Université de Valenciennes et du Hainaut-Cambrésis

## Thèse de doctorat

## Pour obtenir le grade de Docteur de l'Université de

## VALENCIENNES ET DU HAINAUT-CAMBRESIS

Discipline, spécialité selon la liste des spécialités pour lesquelles l'Ecole Doctorale est accréditée :
**Mathématiques Pures**

**Présentée et soutenue par Maya FARHAT**

**Le 21/06/2016, à Valenciennes**

**Ecole doctorale :**
Sciences Pour l'Ingénieur (SPI)

**Equipe de recherche, Laboratoire :**
Théorie des Nombres et Topologie Algébrique
Laboratoire de Mathématiques et ses Applications de Valenciennes (LAMAV)

# Classes de Steinitz, codes cycliques de Hamming et classes galoisiennes réalisables d'extensions non abéliennes de degré $p^3$

## JURY

**Président du jury**
- CASSOU-NOGUÈS, Philippe. Professeur, Université de Bordeaux 1.

**Rapporteurs**
- BYOTT, Nigel Paul, Maître de Conférences, Université d'Exeter (Angleterre).
- CARTER, James Edgar, Professeur, Université de Charleston (USA).

**Examinateurs**
- DÈBES, Pierre, Professeur, Université de Lille 1.
- EL KACIMI ALAOUI, Aziz, Professeur, Université de Valenciennes et du Hainaut Cambrésis.

**Directeur de thèse** *:*
- SODAÏGUI, Bouchaïb, Maître de Conférences HDR, Université de Valenciennes et du Hainaut Cambrésis

# Acknowledgements
# Remerciements

First of all I thank God for his blessing that has guided me through life. Also I am indebted to many people for their advice, assistance and support.

From the formative stages of this thesis, to the final draft, I owe an immense debt of gratitude and heartily thanks to my supervisor Mr. B. Sodaïgui for his continued guidance and support during the preparation of this dissertation. I thank him very much for his valuable help, scientific advice and for providing me with all the needed resources.

I also want to thank those who have done me the honor of judging this work: Professor Ph. Cassou-Noguès, Jury President, distinguished Professors N. P. Byott and J. Carter who assumed the task of writing reports on this thesis, and distinguished Professors P. Dèbes and A. El Kacimi for wanting to review my work and participate in the Jury.

I wouldn't have reached this point without the help of my parents, especially my mother. I want to express my great respect, and thank her for her invaluable and unconditional support, and all what she did for me; without her I wouldn't be where I am today. That this thesis reflects my love for her.

A single person in the world, my Husband, my confidential, who never stopped encouraging me and being present always by my side. To the candle who lightens my way and supports me through all my studies, my lovely daughter Jöelle.

A great thank for my amazing brother, sisters and all my friends for all what they did for me.

# Table des matières

# Introduction

Dans toute cette thèse, si $K$ est un corps de nombres, $O_K$ désigne son anneau d'entiers et $Cl(K)$ son groupe de classes.

Soient $k$ un corps de nombres et $\Gamma$ un groupe fini. Soient $\mathcal{M}$ un $O_k$-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$. Soit $Cl(O_k[\Gamma])$ (resp. $Cl(\mathcal{M})$) le groupe des classes des $O_k[\Gamma]$-modules (resp. $\mathcal{M}$-modules) localement libres (voir [18, Chap. I] ; voir Chap 1, §1 de cette thèse). Soit $M$ un $O_k[\Gamma]$-module localement libre. On peut associer à $M$ une classe, notée $[M]$, dans $Cl(O_k[\Gamma])$, et par extension des scalaires la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} M$, notée $[\mathcal{M} \otimes_{O_k[\Gamma]} M]$, dans $Cl(\mathcal{M})$. Ceci s'applique à $M = O_N$, où $N/k$ est une extension galoisienne, modérément ramifiée et à groupe de Galois isomorphe à $\Gamma$.

On désigne par $\mathcal{R}(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M})$) l'ensemble des classes $c$ de $Cl(O_k[\Gamma])$ (resp. $Cl(\mathcal{M})$) telles qu'il existe une extension $N/k$ modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$, avec $[O_N] = c$ (resp. $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$). Nous dirons que $\mathcal{R}(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M})$ ) est l'ensemble des classes galoisiennes réalisables. Le problème des classes réalisables d'extensions galoisiennes consiste en l'étude de la structure de ces deux ensembles. Signalons que ces derniers sont liés par la relation : $Ex(\mathcal{R}(O_k[\Gamma])) = \mathcal{R}(\mathcal{M})$, où $Ex : Cl(O_k[\Gamma]) \to Cl(\mathcal{M})$ est le morphisme surjectif induit par l'extension des scalaires de $O_k[\Gamma]$ à $\mathcal{M}$.

Notons $Cl^\circ(O_k[\Gamma])$ (resp. $Cl^\circ(\mathcal{M})$) le noyau du morphisme $Cl(O_k[\Gamma]) \to Cl(k)$ (resp. $Cl(\mathcal{M}) \to Cl(k)$) induit par l'augmentation $O_k[\Gamma] \to O_k$ (resp. $\mathcal{M} \to O_k$). Il découle de $Tr_{N/k}(O_N) = O_k$ que $\mathcal{R}(O_k[\Gamma]) \subset Cl^\circ(O_k[\Gamma])$ et $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$, où $Tr_{N/k}$ est la trace dans $N/k$.

On conjecture (voir par exemple [4, Conjectures 1 et 2, p. 2]) que $\mathcal{R}(O_k[\Gamma])$ et $\mathcal{R}(\mathcal{M})$ sont des sous-groupes respectifs de $Cl^\circ(O_k[\Gamma])$ et $Cl^\circ(\mathcal{M})$ ; signalons que cela est vrai lorsque $\Gamma$ est abélien (voir [24, Theorem 6.17, p. 289]). Cette conjecture (non abélienne) peut être considérée comme un complément à celle de Fröhlich sur les anneaux d'entiers de corps de nombres (la conjecture de Fröhlich est démontrée dans [40]).

Pour des résultats récents dans la direction de l'étude de la conjecture non abélienne sur les classes réalisables voir [3, 4, 5, 6, 7, 29, 36]. Nous signalons que la preuve des principaux résultats de [3, 4, 7] utilisent des idéaux de Stickelberger et des propriétés de certains codes cycliques, en particulier ceux de Hamming.

Rappelons la définition de la classe de Steinitz. Soit $M$ un $O_k$-module de type fini, sans torsion et de rang $n$. Alors, il existe un idéal $I$ de $O_k$ tel que $M \simeq O_k^{n-1} \oplus I$ en tant que $O_k$-module. La classe de $I$ dans $Cl(k)$ est appelée la classe de Steinitz de $M$, et on la note $cl_k(M)$. La structure de $M$ en tant que $O_k$-module est complètement déterminée par son rang et sa classe de Steinitz. Ceci s'applique en particulier à $M = O_K$, où $K/k$ est une extension finie de corps de nombres de degré $n$ ; on dira alors que $cl_k(O_K)$ est la classe de Steinitz de $K/k$.

On désigne par $R_m(k, \Gamma)$ ($m$ pour modéré) l'ensemble des classes $c$ de $Cl(k)$ telles qu'il existe une extension $N/k$ modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$, avec $cl_k(O_N) = c$. Nous dirons que $R_m(k, \Gamma)$ est l'ensemble des classes de Steinitz réalisables.

Il est immédiat de voir que le morphisme de restriction $res_1^\Gamma$ : $Cl(O_k[\Gamma]) \to Cl(k)$ qui, à la classe $[M]$ d'un $O_k[\Gamma]$-module localement libre $M$, associe sa classe en tant que $O_k$-module dans $Cl(k)$, est donné par : $res_1^\Gamma([M]) = cl_k(M)$. Il s'ensuit que $res_1^\Gamma(\mathcal{R}(O_k[\Gamma])) = R_m(k, \Gamma)$.

On conjecture (voir par exemple [4, Conjecture 3, p. 6]) que $R_m(k, \Gamma)$ est un sous-groupe de $Cl(k)$ ; signalons que cela est vrai lorsque $\Gamma$ est abélien puisque $\mathcal{R}(O_k[\Gamma])$ est un sous-groupe de $Cl(O_k[\Gamma])$ grâce à [24]. Signalons aussi que l'étude de la structure de $R_m(k, \Gamma)$, qui est intéressante en elle-même, a un lien étroit avec celle de l'ensemble des classes galoisiennes réalisables (voir [4, §1]) .

Les travaux les plus récents concernant l'investigation de $R_m(k, \Gamma)$ sont dans [2, 3, 7, 8, 11, 12, 13, 37, 38].

Les résultats de [5, 6, 7] ont montré que la connaissance de $\mathcal{R}(\mathcal{M})$ fournit une bonne approximation de $\mathcal{R}(O_k[\Gamma])$. La classe $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] \in \mathcal{R}(\mathcal{M})$ se calcule à l'aide des classes de Steinitz d'extensions intermédiaires de $N/k$, et la détermination de la structure de $\mathcal{R}(\mathcal{M})$ (voir par exemple [3, 4, 32, 34, 35, 36]) se fait, en partie, grâce à la résolution d'un problème de plongement en lien avec la donnée de classes de Steinitz.

Le but de la suite est d'énoncer les principaux résultats de cette thèse.

La première partie de la thèse consiste en l'étude de l'ensemble des classes de Steinitz réalisables pour $\Gamma = V \rtimes_\rho C$ défini ci-dessous.

Soit $p$ un nombre premier. Soit $\mathbb{F}_p$ le corps fini à $p$ éléments, que nous identifions souvent à $\mathbb{Z}/p\mathbb{Z}$. Soit $V$ un $p$-groupe abélien élémentaire d'ordre $p^r$, où $r \geq 1$ (donc $V$ est un $\mathbb{F}_p$-espace vectoriel de dimension $r$), et soit $C$ un groupe cyclique d'ordre $m$. Soit $\rho$ une $\mathbb{F}_p$-représentation linéaire de $C$ dans $V$ :

$$\rho : C \to Aut(V) = Aut_{\mathbb{F}_p}(V).$$

Nous notons $\Gamma$ le produit semi-direct de $V$ par $C$ défini par $\rho$ :

$$\Gamma = V \rtimes_\rho C.$$

Supposons $\rho$ fidèle et irréductible. On suppose $m > 1$ de sorte que $\Gamma$ soit non abélien (puisque $\rho$ est fidèle). Dans [7, Theorem 7.2.3 (i)], sous l'hypothèse que $k$ contient une racine primitive $p$-ième de l'unité, il est montré que $R_m(k, \Gamma)$ est un sous-groupe de $Cl(k)$ comme conséquence de l'étude de l'ensemble des classes galoisiennes réalisables.

Dans cette thèse, en utilisant des propriétés d'un code $p$-aire cyclique de Hamming, nous montrerons dans le chapitre 2, directement, sans étudier les classes galoisiennes réalisables, le théorème 1 suivant.

Pour énoncer le théorème 1, nous commençons par fixer quelques notations. Si $K/k$ est une extension finie de corps de nombres, on note $N_{K/k}$ la norme dans $K/k$. Si $G$ est un groupe abélien et $n \in \mathbb{N}$, alors $G^n$ est le sous-groupe des puissances $n$-ièmes des éléments de $G$.

**Théorème 1.** *Soient $k$ un corps de nombres et $\Gamma = V \rtimes_\rho C$. Soit $\xi$ une racine primitive $p$-ième de l'unité. Supposons que $\rho$ est fidèle et irréductible, et $m = (p^r - 1)/(p - 1)$, où $r \geq 2$ et $pgcd(r, p - 1) = 1$. Alors $R_m(k, \Gamma)$ est le sous-groupe de $Cl(k)$ suivant :*

$$\begin{aligned} R_m(k,\Gamma) &= R_t(k,C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi))\big)^{\frac{1}{2}mp^{r-1}(p-1)} \\ &= R_m(k,C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi))\big)^{\frac{1}{2}(p^r-1)p^{r-1}}, \end{aligned}$$

*où le groupe $R_m(k, C)$ est donné par :*

$$R_m(k,C) = \prod_{d|m} N_{k(\xi_d)/k}\big(Cl(k(\xi_d))\big)^{m(d-1)/2d},$$

*ici, $d$ parcourt l'ensemble des diviseurs positifs de $m$ et $\xi_d$ est une racine primitive $d$-ième de l'unité.*

**Remarques.** (1) Théorème 1 est une généralisation de deux théorèmes :

- Supposons $\xi \in k$, alors Théorème 1 est [7, Theorem 7.2.3 (i)] dans le cas $m = (p^r - 1)/(p - 1)$, où $r \geq 2$ et $pgcd(r, p - 1) = 1$.

- Supposons $p = 2$ et $r \geq 2$. Alors $m = 2^r - 1$ et la condition sur le *pgcd* est satisfaite. Théorème 1 est [4, Theorem 1.4 (ii)]. Notons que dans ce cas, si $\rho$ est fidèle, alors elle est irréductible (voir [4, Proposition 2.3(1)]). Le groupe alterné $A_4$ de degré 4 est un exemple de $\Gamma$ (ici $r = 2$ et $m = 3$).

(2) Théorème 1 est le résultat principal d'un article accepté dans : Journal of Number Theory.

Soit $p$ un nombre premier. Le thème de la deuxième partie de cette thèse est l'étude de la conjecture non abélienne sur les classes galoisennes réalisables pour les groupes non abéliens d'ordre $p^3$.

Lorsque $\Gamma$ est le groupe diédral $D_4$ (resp. quaternionien) d'ordre 8 et $k$ est un corps de nombres linéairement disjoint de $\mathbb{Q}(i)$ sur $\mathbb{Q}$, où $i^2 = -1$, on montre dans [35] (resp. [32]) que si le nombre de classes (resp. le nombre de classes au sens restreint) de $k$ est impair, alors $\mathcal{R}(\mathcal{M}) = Cl^\circ(\mathcal{M})$.

Dans [6] on montre que $\mathcal{R}(O_k[D_4]) = Cl^\circ(O_k[D_4])$ sous l'hypothèse que l'ordre du groupe de classes de rayon de $k$ modulo $4O_k$ est impair

Dorénavant on suppose $p$ impair.

La structure d'un groupe non abélien d'ordre $p^3$ est bien connue. On peut la définir par la présentation suivante :

$$\Gamma = \langle \eta,\ \tau,\ \nu \mid \eta^p = \tau^p = 1,\ \nu^p = \eta^q,\ \eta\tau = \tau\eta,\ \eta\nu = \nu\eta,\ \tau\nu\tau^{-1}\nu^{-1} = \eta \rangle,$$

où $q = 0$ ou bien $q = 1$. Le groupe $\Gamma$ est donc, à isomorphisme près, l'un des deux groupes suivants :

(i) Si $q = 0$, $\Gamma \simeq \big(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\big) \rtimes \mathbb{Z}/p\mathbb{Z}$ ; dans ce cas $\Gamma$ est d'exposant $p$.

(ii) Si $q \neq 0$, $\Gamma \simeq (\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$ ; dans ce cas $\Gamma$ est d'exposant $p^2$.

Le point de départ était la lecture des articles [3, 9] et une tentative de la détermination de $\mathcal{R}(\mathcal{M})$. Nous n'avons pas réussi la détermination de $\mathcal{R}(\mathcal{M})$ à cause de grandes difficultés provenant d'un problème de plongement en liaison avec la donnée de classes de Steinitz (on pourrait voir les détails dans le chapitre 3). Mais sous certaines hypothèses, nous avons déterminé à l'aide d'un idéal de Stickelberger, pour chaque type de $\Gamma$, un sous-groupe de $Cl^\circ(\mathcal{M})$ contenu dans $\mathcal{R}(\mathcal{M})$ (voir une démarche analogue dans [29, 34]).

Supposons que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes, où $\xi$ est une racine primitive $p$-ième de l'unité. Dans le chapitre 3, nous déterminons les classes de conjugaison sur $k$ des caractères absolument irréductibles de $\Gamma$, et montrons qu'on a :

$$Cl^\circ(\mathcal{M}) \simeq \prod_{i=0}^{p+1} Cl(k(\xi)).$$

Soit

$$S = Gal(k(\xi)/k) = \{s_i \mid \ 1 \leq i \leq p-1\}, \text{où} \ \ s_i(\xi) = \xi^i.$$

Soit l'élément de Stickelberger

$$\theta = \sum_{i=1}^{p-1} i s_i^{-1},$$

et soit l'idéal de Stickelberger

$$\mathcal{S} = \frac{1}{p}\theta\mathbb{Z}[S] \cap \mathbb{Z}[S].$$

(Dans cette thèse, les éléments de $\mathcal{S}$ sont appelés éléments de Stickelberger.)

L'action naturelle de $S$ sur les idéaux fractionnaires de $k(\xi)$ induit une structure de $\mathbb{Z}[S]$-module sur $Cl(k(\xi))$. On note $\mathcal{S}Cl(k(\xi))$ le sous-groupe de $Cl(k(\xi))$ engendré par les éléments de la forme $\mathfrak{s}c$, où $\mathfrak{s} \in \mathcal{S}$ et $c \in Cl(k(\xi))$.

Si $K/k$ est une extension finie de corps de nombres, on note $\phi_{K/k}$ le morphisme de $Cl(k)$ à valeurs dans $Cl(K)$ qui à la classe d'un idéal fractionnaire $I$ de $O_k$ associe la classe de l'idéal étendu $IO_K$ dans $Cl(K)$.

Dans le chapitre 3, on démontre le théorème suivant :

**Théorème 2.** *Soient $k$ un corps de nombres, $p$ un nombre premier impair et $\xi$ (resp. $\xi_{p^2}$) une racine primitive $p$-ième (resp. $p^2$-ième) de l'unité. Soit $\Gamma$ un groupe non abélien d'ordre $p^3$. Supposons les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ linéairement disjointes. Identifions $Cl^\circ(\mathcal{M})$ et $\prod_{i=0}^{p+1} Cl(k(\xi))$.*

*Si l'exposant de $\Gamma$ est $p$, soit*

$$A_p = \left\{ \Big( c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p, \right.$$
$$\left. x^p \phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big) \Big) \,\Big|\, (c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3 \right\}.$$

*Si l'exposant de $\Gamma$ est $p^2$, soit*

$$A_{p^2} = \Bigg\{ \Big( c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p,$$
$$x^p((s_{p-1}-\theta)c_0)\phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big) \Big| (c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3 \Bigg\}.$$

*Si $\Gamma$ est d'exposant $p$ (resp. d'exposant $p^2$ et $k(\xi_{p^2})/k(\xi)$ non ramifiée), alors $A_p$ (resp. $A_{p^2}$) est un sous-groupe de $Cl^\circ(\mathcal{M})$ contenu dans l'ensemble des classes réalisables $\mathcal{R}(\mathcal{M})$.*

**Remarques.** (1) Lorsque $\Gamma$ est d'exposant $p^2$, l'hypothèse $k(\xi_{p^2})/k(\xi)$ non ramifiée provient de l'utilisation d'une idée de la preuve du [2, Théorème 1.1] dans une partie de la démonstration de notre théorème 1.1 (on pourrait voir [2, §4] pour des exemples d'extensions $k(\xi_{p^2})/k(\xi)$ non ramifiées).

(2) Théorème 2 est le resultat principal d'un article accepté dans : Journal of Number Theory.

Notons par $R_m(k, \Gamma, A_p)$ (resp. $R_m(k, \Gamma, A_{p^2})$) l'ensemble des classes de Steinitz des extensions $N/k$ modérées à groupe de Galois isomorphe à $\Gamma$ d'exposant $p$ (resp. $p^2$) et telles que $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ appartient à $A_p$ (resp. $A_{p^2}$). Dans le chpitre 3, nous verrons que $R_m(k, \Gamma, A_p) = R_m(k, \Gamma)$ (resp. $R_m(k, \Gamma, A_{p^2}) = R_m(k, \Gamma)$).

**Remarque.** Le fait qu'on peut atteindre $R_m(k, \Gamma)$ par $A_p$ et $A_{p^2}$ nous dit que peut-être nous ne sommes pas très loin de la détermination de $\mathcal{R}(\mathcal{M})$.

Le plan de cette thèse est le suivant :

Le premier chapitre contient des définitions et résultats utiles pour la démonstration des théorèmes 1 et 2.

Le second chapitre est dédié à l'étude des classes de Steinitz d'extensions galoisiennes non abéliennes en liason avec les codes $p$-aire cycliques de Hamming. Dans ce chapitre on démontre Théorème 1.

Dans le troisième chapitre, nous étudions les classes galoisiennes réalisables d'extensions non abéliennes de degré $p^3$. Dans ce chapitre on démontre Théorème 2.

# Introduction (in English)

Throughout this thesis, if $K$ is a number field, we denote by $O_K$ its ring of integers and $Cl(K)$ its class group.

Let $k$ be a number field and $\Gamma$ a finite group. Let $\mathcal{M}$ be a maximal $O_k$-order in the semi-simple algebra $k[\Gamma]$ containing $O_k[\Gamma]$. Let $Cl(O_k[\Gamma])$ (respectively $Cl(\mathcal{M})$) be the locally free class group of $O_k[\Gamma]$ (respectively $\mathcal{M}$) (see [18, Chap. I]; see Chap. 1, §1 of this thesis). Let $M$ be a locally free $O_k[\Gamma]$-module. We may assign to $M$ a class, denoted $[M]$, in $Cl(O_k[\Gamma])$, and following extension of scalars, a class to $\mathcal{M} \otimes_{O_k[\Gamma]} M$, denoted $[\mathcal{M} \otimes_{O_k[\Gamma]} M]$, in $Cl(\mathcal{M})$. This applies to $M = O_N$, where $N/k$ is a Galois extension, at most tamely ramified (we abbreviate this to: tame), and with Galois group isomorphic to $\Gamma$.

We denote by $\mathcal{R}(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M})$) the set of classes $c \in Cl(O_k[\Gamma])$ (resp. $Cl(\mathcal{M})$) such that there exists a tame Galois extension, with Galois group isomorphic to $\Gamma$, and for which $[O_N] = c$ (resp. $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$). We say that $\mathcal{R}(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M})$ ) is the set of realizable Galois module classes. The problem of realizable Galois module classes consists in studying the structure of these two sets. Note that they are linked by the relation: $Ex(\mathcal{R}(O_k[\Gamma])) = \mathcal{R}(\mathcal{M})$, where $Ex : Cl(O_k[\Gamma]) \to Cl(\mathcal{M})$ is the surjective morphism induced by the extension of scalars from $O_k[\Gamma]$ to $\mathcal{M}$.

Denote by $Cl^\circ(O_k[\Gamma])$ (resp. $Cl^\circ(\mathcal{M})$) the kernel of the morphism $Cl(O_k[\Gamma]) \to Cl(k)$ (resp. $Cl(\mathcal{M}) \to Cl(k)$) induced by the augmentation $O_k[\Gamma] \to O_k$ (resp. $\mathcal{M} \to O_k$). It follows from $Tr_{N/k}(O_N) = O_k$ that $\mathcal{R}(O_k[\Gamma]) \subset Cl^\circ(O_k[\Gamma])$ and $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$, where $Tr_{N/k}$ is the trace map from $N$ to $k$.

One conjectures (see for instance [4, Conjectures 1 and 2, p. 2]) that $\mathcal{R}(O_k[\Gamma])$ and $\mathcal{R}(\mathcal{M})$ are subgroups of $Cl^\circ(O_k[\Gamma])$ and $Cl^\circ(\mathcal{M})$, respectively; note that this is true when $\Gamma$ is abelian (see [24, Theorem 6.17, p. 289]). This (nonabelian) conjecture may be seen as a complement to that of Fröhlich on rings of integers of number fields (Fröhlich's conjecture is proved in [40]).

For recent works toward the nonabelian conjecture on realizable Galois module classes see [3, 4, 5, 6, 7, 29, 36]. We point out that the proofs of the main results of [3, 4, 7] use Stickelberger ideals and properties of some cyclic codes, in particular Hamming cyclic codes.

Now recall the definition of the Steinitz class. Let $M$ be a finitely generated torsion-free module of rank $n$ over $O_k$. Then, there exists an ideal $I$ of $O_k$ such that $M \simeq O_k^{n-1} \oplus I$ as an $O_k$-module. The class of $I$ in $Cl(k)$ is called the Steinitz class of $M$, and will be denoted by $cl_k(M)$. The structure of $M$ as an $O_k$-module is determined up to isomorphism by its rank and its Steinitz class; for instance, $M$ is a free $O_k$-module if and only if $cl_k(M) = 1$. One applies the previous discussion to $M = O_K$, where $K/k$ is an extension of number fields of degree $n$; we will also say that $cl_k(O_K)$ is the Steinitz class of $K/k$.

We denote by $R_t(k, \Gamma)$ ($t$ means tame) the set of classes $c \in Cl(k)$ satisfying: there exists a tame Galois extension $N/k$ whose Galois group is isomorphic to $\Gamma$ and whose Steinitz class is equal to $c$. We say that $R_t(k, \Gamma)$ is the set of realizable Steinitz classes.

We can immediately see that the restriction morphism $res_1^\Gamma$: $Cl(O_k[\Gamma]) \rightarrow Cl(k)$ that assigns to the class $[M]$ of a locally free $O_k[\Gamma]$-module $M$ its class as an $O_k$-module in $Cl(k)$, is given by: $res_1^\Gamma([M]) = cl_k(M)$. It follows that $res_1^\Gamma(\mathcal{R}(O_k[\Gamma])) = R_t(k, \Gamma)$.

One conjectures (see for instance [4, Conjecture 3, p. 6]) that $R_t(k, \Gamma)$ is a subgroup of $Cl(k)$; we point out that this conjecture is true when $\Gamma$ is abelian because $\mathcal{R}(O_k[\Gamma])$ is a subgroup of $Cl(O_k[\Gamma])$ thanks to [24]. We also point out that the study of $R_t(k, \Gamma)$ has a close link with that of the set of realizable Galois module classes (see [4, §1]).

The most recent works concerning the investigation of $R_t(k, \Gamma)$ are in [2, 3, 7, 8, 11, 12, 13, 37, 38].

The results of [6, 5, 7] showed that $\mathcal{R}(\mathcal{M})$ is a good approximation of $\mathcal{R}(O_k[\Gamma])$. The class $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] \in \mathcal{R}(\mathcal{M})$ is calculated using the Steinitz classes of intermediate extensions of $N/k$, and the determination of the structure of $\mathcal{R}(\mathcal{M})$ (see for example [3, 4, 32, 34, 35, 36]) is due, in part, to the resolution of an embedding problem linked with Steinitz classes.

The objective of the sequel is the statement of the main results of this thesis.

The first part of the thesis concerns the study of the set of realizable Steinitz classes for $\Gamma = V \rtimes_\rho C$ defined below.

Let $p$ be a prime number. Let $\mathbb{F}_p$ be the finite field of $p$ elements, which we will often identify with $\mathbb{Z}/p\mathbb{Z}$. Let $V$ be an elementary abelian group of order $p^r$, where $r \geq 1$ (then $V$ is an $\mathbb{F}_p$-vector space of dimension $r$), and let $C$ be a cyclic group of order $m$. Let $\rho$ be an $\mathbb{F}_p$-linear representation of $C$ in $V$:

$$\rho : C \to Aut(V) = Aut_{\mathbb{F}_p}(V).$$

We denote by $\Gamma$ the semidirect product of $V$ by $C$ which is defined by $\rho$:

$$\Gamma = V \rtimes_\rho C.$$

Suppose that $\rho$ is faithful and irreducible. We suppose that $m > 1$ so that $\Gamma$ is not abelian (since $\rho$ is faithful). In [7, Theorem 7.2.3 (i)], under the hypothesis that $k$ contains a primitive $p$th root of unity, it is shown that $R_t(k, \Gamma)$ is a subgroup of $Cl(k)$ as a consequence of the study of the set of realizable Galois module classes.

In this thesis, using properties of a $p$-ary cyclic Hamming code, we shall prove in Chapter 2, directly, without investigating the Galois module classes, the following Theorem 1.

To state Theorem 1, we begin by fixing some notation. If $K/k$ is a finite extension of number fields, we denote by $N_{K/k}$ its norm map. If $G$ is an abelian group and $n \in \mathbb{N}$, then $G^n$ denotes the subgroup of the $n$th powers of elements of $G$.

**Theorem 1.** *Let $k$ be a number field and $\Gamma = V \rtimes_\rho C$. Let $\xi$ be a primitive $p$th root of unity. Assume that $\rho$ is faithful and irreducible, and $m = (p^r - 1)/(p - 1)$, where $r \geq 2$ and $gcd(r, p - 1) = 1$. Then $R_t(k, \Gamma)$ is the following subgroup of $Cl(k)$:*

$$\begin{aligned} R_t(k, \Gamma) &= R_t(k, C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi))\big)^{\frac{1}{2}mp^{r-1}(p-1)} \\ &= R_t(k, C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi))\big)^{\frac{1}{2}(p^r-1)p^{r-1}}, \end{aligned}$$

*where the group $R_t(k, C)$ is given by:*

$$R_t(k, C) = \prod_{d|m} N_{k(\xi_d)/k}\big(Cl(k(\xi_d))\big)^{m(d-1)/2d},$$

*where $d$ runs through the set of positive divisors of $m$ and $\xi_d$ is a primitive $d$th root of unity.*

**Remarks.** Theorem 1 is a generalization of two theorems:

- Suppose that $\xi \in k$, then Theorem 1 is [7, Theorem 7.2.3 (i)] in the case $m = (p^r - 1)/(p - 1)$, where $r \geq 2$ and $gcd(r, p - 1) = 1$.

- Assume that $p = 2$ and $r \geq 2$. Then $m = 2^r - 1$ and the *gcd* condition is satisfied. Theorem 1 is [4, Theorem 1.4 (ii)]. Note that in this case, if $\rho$ is faithful, then it is irreducible (see [4, Proposition 2.3(1)]). The alternating group $A_4$ of degree 4 is an example of $\Gamma$ (here $r = 2$ and $m = 3$).

(2) Theorem 1 is the main result of an article accepted in: Journal of Number Theory.

The second part of this thesis is dedicated to the study of the set of realizable Galois module classes for $\Gamma$ a nonabelian group of order $p^3$.

When $\Gamma$ is the dihedral group $D_4$ (respectively the quaternion group of order 8) and $k$ is linearly disjoint from $\mathbb{Q}(i)$ over $\mathbb{Q}$, where $i^2 = -1$, it is shown in [35] (resp. [32]) that $\mathcal{R}(\mathcal{M}) = Cl^\circ(\mathcal{M})$ if the class number (resp. the narrow class number) is odd. In [6] the equality $\mathcal{R}(O_k[D_4]) = Cl^\circ(O_k[D_4])$ was established for any number field such that the ray class group of $k$ with modulus $4O_k$ has odd order.

From now on we suppose that $p$ is odd.

The structure of a nonabelian group $\Gamma$ of order $p^3$ is well known. It is given by the presentation:

$$\Gamma = \langle \eta,\ \tau,\ \nu \mid \eta^p = \tau^p = 1,\ \nu^p = \eta^q,\ \eta\tau = \tau\eta,\ \eta\nu = \nu\eta,\ \tau\nu\tau^{-1}\nu^{-1} = \eta \rangle,$$

where $q = 0$ or $q = 1$. Then the group $\Gamma$ is, up to isomorphism, one of the following groups:

(i) if $q = 0$, $\Gamma \simeq \big(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\big) \rtimes \mathbb{Z}/p\mathbb{Z}$; in this case the exponent of $\Gamma$ is $p$.

(ii) if $q \neq 0$, $\Gamma \simeq (\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$; in this case the exponent of $\Gamma$ is $p^2$.

The starting point was the reading of the articles [2, 9] and an attempt to determine the structure of $\mathcal{R}(\mathcal{M})$. We do not succeed in determining completely that structure because of difficulties coming from an embedding problem connected with Steinitz classes (see the details in Chapter 3), but we will define below two subsets of $\mathcal{R}(\mathcal{M})$ and show that they are subgroups of $Cl^\circ(\mathcal{M})$ under some hypotheses.

Suppose that $k$ is linearly disjoint from $\mathbb{Q}(\xi)$ over $\mathbb{Q}$, where $\xi$ is a primitive $p$th root of unity. In Chapter 3, we will determine the conjugacy classes over $k$ of the absolutely irreducible characters of $\Gamma$, and show that:

$$Cl^\circ(\mathcal{M}) \simeq \prod_{i=0}^{p+1} Cl(k(\xi)).$$

Let

$$S = Gal(k(\xi)/k) = \{s_i \mid \ 1 \leq i \leq p-1\}, \text{where} \ \ s_i(\xi) = \xi^i.$$

Let

$$\theta = \sum_{i=1}^{p-1} i s_i^{-1},$$

be a Stickelberger element, and

$$\mathcal{S} = \frac{1}{p}\theta\mathbb{Z}[S] \cap \mathbb{Z}[S]$$

the Stickelberger ideal. (In this thesis the elements of $\mathcal{S}$ are called Stickelberger elements.)

The natural action of $S$ on the fractional ideals of $k(\xi)$ induces a structure of $\mathbb{Z}[S]$-module on $Cl(k(\xi))$. We denote by $\mathcal{S}Cl(k(\xi))$ the subgroup of $Cl(k(\xi))$ generated by the elements of the form $\mathfrak{s}c$, where $\mathfrak{s} \in \mathcal{S}$ and $c \in Cl(k(\xi))$.

If $K/k$ is a finite extension of number fields, $N_{K/k}$ is the norm map from $K$ to $k$, and we denote by $\phi_{K/k}$ the morphism from $Cl(k)$ to $Cl(K)$ that to the class in $Cl(k)$ of a fractional ideal $I$ of $O_k$ assigns the class in $Cl(K)$ of the extended ideal $IO_K$.

We will prove in Chapter 3 the following theorem:

**Theorem 2.** *Let $k$ be a number field, $p$ an odd prime number and $\xi$ (resp. $\xi_{p^2}$) a primitive $p$th (resp. $p^2$th) root of unity. Let $\Gamma$ be a non abelian group of order $p^3$. Suppose that the extensions $k/\mathbb{Q}$ and $\mathbb{Q}(\xi)/\mathbb{Q}$ are linearly disjoint. Identify $Cl^\circ(\mathcal{M})$ with $\prod_{i=0}^{p+1} Cl(k(\xi))$.*

*If the exponent of $\Gamma$ is $p$, let*

$$A_p = \Bigg\{ \Big(c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p,$$
$$x^p \phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big) \Big| (c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3 \Bigg\}.$$

*If the exponent of $\Gamma$ is $p^2$, let*

$$A_{p^2} = \Bigg\{ \Big(c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p,$$
$$x^p((s_{p-1} - \theta)c_0)\phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big) \Big| (c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3 \Bigg\}.$$

*If the exponent of* $\Gamma$ *is* $p$ *(resp.* $p^2$ *and* $k(\xi_{p^2})/k(\xi)$ *is not ramified), then* $A_p$ *(resp.* $A_{p^2}$*) is a subgroup of* $Cl^\circ(\mathcal{M})$ *contained in* $\mathcal{R}(\mathcal{M})$ *the set of realizable Galois module classes.*

**Remarks.** (1) When the exponent of $\Gamma$ is $p^2$, the hypothesis $k(\xi_{p^2})/k(\xi)$ is not ramified comes from the use of an idea in the proof of [2, Theorem 1.1] in a part of the proof of our Theorem 2 (see in [2, §4] examples for $k(\xi_{p^2})/k(\xi)$ not ramified).

(2) Theorem 2 is the main result of an article accepted in: Journal of Number Theory.

We denote by $R_m(k,\Gamma,A_p)$ (resp. $R_m(k,\Gamma,A_{p^2})$) the set of Steinitz classes of tame Galois extensions $N/k$ with Galois group isomorphic to $\Gamma$ having exponent $p$ (resp. $p^2$) and such that $[\mathcal{M}\otimes_{O_k[\Gamma]} O_N]$ belongs to $A_p$ (resp. $A_{p^2}$). In Chapter 3, we will show that $R_m(k,\Gamma,A_p) = R_m(k,\Gamma)$ (resp. $R_m(k,\Gamma,A_{p^2}) = R_m(k,\Gamma)$).

**Remark.**

The fact that we can reach $R_m(k,\Gamma)$ by $A_p$ and $A_{p^2}$ tells us that perhaps we are not far from the determination of $\mathcal{R}(\mathcal{M})$.

The plan of this thesis is the following:

The first chapter contains definitions and results needed in the proofs of Theorems 1 and 2.

The second chapter is dedicated to the study of the realizable Steinitz classes of non abelian Galois extensions and $p$-ary cyclic Hamming codes; in this chapter, we prove Theorem 1.

In the third chapter, we study the realizable Galois module classes of nonabelian extensions of degree $p^3$; in this chapter, we prove Theorem 2.

# Chapitre 1

# Préliminaires

## Notations

Dans toute la suite de la thèse, le groupe multiplicatif $k \setminus \{0\}$ des éléments inversibles d'un corps $k$ sera noté $k^\times$. Si $k$ est un corps de nombres, on note $O_k$ son anneau d'entiers et $Cl(k)$ son groupe des classes. Pour tout idéal fractionnaire $I$ de $k$, on note $cl(I)$ sa classe dans $Cl(k)$. Si $K/k$ est une extension finie, $[K : k]$, $N_{K/k}$ et $\Delta(K/k)$ désigneront respectivement le degré, la norme et le discriminant de l'extension.

## 1.1 Groupe des classes d'un ordre maximal

Soient $k$ un corps de nombres et $\Gamma$ un groupe fini. Un $O_k$-ordre dans l'algèbre semi-simple $k[\Gamma]$ est un sous-anneau $\Lambda$ de $k[\Gamma]$, qui est un $O_k$-module de type fini et tel que $\Lambda \otimes_{O_k} k \simeq k[\Gamma]$. Un $O_k$-ordre est dit maximal s'il est maximal pour l'inclusion parmi les $O_k$-ordres de $k[\Gamma]$.

Soit $\mathfrak{p}$ un idéal premier de $O_k$, on note $O_{k,\mathfrak{p}}$ le complété en $\mathfrak{p}$ de $O_k$, et $\Lambda_\mathfrak{p} = \Lambda \otimes_{O_k} O_{k,\mathfrak{p}}$.

Un $\Lambda$-module $X$ est dit localement libre si c'est un $\Lambda$-module de type fini tel que pour tout idéal premier $\mathfrak{p}$ de $O_k$, le $\Lambda_\mathfrak{p}$-module $X_\mathfrak{p} = X \otimes_\Lambda \Lambda_\mathfrak{p}$ est libre. Le rang de $X$ est défini comme étant le rang du $k[\Gamma]$-module libre $X \otimes_{O_k} k$. Ce rang est fini et il est égal au rang de $X_\mathfrak{p}$ sur $O_{k,\mathfrak{p}}[\Gamma]$ pour tout $\mathfrak{p}$.

Le groupe de Grothendieck $\mathcal{K}_0(\Lambda)$ des $\Lambda$-modules localement libres est le groupe abélien dont les générateurs sont les classes d'isomorphismes $(X)$ des $\Lambda$-modules localement libres $X$, avec les relations $(X \oplus Y) = (X) + (Y)$.

L'application $\mathbb{N} \to \mathcal{K}_0(\Lambda)$, qui à $n \in \mathbb{N}$ associe la classe $(\Lambda^n)$ du $\Lambda$-module libre $\Lambda^n$ de rang $n$, se prolonge en un homomorphisme de $\mathbb{Z} \to \mathcal{K}_0(\Lambda)$. On

définit $Cl(\Lambda)$ comme étant le conoyau de cette application (voir [18, Chap. I, §2]).

Soient $\mathcal{M}$ un $O_k$-ordre maximal dans $k[\Gamma]$ contenant $O_k[\Gamma]$ et $Cl(\mathcal{M})$ son groupe des classes. Dans la suite nous donnerons deux descriptions de $Cl(\mathcal{M})$, l'une utilisant la décomposition de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples et l'autre la Hom-description de Fröhlich.

On appelle caractère absolument irréductible de $\Gamma$ un caractère irréductible d'une représentation $T : \Gamma \to GL_n(\mathbb{C})$. On désigne par $R_\Gamma$ le groupe abélien libre engendré par les caractères absolument irréductibles de $\Gamma$ (appelé aussi le groupe des caractères virtuels de $\Gamma$).

Soient $\overline{k}$ la clôture algébrique de $k$ contenue dans $\mathbb{C}$ et $\Omega_k = Gal(\overline{k}/k)$. Il est clair que $R_\Gamma$ est un $\Omega_k$-module.

**Définition 1.1.1.** *Deux caractères absolument irréductibles $\chi$ et $\varphi$ de $\Gamma$ sont dits conjugués sur $k$ s'il existe $\omega \in \Omega_k$ tel que :*

$$\forall \gamma \in \Gamma,\ \omega(\chi(\gamma)) = \varphi(\gamma).$$

Cette relation est une relation d'équivalence.

Soit $r$ le nombre des classes de conjugaison sur $k$ des caractères absolument irréductibles de $\Gamma$. Pour tout $i \in \{1, \ldots, r\}$, notons $\chi_i$ un représentant de l'une de ces classes de conjugaison. On note $k(\chi_i)$ l'extension de $k$ obtenue par adjonction à $k$ des valeurs de $\chi_i$.

La décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante (voir [15, p. 330 et §74]) :

$$k[\Gamma] = \prod_{i=1}^{r} M_{n_i}(D_i),$$

où $D_i$ est un corps gauche, de centre $k(\chi_i)$, et $M_{n_i}(D_i)$ est l'anneau des matrices carrées d'ordre $n_i$ à coefficients dans $D_i$. Le degré de $D_i$ sur son centre $k(\chi_i)$ est un carré $m_i^2$. L'entier $m_i$ est appelé l'indice de Schur relatif à $k$. On a $\chi_i(1) = n_i m_i$.

On dit qu'une place infinie $v$ de $k(\chi_i)$ est ramifiée dans $M_{n_i}(D_i)$ si $v$ est une place réelle et si l'algèbre $k(\chi_i)_v \otimes_{k(\chi_i)} M_{n_i}(D_i)$, où $k(\chi_i)_v$ est le complété de $k(\chi_i)$ pour $v$ identifié au corps des réels, est isomorphe à une algèbre de matrices sur le corps des quaternions de Hamilton.

On note $\mathfrak{C}l(k(\chi_i))$ le groupe des classes de $k(\chi_i)$, au sens restreint suivant : $\mathfrak{C}l(k(\chi_i))$ est le quotient du groupe des idéaux fractionnaires de $k(\chi_i)$ par le sous-groupe des idéaux principaux possédant un générateur positif à toutes les places infinies de $k(\chi_i)$ ramifiées dans $M_{n_i}(D_i)$.

On dit que $k[\Gamma]$ vérifie la **condition d'Eichler** si pour toute composante simple $M_{n_i}(D_i)$, il existe une place infinie de $k(\chi_i)$ non ramifiée dans $M_{n_i}(D_i)$, ou si $M_{n_i}(D_i)$ n'est pas de dimension 4 sur $k(\chi_i)$ (voir [27, Definition 38.1, p. 343–344 ; Definition 34.3, p. 294]).

Nous rappelons le théorème de Swan suivant (voir [39] ou [27, Theorem 35.14, p. 313, et Remark (38.5)(i),p. 344]) :

**Théorème 1.1.2.** *Supposons que $k[\Gamma]$ vérifie la condition d'Eichler. Soit $\mathcal{M}$ un $O_k$-ordre maximal dans $k[\Gamma]$ contenant $O_k[\Gamma]$. Alors*

$$Cl(\mathcal{M}) \simeq \prod_{i=1}^{r} \mathfrak{C}l(k(\chi_i)).$$

**Remarque.** Supposons que pour tout $i$, $1 \leq i \leq r$, $\chi_i$ n'est pas symplectique. Cette hypothèse entraîne que l'ensemble des places réelles de $k(\chi_i)$ ramifiées dans $M_{n_i}(D_i)$ est vide. Donc, d'une part $k[\Gamma]$ vérifie la condition d'Eichler. D'autre part $Cl(\mathcal{M}) \simeq \prod_{i=1}^{r} Cl(k(\chi_i))$.

Notons $J(\overline{k})$ le groupe des idèles de $\overline{k}$, $U(\overline{k})$ le sous-groupe des idèles de $J(\overline{k})$ dont les composantes aux places finies sont des unités, et $Hom^{+}_{\Omega_k}(R_\Gamma, U(\overline{k}))$ le sous-groupe de $Hom_{\Omega_k}(R_\Gamma, U(\overline{k}))$ formé par les $f$ tels que $f(\chi)_{\mathfrak{p}} > 0$ pour tout caractère symplectique $\chi$ et toute place infinie $\mathfrak{p}$ prolongeant une place réelle de $k$. Identifions $\overline{k}^{\times}$ avec un sous-groupe de $J(\overline{k})$ par plongement diagonal. Alors la Hom-description de Fröhlich de $Cl(\mathcal{M})$ est la suivante (voir [18] ou [15, §52]) :

**Théorème 1.1.3.**

$$Cl(\mathcal{M}) \simeq \frac{Hom_{\Omega_k}(R_\Gamma, J(\overline{k}))}{Hom_{\Omega_k}(R_\Gamma, \overline{k}^{\times}) Hom^{+}_{\Omega_k}(R_\Gamma, U(\overline{k}))}$$

Signalons que dans cette description, on peut remplacer $\overline{k}$ par une extension galoisienne de $k$, de degré fini et contenant les valeurs des caractères absolument irréductibles de $\Gamma$.

Supposons que $k[\Gamma]$ vérifie la condition d'Eichler. Soit $c \in Cl(\mathcal{M})$. Si $f \in Hom_{\Omega_k}(R_\Gamma, J(\overline{k}))$ est un représentant de $c$ sous l'isomorphisme du théorème 1.1.3, alors pour tout $\chi_i$, $1 \leq i \leq r$, (définis ci-dessus), $f(\chi_i)$ est en fait un élément de $J(k(\chi_i))$ le groupe des idèles de $k(\chi_i)$. Pour tout $i$, $1 \leq i \leq r$, on désigne par $I(\chi_i)$ l'idéal fractionnaire de $k(\chi_i)$ égal au contenu de $f(\chi_i)$, et par $cl(I(\chi_i))$ la classe de $I(\chi_i)$ dans $\mathfrak{C}l(k(\chi_i))$. Alors $(cl(I(\chi_1)), cl(I(\chi_2)), \ldots, cl(I(\chi_r)))$ est un représentant de $c$ sous l'isomorphisme du théorème 1.1.2.

## 1.2 Description d'un représentant de la classe d'un anneau d'entiers dans la Hom-description de $Cl(\mathcal{M})$

Soit $N/k$ une extension galoisienne à groupe de Galois isomorphe à $\Gamma$. Soit $\pi$ un isomorphisme défini sur $Gal(N/k)$ et à valeurs dans $\Gamma$. Pour tout $\gamma \in \Gamma$, nous noterons $\pi^{-1}(\gamma) \in Gal(N/k)$ simplement par $\gamma$.

A l'aide de $\pi$, on munit $O_N$ d'une structure de $O_k[\Gamma]$-module défini par : pour tout $x \in N$ et tout $\gamma \in \Gamma$, $\gamma x = \gamma(x)$. On désigne par $O_{N,\pi}$, ou simplement $O_N$ si aucune ambiguïté n'est possible, le $O_k[\Gamma]$-module ainsi défini.

Tout caractère $\chi$ de $\Gamma$ induit un caractère $\chi \circ \pi$ de $Gal(N/k)$ que l'on notera aussi $\chi$.

Soit $B$ une $k$-algèbre commutative. En faisant agir $\Gamma$ sur $N$, $N \otimes_k B$ est un $B[\Gamma]$-module libre de rang 1. Soit $T : \Gamma \to GL_n(\overline{k})$ une représentation linéaire de $\Gamma$ de caractère $\chi$.

**Définition 1.2.1.** *Soit $a \in N \otimes_k B$. On appelle résolvante de Fröhlich-Lagrange de $a$ et de $\chi$, l'élément de $\overline{k} \otimes_k B$, noté $\langle a, \chi \rangle_{N/k}$ (ou $\langle a, \chi \rangle$ si aucune confusion n'est possible), défini par :*

$$\langle a, \chi \rangle = Det(\sum_{\gamma \in \Gamma} \gamma(a) T(\gamma^{-1})),$$

*où Det désigne le déterminant.*

Dans le cas particulier où $\chi$ est un caractère de degré 1, on retrouve la résolvante de Lagrange classique :

$$\langle a, \chi \rangle = \sum_{\gamma \in \Gamma} \gamma(a) \chi(\gamma^{-1}).$$

Rappelons qu'une extension $K/k$ de corps de nombres est dite modérément ramifiée si pour tout idéal premier $\mathfrak{p}$ de $O_k$ et tout idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, l'indice de ramification $e(\mathfrak{P}/\mathfrak{p})$ est premier avec la caractéristique du corps résiduel $O_k/\mathfrak{p}$.

Fixons quelques notations. Pour tout idéal premier $\mathfrak{p}$ de $O_k$, soit $k_\mathfrak{p}$ (resp. $O_{k,\mathfrak{p}}$) la complétion de $k$ (resp. $O_k$) en $\mathfrak{p}$. On pose : $N_\mathfrak{p} = N \otimes_k k_\mathfrak{p}$ et $O_{N,\mathfrak{p}} = O_N \otimes_{O_k} O_{k,\mathfrak{p}}$.

Lorsque $N/k$ est une extension galoisienne modérément ramifiée, on sait que l'anneau d'entiers $O_N$ de $N$ est un $O_k[\Gamma]$-module localement libre de rang 1 (voir [26] ou [18, Chap. I, §3]).

**Théorème 1.2.2.** *[18, p. 30] Soit $N/k$ une extension galoisienne modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$. Soit $a$ une base du $k[\Gamma]$-module $N$. Pour tout idéal premier $\mathfrak{p}$ de $O_k$, soit $\alpha_\mathfrak{p}$ une base du $O_{k,\mathfrak{p}}[\Gamma]$-module $O_{N,\mathfrak{p}}$. Alors un représentant de la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ dans $Cl(\mathcal{M})$ est l'application $f$ définie par :*

$$f(\chi) = \left( \frac{\langle \alpha_\mathfrak{p}, \chi \rangle}{\langle a, \chi \rangle} \right)_\mathfrak{p}.$$

## 1.3 Résultats de la théorie du corps de classes

**Définition 1.3.1.** *Soit $k$ un corps de nombres. Un cycle (ou module) $\mathcal{C}$ de $k$ est un couple $(\mathcal{C}_0, S)$, où $S$ est un ensemble de places infinies réelles de $k$ et $\mathcal{C}_0$ est un idéal entier de $O_k$.*

*On écrit formellement $\mathcal{C}_\infty = \prod_{v \in S} v$ et $\mathcal{C} = \mathcal{C}_0\mathcal{C}_\infty$ (ou $\mathcal{C} = \mathcal{C}_\infty\mathcal{C}_0$).*

**Définition 1.3.2.** *Soit $\alpha \in k^\times$, on dit que $\alpha$ est congru à 1 $mod^*$ $\mathcal{C}$, et on note $\alpha \equiv 1$ $mod^*$ $\mathcal{C}$, si pour tout $v$ divisant $\mathcal{C}_\infty$ (i.e. $v \in S$), $v(\alpha) > 0$, et si pour tout idéal premier $\mathfrak{p}$ de $O_k$ divisant $\mathcal{C}_0$, $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathcal{C}_0)$, où $v_\mathfrak{p}$ désigne la valuation en $\mathfrak{p}$.*

Soit $I(k)_\mathcal{C}$ le groupe des idéaux fractionnaires de $k$ premiers à $\mathcal{C}_0$. Soit $P(k)_\mathcal{C}$ le sous-groupe de $I(k)_\mathcal{C}$ formé par les idéaux fractionnaires principaux de $k$ ayant un générateur congru à 1 $mod^*$ $\mathcal{C}$. **Le groupe quotient $Cl(k, \mathcal{C}) = I(k)_\mathcal{C}/P(k)_\mathcal{C}$ est appelé le groupe des classes de rayon modulo $\mathcal{C}$.**

**Théorème 1.3.3.** ***(Théorème de densité de Chebotarev)****(voir [25, Chap. VII, Theorem (13.4), p. 545]) Soit $c \in Cl(k, \mathcal{C})$. Alors il existe une infinité d'idéaux premiers $\mathfrak{p}$ de $O_k$, de degré résiduel absolu égal à 1 et tel que la classe de $\mathfrak{p}$ dans $Cl(k, \mathcal{C})$ est $c$.*

On en déduit facilement :

**Proposition 1.3.4.** *L'application définie sur $Cl(k, \mathcal{C})$ et à valeurs dans $Cl(k)$, qui à la classe d'un idéal fractionnaire $I$ de $I(k)_\mathcal{C}$ associe la classe de $I$ dans $Cl(k)$, est un morphisme surjectif. On l'appelera la surjection canonique.*

Rappelons le théorème suivant (voir [42, Theorem 10.1, p. 400]) :

**Théorème 1.3.5.** *Soit $E/k$ une extension finie de corps de nombres. On suppose que toute sous-extension abélienne $F/k$ de $E$, avec $F \neq k$, est ramifiée. Alors, $N_{E/k} : Cl(E) \to Cl(k)$ est surjective.*

## 1.4 Classes de Steinitz et Discriminant

Rappelons la définition de la classe de Steinitz. Soit $k$ un corps de nombres. Soit $M$ un $O_k$-module de type fini, sans torsion et de rang $n$. Alors, il existe un idéal $I$ de $O_k$ tel que $M \simeq O_k^{n-1} \oplus I$ en tant que $O_k$-module. La classe de $I$ dans $Cl(k)$ est appelée la classe de Steinitz de $M$, et on la note $cl_k(M)$ (voir [19, Theorem 13, p. 95], ou [14, Theorem 1.2.19, p. 9 and Corollary 1.2.24, p. 11]). La structure de $M$ en tant que $O_k$-module est complètement déterminée par son rang et sa classe de Steinitz. Ceci s'applique en particulier à $M = O_K$, où $K/k$ est une extension finie de corps de nombres de degré $n$ ; on dira alors que $cl_k(O_K)$ est la classe de Steinitz de $K/k$.

Le théorème suivant est dû à Artin (voir [1], on peut trouver une preuve plus récente de ce résultat dans [23]), il permet de calculer une telle classe.

**Théorème 1.4.1.** *(Artin) Soit $K/k$ une extension finie de corps de nombres. Alors*

$$cl_k(O_K) = cl((\Delta(K/k)/d)^{1/2}),$$

*où $d$ est le discriminant d'une base du $k$-espace vectoriel $K$. De plus, si $K/k$ est galoisienne de degré impair, alors $cl_k(O_K) = cl(\Delta(K/k)^{1/2})$.*

Soient $K/k$ une extension galoisienne finie de groupe de Galois $G$, $\chi$ un caractère de $G$ et $f(\chi, K/k)$ son conducteur d'Artin. Rappelons la décomposition d'Artin et Hasse du discriminant en un produit de conducteurs (voir [30, pp. 111–112]) :

$$\Delta(K/k) = \prod_{\chi} f(\chi, K/k)^{\chi(1)},$$

où $\chi$ parcourt l'ensemble des caractères absolument irréductibles de $G$. Si $k'/k$ est une sous-extension galoisienne de $K/k$, correspondant au sous-groupe $H$ de $G$ et si $\chi$ est un caractère de $G/H$, alors

$$f(\chi, K/k) = f(\chi, k'/k).$$

**Proposition 1.4.2.** *Soient $k$, $K$ et $M$ des corps de nombres tels que $k \subset K \subset M$. Alors :*

*(i)* $\Delta(M/k) = \Delta(K/k)^{[M:K]} N_{K/k}(\Delta(M/K))$.

*(ii)* $cl_k(O_M) = cl_k(O_K)^{[M:K]} N_{K/k}(cl_K(O_M))$.

L'assertion $(i)$ résulte de la transitivité de la différente (voir par exemple [19]). L'assertion $(ii)$ est le théorème 4.1 de [16] ; $(ii)$ est appelée parfois la transitivité de la classe de Steinitz dans une tour de corps de nombres.

Rappelons que deux extensions $K_1/k$ et $K_2/k$ de corps de nombres sont dites arithmétiquement disjointes (sur $k$) si elles sont linéairement disjointes (sur $k$) et si leurs discriminants $\Delta(K_1/k)$ et $\Delta(K_2/k)$ sont premiers entre eux. En utilisant la transitivité de la différente, on obtient facilement la proposition suivante :

**Proposition 1.4.3.** *Soient $K_1/k$ et $K_2/k$ des extensions arithmétiquement disjointes. On note $K_1K_2$ la composée de $K_1$ et $K_2$. Alors $\Delta(K_1K_2/K_2) = \Delta(K_1/k)O_{K_2}$.*

Soient $I$ un idéal fractionnaire d'un corps de nombres $k$, et $p$ un nombre premier. Il est clair qu'on peut écrire de façon unique :

$$I = J_0^p \prod_{i=1}^{p-1} J_i^i, \tag{1.1}$$

où $J_0$ est un idéal fractionnaire de $O_k$, et les $J_i, 1 \leq i \leq p-1$, sont des idéaux entiers de $O_k$ sans facteur carré, et premiers entre eux deux à deux. L'idéal $J_0$ est appelé la **$p$-partie** de $I$, et l'idéal $\prod_{i=1}^{p-1} J_i$, que l'on notera $\mathcal{F}(I)$, le **conducteur** de $I$, et (1.1) la **$p$-décomposition de façon unique** de $I$, ou simplement la décomposition unique de $I$, si aucune confusion n'est possible.

Soit $I'$ un idéal fractionnaire de $O_k$. Immédiatement, $\mathcal{F}(I'^pI) = \mathcal{F}(I)$, et si $I$ et $I'$ sont premiers entre eux, alors $\mathcal{F}(II') = \mathcal{F}(I)\mathcal{F}(I')$.

Soit $a \in \mathbb{Z}$. Si $p$ divise $a$, il est évident que $\mathcal{F}(I^a) = O_k$. Si $p$ ne divise pas $a$, alors $\mathcal{F}(I^a) = \mathcal{F}(I)$ ; en effet,

$$I^a = \Big(J_0^a \prod_{i=1}^{p-1} J_i^{(ai-\underline{ai})/p}\Big)^p \prod_{i=1}^{p-1} J_{\overline{i}}^{\underline{ai}},$$

où les $\underline{ai}$ parcourent $\{1, 2, \ldots, p-1\}$ et $\underline{ai}$ est un représentant de la classe de $ai$ dans $\mathbb{Z}/p\mathbb{Z}$ (l'application : $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto \overline{a}x$, est une bijection, où $\overline{a}$ est la classe de $a$ dans $\mathbb{Z}/p\mathbb{Z}$).

Le théorème suivant découle immédiatement de la théorie de Kummer (voir [20, §39], ou [14, §10.2]) et du théorème d'Artin ci-dessus.

**Théorème 1.4.4.** *Soient $p$ un nombre premier et $k$ un corps de nombres contenant $\xi$ une racine primitive $p$-ième de l'unité. Soient $m \in k^\times$ et $K = k(\sqrt[p]{m})$ une extension cyclique de $k$ de degré $p$. Sous les notations précédentes on a :*

*(i)* $\Delta(K/k) = (\mathcal{F}(mO_K)J)^{p-1}$, *où* $J$ *est un idéal entier de* $O_k$ *dont les diviseurs premiers divisent* $pO_k$. *L'extension* $K/k$ *est modérément ramifiée si et seulement si il existe* $b \in O_k$ *tel que* $b^p m \equiv 1 \, mod^* \ (1-\xi)^p O_k$ ; *cette condition est équivalente à* $J = O_k$ *et* $\mathcal{F}(mO_k)$ *est premier à* $pO_k$.

*(ii) Si* $p$ *est impair, alors* $cl_k(O_K) = cl((\mathcal{F}(mO_k)J)^{p-1/2})$.

**Remarques.** On utilise les hypothèses et notations du théorème précédent.

1) Lorsque $p$ est impair, dans le cas de la ramification modérée, le conducteur de $mO_k$ détermine la classe de Steinitz de $K/k$. La $p$-partie, quant à elle, sera utile dans le chapitre 3 pour calculer la classe réalisable.

2) Soit $\chi$ un caractère non trivial de $Gal(K/k)$ et $f(\chi, K/k)$ son conducteur d'Artin. Par la formule d'Artin et Hasse, $\Delta(K/k) = f(\chi, K/k)^{p-1}$. Si $K/k$ est modérée, alors $f(\chi, K/k) = \mathcal{F}(mO_K)$ par l'assertion (i) du théorème précédent ; ceci justifie l'introduction de la terminologie du conducteur d'un idéal.

# Chapter 2

# On Steinitz classes of nonabelian Galois extensions and $p$-ary cyclic Hamming codes

## 2.1 Statement of the main result

Let $\Gamma$ be a finite group and $k$ a number field. Recall that $R_t(k,\Gamma)$ ($t$ for tame) denotes the set of classes $c \in Cl(k)$ such that there exists a tame Galois extension $N/k$ whose Galois group is isomorphic to $\Gamma$, and whose Steinitz class is equal to $c$.

Let $p$ be a prime number. Let $\mathbb{F}_p$ be the finite field of $p$ elements, which we will often identify with $\mathbb{Z}/p\mathbb{Z}$. Let $V$ be an elementary abelian group of order $p^r$, where $r \geq 1$ , and let $C$ be a cyclic group of order $m$. We denote by

$$\Gamma = V \rtimes_\rho C$$

the semidirect product of $V$ by $C$ which is defined by an $\mathbb{F}_p$-linear representation

$$\rho : C \to Aut(V) = Aut_{\mathbb{F}_p}(V)$$

of $C$ in $V$.

Using properties of a $p$-ary cyclic Hamming code, we shall prove in §3 the following theorem.

**Theorem 2.1.1.** *Let $k$ be a number field and $\Gamma = V \rtimes_\rho C$. Let $\xi$ be a primitive $p$th root of unity. Assume that $\rho$ is faithful and irreducible, and $m = (p^r - 1)/(p-1)$, where $r \geq 2$ and $gcd(r, p-1) = 1$. Then $R_t(k,\Gamma)$ is*

*the following subgroup of $Cl(k)$:*

$$\begin{aligned} R_t(k,\Gamma) &= R_t(k,C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi))\big)^{\frac{1}{2}mp^{r-1}(p-1)} \\ &= R_t(k,C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi))\big)^{\frac{1}{2}(p^r-1)p^{r-1}}, \end{aligned}$$

*where the group $R_t(k,C)$ is given by:*

$$R_t(k,C) = \prod_{d|m} N_{k(\xi_d)/k}\big(Cl(k(\xi_d))\big)^{m(d-1)/2d},$$

*where $d$ runs through the set of positive divisors of $m$ and $\xi_d$ is a primitive $d$th root of unity.*

**Remark.** Theorem 2.1.1 is a generalization of two theorems:
(1) If $\xi \in k$, then Theorem 2.1.1 is [7, Theorem 7.2.3 (i)] .
(2) If $p = 2$ and $r \geq 2$ then $m = 2^r - 1$ and the condition on *gcd* is satisfied. Theorem 2.1.1 is [4, Theorem 1.4 (ii)].

## 2.2 Preliminaries

Let $p$ be a prime number. Let $C$ be a cyclic group of order

$$m = (p^r - 1)/(p-1), \text{ where } r \geq 2 \text{ and } gcd(r, p-1) = 1.$$

(Then $\mathbb{F}_p[C]$ is a semisimple algebra since $m$ is coprime to $p$.) Let $V$ be an elementary abelian group of order $p^r$; then $V$ is an $\mathbb{F}_p$-vector space of dimension $r$. Let

$$\rho : C \to Aut(V) = Aut_{\mathbb{F}_p}(V)$$

be an $\mathbb{F}_p$-linear representation of $C$ in $V$. Let

$$\Gamma = V \rtimes_\rho C$$

be the semidirect product of $V$ by $C$ which is defined by $\rho$.

In the sequel, in order to simplify notation, one identifies groups which are isomorphic whenever we can do so without any ambiguity; for instance, we will very often consider $C$ and $V$ as subgroups of $\Gamma$, the multiplication in $\Gamma$ is then determined by $\sigma v \sigma^{-1} = \rho(\sigma)(v)$, for $\sigma \in C$ and $v \in V$.

We have $m = \sum_{i=0}^{r-1} p^i \geq p^{r-1} + 1 > p^s - 1$, for all natural integers $s$ with $1 \leq s < r$. Therefore $m$ divides $p^r - 1$ but does not divide $p^s - 1$ for any $s$ with $1 \leq s < r$. By [7, Proposition 4.1.1], there exists a representation $\rho$ which is faithful and irreducible.

**From now on we suppose that $\rho$ is faithful and irreducible.**

**We fix a generator $\sigma$ of $C$ and denote by $f$ the minimal polynomial of $\rho(\sigma) \in Aut_{\mathbb{F}_p}(V)$.**

It follows from the proof of [7, Proposition 4.1.1] that since $\rho$ is irreducible and faithful, $f$ **is an irreducible factor of** $X^m - 1$**,** $deg(f) = r$ and **the roots of** $f$ **have the same order** $m$ **in** $\mathbb{F}_{p^r}^{\times}$ (recall that the roots of $f$ have the same order because they are conjugate under the Frobenius of $Gal(\mathbb{F}_{p^r}/\mathbb{F}_p)$).

**In all that follows we denote by $g$ the element of $\mathbb{F}_p[X]$ satisfying:**

$$fg = X^m - 1.$$

We recall the (simplest) definition of a cyclic code (see for instance [28, §7.4, p. 320]): it is an ideal of $\mathbb{F}_q[X]/(X^n - 1)$, where $\mathbb{F}_q$ is a finite field with $q$ elements and $n$ a nonzero natural number. Its elements are called codewords. In the terminology of coding theory (see for instance [28, p. 146]), the weight $w(c)$ of a codeword $c$ of a cyclic code is the number of its nonzero components in the canonical basis $(\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1})$, where $\overline{X}^i$ is the class of $X^i$ in $\mathbb{F}_q[X]/(X^n - 1)$.

In our situation, since $\mathbb{F}_p[C] \simeq \mathbb{F}_p[X]/(X^m - 1)$ (the isomorphism is given by $\sigma \mapsto \overline{X}$), one defines a cyclic code of $\mathbb{F}_p[C]$ as an ideal of $\mathbb{F}_p[C]$.

We point out that, since $gcd(r, p-1) = 1$, it follows from the proof of [28, Theorem 7.4.8, p. 329] that the cyclic code

$$(f(\sigma)) \subset \mathbb{F}_p[C]$$

generated by $f(\sigma)$ is a $p$**-ary cyclic Hamming code** having length $m$, dimension $m - r$ and minimum distance 3.

Let

$$\mathcal{C} = (g(\sigma)) \subset \mathbb{F}_p[C]$$

be the cyclic code generated by $g(\sigma)$; it is a code with length $m = (p^r - 1)/(p-1)$ and dimension $r$. Furthermore, $\mathcal{C}$ is an irreducible code since its check polynomial $f$ is irreducible; recall that $m$ is the order of any root of $f$. From $m = r + (p-1)\sum_{i=1}^{r-1}(\frac{p^i-1}{p-1})$ we deduce that

$$gcd(r, p-1) = 1 \text{ is equivalent to } gcd(m, p-1) = 1.$$

Therefore $m/gcd(m, p-1) = (p^r - 1)/(p-1)$. Using [41, Theorem 1] we obtain: all the nonzero code words $c$ of $\mathcal{C}$ have the same weight $w(c) = p^{r-1}$ ($\mathcal{C}$ **is a 1-weight code**).

Let $\hat{g}$ be the reciprocal polynomial of $g$, that is $\hat{g} = X^{deg(g)}g(X^{-1}) = X^{m-r}g(X^{-1})$. Let

$$\hat{\mathcal{C}} = (\hat{g}(\sigma)) \subset \mathbb{F}_p[C]$$

be the cyclic code generated by $\hat{g}(\sigma)$; it has length $m$ and dimension $r$. Then $\hat{\mathcal{C}}$ is the dual of the Hamming code $(f(\sigma))$ (see for instance [28, Theorem 7.4.4 (3), p. 325]); according to [28, p. 256] $\hat{\mathcal{C}}$ is called a simplex code when $p = 2$. It is immediate that **all the nonzero code words** $c$ **of** $\hat{\mathcal{C}}$ **have the same weight** $w(c) = p^{r-1}$ (because $\sum_{i=0}^{m-1} a_i\sigma^i \in \mathcal{C}$ is equivalent to $\sum_{i=0}^{m-1} a_{m-i-1}\sigma^i \in \hat{\mathcal{C}}$).

**Remark.** We can see that the nonzero codewords of $\mathcal{C}$ and $\hat{\mathcal{C}}$ have weight $p^{r-1}$ without appealing to [41, Theorem 1]. The first row of the corresponding Hamming matrix (see [28, pp. 253–254]) has weight $p^{r-1}$ as there are precisely $p^{r-1}$ one-dimensional subspaces of $\mathbb{F}_p^r$ generated by a vector with nonzero first entry. All the other nonzero codewords have the same weight as they are shifts of this one.

Below, we will fix some notation and recall well-known results which will be useful for the proof of Theorem 2.1.1.

Let $k$ be a number field and $\mathcal{C}$ a cycle of $k$. If $I$ is a fractional ideal of $k$ coprime to $\mathcal{C}$, we denote by $cl_{k,\mathcal{C}}(I)$ its class in $Cl(k,\mathcal{C})$ the ray class group of $k$ modulo $\mathcal{C}$. If $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (respectively $\mathbb{Z}$), we denote by $\underline{a}$ the natural number $0 \leq \underline{a} \leq p-1$ such that the class of $\underline{a}$ in $\mathbb{F}_p$ is equal to $a$ (respectively the class of $a$ in $\mathbb{Z}/p\mathbb{Z}$). We recall that $\xi$ is a primitive $p$th root of unity.

For an element $\alpha = \sum_{i=0}^{m-1} a_i\sigma^i \in \mathbb{F}_p[C]$, we will frequently abuse notation by also writing $\alpha$ for the corresponding element of $\mathbb{Z}[C]$: $\alpha = \sum_{i=0}^{m-1} \underline{a_i}\sigma^i$. **We will then refer to** $\sum_{i=0}^{m-1} \underline{a_i}\sigma^i$ **as** $\alpha$ **considered as an element of** $\mathbb{Z}[C]$.

Let $K$ be a number field and let $M/K$ be a finite Galois extension with Galois group $G$. The multiplicative group $M^\times$ and the group $I_M$ of the fractional ideals of $M$ are naturally $\mathbb{Z}[G]$-modules. We choose the following notation for the action of $\mathbb{Z}[G]$: let $\alpha = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, $x \in M^\times$ and $I \in I_E$, then

$$\alpha x = \prod_{g\in G} g(x)^{a_g}, \quad I^\alpha = \prod_{g\in G} g(I)^{a_g}.$$

Let $N/k$ be a Galois extension whose Galois group is isomorphic to $\Gamma$. Let $E/k$ be the subextension of $N/k$ fixed by $V$. Then $E/k$ is cyclic of degree $m$ and $Gal(E/k) \simeq C$. The extension $N/E$ contains $(p^r-1)/(p-1) = m$ cyclic extensions of $E$ of degree $p$; if $L/E$ is one of these, then the others are $\sigma^i(L)$, $1 \leq i \leq (m-1)$.

**Proposition 2.2.1.** *With the above notation we have:*

$$cl_k(O_N) = \big(cl_k(O_E)\big)^{p^r}\big(N_{E/k}\big(cl_E(O_L)\big)\big)^m.$$

*Proof.* The proof is exactly the same as that of [3, Proposition 3.3].

In short, we use three ingredients: a) the transitivity of Steinitz class in a tower of number fields (see Proposition 1.4.2(ii)); applying to our situation we obtain: $cl_k(O_N) = (cl_k(O_E))^{p^r}(N_{E/k}(cl_E(O_N)))$; b) $cl_E(O_N) = \prod_{i=0}^{m-1}(cl_E(O_{\sigma^i(L)}))$; this is a consequence of [4, Lemma 3.4] and [3, Lemma 3.4] for $p = 2$ and $p$ odd, respectively; c) $cl_E(O_{\sigma^i(L)}) = \sigma^i(cl_E(O_L))$. □

**We denote by $d$ the degree of the extension $k(\xi)/k$ (recall that $d$ is a divisor of $p-1$) and $H = Gal(k(\xi)/k)$. We choose a generator $\sigma_0$ of $H$. Let $s$ be the integer such that $\sigma_0(\xi) = \xi^s$ and $1 \leq s \leq p-1$. We fix the notation $s_i = \underline{(s^i)}$, and we define $\theta \in \mathbb{Z}[H]$ by**

$$\theta = \sum_{i=0}^{d-1} s_i \sigma_0^{-i}.$$

**Remark.** In the case $d = p-1$, which is equivalent to $Gal(k(\xi)/k) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, $\theta$ is the usual Stickelberger element.

**Proposition 2.2.2.** *Let $K/k(\xi)$ be a cyclic (Kummer) extension of degree $p$.*

*(1) The extension $K/k$ is abelian if and only if there exists $m \in k(\xi)^\times$ such that $K = k(\xi)\big((\theta m)^{1/p}\big)$.*

*(2) Assume that $K/k$ is abelian and let $\mathfrak{p}$ be a prime ideal of $O_k$ coprime to $pO_k$. If $K/k(\xi)$ is (tamely) ramified at $\mathfrak{p}$, then $\mathfrak{p}$ is totally split in $k(\xi)/k$.*

*Proof.* The assertion (1) is [22, Corollary 1.3, p. 89], and (2) is the main part of [22, Proposition 2.4, pp. 89–90]. □

**Remark.** With the hypotheses and notation of the preceding proposition, assume that $K/k$ is abelian. Since $[K : k] = pd$, $K/k$ has a subextension $L/k$ of degree $p$. Because $p$ is coprime to $d$, the extensions $L/k$ and $k(\xi)/k$ are linearly disjoint. We deduce that $K = Lk(\xi) = L(\xi)$ and $Gal(K/k) \simeq Gal(L/k) \times Gal(k(\xi)/k) (\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \simeq \mathbb{Z}/pd\mathbb{Z})$. Therefore $K/k$ is cyclic and $L$ is unique.

Let $I$ be a fractional ideal of $O_k$. Recall (see Chapter 1) that $I$ can be written uniquely in the form:

$$I = J_0^p \prod_{i=1}^{p-1} J_i^i, \tag{2.1}$$

where $J_0$ is a fractional ideal of $O_k$, and the $J_i$, $1 \leq i \leq p-1$, are pairwise relatively prime square free integral ideals of $O_k$. **The ideal $J_0$ is called the $p$-part of $I$, the ideal $\prod_{i=1}^{p-1} J_i$, which will be denoted by $\mathcal{F}(I)$, the conductor of $I$, and (2.1) the $p$-unique decomposition of $I$.**

## 2.3 Proof of the main result

In this section we will prove Theorem 2.1.1.

*Proof of Theorem 2.1.1.* We have seen, in the remark after Theorem 2.1.1, that when $p = 2$ Theorem 1.1 is [4, Theorem 1.4(ii)]. The proof in this case is in [4, p. 18]).

**In all that follows we assume that $p$ is odd.**

The proof will be divided into three parts.

(1) In this part we prove the inclusion

$$R_t(k,\Gamma) \subset R_t(k,C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi)\big)^{\frac{1}{2}mp^{r-1}(p-1)}. \tag{2.2}$$

Let $N/k$ be a tame Galois extension, with Galois group isomorphic to $\Gamma$.

Let us show that $N/k$ and $k(\xi)/k$ are linearly disjoint. The extensions $E/k$ and $k(\xi)/k$ are linearly disjoint because $[E : k] = m$, $[k(\xi) : k]$ is a divisor of $p-1$ and $gcd(m, p-1) = 1$ (since $gcd(r, p-1) = 1$). From $[N : E] = p^r$ is coprime to $[E(\xi) : E]$, we deduce that $N/E$ and $E(\xi)/E$ are also linearly disjoint. We have $N \cap k(\xi) = (N \cap E(\xi)) \cap k(\xi) = E \cap k(\xi) = k$; therefore the Galois extensions $N/k$ and $k(\xi)/k$ are linearly disjoint, which implies

$$Gal(N(\xi)/k) \simeq Gal(N/k) \times Gal(k(\xi)/k) \simeq \Gamma \times H.$$

Let $L/E$ be a subextension of degree $p$ of $N/E$. We have immediately the following morphisms of restriction:

$$Gal(N(\xi)/k(\xi)) \simeq Gal(N/k) = \Gamma, \quad Gal(E(\xi)/k(\xi)) \simeq Gal(E/k) \simeq C,$$

$$Gal(N(\xi)/N) \simeq Gal(L(\xi)/L) \simeq Gal(E(\xi)/E) \simeq Gal(k(\xi)/k) = H.$$

Since $N(\xi)/k$ is tame as a compositum of tame extensions (recall that $k(\xi)/k$ is tame), $N(\xi)/k(\xi)$ is tame.

In the sequel, in order to simplify notation, if $g \in Gal(N(\xi)/k)$, we will also denote by $g$ its restriction to a subextension of $N(\xi)/k$ if no confusion is possible. Recall that we identify groups which are isomorphic whenever we can do so without any ambiguity.

By Proposition 2.2.1

$$cl_k(O_N) = \big(cl_k(O_E)\big)^{p^r}\big(N_{E/k}\big(cl_E(O_L)\big)\big)^m. \tag{2.3}$$

As $p$ is odd, the well-known theorem of Artin (see Theorem 1.4.1) yields

$$cl_E(O_L) = cl_E\big(\Delta(L/E)^{1/2}\big).$$

It is clear that $L/E$ and $E(\xi)/E$ are linearly disjoint, whence $L(\xi)/E(\xi)$ is cyclic of degree $p$. Since only prime divisors of $pO_E$ can be ramified in $E(\xi)/E$ and $L/E$ is tame of degree $p$, we have that $L/E$ and $E(\xi)/E$ are arithmetically disjoint (that is: linearly disjoint and their discriminants are coprime). Consequently, by Proposition 1.4.3 we have:

$$\Delta(L/E)O_{E(\xi)} = \Delta(L(\xi)/E(\xi)).$$

It follows that

$$\Delta(L/E)^d = N_{E(\xi)/E}\big(\Delta(L(\xi)/E(\xi))\big). \tag{2.4}$$

Let us compute $\Delta(L(\xi)/E(\xi))$ ((2.10) below is the result of our computation).

Since $Gal(E(\xi)/k(\xi)) \simeq C$, $E(\xi)^\times$ and the group of the fractional ideals of $E(\xi)$ are naturally $\mathbb{Z}[C]$-modules (as explained in Section 2).

Now we consider $\hat{g}(\sigma)$ as an element of $\mathbb{Z}[C]$. As $N(\xi)/k(\xi)$ is a tame Galois extension with $Gal(N(\xi)/k(\xi)) \simeq \Gamma$, [7, Lemma 5.1.5] gives us:

$$L(\xi) = E(\xi)\Big(\sqrt[p]{\hat{g}(\sigma)y}\Big)$$

for some $y \in E(\xi)^\times$ satisfying the following conditions: $\hat{g}(\sigma)y \notin E(\xi)^{\times p}$, $y \equiv 1\, mod^*\, (1-\xi)^p O_{E(\xi)}$ and the fractional ideal $yO_{E(\xi)}$ factorizes as

$$yO_{E(\xi)} = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i(\sigma)}$$

for some $n \geq 0$, some $e_i(\sigma) \in \mathbb{Z}[C]$, and some prime ideals $\mathfrak{P}_i$ of $O_{E(\xi)}$ which lie above distinct prime ideals $\mathfrak{q}_i$ of $O_{k(\xi)}$ which split completely in $E(\xi)/k(\xi)$ and do not contain $p$ (when $n = 0$, the product of $n$ ideals of $O_{E(\xi)}$ should be interpreted as $O_{E(\xi)}$ itself).

We have

$$\hat{g}(\sigma)yO_{E(\xi)} = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}.$$

Clearly we may write

$$e_i(\sigma)\hat{g}(\sigma) = pq_i(\sigma) + r_i(\sigma), \tag{2.5}$$

where the coefficients in the basis $C$ of $r_i(\sigma)$ belong to $\{0, 1, \ldots, p-1\}$. Renumbering the $\mathfrak{P}_i$, we can suppose that $\mathfrak{P}_i^{r_i(\sigma)} \neq O_{E(\xi)}$ (which is equivalent to $r_i(\sigma) \neq 0$) if and only if $1 \leq i \leq t$, say. Therefore the $p$-unique decomposition of $\hat{g}(\sigma)yO_{E(\xi)}$ is

$$\hat{g}(\sigma)yO_{E(\xi)} = \Big(\prod_{i=1}^{n} \mathfrak{P}_i^{q_i(\sigma)}\Big)^p \prod_{i=1}^{t} \mathfrak{P}_i^{r_i(\sigma)}. \tag{2.6}$$

(Note that if the set of $i$ such that $\mathfrak{P}_i^{r_i(\sigma)} \neq O_{E(\xi)}$ is empty we use the usual conventions for empty products.)

Because the ideals $\mathfrak{P}_i^{r_i(\sigma)}$, $1 \leq i \leq t$, are pairwise relatively prime (the $\mathfrak{P}_i$ split completely in $E(\xi)/k(\xi)$ and lie above distinct prime ideals of $O_{k(\xi)}$), we have

$$\mathcal{F}(\hat{g}(\sigma)yO_{E(\xi)}) = \prod_{i=1}^{t} \mathcal{F}(\mathfrak{P}_i^{r_i(\sigma)}). \tag{2.7}$$

Since the extension $L(\xi)/E(\xi)$ is a tame cyclic (Kummer) extension of degree $p$ and $L(\xi) = E(\xi)\Big(\sqrt[p]{\hat{g}(\sigma)y}\Big)$, Theorem 1.4.4(i) and (2.7) give us:

$$\Delta(L(\xi)/E(\xi)) = \Big(\prod_{i=1}^{t} \mathcal{F}(\mathfrak{P}_i^{r_i(\sigma)})\Big)^{p-1}. \tag{2.8}$$

For $1 \leq i \leq t$, put

$$r_i(\sigma) = \sum_{l=0}^{m-1} a_{il}\sigma^l, \quad \text{where} \quad a_{il} \in \{0, 1, \ldots, p-1\}.$$

Then

$$\mathcal{F}\big(\mathfrak{P}_i^{r_i(\sigma)}\big) = \prod_{l=0, a_{il}\neq 0}^{m-1} \mathcal{F}(\sigma^l(\mathfrak{P}_i)^{a_{il}}) = \prod_{l=0, a_{il}\neq 0}^{m-1} \sigma^l(\mathfrak{P}_i). \tag{2.9}$$

Let $\mathfrak{P}$ be a prime ideal of $O_{E(\xi)}$ which is ramified in $L(\xi)/E(\xi)$. Below we will show that $\mathfrak{P}$ is totally split in the Galois extension $E(\xi)/k$.

From (2.8) and (2.9) we deduce that there exist $1 \leq i \leq t$ and $0 \leq j \leq m-1$ such that $\mathfrak{P} = \sigma^j(\mathfrak{P}_i)$. We know that $\mathfrak{P}_i$ is totally split in $E(\xi)/k(\xi)$, so is $\mathfrak{P}$. Since $L(\xi)/E$ is abelian and $\mathfrak{P}$ is coprime to $pO_{E(\xi)}$, Proposition 2.2.2(2) tells us that $\mathfrak{P}$ is totally split in $E(\xi)/E$. Let $\mathfrak{p} = \mathfrak{P} \cap O_E$

and $\mathfrak{q} = \mathfrak{P} \cap O_{k(\xi)}$. The prime $\mathfrak{P}$ is not ramified in $E(\xi)/k(\xi)$ and $\mathfrak{q}$ is not ramified in $k(\xi)/k$ implies that $\mathfrak{P}$ is not ramified in $E(\xi)/k$. Using the multiplicativity of the residual degree (which we denote by $f$), we have $f(\mathfrak{P}/\mathfrak{P} \cap O_k) = f(\mathfrak{p}/\mathfrak{p} \cap O_k) = f(\mathfrak{q}/\mathfrak{q} \cap O_k)$; in particular $f(\mathfrak{p}/\mathfrak{p} \cap O_k)$ is a divisor of $gcd(m, d)$. But $gcd(m, d) = 1$, whence $f(\mathfrak{p}/\mathfrak{p} \cap O_k) = 1$. It follows that $f(\mathfrak{P}/\mathfrak{P} \cap O_k) = 1$. We conclude that $\mathfrak{P}$ is totally split in $E(\xi)/k$.

Now let $1 \leq i \leq t$, then $\mathfrak{P}_i$ is also totally split in the Galois extension $E(\xi)/k$, indeed: $r_i(\sigma)$ being nonzero, let $l$ satisfying $a_{il} \neq 0$, then $\sigma^l(\mathfrak{P}_i)$ is ramified in $L(\xi)/E(\xi)$, therefore it is totally split in $E(\xi)/k$, so is $\mathfrak{P}_i$.

Let $0 \leq j \leq d-1$. Since $\sigma_0^j(L(\xi)) = L(\xi)$ ($Gal(L(\xi)/L) \simeq H = \langle \sigma_0 \rangle$), it is immediate that

$$L(\xi) = E(\xi)\Big(\sqrt[p]{\sigma_0^j(\hat{g}(\sigma)y)}\Big).$$

Because the prime ideals $\sigma_0^j(\mathfrak{P}_i)$, $1 \leq i \leq t$, are totally split in $E(\xi)/k$, it follows from (2.6) that the $p$-unique decomposition of $\sigma_0^j(\hat{g}(\sigma)y)O_{E(\xi)}$ is :

$$\sigma_0^j(\hat{g}(\sigma)y)O_{E(\xi)} = \Big(\prod_{i=1}^{n} \sigma_0^j(\mathfrak{P}_i)^{q_i(\sigma)}\Big)^p \prod_{i=1}^{t} \sigma_0^j(\mathfrak{P}_i)^{r_i(\sigma)}.$$

Thanks to Theorem 1.4.4(i), we have

$$\Delta(L(\xi)/E(\xi)) = \Big(\prod_{i=1}^{t} \mathcal{F}\big(\sigma_0^j(\mathfrak{P}_i)^{r_i(\sigma)}\big)\Big)^{p-1}.$$

Therefore we can claim that for all $0 \leq j \leq d-1$ and $1 \leq i \leq t$, $\mathcal{F}\big(\sigma_0^j(\mathfrak{P}_i)^{r_i(\sigma)}\big)$ is a divisor of $\mathcal{F}(\hat{g}(\sigma)yO_{E(\xi)})$.

Renumbering the ideals $\mathfrak{P}_i$, $1 \leq i \leq t$, we can choose $\mathfrak{P}_i$, $1 \leq i \leq t_0$, a system of representatives of the $\mathfrak{P}_i$ under the equivalence relation R : $\mathfrak{P}_i \mathrm{R} \mathfrak{P}_{i'}$ if there exists $0 \leq j \leq d-1$ such that $\mathfrak{P}_{i'} = \sigma_0^j(\mathfrak{P}_i)$. The above claim and (2.8) yield:

$$\Delta(L(\xi)/E(\xi)) = \Big(\prod_{i=1}^{t_0} \Big(\prod_{j=0}^{d-1} \mathcal{F}\big(\sigma_0^j(\mathfrak{P}_i)^{r_i(\sigma)}\big)\Big)\Big)^{p-1}.$$

Recall that $r_i(\sigma) = \sum_{l=0}^{m-1} a_{il}\sigma^l$, $a_{il} \neq 0$ is coprime to $p$ and $Gal(E(\xi)/k) = \langle \sigma, \sigma_0 \rangle$ is abelian. Then

$$\mathcal{F}\big(\sigma_0^j(\mathfrak{P}_i)^{r_i(\sigma)}\big) = \mathcal{F}\Big(\prod_{l=0, a_{il} \neq 0}^{m-1} \sigma^l(\sigma_0^j(\mathfrak{P}_i))^{a_{il}}\Big) = \prod_{l=0, a_{il} \neq 0}^{m-1} \sigma^l(\sigma_0^j(\mathfrak{P}_i)),$$

and

$$\Delta(L(\xi)/E(\xi)) = \Big(\prod_{i=1}^{t_0}\Big(\prod_{j=0}^{d-1}\sigma_0^j\Big(\prod_{l=0,a_{il}\neq 0}^{m-1}\sigma^l(\mathfrak{P}_i)\Big)\Big)\Big)^{p-1}, \tag{2.10}$$

which completes the computation of $\Delta(L(\xi)/E(\xi))$.

Let $\mathfrak{p}_i = \mathfrak{P}_i \cap O_E$. Clearly $N_{E(\xi)/E}(\mathfrak{P}_i) = \mathfrak{p}_i$. We then have (recall that $Gal(E(\xi)/E) = \langle\sigma_0\rangle$):

$$N_{E(\xi)/E}\big(\Delta(L(\xi)/E(\xi))\big) = \Big(\prod_{i=1}^{t_0}\Big(\prod_{l=0,a_{il}\neq 0}^{m-1}\sigma^l(\mathfrak{p}_i)\Big)\Big)^{d(p-1)}.$$

Using (2.4) we obtain

$$\Delta(L/E)^{1/2} = \Big(\prod_{i=1}^{t_0}\Big(\prod_{l=0,a_{il}\neq 0}^{m-1}\sigma^l(\mathfrak{p}_i)\Big)\Big)^{(p-1)/2}.$$

Therefore

$$N_{E/k}\big(\Delta(L/E)^{1/2}\big) = \Big(\prod_{i=1}^{t_0} N_{E/k}(\mathfrak{p}_i)^{w(r_i(\sigma))}\Big)^{(p-1)/2},$$

where we consider $r_i(\sigma)$, $1 \le i \le t_0$, as an element of $\mathbb{F}_p[C]$.

It follows from (2.5) that $r_i(\sigma)$ is a nonzero codeword of the cyclic code $\hat{\mathcal{C}} = (\hat{g}(\sigma))$. Consequently

$$w(r_i(\sigma)) = w(\hat{g}(\sigma)) = p^{r-1}.$$

Hence

$$N_{E/k}(cl_E(O_L)) = \Big(\prod_{i=1}^{t_0} N_{E/k}(cl_E(\mathfrak{p}_i))\Big)^{p^{r-1}(p-1)/2}.$$

Let $\mathfrak{q}_i = \mathfrak{P}_i \cap O_{k(\xi)}$. We have

$$\begin{aligned} N_{E(\xi)/k}(\mathfrak{P}_i) &= N_{E/k}(N_{E(\xi)/E}(\mathfrak{P}_i)) = N_{E/k}(\mathfrak{p}_i) \\ &= N_{k(\xi)/k}(N_{E(\xi)/k(\xi)}(\mathfrak{P}_i)) = N_{k(\xi)/k}(\mathfrak{q}_i). \end{aligned}$$

Therefore $N_{E/k}(\mathfrak{p}_i) = N_{k(\xi)/k}(\mathfrak{q}_i)$. Whence

$$N_{E/k}(cl_E(O_L)) \in N_{k(\xi)/k}\big(Cl(k(\xi)\big)^{p^{r-1}(p-1)/2}. \tag{2.11}$$

We have the inclusion (2.2) thanks to (2.3) and (2.11), which completes the proof of the part (1).

(2) In this part we prove the inclusion

$$R_t(k,C)^{p^r} N_{k(\xi)/k}\big(Cl(k(\xi))\big)^{\frac{1}{2}mp^{r-1}(p-1)} \subset R_t(k,\Gamma). \tag{2.12}$$

**Let** $c_1 \in R_t(k,C)$ **and** $c_2 \in Cl(k(\xi))$**.**

**Let us consider** $c_1$**.** By the assertions (a), (b) and (c) of [24, Theorem 6.17, p. 289], there exists a tame Galois extension $E/k$ with Galois group isomorphic to $C$, such that $c_1 = cl_k(O_E)$, at least one prime ideal of $O_k$ is ramified in each of the subextensions of $E/k$ different from $k$, and the discriminant of $E/k$ is relatively prime to $pO_k$; it follows from the last assertion that $E/k$ and $k(\xi)/k$ are arithmetically disjoint, in particular $Gal(E(\xi)/k(\xi)) \simeq Gal(E/k) \simeq C$, $Gal(E(\xi)/E) \simeq Gal(k(\xi)/k) = H$ and $Gal(E(\xi)/k) = Gal(E(\xi)/E) \times Gal(E(\xi)/k(\xi)) \simeq H \times C$.

Let us show that the only subextension of $E(\xi)/k(\xi)$ unramified over $k(\xi)$ is $k(\xi)$ itself; this fact implies

$$N_{E(\xi)/k(\xi)}\big(Cl(E(\xi)\big) = Cl(k(\xi)) \tag{2.13}$$

by Theorem 1.3.5

Let $K/k(\xi)$ be a subextension of $E(\xi)/k(\xi)$ having degree $d_1 \neq 1$; $K/k(\xi)$ is unique since $Gal(E(\xi)/k(\xi))$ is cyclic. It follows from $d_1$ is a divisor of $[E(\xi) : k(\xi)] = m$ and $E/k$ is abelian of degree $m$ that there exists a subextension $E_1/k$ of $E/k$ of degree $d_1$. It is clear that $E_1/k$ and $k(\xi)/k$ are arithmetically disjoint. Therefore $[E_1(\xi) : k(\xi)] = d_1$ which yields $E_1(\xi) = K$, and $\Delta(E_1/k)O_{k(\xi)} = \Delta(K/k(\xi))$ which gives $K/k(\xi)$ is ramified.

**Now let us consider** $c_2$**.** Thanks to (2.13), **there exists** $c_3 \in Cl(E(\xi))$ such that

$$N_{E(\xi)/k(\xi)}(c_3) = c_2.$$

Let $t > 3$ be an odd natural number such that $c_3^t = c_3$; for instance $t = 4h + 1$, where $h$ is the class number of $E(\xi)$ or the order of $c_3$. Let $a_i$, $1 \leq i \leq t$, be natural numbers coprime to $p$ and such that $\sum_{i=1}^{t} a_i = pt$; for instance: $a_i = p-1$, for $1 \leq i \leq (t+1)/2$, $a_i = p+1$, for $(t+3)/2 \leq i \leq t-1$, and $a_t = p + 2$.

**Let us consider** $c_3$**.** Let $\mathcal{C}$ be the cycle $(1-\xi)^p O_{E(\xi)}$. By the Tchebotarev density theorem (see Theorem 1.3.3), and the canonical surjection from the ray class group $Cl(E(\xi),\mathcal{C})$ onto $Cl(E(\xi))$, that to $cl_{E(\xi),\mathcal{C}}(I)$ assigns $cl_{E(\xi)}(I)$ (see Proposition 1.3.4), where $I$ is a fractional ideal of $O_{E(\xi)}$ coprime to $\mathcal{C}$,

there exist $t$ prime ideals $\mathfrak{P}_i$ of $O_{E(\xi)}$, totally split in $E(\xi)/k$, which lie above distinct prime ideals of $O_k$, coprime to $\mathcal{C}$ and such that for all $i$, $1 \leq i \leq t$, $cl_{E(\xi),\mathcal{C}}(\mathfrak{P}_i) = cl_{E(\xi),\mathcal{C}}(\mathfrak{P}_1)$ and $c_3 = cl_{E(\xi)}(\mathfrak{P}_i)$. Similarly, let $\mathfrak{P}$ be a prime ideal of $O_{E(\xi)}$ coprime to $\mathcal{C}$ (not necessarily totally split in $E(\xi)/k$) such that $cl_{E(\xi),\mathcal{C}}(\mathfrak{P}_1)^{-1} = cl_{E(\xi),\mathcal{C}}(\mathfrak{P})$. Then

$$cl_{E(\xi),\mathcal{C}}\Big(\prod_{i=1}^{t}\mathfrak{P}_i^{a_i}\Big)cl_{E(\xi),\mathcal{C}}(\mathfrak{P}^{pt}) = 1 \text{ in } \ Cl(E(\xi),\mathcal{C}).$$

We conclude that there exists $m \in E(\xi)^{\times}$ satisfying

$$mO_{E(\xi)} = (\mathfrak{P}^t)^p \prod_{i=1}^{t}\mathfrak{P}_i^{a_i} \ \text{ and } \ m \equiv 1 \ mod^* \ (1-\xi)^p O_{E(\xi)},$$

with

$$c_3 = cl_{E(\xi)}(\mathfrak{P}_i), \text{for all } 1 \leq i \leq t.$$

Now we consider $\hat{g}(\sigma)$ as an element of $\mathbb{Z}[C]$. We have the equality:

$$\hat{g}(\sigma)mO_{E(\xi)} = (\mathfrak{P}^{t\hat{g}(\sigma)})^p \prod_{i=1}^{t}\mathfrak{P}_i^{a_i\hat{g}(\sigma)}.$$

Let us identify $Gal(E(\xi)/E)$ with $Gal(k(\xi)/k) = H$, and recall that

$$\theta = \sum_{j=0}^{d-1} s_j \sigma_0^{-j}.$$

It follows from $E(\xi)/k$ abelian that

$$\theta(\hat{g}(\sigma)m) = \hat{g}(\sigma)(\theta m).$$

Therefore

$$\hat{g}(\sigma)(\theta m)O_{E(\xi)} = (\theta\mathfrak{P}^{t\hat{g}(\sigma)})^p \prod_{i=1}^{t}\theta\mathfrak{P}_i^{a_i\hat{g}(\sigma)}, \tag{2.14}$$

where (we recall):

$$\theta m = \prod_{j=0}^{d-1}\sigma_0^{-j}(m)^{s_j}, \quad \theta\mathfrak{P}_i = \prod_{j=0}^{d-1}\sigma_0^{-j}(\mathfrak{P}_i)^{s_j}.$$

We have $\hat{g}(0) = 1$, because $g$ is monic. Consequently $v_{\mathfrak{P}_1}(\hat{g}(\sigma)(\theta m)) \equiv a_1 \ mod \ p$ ($s_0 = 1$; the $\mathfrak{P}_i$ are totally split in $E(\xi)/k$ and lie above distinct

prime ideals of $O_k$), and then $\hat{g}(\sigma)(\theta m)$ is not a $p$th power of an element in $E(\xi)^{\times}$ ($a_1$ is coprime to $p$).

We consider the extension

$$L = E(\xi)\Big(\sqrt[p]{\hat{g}(\sigma)(\theta m)}\Big)/E(\xi)$$

of degree $p$. According to [7, Lemma 5.1.2], the Galois closure of $L/k(\xi)$ is an extension $N/k(\xi)$ with Galois group isomorphic to $\Gamma$; clearly $N$ is the compositum of the extensions $E(\xi)\Big(\sqrt[p]{\sigma^j\hat{g}(\sigma)(\theta m)}\Big)/E(\xi)$, $0 \leq j \leq m-1$, and then

$$N = E(\xi)\Big(\Big\{\sqrt[p]{\sigma^j\hat{g}(\sigma)(\theta m)}, 0 \leq j \leq m-1\Big\}\Big).$$

It is easily seen that $\sigma_0((1-\xi)^pO_{E(\xi)}) = (1-\xi)^pO_{E(\xi)} = \sigma((1-\xi)^pO_{E(\xi)})$. Therefore, from $m \equiv 1\ mod^*\ (1-\xi)^pO_{E(\xi)}$ we deduce $\theta m \equiv 1\ mod^*\ (1-\xi)^pO_{E(\xi)}$ and for $0 \leq j \leq m-1$, $\sigma^j(\theta m) \equiv 1\ mod^*\ (1-\xi)^pO_{E(\xi)}$. Thus for all $j$, $0 \leq j \leq m-1$,

$$\sigma^j\hat{g}(\sigma)(\theta m) \equiv 1\ mod^*\ (1-\xi)^pO_{E(\xi)}.$$

The extensions $E(\xi)\Big(\sqrt[p]{\sigma^j\hat{g}(\sigma)(\theta m)}\Big)/E(\xi)$, $0 \leq j \leq m-1$, are then tame by Theorem 1.4.4(i); therefore $N/E(\xi)$ is tame. Since $E(\xi)/k(\xi)$ is tame, then $N/k(\xi)$ is also tame.

We have

$$\sigma^j(L) = E(\xi)\Big(\sqrt[p]{\sigma^j\hat{g}(\sigma)(\theta m)}\Big).$$

Since $\theta(\sigma^j\hat{g}(\sigma)m) = \sigma^j\hat{g}(\sigma)(\theta m)$, it follows from Proposition 2.2.2(1) and the remark following it that there exists a unique extension $L_j/E$ cyclic of degree $p$ with $L_j \subset \sigma^j(L)$; we point out that $L_j(\xi) = \sigma^j(L)$, in particular

$$L_0(\xi) = L.$$

Let $N_0$ be the compositum of the $L_j$, $0 \leq j \leq m-1$. It is immediate that $L_j = \sigma^j(L_0)$; we deduce that $N_0/k$ is the Galois closure of $L_0/k$. We have $[N_0 : k] = mp^r$ and we check without difficulty that $N_0/k$ and $k(\xi)/k$ are linearly disjoint. We then have $[N_0k(\xi) : k] = dmp^r$. But $[N : k] = dmp^r$, so $N_0k(\xi) = N$ and $Gal(N_0/k)$ is isomorphic to $\Gamma$.

As the ideals $\theta\mathfrak{P}_i^{a_i\hat{g}(\sigma)}$, $1 \leq i \leq t$, are pairwise relatively prime (the $\mathfrak{P}_i$ are totally split in $E(\xi)/k$ and lie above distinct prime ideals of $O_k$), (2.14) and Theorem 1.4.4(i) give us:

$$\Delta(L_0(\xi)/E(\xi)) = \Big(\prod_{i=1}^{t}\mathcal{F}\big(\theta\mathfrak{P}_i^{a_i\hat{g}(\sigma)}\big)\Big)^{p-1}.$$

Put

$$\hat{g}(\sigma) = \sum_{l=0}^{m-1} b_l \sigma^l, \quad \text{where} \quad 0 \leq b_l \leq p-1.$$

We have

$$\theta \mathfrak{P}_i^{a_i \hat{g}(\sigma)} = \prod_{l=0, b_l \neq 0}^{m-1} \prod_{j=0}^{d-1} \sigma^l \sigma_0^{-j} (\mathfrak{P}_i)^{a_i s_j b_l}.$$

Since the $a_i s_j b_l$, where $b_l \neq 0$, are coprime to $p$ and the $\sigma^l \sigma_0^{-j}(\mathfrak{P}_i)$ are pairwise relatively prime

$$\mathcal{F}\big(\theta \mathfrak{P}_i^{a_i \hat{g}(\sigma)}\big) = \prod_{l=0, b_l \neq 0}^{m-1} \prod_{j=0}^{d-1} \sigma^l \sigma_0^{-j} (\mathfrak{P}_i).$$

Therefore

$$\Delta(L_0(\xi)/E(\xi)) = \Big( \prod_{i=1}^{t} \Big( \prod_{j=0}^{d-1} \sigma_0^{-j} \Big( \prod_{l=0, b_l \neq 0}^{m-1} \sigma^l \big(\mathfrak{P}_i\big) \Big) \Big) \Big)^{p-1}. \tag{2.15}$$

We point out that (2.15) is similar to (2.10).

Let $\mathfrak{q}_i = \mathfrak{P}_i \cap O_{k(\xi)}$. Using a similar argument to that in part (1) which is situated just after (2.10), we obtain

$$N_{E/k}(cl_E(O_{L_0})) = \Big( \prod_{i=1}^{t} N_{k(\xi)/k}\big(cl_{k(\xi)}(\mathfrak{q}_i)\big) \Big)^{p^{r-1}(p-1)/2}.$$

Recall that $c_2 \in Cl(k(\xi))$ is given, and $c_3$ is an element of $Cl(E(\xi))$ satisfying

$$N_{E(\xi)/k(\xi)}(c_3) = c_2, \quad c_3 = cl_{E(\xi)}(\mathfrak{P}_i), \quad c_3^t = c_3.$$

We have $N_{E(\xi)/k(\xi)}(\mathfrak{P}_i) = \mathfrak{q}_i$, whence $N_{E(\xi)/k(\xi)}(c_3) = cl_{k(\xi)}(\mathfrak{q}_i)$. Since $N_{E(\xi)/k(\xi)}(c_3) = N_{E(\xi)/k(\xi)}(c_3)^t$, we conclude that

$$cl_{k(\xi)}(\mathfrak{q}_i) = c_2 = c_2^t.$$

Consequently

$$N_{E/k}(cl_E(O_{L_0})) = N_{k(\xi)/k}(c_2)^{tp^{r-1}(p-1)/2} = N_{k(\xi)/k}(c_2)^{p^{r-1}(p-1)/2}.$$

Recall that $cl_k(O_E) = c_1$. Applying Proposition 2.2.1, we obtain

$$cl_k(O_{N_0}) = \big(cl_k(O_E)\big)^{p^r} N_{E/k}\big(cl_E(O_{L_0})\big)^m = c_1^{p^r} N_{k(\xi)/k}(c_2)^{\frac{1}{2} m p^{r-1}(p-1)}.$$

Hence we have the second inclusion (2.12), which ends the proof of the part (2).

(3) We have $m = \sum_{i=0}^{r-1} p^i \equiv r \bmod 2$. Obviously $m$ is odd because $gcd(r, p-1) = 1$. By a result of Endo (see [10, Theorem A.7]):

$$R_t(k, C) = \prod_{d|m} N_{k(\xi_d)/k}\big(Cl(k(\xi_d)\big)^{m(d-1)/2d},$$

where $d$ runs through the set of positive divisors of $m$, and $\xi_d$ is a primitive $d$th root of unity. This completes the proof of Theorem 2.1.1. □

Finally, we think (and hope) that our method to prove Theorem 2.1.1 can be adapted to treat the case $\Gamma = V \rtimes_\rho C$, where $\rho$ is faithful and irreducible and $gcd(m, [k(\xi) : k]) = 1$ (for instance $gcd(m, p-1) = 1$), here $m$ is the order of $C$ (not necessarily equal to $(p^r - 1)/(p-1)$). We will use information about the relevant codes in [7, §3], although they may not be 1-weight codes any more. We hope to return to this generalization in a future work.

# Chapitre 3

# Classes galoisiennes réalisables d'extensions non abéliennes de degré $p^3$

## 3.1 Introduction et énoncé des principaux résultats

Soit $p$ un nombre premier. Le thème de ce chapitre est l'étude de la conjecture non abélienne sur les classes galoisennes réalisables pour les groupes non abéliens d'ordre $p^3$.

Lorsque $\Gamma$ est le groupe diédral $D_4$ (resp. quaternionien) d'ordre 8 et $k$ est un corps de nombres linéairement disjoint de $\mathbb{Q}(i)$ sur $\mathbb{Q}$, où $i^2 = -1$, on montre dans [35] (resp. [32]) que si le nombre de classes (resp. le nombre de classes au sens restreint) de $k$ est impair, alors $\mathcal{R}(\mathcal{M}) = Cl^\circ(\mathcal{M})$.

Dans [6] on montre que $\mathcal{R}(O_k[D_4]) = Cl^\circ(O_k[\Gamma])$ sous l'hypothèse que l'ordre du groupe de classes de rayon de $k$ modulo $4O_k$ est impair

**Dans toute la suite : l'entier $p$ est un nombre premier impair, $\xi$ est une racine primitive $p$-ième de l'unité ; $C$ est le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ dont on se fixe un générateur $\sigma$, et $H$ est le groupe $p$-élementaire $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ dont on se fixe deux générateurs (d'ordre $p$) $\tau_0$ et $\nu_0$ :**

$$C = \langle \sigma \rangle, \quad H = \langle \tau_0, \nu_0 \rangle.$$

Pour ne pas alourdir les notations, on identifiera fréquemment des groupes isomorphes quand c'est faisable sans ambiguïté, et on indiquera l'isomorphisme si c'est nécessaire. Par exemple, si $G$ est un groupe, chaque fois qu'on indique $G \simeq C$ (resp. $H$), l'isomorphisme en question envoie le générateur

apparent de $G$ vers $\sigma$ (resp. les deux générateurs apparents de $G$ vers $\tau_0, \nu_0$).

La structure d'un groupe non abélien d'ordre $p^3$ est bien connue. On peut la définir par la présentation suivante :

$$\Gamma = \langle \eta,\ \tau,\ \nu \mid \eta^p = \tau^p = 1,\ \nu^p = \eta^q,\ \eta\tau = \tau\eta,\ \eta\nu = \nu\eta,\ \tau\nu\tau^{-1}\nu^{-1} = \eta \rangle,$$

où $q = 0$ ou bien $q = 1$. Le groupe $\Gamma$ est donc, à isomorphisme près, l'un des deux groupes suivants :

(i) Si $q = 0$, $\Gamma \simeq H \rtimes C$ ; dans ce cas $\Gamma$ est d'exposant $p$.

(ii) Si $q \neq 0$, $\Gamma \simeq (\mathbb{Z}/p^2\mathbb{Z}) \rtimes C$ ; dans ce cas $\Gamma$ est d'exposant $p^2$.

Le centre $Z(\Gamma)$ de $\Gamma$ est $\langle \eta \rangle \simeq C$ ($\eta \longmapsto \sigma$), et il est égal au groupe dérivé $[\Gamma : \Gamma]$ de $\Gamma$. On a : $\Gamma/Z(\Gamma) = \langle \tau Z(\Gamma), \nu Z(\Gamma) \rangle \simeq H$ ($\tau Z(\Gamma) \longmapsto \tau_0, \nu Z(\Gamma) \longmapsto \nu_0$) et donc

$$\Gamma = \{\tau^r \nu^s \eta^t, 0 \leq r, s, t \leq p-1\}.$$

Le point de départ du présent chapitre était la lecture des articles [3, 9] et une tentative de la détermination de $\mathcal{R}(\mathcal{M})$ lorsque $\Gamma$ est un groupe non abélien d'ordre $p^3$. Nous n'avons pas réussi la détermination de $\mathcal{R}(\mathcal{M})$ à cause de grandes difficultés provenant d'un problème de plongement (voir Proposition 3.2.6 ci-dessous) en liaison avec la donnée d'éléments de l'ensemble $\mathcal{R}(\mathcal{M}(H))$ des classes réalisables des extensions modérées à groupe de Galois $H$, où $\mathcal{M}(H)$ est le $O_k$-ordre maximal dans $k[H]$ (on pourrait consulter Proposition 3.2.2(ii) ci-dessous pour avoir une idée de tels éléments). Mais sous l'hypothèse que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes et $k(\xi_{p^2})/k(\xi)$ est non ramifiée lorsque $\Gamma$ est d'exposant $p^2$, où $\xi_{p^2}$ est une racine $p^2$-ième de l'unité, nous avons déterminé à l'aide d'un idéal de Stickelberger, pour chaque type de $\Gamma$, un sous-groupe de $Cl^\circ(\mathcal{M})$ contenu dans $\mathcal{R}(\mathcal{M})$ (voir une démarche analogue dans [29, 34]).

Le but de la suite est d'énoncer notre principal résultat.

Les caractères absolument irréductibles de $\Gamma$ sont (voir [21, Théorème 26.6, p. 302]) :

$$\begin{aligned} \chi_{u,v}, &\quad 0 \leq u \leq p-1, 0 \leq v \leq p-1, \\ \phi_u, &\quad 1 \leq u \leq p-1, \end{aligned}$$

où pour tout $(r, s, t)$ :

$$\chi_{u,v}(\tau^r \nu^s \eta^t) = \xi^{ru+sv}$$

et

$$\phi_u(\tau^r \nu^s \eta^t) = \begin{cases} p\xi^{ut} & \text{si r=s=0,} \\ 0 & \text{sinon.} \end{cases}$$

Soit $\psi_u$ le caractère de $\langle \eta, \tau \rangle$ défini par :

$$\psi_u(\eta^t) = \xi^{ut}, \psi_u(\tau) = 1.$$

Alors $\phi_u$ (de degré $p$) est induit par $\psi_u$ :

$$\phi_u = Ind^{\Gamma}_{\langle \eta,\tau \rangle}(\psi_u).$$

Notons que les $\chi_{u,v}$ sont les caractères de degré 1 de $\Gamma$ (l'abélianisé $\Gamma/[\Gamma : \Gamma] = \Gamma/Z(\Gamma) \simeq H$). Ils sont triviaux sur $Z(\Gamma)$ et par conséquent permettent de définir des caractères $\overline{\chi_{u,v}}$ sur $\Gamma/Z(\Gamma)$ ($\chi_{u,v} = Inf^{\Gamma}_{\Gamma/Z(\Gamma)}(\overline{\chi_{u,v}})$, où $Inf$ est l'inflation). En identifiant $H$ et $\Gamma/[\Gamma : \Gamma]$ les $\overline{\chi_{u,v}}$ sont les caractères absolument irréductibles de $H$ ; ils sont définis par

$$\overline{\chi_{u,v}}(\tau_0^r \nu_0^s) = \xi^{ru+sv}.$$

De même $\psi_u$ étant trivial sur $\langle \tau \rangle$, il permet de définir un caractère $\overline{\psi_u}$ de $\langle \eta, \tau \rangle / \langle \tau \rangle \simeq C$ ($\eta\langle \tau \rangle \longmapsto \sigma$) ; on a

$$\overline{\psi_u}(\eta\langle \tau \rangle) = \psi_u(\eta) = \xi^u.$$

**Supposons dorénavant $k$ linéairement disjoint de $\mathbb{Q}(\xi)$ sur $\mathbb{Q}$.** Alors on peut choisir les représentants suivants pour les classes de conjugaison sur $k$ des caractères absolument irréductibles de $\Gamma$ :

$$\chi_{0,0},\ \chi_{0,1},\ \chi_{1,1},\ \chi_{2,1},\ \ldots,\ \chi_{p-1,1},\ \chi_{1,0},\ \phi_1.$$

**Pour simplifier les notations, posons**

$$\chi_i = \chi_{i,1} \textbf{ pour tout i}, 0 \leq i \leq p-1, \textbf{ et } \chi_p = \chi_{1,0}.$$

Si $\chi$ est un caractère de $\Gamma$, $k(\chi)$ désigne l'extension de $k$ obtenue par adjonction à $k$ toutes les valeurs de $\chi$.

Il est immédiat que la décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante (Voir Chapitre 1, §1) :

$$k[\Gamma] \simeq \Big(k(\chi_{0,0}) \times \big(\prod_{i=0}^{p} k(\chi_i)\big) \times M_{n_{\phi_1}}(D_{\phi_1})\Big) \simeq k \times \big(\prod_{i=0}^{p} k(\xi)\big) \times M_{n_{\phi_1}}(D_{\phi_1}),$$

où $D_{\phi_1}$ est un corps gauche de centre $k(\phi_1) = k(\xi)$, et $M_{n_{\phi_1}}(D_{\phi_1})$ est l'anneau des matrices carrées d'ordre $n_{\phi_1}$ à coefficients dans $D_{\phi_1}$ ($n_{\phi_1} = \phi_1(1)/s_0$, où $s_0$ est l'indice de Schur relatif à $k$).

Soit $\mathcal{M}$ un $O_k$-ordre maximal de $k[\Gamma]$ contenant $O_k[\Gamma]$. Comme $\Gamma$ est d'ordre impair, les caractères irréductibles de $\Gamma$ ne sont pas symplectiques. Donc, d'une part $k[\Gamma]$ vérifie la condition d'Eichler. D'autre part, le théorème 1.1.2 de Swan nous donne :

$$Cl(\mathcal{M}) \simeq Cl(k) \times \big(\prod_{i=0}^{p} Cl(k(\xi))\big) \times Cl(k(\xi)).$$

D'où :

$$Cl^{\circ}(\mathcal{M}) \simeq \prod_{i=0}^{p+1} Cl(k(\xi)).$$

Nous identifierons fréquemment $Cl^{\circ}(\mathcal{M})$ avec $\prod_{i=0}^{p+1} Cl(k(\xi))$ sous l'isomorphisme précédent.

Soit

$$S = Gal(k(\xi)/k) = \{s_i \mid \ 1 \leq i \leq p-1\}, \text{où} \ \ s_i(\xi) = \xi^i.$$

Soit l'élément de Stickelberger

$$\theta = \sum_{i=1}^{p-1} i s_i^{-1},$$

et soit l'idéal de Stickelberger

$$\mathcal{S} = \frac{1}{p}\theta\mathbb{Z}[S] \cap \mathbb{Z}[S].$$

Dans toute la suite, les éléments de $\mathcal{S}$ sont appelés éléments de Stickelberger.

L'action naturelle de $S$ sur les idéaux fractionnaires de $k(\xi)$ induit une structure de $\mathbb{Z}[S]$-module sur $Cl(k(\xi))$. On note $\mathcal{S}Cl(k(\xi))$ le sous-groupe de $Cl(k(\xi))$ engendré par les éléments de la forme $\mathfrak{s}c$, où $\mathfrak{s} \in \mathcal{S}$ et $c \in Cl(k(\xi))$.

Si $K/k'$ est une extension finie de corps de nombres, on note $\phi_{K/k'}$ le morphisme de $Cl(k')$ à valeurs dans $Cl(K)$ qui à la classe d'un idéal fractionnaire $I$ de $O_{k'}$ associe la classe de l'idéal étendu $IO_K$ dans $Cl(K)$.

Dans la section 3, on démontre le théorème suivant :

**Théorème 3.1.1.** *Soient $k$ un corps de nombres, $p$ un nombre premier impair et $\xi$ (resp. $\xi_{p^2}$) une racine primitive $p$-ième (resp. $p^2$-ième) de l'unité. Soit $\Gamma$ un groupe non abélien d'ordre $p^3$. Supposons les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ linéairement disjointes. Identifions $Cl^{\circ}(\mathcal{M})$ et $\prod_{i=0}^{p+1} Cl(k(\xi))$.*

*Si l'exposant de* $\Gamma$ *est* $p$*, soit*

$$A_p = \Big\{ \Big( c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p, \\ x^p \phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big) \Big| (c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3 \Big\}.$$

*Si l'exposant de* $\Gamma$ *est* $p^2$*, soit*

$$A_{p^2} = \Big\{ \Big( c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p, \\ x^p ((s_{p-1} - \theta) c_0) \phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big) \Big| (c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3 \Big\}.$$

*Si* $\Gamma$ *est d'exposant* $p$ *(resp. d'exposant* $p^2$ *et* $k(\xi_{p^2})/k(\xi)$ *non ramifiée), alors* $A_p$ *(resp.* $A_{p^2}$*) est un sous-groupe de* $Cl^\circ(\mathcal{M})$ *contenu dans l'ensemble des classes réalisables* $\mathcal{R}(\mathcal{M})$*.*

**Remarque.** Lorsque $\Gamma$ est d'exposant $p^2$, l'hypothèse $k(\xi_{p^2})/k(\xi)$ non ramifiée provient de l'utilisation d'une idée de la preuve du [2, Théorème 1.1] dans une partie de la démonstration de notre théorème 3.1.1 (on pourrait voir [2, §4] pour des exemples d'extensions $k(\xi_{p^2})/k(\xi)$ non ramifiées).

Notons par $R_m(k, \Gamma, A_p)$ (resp. $R_m(k, \Gamma, A_{p^2})$) l'ensemble des classes de Steinitz des extensions $N/k$ modérées à groupe de Galois $\Gamma$ d'exposant $p$ (resp. $p^2$) et telles que $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ appartient à $A_p$ (resp. $A_{p^2}$).

Nous verrons dans la section 3 au cours de la démonstration du théorème 3.1.1, sous-forme de deux remarques, qu'on a la proposition suivante comme application du théorème 3.1.1 :

**Proposition 3.1.2.** *Sous les hypothèses du théorème 3.1.1 et les notations précédentes, si* $\Gamma$ *est d'exposant* $p$*, alors*

$$R_m(k, \Gamma, A_p) = R_m(k, \Gamma) = N_{k(\xi)/k}(Cl(k(\xi)))^{p^2(p-1)/2},$$

*et si* $\Gamma$ *est d'exposant* $p^2$*, alors*

$$R_m(k, \Gamma, A_{p^2}) = R_m(k, \Gamma) = N_{k(\xi)/k}(Cl(k(\xi)))^{p(p-1)/2}.$$

**Remarques.** (1) Les deux égalités qui donnent la description explicite de $R_m(k,\Gamma)$ pour chaque type de $\Gamma$ dans la proposition précédente proviennent de [2, Théorème 1.1].

(2) Le fait qu'on peut atteindre $R_m(k,\Gamma)$ par $A_p$ et $A_{p^2}$ nous dit que peut-être nous ne sommes pas très loin de la détermination de $\mathcal{R}(\mathcal{M})$.

Nous terminons cette section par quelques remarques.

Le travail de ce chapitre est une suite naturelle de [2] vu le lien étroit -bien connu- entre les classes de Steinitz et celles galoisiennes. Son principal intérêt est de constituer une première étape pour comprendre le problème des classes galoisiennes réalisables pour les $p$-groupes, $p$ impair. Pour démontrer le principal résultat nous avons utilisé les théories du corps de classes et de Kummer, et des résultats connus de A. Fröhlich et d'un problème de plongement ; cette méthode est une variation de celle utilisée dans des travaux de B. Sodaïgui, mais ici la résolution du problème de plongement en lien avec des classes galoisiennes est nettement plus difficile. En ce qui concerne les perspectives : nous pensons posséder les principaux outils pour espérer dans un futur travail déterminer $\mathcal{R}(\mathcal{M})$ pour les groupes d'ordre $p^3$ sans aucune hypothèse sur le corps de base. Sachant que $\mathcal{R}(\mathcal{M})$ est une bonne approximation de $\mathcal{R}(O_k[\Gamma])$ (voir [5, 6]), nous espérons ensuite déterminer ce dernier (à ce moment nous comparerons notre résultat avec celui de L.R. McCulloh dans le cas non abélien) et généraliser les résultats pour les $p$-groupes. Cette généralisation utilisera en partie une adaptation de la méthode de I.R. Shafarevich concernant la résolution du problème inverse de la théorie de Galois pour les groupes résolubles, et le théorème de Brauer qui permet d'écrire un caractère irréductible de $\Gamma$ comme combinaison linéaire à coefficients dans $\mathbb{Z}$ de caractères induits par des caractères de sous-groupes abéliens de $\Gamma$.

## 3.2 Préliminaires

Le but de cette section est d'établir ou rappeler quelques propositions en vue de la démonstration des principaux résultats de ce chapitre.

**Désormais $N/k$ désigne une extension modérément ramifiée à groupe de Galois isomorphe à $\Gamma$, où $k$ et $\Gamma$ vérifient les hypothèses du théorème 3.1.1 : $k \cap \mathbb{Q}(\xi) = \mathbb{Q}$, $\Gamma$ est un groupe non abélien d'ordre $p^3$ et $p$ est un nombre premier impair.**

**Nous identifions $Gal(N/k)$ et $\Gamma$, et nous notons par $K$, $M$, $E$, $F$ les sous-corps de $N$ fixes respectivement par $Z(\Gamma) = \langle\eta\rangle$, $\langle\tau\rangle$, $\langle\eta,\tau\rangle$, $\langle\eta,\nu\rangle$.** Immédiatement on a : les extensions $N/E$, $K/k$, $M/E$, $E/k$ et $F/k$

sont galoisiennes de groupes de Galois respectifs

$$Gal(N/E) = \langle \eta, \tau \rangle, \quad Gal(K/k) = \langle \tau|_K, \nu|_K \rangle \simeq H,$$

$$Gal(M/E) = \langle \eta|_M \rangle \simeq \langle \eta \rangle \simeq C,$$

$$Gal(E/k) = \langle \nu|_E \rangle \simeq C, \; Gal(F/k) = \langle \tau|_F \rangle \simeq \langle \tau \rangle \simeq C,$$

où $|_L$ désigne la restriction à $L$ lorsque $L$ est un corps de nombres, et les isomorphismes entre un groupe $G$ (ci-dessus) et $H$, ou $G$ et $C$, envoient les générateurs apparents de $G$ vers ceux de $H$, ou $C$. De plus la composée $E(F)/k$ est égale à $K/k$ et la composée $K(M)/k$ est égale à $N/k$.

Soit $L/k$ une sous-extension de $N/k$. Les extensions $L/k$ et $k(\xi)/k$ sont linéairement disjointes, car $[L : k]$ divise $p^3$ et $[k(\xi) : k] = p-1$, et $p^3$ et $p-1$ sont premiers entre eux. On en déduit en particulier :

$$Gal(N(\xi)/k) \simeq Gal(N/k) \times Gal(k(\xi)/k).$$

Les extensions $L/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont elles aussi linéairement disjointes, car $L \cap \mathbb{Q}(\xi) \subset L \cap k(\xi) = k$ et $k \cap \mathbb{Q}(\xi) = \mathbb{Q}$.

On a les isomorphismes de restriction :

$$Gal(N(\xi)/N) \simeq Gal(L(\xi)/L) \simeq Gal(k(\xi)/k) = S,$$

$$Gal(N(\xi)/k(\xi)) \simeq Gal(N/k) = \Gamma.$$

Dans la suite, pour simplifier les notations, nous noterons de la même façon, quand il n' y a aucune confusion possible, un élément de $Gal(N(\xi)/k)$ et sa restriction à une sous-extension de $N(\xi)/k$.

Soit $a$ une base du $k[\Gamma]$-module $N$. Pour tout idéal premier $\mathfrak{p}$ de $O_k$, soit $\alpha_\mathfrak{p}$ une base du $O_{k,\mathfrak{p}}[\Gamma]$-module $O_{N,\mathfrak{p}}$. Soient $b$ et $b_\mathfrak{p}$ des bases respectives du $E[\langle \eta, \tau \rangle]$-module $N$ et du $O_{E,\mathfrak{p}}[\langle \eta, \tau \rangle]$-module $O_{N,\mathfrak{p}}$.

Soit $S_0$ un système de représentants des classes d'équivalence des éléments de $Gal(\overline{\mathbb{Q}}/k)$ modulo $Gal(\overline{\mathbb{Q}}/E)$. Comme $E/k$ et $k(\xi)/k$ sont linéairement disjointes, on peut choisir un prolongement $\overline{\nu}$ de $\nu$ à $\overline{\mathbb{Q}}$ vérifiant $\overline{\nu}(\xi) = \xi$. Il est clair qu'on peut supposer $S_0 = \{\overline{\nu}^i, 0 \leq i \leq (p-1)\}$ ($Gal(E/k)$ est engendré par la restriction de $\nu$ à $E$).

Puisque $\psi_1$ est trivial sur $\langle \tau \rangle$, il permet de définir un caractère $\overline{\psi_1}$ de $Gal(M/E) = \langle \eta|_M \rangle \simeq \langle \eta, \tau \rangle / \langle \tau \rangle \simeq C$ ; en fait on a

$$\overline{\psi_1}(\eta|_M) = \psi_1(\eta) = \xi.$$

Une démonstration similaire à celle de la proposition 4.1 dans [4, pp. 22–23] et la proposition 2.1 dans [29, p. 1824] nous donne :

**Proposition 3.2.1.** *Sous les hypothèses et notations ci-dessus, un représentant de la classe de* $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ *dans* $Cl(\mathcal{M})$ *est l'élément* $f$ *de* $Hom_{\Omega_k}(R_\Gamma, J(\overline{k}))$ *défini par :*

$$f(\chi_{0,0}) = (1),$$

$$f(\chi_i) = \left( \frac{\langle Tr_{N_\mathfrak{p}/K_\mathfrak{p}}(\alpha_\mathfrak{p}), \overline{\chi_i} \rangle_{K/k}}{\langle Tr_{N/K}(a), \overline{\chi_i} \rangle_{K/k}} \right)_\mathfrak{p}, \quad \textit{pour tout } i, 0 \leq i \leq p,$$

$$f(\phi_1) = \left( \frac{e(E_\mathfrak{p}/k_\mathfrak{p})}{e(E/k)} \prod_{i=0}^{p-1} \overline{\nu}^i \left( \frac{\langle Tr_{N_\mathfrak{p}/M_\mathfrak{p}}(b_\mathfrak{p}), \overline{\psi_1} \rangle_{M/E}}{\langle Tr_{N/M}(b), \overline{\psi_1} \rangle_{M/E}} \right) \right)_\mathfrak{p},$$

*où* $e(E/k)^2$ *est le discriminant d'une base du* $k$*-espace vectoriel* $E$ *et* $e(E_\mathfrak{p}/k_\mathfrak{p})^2 O_{k,\mathfrak{p}}$ *est le discriminant de* $E_\mathfrak{p}/k_\mathfrak{p}$.

Comme $\mathbb{Q}(\xi)$ est linéairement disjoint de $k$ sur $\mathbb{Q}$, il est immédiat qu'on peut choisir les représentants suivants pour les classes de conjugaison sur $k$ des caractères absolument irréductibles de $H$ :

$$\overline{\chi_{0,0}},\ \overline{\chi_i},\ 0 \leq i \leq p.$$

La décomposition de Wedderburn de l'algèbre semi-simple $k[H]$ en un produit d'algèbres simples est la suivante :

$$k[H] \simeq \left( k(\overline{\chi_{0,0}}) \times \prod_{i=0}^{p} k(\overline{\chi_i}) \right) = k \times \prod_{i=0}^{p} k(\xi)$$

Soit $\mathcal{M}(H)$ le $O_k$-ordre maximal dans $k[H]$. Comme $H$ est abélien :

$$Cl(\mathcal{M}(H)) \simeq Cl(k) \times \prod_{i=0}^{p} Cl(k(\xi)),$$

et donc

$$Cl^\circ(\mathcal{M}(H)) \simeq \prod_{i=0}^{p} Cl(k(\xi)).$$

Soit $\mathcal{R}(\mathcal{M}(H))$ l'ensemble des classes réalisables par les anneaux d'entiers des extensions galoisiennes et modérées de $k$, dont le groupe de Galois est isomorphe à $H$. D'après [24], $\mathcal{R}(\mathcal{M}(H))$ est un sous-groupe de $Cl^\circ(\mathcal{M}(H))$ qu'on peut décrire par une correspondance de Stickelberger ; on l'identifiera souvent avec un sous-groupe de $\prod_{i=0}^{p} Cl(k(\xi))$.

**Pour toute la suite de ce chapitre, on désigne par** $\chi$ **le caractère de** $C = \langle \sigma \rangle$ **défini par** $\chi(\sigma) = \xi$**.**

Puisque $k/\mathbb{Q}$ (resp. $E/\mathbb{Q}$) et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes, les caractères absolument irréductibles de $C$ donnent deux classes de conjugaison

sur $k$ (resp. $E$) ; pour ces dernières on choisit comme représentants le caractère trivial de $C$ et $\chi$.

Les décompositions de Wedderburn des algèbres semi-simples $k[C]$ et $E[C]$ en un produit d'algèbres simples sont donc :

$$k[C] \simeq k \times k(\xi),\ E[C] \simeq E \times E(\xi).$$

Soit $\mathcal{M}(C)$ (resp. $\mathcal{M}_E(C)$) le $O_k$(resp. $O_E$)-ordre maximal dans $k[C]$ (resp. $E[C]$). Puisque $C$ est abélien,

$$Cl(\mathcal{M}(C)) \simeq Cl(k) \times Cl(k(\xi)),\ Cl(\mathcal{M}_E(C)) \simeq Cl(E) \times Cl(E(\xi)).$$

Par conséquent :

$$Cl^\circ(\mathcal{M}(C)) \simeq Cl(k(\xi)),\ Cl^\circ(\mathcal{M}_E(C)) \simeq Cl(E(\xi)).$$

Soit $\mathcal{R}(\mathcal{M}(C))$ (resp. $\mathcal{R}(\mathcal{M}_E(C))$) l'ensemble des classes réalisables par les anneaux d'entiers des extensions galoisiennes et modérées de $k$ (resp. $E$), dont le groupe de Galois est isomorphe à $C$. En identifiant $Cl^\circ(\mathcal{M}(C))$ (resp. $Cl^\circ(\mathcal{M}_E(C))$) et $Cl(k(\xi))$ (resp. $Cl(E(\xi))$) sous les isomorphismes précédents, le théorème 2.4 de [31] nous donne (attention : $\mathcal{R}(\mathcal{M}(C))$ est noté $\mathcal{R}(O_k[C])$ dans [31]) :

$$\mathcal{R}(\mathcal{M}(C)) = \mathcal{S}Cl(k(\xi)),\ \mathcal{R}(\mathcal{M}_E(C)) = \mathcal{S}Cl(E(\xi)).$$

L'extension $K/k$ (de groupe de Galois $H$) admet $p+1$ sous-extensions $K_i/k$, $0 \leq i \leq p$.

**Posons $K_0 = E$, $K_p = F$. Pour tout $i$, $1 \leq i \leq p-1$, $K_i$ désigne le sous-corps de $K$ fixe par le sous-groupe** $\langle (\tau^{-i^*}\nu)|_K \rangle$ de $Gal(K/k)$, où $i^*$ est un représentant de l'inverse de $i$ modulo $p$. Signalons que $K_0$ est fixe par $\langle \tau|_K \rangle$ et $K_p$ est fixe par $\langle \nu|_K \rangle$.

**Proposition 3.2.2.** *Soient $c_i$, $-1 \leq i \leq p+1$, les composantes de $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $Cl(k) \times (\prod_{i=0}^p Cl(k(\xi))) \times Cl(k(\xi)(\simeq Cl(\mathcal{M}))$. Sous les notations précédentes on a :*

*(i) $c_{-1}$ est la classe triviale dans $Cl(k)$.*

*(ii) $(c_0, c_1, \ldots, c_p)$ est la classe de $[\mathcal{M}(H) \otimes_{O_k[H]} O_K]$ dans $\prod_{i=0}^p Cl(k(\xi))$ et pour tout $i$, $0 \leq i \leq p$, $c_i = [\mathcal{M}(C) \otimes_{O_k[C]} O_{K_i}]$ dans $\mathcal{S}Cl(k(\xi))$.*

*(iii) $c_{p+1} = \phi_{k(\xi)/k}(cl_k(O_E))N_{E(\xi)/k(\xi)}([\mathcal{M}_E(C) \otimes_{O_E[C]} O_M])$ dans $Cl(k(\xi))$.*

*Démonstration.* $(i)$ C'est évident.

$(ii)$ Il est clair que l'élément $f_1$ de $Hom_{\Omega_k}(R_H, J(\overline{k}))$, qui au caractère trivial associe 1, et à $\overline{\chi_i}$, $0 \leq i \leq p$ associe $f_1(\overline{\chi_i}) = f(\chi_i)$ est un représentant de $[\mathcal{M}(H) \otimes_{O_k[H]} O_K]$ dans la Hom-description de $Cl(\mathcal{M}(H))$. On en déduit que les composantes de $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $\prod_{i=0}^{p} Cl(k(\xi))$ sont égales à celles de $[\mathcal{M}(H) \otimes_{O_k[H]} O_K]$ dans $\prod_{i=0}^{p} Cl(k(\xi))$.

Les caractères $\overline{\chi_0}$, $\overline{\chi_p}$, $\overline{\chi_i}$, $1 \leq i \leq p-1$, sont respectivement triviaux sur $\langle \tau|_K \rangle$, $\langle \nu|_K \rangle$, $\langle (\tau^{-i^*}\nu)|_K \rangle$. Ils permettent donc de définir des caractères (non triviaux d'ordre $p$) $\overline{\overline{\chi_0}}$, $\overline{\overline{\chi_p}}$, $\overline{\overline{\chi_i}}$ sur $Gal(K_0/k) = \langle \nu|_{K_0} \rangle \simeq C$, $Gal(K_p/k) = \langle \tau|_{K_p} \rangle \simeq C$, $Gal(K_i/k) = \langle \nu|_{K_i} \rangle \simeq C$, respectivement.

Explicitement, si pour chaque $i$, $0 \leq i \leq p$, on note $g_i$ le générateur ci-dessus de $Gal(K_i/k)$, et $\pi_i$ l' isomorphisme $Gal(K_i/k) \simeq C$, on a :

$$\overline{\overline{\chi_i}}(g_i) = \xi, \quad \pi_i(g_i) = \sigma.$$

D'où pour tout $i$, $0 \leq i \leq p$,

$$\overline{\overline{\chi_i}} = \chi \circ \pi_i.$$

Pour tout $i$, $0 \leq i \leq p$, on a les égalités suivantes (elles découlent de la définition des résolvantes de Fröhlich-Lagrange) :

$$\langle Tr_{N_\mathfrak{p}/K_\mathfrak{p}}(\alpha_\mathfrak{p}), \overline{\chi_i} \rangle_{K/k} = \langle Tr_{N_\mathfrak{p}/(K_i)_\mathfrak{p}}(\alpha_\mathfrak{p}), \overline{\overline{\chi_i}} \rangle_{K_i/k},$$

$$\langle Tr_{N/K}(a), \overline{\chi_i} \rangle_{K/k} = \langle Tr_{N/K_i}(a), \overline{\overline{\chi_i}} \rangle_{K_i/k}.$$

Par conséquent, pour tout $i$, $0 \leq i \leq p$,

$$\begin{aligned} f_1(\overline{\chi_i}) &= \left( \langle Tr_{N_\mathfrak{p}/(K_i)_\mathfrak{p}}(\alpha_\mathfrak{p}), \overline{\overline{\chi_i}} \rangle_{K_i/k} / \langle Tr_{N/K_i}(a), \overline{\overline{\chi_i}} \rangle_{K_i/k} \right)_\mathfrak{p} \\ &= \left( \langle Tr_{N_\mathfrak{p}/(K_i)_\mathfrak{p}}(\alpha_\mathfrak{p}), \chi \circ \pi_i \rangle_{K_i/k} / \langle Tr_{N/K_i}(a), \chi \circ \pi_i \rangle_{K_i/k} \right)_\mathfrak{p}, \end{aligned}$$

où $Tr_{N_\mathfrak{p}/(K_i)_\mathfrak{p}}(\alpha_\mathfrak{p})$ et $Tr_{N/K_i}(a)$ sont des bases respectives du $O_{k,\mathfrak{p}}[C]$-module $O_{K_i,\mathfrak{p}}$ et du $k[C]$-module $K_i$.

Il est maintenant clair que, pour chaque $i$, $0 \leq i \leq p$, l'élément $f_{1,i}$ de $Hom_{\Omega_k}(R_C, J(\overline{k}))$, qui au caractère trivial associe 1, et à $\chi$ associe $f_{1,i}(\chi) = f_1(\overline{\chi_i})$ est un représentant de $[\mathcal{M}(C) \otimes_{O_k[C]} O_{K_i}]$ $(= [\mathcal{M}(C) \otimes_{O_k[C]} O_{K_i,\pi_i}])$ dans la Hom-description de $Cl(\mathcal{M}(C))$. On en déduit que $c_i = [\mathcal{M}(C) \otimes_{O_k[C]} O_{K_i}]$ dans $Cl(k(\xi))$.

$(iii)$ La preuve consiste en la détermination de la classe du contenu de l'idèle suivant, lequel est défini dans la proposition 3.2.1 :

$$f(\phi_1) = \left( \frac{e(E_\mathfrak{p}/k_\mathfrak{p})}{e(E/k)} \prod_{i=0}^{p-1} \overline{\nu}^i \left( \frac{\langle Tr_{N_\mathfrak{p}/M_\mathfrak{p}}(b_\mathfrak{p}), \overline{\psi_1} \rangle_{M/E}}{\langle Tr_{N/M}(b), \overline{\psi_1} \rangle_{M/E}} \right) \right)_\mathfrak{p}.$$

Soit $\pi_{p+1}$ l'isomoprphisme de $Gal(M/E) = \langle \eta|_M \rangle$ dans $C$ défini par $\pi_{p+1}(\eta|_M) = \sigma$. Comme $\overline{\psi_1}(\eta|_M) = \xi$, on a

$$\overline{\psi_1} = \chi \circ \pi_{p+1}.$$

Comme ci-dessus à la fin de $(ii)$, la classe dans $Cl(E(\xi))$ du contenu de l'idèle

$$\left(\langle Tr_{N_{\mathfrak{p}}/M_{\mathfrak{p}}}(b_{\mathfrak{p}}), \overline{\psi_1} = \chi \circ \pi_{p+1}\rangle_{M/E} / \langle Tr_{N/M}(b), \overline{\psi_1} = \chi \circ \pi_{p+1}\rangle_{M/E}\right)_{\mathfrak{p}}$$

est la classe $[\mathcal{M}_E(C) \otimes_{O_E[C]} O_M]$ $(= [\mathcal{M}_E(C) \otimes_{O_E[C]} O_{M,\pi_{p+1}}])$ dans $Cl(E(\xi))$.

Puisque $Gal(E(\xi)/k(\xi)) = \langle \overline{\nu}|_{E(\xi)} \rangle$, on a :

$$\prod_{i=0}^{p-1} \overline{\nu}^i([\mathcal{M}_E(C) \otimes_{O_E[C]} O_M]) = N_{E(\xi)/k(\xi)}([\mathcal{M}_E(C) \otimes_{O_E[C]} O_M]).$$

Soit $I$ l'idéal fractionnaire de $k$ qui est le contenu de l'idèle $(e((E)_{\mathfrak{p}}/k_{\mathfrak{p}})/e(E/k))_{\mathfrak{p}}$. Un raisonnement similaire à celui de la fin de la preuve de la proposition 4.2$(iii)$ dans [4, p. 24] nous donne : $cl(I) = cl_k(O_E)$. Ceci permet d'achever la démonstration de $(iii)$. □

**Proposition 3.2.3.** *Sous les hypothèses et notations de la proposition 3.2.2, avec le rappel* $c_0 = [\mathcal{M}(C) \otimes_{O_k[C]} O_E]$ *et* $c_p = [\mathcal{M}(C) \otimes_{O_k[C]} O_F]$, *on a :*

*(1)* $cl_k(O_E) = N_{k(\xi)/k}(c_0)$.

*(2) Si* $E/k$ *et* $F/k$ *sont arithmétiquement disjointes, alors pour tout* $i$, $1 \leq i \leq p-1$, $c_i = c_0 s_i(c_p)$.

*Démonstration.* Dans la démonstration de la proposition 3.2.2 on a défini $\overline{\overline{\chi_i}}$ pour tout $i$, $0 \leq i \leq p$ $(\overline{\chi_i} = Inf^H_{Gal(K_i/k)}(\overline{\overline{\chi_i}}))$. Pour simplifier les notations, posons

$$\overline{\overline{\chi_i}} = \varphi_i$$

de sorte que

$$\varphi_i = \chi \circ \pi_i.$$

Comme $c_0 = [\mathcal{M}(C) \otimes_{O_k[C]} O_E]$, et en raisonnant comme dans le début de la partie (1) de la preuve du théorème 1.1 dans [4, p. 25] (on utilise le caractère de la représentation régulière de $C$) on obtient :

$$cl_k(O_E) = N_{k(\varphi_0)/k}(c_0)^{\varphi_0(1)} = N_{k(\xi)/k}(c_0).$$

Nous adaptons maintenant la démonstration de [31, Lemmes 3.1 et 3.2] à notre situation tout en précisant quelques détails pour la convenance du lecteur.

Soient $a_E$ et $a_F$ des bases normales respectives de $E/k$ et $F/k$. De $E/k$ et $F/k$ linéairement disjointes on déduit sans peine : pour tout $i$, $1 \leq i \leq p-1$,

$$\langle Tr_{K/K_i}(a_E a_F), \varphi_i \rangle_{K_i/k} = \langle a_E, \varphi_0 \rangle_{E/k} \langle a_F, \varphi_p^i \rangle_{F/k}.$$

Il est immédiat que $a_E a_F$ est une base normale de $K/k$, et donc $Tr_{K/K_i}(a_E a_F)$, qu'on note $a_{K_i}$, en est une de $K_i/k$ pour chaque $i$, $1 \leq i \leq p-1$.

Puisque $Gal(E/k)$, $Gal(F/k)$ et $Gal(K_i/k)$ sont isomorphes à $C$ et les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes, le théorème 2.2 (1) de [31] nous donne les décompositions de façon unique (i.e, **les $p$-décompositions uniques**, voir Chapitre 1, §4, (1,1)) suivantes :

$$\langle a_E, \varphi_0 \rangle_{E/k}^p O_{k(\xi)} = (I(\varphi_0))^p \theta J(\varphi_0),$$

$$\langle a_F, \varphi_p \rangle_{F/k}^p O_{k(\xi)} = (I(\varphi_p))^p \theta J(\varphi_p),$$

$$\langle a_{K_i}, \varphi_i \rangle_{K_i/k}^p O_{k(\xi)} = (I(\varphi_i))^p \theta J(\varphi_i), \quad \text{pour tout } i, 1 \leq i \leq p-1.$$

où $I(\varphi_0)$, $I(\varphi_p))$ et $I(\varphi_i)$ sont des idéaux fractionnaires de $k(\xi)$, et les $s_j(J(\varphi_0))$ (resp. $s_j(J(\varphi_p))$, resp. $s_j(J(\varphi_i))$) , $1 \leq j \leq (p-1)$, sont des idéaux entiers de $O_{k(\xi)}$, sans facteur carré et premiers entre eux deux à deux.

Un calcul simple donne : $s_i(\langle a_F, \varphi_p \rangle_{F/k}) = \langle a_F, \varphi_p^i \rangle_{F/k}$, d'où

$$\langle a_F, \varphi_p^i \rangle_{F/k}^p O_{k(\xi)} = (s_i(I(\varphi_p)))^p \theta s_i(J(\varphi_p)).$$

Par conséquent

$$\langle a_{K_i}, \varphi_i \rangle_{K_i/k}^p O_{k(\xi)} = (I(\varphi_0) s_i(I(\varphi_p)))^p \theta\big(J(\varphi_0) s_i(J(\varphi_p))\big).$$

Notons $J_0$ le PGCD de $J(\varphi_0)$ et $s_i(J(\varphi_p))$.

Soient

$$J_1 = J(\varphi_0) s_i(J(\varphi_p)) J_0^{-2} s_2(J_0)$$

et $\theta_1$ l'élément de Stickelberger (voir Proposition 3.2.7)

$$\theta_1 = \frac{1}{p}(2 - s_2)\theta.$$

On a

$$\theta\big(J(\varphi_0) s_i(J(\varphi_p))\big) = (\theta_1 J_0)^p \theta J_1.$$

On en déduit la décomposition de façon unique :

$$\langle a_{K_i}, \varphi_i \rangle_{K_i/k}^p O_{k(\xi)} = (I(\varphi_0) s_i(I(\varphi_p)) \theta_1 J_0)^p \theta J_1.$$

Comme pour tout $i$, $0 \leq i \leq p$, $\varphi_i = \chi \circ \pi_i$, le théorème 2.3 (1) de [31] nous donne :

$$c_0 = cl(I(\varphi_0))^{-1}, c_p = cl(I(\varphi_p))^{-1}; c_i = cl(I(\varphi_0)s_i(I(\varphi_p))\theta_1 J_0)^{-1}, 1 \leq i \leq p-1.$$

Par conséquent, pour tout $i$, $1 \leq i \leq p-1$,

$$c_i = c_0 s_i(c_p) cl(\theta_1 J_0)^{-1}.$$

Supposons maintenant $E/k$ et $F/k$ arithmétiquement disjointes. D'après le théorème 2.2 (2) de [31] (ou par le théorème 1.4.4), $J_0 = O_{k(\xi)}$. Donc $c_i = c_0 s_i(c_p)$. □

**Soit $a \in k(\xi)$ tel que $a$ n'est pas une puissance $p$-ième dans $k(\xi)$. On considère l'extension de Kummer $E' = k(\xi)(\alpha)/k(\xi)$, où $\alpha$ est un élément de $\overline{k}$ (une clôture algébrique de $k$) vérifiant $\alpha^p = a$.**

**Proposition 3.2.4.** *L'extension $E'/k$ est galoisienne abélienne si, et seulement si, il existe $a' \in k(\xi)^\times$ tel que $E' = k(\xi)((\theta a')^{1/p})$.*

*Démonstration.* Cette proposition est la partie (1) de la proposition 2.2.2 dans le cas de la remarque qui la précède. □

Supposons $E'/k$ galoisienne abélienne. Comme elle est de degré $p(p-1)$ elle admet une sous-extension $E''/k$ cyclique de degré $p$. Puisque $p$ et $p-1$ sont premiers entre eux, les extensions $E''/k$ et $k(\xi)/k$ sont linéairement disjointes. On en déduit que $E' = E''(\xi)$ et $Gal(E''/k) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/p(p-1)\mathbb{Z}$. Donc $E'/k$ est cyclique et $E''/k$ est unique.

Identifions $C$ avec $Gal(E'/k(\xi))$ en faisant agir $\sigma$ sur $E'$ de sorte que $\sigma(\alpha) = \xi\alpha$. Puisque $Gal(E'/k(\xi))$ est isomorphe (par restriction) à $Gal(E''/k)$, on identifie aussi $C$ et $Gal(E''/k)$.

**Proposition 3.2.5.** *Supposons $E'/k$ abélienne et posons $\alpha' = (1/p)Tr_{E'/E''}(\alpha)$. Alors $\langle \alpha', \chi \rangle_{E''/k} = \alpha$.*

*Démonstration.* Nous identifions $S$ et $Gal(E'/E'')$ grâce à l'isomorphisme de restriction $Gal(E'/E'') \simeq Gal(k(\xi)/k)$. On a

$$\begin{aligned}\langle \alpha', \chi \rangle_{E''/k} &= (1/p)\sum_{i=0}^{p-1} Tr_{E'/E''}(\sigma^i(\alpha))\chi(\sigma^{-i}) = (1/p)\sum_{i=0}^{p-1} Tr_{E'/E''}(\xi^i\alpha)\xi^{-i} \\ &= (1/p)\sum_{i=0}^{p-1}\sum_{j=1}^{p-1}(\xi^{i(j-1)}s_j(\alpha)) = (1/p)\sum_{j=1}^{p-1}\Big(\sum_{i=0}^{p-1}\xi^{i(j-1)}\Big)s_j(\alpha).\end{aligned}$$

Si $j \neq 1$, alors $\sum_{i=0}^{p-1}\xi^{i(j-1)} = 0$ ; sinon $\sum_{i=0}^{p-1}\xi^{i(j-1)} = p$. D'où la proposition. □

Nous finissons ce paragraphe par rappeler des résultats bien connus qui seront utiles pour la démonstration de notre théorème 3.1.1.

**Maintenant $E'/k$ n'est pas nécessairement galoisienne (on revient à la situation générale).**

On note $\rho$ un générateur du groupe $Gal(E'/k(\xi))$. L'anneau de groupe $\mathbb{Z}[<\rho>]$ agit sur $(E')^\times$ d'une façon naturelle.

On choisit la notation exponentielle pour cette action :

$$\forall\ x \in (E')^\times, \forall\ r(\rho) = \sum_{i=0}^{p-1} a_i \rho^i \in \mathbb{Z}[<\rho>],\ x^{r(\rho)} = \prod_{i=0}^{p-1} \rho^i(x)^{a_i}.$$

On pose

$$\mathfrak{N} = \sum_{i=0}^{p-1} \rho^i, \quad \hat{\theta} = \sum_{i=0}^{p-1} i\rho^i.$$

La proposition suivante (voir [9, Théorèmes 4 et 6, et la remarque suivant Théorème 6], ou [2, Théorème 2.5]) donne un critère de plongement de l'extension $E'/k(\xi)$ dans une extension $N'/k(\xi)$ galoisienne, non abélienne et de degré $p^3$.

**Proposition 3.2.6.** *Sous les notations précédentes, on a :*

*(1) Pour que $E'/k(\xi)$ soit plongeable dans une extension galoisienne $N'/k(\xi)$ à groupe de Galois $\Gamma$ d'exposant $p$, il faut et il suffit qu'il existe $e \in (E')^\times$ et $\kappa \in k(\xi)^\times$ tels que les classes de $b = e^{-\mathfrak{N}}$ et $c = \kappa e^{\hat{\theta}}$ dans $(E')^\times/(E')^{\times p}$ soient non triviales et engendrent deux sous-groupes distincts de $(E')^\times/(E')^{\times p}$.*

*(2) Pour que $E'/k(\xi)$ soit plongeable dans une extension galoisienne $N'/k(\xi)$ à groupe de Galois $\Gamma$ d'exposant $p^2$, il faut et il suffit qu'il existe $e \in (E')^\times$ et $\kappa \in k(\xi)^\times$ tels que les classes de $b = \xi e^{-\mathfrak{N}}$ et $c = \kappa\alpha e^{\hat{\theta}}$ dans $(E')^\times/(E')^{\times p}$ soient non triviales et engendrent deux sous-groupes distincts de $(E')^\times/(E')^{\times p}$.*

*Dans les assertions (1) et (2), lorsque le plongement est possible, on peut choisir $N' = E'(b^{1/p}, c^{1/p})$.*

**Remarque.** (voir [9, Théorème 6]) Sous les notations de la proposition précédente, supposons que le plongement soit possible. Soit $Gal(N'/k(\xi)) = <\eta,\ \tau,\ \nu \mid \eta^p = \tau^p = 1,\ \nu^p = \eta^q,\ \eta\tau = \tau\eta,\ \eta\nu = \nu\eta,\ \tau\nu\tau^{-1}\nu^{-1} = \eta>$. Alors, en remplaçant éventuellement $e$ par $\xi^u e$ pour un certain entier $u$, on peut supposer que l'action de $Gal(N'/k(\xi))$ sur $N'$ est déterminée par :

| | $a^{1/p}$ | $b^{1/p}$ | $c^{1/p}$ |
|---|---|---|---|
| $\eta$ | $a^{1/p}$ | $b^{1/p}$ | $\xi c^{1/p}$ |
| $\tau$ | $a^{1/p}$ | $\xi b^{1/p}$ | $c^{1/p}$ |
| $\nu$ | $\xi a^{1/p}$ | $b^{1/p}$ | $b^{1/p}c^{1/p}e$ |

**Proposition 3.2.7.** *Soit $\mathcal{S}'$ l'idéal de $\mathbb{Z}[S]$ engendré par les éléments de la forme $c - s_{\underline{c}}$, où $c \in \mathbb{Z}$ est premier avec $p$, $\underline{c} \equiv c \bmod p$ et $1 \leq \underline{c} \leq p-1$. Alors $\mathcal{S} = \frac{1}{p}\theta\mathcal{S}'$.*

*Démonstration.* Voir [42, Lemme 6.9, p. 93]. □

## 3.3 Démonstration des principaux résultats

Cette section est consacrée à la démonstration du théorème 3.1.1 ; dans cette dernière se trouve celle de la proposition 3.1.2.

**Démonstration du théorème 3.1.1.** Nous distinguons deux cas, selon l'exposant de $\Gamma$. Il est clair que, par sa définition, $A_p$ (resp. $A_{p^2}$) est un sous-groupe de $Cl^\circ(\mathcal{M})$.

(1) **Dans cette partie on suppose $\Gamma$ d'exposant $p$.**

Soit $Y = \Big(c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p, x^p \phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big)$ un élément de $A_p$, où $(c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3$. Nous démontrons ci-dessous que $Y \in \mathcal{R}(\mathcal{M})$, d'où $A_p \subset \mathcal{R}(\mathcal{M})$. La démonstration se fera en quatre étapes.

**Etape 1. Considérons $c_0$.** *Dans cette étape on construit une extension modérée $E_1/k$ de groupe de Galois $C$, avec $[\mathcal{M}(C) \otimes_{O_k[C]} O_{E_1}] = c_0$, et on calcule son discriminant.*

D'après [31, Théorème 2.4] (Rappel : attention : $\mathcal{R}(\mathcal{M}(C))$ est noté $\mathcal{R}(O_k[C])$ dans [31]), $c_0$ est réalisable par une extension galoisienne modérée de degré $p$ ; nous reprenons, d'une façon légèrement différente, la seconde partie de la preuve de ce théorème ([31, (2), p. 195]) pour ajouter des précisions et construire une telle extension de façon convenable pour notre démonstration.

D'après la proposition 3.2.7, il existe un entier $j$, des idéaux fractionnaires $I_i$ de $k(\xi)$, $1 \leq i \leq j$, qu'on peut choisir premiers avec $pO_{k(\xi)}$ par le théorème de densité de Chebotarev (voir Théorème 1.3.3), et des éléments $\mathfrak{s}'_i$, $1 \leq i \leq j$, de $\mathcal{S}'$ tels que :

$$c_0 = cl\big(\prod_{i=1}^{j} (1/p)\mathfrak{s}'_i \theta I_i\big).$$

Posons $I = \prod_{i=1}^{j} (1/p)\mathfrak{s}'_i \theta I_i$ et $J = \prod_{i=1}^{j} \mathfrak{s}'_i I_i$. Alors :

$$I^p = \theta J, \quad c_0 = cl(I).$$

Soit le cycle $\mathcal{C} = (1-\xi)^{p^2}O_{k(\xi)}$ ; remarquons que, dans cette première partie, le cycle $(1-\xi)^p O_{k(\xi)}$ nous suffit, mais nous aurons besoin de $\mathcal{C}$ pour la seconde partie. Soit $Cl(k(\xi),\mathcal{C})$ le groupe de classes de rayon de $k(\xi)$ modulo $\mathcal{C}$. On a $J$ est premier avec $\mathcal{C}$, en effet : d'une part pour tout $i'$, $1 \leq i' \leq p-1$, et tout $i$, $1 \leq i \leq j$, $s_{i'}(I_i)$ est premier avec $s_{i'}(pO_{k(\xi)}) = pO_{k(\xi)}$ ; d'autre part, comme $pO_{k(\xi)} = (1-\xi)^{p-1}O_{k(\xi)}$, les idéaux premiers de $O_{k(\xi)}$ divisant toute puissance non triviale de $(1-\xi)O_{k(\xi)}$ sont exactement ceux divisant $pO_{k(\xi)}$. Par le théorème de densité de Chebotarev dans $Cl(k(\xi),\mathcal{C})$ (voir Théorème 1.3.3), il existe un idéal premier $\mathfrak{p}$ de $O_{k(\xi)}$, avec $\mathfrak{p} \cap O_k$ totalement décomposé dans $k(\xi)/k$ et tel que $cl(\mathfrak{p}) = cl(J)$ dans $Cl(k(\xi),\mathcal{C})$. Il s'ensuit qu'il existe $a' \in k(\xi)$ satisfaisant :

$$\mathfrak{p} = a'J, \quad a' \equiv 1 \ mod^* \ (1-\xi)^{p^2}O_{k(\xi)}.$$

Posons

$$a = \theta a'.$$

Alors

$$aO_{k(\xi)} = (I^{-1})^p \theta \mathfrak{p}.$$

L'élément $a$ n'est pas une puissance $p$-ième dans $k(\xi)$, car par exemple $v_{\mathfrak{p}}(a) \equiv 1 \ mod \ p$, où $v_{\mathfrak{p}}$ est la valuation $\mathfrak{p}$-adique.

Soit $\alpha$ un élément de $\overline{k}$ vérifiant

$$\alpha^p = a.$$

Posons

$$E_1' = k(\xi)(\alpha).$$

Alors $E_1'/k(\xi)$ est une extension cyclique (de Kummer) de degré $p$. Elle est modérée, car $\theta a' \equiv 1 \ mod^* \ (1-\xi)^{p^2}O_{k(\xi)}$ ; donc $E_1'/k$ est modérée car $k(\xi)/k$ l'est. L'extension $E_1'/k$ est galoisienne abélienne par la proposition 3.2.4, car $a = \theta a'$ ; elle admet une (unique) sous-extension $E_1/k$ galoisienne, de degré $p$ ; c'est clair que $E_1/k$ est modérée et $E_1' = E_1(\xi)$.

On a $Gal(E_1'/k(\xi)) \simeq C$. Nous identifions $C$ avec $Gal(E_1(\xi)/k(\xi))$ en faisant agir $\sigma$ sur $E_1(\xi)$ de sorte que $\sigma(\alpha) = \xi\alpha$. Puisque $Gal(E_1(\xi)/k(\xi))$ est isomorphe (par restriction) à $Gal(E_1/k)$, on identifie aussi $C$ et $Gal(E_1/k)$, d'où un caractère $\varphi_0$ de $Gal(E_1/k)$, défini par

$$\varphi_0(\sigma) = \xi.$$

Notons qu'en fait, si l'on note $\pi_0$ l'isomorphisme $Gal(E_1/k) \simeq C$ ci-dessus, alors

$$\varphi_0 = \chi \circ \pi_0.$$

Posons $\alpha' = (1/p)Tr_{E_1(\xi)/E_1}(\alpha)$. Alors $\langle \alpha', \varphi_0 \rangle_{E_1/k} = \alpha$ par la proposition 3.2.5. Donc

$$\langle \alpha', \varphi_0 \rangle^p_{E_1/k} O_{k(\xi)} = (I^{-1})^p \theta \mathfrak{p}.$$

Il est immédiat que pour tout $x \in E_1$,

$$\sigma(\langle x, \varphi_0 \rangle_{E_1/k}) = \varphi_0(\sigma)\langle x, \varphi_0 \rangle_{E_1/k}.$$

On en déduit que si $a_0$ est une base normale de $E_1/k$, alors il existe $\lambda \in k(\xi)$ tel que $\langle a_0, \varphi_0 \rangle_{E_1/k} = \lambda \langle \alpha', \varphi_0 \rangle_{E_1/k}$. Par conséquent

$$\langle a_0, \varphi_0 \rangle^p_{E_1/k} O_{k(\xi)} = (\lambda I^{-1})^p \theta \mathfrak{p}.$$

D'après [31, Théorème 2.3 (1)]

$$[\mathcal{M}(C) \otimes_{O_k[C]} O_{E_1}] (= [\mathcal{M}(C) \otimes_{O_k[C]} O_{E_1,\pi_0}]) = cl(\lambda I^{-1})^{-1} = c_0.$$

Notons $\mathfrak{p}_{E_1} = \mathfrak{p} \cap O_k$. On a

$$\Delta(E_1/k) = \mathfrak{p}_{E_1}^{p-1}.$$

En effet : Par le théorème 1.4.4(i)

$$\Delta(E_1'/k(\xi)) = \Big( \Big( \sum_{i=1}^{p-1} s_i \Big) \mathfrak{p} \Big)^{p-1}.$$

Les extensions $E_1/k$ et $k(\xi)/k$ étant arithmétiquement disjointes et $E_1' = E_1 k(\xi)$, la proposition 1.4.3 implique

$$\Delta(E_1'/k(\xi)) = \Delta(E_1/k) O_{k(\xi)}.$$

Des deux égalités précédentes on déduit

$$N_{k(\xi)/k}(\Delta(E_1'/k(\xi))) = \mathfrak{p}_{E_1}^{(p-1)^2} = \Delta(E_1/k)^{p-1},$$

ce qui donne $\Delta(E_1/k) = \mathfrak{p}_{E_1}^{p-1}$. Ceci termine l'étape 1.

**Etape 2. Considérons maintenant $c_p$.** *Dans cette étape on construit une extension modérée $F_1/k$ de groupe de Galois $C$, arithmétiquement disjointe de $E_1/k$, avec $[\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1}] = c_p$ et $F_1(\xi) = k(\xi)(b^{1/p})$, où $b = e^{-\mathfrak{N}}$ pour un certain $e \in E_1(\xi)$ (voir la définition de $\mathfrak{N}$ ci-dessous ; la forme de $b$ est motivée par l'utilisation des conditions de plongement de la proposition 3.2.6 dans l'étape 3).*

L'extension $E_1'/k(\xi)$ est totalement ramifiée en $\mathfrak{p}$. Par suite

$$N_{E_1'/k(\xi)}(Cl(E_1')) = Cl(k(\xi)),$$

par le théorème 1.3.3. On en déduit que

$$N_{E_1'/k(\xi)}(\mathcal{S}Cl(E_1')) = \mathcal{S}Cl(k(\xi)).$$

Soit $c_p' \in \mathcal{S}Cl(E_1')$ satisfaisant

$$N_{E_1'/k(\xi)}(c_p') = c_p.$$

**Considérons $c_p'$.** Comme pour $c_0$, il existe un entier $j'$, des idéaux fractionnaires $I_i'$ de $E_1(\xi)$, $1 \leq i \leq j'$, qu'on peut choisir premiers avec $pO_{E_1(\xi)}$, et des éléments $\mathfrak{s}_i'$, $1 \leq i \leq j'$, de $\mathcal{S}'$ tels que :

$$c_p' = cl\Big(\prod_{i=1}^{j'}(1/p)\mathfrak{s}_i'\theta I_i'\Big).$$

Posons $I' = \prod_{i=1}^{j'}(1/p)\mathfrak{s}_i'\theta I_i'$ et $J' = \prod_{i=1}^{j'}\mathfrak{s}_i' I_i$. Alors :

$$I'^p = \theta J', \quad c_p' = cl(I').$$

Considérons le cycle $\mathcal{C}' = (1-\xi)^{p^2}O_{E_1(\xi)}$ (ici nous faisons la même remarque que pour le cycle $\mathcal{C} : (1-\xi)^p O_{E_1(\xi)}$ suffit) et $Cl(E_1(\xi), \mathcal{C}')$ le groupe de classes de rayon de $E_1(\xi)$ modulo $\mathcal{C}'$. Comme pour $c_0$, il existe un idéal premier $\mathfrak{q}$ de $O_{E_1(\xi)}$, avec $\mathfrak{q} \cap O_k$ totalement décomposé dans $E_1(\xi)/k$, qu'on peut supposer en plus premier avec tous les $s_i(\mathfrak{p}O_{E_1(\xi)})$, $s_i$ parcourant $S$, et tel que $cl(\mathfrak{q}) = cl(J')$ dans $Cl(E_1(\xi), \mathcal{C}')$. Il s'ensuit qu'il existe $\beta \in E_1(\xi)$ satisfaisant :

$$\mathfrak{q} = \beta' J', \quad \beta' \equiv 1 \ mod^* \ (1-\xi)^{p^2}O_{E_1(\xi)}.$$

Posons

$$\beta = \theta\beta'.$$

Alors

$$\beta O_{E_1(\xi)} = (I'^{-1})^p \theta \mathfrak{q}.$$

**Nous désignons par $\rho$ le générateur de $Gal(E_1(\xi)/k(\xi))$ qui est l'image de $\sigma$ sous l'identification $C = Gal(E_1(\xi)/k(\xi))$,** autrement dit

$$\rho(\alpha) = \xi\alpha,$$

et soit

$$\mathfrak{N} = \sum_{i=0}^{p-1}\rho^i.$$

Posons

$$e = \beta^{-1}\ (= \theta(\beta'^{-1})), \qquad b = e^{-\mathfrak{N}}\ (= \theta(\beta'^{\mathfrak{N}})).$$

On a

$$b = N_{E_1(\xi)/k(\xi)}(\beta).$$

Soit

$$\mathfrak{q}_1 = O_{k(\xi)} \cap \mathfrak{q}.$$

Il est immédiat que la décomposition de façon unique de $bO_{k(\xi)}$ est

$$bO_{k(\xi)} = \big(N_{E_1(\xi)/k(\xi)}(I'^{-1})\big)^p \theta \mathfrak{q}_1,$$

car $\mathfrak{q}_1 \cap O_k$ est totalement décomposé dans $k(\xi)/k$ (puisque $\mathfrak{q} \cap O_k$ l'est dans $E_1(\xi)/k$).

De $v_{\mathfrak{q}_1}(b) \equiv 1\ mod\ p$ découle que $b$ n'est pas une puissance $p$-ième dans $k(\xi)$. Soit $\alpha''$ un élément de de $\overline{k}$ vérifiant

$$(\alpha'')^p = b.$$

Posons

$$F_1' = k(\xi)(\alpha'').$$

On a

$$b = \theta(\beta'^{\mathfrak{N}})), \quad \text{et} \quad \theta(\beta'^{\mathfrak{N}})) \equiv 1\ mod^*\ (1-\xi)^{p^2} O_{E_1(\xi)}.$$

Comme pour $E_1'/k$, $F_1'/k$ est galoisienne abélienne et modérée, de degré $p(p-1)$, elle admet une (unique) sous-extension $F_1/k$ galoisienne modérée, de degré $p$ ; c'est clair que $F_1' = F_1(\xi)$. Nous identifions $C$ avec $Gal(F_1(\xi)/k(\xi))$ en faisant agir $\sigma$ sur $F_1(\xi)$ de sorte que $\sigma(\alpha) = \xi\alpha$ et on définit un caractère $\varphi_p$ de $Gal(F_1/k)$ par $\varphi_p(\sigma) = \xi$. En fait, si $\pi_p$ est l'isomorphisme $Gal(F_1/k) \simeq C$, alors $\varphi_p = \chi \circ \pi_p$. On obtient

$$[\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1}](= [\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1,\pi_p}]) = cl\Big(N_{E_1(\xi)/k(\xi)}(I'^{-1})\Big)^{-1} = c_p,$$

et si l'on note $\mathfrak{q}_{F_1} = \mathfrak{q}_1 \cap O_k$, sachant que $\mathfrak{q}_{F_1}$ est totalement décomposé dans $k(\xi)/k$, alors

$$\Delta(F_1/k) = \mathfrak{q}_{F_1}^{p-1}.$$

Signalons que $E_1/k$ et $F_1/k$ sont arithmétiquement disjointes, car $\mathfrak{q}_{F_1} \neq \mathfrak{p}_{E_1}$ par le choix de $\mathfrak{q}$ (premier avec tous les $s_i(\mathfrak{p}O_{E_1(\xi)})$, $s_i$ parcourant $S$). Ceci termine l'étape 2.

**Etape 3. Considérons maintenant** $x$. On rappelle que $x$ apparait dans l'égalité $Y = \Big(c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p, x^p \phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big)$ (où $(c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3$).

*Dans cette étape on construit un élément $c \in E_1(\xi)$ de sorte que les classes de $b$ et $c$ n'engendrent pas le même sous-groupe de $E_1(\xi)^\times/E_1(\xi)^{\times p}$, ce qui permet, grâce à la proposition 3.2.6, de plonger $E_1(\xi)/k(\xi)$ dans une extension $N_1'/k(\xi)$ ($N_1' = E_1(\xi)(b^{1/p}, c^{1/p})$) à groupe de Galois isomorphe à $\Gamma$. Puis on prouve que $N_1'$ contient une extension $N_1/k$ galoisienne modérée de groupe de Galois $\Gamma$, avec $E_1 \subset N_1$ et $F_1 \subset N_1$.*

Puisque $x \in \mathcal{S}Cl(k(\xi))$, comme pour $c_0$ et $c_p$, il existe un idéal premier $\mathfrak{r}$ de $O_{k(\xi)}$, tel que $\mathfrak{r}O_{E_1(\xi)}$ est premier à tous les conjugués de $\mathfrak{q}$ sous $Gal(E_1(\xi)/k)$, avec $\mathfrak{r}\cap O_k$ totalement décomposé dans $E_1(\xi)/k$ ($\mathfrak{r}$ peut être choisi totalement décomposé dans $E_1(\xi)/k(\xi)$ car $N_{E_1(\xi)/k(\xi)}(Cl(E_1(\xi)) = Cl(k(\xi)))$, et il existe un idéal fractionnaire $I''$ de $k(\xi)$ et des éléments $\kappa, \kappa'$ de $k(\xi)$ satisfaisant :

$$\kappa O_{k(\xi)} = (I''^{-1})^p \theta \mathfrak{r}, \quad cl(I'') = x, \quad \kappa = \theta\kappa', \quad \kappa' \equiv 1 \; mod^* \; (1-\xi)^{p^2} O_{k(\xi)}.$$

Soit

$$\hat{\theta} = \sum_{i=0}^{p-1} i\rho^i.$$

Posons

$$c = \kappa^{-1} e^{\hat{\theta}} \quad (= \kappa^{-1}\beta^{-\hat{\theta}} = \theta(\kappa'^{-1}\beta'^{-\hat{\theta}})).$$

Dans un premier temps, nous déterminons la décomposition de façon unique de $bO_{E_1(\xi)}$ et celle de $c^{-1}O_{E_1(\xi)} = \kappa e^{-\hat{\theta}} O_{E_1(\xi)}$.

On a

$$bO_{E_1(\xi)} = \beta^{\mathfrak{N}} O_{E_1(\xi)} = (\mathfrak{N}I'^{-1})^p \mathfrak{N}\theta\mathfrak{q},$$

d'où la décomposition de façon unique de $bO_{E_1(\xi)}$ :

$$bO_{E_1(\xi)} = (\mathfrak{N}I'^{-1})^p \prod_{i=1}^{p-1}\prod_{j=0}^{p-1} (s_i^{-1}\rho^j)(\mathfrak{q})^i.$$

On a

$$e^{-\hat{\theta}} O_{E_1(\xi)} = \beta^{\hat{\theta}} O_{E_1(\xi)} = (\hat{\theta}I'^{-1})^p \hat{\theta}\theta\mathfrak{q}.$$

Pour tout $i \in \mathbb{Z}$ on note $\underline{i}$ l'entier vérifiant : $i \equiv \underline{i} \; mod \; p$ et $0 \leq \underline{i} \leq p-1$. Alors

$$\begin{aligned} \theta\hat{\theta}\mathfrak{q} &= \prod_{i=1}^{p-1}\prod_{j=1}^{p-1} (s_i^{-1}\rho^j)(\mathfrak{q})^{ij} \\ &= \Big(\prod_{i=1}^{p-1}\prod_{j=1}^{p-1} (s_i^{-1}\rho^j)(\mathfrak{q})^{(ij-\underline{ij})/p}\Big)^p \prod_{i=1}^{p-1}\prod_{j=1}^{p-1} (s_i^{-1}\rho^j)(\mathfrak{q})^{\underline{ij}}. \end{aligned}$$

Par conséquent la décomposition de façon unique de $c^{-1}O_{E_1(\xi)}$ est

$$c^{-1}O_{E_1(\xi)} = \Big(I''^{-1}O_{E_1(\xi)}\hat{\theta}I'^{-1}\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{(ij-\underline{ij})/p}\Big)^p \times$$
$$\theta(\mathfrak{r}O_{E_1(\xi)})\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{\underline{ij}}.$$

De $v_{\mathfrak{q}}(b) \equiv 1 \ mod\ p$ et $v_{\rho(\mathfrak{q})}(c) \equiv -1 \ mod\ p$ découle que $b$ et $c$ ne sont pas des puissances $p$-ième dans $E_1(\xi)$, autrement dit : les classes $\bar{b}$ et $\bar{c}$ dans $E_1(\xi)^\times/E_1(\xi)^{\times p}$ ne sont pas triviales.

On a $v_{\mathfrak{q}}(c^{-1}) \equiv 0 \ mod\ p$, d'où $v_{\mathfrak{q}}(c) \equiv 0 \ mod\ p$. Comme $v_{\mathfrak{q}}(b) \equiv 1 \ mod\ p$, on a pour tout $i$, $1 \leq i \leq p-1$, $v_{\mathfrak{q}}(bc^{-i}) \equiv 1 \ mod\ p$. Par suite les classes $\bar{b}$ et $\bar{c}$ n'engendrent pas le même sous-groupe de $E_1(\xi)^\times/E_1(\xi)^{\times p}$.

D'après la proposition 3.2.6, $E_1(\xi)/k(\xi)$ est plongeable dans une extension $N_1'/k(\xi)$ à groupe de Galois isomorphe à $\Gamma$, et on peut prendre

$$N_1' = E_1(\xi)(b^{1/p}, c^{1/p}).$$

On a

$$N_1' = E_1(\xi)(b^{1/p}, c^{-1/p}) = E_1(\xi, a^{1/p}, b^{1/p}, c^{-1/p}).$$

Soit $\gamma$ un élément de $\overline{k}$ vérifiant

$$\gamma^p = c^{-1}.$$

D'après la remarque suivant la proposition 3.2.6, on peut supposer que l'action de $Gal(N_1'/k(\xi))$ sur $N_1'$ est déterminée par :

| | $\alpha$ | $\alpha''$ | $\gamma$ |
|---|---|---|---|
| $\eta$ | $\alpha$ | $\alpha''$ | $\xi^{-1}\gamma$ |
| $\tau$ | $\alpha$ | $\xi\alpha''$ | $\gamma$ |
| $\nu$ | $\xi\alpha$ | $\alpha''$ | $\alpha''\gamma e$ |

Considérons l'extension

$$K_1' = E_1(\xi)(b^{1/p})/E_1(\xi).$$

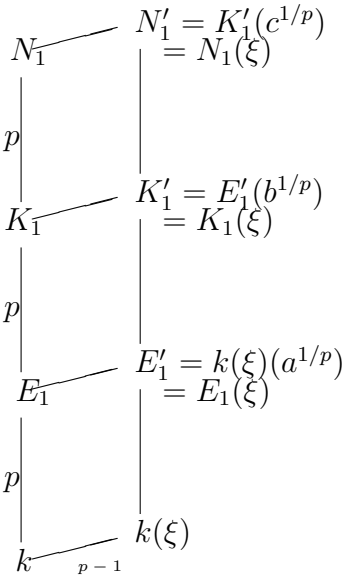
Puisque $b = \theta(\beta'^{\mathfrak{N}})$, la proposition 3.2.4 nous dit que $K_1'/E_1$ est abélienne, et comme elle est cyclique de degré $p(p-1)$ elle contient une unique sous-extension $K_1/E_1$ de degré $p$ ; c'est clair que $K_1' = K_1(\xi)$ . Mais la composée $E_1F_1$ est contenue dans $K_1'$. Il est immédiat que le degré de $E_1F_1/E_1$ est $p$, par conséquent $E_1F_1 = K_1$.

On a $N_1' = K_1(\xi)(c^{1/p})/K_1(\xi)$ $(= K_1(\xi)(c^{-1/p})/K_1(\xi))$. Puisque

$$c = \theta(\kappa'^{-1}\beta'^{-\hat{\theta}}),$$

la proposition 3.2.4 nous dit que $N_1'/K_1$ est abélienne, et comme ci-dessus elle contient une unique sous-extension $N_1/K_1$ de degré $p$ ; c'est clair que $N_1' = N_1(\xi)$

Nous résumons la situation dans le diagramme suivant :




Maintenant on remplace les diagrammes des pages 185 et 186 de [2] (qui sont les mêmes, puisque l'exposant $v$ de $\Gamma$ est $p$) par le nôtre ci-dessus. Sous nos notations, d'une façon très similaire à ce qu'est écrit dans [2, pp. 185–187] (on s'arrête à la ligne avant Etape 4), on montre que $N_1/k$ est galoisienne modérée ayant un groupe de Galois isomorphe à $\Gamma = Gal(N_1'/k(\xi)$ (isomorphisme de restriction). Ceci termine l'étape 3.

**Etape 4.** *Posons* $X = [\mathcal{M} \otimes_{O_k[\Gamma]} O_{N_1}] = (x_0, x_1, \ldots, x_p, x_{p+1}) \in Cl^\circ(\mathcal{M})$. *Dans cette étape on montre que* $Y = X$, *ce qui achève la démonstration de la partie (1).*

Considérons l'extension

$$M_1' = E_1(\xi)(c^{-1/p})/E_1(\xi) \ (= E_1(\xi)(c^{1/p})/E_1(\xi)).$$

Puisque

$$c^{-1} = \theta(\kappa'\beta^{\hat{\theta}}),$$

la proposition 3.2.4 nous dit que $M_1'/E_1$ est abélienne, et comme ci-dessus elle contient une unique sous-extension $M_1/E_1$ de degré $p$ ; c'est clair que $M_1' = M_1(\xi)$ et $N_1 = M_1K_1$.

Nous identifions $C$ avec $Gal(M_1(\xi)/E_1(\xi))$ en faisant agir $\sigma$ sur $M_1(\xi)$ de sorte que $\sigma(\gamma) = \xi\gamma$, et on définit un caractère $\psi_0$ de $Gal(M_1/E_1) \simeq C$ par $\psi_0(\sigma) = \xi$. On obtient

$$[\mathcal{M}_{E_1}(C) \otimes_{O_{E_1}[C]} O_{M_1}] = cl\Big(I''^{-1}O_{E_1(\xi)}\hat{\theta}I'^{-1}\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{(ij-\underline{ij})/p}\Big)^{-1}.$$

En fait, si $\pi_{p+1}$ est l'isomorphisme $Gal(M_1/E_1) \simeq C$, alors $\psi_0 = \chi \circ \pi_{p+1}$ et $[\mathcal{M}(C) \otimes_{O_{E_1}[C]} O_{M_1}] = [\mathcal{M}(C) \otimes_{O_{E_1}[C]} O_{M_1,\pi_{p+1}}]$.

Les extensions $E_1/k$ et $F_1/k$ étant arithmétiquement disjointes, puisque $[\mathcal{M}(C) \otimes_{O_k[C]} O_{E_1}] = c_0$ et $[\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1}] = c_p$, d'après les propositions 3.2.2 et 3.2.3 on a :

$$x_0 = c_0, \quad x_p = c_p, \quad x_i = c_0 s_i(c_p), \quad \text{pour tout} \quad i, 1 \leq i \leq (p-1),$$

$$x_{p+1} = \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0))N_{E_1(\xi)/k(\xi)}([\mathcal{M}_{E_1}(C) \otimes_{O_{E_1}[C]} O_{M_1}]).$$

Comme $Gal(E_1(\xi)/k(\xi)) = \langle\rho\rangle$, $N_{E_1(\xi)/k(\xi)}(\mathfrak{q}) = \mathfrak{q}_1$ (car $\mathfrak{q}_1$ est totalement décomposée dans $E_1(\xi)/k(\xi)$), $cl\Big(N_{E_1(\xi)/k(\xi)}(I'^{-1})\Big)^{-1} = c_p$ et $Cl(I'') = x$ on a :

$$\begin{aligned} N_{E_1(\xi)/k(\xi)}([\mathcal{M}_{E_1}(C) \otimes_{O_{E_1}[C]} O_{M_1}]) &= x^p\hat{\theta}c_p cl\Big(\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q}_1)^{(ij-\underline{ij})/p}\Big)^{-1} \\ &= x^p\hat{\theta}c_p cl\Big(\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1})(\mathfrak{q}_1)^{(ij-\underline{ij})/p}\Big)^{-1}. \end{aligned}$$

Posons

$$\theta_0 = \sum_{i=1}^{p-1}\sum_{j=1}^{p-1}((ij-\underline{ij})/p)s_i^{-1}, \quad \mathcal{N} = \sum_{i=1}^{p-1} s_i.$$

De $\sum_{j=1}^{p-1}((ij-\underline{ij})/p) = ((p-1)/2)(i-1)$ on déduit facilement que

$$\theta_0 = ((p-1)/2)(\theta - \mathcal{N}).$$

Faisons la remarque suivante : $\theta_0$ est un élément de Stickelberger ; en effet : on vérifie sans peine que $\mathcal{N} = (1/p)(s_1 + s_{p-1})\theta \in \mathcal{S}$.

On a donc :

$$N_{E_1(\xi)/k(\xi)}([\mathcal{M}_{E_1}(C) \otimes_{O_{E_1}[C]} O_{M_1}]) = x^p\hat{\theta}c_p\theta_0 cl(\mathfrak{q}_1)^{-1}.$$

Maintenant

$$\hat{\theta}c_p = \prod_{i=1}^{p-1} \rho^i(c_p)^i = c_p^{\sum_{i=1}^{p-1} i} = c_p^{p(p-1)/2}.$$

Il découle de $bO_{k(\xi)} = \big(N_{E_1(\xi)/k(\xi)}(I'^{-1})\big)^p \theta \mathfrak{q}_1$ que

$$\theta cl(\mathfrak{q}_1)^{-1} = c_p^{-p}.$$

D'où

$$\theta_0 cl(\mathfrak{q}_1)^{-1} = c_p^{-p(p-1)/2} cl(\mathcal{N}\mathfrak{q}_1)^{(p-1)/2}.$$

Par le théorème 1.4.4(i)

$$\Delta(F_1(\xi)/k(\xi)) = (\mathcal{N}\mathfrak{q}_1)^{p-1}.$$

Puisque $F_1(\xi)/k(\xi)$ est galoisienne de degré impair, le théorème1.4.1 d'Artin nous donne

$$cl_{O_{k(\xi)}}(O_{F_1(\xi)}) = cl\big(\Delta(F_1(\xi)/k(\xi))^{1/2}\big).$$

Donc

$$\theta_0 cl(\mathfrak{q}_1)^{-1} = c_p^{-p(p-1)/2} cl_{O_{k(\xi)}}(O_{F_1(\xi)}).$$

Les extensions $F_1/k$ et $k(\xi)/k$ étant arithmétiquement disjointes, on vérifie sans difficulté en utilisant le théorème d'Artin que

$$cl_{k(\xi)}(O_{F_1(\xi)}) = \phi_{k(\xi)/k}(cl_k(O_{F_1})).$$

Mais

$$cl_k(O_{F_1}) = N_{k(\xi)/k}(c_p)^{\varphi_p(1)} = N_{k(\xi)/k}(c_p),$$

par conséquent

$$\theta_0 cl(\mathfrak{q}_1)^{-1} = c_p^{-p(p-1)/2} \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_p)).$$

D'où

$$N_{E_1(\xi)/k(\xi)}([\mathcal{M}_{E_1}(C) \otimes_{O_{E_1}[C]} O_{M_1}]) = x^p c_p^{p(p-1)} c_p^{-p(p-1)/2} \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_p)).$$

On conclut que

$$x_{p+1} = x^p \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0 c_p)).$$

Par conséquent $Y = X$, ce qui termine la démonstration de la partie (1).

**Remarque.** L'objet de cette remarque est de montrer la proposition 3.1.2 lorsque $\Gamma$ est d'exposant $p$.

Ecrivons $X = [\mathcal{M} \otimes_{O_k[\Gamma]} O_{N_1}] = (x_0, x_1, \ldots, x_p, x_{p+1})$. En raisonnant comme dans le début de la partie (1) de la preuve du théorème 1.1 dans [4, p. 25] (on utilise le caractère de la représentation régulière de $C$) on obtient :

$$cl_k(O_{N_1}) = \big(\prod_{i=0}^{p} N_{k(\xi)/k}(x_i)^{\varphi_i(1)=1}\big) \times N_{k(\xi)/k}(x_{p+1})^{\phi_1(1)=p}$$

Comme $X = (c_0, c_0 s_1(c_p), c_0 s_2(c_p), \ldots, c_0 s_{p-1}(c_p), c_p, x^p \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0 c_p)))$, on obtient :

$$cl_k(O_{N_1}) = N_{k(\xi)/k}(c_0 c_p x)^{p^2}.$$

Par suite

$$R_m(k, \Gamma, A_p) = N_{k(\xi)/k}(\mathcal{S}Cl(k(\xi)))^{p^2}.$$

On a $N_{k(\xi)/k}(\mathcal{S}Cl(k(\xi))) = \mathcal{S}N_{k(\xi)/k}(Cl(k(\xi)))$, et si $x \in Cl(k(\xi))$, alors $\theta N_{k(\xi)/k}(x) = N_{k(\xi)/k}(x)^{p(p-1)/2}$. On en déduit l'égalité :

$$N_{k(\xi)/k}(\mathcal{S}Cl(k(\xi))) = N_{k(\xi)/k}(Cl(k(\xi)))^{(p-1)/2}.$$

Par conséquent $R_m(k, \Gamma, A_p)$ est égal au sous-groupe $N_{k(\xi)/k}(Cl(k(\xi))^{p^2(p-1)/2}$ ; mais ce dernier est égal à $R_m(k, \Gamma)$ d'après [2, Théorème 1.1 ]. On conclut que

$$R_m(k, \Gamma, A_p) = R_m(k, \Gamma) = N_{k(\xi)/k}(Cl(k(\xi))^{p^2(p-1)/2}.$$

(2) **Dans cette partie on suppose $\Gamma$ d'exposant $p^2$ et $k(\xi_{p^2})/k(\xi)$ non ramifiée.**

Soit $Y$ l'élément de $A_{p^2}$ suivant :

$$Y = \Big(c_0, c_0 s_1(c_p), \ldots, c_0 s_{p-1}(c_p), c_p, x^p((s_{p-1} - \theta)c_0)\phi_{k(\xi)/k}\big(N_{k(\xi)/k}(c_0 c_p)\big)\Big),$$

où $(c_0, c_p, x) \in \mathcal{S}Cl(k(\xi))^3$. Nous démontrons ci-dessous que $Y \in \mathcal{R}(\mathcal{M})$, d'où $A_{p^2} \subset \mathcal{R}(\mathcal{M})$.

Le plan de la démonstration est le suivant : nous procéderons comme dans la partie (1), mais nous modifierons les éléments $b$ et $c$ de la partie (1) en de nouveaux éléments $b'$ et $c'$ afin d'obtenir une extension à groupe de Galois $\Gamma$ d'exposant $p^2$. Comme la démarche est analogue à celle de (1), nous ne donnerons pas tous les détails, mais nous essayerons d'en donner suffisamment afin de rendre notre démonstration aussi compréhensible que possible.

**On considère $c_0$.** On garde tout ce qui est dit dans le début de la partie (1) ; on obtient :

$$[\mathcal{M}(C) \otimes_{O_k[C]} O_{E_1}] = cl(\lambda I^{-1})^{-1} = c_0, \quad \Delta(E_1/k) = \mathfrak{p}_{E_1}^{p-1}.$$

**On considère $c_p$.** On garde ce qui est dit dans la partie (1) à partir de la considération de $c_p$, mais on remplace $b$ par $\xi b$.

On pose

$$b' = \xi b.$$

Alors la décomposition de façon unique de $b'O_{k(\xi)}$ est la même que celle de $bO_{k(\xi)}$ :

$$b'O_{k(\xi)} = \big(N_{E_1(\xi)/k(\xi)}(I'^{-1})\big)^p \theta\mathfrak{q}_1,$$

et

$$b' \equiv \xi \ mod^* \ (1-\xi)^{p^2} O_{k(\xi)};$$

de plus, puisque $\theta(\xi^{-1}) = \xi$, on a

$$b' = \theta(\xi^{-1}\beta'^{\mathfrak{M}}).$$

On désigne maintenant par $\alpha''$ un élément de $\overline{k}$ satisfaisant

$$(\alpha'')^p = b',$$

et on pose

$$F_1' = k(\xi)(\alpha'').$$

Comme $b' = \theta(\xi^{-1}\beta'^{\mathfrak{M}})$, $F_1'/k$ est galoisienne abélienne par la proposition 3.2.4, elle admet une (unique) sous-extension $F_1/k$ galoisienne de degré $p$ et c'est clair que $F_1' = F_1(\xi)$.

Montrons que $F_1/k$ est modérée ; pour cela il suffit de voir que $F_1'/k(\xi)$ est modérée, car dans ce cas $F_1/k$ serait une sous-extension de l'extension modérée $F_1'/k$.

On considère la composée $F_1'k(\xi_{p^2})/k(\xi)$. Les extensions $F_1'/k(\xi)$ et $k(\xi_{p^2})/k(\xi)$ sont linéairement disjointes car $\mathfrak{q}_1$ est ramifié dans $F_1'/k(\xi)$ (par la théorie de Kummer) et les seuls idéaux qui peuvent se ramifier dans $k(\xi_{p^2})/k(\xi)$ sont les idéaux au desus de $p$ (nous n'avons pas besoin pour l'instant de $k(\xi_{p^2})/k(\xi_p)$ non ramifiée). On en déduit que $F_1'k(\xi_{p^2})/k(\xi_{p^2})$ est une extension de Kummer de degré $p$.

On a $F_1'k(\xi_{p^2}) = k(\xi_{p^2})(\alpha'')$. Comme $b' \equiv \xi \ mod^* \ (1-\xi)^{p^2}O_{k(\xi)}$ et $\xi$ est une puissance $p$-ième dans $k(\xi_{p^2})$, $k(\xi_{p^2})(\alpha'')/k(\xi_{p^2})$ est modérée par le théorème 1.4.4. Supposons maintenant $k(\xi_{p^2})/k(\xi_p)$ non ramifiée, alors $k(\xi_{p^2})(\alpha'')/k(\xi)$ est modérée, en particulier la sous-extension $F_1'/k(\xi)$ l'est.

Comme dans la partie (1), on obtient

$$[\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1}] = cl\Big(N_{E_1(\xi)/k(\xi)}(I'^{-1})\Big)^{-1} = c_p, \quad \Delta(F_1/k) = \mathfrak{q}_{F_1}^{p-1}.$$

**Considérons maintenant $x$.** On garde tout ce qu'il y a dans la partie (1), à partir de cette considération et on s'arrête avant le paragraphe débutant

par [D'après la proposition 3.2.6...] ; mais on remplace $b$ par $b'$ et on ajoute (ajout facile à faire) la condition suivante dans le choix de $\mathfrak{r} : \mathcal{N}(\mathfrak{r}O_{E_1(\xi)})$ est premier avec $\mathcal{N}(\mathfrak{p}O_{E_1(\xi)})$ (rappelons que $\mathcal{N} = \sum_{i=1}^{p-1} s_i$).

**Nous allons maintenant modifier l'élément $c$ de la partie (1).**
Rappelons qu'on a :

$$\alpha^p O_{k(\xi)} = aO_{k(\xi)} = (I^{-1})^p \theta \mathfrak{p}, \quad a = \theta a'.$$

L'idéal premier $\mathfrak{p}$ est totalement ramifié dans $E_1(\xi)/k(\xi)$, donc

$$\mathfrak{p}O_{E_1(\xi)} = \hat{\mathfrak{p}}^p,$$

où $\hat{\mathfrak{p}}$ est un idéal premier de $O_{E_1(\xi)}$. On en déduit :

$$\alpha O_{E_1(\xi)} = I^{-1} O_{E_1(\xi)} \theta \hat{\mathfrak{p}}$$

Par le théorème de Tchebotarev, et la surjection de la norme de $Cl(E_1(\xi))$ sur $Cl(k(\xi))$, il existe un idéal premier $\mathfrak{p}_1$ de $O_{k(\xi)}$ totalement décomposé dans $E_1(\xi)/k(\xi)$ avec $\mathfrak{p}_1 \cap O_k$ totalement décomposé dans $k(\xi)/k$ et tel que $\mathcal{N}(\mathfrak{p}_1 O_{E_1(\xi)})$ est premier avec $\mathcal{N}(\mathfrak{r}O_{E_1(\xi)}\hat{\mathfrak{p}})$ et tous les conjugués de $\mathfrak{q}$ sous $Gal(E_1(\xi)/k)$, et il existe $\kappa'' \in k(\xi)$ vérifiant :

$$\kappa'' I^{-1} = \mathfrak{p}_1, \quad \kappa'' \equiv 1 \ mod^* \ (1-\xi)^{p^2} O_{k(\xi)}.$$

On a

$$\rho(\theta\alpha) = \theta\rho(\alpha) = \theta(\xi\alpha) = \theta\xi\theta\alpha = \xi^{-1}\theta\alpha.$$

Donc $\theta\alpha$ a $p$ conjugués. Par suite

$$E_1(\xi) = k(\xi)(\theta\alpha) = k(\xi)(\theta\alpha^{-1}) \ (= (k(\xi)(\alpha)).$$

Posons

$$c' = c\theta\kappa''^{-1}\theta\alpha^{-1}.$$

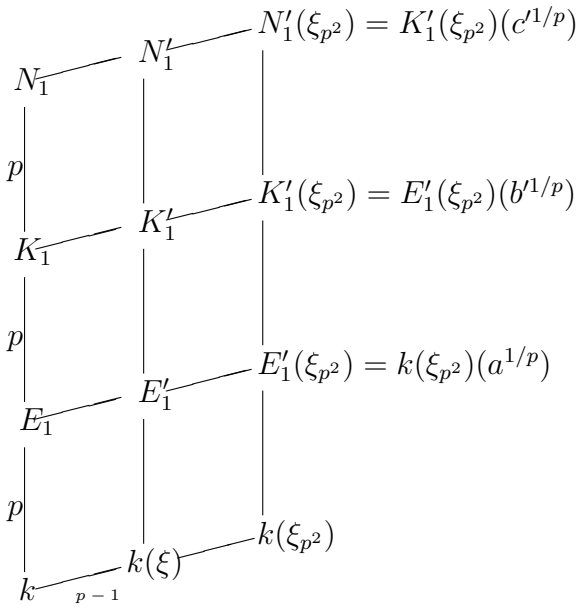
Comme $c = \theta(\kappa'\beta'^{\hat{\theta}})^{-1}$, on a

$$c' = \theta(\kappa''\alpha\kappa'\beta'^{\hat{\theta}})^{-1}.$$

On vérifie facilement que $b'$ et $c'$ vérifient les conditions de l'assertion (2) de la proposition 3.2.6. Donc $E_1(\xi)/k(\xi)$ est plongeable dans une extension $N_1'/k(\xi)$ à groupe de Galois isomorphe à $\Gamma$, et on peut prendre

$$N_1' = E_1(\xi)(b'^{1/p}, c'^{1/p}) = E_1(\xi)(b'^{1/p}, c'^{-1/p}) = E_1(\xi, a^{1/p}, b'^{1/p}, c'^{-1/p}).$$

Comme dans la partie (1) on obtient le diagramme suivant :




Maintenant on remplace les diagrammes des pages 185 et 186 de [2] par le nôtre ci-dessus. Sous nos notations, avec l'hypothèse $k(\xi_{p^2})/k(\xi)$ non ramifiée, d'une façon très similaire à ce qu'est écrit dans les pages [2, pp. 185–187] on montre que $N_1/k$ est galoisienne modérée ayant un groupe de Galois isomorphe à $\Gamma = Gal(N_1'/k(\xi))$.

Considérons

$$M_1' = E_1(\xi)(c'^{1/p}) = E_1(\xi)(c'^{-1/p}).$$

Puisque $c'^{-1} = \theta(\kappa''\alpha\kappa'\beta'^{\hat{\theta}})$, la proposition 3.2.4 nous dit que $M_1'/E_1$ est abélienne, de plus elle contient une unique sous-extension $M_1/E_1$ de degré $p$ modérée ; c'est clair que $M_1' = M_1(\xi)$ et $N_1 = M_1K_1$.

Nous allons déterminer la décomposition de façon unique de $c'^{-1}O_{E_1(\xi)}$, où $c'^{-1} = c^{-1}\theta\kappa''\theta\alpha$.

On a

$$\kappa''\alpha O_{E_1(\xi)} = \kappa'' I^{-1} O_{E_1(\xi)}\theta\hat{\mathfrak{p}} = \mathfrak{p}_1 O_{E_1(\xi)}\theta\hat{\mathfrak{p}}.$$

Par suite

$$\theta\kappa''\theta\alpha O_{E_1(\xi)} = \theta\mathfrak{p}_1 O_{E_1(\xi)}\theta^2\hat{\mathfrak{p}}.$$

De cette égalité et la décomposition de façon unique de $c^{-1}O_{E_1(\xi)}$ figurant dans la partie (1) il découle que

$$c'^{-1}O_{E_1(\xi)} = \Big(I''^{-1}O_{E_1(\xi)}\hat{\theta}I'^{-1}\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{(ij-\underline{ij})/p}\Big)^p \times$$
$$\theta\mathfrak{r}O_{E_1(\xi)}\Big(\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{\underline{ij}}\Big)\theta\mathfrak{p}_1O_{E_1(\xi)}\theta^2\hat{\mathfrak{p}}.$$

On a

$$\theta^2 \equiv s_{p-1}\theta \ mod\ p\mathcal{S},$$

en effet : écrivons $\theta = \sum_{i=1}^{p-1} is_{i^*}$, où $ii^* \equiv 1\ mod\ p$; d'après la proposition 3.2.7, $s_{i^*}\theta \equiv i^*\theta\ mod\ p\mathcal{S}$ et donc

$$\begin{aligned}\theta^2 &\equiv (\sum_{i=1}^{p-1} ii^*)\theta \equiv (p-1)\theta\ mod\ p\mathcal{S}\\ &\equiv -\theta \equiv s_{p-1}\theta\ mod\ p\mathcal{S}.\end{aligned}$$

Par suite :

$$\theta^2 = p(\frac{1}{p}(\theta^2 - s_{p-1}\theta)) + s_{p-1}\theta,$$

où $\frac{1}{p}(\theta^2 - s_{p-1}\theta)$ **est un élément de Stickelberger.** On en déduit que

$$c'^{-1}O_{E_1(\xi)} = \Big(\frac{1}{p}(\theta^2 - s_{p-1}\theta)\hat{\mathfrak{p}}I''^{-1}O_{E_1(\xi)}\hat{\theta}I'^{-1}\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{(ij-\underline{ij})/p}\Big)^p \times$$
$$\theta\mathfrak{r}O_{E_1(\xi)}\Big(\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{\underline{ij}}\Big)\theta\mathfrak{p}_1O_{E_1(\xi)}s_{p-1}\theta\hat{\mathfrak{p}}$$

est la décomposition de façon unique de $c'^{-1}O_{E_1(\xi)}$.

La classe $[\mathcal{M}(C) \otimes_{O_{E_1}[C]} O_{M_1}]$ est égale à :

$$cl\Big(\frac{1}{p}(\theta^2 - s_{p-1}\theta)\hat{\mathfrak{p}}I''^{-1}O_{E_1(\xi)}\hat{\theta}I'^{-1}\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{(ij-\underline{ij})/p}\Big)^{-1}.$$

Posons

$$X = [\mathcal{M} \otimes_{O_k[\Gamma]} O_{N_1}] = (x_0, x_1, \ldots, x_p, x_{p+1}) \in Cl^\circ(\mathcal{M}).$$

Comme $E_1/k$ et $F_1/k$ sont arithmétiquement disjointes, $[\mathcal{M}(C) \otimes_{O_k[C]} O_{E_1}] = c_0$ et $[\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1}] = c_p$, d'après les propositions 3.2.2 et 3.2.3 on a :

$$x_0 = c_0, \quad x_p = c_p, \quad x_i = c_0 s_i(c_p), \quad \text{pour tout} \quad i, 1 \leq i \leq (p-1),$$

$$x_{p+1} = \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0)) N_{E_1(\xi)/k(\xi)}([\mathcal{M}_{E_1}(C) \otimes_{O_{E_1}[C]} O_{M_1}]).$$

Posons

$$Z = cl\Big(N_{E_1(\xi)/k(\xi)}(\frac{1}{p}(\theta^2 - s_{p-1}\theta)\hat{\mathfrak{p}})\Big)^{-1}$$

Alors

$$x_{p+1} = Z x^p \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0 c_p))$$

Dans ce qui suit nous calculons $Z$.

On a

$$N_{E_1(\xi)/k(\xi)}(\frac{1}{p}(\theta^2 - s_{p-1}\theta)\hat{\mathfrak{p}}) = \frac{1}{p}(\theta^2 - s_{p-1}\theta)\mathfrak{p}.$$

De

$$\theta\mathfrak{p} = I^p a O_{k(\xi)} = I^p \theta a' O_{k(\xi)},$$

on déduit

$$(\theta^2 - s_{p-1}\theta)\mathfrak{p} = \Big((\theta - s_{p-1}) I \frac{1}{p}(\theta^2 - s_{p-1}\theta) a' O_{k(\xi)}\Big)^p.$$

Par conséquent

$$Z = cl((s_{p-1} - \theta)I) = (s_{p-1} - \theta)c_0, \quad \text{car} \quad c_0 = cl(I).$$

D'où

$$x_{p+1} = (s_{p-1} - \theta) c_0 x^p \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0 c_p)).$$

On conclut que $Y = X$, ce qui termine la démonstration de la partie (2).

**Remarque.** Dans cette remarque on montre la proposition 3.1.2 lorsque $\Gamma$ est d'exposant $p^2$.

Un calcul analogue à celui de la remarque de la partie (1) nous donne :

$$cl_k(O_{N_1}) = N_{k(\xi)/k}(c_0 c_p x)^{p^2} N_{k(\xi)/k}((s_{p-1} - \theta)c_0)^p.$$

D'où

$$\begin{aligned} cl_k(O_{N_1}) &= N_{k(\xi)/k}(c_0 c_p x)^{p^2} N_{k(\xi)/k}(c_0)^{p(1-p(p-1)/2)} \\ &= N_{k(\xi)/k}(c_0^{(3-p)/2} c_p x)^{p^2} N_{k(\xi)/k}(c_0)^p. \end{aligned}$$

Comme $N_{k(\xi)/k}(\mathcal{S}Cl(k(\xi))) = N_{k(\xi)/k}(Cl(k(\xi)))^{(p-1)/2}$, immédiatement on a $R_m(k,\Gamma,A_{p^2}) \subset N_{k(\xi)/k}(Cl(k(\xi)))^{p(p-1)/2}$ ; pour voir que cette inclusion est en fait une égalité il suffit de prendre $x = 1$ et $c_p = c_0^{(p-3)/2}$, ce qui donne $cl_k(O_{N_1}) = N_{k(\xi)/k}(c_0)^p$, ensuite on fait parcourir $c_0$ dans $\mathcal{S}Cl(k(\xi))$.

D'après [2, Théorême 1.1 ], $R_m(k,\Gamma) = N_{k(\xi)/k}(Cl(k(\xi)))^{p(p-1)/2}$. Donc $R_m(k,\Gamma,A_{p^2}) = R_m(k,\Gamma) = N_{k(\xi)/k}(Cl(k(\xi)))^{p(p-1)/2}$.

# Bibliographie


[1] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, dans : Algèbre et Théorie des Nombres, Colloq. Internat. CNRS, vol. 24, ed. CNRS, Paris 1950, 19–20.

[2] C. Bruche, *Classes de Steinitz d'extensions non abéliennes de degré $p^3$*, Acta Arith. 137.2 (2009) 177–191.

[3] C. Bruche, B. Sodaïgui, *On realizable Galois module classes and Steinitz classes of nonabelian extensions*, J. Number Theory (128) (4) (2008) 954–978.

[4] N. P. Byott, C. Greither, B. Sodaïgui, *Classes réalisables d'extensions non abéliennes*, J. reine angew. Math. 601 (2006) 1–27.

[5] N. P. Byott, B. Sodaïgui, *Realizable Galois module classes for tetrahedral extensions*, Compositio Math. 141 (2005) 573–582.

[6] N. P. Byott, B. Sodaïgui, *Galois module structure for dihedral extensions of degree 8 : realizable classes over the group ring*, J. Number Theory 112 (2005) 1–19.

[7] N. P. Byott, B. Sodaïgui, *Realizable Galois module classes over the group ring for nonabelian extensions*, Ann. Inst. Fourier (Grenoble) (63) (1) (2013) 303–371 (doi : 10.5802/aif.2762).

[8] L. Caputo, A. Cobbe, *An explicit candidate for the set of Steinitz classes of tame Galois extensions with fixed Galois group of odd order*, Proc. Lond. Math. Soc. (3) 107 (2013), no. 2, 391–413.

[9] J. E. Carter, *Characterisations of Galois extensions of prime cubed degree*, Bull. Austral. Math. Soc. (55) (1997) 99–112.

[10] J. E. Carter, B. Sodaïgui, *Classes de Steinitz d'extensions quaterniongiennes généralisées de degreé $4p^r$*, J. London Math. Soc. (2) 76 (2007) 331–344.

[11] A. Cobbe, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, J. Number Theory 130 (2010) 1129–1154.

[12] A. Cobbe, *Steinitz classes of some abelian and nonabelian extensions of even degree*, J. Théor. Nombres Bordeaux 22 (2010), no. 3, 607–628.

[13] A. Cobbe, *Steinitz classes of tamely ramified nonabelian extensions of odd prime power order*, Acta Arith. 149 (2011), no. 4, 347–359.

[14] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer-Verlag, GTM 193, New York, 2000.

[15] C. W. Curtis, I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders*, Vol. II, Wiley-Interscience, New York, 1987.

[16] A. Fröhlich, *The discriminant of relative extensions and the existence of integral bases*, Mathematika 7 (1960), 15–22.

[17] A. Fröhlich, *Galois Module Structure*, in "Algebraic Number Fields", Proceedings of the Durham Symposium, 1975, Academic Press, London (1977), 133–191

[18] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Springer-Verlag, Berlin, 1983.

[19] A. Fröhlich, M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.

[20] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, GTM 77, Springer-Verlag, New York, 1981.

[21] G. James, M. Liebeck, *Representations and Characters of Groups*, second ed., Cambridge University Press, New York, 2001.

[22] R. Long, *Steinitz classes of cyclic extensions of prime degree*, J. reine angew. Math. 250 (1971) 87–98.

[23] J. Martinet, *Sur l'arithmétique d'une extension galoisienne à groupe de Galois diédral d'ordre 2p*, Ann. Inst. Fourier (1969), 1–80.

[24] L. R. McCulloh, *Galois module structure of abelian extensions*, J. reine angew. Math. 375/376 (1987) 259–306.

[25] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

[26] E. Noether, *Normalbasis bei Körpen ohne höhere Verzweigung*, J. reine angew. Math. 167 (1931), 147–152.

[27] I. Reiner, *Maximal Orders*, Academic Press, 1975.

[28] S. Roman, *Coding and Information Theory*, GTM 134, Springer-Verlag, New York, 1992.

[29] F. Sbeity, B. Sodaïgui, *Classes réalisables d'extensions métacycliques de degré lm*, J. Number Theory, 130 (2010) 1818–1834.

[30] J.-P. Serre, *Corps Locaux*, 3ème édition, Hermann, Paris, 1980.

[31] B. Sodaïgui, *Structure galoisienne relative des anneaux d'entiers*, J. Number Theory 28, no.2 (1988) 189–204.

[32] B. Sodaïgui, *"Galois module structure" des extensions quaternioniennes de degré 8*, J. Algebra 213 (1999) 549–556.

[33] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement*, Illinois J. Math. 43, no.1 (1999), 47–60.

[34] B. Sodaïgui, *Realizable Classes of quaternion extensions of degree 4l*, J. Number Theory 80 (2000) 304–315.

[35] B. Sodaïgui, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, J. Algebra 223 (2000) 367–378.

[36] B. Sodaïgui, *Relative Galois module structure of octahedral extensions*, J. Algebra 312 (2007) 590–601.

[37] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes à groupe de Galois un 2-groupe*, Func. Approx. Comment. Math. 48 (2) (2013) 183–196.

[38] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes à groupe de Galois de centre non trivial*, J. Number Theory (133) (2) (2013) 611–619.

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

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

[41] G. Vega, J. Wolfmann, *New classes of 2-weight cyclic codes*, Des Codes Crypt. 42 (2007) 327–334.

[42] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Springer-Verlag, Berlin, 1996.

# Classes de Steinitz, codes cycliques de Hamming et classes galoisiennes réalisables d'extensions non abéliennes de degré $p^3$

La thèse contient deux parties.

Un résumé de la première partie est le suivant. Soient $k$ un corps de nombres et $Cl(k)$ son groupe des classes. Soit $\Gamma$ un groupe fini. Soit $R_m(k,\Gamma)$ le sous-ensemble de $Cl(k)$ formé par les éléments qui sont réalisables par les classes de Steinitz d'extensions galoisiennes de $k$, modérées et dont le groupe de Galois est isomorphe à $\Gamma$. Soit $p$ un nombre premier. Dans la thèse , on suppose que $\Gamma = V \rtimes_\rho C$, où $V$ est un $\mathbb{F}_p$-espace vectoriel de dimension $r \geq 2$, $C$ un groupe cyclique d'ordre $(p^r-1)/(p-1)$ avec $gcd(r, p-1) = 1$ et $\rho$ est une $\mathbb{F}_p$-représentation fidèle et irréductible de $C$ dans $V$. On montre que $R_m(k,\Gamma)$ est un sous-groupe de $Cl(k)$ par l'intermédiaire d'une description explicite et des propriétés d'un code cyclique $p$-aire de Hamming.

Un résumé de la deuxième partie est le suivant. Soient $k$ un corps de nombres et $O_k$ son anneau d'entiers. Soit $p$ un nombre premier impair. Soit $\Gamma$ un groupe non abélien d'ordre $p^3$. Soient $\mathcal{M}$ un $O_k$-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$, et $Cl(\mathcal{M})$ le groupe des classes des $\mathcal{M}$-modules localement libres. On définit l'ensemble $\mathcal{R}(\mathcal{M})$ des classes réalisables comme étant l'ensemble des classes $c \in Cl(\mathcal{M})$ telles qu'il existe une extension $N/k$ modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$, avec la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ égale $c$, où $O_N$ est l'anneau des entiers de $N$. Soit $\xi$ (resp. $\xi_{p^2}$) une racine primitive $p$-ième (resp. $p^2$-ième) de l'unité. Sous l'hypothèse que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes et $k(\xi_{p^2})/k(\xi)$ non ramifiée lorsque $\Gamma$ est d'exposant $p^2$, on définit un sous-ensemble de $Cl(\mathcal{M})$ par l'intermédiaire d'un idéal de Stickelberger, et on montre qu'il est un sous-groupe de $Cl(\mathcal{M})$ contenu dans $\mathcal{R}(\mathcal{M})$.

Mots-clés : Structure de module galoisien ; Anneaux d'entiers ; Classes galoisiennes réalisables ; Classes de Steinitz ; code cyclique de Hamming ; Ordre maximal ; Groupe des classes des modules localement libres ; résolvante de Fröhlich-Lagrange ; Problème de plongement ; Idéal de Stickelberger.

# Steinitz classes, cyclic Hamming codes and realizable Galois module classes of nonabelian extensions of degree $p^3$

The thesis contains two parts.

An abstract for the first part is the following. Let $k$ be a number field and $Cl(k)$ its class group. Let $\Gamma$ be a finite group. Let $R_t(k,\Gamma)$ be the subset of $Cl(k)$ consisting of those classes which are realizable as Steinitz classes of tamely ramified Galois extensions of $k$ with Galois group isomorphic to $\Gamma$. Let $p$ be a prime number. In the thesis, we suppose that $\Gamma = V \rtimes_\rho C$, where $V$ is an $\mathbb{F}_p$-vector space of dimension $r \geq 2$, $C$ a cyclic group of order $(p^r-1)/(p-1)$ with $gcd(r, p-1) = 1$, and $\rho$ a faithful and irreducible $\mathbb{F}_p$-representation of $C$ in $V$. We prove that $R_t(k,\Gamma)$ is a subgroup of $Cl(k)$ by means of an explicit description and properties of a $p$-ary cyclic Hamming code.

An abstract for the second part is the following. Let $k$ be a number field and $O_k$ its ring of integers. Let $p$ be an odd prime number. Let $\Gamma$ be a nonabelian group of order $p^3$. Let $\mathcal{M}$ be a maximal $O_k$-order in the semi-simple algebra $k[\Gamma]$ containing $O_k[\Gamma]$, and $Cl(\mathcal{M})$ its locally free classgroup. We define the set $\mathcal{R}(\mathcal{M})$ of realizable classes to be the set of classes $c \in Cl(\mathcal{M})$ such that there exists a Galois extension $N/k$ which is tame, with Galois group isomorphic to $\Gamma$, and for which the class of $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ is equal to $c$, where $O_N$ is the ring of integers of $N$. Let $\xi$ (resp. $\xi_{p^2}$) be a primitive $p$th (resp. $p^2$th) root of unity. Under the hypothesis that $k/\mathbb{Q}$ and $\mathbb{Q}(\xi)/\mathbb{Q}$ are linearly disjoint and $k(\xi_{p^2})/k(\xi)$ is not ramified when $\Gamma$ has exponent $p^2$, we define a subset of $\mathcal{R}(\mathcal{M})$ by means of a Stickelberger ideal, and prove that it is a subgroup of $Cl(\mathcal{M})$ contained in $\mathcal{R}(\mathcal{M})$.

Keywords : Galois module structure; Ring of integers; Realizable Galois module classes; Steinitz classes; cyclic Hamming codes; Maximal order; Locally free class groups; Fröhlich-Lagrange resolvent; Embedding problem; Stickelberger ideal.

MATHEMATIQUES PURES
Laboratoire de Mathématiques LAMAV, Université de Valenciennes et du Hainaut Cambrésis
Le Mont Houy, 59313 Valenciennes Cedex 9