We look at each place $\mathfrak{p}$ separately and we compute the values at χ_0. By definition of the map Det and considering an element $\alpha := \sum_{s\in G} a_s s \in K^c[G]$, we obtain $\mathrm{Det}(\alpha)(\chi_0) = T_{\chi_0}(\alpha) = \sum_{s\in G} a_s$.
If we take $x_\mathfrak{p} \in (O^c_{K,\mathfrak{p}}[G]^\times/G)^{\Omega_\mathfrak{p}}$ represented by $\alpha_\mathfrak{p} \in O^c_{K,\mathfrak{p}}[G]^\times$, we have

$$\widetilde{\mathrm{Det}}(x_\mathfrak{p})(\chi_0) = \mathrm{rag}'(\mathrm{Det}(\alpha_\mathfrak{p}))(\chi_0) = \mathrm{Det}(\alpha_\mathfrak{p})(\chi_0).$$

Now, for any $\omega \in \Omega_\mathfrak{p}$, we have $\alpha_\mathfrak{p}^\omega = \alpha_\mathfrak{p} \cdot s'$, where $s' \in G$. Thus, applying T_{χ_0}, we get $T_{\chi_0}(\alpha_\mathfrak{p})^\omega = T_{\chi_0}(\alpha_\mathfrak{p})$. Hence, for each $\mathfrak{p}$, the element $\mathrm{Det}(\alpha_\mathfrak{p})(\chi_0)$ belongs to $O^\times_{K,\mathfrak{p}}$, which combine to show that each element in $\mathcal{U}(O_K[G])$ is sent to $U(O_K)$ when evaluated at χ_0.

⋆ $\Theta^t_{\bar{G}}(J(K\bar{\Lambda}))$**:** Given $h \in J(K\bar{\Lambda})$, just by definition, we have $\Theta^t_{\bar{G}}(h)(\chi_0) = h\left(\Theta_{\bar{G}}\left(\chi_0\right)\right)$, but $\Theta_{\bar{G}}(\chi_0) = 0$, since $\chi_0(s) = 1$ for each $s \in G$. Thus every element in $\Theta^t_{\bar{G}}(J(K\bar{\Lambda}))$ evaluated at χ_0 is trivial.

Combining all together, it is now easy to see that, if we take $c \in \mathrm{St}(O_K[G])$ and we consider a representative of it $f \in \mathrm{Hom}_\Omega\left(R_G, J(K^c)\right)$, we obtain $f(\chi_0) \in K^\times \cdot U(O_K)$, as we wanted to prove. □

After this proposition, one may wonder if the reverse inclusion also holds. This is the case for some groups (e.g. $G = A_4$, see [11]), but is not in general true as the next counterexample shows.

Counterexample. Given a prime number p, take $G = C_p$, a cyclic group of order p; then, as shown in [31], we have $\mathrm{Cl}(\mathbb{Z}[C_p]) \cong \mathrm{Cl}(\mathbb{Z}[\zeta_p])$, where ζ_p is a primitive p-th root of unity. Since $\mathrm{Cl}(\mathbb{Z}) = 1$, we get $\mathrm{Cl}^\circ(\mathbb{Z}[C_p]) = \mathrm{Cl}(\mathbb{Z}[C_p])$.
By the Hilbert–Speiser theorem, $R(\mathbb{Z}[C_p]) = 1$ and, by McCulloh's results, the group $\mathrm{St}(\mathbb{Z}[C_p])$ is trivial. So, just taking a cyclic group C_p, with a prime p such that the class number of $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ is not one (e.g. $p = 23$, see [46, Chapter 11]), we have a simple example where $\mathrm{St}(O_K[G]) \subsetneq \mathrm{Cl}^\circ(O_K[G])$.

3.2 Computing $\mathrm{St}(O_K[G])$

In this section we compute explicitly $\mathrm{St}(O_K[G])$ in some special cases, just using its algebraic definition and Stickelberger's classical theorem. The results here contained are summarized in the next theorem (Theorem 0.0.6 in the Introduction).

Theorem 3.2.1. *Given a prime number $p \neq 2$. If $G = C_2$, a cyclic group of order 2, or $G = C_p$, a cyclic group of order p or $G = D_p$, the dihedral group of order $2p$, then $\mathrm{St}(\mathbb{Z}[G]) = 1$.*

This result will immediately imply, just using Theorem A, the following corollary.

Corollary 3.2.2. *In the cases of the theorem above, $R(\mathbb{Z}[G]) = 1$.*

Note that these are already known results. As explained in the Introduction, the case $G = C_p$, with p a prime number, follows from Hilbert–Speiser, while the dihedral case is contained in the more general result by Taylor [43]. The proof given here does not assume either of these results, however, but instead uses the definition of $\mathrm{St}(\mathbb{Z}[G])$ together with Stickelberger's theorem.
The dihedral case is in some sense the more interesting one, since in particular it goes in the direction of extending Theorem B to non-abelian groups, indeed from Theorem 3.2.1 we clearly deduce an easy non-abelian example where the equality $R(\mathbb{Z}[D_p]) = \mathrm{St}(\mathbb{Z}[D_p])$ holds.

3.2.3 Background on C_p and D_p

Let C_p be a cyclic group of order a prime number p with generator denoted by t and let the group of characters $\widehat{C_p}$ be generated by χ_p, where $\chi_p(t) := e^{\frac{2\pi i}{p}}$. We denote by χ_0 the trivial character ($\chi_p^p = \chi_0$).
The following result, that we have already used in the previous counterexample, describes $\mathrm{Cl}(\mathbb{Z}[C_p])$ in terms of the class group of a cyclotomic extension $\mathbb{Q}(\zeta_p)$ and is due to D. S. Rim.

Lemma 3.2.4. *Let ζ_p be a primitive p-th root of unity, then we have the following group isomorphism:*

$$\begin{array}{rccc} \mathcal{L}: & \mathrm{Cl}(\mathbb{Z}[C_p]) & \xrightarrow{\cong} & \mathrm{Cl}(\mathbb{Z}[\zeta_p]) \\ & c = [f] & \longmapsto & [f(\chi_p)] \quad . \end{array}$$

Proof. This is a result contained in [31] and here rewritten in terms of the Hom-description, after having recalled the idelic representation of the ideal class group

$$\mathrm{Cl}(\mathbb{Z}[\zeta_p]) \cong J\left(\mathbb{Q}(\zeta_p)\right) / \left(\mathbb{Q}(\zeta_p)^\times \cdot U(\mathbb{Z}[\zeta_p])\right).$$

The element f, representative of the class c, belongs to $\mathrm{Hom}_\Omega\left(R_{C_p}, J(\mathbb{Q}^c)\right)$. □

The dihedral group D_p is the group of symmetries of a regular polygon with p sides, including both rotations and reflections. It has order $2p$ and it can be represented as

$$D_p := \langle r, s \,|\, r^p = s^2 = 1, s^{-1}rs = r^{-1} \rangle.$$

We will just consider $p \geq 3$, note that D_2 is the Klein four-group.
If $p \geq 3$, the set of irreducible characters over $\mathbb{C}$, denoted by $\mathrm{Irr}(D_p)$, consists of two characters ψ_0 and ψ_0' of dimension 1, and $(p-1)/2$ characters ψ_j (with $j = 1, \ldots, (p-1)/2$) of dimension 2. The character ψ_0 is the trivial character, while ψ_0' sends r^k to 1 and sr^k to -1. The characters ψ_j, for $j = 1, \ldots, (p-1)/2$, are defined as

$$\psi_j : \begin{cases} r^k \longmapsto 2\cos\left(\dfrac{2\pi jk}{p}\right), & k = 0, \ldots, p-1\,; \\ sr^k \longmapsto 0, & k = 0, \ldots, p-1. \end{cases}$$

For D_p an analogous result to Lemma 3.2.4 follows.

Lemma 3.2.5. *Let p be an odd prime and let ζ_p be as above, then the following group isomorphism holds:*

$$\begin{array}{rccc} \mathcal{J}: & \mathrm{Cl}(\mathbb{Z}[D_p]) & \xrightarrow{\cong} & \mathrm{Cl}(\mathbb{Z}(\zeta_p+\zeta_p^{-1})) \\ & [f] & \longmapsto & [f(\psi_1)] \ . \end{array}$$

Proof. This follows from the Wedderburn decomposition $\mathbb{Q}[D_p] \cong \mathbb{Q}\times\mathbb{Q}\times M_2(\mathbb{Q}(\zeta_p+\zeta_p^{-1}))$ and the isomorphism $\mathrm{Cl}(\mathbb{Z}[D_p]) \cong \mathrm{Cl}(\mathcal{M}) \cong \mathrm{Cl}(\mathbb{Z}(\zeta_p+\zeta_p^{-1}))$, where $\mathcal{M}$ denotes a maximal order in $\mathbb{Q}[D_p]$ containing $\mathbb{Z}[D_p]$. See [15, Theorem 50.25] for more details. □

3.2.6 Stickelberger's classical theorem

We briefly recall here some annihilation results for class groups.

Let $N/\mathbb{Q}$ be a finite abelian extension, so, by the Kronecker–Weber theorem, $N \subseteq \mathbb{Q}(\zeta_n)$ (n is assumed to be the minimal integer with this property and ζ_n is a primitive n-th root of unity). If $H = \mathrm{Gal}(N/\mathbb{Q})$, then it can be viewed as a quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$ and we denote by σ_μ, where $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$, both the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ which sends ζ_n to its μ-th power and its restriction to N. Then the Stickelberger element of N is defined as

$$\Psi := \sum_{\mu \in (\mathbb{Z}/n\mathbb{Z})^\times} \left\{\frac{\mu}{n}\right\} \sigma_\mu^{-1} \ \in \ \mathbb{Q}[H]$$

and we have the following classical theorem.

Theorem 3.2.7. (Stickelberger's Theorem). *Let I be a fractional ideal of N, let $\beta \in \mathbb{Z}[H]$, and suppose $\beta\Psi \in \mathbb{Z}[H]$. Then $(\beta\Psi)\cdot I$ is principal.*

Proof. [46, Theorem 6.10]. □

Another useful relation for ideal classes of cyclotomic extensions is given by the next theorem.

Theorem 3.2.8. *Let $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity and denote by σ_μ, for $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$, the automorphism defined above. Let p be a prime number, such that $p \nmid n$ and let us consider a prime ideal $\mathfrak{P}|p$ in O_L. For positive*

integers a, b such that $ab(a+b) \not\equiv 0$ mod n, let us write

$$\Psi_{a,b} := \sum_{\mu \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(\left\lfloor \frac{(a+b)\mu}{n} \right\rfloor - \left\lfloor \frac{a\mu}{n} \right\rfloor - \left\lfloor \frac{b\mu}{n} \right\rfloor \right) \sigma_\mu^{-1}.$$

Then $(\Psi_{a,b}).\mathfrak{P}$ is principal. Since any ideal class contains infinitely many primes, this gives a relation on the ideal class group of $\mathbb{Q}(\zeta_n)$.

Proof. [24, Chapter IV, §4, Theorem 11]. □

3.2.9 The Stickelberger map for C_p and D_p

For any prime number p, in the cyclic case C_p, it is easy to see that $\langle \chi_0, t^j \rangle$ is equal to 0 and $\langle \chi_p^i, t^j \rangle = \left\{ \frac{ij}{p} \right\}$, for $j = 0, \ldots, p-1$ and $i = 1, \ldots, p-1$. Hence

$$\Theta_{C_p} : \begin{cases} \chi_0 & \longmapsto 0 \ , \\ \chi_p^i & \longmapsto \dfrac{i}{p}t + \left\{ \dfrac{2i}{p} \right\} t^2 + \cdots + \left\{ \dfrac{(p-1)i}{p} \right\} t^{p-1} \ , \text{ for } 1 \le i \le p-1. \end{cases}$$

While for the dihedral group D_p (with $p \geq 3$), first we have to think about the restriction of the irreducible characters over the cyclic subgroups $\langle r \rangle$ (of order p) and $\langle sr^k \rangle$ (of order 2). For the characters of dimension 1 we clearly have

$$\begin{aligned} \mathrm{res}^{D_p}_{\langle r \rangle} \psi_0 &= \chi_0 & \qquad \mathrm{res}^{D_p}_{\langle sr^k \rangle} \psi_0 &= \phi_0 \\ \mathrm{res}^{D_p}_{\langle r \rangle} \psi_0' &= \chi_0 & \qquad \mathrm{res}^{D_p}_{\langle sr^k \rangle} \psi_0' &= \phi_0' \end{aligned}$$

where χ_0 represents the trivial character of the cyclic group $\langle r \rangle$ (we use the same notation for the trivial character of C_p, since they are both cyclic group of order p), while ϕ_0, ϕ_0' are the trivial and the non-trivial character of a cyclic group of order 2, respectively.
For the other characters of dimension 2, using the inner products and some computations, since $C_p \cong \langle r \rangle$, we get

$$\mathrm{res}^{D_p}_{\langle r \rangle} \psi_j = \chi_p^j + \chi_p^{p-j}, \quad \text{for } j = 1, \ldots, (p-1)/2.$$

While for the subgroups $\langle sr^k \rangle$, where $k = 0, \ldots, p-1$, we get

$$\mathrm{res}^{D_p}_{\langle sr^k \rangle} \psi_j = \phi_0 + \phi_0', \quad \text{for } j = 1, \ldots, (p-1)/2.$$

Then we easily deduce the values of the Stickelberger pairings on the elements of $\mathrm{Irr}(D_p)$:

$$\begin{gathered}
\langle \psi_0, r^k \rangle = \langle \psi_0, sr^k \rangle = 0, \text{ for } k = 0, \ldots, p-1, \\
\langle \psi_0', r^k \rangle = 0, \ \langle \psi_0', sr^k \rangle = 1/2, \text{ for } k = 0, \ldots, p-1, \\
\langle \psi_j, 1 \rangle = 0, \text{ for } j = 1, \ldots, (p-1)/2, \\
\langle \psi_j, r^k \rangle = 1, \text{ for } k = 1, \ldots, p-1 \text{ and } j = 1, \ldots, (p-1)/2, \\
\langle \psi_j, sr^k \rangle = 1/2, \text{ for } k = 0, \ldots, p-1 \text{ and } j = 1, \ldots, (p-1)/2.
\end{gathered}$$

Thus we can now consider the Stickelberger map on the conjugacy classes

$$\begin{aligned}
\Theta_{\bar{D}_p} : \mathbb{Q} \otimes_{\mathbb{Z}} R_{D_p} &\longrightarrow \mathbb{Q}[\bar{D}_p] \\
\chi &\longmapsto \sum_{\bar{s} \in \bar{D}_p} \langle \chi, \bar{s} \rangle \bar{s}.
\end{aligned}$$

There are $(p+3)/2$ conjugacy classes of D_p:

$$\{1\}, \ \{r^k, r^{-k}\} \text{ for } k = 1, \ldots, (p-1)/2 \text{ and } \{s, sr, sr^2, \ldots, sr^{p-1}\};$$

then, since $\langle \chi, \bar{s} \rangle$ was defined as $\langle \chi, s \rangle$, it is easy to see that we obtain:

$$\Theta_{\bar{D}_p} : \begin{cases}
\psi_0 \longmapsto 0 \ , \\
\psi_0' \longmapsto \dfrac{1}{2}\bar{s} \ , \\
\psi_j \longmapsto \sum_{k=1}^{(p-1)/2} \bar{r^k} + \dfrac{1}{2}\bar{s}, \ \text{ for } j = 1, \ldots, (p-1)/2.
\end{cases}$$

3.2.10 The augmentation kernels $\mathcal{A}_{C_p}$ and $\mathcal{A}_{D_p}$

As we have already seen in Remark 2.2.1, we have the following lemma.

Lemma 3.2.11. *Let C_p be the cyclic group of prime order p, then*

$$\begin{aligned}
\mathcal{A}_{C_2} &= \langle \chi_0, 2\chi_2 \rangle \, , \\
\mathcal{A}_{C_p} &= \langle \chi_0, j\chi_p - \chi_p^j, p\chi_p \rangle, \ \textit{for } \ 2 \leq j \leq p-1, \ \textit{if } p \neq 2.
\end{aligned}$$

An analogous result for the dihedral group D_p follows.

Lemma 3.2.12. *Let D_p be the dihedral group of order $2p$, with $p \geq 3$, then*

$$\mathcal{A}_{D_p} = \langle \psi_0,\, 2\psi_0',\, \psi_0' - \psi_j \rangle \text{ for } j = 1, \ldots, (p-1)/2.$$

Proof. Consider an element $\alpha \in R_{D_p}$ and write it as

$$\alpha = \alpha_0\psi_0 + \alpha_0'\psi_0' + \sum_{j=1}^{(p-1)/2} \alpha_j\psi_j.$$

Since $\det(\psi_j) = \psi_0'$, we have

$$\det(\alpha) = (\psi_0')^{\alpha_0' + \sum_{j=1}^{(p-1)/2} \alpha_j},$$

hence, by the definition of $\mathcal{A}_{D_p}$,

$$\alpha \in \mathcal{A}_{D_p} \iff \alpha_0' + \sum_{j=1}^{(p-1)/2} \alpha_j \equiv 0 \mod 2.$$

Thus writing

$$\alpha = \alpha_0\psi_0 + 2b\psi_0' - \sum_{j=1}^{(p-1)/2} \alpha_j(\psi_0' - \psi_j),$$

where $b \in \mathbb{Z}$ such that $\alpha_0' + \sum_{j=1}^{(p-1)/2} \alpha_j = 2b$, we get our claim. □

3.2.13 The triviality of $\Theta^{\mathrm{t}}_{C_p}$ and $\Theta^{\mathrm{t}}_{\bar{D}_p}$ over $\mathbb{Q}$

Once we know the structure of the augmentation kernel $\mathcal{A}_{C_p}$, we can apply Stickelberger's classical theorem in the computation of $\Theta^{\mathrm{t}}_{C_p}(\mathrm{Hom}_\Omega(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}^c)))$, as the following proposition explains. We warn the reader that, since we are working over $\mathbb{Q}$, the notation Ω here stands for $\Omega_{\mathbb{Q}}$.

Proposition 3.2.14. *For any prime number p,*

$$\Theta^{\mathrm{t}}_{C_p}(\mathrm{Hom}_\Omega(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}^c))) \subseteq \mathrm{Hom}_\Omega\left(\mathcal{A}_{C_p}, \mathbb{Q}(\zeta_p)^\times \cdot U(\mathbb{Z}[\zeta_p])\right).$$

Proof. We first remark that the group $\mathrm{Hom}_\Omega(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}^c))$ is equal to the group $\mathrm{Hom}_\Omega(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}(\zeta_p)))$ (think about the Ω-action) and, given $h \in \mathrm{Hom}_\Omega(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}(\zeta_p)))$, we immediately understand that, thanks to the Ω-action, it is uniquely determined by $h(1)$ and $h(t)$ (where t is the chosen generator

of C_p). Indeed $\sigma_i^{-1} \cdot t = t^i$ (remember the twist in the definition of the action of Ω on $C_p(-1)$), where, as before, $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is such that $\sigma_i(\zeta_p) = \zeta_p^i$, for $i = 1, \ldots, p-1$. Thus if $h(t) = x \in J(\mathbb{Q}(\zeta_p))$, considering the Ω-invariance, we have $h(t^i) = \sigma_i^{-1} \cdot x$.
Now, using the description of the Stickelberger map given in §3.2.9, on the generators of $\mathcal{A}_{C_p}$ we get

$$\Theta_{C_p} : \begin{cases} \chi_0 & \longmapsto 0 \ , \\ p\chi_p & \longmapsto t + 2t^2 + \cdots + (p-1)t^{p-1} \ , \\ j\chi_p - \chi_p^j & \longmapsto \left\lfloor \dfrac{2j}{p} \right\rfloor t^2 + \cdots + \left\lfloor \dfrac{(p-1)j}{p} \right\rfloor t^{p-1} \ , \text{ for } 2 \leq j \leq p-1; \end{cases}$$

where the last line is not considered if $p = 2$.
Thus we can now compute the transpose of the Stickelberger map (again when $p = 2$ we just consider the first two lines) on $h \in \mathrm{Hom}_{\Omega}(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}(\zeta_p)))$, obtaining

$$\Theta_{C_p}^{\mathrm{t}}(h) : \begin{cases} \chi_0 & \longmapsto 1 \ , \\ p\chi_p & \longmapsto \left(\sum_{i=1}^{p-1} i\sigma_i^{-1}\right) \cdot x \ , \\ j\chi_p - \chi_p^j & \longmapsto \left(\sum_{i=1}^{p-1} \left\lfloor \frac{ij}{p} \right\rfloor \sigma_i^{-1}\right) \cdot x \ , \text{ for } 2 \leq j \leq p-1. \end{cases}$$

Now, using the idelic representation of $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ recalled in the proof of Lemma 3.2.4, we immediately deduce from Theorem 3.2.7 that $\Theta_{C_p}^{\mathrm{t}}(h)(p\chi_p)$ is trivial considered in $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ or in other words $\Theta_{C_p}^{\mathrm{t}}(h)(p\chi_p) \in \mathbb{Q}(\zeta_p)^{\times} \cdot U(\mathbb{Z}[\zeta_p])$; which proves the proposition for $p = 2$.
When $p \neq 2$, for the other generators $j\chi_p - \chi_p^j$, we use Theorem 3.2.8 considered for the cyclotomic extension $\mathbb{Q}(\zeta_p)$ and we proceed by induction. Starting with $j = 2$, we get

$$\Theta_{C_p}^{\mathrm{t}}(h)(2\chi_p - \chi_p^2) = \left(\sum_{i=1}^{p-1} \left\lfloor \frac{2i}{p} \right\rfloor \sigma_i^{-1}\right) \cdot x$$

and using Theorem 3.2.8, with $a = b = 1$, we get $\Theta_{C_p}^{\mathrm{t}}(h)(2\chi_p - \chi_p^2) \in \mathbb{Q}(\zeta_p)^{\times} \cdot U(\mathbb{Z}[\zeta_p])$ (proving the result for $p = 3$).
For $p > 3$, let j be a natural number in $\{2, \ldots, p-1\}$, denote $\Theta_{C_p}^{\mathrm{t}}(h)(j\chi_p - \chi_p^j)$ by x_j and assume that $x_j \in \mathbb{Q}(\zeta_p)^{\times} \cdot U(\mathbb{Z}[\zeta_p])$, then we have

$$\frac{x_{j+1}}{x_j} = \left(\sum_{i=1}^{p-1} \left(\left\lfloor \frac{(j+1)i}{p} \right\rfloor - \left\lfloor \frac{ji}{p} \right\rfloor \right) \sigma_i^{-1}\right) \cdot x \, ,$$

which belongs to $\mathbb{Q}(\zeta_p)^{\times} \cdot U(\mathbb{Z}[\zeta_p])$, applying Theorem 3.2.8 with $a = j$ and $b = 1$. Thus we deduce that, if $x_j \in \mathbb{Q}(\zeta_p)^{\times} \cdot U(\mathbb{Z}[\zeta_p])$, then $x_{j+1} \in \mathbb{Q}(\zeta_p)^{\times} \cdot U(\mathbb{Z}[\zeta_p])$,

which by induction gives the proof. □

We do exactly the same for D_p and an analogous result follows.

Proposition 3.2.15. *Let D_p be the dihedral group defined above, with $p \geq 3$, then*

$$\Theta^{\mathrm{t}}_{\bar{D}_p}\left(\mathrm{Hom}_{\,\Omega}\left(\mathbb{Z}[\bar{D}_p(-1)], J(\mathbb{Q}^c)\right)\right) \subseteq \mathrm{Hom}_{\,\Omega}\left(\mathcal{A}_{D_p}, \mathbb{Q}(\zeta_p+\zeta_p^{-1})^{\times} \cdot U\left(\mathbb{Z}[\zeta_p+\zeta_p^{-1}]\right)\right).$$

Proof. Going back to the definition of the Ω-action on $\bar{D}_p(-1)$, we see that $\mathrm{Stab}\,(\bar{s}) = \Omega$, since s is of order 2, while $\mathrm{Stab}\left(\bar{r^k}\right) = \mathrm{Gal}(\mathbb{Q}^{\mathrm{c}}/\mathbb{Q}(\zeta_p+\zeta_p^{-1}))$, for all $k = 1, \ldots, (p-1)/2$.
Thus note that $\mathrm{Hom}_{\,\Omega}\left(\mathbb{Z}[\bar{D}_p(-1)], J(\mathbb{Q}^c)\right) = \mathrm{Hom}_{\,\Omega}\left(\mathbb{Z}[\bar{D}_p(-1)], J\left(\mathbb{Q}(\zeta_p+\zeta_p^{-1})\right)\right)$. Given $h \in \mathrm{Hom}_{\,\Omega}\left(\mathbb{Z}[\bar{D}_p(-1)], J(\mathbb{Q}^c)\right)$, then $\Theta^{\mathrm{t}}_{\bar{D}_p}(h)$ in $\mathrm{Hom}_{\,\Omega}\left(\mathcal{A}_{D_p}, J(\mathbb{Q}^c)\right)$ is defined by the values it assumes on the set of basis elements of $\mathcal{A}_{D_p}$ which we studied in the previous section. In particular, if we denote by $x \in J(\mathbb{Q})$ the element $h(\bar{s})$ and by $y \in J(\mathbb{Q}(\zeta_p+\zeta_p^{-1}))$ the element $h(\bar{r})$, we have

$$\Theta^{\mathrm{t}}_{\bar{D}_p}(h) : \begin{cases} \psi_0 & \longmapsto 1\ , \\ 2\psi_0' & \longmapsto x\ , \\ \psi_0' - \psi_j & \longmapsto -(\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q})} \sigma)\cdot y, \ \text{ for } j = 1, \ldots, (p-1)/2. \end{cases}$$

where in the last computation we used the fact that $\mathrm{Gal}(\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q})$ acts transitively on the set of conjugacy classes $\left\{\bar{r^k}\right\}_{k=1,\ldots,(p-1)/2}$.
We see that $\Theta^{\mathrm{t}}_{\bar{D}_p}(h)(\psi_0)$ and $\Theta^{\mathrm{t}}_{\bar{D}_p}(h)(2\psi_0')$ are in $J(\mathbb{Q})$ so they can be written as a product of a global and a unit element ($\mathrm{Cl}(\mathbb{Z})$=1). While, we have the relation $(\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q})} \sigma)\cdot y = \mathrm{N}_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q}}(y)$, hence $\Theta^{\mathrm{t}}_{\bar{D}_p}(h)(\psi_0' - \psi_j) \in J(\mathbb{Q})$, for $j = 1, \ldots, (p-1)/2$, which concludes the proof. □

3.2.16 Proof of Theorem 3.2.1

Let us consider the isomorphism $\mathcal{L}$, given in Lemma 3.2.4. For every $\omega \in \Omega$ and $c \in \mathrm{Cl}(\mathbb{Z}[C_p])$, represented in terms of the hom-description by $f \in \mathrm{Hom}_{\,\Omega}\left(R_{C_p}, J(\mathbb{Q}^{\mathrm{c}})\right)$, we have:

$$\mathcal{L}(c)^{\omega} = [f(\chi_p)]^{\omega} = [f(\chi_p)^{\omega}] = [f\left(\chi_p^{\omega}\right)],$$

where, in the last equality, we use the Ω-equivariance of f.

Using again Stickelberger's Theorem and the isomorphism $\mathcal{L}$ between $\mathrm{Cl}(\mathbb{Z}[C_p])$ and $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$, we can now prove the following proposition.

Proposition 3.2.17. *Let p be a prime number and $f \in \mathrm{Hom}_{\Omega}\left(R_{C_p}, J(\mathbb{Q}^c)\right)$, such that*

$$\mathrm{rag}'(f) \in \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{C_p}, \mathbb{Q}(\zeta_p)^{\times} \cdot U\left(\mathbb{Z}[\zeta_p]\right)\right).$$

If $c := [f] \in \mathrm{Cl}(\mathbb{Z}[C_p])$, then $c = 1$.

Proof. If $p = 2$, then $\mathrm{Cl}(\mathbb{Z}[C_2]) \cong \mathrm{Cl}(\mathbb{Z}) = 1$, so there is nothing to prove and in our proof we can assume $p \neq 2$. Using the isomorphism $\mathcal{L}$, we have

$$(\mathcal{L}(c))^p = [f(\chi_p)]^p = [f(\chi_p)^p] \overset{(a)}{=} [f(p\chi_p)] \overset{(b)}{=} [\mathrm{rag}'(f)(p\chi_p)] \overset{(c)}{=} 1, \tag{3.1}$$

where (a) is given by the fact that f is a homomorphism, (b) since $p\chi_p \in \mathcal{A}_{C_p}$ and (c) thanks to the idelic representation of the ideal class group $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$.
If $\sigma_j \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is such that $\sigma_j(\zeta_p) = \zeta_p^j$, for $j = 1, \ldots, p-1$, we also get

$$\sigma_j \cdot (\mathcal{L}(c)) = [f\left(j\chi_p - (j\chi_p - \chi_p^j)\right)] = [f(j\chi_p)][f(j\chi_p - \chi_p^j)]^{-1} \overset{(d)}{=} [f(j\chi_p)] = (\mathcal{L}(c))^j,$$

where in (d) we use the fact that $j\chi_p - \chi_p^j \in \mathcal{A}_{C_p}$ and the idelic representation of $\mathrm{Cl}(\mathbb{Z}(\zeta_p))$.
Once we know the action of σ_j on $\mathcal{L}(c)$, we can apply Stickelberger's Theorem to the element of $\mathrm{Cl}\left(\mathbb{Z}[\zeta_p]\right)$ given by $\mathcal{L}(c)$:

$$1 = \sum_{j=1}^{p-1} j\sigma_j^{-1} \cdot (\mathcal{L}(c)) \overset{(e)}{=} \prod_{j=1}^{p-1} (\mathcal{L}(c))^{jj^{-1}} = (\mathcal{L}(c))^{p-1}, \tag{3.2}$$

where the first equality is exactly Stickelberger's Theorem and (e) is assured by $\sigma_j^{-1} = \sigma_{j^{-1}}$, where j^{-1} is the inverse of j in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ belonging to $\{1, \ldots, p-1\}$. Note that the last equality follows from the fact that $jj^{-1} \equiv 1 \mod p$ and from (3.1).
Finally, putting together (3.1) and (3.2), we have

$$\mathcal{L}(c) = 1,$$

which implies $c = 1$ in $\mathrm{Cl}(\mathbb{Z}[C_p])$, thanks to the isomorphism between $\mathrm{Cl}(\mathbb{Z}[C_p])$ and $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$. □

Analogously, using the isomorphism $\mathcal{J}$ given in Lemma 3.2.5, in the dihedral case we have the following result.

Proposition 3.2.18. *If $p \geq 3$, let us consider $f \in \mathrm{Hom}_{\Omega}\left(R_{D_p}, J(\mathbb{Q}^c)\right)$, such that*

$$\mathrm{rag}'(f) \in \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, \mathbb{Q}(\zeta_p+\zeta_p^{-1})^{\times} \cdot U\left(\mathbb{Z}[\zeta_p+\zeta_p^{-1}]\right)\right).$$

If $c := [f] \in \mathrm{Cl}(\mathbb{Z}[D_p])$, then $c = 1$.

Proof. Given $c \in \mathrm{Cl}(\mathbb{Z}[D_p])$ as in the hypothesis, then

$$\mathcal{J}(c) = [f(\psi_1)] = [f(\psi_0' - (\psi_0' - \psi_1))] = [f(\psi_0')][f(\psi_0' - \psi_1)]^{-1}.$$

Now since $\psi_0' - \psi_1$ is contained in $\mathcal{A}_{D_p}$, by hypothesis we have $[f(\psi_0' - \psi_1)] = 1$ and so we get $\mathcal{J}(c) = [f(\psi_0')]$. Since $f(\psi_0') \in J(\mathbb{Q})$, this concludes the proof. □

We can finally prove Theorem 3.2.1.

Proof of Theorem 3.2.1. We consider the case $G = D_p$, the case C_p is analogous. A class $c = [f] \in \mathrm{Cl}(\mathbb{Z}[D_p])$ belongs to $\mathrm{St}(\mathbb{Z}[D_p])$ if and only if

$$\mathrm{rag}'(f) = g \cdot \Theta^{\mathrm{t}}_{\bar{D}_p}(h) \cdot w,$$

where $g \in \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, (\mathbb{Q}^c)^{\times}\right)$, $h \in \mathrm{Hom}_{\Omega}\left(\mathbb{Z}[\bar{D}_p(-1)], J\left(\mathbb{Q}\left(\zeta_p+\zeta_p^{-1}\right)\right)\right)$ and $w \in \mathcal{U}(\mathbb{Z}[D_p]) \subseteq \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, U(\mathbb{Z}^c)\right)$ (see (2.14) for the original definition of $\mathcal{U}(\mathbb{Z}[D_p])$). Since

$$\begin{aligned}\mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, (\mathbb{Q}^c)^{\times}\right) &= \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, \mathbb{Q}(\zeta_p+\zeta_p^{-1})\right)\\ \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, U(\mathbb{Z}^c)\right) &= \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, U(\mathbb{Z}[\zeta_p+\zeta_p^{-1}])\right),\end{aligned}$$

clearly $g \cdot w \in \mathrm{Hom}_{\Omega}\left(\mathcal{A}_{D_p}, \mathbb{Q}(\zeta_p+\zeta_p^{-1})^{\times} \cdot U\left(\mathbb{Z}[\zeta_p+\zeta_p^{-1}]\right)\right)$. Thus, using Proposition 3.2.15 and Proposition 3.2.18, we finally get $c = 1$, as we wanted to show.

□

Chapter 4

Functoriality of $\mathrm{St}(O_K[G])$ under base field restriction

In this chapter G is a finite group (not necessarily abelian).

As seen in §1.8.3, given K a subfield of a number field L, we have a restriction map $\mathrm{res}_{L/K} : \mathrm{Cl}(O_L[G]) \longrightarrow \mathrm{Cl}(O_K[G])$, which in terms of the Hom-description is expressed by the norm map

$$\begin{array}{rccc} \mathcal{N}_{L/K} : \dfrac{\mathrm{Hom}_{\Omega_L}(R_G, J(\mathbb{Q}^c))}{\mathrm{Hom}_{\Omega_L}(R_G, (\mathbb{Q}^c)^\times) \cdot \mathrm{Det}(U(O_L[G]))} & \to & \dfrac{\mathrm{Hom}_{\Omega_K}(R_G, J(\mathbb{Q}^c))}{\mathrm{Hom}_{\Omega_K}(R_G, (\mathbb{Q}^c)^\times) \cdot \mathrm{Det}(U(O_K[G]))} \\ [f] & \mapsto & [\mathcal{N}_{L/K}(f)] \end{array}$$

where $\mathcal{N}_{L/K}(f)(\alpha) := \prod_{\omega \in \Omega_K/\Omega_L} f^\omega(\alpha) = \prod_{\omega \in \Omega_K/\Omega_L} f\left(\alpha^{\omega^{-1}}\right)^\omega$ (by the definition of the left Ω-action on $\mathrm{Hom}\,(R_G, J(\mathbb{Q}^c))$) and instead of taking K^c and L^c, we consider $\mathbb{Q}^c$ in order to homogenize the notation (we can do it since L and K are both algebraic extensions of $\mathbb{Q}$).

From Chapter 2, we know that $R(O_L[G])$ (resp. $R(O_K[G])$) is contained in the Stickelberger subgroup $\mathrm{St}(O_L[G])$ (resp. $\mathrm{St}(O_K[G])$), with equality when the group G is abelian. An interesting question naturally arises: is the Stickelberger subgroup functorial under this map? Or more precisely, does the inclusion

$$\mathcal{N}_{L/K}(\mathrm{St}(O_L[G])) \subseteq \mathrm{St}(O_K[G])$$

hold?
In this chapter we are going to give an affirmative answer to this question, which will have some nice consequences, as explained in the last section.

4.1 Changing the base field for the Stickelberger subgroup

In §2.5, using the group homomorphisms

$$\mathrm{Cl}(O_L[G]) \xrightarrow{\mathrm{Rag}_L} \mathrm{MCl}(O_L[G]) \xleftarrow{\Theta^t_L} J(L\bar{\Lambda}),$$

we defined $\mathrm{St}(O_L[G])$ as $\mathrm{Rag}_L^{-1}(\mathrm{Im}(\Theta^{\mathrm{t}}_L))$. Analogously for $\mathrm{St}(O_K[G])$. Differently from §2.5, it is better to put in evidence the base field in our notation used for the map Rag and $\Theta^t_{\bar{G}}$: namely Rag_L (resp. Rag_K) stands for the map Rag defined over L (resp. K) and analogously Θ^{t}_L (resp. Θ^{t}_K) stands for the map $\Theta^{\mathrm{t}}_{\bar{G}}$ defined over the field L (resp. K).

It is not difficult to see that $\mathcal{N}_{L/K}$ induces the following well-defined group homomorphisms (for which we will use the same name):

$$\begin{aligned} \mathcal{N}_{L/K} : \mathrm{MCl}(O_L[G]) &\longrightarrow \mathrm{MCl}(O_K[G]), \\ \mathcal{N}_{L/K} : \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\bar{G}](-1), J(\mathbb{Q}^{\mathrm{c}})\right) &\longrightarrow \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\bar{G}](-1), J(\mathbb{Q}^{\mathrm{c}})\right). \end{aligned}$$

Thus we can prove the next result.

Proposition 4.1.1. *The following diagram commutes:*

$$\begin{array}{ccccc} \mathrm{Cl}(O_L[G]) & \xrightarrow{\mathrm{Rag}_L} & \mathrm{MCl}(O_L[G]) & \xleftarrow{\Theta^{\mathrm{t}}_L} & \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\bar{G}(-1)], J(\mathbb{Q}^{\mathrm{c}})\right) \\ \downarrow{\scriptstyle \mathcal{N}_{L/K}} & & \downarrow{\scriptstyle \mathcal{N}_{L/K}} & & \downarrow{\scriptstyle \mathcal{N}_{L/K}} \\ \mathrm{Cl}(O_K[G]) & \xrightarrow{\mathrm{Rag}_K} & \mathrm{MCl}(O_K[G]) & \xleftarrow{\Theta^{\mathrm{t}}_K} & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\bar{G}(-1)], J(\mathbb{Q}^{\mathrm{c}})\right). \end{array}$$

Proof. First of all we claim that the following diagram commutes

$$\begin{array}{ccc} \mathrm{Cl}(O_L[G]) & \xrightarrow{\mathrm{Rag}_L} & \mathrm{MCl}(O_L[G]) \\ \downarrow{\scriptstyle \mathcal{N}_{L/K}} & & \downarrow{\scriptstyle \mathcal{N}_{L/K}} \\ \mathrm{Cl}(O_K[G]) & \xrightarrow{\mathrm{Rag}_K} & \mathrm{MCl}(O_K[G]). \end{array}$$

Given $f \in \mathrm{Hom}_{\Omega_K}(R_G, J(\mathbb{Q}^c))$ and an element $\alpha := \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi \in \mathcal{A}_G$, using the definition of $\mathcal{N}_{L/K}$, we have

$$\begin{aligned}
\mathcal{N}_{L/K}(\mathrm{Rag}_L(f))(\alpha) &= \prod_{\omega \in \Omega_K/\Omega_L} \mathrm{Rag}_L(f)\left(\alpha^{\omega^{-1}}\right)^{\omega} \\
&= \prod_{\omega \in \Omega_K/\Omega_L} f\left(\alpha^{\omega^{-1}}\right)^{\omega} \\
&= \mathcal{N}_{L/K}(f)(\alpha) \\
&= \mathrm{Rag}_K(\mathcal{N}_{L/K}(f))(\alpha)
\end{aligned}$$

which proves our claim. From this we deduce in particular that $\mathcal{N}_{L/K}(\mathrm{Ker}(\mathrm{Rag}_L))$ is contained in $\mathrm{Ker}(\mathrm{Rag}_K)$.
We pass now to the proof of the commutativity of the following diagram

$$\begin{array}{ccc}
\mathrm{MCl}(O_L[G]) & \xleftarrow{\Theta_L^{\mathrm{t}}} & \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\bar{G}(-1)], J(\mathbb{Q}^c)\right) \\
\downarrow{\scriptstyle \mathcal{N}_{L/K}} & & \downarrow{\scriptstyle \mathcal{N}_{L/K}} \\
\mathrm{MCl}(O_K[G]) & \xleftarrow{\Theta_K^{\mathrm{t}}} & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\bar{G}(-1)], J(\mathbb{Q}^c)\right).
\end{array}$$

Given $g \in \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\bar{G}(-1)], J(\mathbb{Q}^c)\right)$ and an element $\alpha \in \mathcal{A}_G$, we have

$$\begin{aligned}
\Theta_K^{\mathrm{t}}(\mathcal{N}_{L/K}(g))(\alpha) &= \mathcal{N}_{L/K}(g)\left(\sum_{\bar{s} \in \bar{G}} \langle \alpha, \bar{s} \rangle \bar{s}\right) \\
&= \prod_{\omega \in \Omega_K/\Omega_L} g\left(\left(\sum_{\bar{s} \in \bar{G}} \langle \alpha, \bar{s} \rangle \bar{s}\right)^{\omega^{-1}}\right)^{\omega} \\
&= \prod_{\omega \in \Omega_K/\Omega_L} \left(\prod_{\bar{s} \in \bar{G}} g\left(\bar{s}^{\omega^{-1}}\right)^{\langle \alpha, \bar{s} \rangle}\right)^{\omega} \\
&= \prod_{\omega \in \Omega_K/\Omega_L} \left(\prod_{\bar{t} \in \bar{G}} g\left(\bar{t}\right)^{\langle \alpha, \bar{t}^{\omega} \rangle}\right)^{\omega}
\end{aligned}$$

using the fact that any ω acts as an automorphism. On the other side

$$\begin{aligned}\mathcal{N}_{L/K}(\Theta_L^{\mathrm{t}}(g))(\alpha) &= \prod_{\omega\in\Omega_K/\Omega_L}\Theta_L^{\mathrm{t}}(g)\left(\alpha^{\omega^{-1}}\right)^{\omega}\\ &= \prod_{\omega\in\Omega_K/\Omega_L} g\left(\sum_{\bar{s}\in\bar{G}}\langle\alpha^{\omega^{-1}},\bar{s}\rangle\,\bar{s}\right)^{\omega}\\ &= \prod_{\omega\in\Omega_K/\Omega_L}\left(\prod_{\bar{s}\in\bar{G}} g\left(\bar{s}\right)^{\langle\alpha^{\omega^{-1}},\bar{s}\rangle}\right)^{\omega}\\ &= \prod_{\omega\in\Omega_K/\Omega_L}\left(\prod_{\bar{s}\in\bar{G}} g\left(\bar{s}\right)^{\langle\alpha,\bar{s}^{\omega}\rangle}\right)^{\omega}\end{aligned}$$

where in the last equality we used the relation

$$\langle\alpha^{\omega^{-1}},\bar{s}\rangle = \langle\alpha^{\omega^{-1}},s\rangle = \langle\alpha,s^{\omega}\rangle = \langle\alpha,\overline{s^{\omega}}\rangle = \langle\alpha,\bar{s}^{\omega}\rangle,$$

which one can get using the definition of the action of ω on conjugacy classes, the definition of the Stickelberger pairing for the set of conjugacy classes and property (2.16). This proves the commutativity.
The previous two diagrams combine to prove that the following diagram commutes

$$\begin{array}{ccccc}\mathrm{Cl}(O_L[G]) & \xrightarrow{\mathrm{Rag}_L} & \mathrm{MCl}(O_L[G]) & \xleftarrow{\Theta_L^{\mathrm{t}}} & \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\bar{G}(-1)],J(\mathbb{Q}^{\mathrm{c}})\right)\\ \downarrow{\scriptstyle\mathcal{N}_{L/K}} & & \downarrow{\scriptstyle\mathcal{N}_{L/K}} & & \downarrow{\scriptstyle\mathcal{N}_{L/K}}\\ \mathrm{Cl}(O_K[G]) & \xrightarrow{\mathrm{Rag}_K} & \mathrm{MCl}(O_K[G]) & \xleftarrow{\Theta_K^{\mathrm{t}}} & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\bar{G}(-1)],J(\mathbb{Q}^{\mathrm{c}})\right).\end{array}$$

□

A more precise version of Theorem 0.0.7 of the Introduction now easily follows.

Theorem 4.1.2. *Given a finite group G and a subfield K of a number field L, then*

$$\begin{aligned}\mathcal{N}_{L/K}(\mathrm{Ker}(\mathrm{Rag}_L)) &\subseteq \mathrm{Ker}(\mathrm{Rag}_K)\\ \mathcal{N}_{L/K}(\mathrm{St}(O_L[G])) &\subseteq \mathrm{St}(O_K[G]).\end{aligned}$$

Proof. We have already noted the first inclusion in the proof of Proposition 4.1.1. For the second one it is sufficient to have in mind the definition of the Stickelberger subgroup and use Proposition 4.1.1. □

4.2 Corollaries

The first consequence of Theorem 4.1.2 in the abelian case follows.

Corollary 4.2.1. *Let G be a finite abelian group and let K be a subfield of a number field L. Then $\mathcal{N}_{L/K}(R_{\mathrm{nr}}(O_L[G])) \subseteq R_{\mathrm{nr}}(O_K[G])$ and $\mathcal{N}_{L/K}(R(O_L[G])) \subseteq R(O_K[G])$.*

Proof. This follows from Theorem 4.1.2 and from the equalities in the abelian case of Chapter 2: $R_{\mathrm{nr}}(O_L[G]) = \mathrm{Ker}(\mathrm{Rag}_L)$ (resp. $R_{\mathrm{nr}}(O_K[G]) = \mathrm{Ker}(\mathrm{Rag}_K)$) and $R(O_L[G]) = \mathrm{St}(O_L[G])$ (resp. $R(O_K[G]) = \mathrm{St}(O_K[G])$). □

The following result is valid for any finite group G.

Corollary 4.2.2. *Let G be a finite group and K be a subfield of a number field L, such that $\mathrm{St}(O_K[G]) = 1$. Then for any tame G-Galois L-algebra N, its ring of integers O_N is a stably free $O_K[G]$-module.*

Proof. Clear from Theorem 4.1.2 and from the fact that $[O_N] = 1$ in $\mathrm{Cl}(O_K[G])$ means that O_N is a stably free when seen as an $O_K[G]$-module (see §1.3). □

From this we deduce as an immediate consequence a result of Taylor.

Corollary 4.2.3. *Given a number field L and an abelian tame G-Galois extension N/L, the ring of integers O_N is a free $\mathbb{Z}[G]$-module.*

Proof. It follows from Corollary 4.2.2 with $K = \mathbb{Q}$ and from the fact that, since G is abelian, $R(\mathbb{Z}[G]) = 1$, by Hilbert–Speiser's Theorem. Moreover, note that from the cancellation law (§1.4), in the abelian case, to be a stably free $\mathbb{Z}[G]$-module implies to be free (see Remark 1.4.4). □

Finally, from our result on D_p contained in Chapter 3, we have the following corollary.

Corollary 4.2.4. *Let D_p be a dihedral group of order $2p$, where p is an odd prime number. Given a number field L and a tame D_p-Galois L-algebra N, the ring of integers O_N is a free $\mathbb{Z}[D_p]$-module.*

Proof. The proof is a direct consequence of Theorem 3.2.1, Corollary 4.2.2 and the fact that $\mathbb{Z}[D_p]$ has locally free cancellation. This last claim follows from Theorem 1.4.3, indeed $\mathbb{Q}[D_p]$ satisfies the Eichler condition (see Definition 1.4.2) by the Wedderburn decomposition given in the proof of Lemma 3.2.5. □

Chapter 5

Equidistribution of rings of integers with local splitting behavior

In this chapter the group G will be **abelian** and K, as usual, a number field.

To simplify the notation throughout this chapter, we denote by $A_G(K)$ (resp. $A_G^{\mathrm{t}}(K)$) the set of isomorphism classes of G-Galois K-algebras (resp. tame G-Galois K-algebras) and by $F_G(K)$ (resp. $F_G^{\mathrm{t}}(K)$) the set of isomorphism classes of G-Galois field extensions of K (resp. tame G-Galois field extensions of K). Moreover $A'_G(K)$ (resp. $F'_G(K)$) will denote the set of isomorphism classes of G-Galois K-algebras (resp. field extensions) unramified at every $\mathfrak{p}\big||G|$. We will denote the elements in these sets by $[L]$, where L is an algebra (or field) representative of the class.
Note that $A'_G(K) \subseteq A_G^{\mathrm{t}}(K)$ (resp. $F'_G(K) \subseteq F_G^{\mathrm{t}}(K)$).

Once one knows the structure of $R(O_K[G])$, one may wonder how the G-module structures of the ring of integers of tame G-Galois K-algebras are distributed over the realizable classes, i.e., roughly speaking, given two realizable classes c_1 and c_2, is the number of tame G-Galois K-algebras realizing the two classes asymptotically of the same order of magnitude?
More precisely, given $L \in A_G(K)$, let us denote by $D(L/K)$ the absolute norm of the product of the primes of O_K that ramify in L. Given a class $c \in R(O_K[G])$ and a natural number X, let us write $N_D(c, X)$ for the number of classes $[L]$ in $A_G^{\mathrm{t}}(K)$ such that O_L realizes the class c and $D(L/K) \leq X$. Moreover we denote by $M_D(X)$ the number of classes $[L]$ in $A_G^{\mathrm{t}}(K)$ such that $D(L/K) \leq X$. Then,

when $\lim_{X\to\infty} N_D(c,X)/M_D(X)$ exists, we can define

$$\Pr_A(c) := \lim_{X\to\infty} \frac{N_D(c,X)}{M_D(X)}.$$

Hence our previous question becomes: is $\Pr_A(c)$ independent of the realizable class c?

Adebisi Agboola in [1], using McCulloh's result $R(O_K[G]) = \mathrm{St}(O_K[G])$ (see Chapter 2) and improving a previous result by K. Foster [16], managed to give a positive answer to a slightly modified version of this question.
Let us consider $N'_D(c,X)$ (resp. $M'_D(X)$) obtained considering just the classes $[L] \in A'_G(K)$ in the definition of $N_D(c,X)$ (resp. $M_D(X)$) and let us write

$$\Pr'_A(c) := \lim_{X\to\infty} \frac{N'_D(c,X)}{M'_D(X)}.$$

Then Agboola's result is as follows.

Theorem 5.0.5 ([1, Theorem B])**.** *Let G be a finite abelian group and K a number field. For every $c \in R(O_K[G])$, the limit $\Pr'_A(c)$ exists and it is equal to $1/|R(O_K[G])|$.*

Remark 5.0.6. *Note that every class in $R(O_K[G])$ can be obtained from a G-Galois algebra unramified at the primes dividing $|G|$ (see Theorem B in Chapter 2).*

Moreover, using the fact that every class in $R(O_K[G])$ can be obtained from the ring of integers of a tame G-Galois field extension of K (as McCulloh showed), Agboola also proved that the same result holds if in our definition of $\Pr'_A(c)$ instead of taking classes in $A'_G(K)$ we just consider $F'_G(K)$.

The general result contained in [1] also considers other kinds of "counting functions" different from $D(L/K)$. In particular Agboola showed that for some of them (e.g. using as a counting function the discriminant of L/K) an analogous result to Theorem 5.0.5 is unlikely to hold (actually, in a talk given in Luminy in 2011, he really showed an explicit example of a counting function for which the equidistribution result does not hold). This explains that the equidistribution result depends on the counting function we use (for more details on that see [1]).

As suggested by Agboola in [1], his result has some natural connections with the work [47] by Melanie M. Wood, where she studied the distribution of local

behaviors in abelian G-Galois field extensions. Let us recall the main questions and results of [47].

Given a G-Galois field extension L/K and a finite place $\mathfrak{p}$ of K, we know that

$$\mathfrak{p}O_L \cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^e,$$

where $\mathfrak{P}$ runs over the primes of L over $\mathfrak{p}$, the exponent e is the ramification index of $\mathfrak{p}$ and $|G| = efg$, with f the inertia degree at $\mathfrak{p}$ and g the number of primes $\mathfrak{P}$ over $\mathfrak{p}$ (see [34, Chapter 2]).
Given a pair of natural numbers (e, f) such that ef divides $|G|$, we call $T = (e, f)$ a splitting type and we say that $\mathfrak{p}$ is of type T in L (or L has splitting behavior T at $\mathfrak{p}$), if $\mathfrak{p}$ splits in L with ramification index equal to e and inertia degree f. To simplify the notation, when $\mathfrak{p}$ is of type T in L, we will write $L_{\mathfrak{p}} \equiv T$.

The main question addressed by Wood in [47] is the following: given a prime ideal $\mathfrak{p} \subseteq O_K$, what is the probability that $\mathfrak{p}$ splits in a determined way in a random G-Galois field extension L over K? Or, more precisely, given a splitting type $T = (e, f)$ and setting

$$\mathrm{Pr}_W(T, \mathfrak{p}) := \lim_{X\to\infty} \frac{\sharp\{[L] \in F_G(K) |\, L_{\mathfrak{p}} \equiv T \text{ and } D(L/K) \leq X\}}{\sharp\{[L] \in F_G(K) |\, D(L/K) \leq X\}}, \tag{5.1}$$

where $D(L/K)$ is as above, can we show that it exists and compute $\mathrm{Pr}_W(T, \mathfrak{p})$?

The first problem one encounters in the study of this question is given by the fact that not every splitting type can always be obtained (e.g. if $G = C_8$, the cyclic group of order 8, $L/\mathbb{Q}$ is never inert at the prime 2). This problem has been already studied in detail and a result due to Grunwald–Wang (see [45] and also [3, Chapter 10]) describes, given a finite abelian group G and a finite place $\mathfrak{p}$ of K, all the possible splitting types which are "realizable" as splitting pattern of $\mathfrak{p}$ in a G-Galois K-algebra. We call these splitting types, realizable splitting types at $\mathfrak{p}$ (without making explicit the dependence on G and K).
In particular, given an abelian finite group G and a number field K, there is a finite set of "problematic" primes S_0, for which not every splitting type occurs. This finite set of primes S_0 is defined in the following way: let s be the maximal natural number such that $z_s := \zeta_{2^s} + \zeta_{2^s}^{-1}$ (where ζ_{2^s} denotes a primitive 2^s-th root of unity) belongs to K; then, if 2^{s+1} does not divide the exponent of G, the set S_0 is the empty, otherwise S_0 is the set of all primes $\mathfrak{p}'$ of K dividing the ideal $2O_K$ such that none of -1, $2 + z_s$ and $-2 - z_s$ are squares in $K_{\mathfrak{p}'}$ (this definition

is taken from [47, §2.2]). Note that, if G is of odd order, the set S_0 is empty.
For the precise result explaining which realizable splitting types at the primes contained in S_0 do not occur, we refer to [3, Chapter 10].

Aware of all the realizable splitting types, Wood proved, as corollary of a more general theorem (see [47, Theorem 2.1]), the following result.

Theorem 5.0.7. *Let G be a finite abelian group, let K be an algebraic number field and let $\mathfrak{p}$ be a prime of K not belonging to S_0, if $|S_0| \neq 1$. Then, given $T = (e, f)$ and $T' = (e', f')$ two realizable (via Grunwald-Wang) splitting types at $\mathfrak{p}$, the following formula holds:*

$$\frac{\mathrm{Pr}_W(T, \mathfrak{p})}{\mathrm{Pr}_W(T', \mathfrak{p})} = \frac{C_T / N_{K/\mathbb{Q}}(\mathfrak{p}^{\delta(T)})}{C_{T'} / N_{K/\mathbb{Q}}\left(\mathfrak{p}^{\delta(T')}\right)},$$

where $C_T := \sharp\{$isom. classes of G-Galois $K_{\mathfrak{p}}$-algebras giving the splitting type $T\}$ (analogously for $C_{T'}$), the map $N_{K/\mathbb{Q}}$ is the usual norm map and $\delta(-)$ is defined to be equal to 1 on ramified splitting types ($e > 1$), while equal to 0 on unramified splitting types ($e = 0$).

This result follows as a special case of [47, Corollary 2.2], obtained by restricting it to the single prime $\mathfrak{p}$ and using as counting function the absolute norm of the product of ramified primes (see [47, §2.1]).

Moreover she also proved the next result.

Theorem 5.0.8. *Let S be a finite set of finite places $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n\}$ of K disjoint from S_0, if $|S_0| \neq 1$. Given $T_S := \{T_1, \ldots, T_n\}$ a collection of n splitting types, then*

$$\mathrm{Pr}_W\left(T_S\right) = \prod_{i=1}^{n} \mathrm{Pr}_W(T_i, \mathfrak{p}_i);$$

where $\mathrm{Pr}_W\left(T_S\right)$ denotes the probability, as in (5.1), that a G-Galois field extension L/K is such that $L_{\mathfrak{p}_i} \equiv T_i$ for all $i = 1, \ldots, n$.

This result follows as a special case of [47, Corollary 2.4].

Wood also considered other kinds of counting functions different from $D(L/K)$ and she extended her results to the set of functions that she called "fair" counting functions (for details see [47, page 108]).

We immediately see that the probabilities considered by Agboola and Wood have some connections and a first question arises: are they "independent"?

Namely, given $c \in R(O_K[G])$, a finite place $\mathfrak{p}$ of K and a realizable splitting type T at $\mathfrak{p}$, we can define

$$\Pr(T, \mathfrak{p}, c) := \lim_{X \to \infty} \frac{\sharp\{[L] \in F'_G(K) |\, L_{\mathfrak{p}} \equiv T,\, [O_L] = c,\, D(L/K) \leq X\}}{\sharp\{[L] \in F'_G(K) |\, D(L/K) \leq X\}}. \tag{5.2}$$

Note that, in the definition, it does not matter whether or not $\mathfrak{p}$ divides $|G|$.
Then, does the limit $\Pr(T, \mathfrak{p}, c)$ exist?
Moreover, let $\Pr_W\left((T, \mathfrak{p}) \,\middle|\, L \text{ unr. at all } \mathfrak{p}' \middle| |G|\right)$ denote the conditional probability defined as the quotient

$$\Pr_W\left(\mathfrak{p} \text{ of type } T \,\&\, L \text{ unr. at all } \mathfrak{p}' \middle| |G|\right) / \Pr_W\left(L \text{ unr. at all } \mathfrak{p}' \middle| |G|\right), \tag{5.3}$$

where $\Pr_W\left(\mathfrak{p} \text{ of type } T \,\&\, L \text{ unr. at all } \mathfrak{p}' \middle| |G|\right)$ denotes the probability (as in (5.1)) that a random G-Galois field extension of K has splitting behavior T at $\mathfrak{p}$ and is unramified at all primes of K dividing $|G|$, while $\Pr_W\left(L \text{ unr. at all } \mathfrak{p}' \middle| |G|\right)$ denotes the probability (as in (5.1)) that a random G-Galois field extension of K is unramified at all primes of K dividing $|G|$. Then if $\Pr(T, \mathfrak{p}, c)$ exists, does the equality

$$\Pr(T, \mathfrak{p}, c) = \Pr_W\left((T, \mathfrak{p}) \,\middle|\, L \text{ unr. at all } \mathfrak{p}' \middle| |G|\right) \cdot \Pr'_A(c) \tag{5.4}$$

hold?

The study of this question restricted to the totally split case is the main subject of this chapter, i.e. we focus our attention on the splitting type $T = (1, 1)$ (which is always realizable at every prime, for every abelian group G and number field K). In Proposition 5.3.1 we will find a sufficient and necessary condition such that (5.4) holds when $T = (1, 1)$. To reach this result the main effort will consist in determining $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, the set of realizable classes given by tame G-Galois K-algebras totally split at a given prime $\mathfrak{p}$. In particular in Theorem 5.1.11 we will give a description of this set (actually group) in terms of a modified version of the original Stickelberger subgroup $\mathrm{St}(O_K[G])$.
A natural question arises: is $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ the same as $R(O_K[G])$? It seems reasonable to expect that, for every abelian group G, each realizable class can be realized by a G-Galois K-algebra totally split at every prescribed finite set of primes, by analogy with the statement where "totally split" is replaced with "unramified" (see Theorem B). This will lead us to the following two conjectures (note that the second one is clearly stronger than the first one):

Conjecture 1. *Let K and G be as before. For every prime $\mathfrak{p}$ of K, we have*

$$R_{\mathrm{ts},\mathfrak{p}}(O_K[G]) = R(O_K[G]).$$

Conjecture 2. *Let K and G be as before. Given a finite set S of primes of K, let us denote by $R_{\mathrm{ts},S}(O_K[G])$ the set of classes in $\mathrm{Cl}(O_K[G])$ given by tame G-Galois K-algebras totally split at every prime $\mathfrak{p}$ in S. Then, for every finite set S of primes of K, we have $R_{\mathrm{ts},S}(O_K[G]) = R(O_K[G])$.*

We will discuss these conjectures in Section 5.3.

5.1 Realizable classes totally split at $\mathfrak{p}$

We have seen that $R(O_K[G])$ is defined as the classes in $\mathrm{Cl}(O_K[G])$ which can obtained from the ring of integers of tame G-Galois K-algebras. This set, since we are considering G abelian, is a group, described in terms of idèles by the work of McCulloh (Chapter 2, Theorem B).

Given a finite place $\mathfrak{p}$ of K, we may restrict our attention to the classes in $\mathrm{Cl}(O_K[G])$ which can be obtained from tame G-Galois K-algebras with a particular splitting behavior at $\mathfrak{p}$. Given a splitting type T, we write

$$R_{T,\mathfrak{p}}(O_K[G]) := \{[O_L] \in \mathrm{Cl}(O_K[G]) | \, [L] \in A_G^{\mathrm{t}}(K) \text{ and } L_{\mathfrak{p}} \equiv T\}.$$

In the same way, given $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ a finite set of finite places of K and taking $T_S := \{T_1, \ldots, T_n\}$ a collection of n splitting types, we write

$$R_{T_S}(O_K[G]) := \{[O_L] \in \mathrm{Cl}(O_K[G]) | \, [L] \in A_G^{\mathrm{t}}(K) \text{ and } L_{\mathfrak{p}_i} \equiv T_i, \, \forall \, i = 1, \ldots, n\}.$$

In our work we are going to consider the totally split case, i.e. we will focus our attention on the splitting type decomposition $T = (1, 1)$. Given a finite place $\mathfrak{p}$, we will denote $R_{(1,1),\mathfrak{p}}(O_K[G])$ with the more intuitive notation $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$.

In this section we will modify McCulloh's proof of Theorem B in order to give an idelic description of $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ analogous to the one given for $R(O_K[G])$ in Chapter 2, in terms of the Stickelberger subgroup $\mathrm{St}(O_K[G])$.

5.1.1 Resolvends of local totally split extensions

Given a G-Galois K-algebra K_h (see §1.9) and a finite place $\mathfrak{p}$ of K, by (1.12) and (1.13), we have

$$K_{h,\mathfrak{p}} := K_h \otimes_K K_{\mathfrak{p}} \cong (K_{\mathfrak{p}})_{h_{\mathfrak{p}}} = \mathrm{Map}_{\Omega_{\mathfrak{p}}}\left({}^{h_{\mathfrak{p}}}G, K_{\mathfrak{p}}^{\mathrm{c}}\right) \cong \prod_{i=1}^{[G:h_{\mathfrak{p}}(\Omega_{\mathfrak{p}})]} (K_{\mathfrak{p}}^{\mathrm{c}})^{\mathrm{Ker}(h_{\mathfrak{p}})}.$$

By definition K_h is totally split at $\mathfrak{p}$ if and only if $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}} \cong \prod_{i=1}^{|G|} K_{\mathfrak{p}}$, i.e. if and only if the map $h_{\mathfrak{p}}$ is trivial. Thanks to this remark and Proposition 2.1.5 we can now prove the following result.

Proposition 5.1.2 (NIBG totally split case)**.** *Given $a_{\mathfrak{p}} \in (K_{\mathfrak{p}})_{h_{\mathfrak{p}}}$, we have*

$$a_{\mathfrak{p}} \textit{ is a NIBG and } (K_{\mathfrak{p}})_{h_{\mathfrak{p}}}/K_{\mathfrak{p}} \textit{ is } \textbf{\textit{totally split}} \iff r_G(a_{\mathfrak{p}}) \in O_{K,\mathfrak{p}}[G]^{\times}.$$

Proof. ($\Longrightarrow$) Since the extension is totally split we know that $a_{\mathfrak{p}}(s) \in K_{\mathfrak{p}},\ \forall\, s \in G$ and hence $r_G(a_{\mathfrak{p}}) \in K_{\mathfrak{p}}[G]$. Thus from Proposition 2.1.5, the resolvend $r_G(a_{\mathfrak{p}})$ belongs to $K_{\mathfrak{p}}[G] \cap O_{K,\mathfrak{p}}^{\mathrm{c}}[G]^{\times}$; it remains to show that $K_{\mathfrak{p}}[G] \cap O_{K,\mathfrak{p}}^{\mathrm{c}}[G]^{\times} = O_{K,\mathfrak{p}}[G]^{\times}$. One implication is trivial, for the other one let us consider $\sum_{s\in G} a_s s \in K_{\mathfrak{p}}[G] \cap O_{K,\mathfrak{p}}^{\mathrm{c}}[G]^{\times}$, we know that there is $\sum_{s\in G} b_s s \in O_{K,\mathfrak{p}}^{\mathrm{c}}[G]^{\times}$ such that the product $(\sum_{s\in G} a_s s)(\sum_{s\in G} b_s s)$ is equal to 1. If we enumerate the elements of G as $\{s_1 = 1, s_2, \ldots, s_{|G|}\}$, to find the inverse $\sum_{s\in G} b_s s$ is equivalent, by linear algebra, to solve the system in the variables $x_1, x_2, \ldots, x_{|G|}$ which follows:

$$A \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{|G|} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

where $A = (a_{i,j})_{1\le i,j\le |G|} \in \mathrm{GL}_{|G|}(K_{\mathfrak{p}})$ with $a_{i,j} = a_s$, such that s is the only element in G satisfying $s \cdot s_j = s_i$. Thus we understand that $\sum_{s\in G} b_s s$ actually belongs to $K_{\mathfrak{p}}[G]$.
Moreover considering the intersection at each coefficient, we have $K_{\mathfrak{p}}[G] \cap O_{K,\mathfrak{p}}^{\mathrm{c}}[G] = O_{K,\mathfrak{p}}[G]$, which shows that $\sum_{s\in G} b_s s \in O_{K,\mathfrak{p}}[G]$ and $\sum_{s\in G} a_s s \in O_{K,\mathfrak{p}}[G]^{\times}$, as we wanted to prove.

($\Longleftarrow$) From Proposition 2.1.5, we know that $a_{\mathfrak{p}}$ is a NIBG of the unramified G-Galois algebra $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}}/K_{\mathfrak{p}}$ (where $h_{\mathfrak{p}} \in \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G\right)$). Moreover, since $r_G(a_{\mathfrak{p}}) \in O_{K,\mathfrak{p}}[G]^{\times}$, we have $a_{\mathfrak{p}}(s) \in O_{K,\mathfrak{p}},\ \forall\, s \in G$. Thus, since we also have $(K_{\mathfrak{p}})_{h_{\mathfrak{p}}} =$

$K_\mathfrak{p}[G] \cdot a_\mathfrak{p}$, this implies that $(K_\mathfrak{p})_{h_\mathfrak{p}}$ is equal to a finite product of copies of $K_\mathfrak{p}$ and $h_\mathfrak{p}$ is trivial, so totally split. □

Remark 5.1.3. *In the first part of the proof, the non trivial inclusion*

$$K_\mathfrak{p}[G] \cap O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times \subseteq O_{K,\mathfrak{p}}[G]^\times$$

could also be proved (maybe more easily) in the following way: if $\alpha := \sum_{s\in G} a_s s \in K_\mathfrak{p}[G] \cap O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times$*, then, since it is a unit, the multiplication by* α *gives an isomorphism* $m_\alpha : O^{\mathrm{c}}_{K,\mathfrak{p}}[G] \longrightarrow O^{\mathrm{c}}_{K,\mathfrak{p}}[G]$ *which induces an isomorphism* $\hat{m}_\alpha : K^{\mathrm{c}}_\mathfrak{p}[G] \longrightarrow K^{\mathrm{c}}_\mathfrak{p}[G]$*. By restriction, since* $\alpha \in K_\mathfrak{p}[G]$*, we get an isomorphism* $\overline{m_\alpha} : K_\mathfrak{p}[G] \longrightarrow K_\mathfrak{p}[G]$*. Hereby, looking at the intersection we have that the multiplication by* α *gives an automorphism of* $O_{K,\mathfrak{p}}[G]$*, which says that actually* $\alpha \in O_{K,\mathfrak{p}}[G]^\times$*.*

Analogously to (2.6), the previous proposition also tells us that

$$\begin{aligned} O_{K,\mathfrak{p}}[G]^\times &= \left\{ r_G(a_\mathfrak{p}) |\, a_\mathfrak{p} \text{ NIBG for } (K_\mathfrak{p})_{h_\mathfrak{p}}, \text{ where } h_\mathfrak{p} \in \mathrm{Hom}(\Omega_\mathfrak{p}, G) \text{ is trivial} \right\}, \quad (5.5) \\ \frac{O_{K,\mathfrak{p}}[G]^\times}{G} &= \left\{ \mathrm{rag}(r_G(a_\mathfrak{p})) |\, a_\mathfrak{p} \text{ NIBG for } (K_\mathfrak{p})_{h_\mathfrak{p}}, \text{ where } h_\mathfrak{p} \in \mathrm{Hom}(\Omega_\mathfrak{p}, G) \text{ is trivial} \right\}. \end{aligned}$$

Remark 5.1.4. *The previous equality could also be seen from the exact sequence (2.5), namely the set of reduced resolvends of NIBG for totally split* G*-Galois algebras over* $K_\mathfrak{p}$ *is the kernel of the connecting homomorphism* $\mathcal{H}(O_{K,\mathfrak{p}}[G]) \longrightarrow H^1(\Omega^{\mathrm{nr}}_\mathfrak{p}, G)$*. So by exactness it coincides with* $\mathrm{rag}(O_{K,\mathfrak{p}}[G]^\times) = O_{K,\mathfrak{p}}[G]^\times / G$*.*

For future use, we also prove the following lemma.

Lemma 5.1.5. *Given a finite group* G*, then* $O_{K,\mathfrak{p}}[G]^\times / G \subseteq \mathcal{H}(O_{K,\mathfrak{p}}[G])$ *with finite index.*

Proof. By the previous remark, considering the exact sequence (2.5), if we show that $H^1(\Omega^{\mathrm{nr}}_\mathfrak{p}, G)$ is finite, we have the claim. It is sufficient to remark that $\Omega^{\mathrm{nr}}_\mathfrak{p}$ is the procyclic group generated by the Frobenius automorphism of $K^{\mathrm{nr}}_\mathfrak{p}/K_\mathfrak{p}$ to see that $|H^1(\Omega^{\mathrm{nr}}_\mathfrak{p}, G)| = |\mathrm{Hom}(\Omega^{\mathrm{nr}}_\mathfrak{p}, G)| = |G|$. □

Remark 5.1.6. *Note that Proposition 5.1.2 and Lemma 5.1.5 are valid even if* G *is not abelian.*

Remark 5.1.7. *Another way to prove the previous lemma, which is valid just in the abelian case, is as follows: since G is finite and abelian, it has finite exponent denoted by m, then it is easy to see that*

$$\mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G) = \mathrm{Hom}\left(\Omega_{\mathfrak{p}}^{(\mathrm{nrAB},m)}, G\right),$$

where $\Omega_{\mathfrak{p}}^{(\mathrm{nrAB},m)}$ is the Galois group over $K_{\mathfrak{p}}$ of the maximal unramified abelian extension of exponent m of $K_{\mathfrak{p}}$, known to be finite by local class field theory.

5.1.8 The subgroup $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$

Analogously to Chapter 2 and in the light of the results above, we are going to modify the definition of $\mathrm{St}(O_K[G])$ in order to have a suitable subgroup which will be equal to $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$.

Given a finite place $\mathfrak{p}$ of K, we write

$$\mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G]) := \left(\prod_{\mathfrak{p}'\neq\mathfrak{p}} \mathcal{H}(O_{K,\mathfrak{p}'}[G])\right) \cdot (O_{K,\mathfrak{p}}[G]^{\times}/G) \tag{5.6}$$

and we define

$$\mathrm{MCl}_{\mathrm{ts},\mathfrak{p}}(O_K[G]) := \frac{\mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)}{\mathcal{H}(K[G]) \cdot \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])}.$$

Thus we can consider the group homomorphism

$$\mathrm{Rag}_{\mathrm{ts},\mathfrak{p}} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{MCl}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$$

and the natural map induced by $\Theta_G^{\mathrm{t}} : J(K\Lambda) \longrightarrow \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)$

$$\Theta_{G,\mathrm{ts},\mathfrak{p}}^{\mathrm{t}} : J(K\Lambda) \longrightarrow \mathrm{MCl}_{\mathrm{ts},\mathfrak{p}}(O_K[G]).$$

Analogously to §2.5, we define

$$\mathrm{St}_{\mathrm{ts},\mathfrak{p}}(O_K[G]) := \mathrm{Rag}_{\mathrm{ts},\mathfrak{p}}^{-1}(\mathrm{Im}(\Theta_{G,\mathrm{ts},\mathfrak{p}}^{\mathrm{t}})). \tag{5.7}$$

Defining $F^{\mathfrak{p}} \subseteq F$ (see (2.22)), as the subset of elements $f \in F$ which are trivial at the finite prime $\mathfrak{p}$ (i.e. $f_{\mathfrak{p}} = 1$), we get the following modified version of Theorem 2.6.2.

Theorem 5.1.9. *Let K_h/K be a G-Galois K-algebra and take b a normal basis generator. Then, K_h/K is tame and totally split at $\mathfrak{p}$ if and only if there exist*

$c \in J(K[G])$, $f \in F^{\mathfrak{p}}$ and $w \in \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ such that

$$\mathrm{rag}(r_G(b)) = (\mathrm{rag}(c))^{-1}\Theta^{\mathrm{t}}_G(f)w.$$

Moreover c is a representative of the class $[O_{K_h}]$, the element f is unique and K_h ramifies at $\mathfrak{p}'$ if and only if $f_{\mathfrak{p}'} \neq 1$.

Proof. The proof is essentially the same of Theorem 2.6.2, where we now control the totally split condition using Proposition 5.1.2. □

In order to give an analog of Theorem B, proving in particular that $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ is again a subgroup of $\mathrm{Cl}(O_K[G])$, we have first to introduce a modified version of the approximation result given by Proposition 2.2.9.

Theorem 5.1.10. *For every finite prime $\mathfrak{p}$ of K, there exists a natural number $N_{\mathfrak{p}}$, such that*

$$\mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, (1+\mathfrak{p}^{N_{\mathfrak{p}}}O^c_{K,\mathfrak{p}}) \cap (O^c_{K,\mathfrak{p}})^\times\right) \subseteq O_{K,\mathfrak{p}}[G]^\times/G \subseteq \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, (O^c_{K,\mathfrak{p}})^\times\right).$$

We postpone the proof of this theorem, which is a bit technical, to the next section, we will now rather show how to deduce from this an analog of Theorem B (this corresponds to Theorem 0.0.8 in the Introduction).

Theorem 5.1.11 (Realizable classes totally split at $\mathfrak{p}$)**.** *Let G be a finite abelian group and let K be a number field. For every finite prime $\mathfrak{p}$ of K, we have*

$$R_{\mathrm{ts},\mathfrak{p}}(O_K[G]) = \mathrm{St}_{\mathrm{ts},\mathfrak{p}}(O_K[G]).$$

Moreover every class can be obtained from a G-Galois field extension unramified at a preassigned finite set of finite primes of K.

Proof. One inclusion is clear from Theorem 5.1.9.
For the other one suppose that we have $c \in J(K[G])$ such that $\mathrm{rag}(c) = b\cdot\Theta^{\mathrm{t}}_G(g)\cdot w$, with $b \in \mathcal{H}(K[G])$, $g \in J(K\Lambda)$ and $w \in \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$. Then, using Proposition 2.6.3 with an integral ideal $\mathfrak{m}$ divisible by a sufficiently high power of $|G|$ and of the ideal $\mathfrak{p}$ (i.e. $\mathfrak{p}^{N_{\mathfrak{p}}}$ where $N_{\mathfrak{p}}$ is given by Theorem 5.1.10), we find an element $f \in F^{\mathfrak{p}}$ such that $g \equiv f \bmod ((K\Lambda)^\times \cdot U'_{\mathfrak{m}}(\Lambda))$. We can find f really in $F^{\mathfrak{p}}$ using the property of Proposition 2.6.3 which explains that f can be chosen with support disjoint from any preassigned finite set of finite primes. Then, by Theorem 5.1.10,

we get $\Theta^{\mathrm{t}}_G(g) \equiv \Theta^{\mathrm{t}}_G(f) \bmod \mathcal{H}(K[G]) \cdot \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$. This, applying Theorem 5.1.9, allows us to deduce that

$$\mathrm{rag}(c) = b' \cdot \Theta^{\mathrm{t}}_G(f) \cdot w'$$

with $b' \in \mathcal{H}(K[G])$, $w' \in \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ and $f \in F^{\mathfrak{p}}$.
The proof of the second statement remains the same as in Theorem B. □

Remark 5.1.12. *From the last assertion, we see that in the definition of the set $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, if instead of taking the classes $[L]$ in $A^{\mathrm{t}}_G(K)$ we consider just the classes $[L]$ in $F^{\mathrm{t}}_G(K)$ (or even $F'_G(K)$) the group does not change.*

Remark 5.1.13. *If instead of considering a single prime $\mathfrak{p}$, we take S a finite set of finite primes of K. We can naturally define*

$$\mathcal{U}_{\mathrm{ts},S}(O_K[G]) := \left(\prod_{\mathfrak{p}\notin S} \mathcal{H}(O_{K,\mathfrak{p}}[G])\right) \cdot \prod_{\mathfrak{p}\in S} (O_{K,\mathfrak{p}}[G]^{\times}/G)$$

and, analogously as above, we define the associated group $\mathrm{St}_{\mathrm{ts},S}(O_K[G])$.
If $R_{\mathrm{ts},S}(O_K[G])$ denotes the set of realizable classes given by tame G-Galois K-algebras which are totally split at every prime in S, we can generalize the proof of Theorem 5.1.11 and get $R_{\mathrm{ts},S}(O_K[G]) = \mathrm{St}_{\mathrm{ts},S}(O_K[G])$ (with G abelian of course!).

Remark 5.1.14. *In the non-abelian case, thanks to Remark 5.1.6, an analog of Theorem A holds. It is sufficient to extend the definition of $\mathrm{St}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ to the non-abelian case.*
Let G be a finite group (not necessarily abelian). Given a finite place $\mathfrak{p}$ of K, we write

$$\mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G]) := \left(\prod_{\mathfrak{p}'\neq\mathfrak{p}} \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}'}[G]))\right) \cdot \widetilde{\mathrm{Det}}(O_{K,\mathfrak{p}}[G]^{\times}/G)$$

and we define

$$\mathrm{MCl}_{\mathrm{ts},\mathfrak{p}}(O_K[G]) := \frac{\mathrm{Hom}_{\Omega}(\mathcal{A}_G, J(K^{\mathrm{c}}))}{\widetilde{\mathrm{Det}}(\mathcal{H}(K[G])) \cdot \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])}.$$

Then if $\mathrm{St}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ is defined likewise to the abelian situation (5.7), an analog of Theorem A follows.

Theorem 5.1.15. *Let G be a finite group and let K be a number field, then for every finite place $\mathfrak{p}$ of K, we have*

$$R_{\mathrm{ts},\mathfrak{p}}(O_K[G]) \subseteq \mathrm{St}_{\mathrm{ts},\mathfrak{p}}(O_K[G]).$$

The proof remains exactly the same of Theorem A, imposing the totally split condition via the description of resolvends given in the previous part.

5.1.16 Proof of Theorem 5.1.10

We pass now to the technical proof of Theorem 5.1.10. The proof is based on the properties of profinite groups and the techniques differ from the ones used by McCulloh for proving Proposition 2.2.9.

Before going into details we need to recall three lemmas on profinite groups which will be useful in the proof.

Lemma 5.1.17. *Given M and N profinite groups and a homomorphism $\psi : M \to N$, if ψ is continuous and with finite cokernel, then it is an open map.*

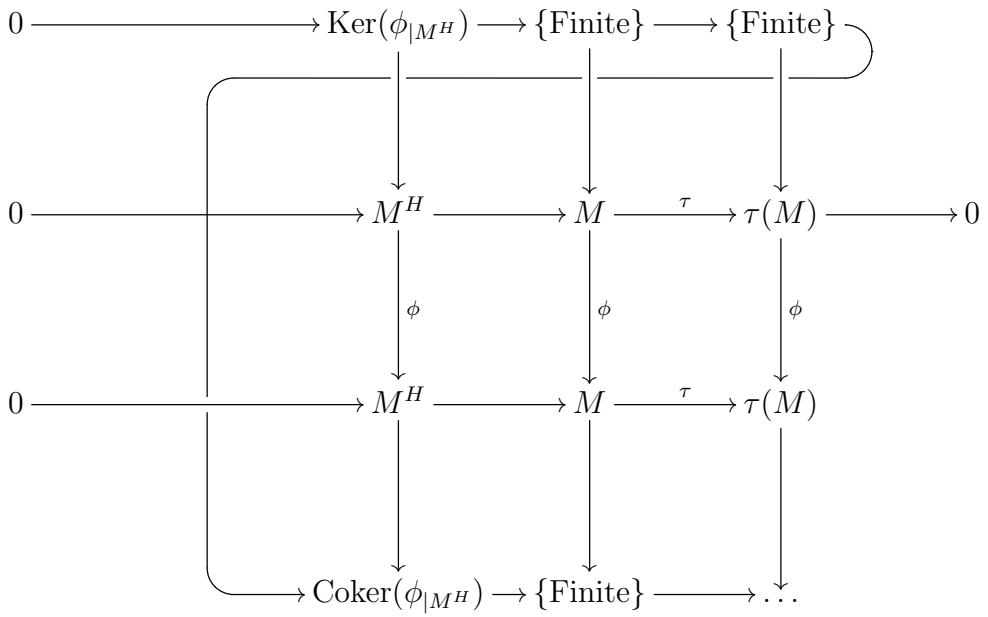
Proof. If we take an open subgroup $M_0 \subseteq M$, then it is closed and of finite index (property of profinite groups). Since M_0 is closed in a compact space, it is compact, as is its image under the continuous ψ. Moreover N is Hausdorff, so we deduce that $\psi(M_0)$ is a closed subgroup of N (compact in a Hausdorff space). Since $M_0 \subseteq M$ with finite index, we have $\psi(M_0) \subseteq \psi(M)$ with finite index and, since the cokernel is finite, we see that $\psi(M_0) \subseteq N$ with finite index.
Finally we have shown that $\psi(M_0)$ is a closed subgroup of finite index in N and so, again using the equivalence for profinite groups, it is open, as we wanted to show. □

Lemma 5.1.18. *Let M be a profinite abelian group and H a finitely generated group acting continuously on it. Given a continuous H-equivariant endomorphism $\phi : M \to M$ with finite kernel and cokernel, its restriction to the subgroup of fixed elements M^H is again continuous and has finite kernel and cokernel.*

Proof. Let $H = \langle s_1, \dots, s_t \rangle$, we can then consider the map $\tau : M \to M^t$ (where M^t denotes the direct product of t copies of M) which sends m to $\tau(m) := (s_1 m - m, \dots, s_t m - m)$ (where M is considered with the additive structure). We can then consider the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M^H & \longrightarrow & M & \xrightarrow{\tau} & \tau(M) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & M^H & \longrightarrow & M & \xrightarrow{\tau} & \tau(M) & \longrightarrow & 0 \end{array}$$

and applying the Snake Lemma we get



which shows our claim. □

Now given M and H as before, for every $n \in \mathbb{N}$ we can consider the continuous H-equivariant automorphism $n : M \to M$ which sends m to m^n (it is continuous since M is a topological group and the multiplication is continuous by definition). Supposing that the cokernel of this map is finite, the next lemma will show that M^H has the property that every finite index subgroup is open.

Lemma 5.1.19. *Let M be, as above, a profinite group with the additional property that for every $n \in \mathbb{N}$ the quotient M/M^n is finite, then every subgroup of M^H of finite index is open in M^H.*

Proof. From the previous two lemmas we see that for every $n \in \mathbb{N}$, the map $n : M^H \to M^H$, previously defined, is open. So, given a subgroup $M_0 \subseteq M^H$ with finite index r, we have $\left(M^H\right)^r \subseteq M_0$. Since $\left(M^H\right)^r$ is open in M^H it will contain a neighborhood of 1 and so the same holds for M_0, which as a consequence is open in M^H, by the structure of topological groups. □

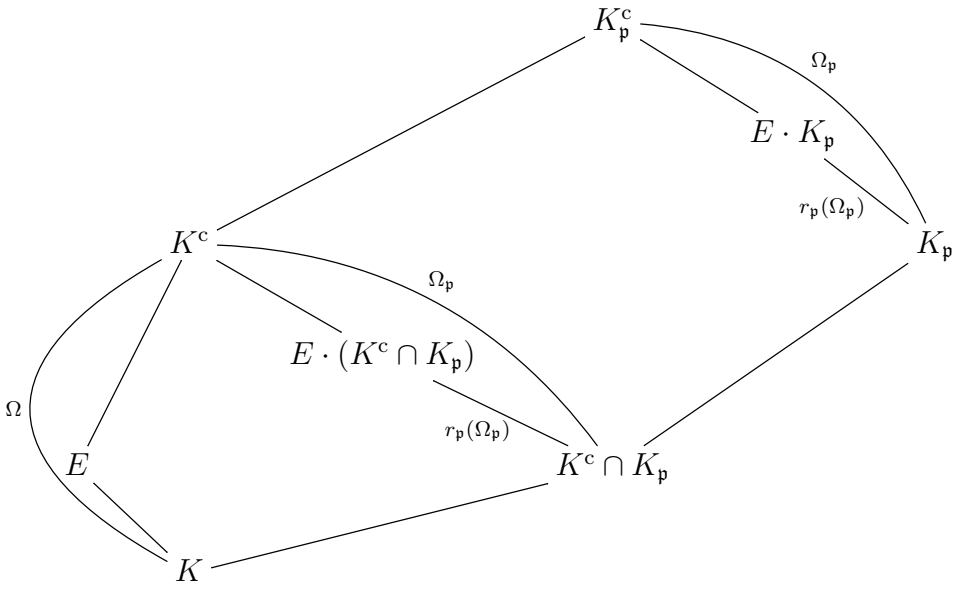
Using these lemmas we can now proceed to the proof of Theorem 5.1.10, but before doing it, let us make the following remark.

Remark 5.1.20. *(Reduction to the finite case.) Looking at* $\mathrm{Hom}_{\Omega_\mathfrak{p}}\left(\mathcal{A}_G, (O^c_{K,\mathfrak{p}})^\times\right)$*, roughly speaking and similarly to §1.7.1, we would like to reduce its definition to*

a finite context.
Let us consider the number field E containing K and all the values of the characters of G; since G is finite, the extension E/K is finite and Galois. So, considering the restriction map $r : \Omega \longrightarrow \mathrm{Gal}(E/K)$, in the definition of the group $\mathrm{Hom}_{\Omega_\mathfrak{p}}\left(\mathcal{A}_G, (O^c_{K,\mathfrak{p}})^\times\right)$ we can just consider the finite group $r_\mathfrak{p}(\Omega_\mathfrak{p})$ (where $r_\mathfrak{p} = r \circ i_\mathfrak{p}$) and we see that

$$\mathrm{Hom}_{\Omega_\mathfrak{p}}\left(\mathcal{A}_G, (O^c_{K,\mathfrak{p}})^\times\right) = \mathrm{Hom}_{r_\mathfrak{p}(\Omega_\mathfrak{p})}\left(\mathcal{A}_G,\, O_L^\times\right) \ ,$$

where L is a finite extension of $K_\mathfrak{p}$ (in particular $L = E \cdot K_\mathfrak{p}$, the compositum of E and $K_\mathfrak{p}$, and $r_\mathfrak{p}(\Omega_\mathfrak{p}) \cong \mathrm{Gal}(E \cdot K_\mathfrak{p}/K_\mathfrak{p})$). Just to be clear, here is a diagram representation:



Finally, we can now write down the proof of Theorem 5.1.10.

Proof of Theorem 5.1.10. As explained in Remark 5.1.20,

$$\mathrm{Hom}_{\Omega_\mathfrak{p}}\left(\mathcal{A}_G, (O^c_{K,\mathfrak{p}})^\times\right) = \mathrm{Hom}_{r_\mathfrak{p}(\Omega_\mathfrak{p})}\left(\mathcal{A}_G,\, O_L^\times\right)$$

where L is a finite extension of $K_\mathfrak{p}$ and $r_\mathfrak{p}(\Omega_\mathfrak{p})$ is finite.
We would like to apply Lemma 5.1.19, where now $M = \mathrm{Hom}\left(\mathcal{A}_G, O_L^\times\right)$ and $H = r_\mathfrak{p}(\Omega_\mathfrak{p})$. The fact that $\mathrm{Hom}\left(\mathcal{A}_G, O_L^\times\right)$ is profinite follows from the fact that it can be written as a finite product of copies of $O_L^\times$ (since $\mathcal{A}_G$ is a finitely generated abelian group). If we look at $M^n = \left(\mathrm{Hom}\left(\mathcal{A}_G, O_L^\times\right)\right)^n$ for every $n \in \mathbb{N}$, we have $\left(\mathrm{Hom}\left(\mathcal{A}_G, O_L^\times\right)\right)^n = \mathrm{Hom}\left(\mathcal{A}_G, \left(O_L^\times\right)^n\right)$ and so we see that M/M^n is finite since $(O_L)^\times / \left((O_L)^\times\right)^n$ is (property of local fields). Thus all hypotheses of Lemma 5.1.19

are satisfied and, combining it with Corollary 5.1.5, we see that $O_{K,\mathfrak{p}}[G]^\times/G$ is open in $\mathrm{Hom}_{r_{\mathfrak{p}}(\Omega_{\mathfrak{p}})}\left(\mathcal{A}_G,\, O_L^\times\right) = \mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, (O^c_{K,\mathfrak{p}})^\times\right)$. Since the set $\{(1+\mathfrak{p}^s O^c_{K,\mathfrak{p}}) \cap (O^c_{K,\mathfrak{p}})^\times\}_{s\in\mathbb{N}}$ forms a fundamental system of neighborhoods of 1 in $(O^c_{K,\mathfrak{p}})^\times$, the open subgroup $O_{K,\mathfrak{p}}[G]^\times/G$ has to contain an open neighborhood of the unity and so there exists a power $\mathfrak{p}^{N_{\mathfrak{p}}}$ such that

$$\mathrm{Hom}_{\Omega_{\mathfrak{p}}}\left(\mathcal{A}_G, (1+\mathfrak{p}^{N_{\mathfrak{p}}} O^c_{K,\mathfrak{p}}) \cap (O^c_{K,\mathfrak{p}})^\times\right) \subseteq O_{K,\mathfrak{p}}[G]^\times/G;$$

which gives the proof. □

5.2 Equidistribution for $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$

Once we know the idelic structure of the realizable classes given by G-Galois K-algebras totally split at a given prime $\mathfrak{p}$ of K, we would like to obtain an analog of Theorem 5.0.5 for the group of classes $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$. More precisely, we would like to prove that $\Pr((1,1),\mathfrak{p},c)$ (see (5.2)), does not depend on the class $c \in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$.

At the beginning we shall work with a general counting function $\mathcal{W}$ (a precise definition will be given in §5.2.4) and not just D as in the introduction of the chapter. Given X a natural number; we denote by $\mathrm{N}_{\mathcal{W},\mathrm{ts},\mathfrak{p}}(c,X)$ the number of classes $[L]$ in $A_G^{\mathrm{t}}(K)$, such that L/K totally split at $\mathfrak{p}$, its ring of integers realizes the class c and such that $\mathcal{W}(L/K) \leq X$. Moreover $\mathrm{M}_{\mathcal{W}}(X)$ will denote the number of classes $[L]$ in $A_G^{\mathrm{t}}(K)$ such that $\mathcal{W}(L/K) \leq X$. Then we would like to understand if the limit

$$\Pr_{\mathcal{W},\mathrm{ts},\mathfrak{p}}(c) := \lim_{X\to\infty} \frac{\mathrm{N}_{\mathcal{W},\mathrm{ts},\mathfrak{p}}(c,X)}{\mathrm{M}_W(X)}$$

exists and is independent of the class c.
In this section we will just adapt the whole proof given in [1] to our setup step by step without any particular modification and, as in the cited work, we will answer the previous question putting some extra conditions at primes dividing $|G|$ (namely, we will have to consider $[L]$ in $A'_G(K)$ and our result will concern $\Pr'_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c)$, a modified version of $\Pr_{\mathcal{W},\mathrm{ts},\mathfrak{p}}(c)$ analogous to $\Pr'_A(c)$ with respect to $\Pr_A(c)$ as in the introduction of the chapter).
When the proofs remain exactly the same of [1], we refer directly to the original paper for explanations and details.

5.2.1 Towards the counting problem

As in [1] we move our problem to a counting one. For that we will transpose the characterization of the group $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, given in Theorem 5.1.11, to the following group:

$$C_{\mathrm{ts},\mathfrak{p}}((O_K[G]) := \frac{\mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)}{(K[G]^{\times}/G)\cdot \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])} \ ,$$

note that this definition is very similar to the one given for $\mathrm{MCl}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ with a slight difference at the denominator. See (5.6) for a definition of $\mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$. Since we are working with an abelian group G sometimes it is better to think of $\mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)$ as the restricted direct product of $\mathcal{H}(K_{\mathfrak{p}}[G])$ with respect to $\mathcal{H}(O_{K,\mathfrak{p}}[G])$.
Let us consider the following three homomorphisms:

1. $$\rho_{\mathrm{ts},\mathfrak{p}} : \mathrm{Cl}(O_K[G]) \longrightarrow C_{\mathrm{ts},\mathfrak{p}}((O_K[G]),$$

   where $\rho_{\mathrm{ts},\mathfrak{p}}$ is induced by the embedding $J(K[G]) \longrightarrow \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right)$ (consider it as the restricted direct product of $\mathcal{H}(K_{\mathfrak{p}}[G])$), using the isomorphism $\mathrm{Cl}(O_K[G]) \cong J(K[G])/(K[G]^{\times}\cdot\prod_{\mathfrak{p}} O_{K,\mathfrak{p}}[G]^{\times})$.

2. $$\psi_{\mathrm{ts},\mathfrak{p}} : \mathrm{Hom}(\Omega, G) \longrightarrow C_{\mathrm{ts},\mathfrak{p}}((O_K[G]),$$

   induced by the following composition of maps

   $$\begin{array}{ccccccc} \mathrm{Hom}(\Omega,G) & \longrightarrow & A_G(K) & \longrightarrow & \dfrac{H(K[G])}{K[G]^{\times}} & \longrightarrow & C_{\mathrm{ts},\mathfrak{p}}((O_K[G]) \\ h & \longmapsto & K_h & \longmapsto & [r_G(b)] & \longmapsto & [r_G(b)] \end{array}$$

   where b is a normal basis generator of K_h and the last map is the natural quotient. The independence of $\psi_{\mathrm{ts},\mathfrak{p}}$ from the choice of b follows from the fact that we quotient by $K[G]^{\times}$.

3. $$\Theta_{\mathrm{ts},\mathfrak{p}} : J(K\Lambda) \longrightarrow C_{\mathrm{ts},\mathfrak{p}}((O_K[G]),$$

   induced by the following composition of maps

   $$\begin{array}{ccccc} J(K\Lambda) & \longrightarrow & \mathrm{Hom}_{\Omega}\left(\mathcal{A}_G, J(K^{\mathrm{c}})\right) & \longrightarrow & C_{\mathrm{ts},\mathfrak{p}}((O_K[G]) \\ f & \longmapsto & \Theta^{\mathrm{t}}_G(f) & \longmapsto & [\Theta^{\mathrm{t}}_G(f)] \end{array}$$

where the last map is the natural quotient.

Proposition 5.2.2 ([1, Proposition 3.4])**.** *The previous homomorphisms have the following properties:*

1. $\rho_{\mathrm{ts},\mathfrak{p}}$ *is injective.*
2. $h \in \mathrm{Ker}(\psi_{\mathrm{ts},\mathfrak{p}}) \iff K_h/K$ *is unramified totally split at* $\mathfrak{p}$ *and* O_{K_h} *is* $O_K[G]$*-free.*
3. $\Theta_{\mathrm{ts},\mathfrak{p}}|_{F^{\mathfrak{p}}}$ *is injective.*

Proof. 1. It is sufficient to note that

$$J(K[G]) \cap \left(\left(\prod_{\mathfrak{p}' \neq \mathfrak{p}} H(O_{K,\mathfrak{p}'}[G]) \right) \times (O_{K,\mathfrak{p}}[G])^{\times} \right) = \prod_{\mathfrak{p}'} (O_{K,\mathfrak{p}'}[G])^{\times}.$$

2. The proof remains the same as in [1] with the adjustment given by Theorem 5.1.11.

3. This follows immediately from the proof given in [1], since $F^{\mathfrak{p}} \subseteq F$.

□

Corollary 5.2.3. $\mathrm{Ker}(\psi_{\mathrm{ts},\mathfrak{p}})$ *is finite.*

We know, by Theorem 5.1.9, that, given a tame G-Galois K-algebra K_h totally split at $\mathfrak{p}$, there exist $c \in J(K[G])$, a unique $f \in F^{\mathfrak{p}}$ and an element $w \in \left((\prod_{\mathfrak{p}' \neq \mathfrak{p}} \mathcal{H}(O_{K,\mathfrak{p}'}[G])) \times (O_{K,\mathfrak{p}}[G]^{\times}/G) \right)$, such that

$$\mathrm{rag}(c) = \mathrm{rag}(r_G(b))^{-1} \cdot \Theta^{\mathrm{t}}_G(f) \cdot w.$$

Thus if we move to $C_{\mathrm{ts},\mathfrak{p}}((O_K[G])$, using the three previous homomorphisms, we get that there exist a unique class $[c] = [O_{K_h}] \in \mathrm{Cl}(O_K[G])$ and a unique $f \in F^{\mathfrak{p}}$, such that

$$\rho_{\mathrm{ts},\mathfrak{p}}([c]) = \psi_{\mathrm{ts},\mathfrak{p}}(h)^{-1} \cdot \Theta_{\mathrm{ts},\mathfrak{p}}(f). \tag{5.8}$$

Moreover, by the previous corollary, if, given a class $[c] \in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ and an element $f \in F^{\mathfrak{p}}$, there exists $h \in \mathrm{Hom}(\Omega, G)$ such that (5.8) is satisfied, then there are $|\mathrm{Ker}(\psi_{\mathrm{ts},\mathfrak{p}})|$ elements in $\mathrm{Hom}(\Omega, G)$ satisfying (5.8) with the same $[c]$ and f.

Thus we have seen that $\rho_{\mathrm{ts},\mathfrak{p}}(R_{\mathrm{ts},\mathfrak{p}}(O_K[G])) \subseteq \mathrm{Im}(\rho_{\mathrm{ts},\mathfrak{p}}) \cap [\mathrm{Im}(\Theta_{\mathrm{ts},\mathfrak{p}}) \cdot \mathrm{Im}(\psi_{\mathrm{ts},\mathfrak{p}})]$, but, thanks to Theorem 5.1.11, we also get the reverse inclusion, obtaining the identity

$$\rho_{\mathrm{ts},\mathfrak{p}}(R_{\mathrm{ts},\mathfrak{p}}(O_K[G])) = \mathrm{Im}(\rho_{\mathrm{ts},\mathfrak{p}}) \cap [\mathrm{Im}(\Theta_{\mathrm{ts},\mathfrak{p}}) \cdot \mathrm{Im}(\psi_{\mathrm{ts},\mathfrak{p}})].$$

Hereby in order to count all the tame G-Galois K-algebras (up to isomorphisms) totally split at $\mathfrak{p}$ realizing a fixed class $[c] \in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, we have to count all the couples (h, f), with $h \in \mathrm{Hom}(\Omega, G)$ and $f \in F^{\mathfrak{p}}$, satisfying equation (5.8), where $[c]$ is fixed.

Counting problem: Let $[c] \in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, then $\rho_{\mathrm{ts},\mathfrak{p}}([c]) = \psi_{\mathrm{ts},\mathfrak{p}}(h)^{-1}\Theta_{\mathrm{ts},\mathfrak{p}}(\lambda_c)$, with $h \in \mathrm{Hom}(\Omega^{\mathrm{t}}, G)$ and $\lambda_c \in F^{\mathfrak{p}}$. Following [1], we can now define the set

$$P_{\Theta_{\mathrm{ts},\mathfrak{p}}} := \{x \in J(K\Lambda) | \Theta_{\mathrm{ts},\mathfrak{p}}(x) \in \mathrm{Im}(\psi_{\mathrm{ts},\mathfrak{p}})\}$$

and one can prove that a couple (h_μ, μ), with $h_\mu \in \mathrm{Hom}\,(\Omega, G)$ and $\mu \in J(K\Lambda)$, satisfies

$$\rho_{\mathrm{ts},\mathfrak{p}}([c]) = \psi_{\mathrm{ts},\mathfrak{p}}(h_\mu)^{-1}\Theta_{\mathrm{ts},\mathfrak{p}}(\mu)$$

if and only if $\mu \in \lambda_c P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$ (see [1, Proposition 3.7], with our modified homomorphisms the proposition remains the same).
Hence we see that counting the couples (h, f), with $h \in \mathrm{Hom}(\Omega^{\mathrm{t}}, G)$ and $f \in F^{\mathfrak{p}}$, satisfying equation (5.8), with $[c]$ fixed (and so counting all the tame G-Galois K-algebras, up to isomorphisms, totally split at $\mathfrak{p}$ realizing the class $[c]$), is the same (up to multiplication by $|\mathrm{Ker}(\psi_{\mathrm{ts},\mathfrak{p}})|$) of counting the elements in $F^{\mathfrak{p}} \cap \lambda_c P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$ for a fixed coset $\lambda_c P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$ of $P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$ in $J(K\Lambda)$.

Following [1], we divide the study of this counting problem into two parts: an algebraic one and an analytic one.

5.2.4 Algebraic part

Using the modified ray class group $\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)$ already defined in (2.25) and Theorem 5.1.10, we can prove the following proposition.

Proposition 5.2.5 ([1, Proposition 3.9])**.** *Let $\mathfrak{m}$ be an integral ideal divisible by a sufficiently high power of $|G|$ and of $\mathfrak{p}$, then we have a natural quotient*

$$q_{\mathfrak{m}} : \mathrm{Cl}'_{\mathfrak{m}}(\Lambda) \longrightarrow J(K\Lambda)/P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$$

and hence $\lambda_c P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$ is equal to a disjoint union of cosets of $(K\Lambda)^{\times} \cdot U'_{\mathfrak{m}}(\Lambda)$ in $J(K\Lambda)$.

Proof. We develop the proof in detail, since the original one ([1, Proposition 3.9]) contains a mistake.
If $\mathfrak{m}$ is an integral ideal divisible by a sufficiently high power of $|G|$ and of $\mathfrak{p}$ (see Theorem 5.1.10 and Proposition 2.2.9), then $\Theta_G^{\mathrm{t}}(U'_{\mathfrak{m}}(\Lambda)) \subseteq \mathcal{U}_{\mathrm{ts},\mathfrak{p}}(O_K[G])$ and hence $\Theta_{\mathrm{ts},\mathfrak{p}}(U'_{\mathfrak{m}}(\Lambda)) = 0$ in $C_{\mathrm{ts},\mathfrak{p}}((O_K[G])$. Moreover $\Theta_{\mathrm{ts},\mathfrak{p}}((K\Lambda)^{\times}) \subseteq \mathcal{H}(K[G])$. Since every element in $\mathcal{H}(K[G])$ can be obtained from a normal basis generator of a G-Galois K-alegbra (2.1), thinking about the definition of $\psi_{\mathrm{ts},\mathfrak{p}}$ and of $P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$, we see that $(K\Lambda)^{\times} \cdot U'_{\mathfrak{m}}(\Lambda_{\mathfrak{p}}) \subseteq P_{\Theta_{\mathrm{ts},\mathfrak{p}}} \subseteq J(K\Lambda)$. Then we have a natural quotient $q_{\mathfrak{m}} : \mathrm{Cl}'_{\mathfrak{m}}(\Lambda) \longrightarrow J(K\Lambda)/P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$, which proves our statement and shows moreover that $J(K\Lambda)/P_{\Theta_{\mathrm{ts},\mathfrak{p}}}$ has to be finite. □

From now on, we fix once and for all $\mathfrak{m}$ to be an integral ideal satisfying the hypothesis of the previous proposition.

As we will see in the sequel the use of the modified ray class group, through the choice of the integral ideal $\mathfrak{m}$, will oblige us to avoid some algebras in our counting procedure, but this will be clearer later on.

Let us recall some facts and notations used in [1] which are useful in the sequel.

Given T a set of representatives of the orbits of $G(-1)$ under the Ω-action, we recall the Wedderburn decomposition given in (2.23):

$$J(K\Lambda) \cong \prod_{t \in T} J(K(t)).$$

Following the description below (2.23), if we consider the set of ideals of Λ obtained taking the ideal content (denoted by $\mathrm{co}(-)$) of the elements in $F^{\mathfrak{p}}$ and we denote it by $\mathfrak{F}^{\mathfrak{p}}$, we see that it consists of the ideals $\mathfrak{P} = (\mathfrak{P}_t)_{t \in T}$ such that:

- $\mathfrak{P}_1 = O_K$,
- $\mathrm{N}_{K\Lambda/K}(\mathfrak{P}) := \prod_{t \in T} \mathrm{N}_{K(t)/K}(\mathfrak{P}_t)$ is a squarefree O_K-ideal,
- $\mathfrak{P}_t$ is coprime to the order of t,
- $\mathfrak{P}$ is coprime to $\mathfrak{p}$.

The function that we shall use to count extensions is defined via the use of weights introduced by Agboola in [1]. A weight on the set of representatives T, given as above, is a function $\mathcal{W} : T \longrightarrow \mathbb{Z}$, which is equal to 0 for $t = 1$ and different from

0 for each $t \neq 1$. The minimum of the values it assumes outside $t = 1$ is denoted by $\alpha_{\mathcal{W}}$. The easiest example of weight is $\mathcal{W}_{\text{ram}}$ which is defined as the constant function 1 for each $t \neq 1$.
For every fractional ideal $\mathfrak{a} = (\mathfrak{a}_t)_{t\in T}$ of Λ, Agboola defined $d_{\mathcal{W}}(\mathfrak{a}) := \left(\mathfrak{a}_t^{\mathcal{W}(t)}\right)_{t\in T}$ and the associated discriminant for Galois algebras over K as

$$D_{\mathcal{W}}(K_h/K) := [\Lambda : d_{\mathcal{W}}(\text{co}(f))],$$

where $f \in F$ is the element of $J(K\Lambda)$ satisfying (5.8) for the given extension. For example using $\mathcal{W}_{\text{ram}}$, we get that $D_{\mathcal{W}_{\text{ram}}}(K_h/K)$ is equal to the absolute norm of the product of primes of K which ramify in K_h/K.

Definition of probability. Given a class $c \in R(O_K[G])$ and a natural number X, $\text{N}_{\mathcal{W},\mathfrak{m},\text{ts},\mathfrak{p}}(c, X)$ is defined as the number of classes in $A_G^{\text{t}}(K)$ such that their representatives K_h/K are totally split at $\mathfrak{p}$, realize the class c (i.e. $[O_{K_h}] = c$) and have $D_{\mathcal{W}}(K_h/K)$ coprime to $\mathfrak{m}$ and less or equal to X. While $\text{M}_{\mathcal{W},\mathfrak{m}}(X)$ denotes the the number of classes in $A_G^{\text{t}}(K)$ such that their representatives K_h/K have $D_{\mathcal{W}}(K_h/K)$ coprime to $\mathfrak{m}$ and less or equal to X. In what follows we will study the behavior of the limit of the quotient of these two quantities as X goes to infinity, which we denote as:

$$\text{Pr}'_{\mathcal{W},\mathfrak{m},\text{ts},\mathfrak{p}}(c) := \lim_{X\to\infty} \frac{\text{N}_{\mathcal{W},\mathfrak{m},\text{ts},\mathfrak{p}}(c, X)}{\text{M}_{\mathcal{W},\mathfrak{m}}(X)}.$$

We shall prove that, if $\mathcal{W}$ is constant on $T \setminus \{1\}$, this limit exists and does not depend on the class c.

Remark 5.2.6. *If $c \notin R_{\text{ts},\mathfrak{p}}(O_K[G])$, then $\text{Pr}'_{\mathcal{W},\mathfrak{m},\text{ts},\mathfrak{p}}(c)$ is clearly equal to 0.*

So, given $c \in R_{\text{ts},\mathfrak{p}}(O_K[G])$, the discussion in §5.2.1 implies that

$$\text{N}_{\mathcal{W},\mathfrak{m},\text{ts},\mathfrak{p}}(c, X) = \mathcal{K}\cdot|\{f \in F^{\mathfrak{p}} \cap \lambda_c P_{\Theta_{\text{ts},\mathfrak{p}}} \,|\, (\text{co}(f), \mathfrak{m}) = 1 \text{ and } [\Lambda : d_{\mathcal{W}}(\text{co}(f))] \leq X\}|,$$

where $\mathcal{K} := |\text{Ker}(\psi_{\text{ts},\mathfrak{p}})|$.
Following Proposition 5.2.5, if for every coset $\mathfrak{c}$ of $(K\Lambda)^\times \cdot U'_{\mathfrak{m}}(\Lambda)$ in $J(K\Lambda)$ we define

$$\kappa_{\mathcal{W},\mathfrak{m},\text{ts},\mathfrak{p}}(\mathfrak{c}, X) := |\{f \in F^{\mathfrak{p}} \cap \mathfrak{c} \,|\, (\text{co}(f), \mathfrak{m}) = 1 \text{ and } [\Lambda : d_{\mathcal{W}}(\text{co}(f))] \leq X\}|, \quad (5.9)$$

we get

$$\mathrm{N}_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c,X) = \mathcal{K}\cdot\left(\sum_{\mathfrak{c}\in q_{\mathfrak{m}}^{-1}(\lambda_c)} \kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)\right), \tag{5.10}$$

where $q_{\mathfrak{m}}$ is the natural quotient of Proposition 5.2.5.
Thus, we see that the asymptotic behavior of $\mathrm{N}_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c,X)$ is controlled by the asymptotic behavior of $\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)$. For example, if we are able to prove that $\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)$ is asymptotically independent of $\mathfrak{c}$ as X goes to ∞, then we will have as a consequence that $\mathrm{Pr}'_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c)$ is independent of c, as we would like to prove. Note that, if $\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)$ is not asymptotically independent of $\mathfrak{c}$ as X goes to ∞, the asymptotic behavior of $\mathrm{N}_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c,X)$ could still be independent of c.

5.2.7 Analytic part

We have reduced our problem to an analytic one: we want to understand the asymptotic behavior of $\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)$ as $X\to\infty$. We shall prove now, that, for certain counting function $\mathcal{W}$, it does not depend on the class c.
As we shall immediately see, the proof of this fact will be a direct consequence of the results contained in [1, Sections 4-8]. So, without repeating arguments which are already in [1, Sections 4-8], we shall explain the main steps which lead to the analytic investigation of the behavior of $\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)$ as $X\to\infty$, refering to [1] when the proofs given by Agboola apply to our case too.

Given a coset $\mathfrak{c}$ of $(K\Lambda)^\times\cdot U'_{\mathfrak{m}}(\Lambda)$ in $J(K\Lambda)$, let us consider the function of $z\in\mathbb{C}$

$$D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z) := \sum_{\substack{\mathfrak{a}\in \mathrm{co}(F^{\mathfrak{p}}\cap\mathfrak{c})\\(\mathfrak{a},\mathfrak{m})=1}} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-z}.$$

Using $\widehat{\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)}$, the group of characters of $\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)$, we can write

$$D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z) = \frac{1}{|\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)|}\sum_{\chi\in\widehat{\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)}} \tilde{\chi}(\mathfrak{c})D_{\mathrm{ts},\mathfrak{p}}(z,\chi),$$

where $D_{\mathrm{ts},\mathfrak{p}}(z,\chi) := \sum_{\mathfrak{a}\in\mathfrak{F}^{\mathfrak{p}}}\chi(\mathfrak{a})[\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-z}$ and χ is considered as a map on the set of integrals ideals of Λ, by establishing $\chi(\mathfrak{a})=0$ if $\mathfrak{a}_1\neq O_K$ (where $\mathfrak{a}=(\mathfrak{a}_t)_{t\in T}$) or if $\mathfrak{a}$ is not coprime to $\mathfrak{m}$.

Since, in our case, we are considering $\mathfrak{m}$ divisible by a sufficiently high power of $|G|$ and of $\mathfrak{p}$, we understand that, by the description of $\mathfrak{F}^{\mathfrak{p}}$ given above, we have

$$\{\mathfrak{a} \in \mathrm{co}(F^{\mathfrak{p}} \cap \mathfrak{c}),\ (\mathfrak{a}, \mathfrak{m}) = 1\} = \{\mathfrak{a} \in \mathrm{co}(F \cap \mathfrak{c}),\ (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

Thus, with our choice of $\mathfrak{m}$, the series $D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z)$ previously defined, is equal to the series

$$D_{\mathfrak{c},\mathfrak{m}}(z) := \sum_{\substack{\mathfrak{a} \in \mathrm{co}(F \cap \mathfrak{c}) \\ (\mathfrak{a},\mathfrak{m})=1}} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-z}$$

considered by Agboola in his paper (see [1, Definition 4.1]). This is the reason why the analytic part remains exactly the same of [1]: we are considering the same series studied by Agboola with just an extra condition on the prime $\mathfrak{m}$.

Proposition 5.2.8. *The series $D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z)$ is convergent in some right hand half-plane.*

Proof. From our discussion above, this result follows from the analogous one proved in [1, Section 4] for the series $D_{\mathfrak{c},\mathfrak{m}}(z)$. See in particular [1, Proposition 4.5] where, through the use of Euler product expansions, Agboola showed that $D_{\mathfrak{c},\mathfrak{m}}(z)$ converges in some right hand half-plane. □

From its definition we know that $D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z)$ is a Dirichlet series $\sum_{n=0}^{\infty} a_n n^{-z}$, where the a_n are non-negative coefficients, and it is moreover clear that

$$\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c}, X) = \sum_{n \leq X} a_n.$$

So we have reduced our problem to study the asymptotic behavior of the sum of the first X coefficients of a convergent Dirichlet series. A classical theorem which helps at this point is the Délange–Ikehara Tauberian Theorem, which is recalled below.

Theorem 5.2.9 (Délange–Ikehara Tauberian Theorem)**.** *Let $\sum_{n=1}^{\infty} a_n n^{-z}$ be a Dirichlet series with non-negative coefficients which is convergent on the half-plane $Re(z) > a > 0$. Assume that in its domain of convergence*

$$\sum_{n=1}^{\infty} a_n n^{-z} = g(z)(z-a)^{-w} + h(z),$$

where $w > 0$ and $g(z)$ and $h(z)$ are holomorphic functions on the closed half-plane on the right of a, such that $g(a) \neq 0$. Then

$$\sum_{n \leq X} a_n \sim \frac{g(a)}{a \cdot \Gamma(w)} \cdot X^a \cdot (\log(X))^{w-1},$$

as $X \to \infty$. At the denominator $\Gamma(w)$ is the value of the classical Gamma function at w.

In order to apply Theorem 5.2.9 to our case, first of all we need to find the most right pole $\beta(\mathfrak{c}, \mathfrak{m})$ of $D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z)$ (which corresponds to $D_{\mathfrak{c},\mathfrak{m}}(z)$ in [1]), its order $\delta(\mathfrak{c}, \mathfrak{m})$ and the "residue" at $\beta(\mathfrak{c}, \mathfrak{m})$ given by

$$\tau(\mathfrak{c}, \mathfrak{m}) := \lim_{z \to \beta(\mathfrak{c},\mathfrak{m})} (z - \beta(\mathfrak{c}, \mathfrak{m}))^{\delta(\mathfrak{c},\mathfrak{m})} D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z).$$

Then, using Theorem 5.2.9, we shall get

$$\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c}, X) \sim \frac{\tau(\mathfrak{c}, \mathfrak{m})}{\beta(\mathfrak{c}, \mathfrak{m}) \cdot \Gamma(\delta(\mathfrak{c}, \mathfrak{m}))} \cdot X^{\beta(\mathfrak{c},\mathfrak{m})} \cdot (\log(X))^{\delta(\mathfrak{c},\mathfrak{m})-1}. \tag{5.11}$$

Hence, from this, if we are able to show the independence of $\beta(\mathfrak{c}, \mathfrak{m})$, $\tau(\mathfrak{c}, \mathfrak{m})$ and $\delta(\mathfrak{c}, \mathfrak{m})$ from $\mathfrak{c}$, we will deduce the independence of $\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c}, X)$ from $\mathfrak{c}$, as $X \to \infty$.

Let $I(\Lambda)$ denote the group of fractional ideals of Λ. The values $\beta(\mathfrak{c}, \mathfrak{m})$, $\tau(\mathfrak{c}, \mathfrak{m})$ and $\delta(\mathfrak{c}, \mathfrak{m})$ can be found, as already done in [1, Sections 6-7], through a comparison of $D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z)$ with the Dirichlet L-series associated to Λ

$$L_\Lambda(z, \chi) := \sum_{\substack{\mathfrak{a} \in I(\Lambda) \\ \mathfrak{a} \subseteq \Lambda}} \chi(\mathfrak{a})[\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-z}.$$

In particular, if we define

$$b_{\alpha_{\mathcal{W}}}(\chi) := \lim_{z \to \frac{1}{\alpha_{\mathcal{W}}}} \left(z - \frac{1}{\alpha_{\mathcal{W}}}\right)^{\delta(\mathfrak{c},\mathfrak{m})} D_{\mathrm{ts},\mathfrak{p}}(z, \chi),$$

from [1, Section 7] (be careful that in Proposition 7.1, the assumption $p \nmid \mathfrak{m}$ is superfluous), we get:

$$\begin{aligned}\beta(\mathfrak{c},\mathfrak{m}) &= \frac{1}{\alpha_{\mathcal{W}}}\\ \delta(\mathfrak{c},\mathfrak{m}) &= \left|t \in T\setminus\{1\} \text{ s.t. } \mathcal{W}(t)=\alpha_{\mathcal{W}}\right|\\ \tau(\mathfrak{c},\mathfrak{m}) &= \frac{1}{|\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)|}\sum_{\chi\in\widehat{\mathrm{Cl}'_{\mathfrak{m}}(\Lambda)}}\tilde{\chi}(\mathfrak{c})b_{\alpha_{\mathcal{W}}}(\chi).\end{aligned}$$

Finally, we have the following result.

Proposition 5.2.10. *Let $\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)$ be defined as in (5.9). Then*

$$\kappa_{\mathcal{W},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X) \text{ is asymptotically independent from } \mathfrak{c} \iff b_{\alpha_{\mathcal{W}}}(\chi)=0\,,\ \forall\,\chi\neq 1.$$

Moreover, in this case we have

$$\lim_{z\to\frac{1}{\alpha_{\mathcal{W}}}}\left(z-\frac{1}{\alpha_{\mathcal{W}}}\right)^{d_{\alpha_{\mathcal{W}}}(1)}D_{\mathfrak{c},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(z)=b_{\alpha_{\mathcal{W}}}(1)/|\mathrm{Cl}'_{\mathfrak{m}}(\Lambda))|.$$

Proof. For a proof of it see [1, Lemma 7.5 - Proposition 7.6]. □

As explained in [1], the easiest case when $b_{\alpha_{\mathcal{W}}}(\chi)=0\,,\ \forall\,\chi\neq 1$, is when $\mathcal{W}$ is chosen to be constant on $T\setminus\{1\}$. While in the non-constant case we can lose the asymptotic independence as explained in [1, Proposition 7.8].

An example, as we have seen, of constant $\mathcal{W}$ is given by $\mathcal{W}_{\mathrm{ram}}$. In this case we have $\alpha_{\mathcal{W}_{\mathrm{ram}}}=1$ and so

$$\kappa_{\mathcal{W}_{\mathrm{ram}},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(\mathfrak{c},X)\sim\frac{b_{\alpha_{\mathcal{W}_{\mathrm{ram}}}}(1)}{\Gamma(|T\setminus\{1\}|)\cdot|\mathrm{Cl}'_{\mathfrak{m}}(\Lambda))|}\cdot X\cdot(\log(X))^{|T\setminus\{1\}|-1},$$

as $X\to\infty$, and hence, from (5.10),

$$\mathrm{N}_{\mathcal{W}_{\mathrm{ram}},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c,X)\sim\mathcal{K}\cdot|\mathrm{Ker}(q_{\mathfrak{m}})|\cdot\frac{b_{\alpha_{\mathcal{W}_{\mathrm{ram}}}}(1)}{\Gamma(|T\setminus\{1\}|)\cdot|\mathrm{Cl}'_{\mathfrak{m}}(\Lambda))|}\cdot X\cdot(\log(X))^{|T\setminus\{1\}|-1},$$

as $X\to\infty$.
Thus the analog of [1, Theorem B] now clearly follows (this is a more precise version of Theorem 0.0.9 in the Introduction).

Theorem 5.2.11. *Let c be a given class in $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$. The asymptotic behavior of $\mathrm{N}_{\mathcal{W}_{\mathrm{ram}},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c,X)$, as $X\to\infty$, does not depend on c. Moreover $\mathrm{Pr}'_{\mathcal{W}_{\mathrm{ram}},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c)$ exists and does not depend on c.*

Proof. Clear from the previous asymptotic approximation and from the definition of $\mathrm{Pr}'_{\mathcal{W}_{\mathrm{ram}},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c)$. □

Remark 5.2.12. *Analogously to [1, Section 9, Proposition 9.5], one can prove that in our definition of probability, if instead of considering G-Galois K-algebras we restrict our attention to just field extensions, the result of Theorem 5.2.11 remains the same.*

Corollary 5.2.13. *The limit $\mathrm{Pr}((1,1),\mathfrak{p},c)$, defined in the introduction of this chapter (see (5.2)), exists and does not depend on the given realizable class $c\in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$.*

Proof. Since $D_{\mathcal{W}_{ram}}(L/K)$ coincides with $D(L/K)$ (see at the beginning of the chapter), taking $\mathfrak{m}:=(|G|\cdot\mathfrak{p})^m O_K$ (where m is the sufficiently high natural number given by Theorem 5.1.10 and Proposition 2.2.9), and thanks to Corollary 5.2.13, we see that $\mathrm{Pr}'_{\mathcal{W}_{\mathrm{ram}},\mathfrak{m},\mathrm{ts},\mathfrak{p}}(c)$ coincides with $\mathrm{Pr}((1,1),\mathfrak{p},c)$. □

5.3 Probabilities on G-Galois K-algebras totally split at $\mathfrak{p}$

Thanks to the previous results, going back to question (5.4), we can now prove the following result.

Proposition 5.3.1. *Let K be a number field and G a finite abelian group. Given a finite prime $\mathfrak{p}$ of K and $c\in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$, we have*

$$\mathrm{Pr}((1,1),\mathfrak{p},c)=\mathrm{Pr}_W\left(((1,1),\mathfrak{p})\;\middle|\;L \text{ unr. at all } \mathfrak{p}'\middle||G|\right)\cdot\mathrm{Pr}'_A(c)$$

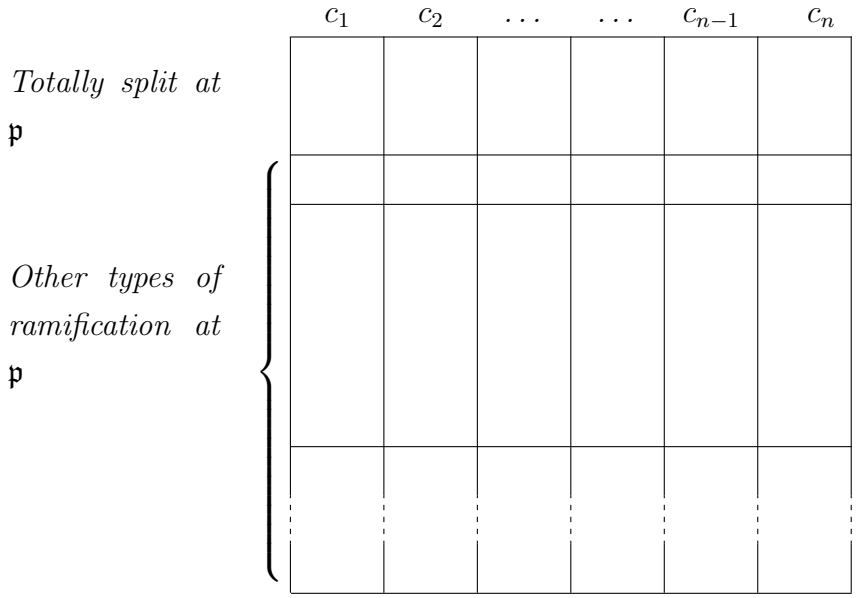
if and only if $R_{\mathrm{ts},\mathfrak{p}}(O_K[G])=R(O_K[G])$.

Proof. The proof is a direct consequence of Corollary 5.2.13. Indeed, from that result, we know that the limit $\mathrm{Pr}((1,1),\mathfrak{p},c)$ does not depend on the given realizable class $c\in R_{\mathrm{ts},\mathfrak{p}}(O_K[G])$. Thus, from the definition of $\mathrm{Pr}((1,1),\mathfrak{p},c)$, we have

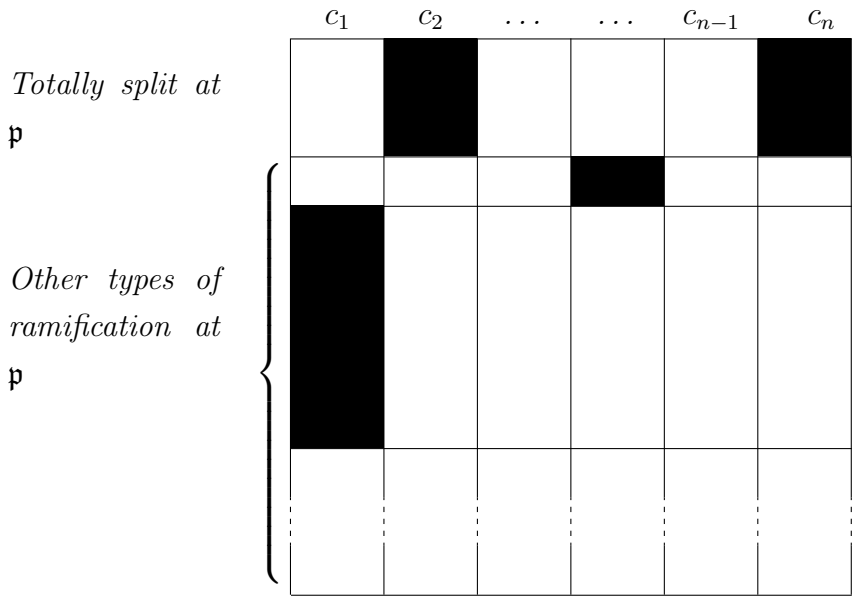
$$\mathrm{Pr}((1,1),\mathfrak{p},c)=\mathrm{Pr}_W\left((1,1),\mathfrak{p}\;\middle|\;L \text{ unr. at all } \mathfrak{p}'\middle||G|\right)/|R_{\mathrm{ts},\mathfrak{p}}(O_K[G])|.$$

Moreover we know from Theorem 5.0.5 that $\Pr'_A(c) = 1/|R(O_K[G])|$. Hence the claim of the proposition is now straightforward. □

Remark 5.3.2. *Assuming that $R(O_K[G]) = \{c_1, c_2, \ldots, c_n\}$, the following diagrams give a representation of the different probabilities computed by Agboola and Wood. We focus our attention on the classes in $F'_G(K)$. The columns are taken of the same width since the realizable classes are equidistributed as Agboola proved, while the different heights of the rows are related to the conditional probabilities at one prime which can be computed through the results of Wood.*



Actually it is conceivable that some classes are not realized by extensions with a particular ramification condition at $\mathfrak{p}$, so a more faithful table should be similar to the following, where a black cell means that the correspondent class is not realized by any extension with the ramification condition of the respective row.



The previous result opens a new conjecture which, surprisingly, seems not to have received any attention.

Conjecture 1. *Let K and G be as before. Given $\mathfrak{p}$ a finite place of K, the equality*

$$R_{\mathrm{ts},\mathfrak{p}}(O_K[G]) = R(O_K[G])$$

holds.

We are not able to prove this conjecture even if we know the representations of the two groups, following McCulloh's method, as explained in the previous sections. The idea that a restriction of such a kind on a single prime can result in the loss of some realizable classes is quite weird and a good motivation which strengthens the conjecture is given passing from realizable to Steinitz classes (which we have already encountered in Chapter 0).

Given L a G-Galois K-algebra, we denote by $\mathrm{st}(L/K)$ its associated Steinitz class in $\mathrm{Cl}(O_K)$. Given a base field K and a finite group G, we define the subset of Steinitz classes given by field extensions as

$$\mathrm{R}_t(O_K, G) := \{c \in \mathrm{Cl}(O_K) : \exists\ [L] \in F_G^{\mathrm{t}}(K) \text{ s.t. } \mathrm{st}(L/K) = c\}. \tag{5.12}$$

As already noted in Chapter 0, there is a link between realizable and Steinitz classes. Namely, given L/K a tame G-Galois algebra, then $\mathrm{st}(L/K)$ is equal to the image of $[O_L]$ under the natural restriction (see 1.8.1) between class groups

$$\mathrm{res}^G_{\{1\}} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_K).$$

There are several works on the problem of describing the set of Steinitz classes, as the recent ones by Alessandro Cobbe and Luca Caputo. In particular in [12, Remark 3], the authors underline that, given a finite prime $\mathfrak{p}$ of K, if we denote by $\mathrm{R}_{t,\mathrm{ts},\mathfrak{p}}(O_K, G)$ the set of Steinitz classes given by tame field extensions which are totally split at $\mathfrak{p}$, we do not lose any class or in other words $\mathrm{R}_t(O_K, G) = \mathrm{R}_{t,\mathrm{ts},\mathfrak{p}}(O_K, G)$. Hereby we obtain that $\mathrm{res}^G_{\{1\}}(R_{\mathrm{ts},\mathfrak{p}}(O_K[G])) = \mathrm{res}^G_{\{1\}}(R(O_K[G]))$, even if this does not allow us to deduce a proof of our original conjecture on realizable classes.

5.3.3 More primes and other types of splitting behavior

Instead of imposing the totally split condition on a single prime we could take a finite set S of finite primes of K and wonder to describe $R_{\mathrm{ts},S}(O_K[G])$, the set of realizable classes given by tame G-Galois K-algebras which are totally split at every $\mathfrak{p} \in S$. As we have already noted in Remark 5.1.13, one has the equality $R_{\mathrm{ts},S}(O_K[G]) = \mathrm{St}_{\mathrm{ts},S}(O_K[G])$ (see Remark 5.1.13 for precise definitions).
Hereby, just using an integral ideal $\mathfrak{m}$ divisible by a sufficiently high power of $|G|$ and of every ideal in S, the results obtained in §5.2 can be easily generalized considering a finite set of primes. More precisely, given $S := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ as above and $T_S := \{T_i\}_{i\in\{1,\ldots,n\}}$ a finite collection of splitting types, we write

$$\Pr(T_S, S, c) := \lim_{X\to\infty} \frac{\sharp\{[L] \in F'_G(K) |\, L_{\mathfrak{p}_i} \equiv T_i, \forall\, i = 1, \ldots, n, [O_L] = c, D(L/K) \leq X\}}{\sharp\{[L] \in F'_G(K) |\, D(L/K) \leq X\}}.$$

Moreover let $\Pr_W\left(\mathfrak{p} \text{ of type } (1,1), \forall\, \mathfrak{p} \in S \,\middle|\, L \text{ unr. at all } \mathfrak{p} \middle| |G|\right)$ be defined similarly to (5.3). Then we have the following proposition analogous to Proposition 5.3.1.

Corollary 5.3.4. *Let K and G be as before. Given a finite set S of finite prime ideals in K, let $T_{\mathrm{ts},S}$ be the finite collection $\{T_{\mathrm{ts},\mathfrak{p}}\}_{\mathfrak{p}\in S}$, where $T_{\mathrm{ts},\mathfrak{p}} = (1,1)$ for every $\mathfrak{p} \in S$, then*

$$\Pr(T_{\mathrm{ts},S}, S, c) = \Pr_W\left(\mathfrak{p} \textit{ of type } (1,1), \forall\, \mathfrak{p} \in S \,\middle|\, L \textit{ unr. at all } \mathfrak{p} \middle| |G|\right) \cdot \Pr'_A(c)$$

if and only if

$$R_{\mathrm{ts},S}(O_K[G]) = R(O_K[G]).$$

Hereby also the following conjecture arises spontaneously.

Conjecture 2. *Let K and G be as before. Given a finite set S of finite places of K, $R_{\mathrm{ts},S}(O_K[G]) = R(O_K[G])$.*

Again the analogous conjecture for the group of Steinitz classes is proved in [12, Remark 3].

Another immediate question is the following: what happens if we consider other types of ramification at a prime (or a finite set of primes)? Following our method used in the previous sections for the totally split case, we can just make the following remark.

Remark 5.3.5. *Let d be a natural number dividing $|G|$. The equidistribution result of the chapter (see Corollary 5.2.13) may be "generalized", replacing the totally split condition with the condition that a G-Galois extension of K is unramified at $\mathfrak{p}$, with $\mathfrak{p}$ splitting into a number of primes divisible by $|G|/d$.*
This follows applying the methods used in the chapter, with the group $O_{K,\mathfrak{p}}[G]^\times/G$, which corresponds to the totally split case, replaced by the subgroup of elements $a \in \mathcal{H}(O_{K,\mathfrak{p}}[G])$ such that $a^d \in O_{K,\mathfrak{p}}[G]^\times/G$. Indeed we have to underline that the quotient $\mathcal{H}(O_{K,\mathfrak{p}}[G])/(O_{K,\mathfrak{p}}[G]^\times/G)$ is isomorphic to $\mathrm{Hom}(\Omega_{\mathfrak{p}}^{\mathrm{nr}}, G)$ ($\cong G$) and that, given K_h/K an unramified extension at $\mathfrak{p}$, the number of primes lying over $\mathfrak{p}$ is equal to $|G|/|\mathrm{Im}(h_{\mathfrak{p}})|$.
Note that our original totally split condition corresponds to the case $d = 1$.

Appendix

Why the map $\mathcal{R}$ is not a group homomorphism

Suppose G to be abelian. We have seen in the Introduction that the image of the map

$$\begin{aligned} \mathcal{R} : H^1(\Omega_K^{\mathrm{t}}, G) &\longrightarrow \mathrm{Cl}(O_K[G]) \\ [L] &\longmapsto [O_L], \end{aligned}$$

is the set of realizable classes $R(O_K[G])$, which McCulloh showed to be a subgroup of $\mathrm{Cl}(O_K[G])$.
This raises the question: is $\mathcal{R}$ a group homomorphism?

When the map is trivial (e.g. when K is equal to $\mathbb{Q}$), the answer to our question is clearly yes. We will now give an explicit example where $\mathcal{R}$ is not a group homomorphism.

To do so, let us consider the group homomorphism $\mathrm{res}^G_{\{1\}} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_K)$. As we have already seen, given $[L] \in H^1(\Omega_K^{\mathrm{t}}, G)$, the compositum $\mathrm{res}^G_{\{1\}}(\mathcal{R}([L]))$ is equal to $\mathrm{st}(L/K)$, the Steinitz class associated to the G-Galois K-algebra L (see Chapter 0). The first cohomology group $H^1(\Omega_K^{\mathrm{t}}, G)$ is equal to $\mathrm{Hom}(\Omega_K^{\mathrm{t}}, G)$ (since G is abelian). Thus, given $h \in \mathrm{Hom}(\Omega_K^{\mathrm{t}}, G)$, we clearly see that $\mathrm{st}(K_h/K) = \mathrm{st}(K_{h^{-1}}/K)$, since as K-algebras $K_h \cong K_{h^{-1}}$. So if the map $\mathrm{st} : H^1(\Omega_K^{\mathrm{t}}, G) \longrightarrow \mathrm{Cl}(O_K)$, which to any $[L] \in H^1(\Omega_K^{\mathrm{t}}, G)$ associates $\mathrm{st}(L/K)$, would be a group homomorphism, any Steinitz class should be of order less or equal than 2. Thus, in order to find an example when st (and so $\mathcal{R}$) is not a group homomorphism, we shall show that there exists a quadratic extension of $K \neq \mathbb{Q}$ with non-trivial Steinitz class of order different from 2.

Let us consider $K = \mathbb{Q}(\sqrt{-26})$, then with MAGMA we find that $\mathrm{Cl}(O_K)$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Let $\mathfrak{p}$ be one of the two primes over (17). We compute that the

ray classgroup $\mathrm{Cl}_{\mathfrak{p}}(O_K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. By Class Field Theory (see [29, Chapter V, §3]), to any subgroup of $\mathrm{Cl}_{\mathfrak{p}}(O_K)$ of index 2 corresponds a quadratic extension of K of conductor dividing $\mathfrak{p}$ and to any subgroup of $\mathrm{Cl}(O_K)$ of index 2 corresponds an unramified (at both finite and infinite places) quadratic extension of K. Since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ contains three subgroups of index 2 (they correspond to the elements of order 2 in $\mathrm{Cl}_{\mathfrak{p}}(O_K)/2\mathrm{Cl}_{\mathfrak{p}}(O_K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), while $\mathbb{Z}/6\mathbb{Z}$ only contains one, by the results of Class Field Theory just stated, we can find two tame quadratic extensions L, L' of K with discriminant over K equal to $\mathfrak{p}$.
Let us consider just L and suppose that $\alpha \in K$ satisfies $L = K(\sqrt{\alpha})$. Then, by a general result on Steinitz classes (see for example [13, Theorem 1.3.6]), the ideal $\mathfrak{p}/\alpha$ is a square and the class of its square root is equal to $\mathrm{st}(L/K)$. Always with the help of MAGMA, we see that $\mathfrak{p}$ is not a principal ideal, proving in particular that $\mathrm{st}(L/K) \neq 1$, as well as $\mathrm{st}(L/K)^2 \neq 1$.

This can also be seen as a consequence of the more general result $R_{\mathrm{t}}(O_K, C_2) = \mathrm{Cl}(O_K)$, where $R_{\mathrm{t}}(O_K, C_2)$ denotes the set of classes in $\mathrm{Cl}(O_K)$ which can obtained as Steinitz classes of quadratic extensions over K (see [13, Proposition 2.2.3], even if this result goes back at least as far as McCulloh's paper [25]).

Remark. *The question if $\mathcal{R}$ is a group homomorphism was already answered "no" by Jan Brinkhuis in [5], without giving an explicit example as we did. Moreover, in the same paper, he also showed that a weaker group law holds: given $h_1, h_2 \in H^1(\Omega_K^{\mathrm{t}}, G)$, such that the corresponding G-Galois K-algebras have disjoint ramification, then*

$$\mathcal{R}(h_1 h_2) = \mathcal{R}(h_1) + \mathcal{R}(h_2).$$

For details on this "weak" group law version, see [5, Section 3].

Bibliography

[1] A. Agboola. On counting rings of integers as Galois modules. *J. Reine Angew. Math.*, 663:1–31, 2012.

[2] A. Agboola and D. Burns. On the Galois structure of equivariant line bundles on curves. *Amer. J. Math.*, 120(6):1121–1163, 1998.

[3] E. Artin and J. Tate. *Class field theory.* AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[4] H. Bass. *Algebraic K-theory.* W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[5] J. Brinkhuis. Galois modules and embedding problems. *J. Reine Angew. Math.*, 346:141–165, 1984.

[6] C. Bruche and B. Sodaïgui. On realizable Galois module classes and Steinitz classes of nonabelian extensions. *J. Number Theory*, 128(4):954–978, 2008.

[7] N. P. Byott. Tame realisable classes over Hopf orders. *J. Algebra*, 201(1):284–316, 1998.

[8] N. P. Byott, C. Greither, and B. Sodaïgui. Classes réalisables d'extensions non abéliennes. *J. Reine Angew. Math.*, 601:1–27, 2006.

[9] N. P. Byott and B. Sodaïgui. Realizable Galois module classes over the group ring for non abelian extensions. *to appear in Annales de l'Institut Fourier.*

[10] N. P. Byott and B. Sodaïgui. Galois module structure for extensions of degree 8: realizable classes over the group ring. *J. Number Theory*, 112(1):1–19, 2005.

[11] N. P. Byott and B. Sodaïgui. Realizable Galois module classes for tetrahedral extensions. *Compos. Math.*, 141(3):573–582, 2005.

[12] L. Caputo and A. Cobbe. An explicit candidate for the set of Steinitz classes of tame Galois extensions with fixed Galois group of odd order. *to appear in PLMS*.

[13] A. Cobbe. *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*. PhD thesis, Scuola Normale Superiore di Pisa.

[14] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1981. With applications to finite groups and orders, A Wiley-Interscience Publication.

[15] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. II*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1987. With applications to finite groups and orders, A Wiley-Interscience Publication.

[16] K. Foster. *An equal-distribution result for Galois module structure*. PhD thesis, University of Illinois at Urbana-Champaign.

[17] A. Fröhlich. Locally free modules over arithmetic orders. *J. Reine Angew. Math.*, 274/275:112–124, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.

[18] A. Fröhlich. Arithmetic and Galois module structure for tame extensions. *J. Reine Angew. Math.*, 286/287:380–440, 1976.

[19] A. Fröhlich. *Galois module structure of algebraic integers*, volume 1 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1983.

[20] M. Godin and B. Sodaïgui. Realizable classes of tetrahedral extensions. *J. Number Theory*, 98(2):320–328, 2003.

[21] C. Greither, D. R. Replogle, K. Rubin, and A. Srivastav. Swan modules and Hilbert-Speiser number fields. *J. Number Theory*, 79(1):164–173, 1999.

[22] I. M. Isaacs. *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

[23] N. Jacobson. *Lectures in abstract algebra. III*. Springer-Verlag, New York, 1975. Theory of fields and Galois theory, Second corrected printing, Graduate Texts in Mathematics, No. 32.

[24] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[25] L. R. McCulloh. Cyclic extensions without relative integral bases. *Proc. Amer. Math. Soc.*, 17:1191–1194, 1966.

[26] L. R. McCulloh. A Stickelberger condition on Galois module structure for Kummer extensions of prime degree. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 561–588. Academic Press, London, 1977.

[27] L. R. McCulloh. Galois module structure of elementary abelian extensions. *J. Algebra*, 82(1):102–134, 1983.

[28] L. R. McCulloh. Galois module structure of abelian extensions. *J. Reine Angew. Math.*, 375/376:259–306, 1987.

[29] J. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[30] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, with a foreword by M. J. Taylor.

[31] D. S. Rim. Modules over finite groups. *Ann. of Math. (2)*, 69:700–712, 1959.

[32] F. Sbeity and B. Sodaïgui. Classes réalisables d'extensions métacycliques de degré *lm*. *J. Number Theory*, 130(8):1818–1834, 2010.

[33] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[34] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[35] J.-P. Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[36] B. Sodaïgui. Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger. *J. Number Theory*, 65(1):87–95, 1997.

[37] B. Sodaïgui. "Galois module structure" des extensions quaternioniennes de degré 8. *J. Algebra*, 213(2):549–556, 1999.

[38] B. Sodaïgui. Realizable classes of quaternion extensions of degree $4l$. *J. Number Theory*, 80(2):304–315, 2000.

[39] B. Sodaïgui. Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8. *J. Algebra*, 223(1):367–378, 2000.

[40] B. Sodaïgui. Relative Galois module structure of octahedral extensions. *J. Algebra*, 312(2):590–601, 2007.

[41] R. G. Swan. Induced representations and projective modules. *Ann. of Math. (2)*, 71:552–578, 1960.

[42] R. G. Swan. Projective modules over group rings and maximal orders. *Ann. of Math. (2)*, 76:55–61, 1962.

[43] M. J. Taylor. On Fröhlich's conjecture for rings of integers of tame extensions. *Invent. Math.*, 63(1):41–79, 1981.

[44] C. T. C. Wall. On the classification of Hermitian forms. IV. Adele rings. *Invent. Math.*, 23:241–260, 1974.

[45] S. Wang. On Grunwald's theorem. *Ann. of Math. (2)*, 51:471–484, 1950.

[46] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[47] M. M. Wood. On the probabilities of local behaviors in abelian field extensions. *Compos. Math.*, 146(1):102–128, 2010.

Curriculum Vitae

Andrea Siviero was born on the 20^{th} of July 1986 in Rovigo (Italy).
He attended the *Liceo Scientifico "P. Paleocapa"* (Italian equivalent of Scientific High School) in his hometown from 2000 to 2005, when he passed the final *Esame di Maturità*.
In September 2005 he started a first level degree in Mathematics at the *Università degli Studi di Padova* (Italy), successfully completed in September 2008 with the defense of a thesis entitled "Gaussian Measures in infinite dimension".
After that, he was admitted to the joint ALGANT Master degree in Mathematics at the *Università degli studi di Padova* (Italy) and at the *Université Bordeaux I* (France), where he defended his master thesis, entitled "On Realizable classes", in July 2010.
Funded by the *Université Bordeaux I*, within the framework of the european ALGANT-Doc program, he started a joint Ph.D. project at the *Université Bordeaux I* (France) and at the *Universiteit Leiden* (The Netherlands) in October 2010, the research results of which are contained in this dissertation.

Samenvatting

Klasse-invarianten voor tamme Galoisalgebra's

Zij K een getallenlichaam met ring van gehelen O_K en G een eindige groep.

Een algebra N over K met een werking van G heet een Galoisalgebra met groep G als N étale is (d.w.z. N is een eindig product van lichaamsuitbreidingen van K) en als G op N werkt als een groep van automorfismen zodanig dat:

- $[N : K] = |G|$,
- $N^G = K$.

Galoisuitbreidingen van lichamen zijn speciale gevallen van Galoisalgebra's.

Een Galoisalgebra N over K met groep G wordt *tam vertakt* genoemd als voor alle maximale idealen $\mathfrak{p}$ van O_K, de vertakkingsindex van $\mathfrak{p}$ copriem is met de karakteristiek van het restklassenlichaam van $\mathfrak{p}$ (dit is equivalent met het bestaan van een element in de gehele afsluiting O_N van O_K in N met spoor 1).

De Stelling van Noether

De *Stelling van de normale basis* vertelt ons dat een Galoisalgebra N/K een vrij $K[G]$-moduul van rang 1 is, d.w.z. er bestaat een element $b \in N$ zodanig dat $\{s \cdot b\}_{s \in G}$ - de baan van b onder de actie van G - een basis vormt voor N over K.

De vraag die ten grondslag ligt aan dit proefschrift is het verkrijgen van een analagon voor de ring van gehelen O_N: zij N een Galoisalgebra over K met Galoisgroep G, wanneer bestaat er een voortbrenger van een normale basis van gehelen, d.w.z. een element $a \in O_N$ zondanig dat $\{s \cdot a\}_{s \in G}$ een basis vormt voor O_N over O_K? Of, equivalent, wanneer bestaat er een element $a \in O_N$ zondanig dat $O_N = O_K[G] \cdot a$?
Dit probleem wordt *probleem van de normale basis van gehelen* genoemd.

Als G abels is en $K = \mathbb{Q}$, dan is het probleem geheel opgelost door de Stelling van Hilbert-Speiser: een abelse Galoisalgebra $N/\mathbb{Q}$ heeft een normale basis van gehelen dan en slechts dan als $N/\mathbb{Q}$ tam vertakt is.

Als K ongelijk aan $\mathbb{Q}$ is of G is niet abels, dan is het resultaat in het algemeen incorrect, maar dankzij E. Noether hebben we een resultaat dat net iets zwakker is.

De *Stelling van Noether* zegt dat een Galoisalgebra N over K met Galoisgroep G tam vertakt is dan en slechts dan als O_N een *lokaal vrij* $O_K[G]$-moduul van rang 1 is.
Het $O_K[G]$-moduul O_N is *lokaal vrij* van rang 1 als voor elk priemideaal $\mathfrak{p} \subseteq O_K$ de ring $O_{N,\mathfrak{p}} := O_N \otimes_{O_K} O_{K,\mathfrak{p}}$ een vrij $O_{K,\mathfrak{p}}$-moduul is van rang 1 (hierbij is $O_{K,\mathfrak{p}}$ de completering van O_K bij de metriek geïnduceerd door $\mathfrak{p}$), d.w.z. als er voor elke $\mathfrak{p}$ een voortbrenger $a_\mathfrak{p} \in O_{N,\mathfrak{p}}$ van een normale basis van de ring van gehelen van $O_{N,\mathfrak{p}}$ over $O_{K,\mathfrak{p}}$ bestaat.
Het is duidelijk dat een vrij moduul noodzakelijkerwijs lokaal vrij is, dus we zien dat tam vertakte Galoisalgebra's het correcte framework zijn voor het bestuderen van het probleem van de normale basis van gehelen. Wanneer we ons beperken tot tam vertakte Galoisalgebra's, dan is het probleem van de normale basis van gehelen dankzij de Stelling van Noether equivalent met het begrijpen wanneer een zeker lokaal vrij moduul vrij is.

Met $A_G^t(K)$ noteren we de *verzameling* van isomorfieklassen van tam vertakte Galoisalgebra's over K met Galoisgroep G, en we bekijken $\mathrm{Cl}(O_K[G])$, de groep van klassen van $O_K[G]$-modulen die lokaal vrij van rang 1 zijn, d.w.z. de groep gegeven door de stabiele isomorfieklassen van lokaal vrije $O_K[G]$-modulen.
Dankzij de Stelling van Noether hebben we een afbeelding

$$\mathcal{R} : A_G^t(K) \longrightarrow \mathrm{Cl}(O_K[G])$$

die aan elke klasse van $A_G^t(K)$, gerepresenteerd door N, de klasse van de ring van gehelen O_N in $\mathrm{Cl}(O_K[G])$ toekent.
Dit proefschrift behandelt verschillende vragen die gerelateerd zijn aan de studie van deze afbeelding.

Het beeld van $\mathcal{R}$ en de verzameling van realiseerbare klassen

De eerste vraag die we behandelen is de studie van het beeld van de afbeelding $\mathcal{R}$. Het beeld van deze afbeelding wordt genoteerd als $R(O_K[G])$, en de elementen van $R(O_K[G])$ heten realiseerbare klassen. Explicieter, de verzameling van realiseerbare klassen is de deelverzameling van $\mathrm{Cl}(O_K[G])$ bestaande uit de klassen van ringen van gehelen van tam vertakte Galoisalgebra's over K met Galoisgroep G.

De studie van de realiseerbare klassen wordt ook gemotiveerd door haar toepassingen in andere problemen in de getaltheorie. Zo zijn er connecties met de zoektocht naar een expliciete versie van zekere stellingen van het type Adams–Riemann–Roch verbonden aan $\mathrm{Cl}(O_K[G])$ en geeft deze studie belangrijke informatie bij het bestuderen van de deelverzameling van $\mathrm{Cl}(O_K)$ van Steinitz-klassen.

Aangezien de afbeelding $\mathcal{R}$ slechts een afbeelding van verzamelingen is, kunnen we ons afvragen wanneer het beeld, d.w.z. de verzameling van realiseerbare klassen, een ondergroep van $\mathrm{Cl}(O_K[G])$ is.

In 1986 heeft L. McCulloh, na het introduceren van $\mathrm{St}(O_K[G])$, een ondergroep van $\mathrm{Cl}(O_K[G])$ gedefinieerd in termen van zekere Stickelbergerelementen, bewezen dat

$$R(O_K[G]) = \mathrm{St}(O_K[G]),$$

als G *abels* is.
Hieruit volgt een positief antwoord op de vraag of de verzameling van realiseerbare klassen een groep vormt in het geval dat G abels is, d.w.z. gegeven twee klassen c_1, $c_2 \in R(O_K[G])$, bestaat er een Galoisalgebra N over K, met Galoisgroep G, tam vertakt, zodanig dat $\mathcal{R}([N]) = c_1 + c_2$, waarbij $[N]$ de isomorfieklasse van N aangeeft (een vergelijkbare opmerking is waar voor de inverse van een realiseerbare klasse).

In het geval dat G niet abels is, is de vraag of de verzamling van realiseerbare klassen een ondergroep van $\mathrm{Cl}(O_K[G])$ vormt nog een open probleem.
In het eerste deel van dit proefschrift geven wij een gedetailleerd bewijs van een ongepubliceerd resultaat van L. McCulloh dat ook in het niet abelse geval de inclusie

$$R(O_K[G]) \subseteq \mathrm{St}(O_K[G])$$

geldt. Of de bovenstaande inclusie een gelijkheid is in het niet-abelse geval is een open probleem.

De kern van $\mathcal{R}$ en het probleem van de normale basis van gehelen

De studie van de kern van de afbeelding $\mathcal{R}$ is sterk verbonden met het probleem van de normale basis dat we hiervoor besproken hebben.
In het geval dat G abels is en in verschillende niet-abelse gevallen (bijvoorbeeld als G dihedraal is, de orde van G oneven is, ...) is een klasse van $\mathrm{Cl}(O_K[G])$ triviaal dan en slechts dan als zijn representant een vrij $O_K[G]$-moduul van rang 1 is.

Alleen gebruikmakend van de definitie van $\mathrm{St}(O_K[G])$ en de Stelling van Stickelberger tonen we in dit proefschrift aan dat $\mathrm{St}(\mathbb{Z}[G])$ triviaal is als $G = C_p$, een cyclische groep van priemorde p, of $G = D_p$, een dihedrale groep van orde $2p$, met $p \geq 3$ priem.
Met de resultaten van McCulloh geeft dit een nieuw bewijs voor het welbekende feit dat $R(\mathbb{Z}[G]) = 1$ in de bovenstaande gevallen, d.w.z. dat de ring van gehelen van een tam vertakte Galoisalgebra over $\mathbb{Q}$ met groep G (waarbij $G = C_p$ of $G = D_p$) een normale basis van gehelen heeft.

Het gedrag van $\mathrm{St}(O_K[G])$ onder basisuitbreiding

Als K een deellichaam van L is, dan induceert de restrictie van L tot K de volgende natuurlijke functor:

$$\mathcal{N}_{L/K} : \mathrm{Cl}(O_L[G]) \longrightarrow \mathrm{Cl}(O_K[G]).$$

In dit proefschrift bestuderen wij het gedrag van de groep $\mathrm{St}(O_K[G])$ onder deze functor.

In het bijzonder tonen we aan dat, voor alle lichamen L en deellichamen K en voor alle eindige groepen G geldt:

$$\mathcal{N}_{L/K}(\mathrm{St}(O_L[G])) \subseteq \mathrm{St}(O_K[G]).$$

Dit heeft de volgende interessante gevolgen:

- als G abels is, volgt met de resultaten van McCulloh dat

$$\mathcal{N}_{L/K}(R(O_L[G])) \subseteq R(O_K[G]),$$

- als elk stabiel vrij $O_K[G]$-moduul vrij is, en $\mathrm{St}(O_K[G]) = 1$ (wat het geval is als $K = \mathbb{Q}$ en $G = C_p$ of $G = D_p$ voor een priemgetal $p \geq 3$), dan leiden wij af dat de ring van gehelen van een tam vertakte Galoisalgebra met Galoisgroep G over een getallenlichaam L dat K bevat, vrij is als $O_K[G]$-moduul.

De vezels van $\mathcal{R}$ en de verdeling van realiseerbare klassen

Als de structuur van $R(O_K[G])$ bekend is, kan men zich afvragen of het aantal tam vertakte Galoisalgebra's dat een bepaalde klasse realiseert, afhankelijk is van de gekozen klasse. We kunnen dit probleem opvatten als de studie van de vezels van onze afbeelding $\mathcal{R}$.

Het werk van A. Agboola laat ons zien dat, als we de tam vertakte Galoisuitbreidingen van K op een bepaalde manier tellen, in het abelse geval het asymptotische aantal van tam vertakte Galoisuitbreidingen die een klasse realiseren onafhankelijk van de gekozen klasse is, of anders gezegd, de tam vertakte Galoisuitbreidingen zijn gelijk verdeeld over de realiseerbare klassen.

In het laatste deel van dit proefschrift beperken we ons tot het abelse geval en bestuderen we aan hieraan gerelateerde vragen.
Eerst beschrijven wij, in termen van een aangepaste versie van $\mathrm{St}(O_K[G])$, de verzameling van realiseerbare klassen verkregen uit tam vertakte Galoisuitbreidingen waar een gegeven priem $\mathfrak{p} \subseteq O_K$ volledig splitst.
Vervolgens bewijzen we dat een analogon van de resultaten van A. Agboola kan worden verkregen voor deze deelverzameling van realiseerbare klassen, d.w.z. het aantal tam vertakte Galoisuitbreidingen waar $\mathfrak{p}$ volledig splitst, die een klasse c realiseren, is in de limiet niet afhankelijk van c;

We eindigen met een vergelijking tussen het zojuist geciteerde werk van A. Agboola en het werk van M. M. Wood die de kansen van verschillende decompositietypes van een vast priemideaal in een Galoisuitbreiding van K met Galoisgroep G bestudeert.

Résumé

Invariants de classe pour algèbres galoisiennes modérément ramifiées

Soient K un corps de nombres d'anneau d'entiers O_K et G un groupe fini.

Une algèbre N sur K, avec une action de G, est dite galoisienne de groupe de Galois G, si N est étale (c.-à-d. un produit d'un nombre fini d'extensions finies de corps sur K) et si G agit sur N comme un groupe d'automorphismes tel que :

- $[N : K] = |G|$,
- $N^G = K$.

Les extensions galoisiennes de corps sont des cas particuliers d'algèbres galoisiennes.

Une algèbre galoisienne N sur K, de groupe de Galois G, est dite *modérément ramifiée* si pour tout $\mathfrak{p}$, idéal maximal de O_K, l'indice de ramification en $\mathfrak{p}$ est premier à la caractéristique du corps résiduel de $\mathfrak{p}$ (ou de façon équivalente s'il existe dans la clôture intégrale O_N de O_K dans N un élément de trace 1).

Le Théorème de Noether

Le *Théorème de la base normale* nous dit qu'une algèbre galoisienne N/K est un $K[G]$-module libre de rang 1, c.-à-d. il existe un élément $b \in N$ tel que $\{s \cdot b\}_{s \in G}$ - l'orbite de b sous l'action de G - forme une base de N sur K.

La question à l'origine du sujet principal de cette thèse est d'obtenir un analogue pour l'anneau d'entiers O_N: soit N une algèbre galoisienne sur K de groupe de Galois G, quand existe-t-il un générateur de base normale d'entiers, c.-à-d. un élément $a \in O_N$ tel que $\{s \cdot a\}_{s \in G}$ forme une base de O_N sur O_K ? Ou, d'une façon équivalente, quand existe-t-il un élément $a \in O_N$ tel que $O_N = O_K[G] \cdot a$? Ce problème est appelé *problème de la base normale d'entiers.*

Si $K = \mathbb{Q}$ et G est abélien, le problème est complètement résolu par le Théorème de Hilbert- Speiser : une algèbre galoisienne abélienne $N/\mathbb{Q}$ a une base normale d'entiers si et seulement si $N/\mathbb{Q}$ est modérément ramifiée.

Si K est différent de $\mathbb{Q}$ ou G est non abélien, ce résultat n'est plus valable en général, même si, grâce à E. Noether, on a un résultat un peu plus faible.

Le *Théorème de Noether* dit qu'une algèbre galoisienne N sur K de groupe de Galois G est modérément ramifiée si et seulement si O_N est un $O_K[G]$-module *localement libre* de rang 1.
L' $O_K[G]$-module O_N est dit *localement libre* de rang 1 si, pour tout idéal premier $\mathfrak{p} \subseteq O_K$, l'anneau $O_{N,\mathfrak{p}} := O_N \otimes_{O_K} O_{K,\mathfrak{p}}$ est un $O_{K,\mathfrak{p}}[G]$-module libre de rang 1 ($O_{K,\mathfrak{p}}$ dénote le complété de O_K par rapport à la métrique induite par $\mathfrak{p}$), c.-à-d. si pour tout $\mathfrak{p}$ il existe un élément $a_\mathfrak{p} \in O_{N,\mathfrak{p}}$ générateur d'une base normale d'entiers de $O_{N,\mathfrak{p}}$ sur $O_{K,\mathfrak{p}}$.
On comprend tout de suite qu'un module libre doit nécessairement être localement libre, donc on voit bien que les algèbres galoisiennes modérément ramifiées sont le cadre correct pour étudier le problème de la base normale d'entiers. En outre, grâce au Théorème de Noether, en restreignant notre attention à l'ensemble des algèbres galoisiennes modérément ramifiées, on peut donc voir que le problème de la base normale d'entiers consiste à comprendre quand un certain module localement libre est libre.

Nous notons $A_G^t(K)$ l'*ensemble* des classes d'isomorphisme des algèbres galoisiennes sur K, de groupe de Galois G, modérément ramifiées et nous considérons $\mathrm{Cl}(O_K[G])$, le groupe des classes des $O_K[G]$-modules localement libres de rang 1, c.-à-d. le groupe donné par les classes d'isomorphisme stable des $O_K[G]$-modules localement libres.
Grâce au Théorème de Noether, on peut considérer l'application d'ensembles pointés

$$\mathcal{R} : A_G^t(K) \longrightarrow \mathrm{Cl}(O_K[G])$$

qui associe à une classe de $A_G^t(K)$ de représentant N la classe dans $\mathrm{Cl}(O_K[G])$ de représentant l'anneau d'entiers O_N.
Cette thèse aborde plusieurs questions liées à l'étude de cette application.

L'image de $\mathcal{R}$ et l'ensemble des classes réalisables

La première question que nous considérons consiste à étudier l'image de l'application $\mathcal{R}$. Nous appelons cette image ensemble des *classes réalisables* et elle sera notée $R(O_K[G])$. Plus explicitement, l'ensemble des classes réalisables est l'ensemble des classes de $\mathrm{Cl}(O_K[G])$ que l'on peut obtenir à partir des anneaux d'entiers des algèbres galoisiennes sur K, de groupe de Galois G, modérément ramifiées.

L'étude des classes réalisables est motivée aussi par ses applications dans d'autres problèmes en théorie des nombres, elle intervient par exemple dans la recherche d'un analogue explicite de certains théorèmes de type Adams–Riemann–Roch connus pour $\mathrm{Cl}(O_K[G])$ et elle donne des informations importantes pour l'étude de l'ensemble en $\mathrm{Cl}(O_K)$ des classes de Steinitz.

Même si l'application $\mathcal{R}$ est une application d'ensembles pointés, on peut se demander si son image, c.-à-d. l'ensemble des classes réalisables, est un sous-groupe de $\mathrm{Cl}(O_K[G])$.

En 1986, L. McCulloh, après avoir introduit un sous-groupe $\mathrm{St}(O_K[G])$ du groupe des classes $\mathrm{Cl}(O_K[G])$ défini en termes de certaines applications de Stickelberger, a montré que, si G est *abélien*, alors

$$R(O_K[G]) = \mathrm{St}(O_K[G]).$$

De ce résultat émerge, dans le cas abélien, une réponse affirmative à la question précédente sur la structure de sous-groupe, c.-à-d., étant données deux classes $c_1,\, c_2 \in R(O_K[G])$, il existe une algèbre galoisienne N sur K, de groupe de Galois G, modérément ramifiée telle que, si $[N]$ dénote sa classe d'isomorphisme, alors $\mathcal{R}([N]) = c_1 + c_2$ (des considérations analogues sont valables pour l'inverse d'une classe réalisable).

Dans le cas d'un groupe G non abélien, la question si l'ensemble des classes réalisables est un sous-groupe de $\mathrm{Cl}(O_K[G])$ est encore ouverte aujourd'hui.
Dans la première partie de cette thèse nous donnons une preuve détaillée d'un résultat non publié de L. McCulloh qui montre que même dans le cas non abélien

$$R(O_K[G]) \subseteq \mathrm{St}(O_K[G]).$$

Savoir si cette inclusion est une égalité, même dans le cas non abélien, est une question encore ouverte.

Le noyau de $\mathcal{R}$ et le problème de la base normale d'entiers

L'étude du noyau de l'application $\mathcal{R}$ est strictement liée au problème de la base normale d'entiers, que nous avons rappelé précédemment.
En fait, dans le cas abélien et dans plusieurs cas non abéliens (p. ex. G diédral, G d'ordre impair, ...), une classe de $\mathrm{Cl}(O_K[G])$ est triviale si et seulement si son représentant est un $O_K[G]$-module libre de rang 1.

Dans cette thèse, en n'utilisant que la définition de $\mathrm{St}(O_K[G])$ et le Théorème classique de Stickelberger, nous montrons que, si $G = C_p$, un groupe cyclique d'ordre premier p, ou $G = D_p$, un groupe diédral d'ordre $2p$, avec p premier impair, alors $\mathrm{St}(\mathbb{Z}[G])$ est trivial.
Comme conséquence, en utilisant les résultats de McCulloh, nous obtenons, par une méthode différente, le résultat bien connu $R(\mathbb{Z}[G]) = 1$ dans les cas ci-dessus, c.-à-d. l'anneau d'entiers d'une algèbre galoisienne sur $\mathbb{Q}$, de groupe de Galois G (où $G = C_p$ ou $G = D_p$), modérément ramifié a une base normale d'entiers.

Le comportement de $\mathrm{St}(O_K[G])$ par rapport au changement de corps de base

Si on considère K contenu dans un autre corps L, la restriction de L à K induit naturellement le foncteur suivant :

$$\mathcal{N}_{L/K} : \mathrm{Cl}(O_L[G]) \longrightarrow \mathrm{Cl}(O_K[G]).$$

Dans cette thése nous étudions le comportement du groupe $\mathrm{St}(O_K[G])$ par rapport à ce foncteur.

En particulier nous montrons que, pour tout corps L et sous-corps K et pour tout groupe fini G,

$$\mathcal{N}_{L/K}(\mathrm{St}(O_L[G])) \subseteq \mathrm{St}(O_K[G]).$$

Ce résultat a des conséquences intéressantes :

- d'abord, si G est abélien, en utilisant les résultats de McCulloh, nous voyons que
$$\mathcal{N}_{L/K}(R(O_L[G])) \subseteq R(O_K[G]),$$
- ensuite si K et G ont les deux propriétés suivantes: pour un $O_K[G]$-module être stablement libre est équivalent a être libre et K est tel que $\mathrm{St}(O_K[G]) = 1$ (ce qui est le cas dans le paragraphe précédent), alors nous en déduisons que l'anneau d'entiers d'une algèbre galoisienne sur un corps de nombres L qui contient K, de groupe de Galois G, modérément ramifiée est libre en tant que $O_K[G]$-module.

Les fibres de $\mathcal{R}$ et la distribution des classes réalisables

Une fois que l'on connait la structure de l'ensemble $R(O_K[G])$, on peut se demander si le nombre d'algèbres galoisiennes modérément ramifiées qui réalisent une classe

varie selon la classe. On peut considérer ce problème comme une étude des fibres de notre application $\mathcal{R}$.

Par rapport à cette question un travail de A. Agboola nous montre que, si on compte les extensions galoisiennes modérément ramifiées de K avec des fonctions qui satisfont certaines caractéristiques, alors dans le cas abélien le nombre asymptotique des extensions galoisiennes modérément ramifiées qui réalisent une classe ne dépend pas de la classe choisie, ou, dit d'une autre façon, les extensions galoisiennes modérément ramifiées sont équidistribuées par rapport à l'ensemble des classes réalisables.

Dans la dernière partie de cette thèse, en nous restreignant au cas abélien, nous avons étudié un problème lié à ce travail.
D'abord nous avons décrit, en termes d'une version modifiée de $\mathrm{St}(O_K[G])$, l'ensemble des classes réalisables obtenues des extensions galoisiennes modérément ramifiées totalement décomposées en un idéal premier $\mathfrak{p} \subseteq O_K$ donné.
Puis nous montrons qu'un analogue des résultats de A.Agboola peut être obtenu pour ce sous-ensemble de classes réalisables, c.-à-d. le nombre des extensions galoisiennes modérément ramifiées totalement décomposées en un idéal premier $\mathfrak{p}$, qui réalisent une classe c, asymptotiquement ne dépend pas de c.

Enfin nous terminons en mettant en évidence des relations entre le travail d'Agboola déjà cité et un travail de M. M. Wood qui étudie les probabilités des différents types de décomposition d'un idéal premier fixé dans une extension galoisienne de K de groupe de Galois G.