Classes de Steinitz et classes galoisiennes réalisables d'extensions non abéliennes

Farah Sbeity

N° d'ordre : 10/16

THÈSE

présentée à

L'UNIVERSITÉ DE VALENCIENNES ET DU HAINAUT-CAMBRÉSIS

par **Farah SBEITY**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

Classes de Steinitz et classes galoisiennes réalisables d'extensions non abéliennes

Soutenue le 25 Juin 2010

Composition du jury

Président : Ph. CASSOU-NOGUÈS, Professeur, Université Bordeaux 1
Rapporteurs : N. P. BYOTT, Maître de Conférences, Université d'Exeter (Angleterre)
C. GREITHER, Professeur, Université de Munich (Allemagne)
Examinateurs : J. CARTER, Professeur, Université de Charleston (USA)
J.C. DOUAI, Professeur, Université Lille 1
Directeur de Thèse : B. SODAÏGUI, Maître de Conférences HDR, Université de Valenciennes

Remerciements

Je tiens, en tout premier lieu, à exprimer ma profonde gratitude à Monsieur B. SODAÏGUI, pour avoir accepté la charge de m'encadrer. Il a su me donner une large marge de liberté tout en restant présent pour discuter des problèmes rencontrés, des résultats obtenus et des orientations à suivre tout au long des ces trois années. Je le remercie vivement pour l'aide scientifique précieuse et tous ses conseils qu'il a pu me fournir pendant la durée de ma thèse.

Je tiens aussi à remercier ceux qui m'ont fait l'honneur de juger ce travail : Monsieur le Professeur Ph. CASSOUS-NOGUÈS, Président du Jury, Messieurs les Professeurs N. P. BYOTT et C. GREITHER qui ont assumé la tâche de rapporteurs de cette thèse, ainsi que Messieurs les Professeurs J. CARTER et J.C. DOUAI pour avoir voulu examiner mon travail et participer au Jury.

Mes remerciements iront également à mon pays pour la bourse de thèse dont j'ai bénéficié.

Je ne serai pas arrivé à ce point sans l'aide de ma famille, surtout ma mère. Elle a été toujours présente et d'un soutien sans faille. Je tiens à lui exprimer mon plus grand respect, et à la remercier pour son irremplaçable et inconditionnel soutien, et de tout ce qu'elle a fait pour moi ; sans elle je ne serai pas devenu celui que je suis. Que cette thèse témoigne de mon amour pour elle.

A une personne unique au monde, ma soeur, ma confidente, qui n'a jamais cessé de m'encourager et d'être présente à mes côtés.

Toute mon amitié à Clément Bruche avec qui j'ai partagé le bureau pendant les deux premières années, et avec qui j'ai eu tant de discussions intéressantes.

J'ai une pensée tendre à Alena, qui m'a donné l'espoir d'aller de l'avant.

Aux amis bien sûr qui me sont si chers, spécialement Hicham, Laura et Maria pour l'affectueuse amitié dont ils ont toujours fait preuve, et à tout les autres avec qui j'ai partagé un repas, un café, une sortie : Anil, Bruno, Joao, Mayara, Rodrigo...

Table des matières

Introduction

Soient k un corps de nombres et Γ 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 [15, Chap. I]). 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 Γ.

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 Γ, 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]) 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 Γ est abélien (voir [26]). 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 [46]).

Pour des résultats récents dans la direction de l'étude de la conjecture non abélienne sur les classes réalisables voir [3, 4, 5, 6, 43].

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

Pour ne pas alourdir les notations, on identifiera fréquemment des groupes isomorphes quand c'est faisable sans ambiguïté.

Soit H un groupe fini d'ordre un entier naturel m. Soient l un nombre premier et C un groupe cyclique d'ordre l. Soit μ une représentation $\mathbb{F}_l$-linéaire de H dans C :

$$\mu : H \longrightarrow Aut(C)(\simeq (\mathbb{Z}/l\mathbb{Z})^*),$$

où $(\mathbb{Z}/l\mathbb{Z})^*$ est le groupe des éléments inversibles de $\mathbb{Z}/l\mathbb{Z}$. Notons Γ le produit semi-direct de C et H défini à l'aide de μ :

$$\Gamma = C \rtimes_\mu H.$$

Supposons μ fidèle dans toute la suite. Alors H est cyclique et m divise $l-1$. On peut dire plus (voir [21, p. 12]) : à isomorphisme près, il existe un unique tel groupe Γ et il est isomorphe à l'unique sous-groupe d'ordre lm du groupe affine d'une droite sur $\mathbb{F}_l$. Si $m = l-1$, alors Γ est le groupe affine lui-même. Pour $m = 1$ (resp. $m = 2$), Γ est cyclique (resp. diédral). On peut caractériser ces groupes métacycliques comme étant les groupes résolubles transitifs de degré premier (théorème de Burnside). Le groupe Γ peut être défini par la présentation suivante :

$$\Gamma =< \sigma, \tau : \sigma^l = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^r >,$$

où r est un entier, avec $1 \leq r \leq (l-1)$, et la classe de r dans $(\mathbb{Z}/l\mathbb{Z})^*$ est d'ordre m.

Désormais on suppose $m \neq 1$ (donc $l \neq 2$) de sorte que Γ soit non abélien.

Dans cette thèse, toute extension galoisienne N/k dont le groupe de Galois est isomorphe à Γ est appelée extension métacyclique de degré lm.

Le point de départ du premier travail de cette thèse était la lecture de [21] et une tentative de généralisations des arguments et résultats de [38] (dans [38], Γ est un groupe métacyclique d'ordre lm, avec $m = q$ est un nombre premier, et $k/\mathbb{Q}$ est linéairement disjoint du lq-ième corps cyclotomique sur $\mathbb{Q}$), avec comme objectif la détermination de $\mathcal{R}(\mathcal{M})$ lorsque Γ est un groupe résoluble transitif de degré premier. On n'a pas réussi à atteindre cet objectif, mais on a défini un sous-ensemble $\mathcal{R}_1(\mathcal{M})$ de $\mathcal{R}(\mathcal{M})$ et montré qu'il est un sous-groupe de $Cl^\circ(\mathcal{M})$ sous une certaine hypothèse (voir ci-dessous). (On pourrait consulter [42] pour une démarche analogue.)

Dans toute la suite ξ désigne une racine primitive l-ième de l'unité. On définit $\mathcal{R}_1(\mathcal{M})$ comme étant l'ensemble des classes réalisables des extensions

métacycliques N/k de degré lm, telles que la sous-extension k_1/k de N/k de degré m est linéairement disjointe de $k(\xi)/k$.

Dans cette thèse, on détermine $\mathcal{R}_1(\mathcal{M})$ à l'aide d'un idéal de Stickelberger, et on montre qu'il est un sous-groupe de $Cl^\circ(\mathcal{M})$, sous l'hypothèse que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes.

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

$$k[H] \simeq \prod_{i=0}^{n} k(\chi_i),$$

où $n+1$ est le nombre des classes de conjugaison sur k des caractères absolument irréductibles de H (i.e., les caractères des représentations complexes irréductibles), et pour tout $i \in \{0, 1, ..., n\}$, χ_i est un représentant de l'une de telles classes, χ_0 est le caractère trivial, et $k(\chi_i)$ est l'extension de k obtenue en adjoignant à k les valeurs de χ_i.

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

$$Cl(\mathcal{M}(H)) \simeq \prod_{i=0}^{n} Cl(k(\chi_i)), \quad \text{et donc } Cl^\circ(\mathcal{M}(H)) \simeq \prod_{i=1}^{n} Cl(k(\chi_i)).$$

Soit $\mathcal{R}(\mathcal{M}(H))$ l'ensemble des classes de $Cl(\mathcal{M}(H))$ qui sont réalisables par des extensions galoisiennes de k, modérément ramifiées et dont le groupe de Galois est isomorphe à H. D'après [26], $\mathcal{R}(\mathcal{M}(H))$ est un sous-groupe de $Cl^\circ(\mathcal{M}(H))$ qui peut être décrit par une correspondance de Stickelberger. On identifiera souvent $\mathcal{R}(\mathcal{M}(H))$ avec un sous-groupe de $\prod_{i=1}^{n} Cl(k(\chi_i))$.

Maintenant supposons que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ soient linéairement disjointes de sorte que $Gal(k(\xi)/k) \simeq Gal(\mathbb{Q}(\xi)/\mathbb{Q})$. Soit E_0/k la sous-extension de $k(\xi)/k$ de degré $(l-1)/m$. Soit $\mathcal{M}$ un O_k-ordre maximal dans $k[\Gamma]$ contenant $O_k[\Gamma]$. Dans le chapitre 3, on détermine les classes de conjugaison sur k des caractères absolument irréductibles de Γ, et on montre que

$$Cl^\circ(\mathcal{M}) \simeq \prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(E_0).$$

Nous identifierons fréquemment $Cl^\circ(\mathcal{M})$ avec $\prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(E_0)$ sous l'isomorphisme précédent.

Soit

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

Soit l'élément de Stickelberger

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

et soit l'idéal de Stickelberger

$$\mathcal{S} = (1/l)\theta\mathbb{Z}[S] \cap \mathbb{Z}[S].$$

L'action naturelle de S par restriction sur les idéaux fractionnaires de E_0 induit une structure de $\mathbb{Z}[S]$-module sur $Cl(E_0)$. On note $\mathcal{S}Cl(E_0)$ le sous-groupe de $Cl(E_0)$ engendré par les éléments de la forme $\mathfrak{s}c$, où $\mathfrak{s} \in \mathcal{S}$ et $c \in Cl(E_0)$.

Si K/k est une extension finie de corps de nombres, $N_{K/k}$ désigne la norme dans K/k, et l'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 1. *Soient k un corps de nombres et $\Gamma = C \rtimes_\mu H$. Supposons que la représentation μ soit fidèle, et que les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ soient linéairement disjointes. Soit E_0/k la sous-extension de $k(\xi)/k$ de degré $(l-1)/m$. Alors $\mathcal{R}_1(\mathcal{M})$ est un sous-groupe de $Cl^\circ(\mathcal{M})$, égal au sous-groupe A suivant :*

$$A = \left\{ \left(c_1, c_2, \ldots, c_n, x\phi_{E_0/k}\Big(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)\Big)\right) \Big| \right.$$
$$\left. (c_1, c_2, \ldots, c_n) \in \mathcal{R}(\mathcal{M}(H)), x \in \mathcal{S}Cl(E_0) \right\}.$$

Remarques. (1) On déduit immédiatement de ce théorème que $\mathcal{R}_1(\mathcal{M})$ est isomorphe au groupe produit $\mathcal{R}(\mathcal{M}(H)) \times \mathcal{S}Cl(E_0)$.

(2) Dans le chapitre 3, comme application de ce théorème on retrouve un résultat de L.P. Endo avec une démonstration différente et plus courte, et on corrige [38].

Rappelons la définition de la classe de Steinitz. Soit M un O_k-module de type fini, sans torsion et de rang s. Alors, il existe un idéal I de O_k tel que $M \simeq O_k^{s-1} \oplus I$ 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 s ; on dira alors que $cl_k(O_K)$ est la classe de Steinitz de K/k.

Une autre partie de cette thèse est l'étude des classes de Steinitz dans le cadre défini ci-dessous.

Soit Γ un groupe fini. 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 Γ, 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^Γ : $Cl(O_k[\Gamma]) \to Cl(k)$ 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]) que $R_m(k,\Gamma)$ est un sous-groupe de $Cl(k)$; signalons que cela est vrai lorsque Γ est abélien puisque $\mathcal{R}(O_k[\Gamma])$ est un sous-groupe de $Cl(O_k[\Gamma])$ (d'après [26]). L'étude de la structure de $R_m(k,\Gamma)$ (voir par exemple [2, 3, 4, 7, 8, 39, 41]), qui est intéressante en elle-même, peut être vue aussi comme une étape de l'étude de celle de $\mathcal{R}(O_k[\Gamma])$.

Les résultats de [5, 6] 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, 40, 41, 42, 43]) se fait, en partie, grâce à la résolution d'un problème de plongement en lien avec la donnée de classes de Steinitz.

L'autre partie de la thèse consiste en l'étude de $R_m(k,\Gamma)$ et d'un problème de plongement en liaison avec la donnée de classes de Steinitz, dans la situation non abélienne, dans le cas où Γ est un groupe non abélien d'ordre 16, ou un groupe extraspécial d'ordre 32. (En ce qui concerne les 2-groupes non abéliens, signalons qu'une étude similaire a été faite lorsque Γ est le groupe quaternionien (resp. diédral) d'ordre 8 dans [39] (resp. [41]).)

A isomorphisme près, il y a quatorze groupes d'ordre 16 dont neuf sont non abéliens (voir par exemple [18, 19, 23]).

Soient p un nombre premier et G un p-groupe. On rappelle qu'on dit que G est un groupe extraspécial si son centre et son groupe dérivé $[G,G]$ (engendré par les commutateurs) sont égaux et leur ordre est p. Les groupes non abéliens d'ordre p^3 sont des exemples de tels groupes ; en particulier un groupe diédral (resp. quaternionien) d'ordre 8 est un groupe extraspécial. Il est bien connu que, à isomorphisme près, il existe deux groupes extraspéciaux d'ordre 32.

Ci-dessous, nous utiliserons l'abréviation "modéré" pour signifier "modérément ramifié".

Dans le chapitre 2 on démontre le résultat suivant.

Théorème 2. *Soient k un corps de nombres et ξ_4 une racine primitive 4ème de l'unité. Soit Γ un groupe non abélien d'ordre 16, ou un groupe extraspécial d'ordre 32. Lorsque Γ est le groupe modulaire d'ordre 16, on suppose que $\xi_4 \in k$. Alors :*

(i) Pour tout $c \in Cl(k)$, il existe une extension quadratique de k, modérée, dont la classe de Steinitz est c, et qui est plongeable dans une extension galoisienne de k, modérée et à groupe de Galois isomorphe à Γ.

(ii) Supposons le nombre des classes de k impair. Alors $R_m(k,\Gamma)$ est un sous-groupe de $Cl(k)$ égal à $Cl(k)$.

Remarques. (1) Il résulte de l'assertion (i) du théorème précédent qu'on a : pour tout corps de nombres k, tout groupe extraspécial d'ordre 32, ou non abélien d'ordre 16 distinct du groupe modulaire d'ordre 16 est réalisable comme groupe de Galois d'une extension galoisienne modérée sur k ; cette conséquence du théorème 2 est valable pour M_{16} en supposant $\xi_4 \in k$.

(2) Un résultat similaire au théorème 2.(i) lorsque Γ est le groupe quaternionien (resp. diédral) d'ordre 8 est obtenu dans [39, Corollaire 5.4, p. 58] (resp. [41, Theorem (1.3)(i), p. 369]).

(3) Soit Γ un groupe non abélien d'ordre 8. Supposons le nombre des classes de k impair. On démontre que $R_m(k,\Gamma) = Cl(k)$ lorsque Γ est le groupe quaternionien (resp. diédral) dans [39, Théorème 1.1 (ii), p. 48] (resp. [41, Theorem (1.3)(ii), p. 369]).

Le plan de cette thèse est le suivant.

Le premier chapitre contient des définitions et des résultats nécessaires pour les preuves des théorèmes 1 et 2.

Le deuxième chapitre est consacré à l'étude des classes de Steinitz d'extensions non abéliennes à groupe de Galois d'ordre 16, ou extraspécial d'ordre 32 ; dans ce chapitre, on démontre le théorème 2.

Dans le troisième chapitre, on démontre le théorème 1.

Chapitre 1

Préliminaires

Notations

Dans toute la suite de la thèse, le groupe multiplicatif des éléments inversibles d'un corps k sera noté $k^\times = k \setminus \{0\}$. 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 Γ un groupe fini. Un O_k-ordre dans l'algèbre semi-simple $k[\Gamma]$ est un sous-anneau Λ 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 Λ-module X est dit localement libre si c'est un Λ-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 Λ-modules localement libres est le groupe abélien dont les générateurs sont les classes d'isomorphismes (X) des Λ-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 (Λ^n) du Λ-module libre Λ^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 [15, 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 Γ un caractère irréductible d'une représentation $T : \Gamma \to GL_n(\mathbb{C})$. On désigne par R_Γ le groupe abélien libre engendré par les caractères absolument irréductibles de Γ (appelé aussi le groupe des caractères virtuels de Γ).

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

Définition 1.1.1. *Deux caractères absolument irréductibles χ et φ de Γ 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 Γ. Pour tout $i \in \{1, \ldots, r\}$, notons χ_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 χ_i.

La décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante (voir [11, 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 $\mathfrak{Cl}(k(\chi_i))$ le groupe des classes de $k(\chi_i)$, au sens restreint suivant : $\mathfrak{Cl}(k(\chi_i))$ 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 [32, Definition 38.1, p. 343–344 ; Definition 34.3, p. 294]).

Nous rappelons le théorème de Swan suivant (voir [45] ou [32, 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*

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

Remarque. Supposons que pour tout i, $1 \leq i \leq r$, χ_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 χ 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 [15] ou [11, §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 Γ.

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 χ_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 $\mathfrak{Cl}(k(\chi_i))$. 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 Γ. Si π est un isomorphisme défini sur $Gal(N/k)$ et à valeurs dans Γ, alors tout caractère χ de Γ induit un caractère $\chi \circ \pi$ de $Gal(N/k)$ que l'on notera aussi χ. Si $\gamma \in \Gamma$, nous noterons $\pi^{-1}(\gamma) \in Gal(N/k)$ simplement par γ. Soit B une k-algèbre commutative. En faisant agir Γ 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 Γ de caractère χ.

Définition 1.2.1. *Soit $a \in N \otimes_k B$. On appelle résolvante de Fröhlich-Lagrange de a et de χ, 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 χ 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 [30] ou [15, Chap. I, §3]).

Théorème 1.2.2. *[15, p. 30] Soit N/k une extension galoisienne modérément ramifiée, à groupe de Galois isomorphe à Γ. 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 α 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 [29, 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 [47, 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 [17, Theorem 13, p. 95], ou [9, 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 [24]), 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 $cl_k(O_K) = cl(\Delta(K/k)^{1/2})$.

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 [17]). L'assertion (ii) est le théorème 4.1 de [12].

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 (voir [17, (2.13), p. 124, et début p. 125]). 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 $\Delta(K_1K_2/K_2) = \Delta(K_1/k)O_{K_2}$.*

Soit $m \in k^\times$, il est clair qu'on peut écrire de manière unique :

$$mO_k = I(m)^2 J,$$

où $I(m)$ un idéal fractionnaire de O_k, et J est un idéal entier de O_k sans facteur carré.

Soit K/k une extension quadratique. D'après la théorie de Kummer (voir [20, §39], ou [9, §10.2]), K/k est modérément ramifiée si, et seulement si, on peut choisir $x \in k^\times$ tel que :

$$K = k(\sqrt{x}) \text{ et } x \equiv 1 \ mod^* \ 4O_k,$$

dans ce cas, pour tout $m \in k^\times$ tel que $K = k(\sqrt{m})$, on peut écrire de manière unique :

$$mO_k = I(m)^2 \Delta(K/k),$$

et par le théorème d'Artin ci-dessus on a :

$$cl_k(O_K) = cl(I(m)^{-1}).$$

Maintenant soit K/k une extension galoisienne dont le groupe de Galois est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^r$, où r est un entier naturel non nul. Soient k_i/k, $1 \leq i \leq 2^r - 1$, les sous-extensions quadratiques de K/k. Alors (voir [4, Lemme 3.4, et le début de sa preuve]) :

$$\Delta(K/k) = \prod_{i=1}^{2^r-1} \Delta(k_i/k), \quad cl_k(O_K) = \prod_{i=1}^{2^r-1} cl_k(O_{k_i}).$$

1.5 Algèbre des quaternions et symboles locaux

Soient $a, b \in k^\times$. On désigne par $(\frac{a,b}{k})$ l'algèbre des quaternions sur k définie par a et b, et l'on note (a, b) sa classe dans le groupe de Brauer $Br(k)$ de k. Rappelons que $(a, b)^2 = 1$ dans $Br(k)$, et que $(a, b) = 1$ dans $Br(k)$, si, et seulement si, la forme quadratique $< a, b >$ sur k représente 1 ; condition équivalente à b est une norme dans l'extension $k(\sqrt{a})/k$ (voir par exemple [22, Theorem 2.7, p. 58, et Chapter IV, §1]).

Soient v une place de k et $a, b \in k^\times$, $(a, b)_v$ est le symbole (local) de Hilbert (voir [34, Chapitre XIV, cas $n = 2$]). Rappelons que $(a, b)_v = 1$ ou -1, et pour que $(a, b)_v = 1$, il faut et il suffit que la forme quadratique $< a, b >$ sur le complété k_v de k représente 1 ; condition équivalente à b est une norme (locale) dans l'extension $k_v(\sqrt{a})/k_v$. La formule du produit nous dit qu'on a : $\prod_{v \text{ place de } k}(a, b)_v = 1$.

Le théorème de Hasse-Minkowski (voir par exemple [22, Corollary 3.2, Chapter VI, §3, p. 168]) affirme qu'une forme quadratique $< a, b >$ sur k représente un élément x de k si, et seulement si, pour toute place v de k, la forme quadratique $< a, b >$ sur le complété k_v de k représente x. Donc : pour que $(a, b) = 1$, il faut et il suffit que pour toute place v de k, $(a, b)_v = 1$.

Dans ce qui suit, on rappelle aussi les calculs explicites du symbole $(a, b)_v$.

Si v est complexe, alors $(a,b)_v = 1$. Si v est réelle, alors $(a,b)_v = 1$ si, et seulement si, $v(a) > 0$ ou $v(b) > 0$.

Soit $\mathfrak{p}$ un idéal premier de O_k. Soit $k_\mathfrak{p}$ le complété de k en la place $\mathfrak{p}$, et notons $\overline{k_\mathfrak{p}}$ son corps résiduel.

Soit

$$c = (-1)^{v_\mathfrak{p}(a)v_\mathfrak{p}(b)} a^{v_\mathfrak{p}(b)} b^{-v_\mathfrak{p}(a)},$$

et soit $\overline{c}$ la classe de c dans $\overline{k_\mathfrak{p}}$. Supposons que $\mathfrak{p}$ ne soit pas au dessus de 2. Alors (voir [34, Proposition 8 et son corollaire, p. 217]) :

$$(a,b)_\mathfrak{p} = \overline{c}^{(N_{k/\mathbb{Q}}(\mathfrak{p})-1)/2}.$$

Supposons maintenant que $\mathfrak{p}$ soit au dessus de 2, et soit $e = v_\mathfrak{p}(2O_k)$ son indice de ramification absolu. Si $v_\mathfrak{p}(b-1) \geq 2e$, alors (voir [34, Proposition 6, p. 237])

$$(a,b)_\mathfrak{p} = (-1)^{v_\mathfrak{p}(a)m(b)}, \text{ avec } m(b) = Tr_{\overline{k_\mathfrak{p}}/\mathbb{F}_2}(\overline{(b-1)/4}),$$

où Tr désigne la trace, $\mathbb{F}_2$ est le corps à deux éléments, et $\overline{(b-1)/4}$ est la classe de $(b-1)/4$ dans $\overline{k_\mathfrak{p}}$.

Chapitre 2

Classes de Steinitz d'extensions non abéliennes à groupe de Galois d'ordre 16 ou extraspécial d'ordre 32

2.1 Préliminaires

Soient Γ un groupe fini et k un corps de nombres. Rappelons que $R_m(k,\Gamma)$ désigne l'ensemble des classes $c \in Cl(k)$ telles qu'il existe une extension galoisienne et modérément ramifiée N/k, avec $Gal(N/k) \simeq \Gamma$, et dont la classe de Steinitz est c.

Le but de ce chapitre est l'étude de $R_m(k,\Gamma)$ et d'un problème de plongement en liaison avec la donnée de classes de Steinitz, dans la situation non abélienne, dans le cas où Γ est un groupe non abélien d'ordre 16, ou un groupe extraspécial d'ordre 32. (En ce qui concerne les 2-groupes non abéliens, signalons qu'une étude similaire a été faite lorsque Γ est le groupe quaternionien (resp. diédral) d'ordre 8 dans [39] (resp. [41]).)

A isomorphisme près, il y a quatorze groupes d'ordre 16 dont neuf sont non abéliens (voir par exemple [18, 19, 23]).

Soient p un nombre premier et G un p-groupe. On rappelle qu'on dit que G est un groupe extraspécial si son centre et son groupe dérivé $[G,G]$ (engendré par les commutateurs) sont égaux et leur ordre est p. Les groupes non abéliens d'ordre p^3 sont des exemples de tels groupes ; en particulier un groupe diédral (resp. quaternionien) d'ordre 8 est un groupe extraspécial. Il est bien connu que tout groupe extraspécial est un produit central de n non abéliens sous-groupes d'ordre p^3, son ordre est p^{1+2n}, et, à isomorphisme près,

il existe deux groupes extraspéciaux d'ordre p^{1+2n} (voir [33, 5.3.8 et Exercice 5.3.7, p. 141]). Il y a donc, à isomorphisme près, deux groupes extraspéciaux d'ordre 32.

Dans toute la suite, on identifiera souvent des groupes isomorphes quand c'est faisable sans ambiguïté, et l'on désignera par C (resp. D, resp. Q) le groupe cyclique (resp. diédral, resp. quaternionien) d'ordre 4 (resp. 8, resp. 8).

Les groupes non abéliens d'ordre 16 sont (voir [18, 19, 23]) :

- Les produits directs $D \times (\mathbb{Z}/2\mathbb{Z})$ et $Q \times (\mathbb{Z}/2\mathbb{Z})$.
- Le groupe, noté DC, produit central de D et C, défini par la présentation :

$$DC = \langle \sigma, \tau, \nu : \sigma^2 = \tau^2 = \nu^4 = 1, \tau\sigma\tau^{-1} = \sigma\nu^2, [\sigma, \nu] = [\tau, \nu] = 1 \rangle.$$

- Le groupe $D \curlywedge C$ isomorphe au produit semidirect $(C \times (\mathbb{Z}/2\mathbb{Z})) \rtimes (\mathbb{Z}/2\mathbb{Z})$:

$$D \curlywedge C = \langle \sigma, \tau, \nu : \sigma^4 = \tau^2 = \nu^2 = 1, \tau\sigma\tau^{-1} = \sigma\nu, [\sigma, \nu] = [\tau, \nu] = 1 \rangle.$$

- Le groupe $Q \curlywedge C$ isomorphe au produit semidirect $C \rtimes C$:

$$Q \curlywedge C = \langle \sigma, \tau : \sigma^4 = \tau^4 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle.$$

- Le groupe diédral d'ordre 16 : D_{16} :

$$D_{16} = \langle \sigma, \tau : \sigma^8 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle.$$

- Le groupe semidiédral d'ordre 16 : SD_{16} :

$$SD_{16} = \langle \sigma, \tau : \sigma^8 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^3 \rangle.$$

- Le groupe modulaire d'ordre 16 : M_{16} :

$$M_{16} = \langle \sigma, \tau : \sigma^8 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^5 \rangle.$$

- Le groupe quaternionien d'ordre 16 : Q_{16} :

$$Q_{16} = \langle \sigma, \tau : \sigma^8 = \tau^4 = 1, \tau\sigma\tau^{-1} = \sigma^{-1}, \sigma^4 = \tau^2 \rangle.$$

Les deux groupes extraspéciaux d'ordre 32 sont (voir [35]) :

- Le groupe, noté DD, produit central de D et D, défini par la présentation :

$$DD = \langle \sigma, \tau, \mu, \nu : \sigma^2 = \tau^2 = \mu^2 = \nu^2 = [\sigma, \tau]^2 = [\mu, \nu]^2 = 1, [\sigma, \tau] = [\mu, \nu] \text{ central d'ordre } 2, [\sigma, \mu] = [\sigma, \nu] = [\tau, \mu] = [\tau, \nu] = 1 \rangle.$$

- Le groupe, noté DQ, produit central de D et Q, défini par la présentation :

$$DQ = \langle \sigma, \tau, \mu, \nu : \sigma^2 = \tau^2 = \mu^4 = \nu^4 = [\sigma,\tau]^2 = [\mu,\nu]^2 = 1, [\sigma,\tau] = [\mu,\nu] = \mu^2 = \nu^2 \text{ central d'ordre } 2,\ [\sigma,\mu] = [\sigma,\nu] = [\tau,\mu] = [\tau,\nu] = 1\rangle.$$

Remarque. Nous n'utiliserons pas les présentations précédentes pour la démonstration de nos résultats, mais nous les avons données pour la convenance du lecteur.

Soit N/k une extension galoisienne à groupe de Galois un 2-groupe. Il est immédiat que N/k est modérément ramifiée si, et seulement si, les idéaux premiers de O_k au dessus de 2 ne sont pas ramifiés dans N/k.

Dans toute la suite, nous utiliserons souvent l'abréviation "modéré" pour signifier "modérément ramifié".

Les principaux résultats de ce chapitre sont les théorèmes suivants.

Théorème 2.1.1. *Soient k un corps de nombres et ξ_4 une racine primitive 4ème de l'unité. Soit Γ un groupe non abélien d'ordre 16, ou un groupe extraspécial d'ordre 32. Lorsque Γ est le groupe modulaire M_{16}, on suppose que $\xi_4 \in k$. Alors pour tout $c \in Cl(k)$, il existe une extension quadratique de k, modérée, dont la classe de Steinitz est c, et qui est plongeable dans une extension galoisienne de k, modérée et à groupe de Galois isomorphe à Γ.*

Remarques. (1) Il résulte du théorème précédent qu'on a : pour tout corps de nombres k, tout groupe extraspécial d'ordre 32, ou non abélien d'ordre 16 distinct de M_{16} est réalisable comme groupe de Galois d'une extension galoisienne modérée sur k ; cette conséquence du théorème 2.1.1 est valable pour M_{16} en supposant $\xi_4 \in k$.

(2) Un résultat similaire au théorème 2.1.1 lorsque Γ est le groupe quaternionien (resp. diédral) d'ordre 8 est obtenu dans [39, Corollaire 5.4, p. 58] (resp. [41, Theorem (1.3)(i), p. 369]).

Théorème 2.1.2. *Soient k un corps de nombres et Γ un groupe non abélien d'ordre 16, ou un groupe extraspécial d'ordre 32. Lorsque Γ est le groupe modulaire M_{16}, on suppose que $\xi_4 \in k$. Supposons le nombre des classes de k impair. Alors $R_m(k,\Gamma)$ est un sous-groupe de $Cl(k)$ égal à $Cl(k)$.*

Remarque. Soit Γ un groupe non abélien d'ordre 8. Supposons le nombre des classes de k impair. On démontre que $R_m(k,\Gamma) = Cl(k)$ lorsque Γ est le

groupe quaternionien (resp. diédral) dans [39, Théorème 1.1 (ii), p. 48] (resp. [41, Theorem (1.3)(ii), p. 369]).

Soit k un corps de nombres. Soient $a, b \in k^\times$. Rappelons (voir Chap. 1, §1.5) que $(\frac{a,b}{k})$ est l'algèbre des quaternions sur k définie par a et b et que (a, b) désigne sa classe dans le groupe de Brauer $Br(k)$ de k.

Les assertions suivantes sont bien connues (voir par exemple [18, 19, 23]) :

- Soit $E = k(\sqrt{a})/k$ une extension quadratique. Alors E est plongeable dans une extension à groupe de Galois C si, et seulement si, $(-1, a) = 1$.

Soit $E = k(\sqrt{a}, \sqrt{b})/k$ une extension biquadratique. Alors :

- E est plongeable dans une extension à groupe de Galois D cyclique sur $k(\sqrt{ab})$ si, et seulement si, $(a, b) = 1$.

- E est plongeable dans une extension à groupe de Galois Q si, et seulement si, $(-1, a)(-1, b)(a, b) = 1$.

Nous avons utilisé les références [18, 19, 23, 35, 36] pour énoncer les conditions suffisantes de plongements $(2.i)$, $1 \leq i \leq 9$, (voir ci-dessous) dans la manière qui nous convient pour démontrer nos propres résultats. Signalons qu'on peut énoncer des conditions nécessaires de plongements (au prix de quelques complications) intéressantes en elles-mêmes mais inutiles pour les démonstrations de nos théorèmes.

Soit E/k une extension galoisienne à groupe de Galois D. Soit $k(\sqrt{a}, \sqrt{b})/k$ sa sous-extension biquadratique de sorte que $E/k(\sqrt{ab})$ soit cyclique ; donc $(a, b) = 1$. Alors :

(2.1) : E/k est plongeable dans une extension à groupe de Galois $D \curlywedge C$ si $(-1, a) = 1$ (voir [23, Example 4.6, p. 1267], [18, Proposition 1 (6)]).

(2.2) : E/k est plongeable dans une extension à groupe de Galois D_{16} s'il existe $x \in k^\times$ tel que $(a, 2)(x, -ab) = 1$ (voir [23, Example 4.3, p. 1266], [18, Proposition 1 (7)]).

(2.3) : E/k est plongeable dans une extension à groupe de Galois SD_{16} s'il existe $x \in k^\times$ tel que $(a, -2)(x, -ab) = 1$ (voir [23, Example 4.1, p. 1265], [18, Proposition 1 (9)]).

(2.4) : E/k est plongeable dans une extension à groupe de Galois Q_{16} s'il existe $x \in k^\times$ tel que $(a, 2)(x, -ab)(-1, ab) = 1$ (voir [23, Example 4.4, p. 1266], [18, Proposition 1 (8)]).

Soit E/k une extension galoisienne à groupe de Galois Q. Soit $k(\sqrt{a}, \sqrt{b})/k$ sa sous-extension biquadratique de sorte que $(-1, a)(-1, b)(a, b) = 1$. Alors :

(2.5) : E/k est plongeable dans une extension à groupe de Galois $Q \curlywedge C$ si $(-1, a) = 1$ (voir [18, Proposition 1 (5)]).

Soit $E = k(\sqrt{a}, \sqrt{b}, \sqrt{c})$ une extension galoisienne de k, à groupe de Galois isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$. Alors

(2.6) : E/k est plongeable dans une extension à groupe de Galois DC si $(a,b)(-1,c) = 1$ (voir [18, Proposition 1 (4)] ; voir [36, Corollary 1.3 (iv)], c'est un corollaire de [36, Theorem 1.2] qui est un rappel de [16, (7.6), p. 106])

Soit E/k une extension galoisienne de k, à groupe de Galois isomorphe à $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$; c'est une composée d'une extension K/k cyclique de degré 4 et d'une extension quadratique $k(\sqrt{b})/k$ (non contenue dans K). Soit $k(\sqrt{a})/k$ la sous-extension quadratique de K de sorte que $(-1,a) = 1$ (condition équivalente à a est somme de deux carrées dans k). Soient a_1, $a_2 \in k^\times$ tels que $a = a_1^2 + a_2^2$. Posons $a_0 = a/a_1^2$. Il n'est pas difficile de voir que toute extension cyclique de k, de degré 4 et contenant $k(\sqrt{a})$ peut s'écrire sous la forme $k(\sqrt{r(a_0 + \sqrt{a_0})})$, où $r \in k^\times$. Il est clair que $k(\sqrt{a}) = k(\sqrt{a_0})$, et pour tout $y \in k^\times$, $(a_0, y) = (a, y)$. Soit $x \in k^\times$ tel que $K = k(\sqrt{x(a_0 + \sqrt{a_0})})$. Alors (voir [23, Example 3.3, p. 1262]) et [18, Proposition 1 (10)]) :

(2.7) : E/k est plongeable dans une extension à groupe de Galois M_{16} si $(a, 2b)(-1, x) = 1$.

Soit $E = k(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$ une extension galoisienne de k, à groupe de Galois isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$. Alors (voir [35, Proposition 2.1] ; cette proposition est une conséquence de [16, (7.6), p. 106])

(2.8) : E/k est plongeable dans une extension à groupe de Galois DD si $(a,b)(c,d) = 1$.

(2.9) : E/k est plongeable dans une extension à groupe de Galois DQ si $(-1,a)(-1,b)(a,b)(c,d) = 1$.

Enfin, soit E/k une extension galoisienne à groupe de Galois D (resp. Q). Il est clair qu'il suffit de composer E/k avec une extension quadratique de k, linéairement disjointe de E/k, pour la plonger dans une extension galoisienne à groupe de Galois $D \times (\mathbb{Z}/2\mathbb{Z})$ (resp. $Q \times (\mathbb{Z}/2\mathbb{Z})$).

Signalons que, dans tous les cas précédents (incluant $\Gamma = C$, D ou Q), il s'agit d'un problème de plongement (central) associé à l'extension centrale (scindée seulement dans les cas : $\Gamma = D \times (\mathbb{Z}/2\mathbb{Z})$, ou $Q \times (\mathbb{Z}/2\mathbb{Z})$) :

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \Gamma \to Gal(E/k) \to 1.$$

Comme cette extension est à noyau abélien, si l'on suppose E/k modérée, et si le problème de plongement a une solution, alors il en existe une modérée sur k par [28, Théorème 6.6].

2.2 Démonstration des résultats principaux

Dans cette section nous démontrons les théorèmes 2.1.1 et 2.1.2.

Démonstration du théorème 2.1.1 . Soit $c_1 \in Cl(k)$. Soit $\mathcal{C}_\infty = \prod_{v(k)\subset\mathbb{R}} v$, où v parcourt l'ensemble des places infinies réelles de k. Considérons c_1^{-1} et le cycle $\mathcal{C}_\infty 8O_k$. D'après le théorème de densité de Tchebotarev (Théorème 1.3.3) et la surjection canonique de $Cl(k, \mathcal{C}_\infty 8O_k)$ sur $Cl(k)$ (Proposition 1.3.4), qui à $cl(I)$ dans $Cl(k, \mathcal{C}_\infty 8O_k)$ associe $cl(I)$ dans $Cl(k)$, il existe un idéal fractionnaire I_1 de O_k dans c_1^{-1} tel que I_1 est premier à $2O_k$, et un idéal premier $\mathfrak{p}_1$ de O_k ne divisant pas $2O_k$ vérifiant $cl(I_1)^{-2} = Cl(\mathfrak{p}_1)$ dans $Cl(k, \mathcal{C}_\infty 8O_k)$. Par conséquent, il existe $a \in k$ tel que :

$$aO_k = I_1^2\mathfrak{p}_1,\ a \equiv\ 1\ mod^*\ \mathcal{C}_\infty 8O_k,\ c_1 = cl(I_1)^{-1}.$$

Il est clair que $k(\sqrt{a})/k$ est quadratique ($v_{\mathfrak{p}_1}(a) = 1$). Par la théorie de Kummer elle est modérée de discriminant $\Delta(k(\sqrt{a})/k) = \mathfrak{p}_1$, et par le théorème d'Artin sa classe de Steinitz $cl_k(O_{k(\sqrt{a})})$ est égale à c_1 (voir Chap. 1, §1.4) :

$$\Delta(k(\sqrt{a})/k) = \mathfrak{p}_1,\ cl_k(O_{k(\sqrt{a})}) = c_1.$$

Soit $c_2 \in Cl(k)$. En considérant c_2^{-1} et le cycle $\mathcal{C}_\infty 4\mathfrak{p}_1$, et en procédant comme ci-dessus on obtient : il existe un idéal premier $\mathfrak{p}_2$ de O_k ne divisant pas $2\mathfrak{p}_1$, un idéal fractionnaire I_2 de O_k premier à $\mathfrak{p}_1$ et un élément b de $k^\times$ tels que :

$$bO_k = I_2^2\mathfrak{p}_2,\ b \equiv\ 1\ mod^*\ \mathcal{C}_\infty 4\mathfrak{p}_1,\ c_2 = cl(I_2)^{-1}.$$

Il est immédiat que l'extension $k(\sqrt{b})/k$ est une extension quadratique modérée,

$$\Delta(k(\sqrt{b})/k) = \mathfrak{p}_2,\ cl_k(O_{k(\sqrt{b})}) = c_2,$$

et est distincte de $k(\sqrt{a})/k$. Donc $k(\sqrt{a}, \sqrt{b})/k$ est une extension biquadratique modérée car c'est une composée de deux extensions modérées.

La 3ème sous-extension quadratique $k(\sqrt{ab})/k$ de $k(\sqrt{a}, \sqrt{b})$ est évidemment modérée. De l'unicité de la décomposition $abO_k = (I_1I_2)^2\mathfrak{p}_1\mathfrak{p}_2$ on tire :

$$\Delta(k(\sqrt{ab})/k) = \mathfrak{p}_1\mathfrak{p}_2.$$

Comme (voir Chap. 1, fin §1.4)

$$\Delta(k(\sqrt{a}, \sqrt{b})/k) = \Delta(k(\sqrt{a})/k)\Delta(k(\sqrt{b})/k)\Delta(k(\sqrt{ab})/k),$$

on obtient :

$$\Delta(k(\sqrt{a}, \sqrt{b})/k) = (\mathfrak{p}_1\mathfrak{p}_2)^2.$$

Nous allons montrer les assertions suivantes :

$$(-1, a) = 1,\ (-1, b) = 1,\ (a, b) = 1,\ (a, 2) = 1.$$

Soit v une place archimédienne de k. Si v est complexe, alors $(-1,a)_v = (-1,b)_v = (a,b)_v = (a,2)_v = 1$. Si v est réelle, $(-1,a)_v = (-1,b)_v = (a,b)_v = (a,2)_v = 1$ car a et b sont totalement positifs par les congruences $(mod^*\ C_\infty)$ qu'ils vérifient.

Soit $v = \mathfrak{p}$ une place non archimédienne de k.

Si $\mathfrak{p}$ est au dessus de 2 et e son indice de ramification absolu, les congruences que vérifient a et b entraînent : $v_\mathfrak{p}(a-1) \geq v_\mathfrak{p}(8O_k) = 3e$ et $v_\mathfrak{p}(b-1) \geq v_\mathfrak{p}(4O_k) = 2e$. Donc (voir (voir Chap. 1, §1.5) :

$$(-1,a)_\mathfrak{p} = (-1)^{v_\mathfrak{p}(-1)m(a)},\ (-1,b)_\mathfrak{p} = (-1)^{v_\mathfrak{p}(-1)m(b)},\ (a,b)_\mathfrak{p} = (-1)^{v_\mathfrak{p}(a)m(b)},$$

et

$$(a,2)_\mathfrak{p} = (2,a)_\mathfrak{p} = (-1)^{v_\mathfrak{p}(2)m(a)}.$$

Les trois premiers symboles sont tous égaux à 1, car $v_\mathfrak{p}(a) \equiv v_\mathfrak{p}(-1) \equiv 0\ mod\ 2$. Il est immédiat que $v_\mathfrak{p}((a-1)/4) \geq e$. Donc la classe de $(a-1)/4$ dans le corps résiduel $\overline{k_\mathfrak{p}}$ est égale à 0. Par suite $m(b) = 0$ dans $\mathbb{F}_2$, et donc $(a,2)_\mathfrak{p} = 1$.

Supposons maintenant que $\mathfrak{p}$ ne soit pas au dessus de 2.

Si $\mathfrak{p} \neq \mathfrak{p}_1$, alors $(-1,a)_\mathfrak{p} = 1$ car $v_\mathfrak{p}(a)$ est paire. Par la formule du produit on a $(-1,a)_{\mathfrak{p}_1} = 1$. On en déduit que pour toute place v de k, $(-1,a)_v = 1$. Il s'ensuit que $(-1,a) = 1$.

Si $\mathfrak{p} \neq \mathfrak{p}_2$, alors $(-1,b)_\mathfrak{p} = 1$ car $v_\mathfrak{p}(b)$ est paire. Par la formule du produit on a $(-1,b)_{\mathfrak{p}_2} = 1$. Donc (comme ci-dessus) $(-1,b) = 1$.

Si $\mathfrak{p} \neq \mathfrak{p}_1$ et $\mathfrak{p} \neq \mathfrak{p}_2$, alors $(a,b)_\mathfrak{p} = 1$ car $v_\mathfrak{p}(a)$ et $v_\mathfrak{p}(b)$ sont paires. Si $\mathfrak{p} = \mathfrak{p}_1$, alors $(a,b)_{\mathfrak{p}_1} = (\overline{b})^{-v_{\mathfrak{p}_1}(a)(N_{k/\mathbb{Q}}(\mathfrak{p})-1)/2}$ dans $\overline{k_{\mathfrak{p}_1}}$, car $v_{\mathfrak{p}_1}(b) = 0$ (rappelons que I_2 est premier à $\mathfrak{p}_1$). On a $(a,b)_{\mathfrak{p}_1} = 1$ car $\overline{b} = 1$ dans $\overline{k_{\mathfrak{p}_1}}$ par la congruence $(mod^*\ \mathfrak{p}_1)$ qu'il vérifie. La formule du produit nous donne $(a,b)_{\mathfrak{p}_2} = 1$. Par conséquent $(a,b) = 1$.

Puisque $v_\mathfrak{p}(2) = 0$, $(a,2)_\mathfrak{p} = (\overline{2})^{-v_\mathfrak{p}(a)(N_{k/\mathbb{Q}}(\mathfrak{p})-1)/2}$. Si $\mathfrak{p} \neq \mathfrak{p}_1$, alors $(a,2)_\mathfrak{p} = 1$ car $v_\mathfrak{p}(a)$ est paire. Par la formule du produit on a $(a,2)_{\mathfrak{p}_1} = 1$. On conclut que $(a,2) = 1$. Ceci termine la démonstration des assertions énoncées.

Comme $(a,b) = 1$, l'extension biquadratique $k(\sqrt{a},\sqrt{b})/k$ est plongeable dans une extension diédrale E_1/k à groupe de Galois isomorphe à D (cyclique sur $k(\sqrt{ab})$), que l'on peut choisir modérée (par [28, Théorème 6.6]). (Remarque : ceci nous donne une partie de [41, Theorem 1.3.(i)].) Soit $k(\sqrt{a'})/k$ une extension quadratique modérée, linéairement disjointe de E_1/k, alors la composée de E_1/k et $k(\sqrt{a'})/k$ est galoisienne modérée, à groupe de Galois $D \times (\mathbb{Z}/2\mathbb{Z})$. Une telle extension $k(\sqrt{a'})/k$ existe, en effet : par exemple, il suffit de reprendre le début de la démonstration du théorème 2.1.1 en oubliant C_∞ (on en a pas besoin) et en remplaçant $8O_k$ par $4O_k$; on sait qu'il

existe une infinité d'idéaux premiers $\mathfrak{p}$ de O_k tel que $cl(I_1)^{-2} = Cl(\mathfrak{p})$ dans $Cl(k, 4O_k)$. Par conséquent, il existe $a' \in k$ et un idéal premier $\mathfrak{p}'$, ne divisant pas le discriminant de E_1/k et tel que : $a'O_k = I_1^2\mathfrak{p}'$, $a' \equiv 1 \ mod^* \ 4O_k$ (notons que E_1/k et $k(\sqrt{a'})/k$ sont arithmétiquement disjointes). Puisque la classe de Steinitz de $k(\sqrt{a})/k$ est égale à c_1, on a le théorème 2.1.1 pour $D \times (\mathbb{Z}/2\mathbb{Z})$.

Comme $(-1, a)(-1, b)(a, b) = 1$, l'extension biquadratique $k(\sqrt{a}, \sqrt{b})/k$ est plongeable dans une extension quaternionienne E_2/k, à groupe de Galois isomorphe à Q, que l'on peut choisir modérée. (Remarque : ceci nous donne une partie de [39, Théorème 1.2] sans l'hypothèse $\xi_4 \in k$ ou $k(\xi_4)/k$ est ramifiée.) Soit $k(\sqrt{a''})/k$ une extension quadratique modérée, linéairement disjointe de E_2/k, alors la composée de E_2/k et $k(\sqrt{a''})/k$ est galoisienne modérée, à groupe de Galois $Q \times (\mathbb{Z}/2\mathbb{Z})$. Donc on a le théorème 2.1.1 pour $Q \times (\mathbb{Z}/2\mathbb{Z})$.

Il s'ensuit de $(-1, a) = 1$ et (2.1) que l'extension diédrale (de degré 8) E_1/k est plongeable dans une extension à groupe de Galois $D \leftthreetimes C$, que l'on peut choisir modérée. D'une façon plus explicite : Puisque $(-1, a) = 1$, $k(\sqrt{a})/k$ est plongeable dans une extension E_3/k, cyclique de degré 4, que l'on peut choisir modérée. (Remarque : ceci nous donne une autre partie de [39, Théorème 1.2].) Par des considérations élémentaires de la théorie de Galois, la composée E_1E_3 de E_1/k et E_3/k est une extension à groupe de Galois $D \leftthreetimes C$; elle est modérée car E_1/k et E_3/k le sont. Comme la classe de Steinitz de $k(\sqrt{a})/k$ est égale à c_1, on a le théorème 2.1.1 pour $\Gamma = D \leftthreetimes C$.

Puisque $(-1, a) = 1$, d'après (2.5), l'extension quaternionienne (de degré 8) E_2/k est plongeable dans une extension modérée à groupe de Galois $Q \leftthreetimes C$, que l'on peut choisir modérée. En fait, par la théorie de Galois, la composée E_2E_3 de E_2/k et E_3/k est une extension à groupe de Galois $Q \leftthreetimes C$; elle est modérée car E_2/k et E_3/k le sont. Donc on a le théorème 2.1.1 pour $\Gamma = Q \leftthreetimes C$.

On considère l'extension diédrale E_1/k. On a $(-1, a) = 1$, $(a, 2) = 1$ et $(-1, ab) = (-1, a)(-1, b) = 1$, donc les assertions (2.2), (2.3) et (2.4) sont équivalentes à : il existe $x \in k^\times$ tel que $(x, -ab)$=1. Prenons $x = a$, alors : $(a, -ab) = (a, -a)(a, b) = 1$, car $(a, b) = 1$ et il est bien connu (et immédiat) que $(a, -a) = 1$. On conclut qu'on a le théorème 2.1.1 pour $\Gamma = D_{16}, SD_{16}$, ou Q_{16}.

Montrons maintenant le théorème 2.1.1 pour le groupe M_{16}. Rappelons que E_3/k est une extension cyclique de degré 4, modérée et contenant $k(\sqrt{a})/k$ (l'unique sous-extension quadratique de E_3/k). Soit $x \in k^\times$ tel que $E_3 = k(\sqrt{x(a_0 + \sqrt{a_0})})$ (on rappelle que $a = a_1^2 + a_2^2$ et $a_0 = a/a_1^2$).

Soit E_4/k la composée des deux extensions linéairement disjointes E_3/k et $k(\sqrt{b})/k$; E_4/k est une extension galoisienne modérée, à groupe de Galois isomorphe à $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. On a $(a, 2b)(-1, x) = (a, b)(a, 2)(-1, x) = (-1, x)$. Supposons $\xi_4 \in k$. Alors $(-1, x) = (\xi_4, x)^2 = 1$. D'après (2.7) l'extension E_4/k est plongeable dans une extension galoisienne, à groupe de Galois M_{16}, que l'on peut choisir modérée.

Remarque. Soit k un corps de nombres quelconque. Soit $E_3' = k(\sqrt{(a_0 + \sqrt{a_0})})$. Puisque $(-1, 1) = 1$, la composée $(E_4'/k) = (E_3'k(\sqrt{b})/k)$, qui n'est pas nécessairement modérée, est plongeable, par (2.7), dans une extension galoisienne (contenant $k(\sqrt{a})/k$), à groupe de Galois M_{16}. On en déduit : pour tout $c \in Cl(k)$, il existe une extension quadratique de k, modérée dont la classe de Steinitz est c, et qui est plongeable dans une extension galoisienne de k à groupe de Galois isomorphe à M_{16}.

Pour démontrer le théorème 2.1.1 pour le groupe DC, DD, et DQ, considérons (deux fois) la classe triviale de $Cl(k)$ et procédons comme au début de la démonstration du théorème 2.1.1 (cela revient à remplacer les classes c_1 et c_2 par la classe triviale) en imposant quelques conditions de ramification. On obtient : il existe deux idéaux premiers distincts $\mathfrak{p}_3$, $\mathfrak{p}_4$ de O_k, premiers tous les deux avec $\mathfrak{p}_1$, $\mathfrak{p}_2$, et deux éléments c, d de $k^\times$ vérifiant :

$$cO_k = \mathfrak{p}_3,\ c \equiv\ 1\ mod^*\ \mathcal{C}_\infty 4O_k.$$

$$dO_k = \mathfrak{p}_4,\ d \equiv\ 1\ mod^*\ \mathcal{C}_\infty 4\mathfrak{p}_3.$$

Comme pour a et b, on vérifie sans peine qu'on a :

$$(-1, c) = 1,\ (-1, d) = 1,\ (c, d) = 1.$$

L'extension $k(\sqrt{c})/k$ est quadratique modérée de discriminant $\mathfrak{p}_3$. Elle est linéairement disjointe de $k(\sqrt{a}, \sqrt{b})/k$; car par exemple $\mathfrak{p}_3$ n'est pas ramifié dans $k(\sqrt{a}, \sqrt{b})/k$ et donc $k(\sqrt{a}, \sqrt{b}) \cap k(\sqrt{c}) = k$. Soit E_6 l'extension $k(\sqrt{a}, \sqrt{b}, \sqrt{c})/k$, alors c'est une extension galoisienne modérée, à groupe de Galois isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

On a $(a, b)(-1, c) = 1$. Grâce à (2.6), E_6/k est plongeable dans une extension galoisienne de k, à groupe de Galois isomorphe à DC, que l'on peut choisir modérée. Par conséquent on a le théorème 2.1.1 pour $\Gamma = DC$.

L'extension $k(\sqrt{d})/k$ est quadratique modérée de discriminant $\mathfrak{p}_4$; elle est linéairement disjointe de $k(\sqrt{a}, \sqrt{b}, \sqrt{c})/k$, car par exemple $\mathfrak{p}_4$ n'est pas ramifié dans cette dernière (les idéaux premiers ramifiés dans $k(\sqrt{a}, \sqrt{b}, \sqrt{c})/k$ sont : $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$). Soit E_7 l'extension $k(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})/k$, alors c'est une extension galoisienne modérée, à groupe de Galois isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$.

On a $(a,b)(c,d)=1$ (resp. $(-1,a)(-1,b)(a,b)(c,d)=1$) ; par $(2,8)$ (resp. $(2,9)$), E_7/k est plongeable dans une extension galoisienne à groupe de Galois isomorphe à DD (resp. DQ), que l'on peut choisir modérée. Par suite on a le théorème 2.1.1 pour $\Gamma = DD$ et $\Gamma = DQ$. Ceci achève la démonstration du théorème 2.1.1. □

Démonstration du théorème 2.1.2. Nous adaptons, à notre situation, l'idée principale de la démonstration du théorème 1.1(ii) dans [39] et du théorème 1.3(ii) dans [41].

Soit Γ un groupe non abélien d'ordre 16, ou extraspécial d'ordre 32. Lorsque Γ est le groupe modulaire M_{16}, on suppose que $\xi_4 \in k$. D'après le théorème 2.1.1, il existe une extension galoisienne N/k, modérée dont le groupe de Galois est isomorphe à Γ. Soit E/k la sous-extension de N/k correspondante à l'extension centrale :

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \Gamma \to Gal(E/k) \to 1.$$

Soit $c \in k$. Le théorème de Chebotarev et la surjection canonique de $Cl(k, 4O_k)$ sur $Cl(k)$ nous permettent d'affirmer : il existe un idéal fractionnaire I de O_k, un idéal premier $\mathfrak{p}$ de O_k premier avec le discriminant de N/k et un $r \in k^\times$ tels que :

$$rO_k = I^2\mathfrak{p},\ r \equiv\ 1\ mod^*\ 4O_k,\ c = cl(I)^{-1}.$$

L'extension $k(\sqrt{r})/k$ est quadratique modérée de discriminant $\mathfrak{p}$ et classe de Steinitz c.

Soit $\gamma \in E$ tel que $E(\sqrt{\gamma}) = N$. Par des considérations élémentaires de la théorie de Galois, la composée $Nk(\sqrt{r})$ de N/k et $k(\sqrt{r})/k$ contient l'extension $N_r = E(\sqrt{r\gamma})/k$, qui est galoisienne à groupe de Galois isomorphe à Γ (on pourrait voir aussi [23, Theorem 1.1]) ; elle est modérée car c'est une sous-extension de l'extension modérée $(Nk(\sqrt{r}))/k$.

D'après la transitivité de la classe de Steinitz dans une tour de corps de nombres on a :

$$cl_k(O_{N_r}) = cl_k(O_E)^2 N_{E/k}(cl_E(O_{N_r})).$$

L'extension $E(\sqrt{\gamma})/E$ étant modérée, il existe un (unique) idéal fractionnaire $I(\gamma)$ de O_E satisfaisant :

$$\gamma O_E = I(\gamma)^2\Delta(N/E),\quad cl(I(\gamma)^{-1}) = cl_E(O_N).$$

On a la décomposition :

$$r\gamma O_E = (IO_E I(\gamma))^2\Delta(N/E)\mathfrak{p}O_E,$$

où $\Delta(N/E)\mathfrak{p}O_E$ est sans facteur carré car $\Delta(N/k)$ est premier à $\mathfrak{p}$. Puisque l'extension $N_r = E(\sqrt{r\gamma})/E$ est quadratique modérée, on en déduit que

$$cl_E(O_{N_r}) = cl(IO_E I(\gamma))^{-1}.$$

Par conséquent :

$$cl_k(O_{N_r}) = cl_k(O_N)c^{[E:k]}.$$

D'où $A = \{cl_k(O_N)c^{[E:k]} \mid c \in Cl(k)\} \subset R_m(k,\Gamma)$. Supposons le nombre des classes de k impair. Alors $A = Cl(k)$, car $[E : k]$ est une puissance de 2 ($= 8$, ou 16), et donc $R_m(k,\Gamma) = Cl(k)$. Ceci termine la preuve du théorème 2.1.2. □

Chapitre 3

Classes galoisiennes réalisables d'extensions métacycliques de degré lm

3.1 Introduction

Soient k un corps de nombres, Γ un groupe fini, et N/k une extension galoisienne à groupe de Galois isomorphe à Γ. Soit $\mathcal{M}$ un O_k-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$, contenant $O_k[\Gamma]$. On rappelle que lorsque N/k est modérément ramifiée, on peut associer à O_N, par extension des scalaires, la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$, notée $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$, dans $Cl(\mathcal{M})$. On désigne par $\mathcal{R}(\mathcal{M})$ l'ensemble des classes c de $Cl(\mathcal{M})$ telles qu'il existe une extension N/k modérément ramifiée, à groupe de Galois isomorphe à Γ, avec $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$; on dira que c est réalisable par l'extension N/k et on appelle $\mathcal{R}(\mathcal{M})$ l'ensemble des classes réalisables.

Dans la suite, pour ne pas alourdir les notations, on identifiera fréquemment des groupes isomorphes quand c'est faisable sans ambiguïté.

Soit H un groupe fini d'ordre un entier naturel m. Soient l un nombre premier et C un groupe cyclique d'ordre l. Soit μ une représentation $\mathbb{F}_l$-linéaire de H dans C :

$$\mu : H \longrightarrow Aut(C)(\simeq (\mathbb{Z}/l\mathbb{Z})^*),$$

où $(\mathbb{Z}/l\mathbb{Z})^*$ est le groupe des éléments inversibles de $\mathbb{Z}/l\mathbb{Z}$. Notons Γ le produit semi-direct de C et H défini à l'aide de μ :

$$\Gamma = C \rtimes_\mu H.$$

Supposons μ fidèle dans toute la suite de ce chapitre. Alors H est cyclique et m divise $l-1$. On peut dire plus (voir [21, p. 12]) : à isomorphisme près, il existe un unique tel groupe Γ et il est isomorphe à l'unique sous-groupe d'ordre lm du groupe affine d'une droite sur $\mathbb{F}_l$. Si $m = l-1$, alors Γ est le groupe affine lui-même. Pour $m = 1$ (resp. $m = 2$), Γ est cyclique (resp. diédral). On peut caractériser ces groupes métacycliques comme étant les groupes résolubles transitifs de degré premier (théorème de Burnside). Le groupe Γ peut être défini par la présentation suivante :

$$\Gamma =< \sigma, \tau : \sigma^l = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^r >,$$

où r est un entier, avec $1 \leq r \leq (l-1)$, et la classe de r dans $(\mathbb{Z}/l\mathbb{Z})^*$ est d'ordre m.

Désormais on suppose $m \neq 1$ (donc $l \neq 2$) de sorte que Γ soit non abélien.

Dans ce chapitre, toute extension galoisienne N/k dont le groupe de Galois est isomorphe à Γ est appelée extension métacyclique de degré lm.

Le point de départ du présent chapitre était la lecture de [21] et une tentative de généralisations des arguments et résultats de [38], avec comme objectif la détermination de $\mathcal{R}(\mathcal{M})$ lorsque Γ est un groupe résoluble transitif de degré premier. Nous n'avons pas réussi à atteindre notre objectif, mais nous avons défini un sous-ensemble $\mathcal{R}_1(\mathcal{M})$ de $\mathcal{R}(\mathcal{M})$ et montré qu'il est un sous-groupe de $Cl^\circ(\mathcal{M})$ sous une certaine hypothèse (voir ci-dessous). (On pourrait consulter [42] pour une démarche analogue.)

Dans toute la suite, ξ désigne une racine primitive l-ième de l'unité. On définit $\mathcal{R}_1(\mathcal{M})$ comme étant l'ensemble des classes réalisables des extensions métacycliques N/k de degré lm, telles que la sous-extension k_1/k de N/k de degré m est linéairement disjointe de $k(\xi)/k$.

Dans ce chapitre, nous déterminons $\mathcal{R}_1(\mathcal{M})$ à l'aide d'un idéal de Stickelberger, et montrons qu'il est un sous-groupe de $Cl^\circ(\mathcal{M})$ sous l'hypothèse que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes.

Dans [38], Γ est un groupe métacyclique d'ordre lm, avec $m = q$ est un nombre premier, et $k/\mathbb{Q}$ est linéairement disjoint du lq-ième corps cyclotomique sur $\mathbb{Q}$; le corps k' de [38] correspond à k_1. Après lecture attentive de [38], nous avons constaté qu'on a besoin de supposer que $k' \cap k(\xi) = k$ dans [38, p. 91, ligne 18] et jusqu'à la fin de l'article. Donc, dans [38], on a en fait déterminé $\mathcal{R}_1(\mathcal{M})$ et non $\mathcal{R}(\mathcal{M})$. En résumé : l'énoncé du [38, Théorème, p. 89] est correct avec $\mathcal{R}_1(\mathcal{M})$ au lieu de $\mathcal{R}(\mathcal{M})$, et la description correcte de $\mathcal{R}_1(\mathcal{M})$ (au lieu de $\mathcal{R}(\mathcal{M})$) est dans [6, Appendix, p. 18]. On pourrait utiliser

le présent chapitre comme une correction définitive de [38] (voir ci-dessous la seconde remarque après le théorème 3.1.1).

Le but de la suite est d'énoncer nos principaux résultats.

Comme Γ/C (isomorphe à H) est abélien, C d'ordre premier et Γ non abélien, le groupe dérivé de Γ est C. Donc il y a m caractères absolument irréductibles de Γ de degré 1 : on les obtient en composant les caractères de degré 1 de Γ/C avec la surjection canonique de Γ sur Γ/C. Soient $n+1$ le nombre des classes de conjugaison sur k de ces caractères, et $\{\psi_i, 0 \leq i \leq n\}$ un système de leurs représentants, avec ψ_0 le caractère trivial.

Pour tout i, $0 \leq i \leq n$, la restriction de ψ_i à H définit un caractère de H, car $C \subset Ker(\psi_i)$, qu'on note χ_i. Il est clair que $\{\chi_i, 0 \leq i \leq n\}$ est un système de représentants des classes de conjugaison sur k des caractères absolument irréductibles de H. Soit $k(\psi_i)$ (resp. $k(\chi_i)$) l'extension de k obtenue par adjonction à k des valeurs de ψ_i (resp. χ_i), alors $k(\psi_i) = k(\chi_i)$ pour tout i, $0 \leq i \leq n$.

Soit $F/\mathbb{Q}$ la sous-extension de $\mathbb{Q}(\xi)/\mathbb{Q}$ de degré $(l-1)/m$. Les autres caractères absolument irréductibles de Γ sont de degré m, et il y en a $(l-1)/m$; ils sont induits par des caractères de degré 1 et d'ordre l de C, sont à valeurs dans F et sont conjugués sous $Gal(F/\mathbb{Q})$ (voir [21, §2, p. 13]).

Maintenant supposons que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ soient linéairement disjointes si bien que $Gal(k(\xi)/k) \simeq Gal(\mathbb{Q}(\xi)/\mathbb{Q})$. Soit E_0/k la sous-extension de $k(\xi)/k$ de degré $(l-1)/m$. Signalons que sous l'hypothèse précédente, notre E_0 est le même que celui défini dans [7, Appendice, p. 341] (attention à la différence des notations : les p et q de [7, Appendice] correspondent respectivement à l et m). Puisque $Gal(E_0/k) \simeq Gal(F/\mathbb{Q})$, il y a une seule classe de conjugaison sur k des caractères irréductibles de Γ de degré m ; notons que son cardinal est $(l-1)/m$. On note χ un représentant d'une telle classe, et ψ un caractère de degré 1 et d'ordre l de C tel que :

$$\chi = Ind_C^{\Gamma}\psi.$$

Remarques. (1) Puisque C est un sous-groupe distingué de Γ, il est immédiat que pour tout $\gamma \in \Gamma \backslash C$, $\chi(\gamma) = 0$. En utilisant la formule bien connue donnant $Ind_C^{\Gamma}\psi$ et le fait que s_r, défini par $s_r(\xi) = \xi^r$, est un générateur de $Gal(\mathbb{Q}(\xi)/F)$, on vérifie facilement que pour tout i, $0 \leq i \leq (l-1)$, on a : $\chi(\sigma^i) = Tr_{\mathbb{Q}(\xi)/F}(\psi(\sigma)^i)$, où Tr désigne la trace.

(2) Le but de cette remarque est de montrer que χ n'est pas symplectique.

Soit $c(\chi) = |\Gamma|^{-1} \sum_{\gamma \in \Gamma} \chi(\gamma^2)$ l'indicateur de Frobenius-Schur de χ (voir [11, (73.12) et (73.14), pp. 725-726]), où $|\Gamma|$ est l'ordre de Γ. On a $c(\chi) = 0$, en effet :

- Si m est impair, alors $|\Gamma|$ est impair (rappelons que $l \neq 2$). Donc $\{\gamma^2, \gamma \in \Gamma\} = \Gamma$ et $c(\chi) = |\Gamma|^{-1} \sum_{\gamma \in \Gamma} \chi(\gamma)$; d'où $c(\chi) = 0$ car χ est orthogonal au caractère trivial.

- Si m est pair, les éléments de Γ tels que $\gamma^2 \in C$ sont : les éléments de C et les $\sigma^i \tau^{m/2}$, $0 \leq i \leq (l-1)$. On a $(\sigma^i \tau^{m/2})^2 = \sigma^{ir^{m/2}}$. En utilisant le fait que $\sigma^{r^{m/2}}$ est un générateur de C, car r est premier avec l, on obtient : $c(\chi) = 2|\Gamma|^{-1} \sum_{\gamma \in C} \chi(\gamma)$. Or $\sum_{\gamma \in C} \chi(\gamma) = Tr_{\mathbb{Q}(\xi)/F}(\sum_{i=0}^{l-1} \psi(\sigma)^i) = Tr_{\mathbb{Q}(\xi)/F}(0) = 0$ (ψ est d'ordre l). Par conséquent $c(\chi) = 0$.

Puisque $c(\chi) \neq -1$, χ n'est pas symplectique d'après [11, (73.13), p. 726] (χ est unitaire car $c(\chi) = 0$; voir la définition de unitaire dans [11, (73.10)(i), p. 724]). Ceci termine la seconde remarque.

Soit $k(\chi)$ l'extension de k obtenue par adjonction à k des valeurs de χ. En utilisant [11, p. 330 et §74] (voir Chap. 1, §1.1), il est immédiat que la décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante (on rappelle que $k(\psi_i) = k(\chi_i)$) :

$$k[\Gamma] \simeq \prod_{i=0}^{n} k(\psi_i) \times M_{n_\chi}(D_\chi) = \prod_{i=0}^{n} k(\chi_i) \times M_{n_\chi}(D_\chi),$$

où D_χ est un corps gauche de centre $k(\chi)$, et $M_{n_\chi}(D_\chi)$, qui est l'anneau des matrices carrées d'ordre n_χ à coefficients dans D_χ (on rappelle que $n_\chi = \chi(1)/s_0$, où s_0 est l'indice de Schur relatif à k), est la composante simple associée à χ.

De plus (voir [11, p. 330]), le degré de $k(\chi)/k$ est égal au nombre t des conjugués sur k de χ. On a vu, ci-dessus juste avant les remarques, que $t = (l-1)/m$. Comme $k(\chi)/k$ est une sous-extension de l'extension cyclique $k(\xi)/k$ et le degré de E_0/k est $(l-1)/m$, on a $k(\chi) = E_0$.

Soit $\mathcal{M}$ un O_k-ordre maximal dans $k[\Gamma]$ contenant $O_k[\Gamma]$. Puisque les caractères χ et ψ_i, $0 \leq i \leq n$, ne sont pas symplectiques, la remarque qui suit le théorème 1.1.2 nous donne :

$$Cl(\mathcal{M}) \simeq \prod_{i=0}^{n} Cl(k(\psi_i)) \times Cl(E_0) = \prod_{i=0}^{n} Cl(k(\chi_i)) \times Cl(E_0).$$

D'où :

$$Cl^\circ(\mathcal{M}) \simeq \prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(E_0).$$

Nous identifierons fréquemment $Cl^\circ(\mathcal{M})$ avec $\prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(E_0)$ sous l'isomorphisme précédent.

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

$$k[H] \simeq \prod_{i=0}^{n} k(\chi_i).$$

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

$$Cl(\mathcal{M}(H)) \simeq \prod_{i=0}^{n} Cl(k(\chi_i)), \quad \text{et donc } Cl^\circ(\mathcal{M}(H)) \simeq \prod_{i=1}^{n} Cl(k(\chi_i)).$$

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 [26], $\mathcal{R}(\mathcal{M}(H))$ 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 $\prod_{i=1}^{n} Cl(k(\chi_i))$.

Soit

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

Soit l'élément de Stickelberger

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

et soit l'idéal de Stickelberger

$$\mathcal{S} = (1/l)\theta\mathbb{Z}[S] \cap \mathbb{Z}[S].$$

L'action naturelle de S par restriction sur les idéaux fractionnaires de E_0 induit une structure de $\mathbb{Z}[S]$-module sur $Cl(E_0)$. On note $\mathcal{S}Cl(E_0)$ le sous-groupe de $Cl(E_0)$ engendré par les éléments de la forme $\mathfrak{s}c$, où $\mathfrak{s} \in \mathcal{S}$ et $c \in Cl(E_0)$.

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 ce chapitre, on démontre le théorème suivant :

Théorème 3.1.1. *Soient k un corps de nombres et $\Gamma = C \rtimes_\mu H$. Supposons que la représentation μ soit fidèle, et que les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ soient linéairement disjointes. Soit E_0/k la sous-extension de $k(\xi)/k$ de degré $(l-1)/m$. Alors $\mathcal{R}_1(\mathcal{M})$ est un sous-groupe de $Cl^\circ(\mathcal{M})$, égal au sous-groupe A suivant :*

$$A = \left\{ \left(c_1, c_2, \ldots, c_n, x\phi_{E_0/k}\Big(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)\Big)\right) \Big| \right.$$
$$\left. (c_1, c_2, \ldots, c_n) \in \mathcal{R}(\mathcal{M}(H)), x \in \mathcal{S}Cl(E_0) \right\}.$$

Remarques. (1) On déduit immédiatement de ce théorème que $\mathcal{R}_1(\mathcal{M})$ est isomorphe au groupe produit $\mathcal{R}(\mathcal{M}(H)) \times \mathcal{S}Cl(E_0)$.

(2) Considérons le cas particulier où $m = q$ est un nombre premier, et $k/\mathbb{Q}$ est linéairement disjoint du lq-ième corps cyclotomique sur $\mathbb{Q}$: c'est la situation de l'article [38] ; précisons que le corps K de [38] et [6, Appendix] est égal à E_0. On a $\mathcal{R}(\mathcal{M}(H)) = \mathcal{S}_q Cl(k(\xi_q))$ d'après [37, Théorème, p. 191] car $k \cap \mathbb{Q}(\xi_q) = \mathbb{Q}$, où $\mathcal{S}_q$ est un idéal de Stickelberger qui se définit de façon similaire à $\mathcal{S}$, et ξ_q est une racine primitive q-ième de l'unité. D'une façon explicite, la correction définitive de [38] signalée ci-dessus est : $\mathcal{R}_1(\mathcal{M}) \simeq \mathcal{S}_q Cl(k(\xi_q)) \times \mathcal{S}Cl(E_0)$ et $\mathcal{R}_1(\mathcal{M}) = \{(c, x\phi_{E_0/k}(N_{k(\xi_q)/k}(c)) | c \in \mathcal{S}_q Cl(k(\xi_q)), x \in \mathcal{S}Cl(E_0)\}$.

Si G est un groupe fini, on désigne par $R_{mo}(k, G)$ (mo pour modéré ; on note mo au lieu de m pour éviter toute confusion avec le cardinal m de H) l'ensemble des classes de Steinitz des extensions galoisiennes modérées de k, dont le groupe de Galois est isomorphe à G. Rappelons que si G est abélien, alors $R_{mo}(k, G)$ est un sous-groupe de $Cl(k)$.

Une application du théorème précédent est la proposition suivante.

Proposition 3.1.2. *Soit k un corps de nombres. Supposons que les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ soient linéairement disjointes. Alors l'ensemble $R_{mo}(k, \Gamma)$ des classes de Steinitz des extensions métacycliques de degré lm est le sous-groupe de $Cl(k)$ suivant :*

$$R_{mo}(k, \Gamma) = R_{mo}(k, H)^l N_{E_0/k}(Cl(E_0))^{m(l-1)/2}.$$

Remarque. Cette proposition est un cas particulier de [7, Théorème A.5, p. 342] (A pour Appendice) qui est un résultat de L.P. Endo. Mais ici la démonstration est différente et plus courte. Signalons que l'appendice de [7] est un résumé de plusieurs résultats contenus dans la thèse de Endo.

3.2 Préliminaires

Le but de cette section est d'établir ou rappeler quelques propositions en vue de la démonstration du principal résultat de ce chapitre.

Désormais N/k désigne une extension modérément ramifiée à groupe de Galois isomorphe à Γ, où k et Γ vérifient les hypothèses du théorème 3.1.1 : $k \cap \mathbb{Q}(\xi) = \mathbb{Q}$ et $\Gamma = C \rtimes_\mu H$ avec μ fidèle. Nous notons par k_1 le sous-corps de N fixe par C ; on a : k_1/k est galoisienne et $Gal(k_1/k) \simeq H$. 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 $O_{N,\mathfrak{p}}$.

Soit i, $1 \leq i \leq n$. Les égalités suivantes découlent facilement de la définition des résolvantes de Fröhlich-Lagrange :

$$\langle \alpha_\mathfrak{p}, \psi_i \rangle = \langle Tr_{N_\mathfrak{p}/(k_1)_\mathfrak{p}}(\alpha_\mathfrak{p}), \chi_i \rangle_{k_1/k}, \quad \langle a, \psi_i \rangle = \langle Tr_{N/k_1}(a), \chi_i \rangle_{k_1/k}.$$

Signalons que $Tr_{N_\mathfrak{p}/(k_1)_\mathfrak{p}}(\alpha_\mathfrak{p})$ et $Tr_{N/k_1}(a)$ sont des bases respectives du $O_{k,\mathfrak{p}}[H]$-module $O_{k_1,\mathfrak{p}}$ et du $k[H]$-module k_1.

Soient b et $b_\mathfrak{p}$ des bases respectives du $k_1[C]$-module N et du $O_{k_1,\mathfrak{p}}[C]$-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 $Gal(\overline{\mathbb{Q}}/k_1)$ (rappelons que $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$). Puisque $\chi = Ind_C^\Gamma \psi$, par un résultat de Fröhlich (voir [13, (5.12), p. 401] ou [14, Theorem 12, p. 165]), il existe λ et $\lambda_\mathfrak{p}$ des éléments inversibles respectifs des anneaux $k[C]$ et $O_{k,\mathfrak{p}}[C]$ tels que :

$$\langle a, \chi \rangle \psi(\lambda) = \mathfrak{N}_{k_1/k}(\langle b, \psi \rangle_{N/k_1}) e(k_1/k),$$

et

$$\langle \alpha_\mathfrak{p}, \chi \rangle \psi(\lambda_\mathfrak{p}) = \mathfrak{N}_{k_1/k}(\langle b_\mathfrak{p}, \psi \rangle_{N/k_1}) e((k_1)_\mathfrak{p}/k_\mathfrak{p}),$$

où ψ a été prolongé par linéarité à $k_\mathfrak{p}[C]$, $e(k_1/k)^2$ est le discriminant d'une base du k-espace vectoriel k_1, $e((k_1)_\mathfrak{p}/k_\mathfrak{p})^2 O_{k,\mathfrak{p}}$ est le discriminant de $(k_1)_\mathfrak{p}/k_\mathfrak{p}$, et

$$\mathfrak{N}_{k_1/k}(\langle x, \psi \rangle_{N/k_1}) = \prod_{\gamma \in S_0} \gamma(\langle x, \gamma^{-1}\psi \rangle_{N/k_1}).$$

Supposons que k_1/k et $k(\xi)/k$ soient linéairement disjointes. On peut donc choisir un prolongement $\overline{\tau}$ de τ à $\overline{\mathbb{Q}}$ vérifiant $\overline{\tau}(\xi) = \xi$. Il est clair qu'on peut supposer $S_0 = \{\overline{\tau}^i, 0 \leq i \leq (m-1)\}$. Alors

$$\mathfrak{N}_{k_1/k}(\langle x, \psi \rangle_{N/k_1}) = \prod_{\gamma \in S} \gamma(\langle x, \psi \rangle_{N/k_1}) = \prod_{i=0}^{m-1} \overline{\tau}^i(\langle x, \psi \rangle_{N/k_1}).$$

Une démonstration similaire à celle de la proposition 4.1 dans [4, pp. 22–23] 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 :*

$$f(\psi_0) = (1),$$

$$f(\psi_i) = \left(\frac{\langle Tr_{N_\mathfrak{p}/(k_1)_\mathfrak{p}}(\alpha_\mathfrak{p}), \chi_i \rangle_{k_1/k}}{\langle Tr_{N/k_1}(a), \chi_i \rangle_{k_1/k}} \right)_\mathfrak{p}, \quad \textit{pour tout } i, 1 \leq i \leq n,$$

$$f(\chi) = \left(\frac{e((k_1)_\mathfrak{p}/k_\mathfrak{p})}{e(k_1/k)} \prod_{i=0}^{m-1} \overline{\tau}^i \left(\frac{\langle b_\mathfrak{p}, \psi \rangle_{N/k_1}}{\langle b, \psi \rangle_{N/k_1}} \right) \right)_\mathfrak{p}.$$

Rappelons qu'on identifie des groupes isomorphes pour ne pas alourdir les notations.

Soit *Res* le morphisme de restriction de $Gal(k_1(\xi)/k)$ sur $Gal(k_1/k)$ ($\simeq H$). Nous noterons aussi par μ le morphisme $\mu \circ Res$:

$$\mu : Gal(k_1(\xi)/k) \longrightarrow (\mathbb{Z}/l\mathbb{Z})^* (\simeq Aut(C)).$$

Soit $\nu : Gal(k_1(\xi)/k) \longrightarrow (\mathbb{Z}/l\mathbb{Z})^*$ le morphisme défini par : si g est un élément de $Gal(k_1(\xi)/k)$ et $g(\xi) = \xi^i$, alors $\nu(g)$ est la classe de i modulo $l\mathbb{Z}$.

On désigne par λ le morphisme suivant :

$$\lambda : Gal(k_1(\xi)/k) \longrightarrow (\mathbb{Z}/l\mathbb{Z})^*$$

$$g \longmapsto \nu(g)\mu(g)^{-1}.$$

Soit Z le sous-corps de $k_1(\xi)/k$ fixe par $Ker(\lambda)$. Supposons que k_1/k et $k(\xi)/k$ soient linéairement disjointes. D'après [7, Proposition A.2(1), p. 341], le sous-groupe $Ker(\lambda)$ est cyclique d'ordre m (dans notre situation $m = pgcd(m, [k(\xi) : k])$; attention à la différence des notations : les p et q de [7, Appendice] correspondent respectivement à l et m). De plus, $k_1(\xi)$ est égal à la composée des extensions Z et $k(\xi)$ (resp. k_1).

Comme les extensions $Z/Z \cap k(\xi)$ et $k(\xi)/Z \cap k(\xi)$ sont linéairement disjointes et $[Zk(\xi) : Z] = [k_1(\xi) : Z] = m$, on a $[k(\xi) : Z \cap k(\xi)] = m$. Puisque $k(\xi)/k$ est cyclique on en déduit que $Z \cap k(\xi) = E_0$. Par conséquent Z/E_0 et $k(\xi)/E_0$ sont linéairement disjointes et $Gal(Z/E_0) \simeq Gal(k_1(\xi)/k(\xi))(\simeq Gal(k_1/k))$.

De $Z/Z \cap k_1$ et $k_1/Z \cap k_1$ sont linéairement disjointes et $[Zk_1 : Z] = [k_1(\xi) : Z] = m$, on tire $[k_1 : Z \cap k_1] = m$. D'où $Z \cap k_1 = k$. Il s'ensuit que Z/k et k_1/k sont linéairement disjointes, et $Gal(Z/k) \simeq Gal(k_1(\xi)/k_1) \simeq Gal(k(\xi)/k)(= S)$.

Les extensions N/k_1 et $k_1(\xi)/k_1$ sont linéairement disjointes car leurs degrés respectifs l et $l-1$ sont premiers entre eux. On a : $N \cap k(\xi) = N \cap k_1(\xi) \cap k(\xi) = k_1 \cap k(\xi) = k$. Par suite N/k et $k(\xi)/k$ sont linéairement disjointes. Donc $Gal(N(\xi)/k) \simeq Gal(N/k) \times Gal(k(\xi)/k)$.

Rappelons les notations :

$$Gal(N/k) =< \sigma, \tau : \sigma^l = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^r >,$$

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

On a les isomorphismes de restriction :

$$Gal(N(\xi)/N) \simeq Gal(k_1(\xi)/k_1) \simeq Gal(k(\xi)/k) = S,$$
$$Gal(N(\xi)/k(\xi)) \simeq Gal(N/k) =< \sigma, \tau >,$$
$$Gal(N(\xi)/k_1(\xi)) \simeq Gal(N/k_1) =< \sigma >= C,$$
$$Gal(k_1(\xi)/k(\xi)) \simeq Gal(k_1/k) \simeq H =< \tau > .$$

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 $N(\xi)/k$. Si $i \in \mathbb{Z}$, on notera aussi i sa classe dans $\mathbb{Z}/l\mathbb{Z}$, et l'on désignera par i^* son inverse modulo $l\mathbb{Z}$ lorsque i est premier à l.

Il découle de k_1/k et $k(\xi)/k$ sont linéairement disjointes que $Gal(k_1(\xi)/k)$ est isomorphe à $Gal(k(\xi)/k) \times Gal(k_1/k)$. On peut donc noter

$$Gal(k_1(\xi)/k) = \{s_i\tau^j \mid \ 1 \leq i \leq l-1, 0 \leq j \leq m-1\}.$$

On a : $\nu(s_i) = i, \nu(\tau) = 1$, $\mu(s_i) = 1$ et $\mu(\tau) = r$. D'où

$$\lambda(s_i\tau^j) = i(r^*)^j.$$

Un calcul simple montre que le groupe cyclique $Ker(\lambda)$ est engendré par τs_r. Par conséquent Z/k est la sous-extension de $k_1(\xi)/k$ fixe par τs_r.

Remarque. Le corps $\tilde{k}$ défini dans [21, §5] est égal à Z.

Soit φ un caractère de degré 1 et d'ordre l de C. Soit x un élément de N. Rappelons la définition de la résolvante de Fröhlich-Lagrange $\langle x, \varphi \rangle_{N/k_1}$:

$$\langle x, \varphi \rangle_{N/k_1} = \sum_{i=0}^{l-1} \varphi(\sigma^{-i})\sigma^i(x).$$

On vérifie sans peine les propriétés suivantes :

$$\sigma(\langle x,\varphi\rangle_{N/k_1}) = \varphi(\sigma)\langle x,\varphi\rangle_{N/k_1},\quad \tau(\langle x,\varphi\rangle_{N/k_1}) = \langle \tau(x),\varphi^{r*}\rangle_{N/k_1},$$

$$s_i(\langle x,\varphi\rangle_{N/k_1}) = \langle x,\varphi^i\rangle_{N/k_1}.$$

Soit K_0/k une sous-extension de degré l de N/k. Puisque N/k est une extension décomposée au sens de [31] (i.e., composée de K_0/k et k_1/k qui sont linéairement disjointes), d'après [31, Lemme 5], il existe $b \in K_0$ telle que $\{\sigma(b), \sigma \in C\}$ est une base normale de N/k_1 (la démonstration est simple : elle consiste en l'adaptation de celle du théorème de la base normale dans une extension galoisienne). Choisissons K_0/k la sous-extension de N/k fixe par $H =< \tau >$, de sorte que $\tau(b) = b$.

Des trois propriétés ci-dessus, on déduit immédiatement que $\langle b,\psi\rangle^l_{N/k_1}$ est un élément de Z.

On peut écrire d'une manière unique :

$$\langle b,\psi\rangle^l_{N/k_1} O_Z = (I(\psi))^l \prod_{i=1}^{l-1} J_i(\psi)^i,$$

où $I(\psi)$ est un idéal fractionnaire de Z, et les $J_i(\psi)$, $1 \leq i \leq (l-1)$, sont des idéaux entiers de O_Z, sans facteur carré et premiers entre eux deux à deux.

En utilisant l'unicité de la décomposition précédente et les propriétés de $\langle b,\psi\rangle_{N/k_1}$ on montre facilement qu'on a :

$$s_i(J_1(\psi)) = J_1(\psi^i),\quad J_i(\psi) = J_1(\psi^{i^*}).$$

On en déduit :

$$\langle b,\psi\rangle^l_{N/k_1} O_Z = (I(\psi))^l \theta J_1(\psi),$$

où $\theta J_1(\psi)$ se calcule en utilisant la structure naturelle de $\mathbb{Z}[S]$-module de l'ensemble des idéaux fractionnaires de Z.

Rappelons que si K/k est une extension finie de corps de nombres, on note $cl_k(O_K)$ sa classe de Steinitz, et si I est un idéal fractionnaire de k, on désigne par $cl(I)$ sa classe dans $Cl(k)$ le groupe des classes de k.

Proposition 3.2.2. *Soient c_i, $0 \leq i \leq n+1$, les composantes de $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $\prod_{i=0}^n Cl(k(\chi_i)) \times Cl(E_0)$. Alors :*

(i) c_0 est la classe triviale dans $Cl(k)$.

(ii) $(c_1, c_2, \ldots, c_n)$ est la classe de $[\mathcal{M}(H) \otimes_{O_k[H]} O_{k_1}]$ dans $\prod_{i=1}^n Cl(k(\chi_i))$.

(iii) $c_{n+1} = \phi_{E_0/k}(cl_k(O_{k_1}))N_{Z/E_0}(cl(I(\psi)^{-1}))$ *dans* $Cl(E_0)$.

Nous aurons besoin d'un lemme pour la démonstration de l'assertion *(iii)* de la proposition précédente. Avant de l'énoncer, précisons quelques notations.

Comme ci-dessus, on peut écrire d'une manière unique :

$$\langle b, \psi\rangle^l_{N/k_1} O_{k_1(\xi)} = (I'(\psi))^l \prod_{i=1}^{l-1} J_i'(\psi)^i,$$

où $I'(\psi)$ est un idéal fractionnaire de $k_1(\xi)$, et les $J_i'(\psi)$, $1 \leq i \leq (l-1)$, sont des idéaux entiers de $O_{k_1(\xi)}$, sans facteur carré et premiers entre eux deux à deux. On montre sans difficulté qu'on a :

$$s_i(J_1'(\psi)) = J_1'(\psi^i),\ J_i'(\psi) = J_1'(\psi^{i^*}),\ \tau(J_i'(\psi)) = J_i'(\psi^{r^*}),$$

et l'on obtient :

$$\langle b, \psi\rangle^l_{N/k_1} O_{k_1(\xi)} = (I'(\psi))^l \theta J_1'(\psi),$$

où $\theta J_1'(\psi)$ se calcule en utilisant la structure naturelle de $\mathbb{Z}[S]$-module de l'ensemble des idéaux fractionnaires de $k_1(\xi)$.

Lemme 3.2.3. *Sous les notations précédentes on a :* $J_1'(\psi) = J_1(\psi)O_{k_1(\xi)}$ *et* $I'(\psi) = I(\psi)O_{k_1(\xi)}$.

Démonstration. On a $\tau s_r(J_1'(\psi)) = J_1'(\psi^{rr^*}) = J_1'(\psi)$. Donc $J_1'(\psi)$ est un idéal ambige de l'extension $k_1(\xi)/Z$ (i.e., $J_1'(\psi)$ est invariant sous $Gal(k_1(\xi)/Z)$). Puisque ψ est non trivial et $\langle b, \psi\rangle_{N/k_1} \neq 0$, on a $N(\xi) = k_1(\xi)(\langle b, \psi\rangle_{N/k_1})$. Les extensions N/k_1 et $k_1(\xi)/k_1$ étant modérées, on obtient : la composée $N(\xi)/k_1$ est modérée et donc $N(\xi)/k_1(\xi)$ l'est aussi. Par la théorie de Kummer $\Delta(N(\xi)/k_1(\xi)) = (\prod_{i=1}^{l-1} J_i'(\psi))^{l-1}$. Par conséquent $J_1'(\psi)$ est premier avec $lO_{k_1(\xi)}$. Parce que $k_1(\xi) = Z(\xi)$, les seuls idéaux premiers de O_Z qui peuvent éventuellement se ramifier dans $k_1(\xi)/Z$ sont des diviseurs de lO_Z. Comme $J_1'(\psi)$ est un idéal ambige de $k_1(\xi)/Z$, sans facteur carré et est premier avec $\Delta(k_1(\xi)/Z)O_Z$ on obtient : il existe un idéal X de O_Z satisfaisant $J_1'(\psi) = XO_{k_1(\xi)}$.

Posons $\alpha = \langle b, \psi\rangle^l_{N/k_1}$ et $J = \theta X$. Alors $(\alpha J^{-1})^m = N_{k_1(\xi)/Z}(I'(\psi))^l$. Mais l et m sont premiers entre eux, d'où $N_{k_1(\xi)/Z}(I'(\psi)) = Y^m$, où Y est un idéal fractionnaire de Z. On vérifie facilement que $s_i((I'(\psi)) = I'(\psi^i)$ et $\tau((I'(\psi)) = I'(\psi^{r^*})$; on en déduit que $I'(\psi)$ est un idéal ambige de $k_1(\xi)/Z$. Comme $N_{k_1(\xi)/Z}(I'(\psi))O_{k_1(\xi)} = \prod_{\gamma \in Gal(k_1(\xi)/Z)} \gamma(I'(\psi))$, on a $(YO_{k_1(\xi)})^m = I'(\psi)^m$. Par conséquent $I'(\psi) = YO_{k_1(\xi)}$.

De ce qui précède on tire $[I(\psi)^{l}\theta J_1(\psi)]O_{k_1(\xi)} = [Y^{l}\theta X]O_{k_1(\xi)}$. Par suite $I(\psi)^{l}\theta J_1(\psi) = Y^{l}\theta X$; donc $I(\psi) = Y$ et $J_1(\psi) = X$ par l'unicité de la décomposition. Ceci termine la démonstration du lemme. □

Démonstration de la proposition 3.2.2. (*i*) C'est évident.

(*ii*) La démonstration est analogue à celle de l'assertion (*ii*) de la proposition 4.2 dans [4, p. 24].

(*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 :

$$f(\chi) = \left(\frac{e((k_1)_{\mathfrak{p}}/k_{\mathfrak{p}})}{e(k_1/k)} \prod_{i=0}^{m-1} \overline{\tau}^{i} \left(\frac{\langle b_{\mathfrak{p}}, \psi \rangle_{N/k_1}}{\langle b, \psi \rangle_{N/k_1}} \right) \right)_{\mathfrak{p}}.$$

Il suit de [15, Note 4, pp. 50–51] que la classe dans $Cl(k_1(\xi))$ du contenu de l'idèle $(\langle b_{\mathfrak{p}}, \psi \rangle_{N/k_1} / \langle b, \psi \rangle_{N/k_1})_{\mathfrak{p}}$ est la classe de l'idéal fractionnaire $\langle O_N, \psi \rangle_{N/k_1} / \langle b, \psi \rangle_{N/k_1}$. Mais la classe de ce dernier est égale à $cl(I'(\psi)^{-1})$ par le théorème 2.3(1) de [37]. Par le lemme 3.2.3, $cl(I'(\psi)^{-1}) = cl(I(\psi)^{-1}O_{k_1(\xi)})$.

D'après [31], on peut choisir $b_{\mathfrak{p}} \in O_{K_0,\mathfrak{p}}$ (rappelons que K_0/k est la sous-extension de N/k fixe par $H =< \tau >$, de telle sorte que $\tau(b) = b$). La résolvante $\langle b_{\mathfrak{p}}, \psi \rangle_{N/k_1}$ vérifiant les mêmes propriétés que $\langle b, \psi \rangle_{N/k_1}$, on obtient $\langle b_{\mathfrak{p}}, \psi \rangle_{N/k_1} / \langle b, \psi \rangle_{N/k_1} \in Z_{\mathfrak{p}}$. Comme $Gal(k_1(\xi)/k(\xi))$ est isomorphe par restriction à $Gal(Z/E_0)$, et la restriction de $\overline{\tau}$ à $k_1(\xi)$ est un générateur de $Gal(k_1(\xi)/k(\xi))$, on a : $Gal(Z/E_0)$ est engendré par la restriction de $\overline{\tau}$ à Z. On en déduit que la classe dans $Cl(E_0)$ du contenu de l'idèle $(\prod_{i=0}^{m-1} \overline{\tau}^{i}(\langle b_{\mathfrak{p}}, \psi \rangle_{N/k_1} / \langle b, \psi \rangle_{N/k_1}))_{\mathfrak{p}}$ est $N_{Z/E_0}(cl(I(\psi)^{-1})$.

Soit I l'idéal fractionnaire de k qui est le contenu de l'idèle $(e((k_1)_{\mathfrak{p}}/k_{\mathfrak{p}})/e(k_1/k))_{\mathfrak{p}}$. Un raisonnement similaire à celui de la fin de la preuve de la proposition 4.2(*iii*) dans [4, p. 24] nous donne : $cl(I) = cl_k(O_{k_1})$. Ceci permet d'achever la démonstration de (*iii*). □

Proposition 3.2.4. *Supposons que le discriminant de k_1/k soit premier à lO_k, et que toute sous-extension de k_1/k différente de k soit ramifiée en au moins une place finie. Alors toute sous-extension de Z/E_0 différente de E_0 est ramifiée en au moins une place finie.*

Démonstration. Soit X/E_0 une sous-extension de Z/E_0 de degré $x \neq 1$. Comme k_1/k est cyclique et x divise m (rappelons que le degré de Z/F_0 est m), il existe une (unique) sous-extension Y/k de k_1/k de degré x. Les extensions k_1/k et $k(\xi)/k$ étant arithmétiquement disjointes (i.e., linéairement disjointes et de discriminants premiers entre eux), il en est de même de Y/k et $k(\xi)/k$. Par suite le degré de $Y(\xi)/k(\xi)$ est x et $\Delta(Y(\xi)/k(\xi)) = \Delta(Y/k)O_{k(\xi)}$, où Δ désigne le discriminant. Puisque les extensions Z/E_0 et $k(\xi)/E_0$ sont

linéairement disjointes, X/E_0 et $k(\xi)/E_0$ le sont aussi; d'où le degré de $X(\xi)/k(\xi)$ est x. Comme $k_1(\xi)/k(\xi)$ est cyclique, on a $X(\xi) = Y(\xi)$. Par conséquent $X(\xi)/k(\xi)$ est ramifiée en au moins une place finie première à $lO_{k(\xi)}$. Mais $X(\xi)/X$ et $k(\xi)/E_0$ sont non ramifiés en toute place finie sauf peut-être en une place au dessus de l. On en déduit que X/E_0 est ramifiée en au moins une place finie. Ce qui termine la démonstration. □

Proposition 3.2.5. *Soit $\mathcal{S}'$ l'idéal de $\mathbb{Z}[S]$ engendré par les éléments de la forme $c - s_c$, où c est premier avec l et $s_c(\xi) = \xi^c$ ($s_c = s_i$, où $c \equiv i \ mod\ l$ et $1 \leq i \leq l-1$).*

(1) *On a : $\mathcal{S} = (1/l)\theta\mathcal{S}'$.*

(2) *Soit M un $\mathbb{Z}[S]$-module. Notons $\mathcal{S}M$ le sous-module de M engendré par les éléments de la forme $\mathfrak{s}m$, où $\mathfrak{s} \in \mathcal{S}$ et $m \in M$. Soit $m \in M$, alors les deux assertions suivantes sont équivalentes :*

(i) $m \in \mathcal{S}M$.

(ii) Pour tout $\mathfrak{s}' \in \mathcal{S}'$, $\mathfrak{s}'m \in \mathcal{S}M$.

Démonstration. (1) Voir [47, Lemma 6.9, p. 93].

(2) Voir [25, Lemma 4.1.5, p. 577]. □

Enfin, soient K un corps de nombres contenant ξ et $K(\alpha^{1/l})/K$ une extension cyclique (de Kummer) de degré l. Puisque $l \neq 2$ et $lO_K = (1-\xi)^{l-1}O_K$, si $\alpha \equiv 1 \ mod^*\ l^2O_K$, alors, d'après [20, Theorem 119, p. 136], tout idéal premier $\mathfrak{p}$ de O_K divisant lO_K est totalement décomposé dans $K(\alpha^{1/l})/K$; en particulier, $K(\alpha^{1/l})/K$ est modérément ramifiée.

3.3 Démonstration des résultats principaux

Dans cette section, nous démontrons le théorème 3.1.1 et la proposition 3.1.2.

Démonstration du théorème 3.1.1. Rappelons qu'on veut montrer l'égalité $\mathcal{R}_1(\mathcal{M}) = \Lambda$, où Λ est le sous-ensemble de $\prod_{i=1}^n Cl(k(\chi_i)) \times Cl(E_0)$:

$$A = \left\{ \left(c_1, c_2, \ldots, c_n, x\phi_{E_0/k}\Big(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)\Big)\right) \Big| \right.$$
$$\left. (c_1, c_2, \ldots, c_n) \in \mathcal{R}(\mathcal{M}(H)), x \in \mathcal{S}Cl(E_0) \right\}.$$

(1) Montrons l'inclusion $\mathcal{R}_1(\mathcal{M}) \subset A$.

On utilise les hypothèses et notations de la proposition 3.2.2. Tout d'abord $(c_1, c_2, \ldots, c_n) \in \mathcal{R}(\mathcal{M}(H))$ par cette dernière. 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 H et [27, Proposition 12]) on obtient :

$$cl_k(O_{k_1}) = \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)^{\chi_i(1)} = \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i).$$

Rappelons l'égalité :

$$\langle b, \psi \rangle_{N/k_1}^{l} O_Z = (I(\psi))^l \theta J_1(\psi).$$

Dans ce qui suit on notera $\langle b, \psi \rangle_{N/k_1}$ simplement par $\langle b, \psi \rangle$. D'une façon naturelle, $N(\xi) \setminus \{0\}$ est un $\mathbb{Z}[Gal(N(\xi)/k)]$-module.

Soit $\mathfrak{s}' \in \mathcal{S}'$. On a :

$$(\mathfrak{s}' \langle b, \psi \rangle^l) O_Z = \mathfrak{s}' I(\psi)^l (\theta/l) \mathfrak{s}' J_1(\psi)^l.$$

Soit $(c - s_c) \in \mathcal{S}'$. L'élément $(c - s_c)\langle b, \psi \rangle$ appartient à Z car : D'une part

$$\begin{aligned} \sigma(c - s_c)\langle b, \psi \rangle &= \sigma(\langle b, \psi \rangle^c / s_c(\langle b, \psi \rangle)) \\ &= (\psi(\sigma)^c / \psi^c(\sigma))(c - s_c)\langle b, \psi \rangle = (c - s_c)\langle b, \psi \rangle. \end{aligned}$$

D'autre part, les égalités $\tau s_r(c - s_c) = (c - s_c)\tau s_r$ et $\tau s_r \langle b, \psi \rangle = \langle b, \psi \rangle$ impliquent $\tau s_r(c - s_c)\langle b, \psi \rangle = (c - s_c)\langle b, \psi \rangle$. Il s'ensuit que $\mathfrak{s}' \langle b, \psi \rangle \in Z$. D'où

$$(\mathfrak{s}' \langle b, \psi \rangle) O_Z = \mathfrak{s}' I(\psi)(\theta/l) \mathfrak{s}' J_1(\psi),$$

et donc $\mathfrak{s}' cl(I(\psi)^{-1}) \in \mathcal{S}Cl(Z)$ ($Cl(Z)$ a une structure naturelle de $\mathbb{Z}[S]$-module) car $\mathcal{S} = (1/l)\theta \mathcal{S}'$ en vertu de Proposition 3.2.5(1). On en déduit que $cl(I(\psi)^{-1})$ est un élément de $\mathcal{S}Cl(Z)$ par l'assertion (2) de la proposition 3.2.5. Par conséquent $N_{Z/E_0}(cl(I(\psi)^{-1})) \in \mathcal{S}Cl(E_0)$.

Posons $N_{Z/E_0}(cl(I(\psi)^{-1})) = x$. Alors $c_{n+1} = x\phi_{E_0/k}(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i))$. Ceci termine la démonstration de l'inclusion (1).

(2) Montrons l'inclusion $\Lambda \subset \mathcal{R}_1(\mathcal{M})$.

Soit $X = \Big(c_1, c_2, \ldots, c_n, x\phi_{E_0/k}\big(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)\big)\Big)$ un élément de A.

Tout d'abord on considère l'élément $(c_1, c_2, \ldots, c_n)$ de $\mathcal{R}(\mathcal{M}(H))$. Soit $Ex : Cl(O_k[H]) \to Cl(\mathcal{M}(H))$ la surjection induite par l'extension des scalaires de $O_k[H]$ à $\mathcal{M}(H)$. Puisque $Ex(\mathcal{R}(O_k[H])) = \mathcal{R}(\mathcal{M}(H))$, les assertions

(a), (b), et (c) de [26, Theorem 6.17, p. 289], nous affirment l'existence d'une extension modérée k_1/k à groupe de Galois isomorphe à $H =< \tau >$, telle que $[\mathcal{M}(H) \otimes_{O_k[H]} O_{k_1}] = (c_1, c_2, \ldots, c_n)$, la seule sous-extension de k_1/k non ramifiée sur k est k lui-même, et dont le discriminant est premier à lO_k. Signalons que la dernière condition sur le discriminant implique que k_1/k et $k(\xi)/k$ sont linéairement disjointes.

On rappelle qu'on peut définir $\lambda : Gal(k_1(\xi)/k) \longrightarrow (\mathbb{Z}/l\mathbb{Z})^*$, le morphisme de groupes qui à g fait correspondre $\nu(g)\mu(g)^{-1}$ (voir §3.2 juste après la proposition 3.2.1). Les extensions k_1/k et $k(\xi)/k$ étant linéairement disjointes, nous rappelons aussi qu'on peut appliquer [7, Proposition A.2(1), p. 341] et noter

$$Gal(k_1(\xi)/k) = \{s_i\tau^j \mid 1 \leq i \leq l-1, 0 \leq j \leq m-1\}.$$

Soit Z le sous-corps de $k_1(\xi)/k$ fixe par $ker(\lambda)(=< \tau s_r >)$. Par la proposition 3.2.4, toute sous-extension de Z/E_0 différente de E_0 est ramifiée. Ce dernier fait entraîne que $N_{Z/E_0} : Cl(Z) \to Cl(E_0)$ est surjective grâce au théorème 1.3.5. On en déduit que N_{Z/E_0} induit un morphisme surjectif de $\mathcal{S}Cl(Z)$ sur $\mathcal{S}Cl(E_0)$

Ensuite on considère l'élément x de $\mathcal{S}Cl(E_0)$. Soit $y \in \mathcal{S}Cl(Z)$ vérifiant

$$N_{Z/E_0}(y) = x.$$

D'après l'assertion (1) de la proposition 3.2.5, il existe un entier a, des idéaux fractionnaires I_i de O_Z, $1 \leq i \leq a$, qu'on peut choisir premiers avec lO_Z par le théorème de densité de Chebotarev, et des éléments $\mathfrak{s}'_i$, $1 \leq i \leq a$, de $\mathcal{S}'$ tels que :

$$y = cl\Big(\prod_{i=1}^{a}(1/l)\mathfrak{s}'_i\theta I_i\Big).$$

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

$$I^l = \theta J.$$

Soit le cycle $\mathcal{C} = l^2O_Z$. Par la surjection canonique de $Cl(Z,\mathcal{C})$ sur $Cl(Z)$ et le théorème de densité de Chebotarev, il existe un idéal premier $\mathfrak{p}$ de O_Z, totalement décomposé dans Z/k et tel que $cl(\mathfrak{p}) = cl(J)$ dans $Cl(Z,\mathcal{C})$. Il s'ensuit qu'il existe $\alpha' \in Z$ satisfaisant :

$$\mathfrak{p} = \alpha' J, \quad \alpha' \equiv 1 \ mod^* \ l^2O_Z.$$

Posons

$$\alpha = \theta\alpha'.$$

Alors

$$\alpha O_Z = (I^{-1})^l \theta \mathfrak{p}.$$

L'élément α n'est pas une puissance l-ième dans Z, car par exemple $v_{\mathfrak{p}}(\alpha) = 1$, où $v_{\mathfrak{p}}$ est la valuation $\mathfrak{p}$-adique. Il ne peut être une puissance l-ième dans $k_1(\xi)$, car sinon $Z(\alpha^{(1/l)})/Z$ serait une sous-extension de $k_1(\xi)/Z$ de degré l, et donc l diviserait m, ce qui est impossible.

Soit ω un élément d'une clôture algébrique de k vérifiant $\omega^l = \alpha$. Posons $L = k_1(\xi)(\omega)$. Alors $L/k_1(\xi)$ est une extension cyclique (de Kummer) de degré l. Rappelons que ψ est un caractère de degré 1 et d'ordre l du groupe (abstrait) C ; ψ a été choisi au §3.1. Tout d'abord choisissons un générateur σ de C tel que $\psi(\sigma) = \xi$. Ensuite identifions C avec $Gal(L/k_1(\xi))$ en faisant agir σ sur L de sorte que $\sigma(\omega) = \xi\omega$.

Pour tout i, $1 \leq i \leq (l-1)$, soit θ_i l'élément de Stickelberger : $\theta_i = (1/l)(i - s_i)\theta$. De $s_i\theta = i\theta - l\theta_i$, et en posant $c_i = (\theta_i\alpha')^{-1}$ on tire :

$$s_i(\alpha) = \alpha^i c_i^l, \quad \text{où} \quad c_i \in Z.$$

De l'égalité précédente on déduit que $Gal(k_1(\xi)/k_1)$ opère sur le sous-groupe $< \overline{\alpha} >$ de $k_1(\xi)^\times/(k_1(\xi)^\times)^l$ engendré par la classe de α (c'est le sous-groupe associé à l'extension $L/k_1(\xi)$ par la théorie de Kummer). Par conséquent L/k_1 est galoisienne ; elle est de degré $l(l-1)$.

Soit s_{i_0} un générateur de $Gal(k_1(\xi)/k_1)$. Notons s_{i_0} et c_{i_0} tout simplement par s et c, de sorte que $s(\alpha) = \alpha^{i_0}c^l$. Notons aussi par s un prolongement de s à L. L'égalité $\omega^l = \alpha$ entraîne $s(\omega)^l = s(\alpha) = (\omega^{i_0}c)^l$. On choisit le prolongement de s défini par $s(\omega) = \omega^{i_0}c$.

L'extension L/k_1 est abélienne, en effet : $\sigma s(\omega) = (\xi\omega)^{i_0}c = s\sigma(\omega)$. Le degré de L/k_1 étant égal à $l(l-1)$, le groupe abélien $Gal(L/k_1)$ admet un sous groupe d'ordre $l-1$. Donc il existe une sous-extension galoisienne N/k_1 de L/k_1 de degré l. Notons que puisque N/k_1 et $k_1(\xi)/k_1$ sont linéairement disjointes, on a $Nk_1(\xi) = L$, et les isomorphismes de restriction : $Gal(L/k_1(\xi)) \simeq Gal(N/k_1)$ et $Gal(L/N) \simeq Gal(k_1(\xi)/k_1)$.

Comme $\tau s_r(\alpha) = \alpha$ (rappelons que $Gal(k_1(\xi)/Z) =< \tau s_r >$), on a :

$$\tau(\alpha) = s_{r^*}(\alpha) = \alpha^{r^*} c_{r^*}^l.$$

On en déduit que $Gal(k_1(\xi)/k)$ opère sur $< \overline{\alpha} >$. Par suite L/k est galoisienne. En particulier, $L/k(\xi)$ est galoisienne de degré lm.

Pour simplifier les notations, posons $c_{r^*} = d$ et notons aussi par τ un prolongement de τ à L. De $\omega^l = \alpha$ on tire $\tau(\omega)^l = (\omega^{r^*}d)^l$. Choisissons le prolongement de τ défini par $\tau(\omega) = \omega^{r^*}d$.

Ci-dessous nous montrons que $Gal(L/k(\xi))$ est isomorphe à Γ. Pour cela, comme σ est d'ordre l, il reste à montrer que $\tau\sigma\tau^{-1} = \sigma^r$ et τ est d'ordre m. Il est immédiat qu'il suffit de faire les calculs à l'aide de ω.

D'une part $\tau\sigma(\omega) = \tau(\xi\omega) = \xi\omega^{r^*}d$, et d'autre part $\sigma^r\tau(\omega) = \sigma^r(\omega^{r^*}d) = d\sigma^r(\omega)^{r^*} = d(\xi^r\omega)^{r^*}$. Donc $\tau\sigma\tau^{-1} = \sigma^r$.

De $\tau(\omega) = \omega^{r^*}d$, on déduit $\tau^2(\omega) = \omega^{r^{*2}}d^{r^*}\tau(d)$. En réitérant le procédé, on obtient :

$$\tau^m(\omega) = \omega^{r^{*m}} \prod_{j=0}^{m-1} \tau^j(d)^{r^{*(m-1-j)}}.$$

Rappelons que la classe de r dans $(\mathbb{Z}/l\mathbb{Z})^*$ est d'ordre m, et donc celle de r^* aussi. Soit e un entier naturel vérifiant $r^{*m} = 1 + el$. Alors

$$\tau^m(\omega) = \omega\alpha^e \prod_{j=0}^{m-1} \tau^j(d)^{r^{*(m-1-j)}}.$$

De $\tau(\alpha) = \alpha^{r^*}d^l$ on obtient comme ci-dessus :

$$\tau^m(\alpha) = \alpha^{r^{*m}}[\prod_{j=0}^{m-1} \tau^j(d)^{r^{*(m-1-j)}}]^l = \alpha[\alpha^e \prod_{j=0}^{m-1} \tau^j(d)^{r^{*(m-1-j)}}]^l.$$

Mais $\tau^m(\alpha) = \alpha$ (puisque la restriction de τ à $k_1(\xi)$ est d'ordre m). Donc

$$[\alpha^e \prod_{j=0}^{m-1} \tau^j(d)^{r^{*(m-1-j)}}]^l = 1.$$

Comme $\xi \notin Z$ (rappelons que $Z(\xi) = k_1(\xi)$), $\alpha^e \prod_{j=0}^{m-1} \tau^j(d)^{r^{*(m-1-j)}} = 1$. Par suite $\tau^m(\omega) = \omega$, d'où τ est d'ordre m. Ceci achève la démonstration de l'assertion : $Gal(L/k(\xi))$ est isomorphe à Γ.

Nous allons maintenant prouver que N/k est galoisienne modérée, à groupe de Galois isomorphe à Γ.

Montrons l'égalité : $s\tau = \tau s$. On a $s\tau(\omega) = \omega^{i_0r^*}c^{r^*}s(d)$ et $\tau s(\omega) = \omega^{i_0r^*}d^{i_0}\tau(c)$. Mais $s\tau(\alpha) = \tau s(\alpha)$, d'où $[c^{r^*}s(d)]^l = [d^{i_0}\tau(c)]^l$, ce qui entraîne $c^{r^*}s(d) = d^{i_0}\tau(c)$ puisque $\xi \notin Z$. Donc $s\tau(\omega) = \tau s(\omega)$, d'où $s\tau = \tau s$.

Rappelons que $s\sigma = \sigma s$. Par conséquent s appartient au centre de $Gal(L/k)$, en particulier le sous-groupe $< s >$ engendré par s est un sous-groupe distingué de $Gal(L/k)$. Comme N est le sous-corps de L fixe par

$< s >$, N/k est galoisienne. Il est immédiat que N/k et $k(\xi)/k$ sont linéairement disjointes et $L = Nk(\xi)$. On en déduit que $Gal(L/k(\xi))$ est isomorphe par restriction à $Gal(N/k)$. Donc $Gal(N/k) \simeq \Gamma$.

De $\alpha' \equiv 1 \ mod^* \ l^2 O_Z$ et $\alpha = \theta\alpha'$, on tire $\alpha \equiv 1 \ mod^* \ l^2 O_Z$. Il s'ensuit que

$$\alpha \equiv 1 \ mod^* \ l^2 O_{k_1(\xi)}.$$

Par conséquent $L/k_1(\xi)$ est modérément ramifiée par le rappel provenant de la théorie de Kummer et situé à la fin du §3.2. Comme $k_1(\xi)/k$ est modérée car c'est une composée des extensions k_1/k et $k(\xi)/k$ qui le sont, l'extension L/k est modérée. Par suite N/k est modérée puisque c'est une sous-extension de L/k.

Soit K/k la sous-extension de degré l de N/k fixe par $< \tau >$. Soit b un élément de K engendrant une base normale de N/k_1 (donc $\langle b, \psi \rangle \neq 0$). On a $L = k_1(\xi)(\langle b, \psi \rangle)$, car ψ est non trivial, $\langle b, \psi \rangle \neq 0$ et $\langle b, \psi \rangle^l \in k_1(\xi)$. Par la théorie de Kummer, il existe $g \in k_1(\xi)$ et i, $1 \leq i \leq (l-1)$, tels que $\alpha = g^l \langle b, \psi \rangle^{li}$. Comme $\omega^l = \alpha$, il existe j, $0 \leq j \leq (l-1)$, satisfaisant $\omega = g\langle b, \psi \rangle^i \xi^j$. Rappelons que $\sigma(\langle b, \psi \rangle) = \psi(\sigma)\langle b, \psi \rangle$ et $\psi(\sigma) = \xi$. D'où $\sigma(\omega) = \xi^i \omega$. Par conséquent $i = 1$, car $\sigma(\omega) = \xi\omega$. Donc

$$\alpha = g^l \langle b, \psi \rangle^l.$$

Mais $\langle b, \psi \rangle^l \in Z$ et $\alpha \in Z$, par suite $g \in Z$ (sinon $Z(g)/Z$ serait une sous-extension de $k_1(\xi)/Z$ de degré l, et l diviserait m). En utilisant la décomposition (de façon unique) $\alpha O_Z = (I^{-1})^l \theta \mathfrak{p}$ on obtient :

$$\langle b, \psi \rangle^l O_Z = ((gI)^{-1})^l \theta \mathfrak{p}$$

est la décomposition (de façon unique) de $\langle b, \psi \rangle^l O_Z$.

Rappelons que $y = cl(I)$ et $N_{Z/E_0}(y) = x$. Alors

$$N_{Z/E_0}(cl((gI))) = N_{Z/E_0}(cl(I)) = x.$$

Puisque $cl_k(O_{k_1}) = \prod_{i=1}^n N_{k(\chi_i)/k}(c_i)$, on conclut que $X = [\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ grâce à la proposition 3.2.2. Donc $A \subset \mathcal{R}_1(\mathcal{M})$. Ceci termine la démonstration du théorème 3.1.1.

Remarque. Nous n'avons pas réussi à montrer l'existence de N/k à l'aide de [7, Proposition A.1, p. 341], cela aurait pu nous raccourcir la démonstration précédente en évitant un calcul explicite de $Gal(L/k(\xi))$; lorsque m est un nombre premier, on peut trouver un calcul similaire au notre dans [10, 44].

Démonstration de la proposition 3.1.2.

(1) Montrons l'inclusion $R_{mo}(k,\Gamma) \subset R_{mo}(k,H)^l N_{E_0/k}(Cl(E_0))^{m(l-1)/2}$ pour tout corps de nombres k.

Soit N/k une extension galoisienne modérée à groupe de Galois isomorphe à Γ. Soit k_1/k sa sous-extension fixe par C. Par la transitivité de la classe de Steinitz dans une tour de corps de nombres (voir Proposition 1.4.2(ii))

$$cl_k(O_N) = (cl_k(O_{k_1}))^l N_{k_1/k}(cl_{k_1}(O_N)).$$

Comme le degré de l'extension N/k_1 est impair, par un résultat d'Artin (voir Théorème 1.4.1) on a

$$cl_{k_1}(O_N) = cl(\Delta(N/k_1)^{1/2}).$$

Soit $\mathfrak{F}$ le conducteur d'Artin d'un caractère de degré 1 et d'ordre l de C. Alors $\Delta(N/k_1) = \mathfrak{F}^{l-1}$ par la décomposition d'Artin et Hasse du discriminant en un produit de conducteurs. Comme N/k_1 est modérée, il suit de [21, Proposition 2.5] que

$$\mathfrak{F} = (\prod_{i=1}^{a} \mathfrak{p}_i) O_{k_1},$$

où a est un entier et les $\mathfrak{p}_i$ sont des idéaux premiers distincts de O_k. On en déduit :

$$N_{k_1/k}(cl_{k_1}(O_N)) = cl(\prod_{i=1}^{a} \mathfrak{p}_i)^{m(l-1)/2}.$$

On conclut qu'on a notre première inclusion car $cl(\mathfrak{p}_i) \in N_{E_0/k}(Cl(E_0))$ par [7, Proposition A.4(3), p. 342] et $cl_k(O_{k_1}) \in R_{mo}(k,H)$.

(2) Montrons l'inclusion : $R_{mo}(k,H)^l N_{E_0/k}(Cl(E_0))^{m(l-1)/2} \subset R_{mo}(k,\Gamma)$.

Soit $c \in R_{mo}(k,H)$. Par [26], il existe k_1/k une extension galoisienne modérée à groupe de Galois isomorphe à H, telle que $cl_k(O_{k_1}) = c$, la seule sous-extension de k_1/k non ramifiée sur k est k lui-même, et dont le discriminant est premier à lO_k. Il est clair que k_1/k et $k(\xi)/k$ sont linéairement disjointes.

Soit $(c_1, c_2, \ldots, c_n)$ la classe de $[\mathcal{M}(H) \otimes_{O_k[H]} O_{k_1}]$ dans $\prod_{i=1}^{n} Cl(k(\chi_i))$. Supposons dorénavant que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ soient linéairement disjointes. Soient $x \in SCl(E_0)$ et $X = (c_1, c_2, \ldots, c_n, x\phi_{E_0/k}(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)))$. D'après le théorème 3.1.1, $X \in \mathcal{R}_1(\mathcal{M})$. Donc il existe une extension galoisienne modérée N_x/k, à groupe de Galois isomorphe à Γ, telle que $X = [\mathcal{M} \otimes_{O_k[\Gamma]} O_{N_x}]$. Soient f un représentant de X dans la Hom-description de $Cl(\mathcal{M})$ et r_Γ le

caractère de la représentation régulière de Γ. En utilisant [15, pp. 62-63], on voit que $cl_k(O_{N_x})$ est représentée par le contenu de l'idèle $f(r_C) \in J(k)$ (ceci est [27, Proposition 12] et l'idée de sa preuve). On en déduit :

$$cl_k(O_{N_x}) = \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)^{\chi_i(1)} N_{E_0/k}\Big(x\phi_{E_0/k}(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i))\Big)^{\chi(1)}.$$

Rappelons que $\chi_i(1) = 1$, $\chi(1) = m$ et $cl_k(O_{k_1}) = \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)^{\chi_i(1)} = c$. Donc

$$cl_k(O_{N_x}) = cc^{m(l-1)/m} N_{E_0/k}(x)^m = c^l N_{E_0/k}(x)^m.$$

Par conséquent $c^l N_{E_0/k}(\mathcal{S}Cl(E_0))^m \subset R_{mo}(k, \Gamma)$.

Il est immédiat que $N_{E_0/k}(\mathcal{S}Cl(E_0)) = N_{E_0/k}(Cl(E_0))^{(l-1)/2}$. Il s'ensuit que $c^l N_{E_0/k}(Cl(E_0))^{m(l-1)/2} \subset R_{mo}(k, \Gamma)$, d'où notre seconde inclusion. Ceci achève la démonstration de la proposition 3.1.2.

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 (2009), no. 2, 177–191.

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

[4] N. P. Byott, C. Greither et B. Sodaïgui, *Classes réalisables d'extensions non abéliennes*, J. reine angew. Math. 601 (2006) 1–27.

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

[6] N. P. Byott and 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] J. E. Carter et B. Sodaïgui, *Classes de Steinitz d'extensions quaternioniennes généralisées de degreé $4p^r$*, J. London Math. Soc. (2) 76 (2007) 331–344.

[8] A. Cobbe, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, J. Number Theory 130 (2010) 1129–1154.

[9] H. Cohen, *Advanced Topics in Computational Number Theory*, Grad. Texts in Math. 193, Springer-Verlag, New York, 2000.

[10] J. Cougnard, *Construction des extensions galoisiennes non abéliennes d'ordre pq (p et q premiers) du corps des rationnels*, Séminaire de Théorie des Nombres de Bordeaux, 1971–1972, Exposé no.10 bis, 12 pp.

[11] C. W. Curtis and I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders*, Vol. II, Wiley-Interscience, New York, 1987.

[12] A. Fröhlich, *The discriminant of relative extensions and the existence of integral bases*, Mathematika 7 (1960) 15–22.

[13] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, J. reine angew. Math. 286/287 (1976) 380–440.

[14] A. Fröhlich, *Galois Module Structure*, in : Algebraic Number Fields, Proceedings of the Durham Symposium, 1975, Academic Press, London, 1977, pp. 133–191.

[15] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Springer-Verlag, Berlin, 1983.

[16] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. reine angew. Math. 360 (1985) 84–123.

[17] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1991.

[18] H. G. Grundman and T. L. Smith, *Automatic realizability of Galois groups of order* 16, Proc. Amer. Math. Soc. 124 (1996) 2631–2640.

[19] H. G. Grundman, T. L. Smith and J. R. Swallow, *Groups of order* 16 *as Galois groups*, Exposition. Math. 13 (1995) 289–319.

[20] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer-Verlag, New York, 1981.

[21] S. Kwon et J. Martinet, *Sur les corps résolubles de degré premier*, J. reine angew. Math. 375/376 (1987) 12–23.

[22] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, Benjamin, New York/Addison-Wesley, Massachusetts, 1973 (Revised printing 1980).

[23] A. Ledet, *On* 2*-groups as Galois groups*, Can. J. Math. (47) (6) (1995) 1253–1273.

[24] J. Martinet, *Sur l'arithmétique d'une extension galoisienne à groupe de Galois diédral d'ordre* $2p$, Ann. Inst. Fourier (1969) 1–80.

[25] L. R. McCulloh, *A Stickelberger condition on Galois module structure for Kummer extensions of prime degree*, in : Algebraic Number Fields, Proceedings of the Durham Symposium, 1975, Academic Press, London (1977), pp. 561–588.

[26] L. R. McCulloh, *Galois module structure of abelian extensions*, J. reine angew. Math. 375/376 (1987) 259–306.

[27] L. R. McCulloh, *From Galois module classes to Steinitz classes*, Informal report (2002), Oberwolfach (Orders in arithmetic and geometry).

[28] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. 21 (1973) 59–116.

[29] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

[30] E. Noether, *Normalbasis bei Körpen ohne höhere Verzweigung*, J. reine angew. Math. 167 (1931), 147–152.

[31] J.-J. Payan, *Critère de décomposition d'une extension de Kummer sur un sous corps du corps de base*, Ann. Sci. Ecole Norm. Sup. 1 (1968) 445–458.

[32] I. Reiner, *Maximal Orders*, Oxford University Press, 2003.

[33] D.J.S. Robinson, *A Course in The Theory of Groups*, Grad. Texts in Math. 80, Springer-Verlag, New York, 1982.

[34] J.-P. Serre, *Corps Locaux*, 3ème édition, Hermann, Paris, 1980.

[35] T. L. Smith, *Extra-special groups of order* 32 *as Galois groups*, Can. J. Math. 46 (4) (1995) 886–896.

[36] T. L. Smith and J. Minac, *A characterisation of C-fields via Galois groups*, J. Algebra 137 (1991) 1–11.

[37] B. Sodaïgui, *Structure galoisienne relative des anneaux d'entiers*, J. Number Theory 28, no.2 (1988) 189–204.

[38] B. Sodaïgui, *Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger*, J. Number Theory 65 (1997) 87–95.

[39] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement*, Illinois J. Math. 43 (1999) 47–60.

[40] B. Sodaïgui, *"Galois module structure" des extensions quaternioniennes de degré 8*, J. Algebra 213 (1999) 549–556.

[41] B. Sodaïgui, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, J. Algebra 223 (2000) 367–378.

[42] B. Sodaïgui, *Realizable Classes of quaternion extensions of degree 4l*, J. Number Theory 80 (2000) 304–315.

[43] B. Sodaïgui, *Relative Galois module structure of octahedral extensions*, J. Algebra 312 (2007) 590–601.

[44] E. Soverchia, *Steinitz classes of metacyclic extensions*, J. London Math. Soc. (2) 66 (1) (2002) 61–72.

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

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

[47] L. C. Washington, *Introduction to Cyclotomic Fields*, second ed., Springer-Verlag, Berlin, 1996.

Classes de Steinitz et classes galoisiennes réalisables d'extensions non abéliennes

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 Γ un groupe non abélien d'ordre 16, ou un groupe extraspécial d'ordre 32. 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 Γ. Lorsque Γ est le groupe modulaire d'ordre 16, on suppose que k contienne une racine primitive 4ème de l'unité. Dans la thèse on montre que $R_m(k,\Gamma)$ est le groupe $Cl(k)$ tout entier si le nombre des classes de k est impair. On étudie un problème de plongement en liaison avec les classes de Steinitz dans la perspective de l'étude des classes galoisiennes réalisables. On prouve que pour tout $c \in Cl(k)$, il existe une extension quadratique de k, modérée, dont la classe de Steinitz est c, et qui est plongeable dans une extension galoisienne de k, modérée et à groupe de Galois isomorphe à Γ.

Un résumé de la deuxième partie est le suivant. Soient k un corps de nombres et O_k son anneau d'entiers. Soit C (resp. H) un groupe cyclique d'ordre l (resp. m). Soit $\Gamma = C \rtimes H$ un groupe métacyclique d'ordre lm, avec H opérant fidèlement sur C. 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 galoisiennes réalisables comme étant l'ensemble des classes $c \in Cl(\mathcal{M})$ telles qu'il existe une extension N/k modérée, à groupe de Galois isomorphe à Γ, avec la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ est égale à c, où O_N est l'anneau des entiers de N. Dans la thèse, on définit un sous-ensemble de $\mathcal{R}(\mathcal{M})$ et on montre, par l'intermédiaire d'une description utilisant un idéal de Stickelberger, qu'il est un sous-groupe de $Cl(\mathcal{M})$, sous l'hypothèse que k est linéairement disjoint du l-ième corps cyclotomique sur $\mathbb{Q}$.

Mots-clés : Structure de module galoisien ; Anneaux d'entiers ; Classes réalisables ; Classes de Steinitz ; Ordre maximal ; Groupe des classes des modules localement libres ; Problème de plongement ; Idéal de Stickelberger.

Steinitz classes and realizable Galois module classes of nonabelian extensions

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 Γ be a nonabelian group of order 16 or an extra-special group of order 32. Let $R_m(k,\Gamma)$ be the subset of $Cl(k)$ consisting of those classes which are realizable as Steinitz classes of tame Galois extensions of k with Galois group isomorphic to Γ. When Γ is the modular group of order 16, we assume that k contains a primitive 4th root of unity. In the thesis we show that $R_m(k,\Gamma)$ is the full group $Cl(k)$ if the class number of k is odd. We study an embedding problem connected with Steinitz classes in the perspective of studying realizable Galois module classes. We prove that for all $c \in Cl(k)$, there exist a tame quadratic extension of k, with Steinitz class c, and which is embeddable in a tame Galois extension of k with Galois group isomorphic to Γ.

An abstract for the second part is the following. Let k be a number field and O_k its ring of integers. Let l be a prime number and m a natural number. Let C (resp. H) be a cyclic group of order l (resp. m). Let $\Gamma = C \rtimes H$ be a metacyclic group of order lm, with H acting faithfully on C. 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 Galois module 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 Γ, and for which $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$, where O_N is the ring of integers of N. In the thesis, we define a subset of $\mathcal{R}(\mathcal{M})$ and prove, by means of a description using a Stickelberger ideal, that it is a subgroup of $Cl(\mathcal{M})$, under the hypothesis that k and the l-th cyclotomic field over $\mathbb{Q}$ are linearly disjoint.

Keywords : Galois module structure ; Ring of integers ; Realizable classes ; Steinitz classes ; Maximal order ; Locally free class groups ; Embedding problem ; Stickelberger ideal.

MATHEMATIQUES PURES

Laboratoire de Mathématiques LAMAV, Université de Valenciennes et du Hainaut Cambrésis

Le Mont Houy, 59313 Valenciennes Cedex 9