Publications mathématiques de Besançon
Algèbre et théorie des nombres

Andrea Siviero

Realisable classes, Stickelberger subgroup and its behaviour under change of the base field

2015, p. 69-92.

<http://pmb.cedram.org/item?id=PMB_2015____69_0>

Publication éditée par le laboratoire de mathématiques de Besançon, UMR 6623 CNRS/UFC

Publications mathématiques de Besançon – 2015, 69-92

REALISABLE CLASSES, STICKELBERGER SUBGROUP AND ITS BEHAVIOUR UNDER CHANGE OF THE BASE FIELD

by

Andrea Siviero

Abstract. — Let K be an algebraic number field with ring of integers O_K and let G be a finite group. We denote by $\mathrm{R}(O_K[G])$ the set of classes in the locally free class group $\mathrm{Cl}(O_K[G])$ realisable by rings of integers in tamely ramified G-Galois K-algebras. McCulloh showed that, for every G, the set $\mathrm{R}(O_K[G])$ is contained in the so-called Stickelberger subgroup $\mathrm{St}(O_K[G])$ of $\mathrm{Cl}(O_K[G])$.

In this paper first we describe the relation between $\mathrm{St}(O_K[G])$ and $\mathrm{Cl}^\circ(O_K[G])$, where $\mathrm{Cl}^\circ(O_K[G])$ is the kernel of the morphism $\mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_K)$, induced by the augmentation map $O_K[G] \longrightarrow O_K$. Then, as an example of computation of $\mathrm{St}(O_K[G])$, we show, just using its definition, that $\mathrm{St}(\mathbb{Z}[G])$ is trivial, when G is a cyclic group of order p or a dihedral group of order $2p$, where p is an odd prime number.

Finally we prove that $\mathrm{St}(O_K[G])$ has good functorial behaviour under change of the base field. This has the interesting consequence that, given an algebraic number field L, if N is a tame Galois L-algebra 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.

Résumé. — Soient K un corps de nombres d'anneau des entiers O_K et G un groupe fini. On note $\mathrm{R}(O_K[G])$ l'ensemble des classes dans le groupe des classes des modules localement libres $\mathrm{Cl}(O_K[G])$ qui peuvent être obtenues par l'anneau des entiers des K-algèbres galoisiennes modérément ramifiées de groupe de Galois G. McCulloh a prouvé que, pour tout G, l'ensemble $\mathrm{R}(O_K[G])$ est contenu dans le soi-disant sous-groupe de Stickelberger $\mathrm{St}(O_K[G])$ dans $\mathrm{Cl}(O_K[G])$.

Dans ce papier d'abord nous nous focalisons sur la relation entre $\mathrm{St}(O_K[G])$ et $\mathrm{Cl}^\circ(O_K[G])$, où $\mathrm{Cl}^\circ(O_K[G])$ est le noyau du morphisme $\mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_K)$, induit par l'augmentation $O_K[G] \longrightarrow O_K$. Puis, comme exemple de calcul du groupe $\mathrm{St}(O_K[G])$, nous montrons, en utilisant sa définition, que $\mathrm{St}(\mathbb{Z}[G])$ est trivial si G est soit un groupe cyclique d'ordre p soit un groupe diédral d'ordre $2p$, avec p premier impair.

Enfin, nous montrons la fonctorialité de $\mathrm{St}(O_K[G])$ par rapport au changement du corps de base. Ceci implique que, soit L est un corps de nombres, si N est une L-algèbre 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.

Mathematical subject classification (2010). — 11R33, 11R04, 11R18, 11R29, 11R32, 11R65.

Key words and phrases. — Galois module structure, Realisable classes, Locally free class groups, Fröhlich's Hom-description of locally free class groups, Stickelberger's theorem.

1. Introduction

Let K be an algebraic number field with ring of integers O_K and let G be a finite group. Given a Galois field extension N/K with Galois group isomorphic to G, we can consider the ring of integers O_N as an $O_K[G]$-module. The classical Noether criterion implies that, when N/K is tamely ramified, then O_N is a *locally free* $O_K[G]$-module of rank 1 and determines a class in the locally free class group $\mathrm{Cl}(O_K[G])$ (for a precise definition see (1) in Section 2). Noether's criterion holds in general for G-Galois K-algebras (a K-algebra N is G-Galois if it is étale and G acts on the left on N as a group of automorphisms, such that $[N:K]=|G|$ and $N^G=K$). Hence, as for field extensions, to every tame G-Galois K-algebra we can associate a class in $\mathrm{Cl}(O_K[G])$.
Let K^{c} be a chosen algebraic closure of K, then it is well-known that, if Ω_K^{t} denotes the Galois group of the maximal tame extension K^{t}/K in K^{c}, then the set of isomorphism classes of tame G-Galois K-algebras is in bijection with $H^1(\Omega_K^{\mathrm{t}}, G)$ (see [Ser94, Chapter I, §5] for a precise definition), the first cohomology set of Ω_K^{t} with coefficients in G (where Ω_K^{t} acts trivially on G). Hence, thanks to Noether's criterion, we can consider the following morphism of pointed sets:

$$\begin{array}{rcl} \mathcal{R}: H^1(\Omega_K^{\mathrm{t}}, G) & \longrightarrow & \mathrm{Cl}(O_K[G]) \\ {[N]} & \longmapsto & [O_N], \end{array}$$

where $[N]$ (resp. $[O_N]$) denotes the associated class of the G-Galois K-algebra N (resp. O_N) in $H^1(\Omega_K^{\mathrm{t}}, G)$ (resp. $\mathrm{Cl}(O_K[G])$).
The set of *realisable classes*, denoted by $\mathrm{R}(O_K[G])$, is defined as the image of $\mathcal{R}$, i.e. it is the set of all classes in $\mathrm{Cl}(O_K[G])$ which can be obtained from the rings of integers of tame G-Galois K-algebras. The problem of realisable classes consists in the study of the structure of this set. One of the main question which is still open nowadays is the following:

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

Note that $\mathcal{R}$, when not trivial, is not a priori a group homomorphism. Indeed, if G is not abelian, the domain of $\mathcal{R}$ is just a pointed set, but even if G is abelian (and so $H^1(\Omega_K^{\mathrm{t}}, G)$ is a group), it is not difficult to find an example which explains why $\mathcal{R}$ is not a group homomorphism (see [Siv13, Appendix]).

When the base field equals $\mathbb{Q}$ and G is abelian it follows from a result by Taylor ([Tay81]), proving a conjecture of Fröhlich, that $\mathrm{R}(\mathbb{Z}[G])$ is trivial. By [Tay81], the same holds if $K=\mathbb{Q}$ and G is a non-abelian group with no irreducible symplectic characters. More generally Taylor proved that any element in $\mathrm{R}(\mathbb{Z}[G])$ has order at most 2 in $\mathrm{Cl}(\mathbb{Z}[G])$.

Over a general number field K, when G is abelian, a positive answer to the previous question is given by Leon McCulloh in [McC87]. 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 Section 2), and he proved the following result.

Theorem 1.1. — *Let G be a finite abelian group. Then, for every algebraic number field K, we have*

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

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, [McC] - for a detailed proof of it, see [Siv13, Chapter 2]).

Theorem 1.2. — *For every algebraic number field K and finite group G, the inclusion* $\mathrm{R}(O_K[G]) \subseteq \mathrm{St}(O_K[G])$ *holds.*

The proof of the reverse inclusion is still unknown. Indeed, when G is non-abelian and $K \neq \mathbb{Q}$, determining if $\mathrm{R}(O_K[G])$ forms a subgroup is in general an open problem.
Nevertheless, starting from the inclusion $\mathrm{R}(O_K[G]) \subseteq \mathrm{Cl}^\circ(O_K[G])$ (where the subgroup $\mathrm{Cl}^\circ(O_K[G])$ is the kernel of the augmentation map from $\mathrm{Cl}(O_K[G])$ to $\mathrm{Cl}(O_K)$, see Section 3), some non-abelian results have been achieved. In particular, it has been proved that $\mathrm{R}(O_K[G]) = \mathrm{Cl}^\circ(O_K[G])$ 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 [BS05a]); and $G = A_4$, without any restriction on the base field K (see [BS05b]).
Recently in [BS13], Nigel P. Byott and Bouchaïb Sodaïgui, under the assumption that K contains a root of unity of prime order p, showed that $\mathrm{R}(O_K[G])$ 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 [BS05b].
More recently, Adebisi Agboola and Leon McCulloh showed that $\mathrm{R}(O_K[G])$ is a subgroup of $\mathrm{Cl}(O_K[G])$ when G is a nilpotent group subject to certain conditions (see [AC15] for the original preprint and further details).
In the non-abelian context, more has been done in describing a weaker form of $\mathrm{R}(O_K[G])$. If $\mathcal{M}$ denotes a maximal order in $K[G]$ containing $O_K[G]$, then, as done for $\mathrm{R}(O_K[G])$, we can define $\mathrm{R}(\mathcal{M})$ to be the subset in $\mathrm{Cl}(\mathcal{M})$ of the classes $[\mathcal{M} \otimes_{O_K[G]} O_L]$, where L runs through the tame G-Galois algebras over K. The two sets $\mathrm{R}(\mathcal{M})$ and $\mathrm{R}(O_K[G])$ are linked by the extension of scalars $\mathrm{Ex} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(\mathcal{M})$ and in fact one has $\mathrm{R}(\mathcal{M}) = \mathrm{Ex}(\mathrm{R}(O_K[G]))$. For a complete list of the works on $\mathrm{R}(\mathcal{M})$ we refer to [Siv13, Introduction].

After a general review of the main definitions and tools, the first aim of this paper is to study explicitly the relation between $\mathrm{St}(O_K[G])$ and $\mathrm{Cl}^\circ(O_K[G])$. In Section 3, we shall prove the following proposition.

Proposition 1. — *For every algebraic number field K and finite group G, the inclusion* $\mathrm{St}(O_K[G]) \subseteq \mathrm{Cl}^\circ(O_K[G])$ *holds.*

We shall exhibit an abelian counterexample showing that the reverse inclusion is not in general true.

In Section 4 we shall give the first main result of this paper. As an example of computation of the group $\mathrm{St}(O_K[G])$, just using its definition, we shall prove the following theorem.

Theorem 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 $G = D_p$, a dihedral group of order $2p$, then* $\mathrm{St}(\mathbb{Z}[G])$ *is trivial.*

This result will immediately imply, just using Theorem 1.2, the following corollary.

Corollary 1. — *In the cases of the theorem above,* $\mathrm{R}(\mathbb{Z}[G])$ *is trivial.*

Remark 1.3. — *For* $p = 2$ *we have that* D_2 *is the Klein four group. Also in this case Theorem 1 holds, thanks to the fact that* $\mathrm{Cl}(\mathbb{Z}[D_2])$ *is trivial (cf.* [CR87, Corollary 50.17]*).*

Note that the result of Corollary 1 was already included in the more general result by Taylor contained in [Tay81]. The proof of Theorem 1 given here does not assume [Tay81], however, but instead uses the definition of $\mathrm{St}(\mathbb{Z}[G])$ and its connection to the classical Stickelberger theorem.
In the dihedral case, the result of Theorem 1 is genuinely new, since the inclusion $\mathrm{R}(\mathbb{Z}[D_p]) \supseteq \mathrm{St}(\mathbb{Z}[D_p])$ is not known a priori because the dihedral group D_p is not abelian. The result obtained for the dihedral case is the more interesting one, since in particular it goes in the direction of extending the equality of Theorem 1.1 to non-abelian groups, giving a non-abelian example where the equality $\mathrm{R}(\mathbb{Z}[G]) = \mathrm{St}(\mathbb{Z}[G])$ holds.

In Section 5 we shall obtain the second main result of this paper concerning the behaviour of $\mathrm{St}(O_K[G])$ under change of the base field K. Namely, if L is an algebraic number field containing K, considering every $O_L[G]$-module as an $O_K[G]$-module, there is a restriction map $\mathcal{N}_{L/K} : \mathrm{Cl}(O_L[G]) \longrightarrow \mathrm{Cl}(O_K[G])$ (see [CR87, §52]). We shall prove the following result.

Theorem 2. — *For every finite group* G*, we have*

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

This will have some nice consequences, such as a new proof of a result by Taylor, contained in [Tay81], which says that the ring of integers of an abelian tame G-Galois K-algebra is free (of rank $[K : \mathbb{Q}]$) over $\mathbb{Z}[G]$.
A final remark will explain that, if we consider the homomorphism given by extension of the base field $\mathrm{ext}_{L/K} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_L[G])$, an analogous result to the previous theorem holds.

Notation and conventions. — Let K be an algebraic 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. $K_\mathfrak{p}^{\mathrm{c}}$) of K (resp. $K_\mathfrak{p}$) and let Ω_K (resp. $\Omega_{K_\mathfrak{p}}$) denote the Galois group of K^{c}/K (resp. $K_\mathfrak{p}^{\mathrm{c}}/K_\mathfrak{p}$).
The symbol Ω_K^{nr} (resp. $\Omega_{K_\mathfrak{p}}^{\mathrm{nr}}$) will denote the Galois group of the maximal unramified (at finite places) extension K^{nr}/K (resp. $K_\mathfrak{p}^{\mathrm{nr}}/K_\mathfrak{p}$) in K^{c} (resp. $K_\mathfrak{p}^{\mathrm{c}}$) and Ω_K^{t} (resp. $\Omega_{K_\mathfrak{p}}^{\mathrm{t}}$) will be the Galois group of the maximal tame extension K^{t}/K (resp. $K_\mathfrak{p}^{\mathrm{t}}/K_\mathfrak{p}$) in K^{c} (resp. $K_\mathfrak{p}^{\mathrm{c}}$). At the infinite places we take $K_\mathfrak{p}^{\mathrm{nr}} = K_\mathfrak{p}^{\mathrm{t}} = K_\mathfrak{p}^{\mathrm{c}}$.
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 $O_{K,\mathfrak{p}}^{\mathrm{c}}$ the integral closure of O_K in $K_\mathfrak{p}^{\mathrm{c}}$. 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 $\{K_{\mathfrak{p}}[G]^\times\}_{\mathfrak{p}}$ with respect to $\{O_{K,\mathfrak{p}}[G]^\times\}_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through the places of K, and $U(O_K[G])$ stands for the product $\prod_{\mathfrak{p}} O_{K,\mathfrak{p}}[G]^\times$. The symbol $J(K^{\mathrm{c}})$ (resp. $U(O_K^{\mathrm{c}})$) 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 paper, G will denote a finite group, G^{ab} its abelianization and $\overline{G}$ its set of conjugacy classes. Given an element s in G, we denote by $\overline{s}$ its conjugacy class.
The set of irreducible complex characters of G will be denoted by $\mathrm{Irr}(G)$ and R_G will stand for the ring of virtual characters of G, i.e. the ring of $\mathbb{Z}$-linear combinations of elements in $\mathrm{Irr}(G)$.

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 $f \in \mathrm{Hom}(H, H')$, 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 absolute Galois group Ω_K naturally acts on the left on $\mathrm{Irr}(G)$ by $\chi^\omega(s) = \chi(s)^\omega$, where $\omega \in \Omega_K$, $\chi \in \mathrm{Irr}(G)$ and $s \in G$. We extend this action by linearity to R_G. When we have an Ω_K-action on a set, we can always consider a $\Omega_{K_{\mathfrak{p}}}$-action on the same set, considering $\Omega_{K_{\mathfrak{p}}}$ embedded into Ω_K.

Given a rational number $a \in \mathbb{Q}$, the symbol $\lfloor a \rfloor$ (resp. $\{a\}$) denotes its integer (resp. fractional) part.

2. Review of the main definitions and tools

In this section we briefly recall the main tools needed to describe McCulloh's results on realisable classes. We will not focus on any proof in particular, referring to the original works for more details. We recall from the Introduction that K is an algebraic number field and G a finite group.

2.1. Locally free class group. — Let M be an $O_K[G]$-lattice (i.e. an $O_K[G]$-module, finitely generated and projective as O_K-module) and let $M_{\mathfrak{p}}$ denote the tensor product $O_{K,\mathfrak{p}} \otimes_{O_K} M$. We say that M is in the genus of $O_K[G]$ (or M is a locally free $O_K[G]$-module of rank 1) if, for every maximal ideal $\mathfrak{p}$ of O_K, there is an isomorphism $M_{\mathfrak{p}} \cong O_{K,\mathfrak{p}}[G]$. We denote by $g(O_K[G])$ the set of all $O_K[G]$-lattices in the genus of $O_K[G]$. Moreover given two $O_K[G]$-lattices M and N, we say that M is stably isomorphic to N and we denote it by $M \cong_s N$, if $M \oplus O_K[G]^n \cong N \oplus O_K[G]^n$, for some $n \geq 1$.

Remark 2.2. — *Note that in general $M \cong_s N \not\Rightarrow M \cong N$ (see* [Swa62] *for an explicit example). Nevertheless there are many groups G for which two $O_K[G]$-lattices which are stably* *isomorphic are isomorphic too (e.g. abelian groups, dihedral groups, groups of odd order). We refer to* [CR87, §51C] *for more details.*

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

$$\mathrm{Cl}(O_K[G]) := \{[M]_s : M \in g(O_K[G])\} \tag{1}$$

and we call it the *locally free class group* of $O_K[G]$. Now, on this set, we can define a well-defined operation. Given $[M_1]_s$ and $[M_2]_s$ in $\mathrm{Cl}(O_K[G])$, let us set

$$[M_1]_s + [M_2]_s := [M_3]_s, \tag{2}$$

where, M_3 is an $O_K[G]$-lattice in $g(O_K[G])$ such that $M_1 \oplus M_2 \cong O_K[G] \oplus M_3$ (the existence of such an $O_K[G]$-lattice M_3 follows from a lemma of Roiter, see [CR81, 31.6]).
As one can see, under this operation, $\mathrm{Cl}(O_K[G])$ is an abelian group (see [CR87, §49A] for more details). Moreover, Jordan–Zassenhaus theorem (see [Rei03, Theorem 26.4]) tells us that the number of isomorphism classes of $O_K[G]$-lattices in $g(O_K[G])$ is finite, so a fortiori $\mathrm{Cl}(O_K[G])$ is finite.

Remark 2.3. — *Given an $O_K[G]$-lattice M, its associated class in* $\mathrm{Cl}(O_K[G])$ *is trivial if and only if $M \cong_s O_K[G]$. Note that by the previous remark, if G is abelian, dihedral or of odd order, then this is equivalent to say that $M \cong O_K[G]$.*

2.4. Hom-description. — Fröhlich gave a useful description of the locally free class group $\mathrm{Cl}(O_K[G])$ in terms of some Ω_K-equivariant homomorphisms. This description is well-known as the Hom-description of $\mathrm{Cl}(O_K[G])$.
Let us consider the determinant map $\mathrm{Det} : U(O_K[G]) \longrightarrow \mathrm{Hom}_{\Omega_K}(R_G, J(K^c))$, obtained componentwise by the linear extension of the map on $\mathrm{Irr}(G)$ given by $\mathrm{Det}(a)(\chi) = \det(T_\chi(a))$, where T_χ is a complex representation affording the character χ and det is the usual determinant of a matrix.
The Hom-description of $\mathrm{Cl}(O_K[G])$ is given by the following isomorphism

$$\mathrm{Cl}(O_K[G]) \cong \frac{\mathrm{Hom}_{\Omega_K}(R_G, J(K^{\mathrm{c}}))}{\mathrm{Hom}_{\Omega_K}(R_G, (K^{\mathrm{c}})^\times) \cdot \mathrm{Det}(U(O_K[G]))}. \tag{3}$$

Remark 2.5. — *For a given class in* $\mathrm{Cl}(O_K[G])$ *to be trivial means that the representative homomorphism $f \in \mathrm{Hom}_{\Omega_K}(R_G, J(K^{\mathrm{c}}))$, under the previous isomorphism, can be written as $f = gd$, where $g \in \mathrm{Hom}_{\Omega_K}\left(R_G, (K^c)^\times\right)$, a global homomorphism fixed by Ω_K, and d belongs to* $\mathrm{Det}\left(U\left(O_K[G]\right)\right)$.

2.6. The map Rag_K. — Given a character $\chi \in \mathrm{Irr}(G)$, we define a map $\det_\chi$ on the group G as

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

where T_χ is, as above, a complex representation associated to χ. Note that $\det_\chi$ can be considered as a character of G of degree 1 (or equivalently as a character of G^{ab}).
This definition is independent of the choice of the representation T_χ and we can in turn consider the homomorphism $\overline{\det} : R_G \longrightarrow \mathrm{Irr}(G^{\mathrm{ab}})$ defined by

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

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:

$$0 \longrightarrow \mathcal{A}_G \longrightarrow R_G \xrightarrow{\overline{\det}} \mathrm{Irr}(G^{\mathrm{ab}}) \longrightarrow 1. \tag{4}$$

Remark 2.7. — *When the group G is abelian we have an explicit $\mathbb{Z}$-basis of $\mathcal{A}_G$. From the proof of* [McC87, 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 every $\chi \in \mathrm{Irr}(G)$ is written uniquely as $\chi = \prod_{i=1}^{k} \chi_i^{r_i(\chi)}$, where $0 \le r_i(\chi) < e_i$; a $\mathbb{Z}$-basis of $\mathcal{A}_G$ is given by the non-zero elements in the collection $\{e_i\chi_i | \, i = 1, \ldots, k\} \cup \{\chi - \sum_{i=1}^{k} r_i(\chi)\chi_i | \, \chi \in \mathrm{Irr}(G)\}$.*

For every finite place $\mathfrak{p}$ of K, applying the functor $\mathrm{Hom}(-, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times)$ to the short exact sequence (4), we get the following short exact sequence

$$1 \to \mathrm{Hom}\left(\mathrm{Irr}(G^{\mathrm{ab}}), (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right) \to \mathrm{Hom}\left(R_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right) \xrightarrow{\mathrm{rag}} \mathrm{Hom}\left(\mathcal{A}_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right) \to 1$$

where the map rag is just the restriction map to the augmentation kernel (this also explains its name). Now using the local analog of the functor Det, previously defined, we have the following proposition.

Proposition 2.8. — *For every finite place $\mathfrak{p}$ of K, there is a commutative $\Omega_{K_\mathfrak{p}}$-diagram (every map preserves the $\Omega_{K_\mathfrak{p}}$-action) of pointed sets with exact rows:*

$$\begin{tikzcd}
1 \arrow[r] & G \arrow[r] \arrow[d, "\mathrm{Det}"] & O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times \arrow[r] \arrow[d, "\mathrm{Det}"] & O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times/G \arrow[r] \arrow[d, "\widetilde{\mathrm{Det}}"] & 1 \\
1 \arrow[r] & G^{\mathrm{ab}} \arrow[r] & \mathrm{Hom}\left(R_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right) \arrow[r, "\mathrm{rag}"] & \mathrm{Hom}\left(\mathcal{A}_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right) \arrow[r] & 1
\end{tikzcd}$$

Proof. — If $s \in G$, then $\mathrm{Det}(s)(\chi) = \det_\chi(s)$. So, from the definition of the map Det and from the identification of $\mathrm{Hom}\left(\mathrm{Irr}(G^{\mathrm{ab}}), (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right)$ with G^{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 $G/[G,G]$. Thus Det induces a map $\widetilde{\mathrm{Det}} : O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times/G \longrightarrow \mathrm{Hom}\left(\mathcal{A}_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right)$, making the diagram commute. □

Let us define the pointed set

$$\mathcal{H}(O_{K,\mathfrak{p}}[G]) := (O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times/G)^{\Omega_{K_\mathfrak{p}}} \tag{5}$$

Taking now the $\Omega_{K_\mathfrak{p}}$-invariants we deduce the following proposition.

Proposition 2.9. — *For every finite place $\mathfrak{p}$ of K, we have the following commutative diagram with exact rows:*

$$\begin{tikzcd}
1 \arrow[r] & G \arrow[r] \arrow[d, "\mathrm{Det}"] & O_{K,\mathfrak{p}}[G]^\times \arrow[r] \arrow[d, "\mathrm{Det}"] & \mathcal{H}(O_{K,\mathfrak{p}}[G]) \arrow[r] \arrow[d, "\widetilde{\mathrm{Det}}"] & H^1(\Omega^{\mathrm{nr}}_{K_\mathfrak{p}}, G) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & G^{\mathrm{ab}} \arrow[r] & \mathrm{Hom}_{\Omega_{K_\mathfrak{p}}}\left(R_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right) \arrow[r, "\mathrm{rag}"] & \mathrm{Hom}_{\Omega_{K_\mathfrak{p}}}\left(\mathcal{A}_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right) \arrow[r] & \mathrm{Hom}\left(\Omega^{\mathrm{nr}}_{K_\mathfrak{p}}, G^{\mathrm{ab}}\right) \arrow[r] & 1 .
\end{tikzcd}$$

Moreover the set $\widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$ is a subgroup of $\mathrm{Hom}_{\Omega_{K_\mathfrak{p}}}\left(\mathcal{A}_G, (O^{\mathrm{c}}_{K,\mathfrak{p}})^\times\right)$.

Proof. — The first part of the proposition follows from Proposition 2.8, applying $\Omega_{K_{\mathfrak{p}}}$-cohomology. In particular exactness at the top row comes from the fact that any local unramified extension has a normal integral basis generator, while exactness at the bottom row is a consequence of the fact that the map $H^1(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G) \longrightarrow \mathrm{Hom}(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G^{\mathrm{ab}})$, induced by the natural map from $\mathrm{Hom}(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G)$ to $\mathrm{Hom}(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G^{\mathrm{ab}})$, is surjective as one can check using the description of $\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}$ as a procyclic group.
For the second part of the proposition, we observe that, for every finite place $\mathfrak{p}$, there is a one-to-one correspondence between $O_{K,\mathfrak{p}}[G]^{\times}\backslash\mathcal{H}(O_{K,\mathfrak{p}}[G])$ and $H^1(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G)$. Thus, applying the map $\widetilde{\mathrm{Det}}$ and using the fact that the map $H^1(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G) \longrightarrow \mathrm{Hom}(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G^{\mathrm{ab}})$ is surjective, we get

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

From this and using the fact that $\mathrm{Hom}(\Omega_{K_{\mathfrak{p}}}^{\mathrm{nr}}, G^{\mathrm{ab}})$ is an abelian group, the group structure of $\widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G]))$ follows. For more details on this proof we refer to [Siv13, Propositions 2.2.6 and 2.2.7]. □

Now, if we write

$$\mathcal{U}(O_K[G]) := \prod_{\mathfrak{p}} \widetilde{\mathrm{Det}}(\mathcal{H}(O_{K,\mathfrak{p}}[G])) \subseteq \mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, J(K^{\mathrm{c}})) \tag{6}$$

and we define the group

$$\mathrm{MCl}(O_K[G]) := \frac{\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, J(K^{\mathrm{c}}))}{\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}) \cdot \mathcal{U}(O_K[G])}, \tag{7}$$

we see that the restriction map $\mathrm{rag} : \mathrm{Hom}_{\Omega_K}(R_G, J(K^{\mathrm{c}})) \longrightarrow \mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, J(K^{\mathrm{c}}))$ and Proposition 2.9, yield a group homomorphism

$$\mathrm{Rag}_K : \frac{\mathrm{Hom}_{\Omega_K}(R_G, J(K^{\mathrm{c}}))}{\mathrm{Hom}_{\Omega_K}(R_G, (K^{\mathrm{c}})^{\times}) \cdot \mathrm{Det}(U(O_K[G]))} \longrightarrow \frac{\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, J(K^{\mathrm{c}}))}{\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, (K^{\mathrm{c}})^{\times}) \cdot \mathcal{U}(O_K[G])}. \tag{8}$$

Using the Hom-description of $\mathrm{Cl}(O_K[G])$ (see (3)), this can be written as

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

2.10. The Stickelberger map. — We introduce now one of the main ingredient of McCulloh's results, the so called Stickelberger map. The original definition of the Stickelberger map, when G is abelian, is contained in [McC87], while its extension to the non-abelian case was presented for the first time by McCulloh in a talk given in Oberwolfach in 2002 ([McC]). 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 [McC87] (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 $\langle -, - \rangle : \mathbb{Q} \otimes_{\mathbb{Z}} R_G \times \mathbb{Q}[G] \longrightarrow \mathbb{Q}$.

⋆ *Characters of higher degree*: If χ is a character of degree bigger than 1, then we define

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

where $\operatorname{res}^G_{\langle s\rangle} \chi$ 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 as

$$\Theta_G(\alpha) := \sum_{s\in G} \langle \alpha, s\rangle s, \quad \text{for } \alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G.$$

An important property of $\mathcal{A}_G$ is given by the following proposition.

Proposition 2.11. — *Let $\alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G$, then $\Theta_G(\alpha) \in \mathbb{Z}[G] \iff \alpha \in \mathcal{A}_G$. In particular Θ_G induces a homomorphism $\Theta_G : \mathcal{A}_G \longrightarrow \mathbb{Z}[G]$.*

Proof. — See [McC, Proposition 1]. □

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

Definition. — *Let m be the exponent of G and let μ_m be the group of m-th roots of unity. Restricting Ω_K to $\mathrm{Gal}\,(K\,(\mu_m)\,/K)$, we consider the map $\kappa : \Omega_K \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ 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_K-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 $\chi\,(s)^\omega$, we get

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

By bilinearity, we deduce that, for all $\alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G$ and for all $s \in G(-1)$,

$$\langle \alpha^\omega, s\rangle = \langle \alpha, s^{\kappa(\omega)}\rangle = \langle \alpha, s^{\omega^{-1}}\rangle. \tag{9}$$

Applying this to the Stickelberger map, we get

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

from which we deduce the following proposition.

Proposition 2.12. — *The map $\Theta_G : \mathbb{Q}\otimes_{\mathbb{Z}} R_G \longrightarrow \mathbb{Q}[G(-1)]$ is an Ω_K-homomorphism, i.e.*

$$\Theta_G(\alpha^\omega) = \Theta_G\,(\alpha)^\omega\,, \text{ for all } \alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} R_G \text{ and } \omega \in \Omega_K.$$

The pairing $\langle \chi, s\rangle$ just depends on the conjugacy class of $s \in G$ and hence $\Theta_G(\mathbb{Q} \otimes_{\mathbb{Z}} R_G) \subseteq Z(\mathbb{Q}[G])$, where $Z(\mathbb{Q}[G])$ is the centre of the group algebra $\mathbb{Q}[G]$, with basis the conjugacy class sum of G. If we denote by $\overline{G}$ the set of conjugacy classes of G, then the action of Ω_K via κ^{-1} preserves conjugacy classes and it induces an Ω_K-action on $\mathbb{Z}[\overline{G}]$; we denote this Ω_K-module by $\mathbb{Z}[\overline{G}(-1)]$. Thus, defining the Stickelberger pairing on the set of conjugacy classes as

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

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

$$\begin{aligned}(10)\qquad \Theta_{\overline{G}}:\ \mathbb{Q}\otimes_{\mathbb{Z}} R_G &\longrightarrow \mathbb{Q}[\overline{G}]\\ \alpha &\longmapsto \sum_{\overline{s}\in\overline{G}}\langle\alpha,\,\overline{s}\rangle\overline{s}.\end{aligned}$$

Again we have $\Theta_{\overline{G}}(\alpha)\in\mathbb{Z}[\overline{G}]\iff\alpha\in\mathcal{A}_G$. Thus, transposing the map $\Theta_{\overline{G}}:\mathcal{A}_G\to\mathbb{Z}[\overline{G}(-1)]$, we get the Ω_K-equivariant homomorphism

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

Hence, if we write

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

the map $\Theta^{\mathrm{t}}_{\overline{G},K}$ induces a homomorphism

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

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

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

Moreover $\Theta^{\mathrm{t}}_{\overline{G},K_{\mathfrak{p}}}(\overline{\Lambda}_{\mathfrak{p}}^{\times})\subseteq\mathrm{Hom}_{\Omega_{K_{\mathfrak{p}}}}\left(\mathcal{A}_G,(O_{K,\mathfrak{p}}^{\mathrm{c}})^{\times}\right)$. At the infinite places, since we set $O_{K,\mathfrak{p}}=K_{\mathfrak{p}}$, we have $\overline{\Lambda}_{\mathfrak{p}}=K_{\mathfrak{p}}\overline{\Lambda}_{\mathfrak{p}}$.
Thus, defining the idèle group $J(K\overline{\Lambda})$ as the restricted product of $\{(K_{\mathfrak{p}}\overline{\Lambda}_{\mathfrak{p}})^{\times}\}_{\mathfrak{p}}$ with respect to $\{\overline{\Lambda}_{\mathfrak{p}}^{\times}\}_{\mathfrak{p}}$, the homomorphisms $\Theta^{\mathrm{t}}_{\overline{G},K_{\mathfrak{p}}}$ combine to give an idelic transpose Stickelberger homomorphism:

$$(11)\qquad \Theta^{\mathrm{t}}_{\overline{G},K}:J(K\overline{\Lambda})\longrightarrow\mathrm{Hom}_{\Omega_K}\left(\mathcal{A}_G,J\left(K^{\mathrm{c}}\right)\right).$$

Remark 2.13. — *We can also define $J(K\overline{\Lambda})$ as $\mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\overline{G}(-1)],J(K^{\mathrm{c}})\right)$; for details see* [McC87, Remark 6.22].

Remark 2.14. — *If G is abelian, we can remove the "bar" from all our notation, since $G=\overline{G}$. In the sequel, if G is abelian, we will adopt this simplification in the notation.*

2.15. The Stickelberger subgroup and McCulloh's results. — We can finally define the Stickelberger subgroup $\mathrm{St}(O_K[G])$ and state McCulloh's main results on realisable classes. Thanks to the definitions given in the previous parts, we have the following group homomorphisms

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

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

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

$$\mathrm{St}(O_K[G]) := \mathrm{Rag}_K^{-1}\left(\mathrm{Im}\left(\Theta^{\mathrm{t}}_{\overline{G},K}\right)\right).$$

Remark 2.16. — *The description and the notation used for* $\mathrm{St}(O_K[G])$ *do not reflect McCulloh's original choice, but they are rather inspired from some later informal notes by A. Agboola.*

Denoting by $\mathrm{R}_{\mathrm{nr}}(O_K[G])$, the set of realisable classes obtained from unramified G-Galois K-algebras, McCulloh's results then follow (the next theorem is a more detailed version of Theorem 1.1 and Theorem 1.2 in the Introduction).

Theorem 2.17. — *For every finite group G and algebraic number field K, we get*

$$\mathrm{R}_{\mathrm{nr}}(O_K[G]) \subseteq \mathrm{Ker}(\mathrm{Rag}_K), \tag{12}$$

$$\mathrm{R}(O_K[G]) \subseteq \mathrm{St}(O_K[G]). \tag{13}$$

Furthermore, when G is abelian, we have

$$\mathrm{R}_{\mathrm{nr}}(O_K[G]) = \mathrm{Ker}(\mathrm{Rag}_K), \tag{14}$$

$$\mathrm{R}(O_K[G]) = \mathrm{St}(O_K[G]). \tag{15}$$

Proof. — The equalities concerning the abelian case are proved in [McC87], while the first inclusions are claimed in some unpublished notes on two talks given by McCulloh in Oberwolfach in 2002 ([McC]) and in Luminy in 2011. For a precise proof of them we refer to [Siv13, Chapter 2]. □

3. Comparison between $\mathrm{St}(O_K[G])$ and $\mathrm{Cl}^\circ(O_K[G])$

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

Proposition 3.1. — *For every algebraic number field K and finite group G,*

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

Proof. — The original proof is contained in [McC77] (see also [McC83]). □

Remark 3.2. — *In terms of the Hom-description, we have the following isomorphism*

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

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 [BS05a]*).*

Considering the inclusion $\mathrm{R}(O_K[G]) \subseteq \mathrm{St}(O_K[G])$ (cf. Theorem 2.17), 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 1. — *For every algebraic number field K and finite group G, we get*

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

Proof. — Let us consider a class $c \in \mathrm{St}(O_K[G])$ represented in terms of the Hom-description by $f \in \mathrm{Hom}_{\Omega_K}(R_G, J(K^{\mathrm{c}}))$. In order to prove that c belongs to $\mathrm{Cl}^\circ(O_K[G])$, we need to show that $f(\chi_0) \in K^\times \cdot U(O_K)$ (see [BS05a, Proposition 2.1]).
Since for every 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

$$\mathrm{rag}(f) \in \mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, (K^{\mathrm{c}})^\times) \cdot \mathcal{U}(O_K[G]) \cdot \Theta^{\mathrm{t}}_{\overline{G}, K}(J(K\overline{\Lambda})),$$

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

- $\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, (K^{\mathrm{c}})^\times)$: If we take $g \in \mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, (K^{\mathrm{c}})^\times)$, the fact that it is Ω_K-equivariant means that, for every $\omega \in \Omega_K$, we have $g(\chi)^\omega = g(\chi^\omega)$. Thus, when we consider the value $g(\chi_0)$, we get that, for every $\omega \in \Omega_K$,

  $$g(\chi_0)^\omega = g(\chi_0^\omega) = g(\chi_0).$$

  Then $g(\chi_0) \in K^\times$, since it is fixed by Ω_K. So we have shown that every element in the group $\mathrm{Hom}_{\Omega_K}(\mathcal{A}_G, (K^{\mathrm{c}})^\times)$ evaluated at χ_0 gives a an 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 $a := \sum_{s \in G} a_s s \in K^{\mathrm{c}}[G]$, we obtain $\mathrm{Det}(a)(\chi_0) = T_{\chi_0}(a) = \sum_{s \in G} a_s$ (where T_{χ_0} is the trivial representation).
  If we take $x_\mathfrak{p} \in (O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times / G)^{\Omega_{K_\mathfrak{p}}}$ represented by $a_\mathfrak{p} \in O^{\mathrm{c}}_{K,\mathfrak{p}}[G]^\times$, we have

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

  Now, for every $\omega \in \Omega_{K_\mathfrak{p}}$, we have $a_\mathfrak{p}^\omega = a_\mathfrak{p} \cdot s'$, where $s' \in G$. Thus, applying T_{χ_0}, we get $T_{\chi_0}(a_\mathfrak{p})^\omega = T_{\chi_0}(a_\mathfrak{p})$. Hence, for each $\mathfrak{p}$, the element $\mathrm{Det}(a_\mathfrak{p})(\chi_0)$ belongs to $O^\times_{K,\mathfrak{p}}$. Thus, every element in $\mathcal{U}(O_K[G])$, when evaluated at χ_0, gives an element in $U(O_K)$.

- $\Theta^{\mathrm{t}}_{\overline{G}, K}(J(K\overline{\Lambda}))$: Given $h \in J(K\overline{\Lambda})$, by definition, we have that $\Theta^{\mathrm{t}}_{\overline{G}, K}(h)(\chi_0)$ equal to $h(\Theta_{\overline{G}}(\chi_0))$. Moreover $\Theta_{\overline{G}}(\chi_0) = 0$, since $\chi_0(s) = 1$ for every $s \in G$. Thus, every element in $\Theta^{\mathrm{t}}_{\overline{G}, K}(J(K\overline{\Lambda}))$ evaluated at χ_0 is trivial.

Combining all together, we can now see that, if we take $c \in \mathrm{St}(O_K[G])$ and we consider a representative of it $f \in \mathrm{Hom}_{\Omega_K}(R_G, J(K^{\mathrm{c}}))$, 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 [BS05b]), 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 [Rim59], 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 $\mathrm{Cl}(\mathbb{Z})$ is trivial, we get $\mathrm{Cl}^\circ(\mathbb{Z}[C_p]) = \mathrm{Cl}(\mathbb{Z}[C_p])$.

We know that $\mathrm{R}(\mathbb{Z}[C_p])$ is trivial and so, by McCulloh's results, the same is true for $\mathrm{St}(\mathbb{Z}[C_p])$. Thus, just taking a cyclic group C_p, with a prime number p such that the class number of $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ is not one (e.g. $p = 23$, see [Was97, Chapter 11]), we have a simple example of a group G and a number field K for which $\mathrm{St}(O_K[G]) \subsetneq \mathrm{Cl}^\circ(O_K[G])$.

4. Computing the Stickelberger subgroup

In this section we explicitly compute $\mathrm{St}(O_K[G])$ in some special cases, just using its algebraic definition and the classical Stickelberger theorem. In particular, we shall prove the next result, already announced in the Introduction.

Theorem 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 $G = D_p$, a dihedral group of order $2p$, then* $\mathrm{St}(\mathbb{Z}[G])$ *is trivial.*

This result, as explained in the Introduction, implies the following corollary.

Corollary 1. — *In the cases of the theorem above,* $\mathrm{R}(\mathbb{Z}[G])$ *is trivial.*

4.1. The classical Stickelberger theorem. — First, we briefly recall here some annihilation results for class groups.

Let $N/\mathbb{Q}$ be a finite abelian extension, by the Kronecker–Weber theorem, $N \subseteq \mathbb{Q}(\zeta_n)$ (where 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

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

We have the following classical theorem.

Theorem 4.2. — (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. — [Was97, Theorem 6.10]. □

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

Theorem 4.3. — *Let L be the cyclotomic extension $\mathbb{Q}(\zeta_n)$, 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 $(\Psi_{a,b}) \cdot \mathfrak{P}$ 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. — [Lan94, Chapter IV, §4, Theorem 11]. □

4.4. 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 $\mathrm{Irr}(C_p)$ 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 counterexample of the previous section, describes $\mathrm{Cl}(\mathbb{Z}[C_p])$ in terms of the class group of the cyclotomic extension $\mathbb{Q}(\zeta_p)$ and is due to D. S. Rim. Using the Hom-description for the class group $\mathrm{Cl}(\mathbb{Z}[C_p])$, we can state it in the following way.

Lemma 4.5. — *Let p be a prime number and let ζ_p be a primitive p-th root of unity. The following group isomorphism holds:*

$$\begin{array}{rccc} \mathcal{L}: & \mathrm{Cl}(\mathbb{Z}[C_p]) & \xrightarrow{\cong} & \mathrm{Cl}(\mathbb{Z}[\zeta_p]) \\ & c = [f] & \longmapsto & [f(\chi_p)]\ . \end{array} \tag{16}$$

Proof. — This is a result contained in [Rim59] and here rewritten in terms of the Hom-description, after having recalled the idelic representation of the ideal class group

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

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

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 $\mathrm{Irr}(D_p)$ consists of two characters ψ_0 and ψ_0' of dimension 1 and $(p-1)/2$ characters ψ_j (with $j = 1, \dots, (p-1)/2$) of dimension 2. The character ψ_0 is the trivial character, while ψ_0' sends r^k to 1 and sr^k to -1, for $k = 0, \dots, p-1$. The characters ψ_j, for $j = 1, \dots, (p-1)/2$, are defined as

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

For D_p an analogous result to Lemma 4.5 follows.

Lemma 4.6. — *Let p be an odd prime number and let ζ_p be as above. 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 [CR87, Theorem 50.25] for more details. □

4.7. The Stickelberger map for C_p and D_p. — For every 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 $\langle \chi_p^i, t^j\rangle = \left\{\dfrac{ij}{p}\right\}$, for $j = 0, \dots, p-1$ and $i = 1, \dots, p-1$. 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 $k = 0, \dots, p - 1$. We adopt the same notation of the characters of C_p used above for the characters of $\langle r\rangle$ and we denote by ϕ_0, ϕ_0' the trivial and the non-trivial character of $\langle sr^k\rangle$, respectively. Then, for the characters of dimension 1 we clearly have

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

while, for the characters of dimension 2, using the inner products and some computations, we get

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

and for the subgroups $\langle sr^k\rangle$, where $k = 0, \dots, p-1$, we have

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

We easily deduce the values of the Stickelberger pairings on the elements of $\operatorname{Irr}(D_p)$:

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

We can now consider the Stickelberger map on the conjugacy classes $\Theta_{\overline{D_p}} : \mathbb{Q}\otimes_{\mathbb{Z}} R_{D_p} \to \mathbb{Q}[\overline{D_p}]$ (cf. (10)). There are $(p+3)/2$ conjugacy classes of D_p:

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

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

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

4.8. The augmentation kernels $\mathcal{A}_{C_p}$ and $\mathcal{A}_{D_p}$. — As we have already seen in Remark 2.7, we have the following lemma.

Lemma 4.9. — *Let p be a prime number, then*

$$\mathcal{A}_{C_2} = \langle \chi_0,\, 2\chi_2 \rangle\,,$$
$$\mathcal{A}_{C_p} = \langle \chi_0,\, j\chi_p - \chi_p^j,\, p\chi_p \rangle, \;\; \textit{for}\;\; 2 \le j \le p-1, \;\; \textit{with}\; p \neq 2.$$

An analogous result for the dihedral group D_p follows.

Lemma 4.10. — *Let p be an odd prime number, then*

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

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

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

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

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

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

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

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. □

4.11. The triviality of $\Theta^{\mathrm{t}}_{C_p,\mathbb{Q}}$ and $\Theta^{\mathrm{t}}_{\overline{D_p},\mathbb{Q}}$. — Once we know the structure of the augmentation kernel $\mathcal{A}_{C_p}$, we can apply the classical Stickelberger theorem for the computation of $\Theta^{\mathrm{t}}_{C_p,\mathbb{Q}}\left(\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}^c))\right)$, as the following proposition explains.

Proposition 4.12. — *For every prime number p,*

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

Proof. — The group $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}^c))$ is equal to $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}(\zeta_p)))$ (think about the $\Omega_{\mathbb{Q}}$-action) and, given an element $h \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathbb{Z}[C_p(-1)], J(\mathbb{Q}(\zeta_p)))$, we immediately understand that, thanks to the $\Omega_{\mathbb{Q}}$-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 $\Omega_{\mathbb{Q}}$-action on $C_p(-1)$), where, as before, the automorphism $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 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 $\Omega_{\mathbb{Q}}$-invariance, we have $h(t^i) = \sigma_i^{-1} \cdot x$.

Now, using the description of the Stickelberger map given above, on the generators of $\mathcal{A}_{C_p}$ we get

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

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

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

Now, using the idelic representation of $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ recalled in the proof of Lemma 4.5, we immediately deduce from Theorem 4.2 that $\Theta^{\mathrm{t}}_{C_p,\mathbb{Q}}(h)(p\chi_p)$ is trivial once considered in $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$. This means that $\Theta^{\mathrm{t}}_{C_p,\mathbb{Q}}(h)(p\chi_p)\in\mathbb{Q}(\zeta_p)^\times\cdot U(\mathbb{Z}[\zeta_p])$, which proves the proposition for $p=2$. When $p\neq 2$, for the other generators $j\chi_p-\chi_p^j$, we use Theorem 4.3 on the cyclotomic extension $\mathbb{Q}(\zeta_p)$ and we proceed by induction. Starting with $j=2$, we get

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

and using Theorem 4.3, with $a=b=1$, we get $\Theta^{\mathrm{t}}_{C_p,\mathbb{Q}}(h)(2\chi_p-\chi_p^2)\in\mathbb{Q}(\zeta_p)^\times\cdot U(\mathbb{Z}[\zeta_p])$ (proving the result for $p=3$).
For $p>3$, let j be a natural number in $\{2,\dots,p-1\}$, denote $\Theta^{\mathrm{t}}_{C_p,\mathbb{Q}}(h)(j\chi_p-\chi_p^j)$ 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 4.3 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 concludes the proof. ☐

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

Proposition 4.13. — *Let p be an odd prime number. Then*

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

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

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

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 $\left\{\overline{r^k}\right\}_{k=1,\ldots,(p-1)/2}$.

We see that $\Theta^{\mathrm{t}}_{\overline{D_p},\mathbb{Q}}(h)(\psi_0)$ and $\Theta^{\mathrm{t}}_{\overline{D_p},\mathbb{Q}}(h)(2\psi_0')$ 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). The same holds for $\Theta^{\mathrm{t}}_{\overline{D_p},\mathbb{Q}}(h)(\psi_0' - \psi_j)$, with $j = 1, \ldots, (p-1)/2$, since $(\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q})} \sigma) \cdot y = \mathrm{N}_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q}}(y)$. This concludes the proof. □

4.14. Proof of Theorem 1. — Let us consider the isomorphism $\mathcal{L}$, given in Lemma 4.5. For every $\omega \in \Omega_{\mathbb{Q}}$ and $c \in \mathrm{Cl}(\mathbb{Z}[C_p])$, represented in terms of the Hom-description by $f \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{C_p}, J(\mathbb{Q}^c))$, 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 $\Omega_{\mathbb{Q}}$-equivariance of f.

Using again the classical Stickelberger theorem and the isomorphism $\mathcal{L}$ between the locally free class group $\mathrm{Cl}(\mathbb{Z}[C_p])$ and the ideal class group $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$, we can now prove the following proposition.

Proposition 4.15. — *Let p be a prime number and let f be in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{C_p}, J(\mathbb{Q}^c))$, such that*

$$\mathrm{rag}(f) \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathcal{A}_{C_p}, \mathbb{Q}(\zeta_p)^{\times} \cdot U(\mathbb{Z}[\zeta_p])) .$$

If $c := [f] \in \mathrm{Cl}(\mathbb{Z}[C_p])$, then c is trivial.

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

$$\mathcal{L}(c)^p = [f(\chi_p)]^p = [f(\chi_p)^p] \overset{(a)}{=} [f(p\chi_p)] \overset{(b)}{=} [\mathrm{rag}(f)(p\chi_p)] \overset{(c)}{=} 1, \tag{17}$$

where (a) is given by the fact that f is a homomorphism, (b) follows since $p\chi_p \in \mathcal{A}_{C_p}$ and (c) is given by hypothesis and 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

$$\sigma_j \cdot (\mathcal{L}(c)) = [f(j\chi_p - (j\chi_p - \chi_p^j))] = [f(j\chi_p)][f(j\chi_p - \chi_p^j)]^{-1} \overset{(d)}{=} [f(j\chi_p)] = \mathcal{L}(c)^j,$$

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 $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$ given by $\mathcal{L}(c)$:

$$1 = \sum_{j=1}^{p-1} j\sigma_j^{-1} \cdot (\mathcal{L}(c)) \overset{(e)}{=} \prod_{j=1}^{p-1} \mathcal{L}(c)^{jj^{-1}} = \mathcal{L}(c)^{p-1}, \tag{18}$$

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 $\{1, \dots, p-1\}$. Note that the last equality follows from the fact that $jj^{-1} \equiv 1 \mod p$ and from (17).
Finally, putting together (17) and (18), we have $\mathcal{L}(c) = 1$, which, thanks to the isomorphism (16), implies the triviality of c in $\mathrm{Cl}(\mathbb{Z}[C_p])$. □

Using the isomorphism $\mathcal{J}$ given in Lemma 4.6, an analogous result for the dihedral case follows.

Proposition 4.16. — *Let p be an odd prime and let f be in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_{D_p}, J(\mathbb{Q}^c))$, such that*

$$\mathrm{rag}(f) \in \mathrm{Hom}_{\Omega_\mathbb{Q}}\left(\mathcal{A}_{D_p}, \mathbb{Q}(\zeta_p + \zeta_p^{-1})^\times \cdot U\left(\mathbb{Z}[\zeta_p + \zeta_p^{-1}]\right)\right).$$

If $c := [f] \in \mathrm{Cl}(\mathbb{Z}[D_p])$, then c is trivial.

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 1.
Proof of Theorem 1. We consider the case $G = D_p$, the C_p case 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

$$\mathrm{rag}(f) = g \cdot w \cdot \Theta^{\mathrm{t}}_{\overline{D_p}, \mathbb{Q}}(h),$$

where g is in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathcal{A}_{D_p}, (\mathbb{Q}^c)^\times)$, $w \in \mathcal{U}(\mathbb{Z}[D_p]) \subseteq \mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathcal{A}_{D_p}, U(\mathbb{Z}^c))$ (see (6) for the original definition of $\mathcal{U}(\mathbb{Z}[D_p])$) and h is in $\mathrm{Hom}_{\Omega_\mathbb{Q}}\left(\mathbb{Z}[\overline{D_p}(-1)], J\left(\mathbb{Q}\left(\zeta_p + \zeta_p^{-1}\right)\right)\right)$.
Since

$$\begin{aligned}
\mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathcal{A}_{D_p}, (\mathbb{Q}^c)^\times) &= \mathrm{Hom}_{\Omega_\mathbb{Q}}\left(\mathcal{A}_{D_p}, \mathbb{Q}(\zeta_p + \zeta_p^{-1})^\times\right) \\
\mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathcal{A}_{D_p}, U(\mathbb{Z}^c)) &= \mathrm{Hom}_{\Omega_\mathbb{Q}}\left(\mathcal{A}_{D_p}, U(\mathbb{Z}[\zeta_p + \zeta_p^{-1}])\right),
\end{aligned}$$

clearly $g \cdot w \in \mathrm{Hom}_{\Omega_\mathbb{Q}}\left(\mathcal{A}_{D_p}, \mathbb{Q}(\zeta_p + \zeta_p^{-1})^\times \cdot U\left(\mathbb{Z}[\zeta_p + \zeta_p^{-1}]\right)\right)$. Thus, using Proposition 4.13 and Proposition 4.16, we finally get that c is trivial, as we wanted to show. □

5. Some functorial properties of $\mathrm{St}(O_K[G])$

In this section, we shall study the behaviour of the subgroup $\mathrm{St}(O_K[G])$ under change of the base field.

Given K a subfield of a number field L, as already explained in the Introduction, we have a restriction map $\mathcal{N}_{L/K} : \mathrm{Cl}(O_L[G]) \longrightarrow \mathrm{Cl}(O_K[G])$. In terms of the Hom-description it is expressed by the norm map

$$\begin{aligned}
\mathcal{N}_{L/K} : \frac{\mathrm{Hom}_{\Omega_L}(R_G, J(\mathbb{Q}^c))}{\mathrm{Hom}_{\Omega_L}(R_G, (\mathbb{Q}^c)^\times) \cdot \mathrm{Det}(U(O_L[G]))} &\longrightarrow \frac{\mathrm{Hom}_{\Omega_K}(R_G, J(\mathbb{Q}^c))}{\mathrm{Hom}_{\Omega_K}(R_G, (\mathbb{Q}^c)^\times) \cdot \mathrm{Det}(U(O_K[G]))} \\
[f] &\longmapsto [\mathcal{N}_{L/K}(f)]
\end{aligned}$$

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 $\Omega_{\mathbb{Q}}$-action on $\mathrm{Hom}\left(R_G, J(\mathbb{Q}^{\mathrm{c}})\right)$), for every $\alpha \in R_G$. Instead of taking K^{c} (resp. L^{c}) in the Hom-description of $\mathrm{Cl}(O_K[G])$ (resp. $\mathrm{Cl}(O_L[G])$), we consider $\mathbb{Q}^{\mathrm{c}}$ in order to homogenize the notation (we can do it as L and K are both algebraic extensions of $\mathbb{Q}$ - cf. (3)).
From Theorem 2.17, we know that $\mathrm{R}(O_L[G])$ (resp. $\mathrm{R}(O_K[G])$) 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 section we are going to give an affirmative answer to this question, which will have some nice consequences, as explained in the last part.

5.1. Changing the base field for the Stickelberger subgroup. — Using the group homomorphisms

$$\mathrm{Cl}(O_L[G]) \xrightarrow{\mathrm{Rag}_L} \mathrm{MCl}(O_L[G]) \xleftarrow{\Theta^{t}_{\overline{G},\,L}} J(L\overline{\Lambda}),$$

we defined $\mathrm{St}(O_L[G])$ as $\mathrm{Rag}_L^{-1}(\mathrm{Im}(\Theta^{\mathrm{t}}_{\overline{G},\,L}))$. Analogously $\mathrm{St}(O_K[G])$ is $\mathrm{Rag}_K^{-1}(\mathrm{Im}(\Theta^{\mathrm{t}}_{\overline{G},\,K}))$.
The norm map $\mathcal{N}_{L/K}$ induces the following well-defined group homomorphisms (for which we will use the same name):

$$\begin{array}{rcl} \mathcal{N}_{L/K} : \mathrm{MCl}(O_L[G]) & \longrightarrow & \mathrm{MCl}(O_K[G]), \\ \mathcal{N}_{L/K} : \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\overline{G}](-1), J(\mathbb{Q}^{\mathrm{c}})\right) & \longrightarrow & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\overline{G}](-1), J(\mathbb{Q}^{\mathrm{c}})\right). \end{array}$$

Thus we can prove the next result.

Proposition 5.2. — *The following diagram commutes:*

$$\begin{tikzcd} \mathrm{Cl}(O_L[G]) \arrow[r, "\mathrm{Rag}_L"] \arrow[d, "\mathcal{N}_{L/K}"] & \mathrm{MCl}(O_L[G]) \arrow[d, "\mathcal{N}_{L/K}"] & \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^{\mathrm{c}})\right) \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},\,L}"'] \arrow[d, "\mathcal{N}_{L/K}"] \\ \mathrm{Cl}(O_K[G]) \arrow[r, "\mathrm{Rag}_K"] & \mathrm{MCl}(O_K[G]) & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^{\mathrm{c}})\right). \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},\,K}"'] \end{tikzcd}$$

Proof. — First of all we claim that the following diagram commutes

$$\begin{tikzcd} \mathrm{Cl}(O_L[G]) \arrow[r, "\mathrm{Rag}_L"] \arrow[d, "\mathcal{N}_{L/K}"] & \mathrm{MCl}(O_L[G]) \arrow[d, "\mathcal{N}_{L/K}"] \\ \mathrm{Cl}(O_K[G]) \arrow[r, "\mathrm{Rag}_K"] & \mathrm{MCl}(O_K[G]). \end{tikzcd}$$

Given a homomorphism $f \in \mathrm{Hom}_{\Omega_K}\left(R_G, J(\mathbb{Q}^{\mathrm{c}})\right)$ and $\alpha := \sum_{\chi\in\mathrm{Irr}(G)} a_{\chi}\chi$ in $\mathcal{A}_G$, using the definition of $\mathcal{N}_{L/K}$, we have

$$\begin{aligned} \mathcal{N}_{L/K}(\mathrm{Rag}_L(f))(\alpha) &= \prod_{\omega\in\Omega_K/\Omega_L} \mathrm{Rag}_L(f)\left(\alpha^{\omega^{-1}}\right)^{\omega} \\ &= \prod_{\omega\in\Omega_K/\Omega_L} f\left(\alpha^{\omega^{-1}}\right)^{\omega} \end{aligned}$$

$$\begin{aligned} &= \mathcal{N}_{L/K}(f)(\alpha) \\ &= \mathrm{Rag}_K(\mathcal{N}_{L/K}(f))(\alpha) \end{aligned}$$

which proves our claim. From this, we have $\mathcal{N}_{L/K}(\mathrm{Ker}(\mathrm{Rag}_L)) \subseteq \mathrm{Ker}(\mathrm{Rag}_K)$.
We pass now to the proof of the commutativity of the following diagram

$$\begin{tikzcd} \mathrm{MCl}(O_L[G]) \arrow[d, "\mathcal{N}_{L/K}"] & \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^{\mathrm{c}})\right) \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},L}"'] \arrow[d, "\mathcal{N}_{L/K}"] \\ \mathrm{MCl}(O_K[G]) & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^{\mathrm{c}})\right). \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},K}"'] \end{tikzcd} \tag{19}$$

Given $g \in \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^{\mathrm{c}})\right)$ and an element $\alpha \in \mathcal{A}_G$, we have

$$\begin{aligned} \Theta^{\mathrm{t}}_{\overline{G},K}(\mathcal{N}_{L/K}(g))(\alpha) &= \mathcal{N}_{L/K}(g)\left(\sum_{\overline{s}\in\overline{G}(-1)} \langle\alpha,\overline{s}\rangle\overline{s}\right) \\ &= \prod_{\omega\in\Omega_K/\Omega_L} g\left(\left(\sum_{\overline{s}\in\overline{G}(-1)} \langle\alpha,\overline{s}\rangle\overline{s}\right)^{\omega^{-1}}\right)^{\omega} \\ &= \prod_{\omega\in\Omega_K/\Omega_L}\left(\prod_{\overline{s}\in\overline{G}(-1)} g\left(\overline{s}^{\omega^{-1}}\right)^{\langle\alpha,\overline{s}\rangle}\right)^{\omega} \\ &= \prod_{\omega\in\Omega_K/\Omega_L}\left(\prod_{\overline{t}\in\overline{G}(-1)} g\left(\overline{t}\right)^{\langle\alpha,\overline{t}^{\omega}\rangle}\right)^{\omega} \end{aligned}$$

using the fact that every ω acts as an automorphism. On the other side

$$\begin{aligned} \mathcal{N}_{L/K}(\Theta^{\mathrm{t}}_{\overline{G},L}(g))(\alpha) &= \prod_{\omega\in\Omega_K/\Omega_L} \Theta^{\mathrm{t}}_{\overline{G},L}(g)\left(\alpha^{\omega^{-1}}\right)^{\omega} \\ &= \prod_{\omega\in\Omega_K/\Omega_L} g\left(\sum_{\overline{s}\in\overline{G}(-1)} \langle\alpha^{\omega^{-1}},\overline{s}\rangle\overline{s}\right)^{\omega} \\ &= \prod_{\omega\in\Omega_K/\Omega_L}\left(\prod_{\overline{s}\in\overline{G}(-1)} g\left(\overline{s}\right)^{\langle\alpha^{\omega^{-1}},\overline{s}\rangle}\right)^{\omega} \\ &= \prod_{\omega\in\Omega_K/\Omega_L}\left(\prod_{\overline{s}\in\overline{G}(-1)} g\left(\overline{s}\right)^{\langle\alpha,\overline{s}^{\omega}\rangle}\right)^{\omega} \end{aligned}$$

where in the last equality we used the relation $\langle\alpha^{\omega^{-1}},\overline{s}\rangle = \langle\alpha^{\omega^{-1}},s\rangle = \langle\alpha,s^{\omega}\rangle = \langle\alpha,\overline{s^{\omega}}\rangle = \langle\alpha,\overline{s}^{\omega}\rangle$, which one can get using the definition of the action of ω on $\overline{G}(-1)$, the definition of the Stickelberger pairing for the set of conjugacy classes and property (9). This proves the

commutativity of (19).
The previous two diagrams combine to prove that the following diagram commutes

$$\begin{tikzcd}
\mathrm{Cl}(O_L[G]) \arrow[r, "\mathrm{Rag}_L"] \arrow[d, "\mathcal{N}_{L/K}"] & \mathrm{MCl}(O_L[G]) \arrow[d, "\mathcal{N}_{L/K}"] & \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^c)\right) \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},L}"'] \arrow[d, "\mathcal{N}_{L/K}"] \\
\mathrm{Cl}(O_K[G]) \arrow[r, "\mathrm{Rag}_K"] & \mathrm{MCl}(O_K[G]) & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^c)\right). \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},K}"']
\end{tikzcd}$$

□

Thus the following result now easily follows (this is a refined version of Theorem 2 in the Introduction).

Theorem 5.3. — *Given a finite group G and a subfield K of an algebraic 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. — The first inclusion is already included in the proof of Proposition 5.2. For the second one it is sufficient to have in mind the definition of the Stickelberger subgroup and use Proposition 5.2. □

A first consequence of Theorem 5.3 in the abelian case follows.

Corollary 5.4. — *Let G be a finite abelian group and let K be a subfield of an algebraic number field L. Then $\mathcal{N}_{L/K}(\mathrm{R}_{\mathrm{nr}}(O_L[G])) \subseteq \mathrm{R}_{\mathrm{nr}}(O_K[G])$ and $\mathcal{N}_{L/K}(\mathrm{R}(O_L[G])) \subseteq \mathrm{R}(O_K[G])$.*

Proof. — This follows from Theorem 5.3 and from the equalities in the abelian case of Theorem 2.17: $\mathrm{R}_{\mathrm{nr}}(O_L[G]) = \mathrm{Ker}(\mathrm{Rag}_L)$ (respectively $\mathrm{R}_{\mathrm{nr}}(O_K[G]) = \mathrm{Ker}(\mathrm{Rag}_K)$) and $\mathrm{R}(O_L[G]) = \mathrm{St}(O_L[G])$ (respectively $\mathrm{R}(O_K[G]) = \mathrm{St}(O_K[G])$). □

The following result is valid for every finite group G.

Corollary 5.5. — *Let G be a finite group and K be a subfield of an algebraic number field L, such that $\mathrm{St}(O_K[G]) = 1$. Then for every tame G-Galois L-algebra N, its ring of integers O_N is a stably free $O_K[G]$-module.*

Proof. — Clear from Theorem 5.3 and from the fact that the class $[O_N]$ in the class group $\mathrm{Cl}(O_K[G])$ is trivial if and only if O_N is stably free when seen as an $O_K[G]$-module (cf. Remark 2.3). □

From this we deduce the two following corollaries which are contained in a more general result by Taylor ([Tay81]).

Corollary 5.6. — *Given an algebraic number field L and an abelian tame G-Galois L-algebra N, its ring of integers O_N is a free $\mathbb{Z}[G]$-module.*

Proof. — It follows from Corollary 5.5 with $K = \mathbb{Q}$ and from the fact that, since G is abelian, $\mathrm{St}(\mathbb{Z}[G]) = \mathrm{R}(\mathbb{Z}[G]) = 1$, by [Tay81] and McCulloh's results. Moreover, note that in the abelian case to be a stably free $\mathbb{Z}[G]$-module is equivalent to be a free $\mathbb{Z}[G]$-module (see Remark 2.3). □

Corollary 5.7. — *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, its ring of integers O_N is a free $\mathbb{Z}[D_p]$-module.*

Proof. — The proof is a direct consequence of Theorem 1, Corollary 5.5 and the statement concerning the dihedral groups in Remark 2.3. $\square$

As the following remark explains, an analogous result to Theorem 5.3 holds when we consider the behaviour of $\mathrm{St}(O_K[G])$ under extension of the base field.

***Remark 5.8* (Extension of the base field).** — *Let L be a finite extension of K as above. There is a homomorphism $\mathrm{ext}_{L/K} : \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_L[G])$ obtained considering the extension of scalars via the tensor product $O_L \otimes_{O_K} -$. In terms of the Hom-description this functor is induced by the canonical injection $\mathrm{Hom}_{\Omega_K}(R_G, J(\mathbb{Q}^c)) \longrightarrow \mathrm{Hom}_{\Omega_L}(R_G, J(\mathbb{Q}^c))$. Analogously as before, the following diagram commutes*

$$\begin{tikzcd}
\mathrm{Cl}(O_L[G]) \arrow[r, "\mathrm{Rag}_L"] & \mathrm{MCl}(O_L[G]) & \mathrm{Hom}_{\Omega_L}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^c)\right) \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},L}"'] \\
\mathrm{Cl}(O_K[G]) \arrow[r, "\mathrm{Rag}_K"] \arrow[u, "\mathrm{ext}_{L/K}"'] & \mathrm{MCl}(O_K[G]) \arrow[u, "\mathrm{ext}_{L/K}"'] & \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^c)\right), \arrow[l, "\Theta^{\mathrm{t}}_{\overline{G},K}"'] \arrow[u, "\mathrm{ext}_{L/K}"']
\end{tikzcd}$$

indeed, if $f \in \mathrm{Hom}_{\Omega_K}(R_G, J(\mathbb{Q}^c))$, $g \in \mathrm{Hom}_{\Omega_K}\left(\mathbb{Z}[\overline{G}(-1)], J(\mathbb{Q}^c)\right)$, and $\alpha \in \mathcal{A}_G$, we have

$$\mathrm{ext}_{L/K}(\mathrm{Rag}_K)(f)(\alpha) = \mathrm{Rag}_K(f)(\alpha) = \mathrm{Rag}_L(f)(\alpha) = \mathrm{Rag}_L(\mathrm{ext}_{L/K})(f)(\alpha),$$
$$\mathrm{ext}_{L/K}(\Theta^{\mathrm{t}}_{\overline{G},K})(g)(\alpha) = \Theta^{\mathrm{t}}_{\overline{G},K}(g)(\alpha) = g(\Theta_{\overline{G}}(\alpha)) = \Theta^{\mathrm{t}}_{\overline{G},L}(\mathrm{ext}_{L/K}(g))(\alpha).$$

From this we deduce the following inclusions

$$\begin{aligned}
\mathrm{ext}_{L/K}(\mathrm{Ker}(\mathrm{Rag}_K)) &\subseteq \mathrm{Ker}(\mathrm{Rag}_L),\\
\mathrm{ext}_{L/K}(\mathrm{St}(O_K[G])) &\subseteq \mathrm{St}(O_L[G]).
\end{aligned}$$

Acknowledgments. — I am very grateful to Philippe Cassou-Noguès, Bart de Smit and Boas Erez for their suggestions and precious help. Further I would like to thank Alessandro Cobbe for his interest on this paper. Finally, I also wish to thank Adebisi Agboola, Nigel P. Byott and Jean Gillibert for all the remarks and advices they gave me as part of my thesis committee.

References

[AC15] A. Agboola and L. McCulloh, *On the relative Galois module structure of rings of integers in tame extensions*, Available at: http://arxiv.org/abs/1410.4829.

[BS05a] 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.

[BS05b] N. P. Byott and B. Sodaïgui, *Realizable Galois module classes for tetrahedral extensions*, Compos. Math., **141** (3):573–582, 2005.

[BS13] N. P. Byott and B. Sodaïgui, *Realizable Galois module classes over the group ring for non abelian extensions*, Ann. Inst. Fourier (Grenoble), **63** (1):303–371, 2013.

[CR81] 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.

[CR87] 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.

[Lan94] S. Lang, *Algebraic number theory*, volume **110** of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994.

[McC] L. R. McCulloh, *From galois module classes to steinitz classes.* arXiv:1207.5702 - Informal report given in Oberwolfach in February 2002.

[McC77] 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.

[McC83] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra, **82** (1):102–134, 1983.

[McC87] L. R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math., **375/376**:259–306, 1987.

[Rei03] 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.

[Rim59] D. S. Rim, *Modules over finite groups*, Ann. of Math. (2), **69**:700–712, 1959.

[Ser94] J. P. Serre, *Cohomologie galoisienne*, volume **5** of Lecture Notes in Mathematics. Springer-Verlag, Berlin, fifth edition, 1994.

[Siv13] A. Siviero, *Class invariants for tame Galois algebras.* PhD thesis, Université Bordeaux I - Universiteit Leiden, 2013. Available at: http://tel.archives-ouvertes.fr/tel-00847787.

[Swa62] R. G. Swan, *Projective modules over group rings and maximal orders* Ann. of Math. (2), **76**:55–61, 1962.

[Tay81] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math., **63**(1):41–79, 1981.

[Was97] L. C. Washington, *Introduction to cyclotomic fields*, volume **83** of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997.

July 15, 2014

Andrea Siviero, Université Bordeaux I – 351, cours de la Libération – F 33405 Talence cedex – Universiteit Leiden – Niels Bohrweg, 1 – 2333 CA Leiden • *E-mail :* andsiviero@gmail.com