# Structure galoisienne d'anneaux entiers

Marjory Godin

N° d'ordre : 02/18

# THÈSE

présentée à

**L'UNIVERSITÉ DE VALENCIENNES ET DU HAINAUT CAMBRÉSIS**

par **Marjory GODIN**

POUR OBTENIR LE GRADE DE

**DOCTEUR**

SPÉCIALITÉ : MATHÉMATIQUES PURES

# Structure Galoisienne d'anneaux d'entiers

Soutenue le 25 Juin 2002

**Composition du jury**

**Président** : Ph. CASSOU-NOGUÈS, Professeur, Université Bordeaux 1
**Rapporteurs** : L. McCULLOH, Professeur, Université d'Illinois à Urbana (U.S.A.)
C. GREITHER, Professeur, Université de Munich (Allemagne)
**Examinateurs** : N. BYOTT, Maître de Conférences, Université d'Exeter (Angleterre)
J.C. DOUAI, Professeur, Université Lille 1
**Directeur de Thèse** : B. SODAÏGUI, Maître de Conférences H.D.R., Université de Valenciennes

N° d'ordre : 02/18

# THÈSE

présentée à

**L'UNIVERSITÉ DE VALENCIENNES ET DU HAINAUT CAMBRÉSIS**

par **Marjory GODIN**

POUR OBTENIR LE GRADE DE

**DOCTEUR**

SPÉCIALITÉ : MATHÉMATIQUES PURES

# Structure Galoisienne d'anneaux d'entiers

Soutenue le 25 Juin 2002

**Composition du jury**

**Président** : Ph. CASSOU-NOGUÈS, Professeur, Université Bordeaux 1
**Rapporteurs** : L. McCULLOH, Professeur, Université d'Illinois à Urbana (U.S.A.)
C. GREITHER, Professeur, Université de Munich (Allemagne)
**Examinateurs** : N. BYOTT, Maître de Conférences, Université d'Exeter (Angleterre)
J.C. DOUAI, Professeur, Université Lille 1
**Directeur de Thèse** : B. SODAÏGUI, Maître de Conférences H.D.R., Université de Valenciennes

# REMERCIEMENTS

Quelques mots pour remercier les personnes qui m'ont permis de mener à terme ce travail.

Je voudrais tout d'abord exprimer ma reconnaissance à Bouchaïb SODAÏGUI, mon directeur de thèse. Il a toujours su se montrer disponible, son optimisme et son dynamisme ont été des éléments moteurs pendant ces trois années. Je le remercie également pour le sujet riche en perspectives qu'il m'a confié.

Je remercie les membres du jury pour l'intêret qu'ils ont porté à ce travail.

Je suis reconnaissante à Cornelius GREITHER et Leon McCULLOH d'avoir accepté d'être les rapporteurs de ce travail. Leurs lectures attentives sont à l'origine de certaines améliorations.

Je remercie Philippe CASSOU-NOGUÈS d'avoir bien voulu présider le jury de soutenance. J'adresse ma gratitude à Nigel BYOTT et Jean-Claude DOUAI qui ont accepté d'examiner ce travail.

Merci à Laurence NISON pour sa confiance et son dévouement. Elle a été à l'origine de ma rencontre avec Bouchaïb SODAÏGUI.

Enfin je remercie tous mes proches qui m'ont supportée et soutenue. En particulier, je remercie mes parents qui m'ont soutenue moralement et financièrement tout au long de ce parcours.

# Table des matières

# Introduction

Soient $k$ un corps de nombres et $O_k$ son anneau d'entiers. Soient $\overline{k}$ une clôture algèbrique de $k$ et $Gal(\overline{k}/k)$ son groupe de Galois. Soit $\Gamma$ un groupe fini. A tout homomorphisme surjectif $\pi$ défini sur $Gal(\overline{k}/k)$ et à valeurs dans $\Gamma$, on associe le sous corps $N$ de $\overline{k}$ fixe par $Ker\pi$. L'extension $N/k$ est galoisienne et son groupe de Galois $Gal(N/k)$ est isomorphe à $Gal(\overline{k}/k)/Ker\pi$, d'où un isomorphisme, que l'on note aussi $\pi$, défini sur $Gal(N/k)$ et à valeurs dans $\Gamma$. Soit $O_N$ l'anneau d'entiers de $N$. A l'aide de $\pi$ on munit $O_N$ d'une structure de $O_k[\Gamma]$-module définie de la manière suivante : pour tout $x \in O_N$ et tout $\gamma \in \Gamma$, on pose $\gamma x = \pi^{-1}(\gamma)(x)$. Soit $\mathcal{M}$ un ordre maximal de $O_k$ dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$. Lorsque $N/k$ est modérément ramifiée, on peut associer à $O_N$ une classe, notée $[O_N]$, dans $Cl(O_k[\Gamma])$ le groupe des classes de $O_k[\Gamma]$, et 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 $Cl(\mathcal{M})$ le groupe des classes de $\mathcal{M}$.

On désigne par $\mathcal{R}(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M})$) l'ensemble des classes $c$ de $Cl(O_k[\Gamma])$ (resp. $Cl(\mathcal{M})$) telle qu'il existe une extension $N/k$ modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$, avec $[O_N] = c$ (resp. $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$) ; on dira que $c$ est réalisable par l'extension $N/k$ et que $\mathcal{R}(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M})$) est l'ensemble des classes réalisables.

Il est bien connu que $\mathcal{R}(O_k[\Gamma]) \subset Cl^\circ(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$) (voir [Mc1]), où $Cl^\circ(O_k[\Gamma])$ (resp. $Cl^\circ(\mathcal{M})$) est 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. $\mathcal{M} \to O_k$).

Les résultats de McCulloh (voir [Mc2]) vont dans le sens de la conjecture suivante :

**Conjecture 1.** *$\mathcal{R}(O_k[\Gamma])$ est un sous-groupe de $Cl^\circ(O_k[\Gamma])$.*

Pour prouver cette conjecture, il y a des difficultés qui proviennent des unités locales des algèbres de groupes (voir la preuve d'une conjecture de Fröhlich dans [T]). Pour contourner cette difficulté on étudie la conjecture plus faible suivante :

**Conjecture 2.** *$\mathcal{R}(\mathcal{M})$ est un sous-groupe de $Cl^\circ(\mathcal{M})$.*

Signalons qu'une conséquence de la preuve de l'une de ces deux conjectures serait la résolution du problème inverse de la théorie de Galois (voir [Se3]) par une nouvelle méthode qui provient de l'étude des questions concernant la structure galoisienne des anneaux d'entiers ; ce qui renforce, encore une nouvelle fois, avec (entre autres) la découverte d'un lien étroit entre cette structure et des invariants arithmétiques associés aux caractères de $\Gamma$ provenant de l'équation fonctionnelle des fonctions $L$ d'Artin (voir [F3] et [T]), le caractère profond de ces questions.

Le cas où $k = \mathbb{Q}$ et $\Gamma$ réalisable comme groupe de Galois sur $\mathbb{Q}$ est bien connu. La conjecture 1 est vérifiée (voir [T]) ; plus précisément $\mathcal{R}(\mathbb{Z}[\Gamma])$ est un 2-groupe, de plus il est trivial si $\Gamma$ ne possède pas de caractère symplectique (c'est le cas par exemple de $\Gamma$ abélien ou d'ordre impair). Quant à $\mathcal{R}(\mathcal{M})$, il est toujours trivial (voir [F3, corollaire du théorème 6, p. 40–41]).

Si $k$ est un corps de nombres quelconque et $\Gamma$ est abélien, McCulloh (voir [Mc2]) a montré que la conjecture 1 est vraie en utilisant une "correspondance de Stickelberger".

Dans [So2] on se place dans la situation où $\Gamma$ est le groupe métacyclique non abélien d'ordre $lq$, où $l$ et $q$ sont deux nombres premiers, et $k/\mathbb{Q}$ est linéairement disjoint du $lq^{\text{ième}}$ corps cyclotomique de $\mathbb{Q}$. On montre qu'on a la conjecture 2.

Lorsque $\Gamma$ est le groupe diédral (resp. quaternionien) d'ordre 8 et $k$ est un corps de nombres linéairement disjoint sur $\mathbb{Q}$ de $\mathbb{Q}(i)$, où $i^2 = -1$, on montre dans [So4] (resp. [So5]) que si le nombre des classes (resp. le nombre des classes au sens restreint) de $k$ est impair, alors $\mathcal{R}(\mathcal{M}) = Cl^\circ(\mathcal{M})$.

Dans [So6], on considère le cas où $\Gamma$ est le groupe quaternonien d'ordre $4l$, où $l$ est un nombre premier impair. On définit deux sous-ensembles de $\mathcal{R}(\mathcal{M})$ et on montre qu'ils sont deux sous-groupes de $Cl^\circ(\mathcal{M})$ pourvu que 2 et $l$ ne soient pas ramifiés dans $k$.

Dans la suite, si $K$ est un corps de nombres, $O_K$ désigne l'anneau des entiers de $K$ et $Cl(K)$ son groupe des classes.

Dans cette thèse, l'un des principaux résultats est le théorème suivant :

**Théorème 1.** *Soit $\Gamma$ le groupe alterné $A_4$. Soient $j$ une racine primitive $3^{ième}$ de l'unité et $k$ un corps de nombres linéairement disjoint de $\mathbb{Q}(j)$ sur $\mathbb{Q}$. Alors $\mathcal{R}(\mathcal{M})$ est le groupe $Cl^{\circ}(\mathcal{M})$. Dans ce cas, $\mathcal{R}(\mathcal{M}) \simeq Cl(k(j)) \times Cl(k)$.*

Rappelons la définition de la classe de Steinitz. Soit $K/k$ une extension finie de corps de nombres de degré $n$. L'anneau $O_K$ est un $O_k$-module sans torsion de rang $n$, donc il existe un idéal $I$ de $O_k$ tel que $O_K \simeq O_k^{n-1} \oplus I$ en tant que $O_k$-module. La classe de $I$ dans $Cl(k)$ est appelée la classe de Steinitz de l'anneau $O_K$ ou de l'extension $K/k$, et on la note $cl_k(O_K)$ (voir [FT,Theorem 13, p. 95]).

Lorsque nous essayons d'étudier la conjecture 2, nous sommes confrontés au problème de plongement en liaison avec les classes de Steinitz.

Une autre partie de la thèse est l'étude des classes de Steinitz dans le cadre qu'on va maintenant définir.

Soient $\Gamma$ un groupe fini et $\Delta$ un sous-groupe normal de $\Gamma$. On a donc la suite exacte de groupes suivante :

$$\Sigma : 1 \longrightarrow \Delta \longrightarrow \Gamma \longrightarrow \Gamma/\Delta \longrightarrow 1.$$

Fixons $E/k$ une extension galoisienne dont le groupe de Galois est isomorphe à $\Gamma/\Delta$. On désigne par $R(E/k,\Sigma)$ (resp. $R_m(E/k,\Sigma)$) l'ensemble des classes $c \in Cl(k)$ vérifiant : il existe une extension galoisienne (resp. galoisienne et modérément ramifiée) $N/k$ dont la classe de Steinitz est $c$, contenant $E$, et dont le groupe de Galois est isomorphe à $\Gamma$, avec un isomorphisme $\pi$ de $Gal(N/k)$ dans $\Gamma$ satisfaisant $E$ est le sous-corps de $N$ fixe par $\pi^{-1}(\Delta)$.

Lorsque $\Delta = \Gamma$, $R(E/k,\Sigma)$ (resp. $R_m(E/k,\Sigma)$) est tout simplement l'ensemble des classes de Steinitz des extensions galoisiennes (resp. galoisiennes et modérées) de $k$, dont le groupe de Galois est isomorphe à $\Gamma$ ; on note $R(k,\Gamma)$ et $R_m(k,\Gamma)$ au lieu de $R(E/k,\Sigma)$ et $R_m(E/k,\Sigma)$.

Signalons un lien immédiat avec les deux conjectures précédentes. Oublions l'action de $\Gamma$, il est clair que la conjecture 1 implique la conjecture suivante :

**Conjecture 3.** *$R_m(k,\Gamma)$ est un sous-groupe de $Cl(k)$.*

Soient $p$ et $q$ deux nombres premiers impairs. Dans [C1], sous l'hypothèse que $k$ contient les racines $p^{\text{ième}}$ de l'unité, on détermine $R_m(E/k,\Sigma)$ lorsque $\Gamma$ est un groupe non abélien d'ordre $p^3$ d'exposant $p$ et $\Delta$ un sous-groupe de $\Gamma$ d'ordre $p^2$, et on montre que si $O_E$ est un $O_k$-module libre alors $R_m(E/k,\Sigma)$ est un sous-groupe de $Cl(k)$. Dans [C3] on montre des résultats analogues à ceux de [C1] dans la situation où $k$ contient les racines $pq^{\text{ième}}$ de l'unité, $\Gamma$ est un groupe métacylique d'ordre $pq$, et $\Delta$ est le sous-groupe de $\Gamma$ d'ordre $p$.

Lorsque $\Gamma$ est abélien, une conséquence des travaux de McCulloh (voir [Mc2]) est : $R_m(k,\Gamma)$ est un sous-groupe de $Cl(k)$. Dans [C2], on montre que $R_m(k,\Gamma)$ est un sous-groupe de $Cl(k)$ dans le cas où $\Gamma$ est un groupe non abélien d'ordre $p^3$ ($p$ premier impair), et $k$ contient les racines $m^{\text{ième}}$ de l'unité, où $m$ est l'exposant de $\Gamma$. Lorsque $\Gamma$ est le groupe quaternionien (resp. diédral) d'ordre 8, on montre dans [So3] (resp. [So4]) que si le nombre des classes de $k$ est impair alors $R_m(k,\Gamma) = Cl(k)$.

Dans cette thèse, on s'intéresse à la situation où $\Gamma$ est le groupe alterné $A_4$ défini par la présentation :

$$A_4 = \langle \sigma, \tau, \nu : \sigma^3 = \tau^2 = \nu^2 = 1, \tau\nu = \nu\tau, \sigma\tau\sigma^{-1} = \nu, \sigma\nu\sigma^{-1} = \tau\nu \rangle,$$

et

$$\Delta = \langle \tau, \nu \rangle.$$

On a $Gal(E/k) \cong \langle \sigma \rangle$, donc $E/k$ est une extension cyclique de degré 3.

On démontre le résultat suivant :

**Théorème 2.** *Soient $k$ un corps de nombres et $E/k$ une extension cyclique de degré 3. Alors :*

*(i)* $$R(E/k,\Sigma) = cl_k(O_E)(N_{E/k}(Cl(E)))^3,$$

*où $N_{E/k}$ est la norme dans $E/k$ et $(N_{E/k}(Cl(E)))^3$ est le sous-groupe des puissances $3^{\text{ième}}$ des éléments du groupe $N_{E/k}(Cl(E))$.*

*De plus, si $E/k$ est modérée alors $R_m(E/k,\Sigma) = R(E/k,\Sigma)$.*

*(ii) Soit $j$ une racine primitive troisième de l'unité. Soit $W$ le sous-groupe de $Cl(k)$ engendré par $N_{k(j)/k}(Cl(k(j)))$ et les classes des idéaux premiers de $O_k$ au-dessus de 3, où $N_{k(j)/k}$ désigne la norme dans $k(j)/k$. Alors*

$$R(k, A_4) = WCl(k)^3,$$

$$R_m(k, A_4) = N_{k(j)/k}(Cl(k(j)))Cl(k)^3.$$

Nous avons aussi étudié le cas où $\Gamma = S_4$ ; sous l'hypothèse que le nombre des classes de $k$ est impair nous avons montré un théorème analogue au théorème 2 (voir Chap. 2, §1, Théorème 2.3.1).

Nous donnons ci-dessous les grandes lignes de la démarche adoptée dans cette thèse.

Fröhlich a généralisé au cas non abélien la notion classique de résolvante de Lagrange et a donné une nouvelle description du groupe des classes d'un ordre en terme d'homomorphismes galoisiens du groupe des caractères virtuels de $\Gamma$ dans certains autres groupes (voir [F3]). D'autre part, un résultat de Swan (voir Chap. 1, §1, Théorème 1.1.2) permet de décrire le groupe des classes d'un ordre maximal comme un produit de groupes des classes des centres des facteurs simples de l'algèbre semi-simple $k[\Gamma]$.

Les outils fondamentaux de la démarche sont :

-Les deux descriptions précédentes.

-Les propriétés des résolvantes de Lagrange sous l'action galoisienne, et leurs propriétés fonctorielles relatives à l'induction, restriction et inflation de caractères de sous-groupes de $\Gamma$.

-La résolution de problèmes de plongement en liaison avec les classes de Steinitz, grâce aux critères de plongement, le calcul des classes de Steinitz, la théorie du corps de classes et le théorème de densité généralisé de Dirichlet dans les groupes de classes de rayon.

Le plan de cette thèse est le suivant :

Le premier chapitre contient les définitions et résultats nécessaires pour la preuve de nos principaux théorèmes.

Le deuxième chapitre est consacré à l'étude des classes de Steinitz d'extensions tétraédrales et octaédrales. Dans ce chapitre nous démontrons le théorème 2.

Dans le troisième chapitre nous déterminons effectivement les éléments de l'ensemble des classes réalisables des extensions tétraédrales, puis nous montrons le théorème 1.

# Chapitre 1

# Préliminaires

## 1.1 Groupe des classes d'un ordre maximal

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

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

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

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

L'application $\mathbb{N} \to \mathcal{K}_0(\Lambda)$ qui à $n \in \mathbb{N}$ associe la classe $(\Lambda^n)$ du $\Lambda$-module libre $\Lambda^n$ de rang $n$, se prolonge en un homomorphisme de $\mathbb{Z} \to \mathcal{K}_0(\Lambda)$. On définit $Cl(\Lambda)$ comme étant le conoyau de cette application (voir [F3, Chap. 1, §2]).

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

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

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

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

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

Cette relation est une relation d'équivalence.

Soit $r$ le nombre des classes de conjugaisons sur $k$ des caractères absolument irréductibles de $\Gamma$. Pour tout $i \in \{1, \ldots, r\}$, notons $\chi_i$ un représentant de l'une de ces classes de conjugaison.

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

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

où $D_i$ est un corps gauche, de centre $k(\chi_i)$ l'extension de $k$ obtenu par adjonction à $k$ des valeurs de $\chi_i$, 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 $k$, ainsi $\chi_i(1) = n_i m_i$.

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

Nous rappelons le théorème de Swan suivant (voir [R, Theorem 35.14, p. 313]) :

**Théorème 1.1.2.** *Soit $\mathcal{M}$ un ordre maximal de $O_k$ dans $k[\Gamma]$ contenant $O_k[\Gamma]$. Alors*

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

*où $\mathfrak{Cl}(k(\chi_i))$ est 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 à l'infini de $k(\chi_i)$ ramifiées dans $M_{n_i}(D_i)$.*

De plus si $k[\Gamma]$ vérifie **la condition d'Eichler** suivante : pout toute composante simple $M_{n_i}(D_i)$ il existe une place à l'infini 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 [R, Definition 38.1, p. 343–344]), alors :

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

où $Cl(k(\chi_i))$ est le groupe des classes de $k(\chi_i)$.

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 $\overline{k}^* = \overline{k} - \{0\}$. On peut identifier $\overline{k}^*$ à un sous-groupe de $J(\overline{k})$ par plongement diagonal. On suppose que $k[\Gamma]$ vérifie la condition d'Eichler. Alors la "Hom-description" de Fröhlich de $Cl(\mathcal{M})$ est la suivante (voir [F3] ou [CR, §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 une extension galoisienne de $k$, de degré fini et contenant les valeurs des caractères absolument irréductibles de $\Gamma$.

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

La notion de résolvante de Fröhlich-Lagrange, dont nous rappelons la définition ci-dessous (voir [F3, p. 28–29]), est un outil fondamental pour étudier le problème des classes réalisables.

Soit $N/k$ une extension galoisienne à groupe de Galois isomorphe à $\Gamma$. Si $\pi$ est un isomorphisme défini sur $Gal(N/k)$ et à valeurs dans $\Gamma$, alors tout caractère $\chi$ de $\Gamma$ induit un caractère $\chi \circ \pi$ de $Gal(N/k)$ que l'on notera aussi $\chi$. Si $\gamma \in \Gamma$, nous noterons $\pi^{-1}(\gamma) \in Gal(N/k)$ simplement par $\gamma$. Soit $B$ une $k$-algèbre commutative, en faisant agir $\Gamma$ sur $N$, $N \otimes_k B$ est un $B[\Gamma]$-module libre de rang 1. Soit $T : \Gamma \to GL_n(\overline{k})$ une représentation linéaire de $\Gamma$ de caractère $\chi$.

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

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

*où Det désigne le déterminant.*

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

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

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

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

Lorsque $N/k$ est une extension galoisienne modérément ramifiée, on sait que l'anneau d'entiers $O_N$ de $N$ est un $O_k[\Gamma]$-module localement libre de rang 1 (voir [No] ou [F3, Chap. 1, §3, p. 26–28]).

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

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

## 1.3 Résultats de la théorie du corps de classes

Soient $k$ un corps de nombres, $O_k$ son anneau d'entiers et $Cl(k)$ son groupe des classes.

**Définition 1.3.1.** *Un cycle $\mathfrak{M}$ de $k$ est un produit formel d'un idéal entier $\mathfrak{M}_0$ de $O_k$ et d'une famille $\mathfrak{S}$ de places infinies réelles de $k$, on le note $\mathfrak{M} = \mathfrak{M}_0\mathfrak{S}$.*

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

Soit $I(k)_\mathfrak{M}$ l'ensemble des idéaux fractionnaires de $k$ premiers à $\mathfrak{M}_0$. Soit $P(k)_\mathfrak{M}$ l'ensemble des idéaux fractionnaires principaux de $k$ ayant un générateur congru à 1 mod*$\mathfrak{M}$. Le groupe quotient $Cl(k, \mathfrak{M}) = I(k)_\mathfrak{M}/P(k)_\mathfrak{M}$ est appelé le groupe des classes de rayon modulo $\mathfrak{M}$.

**Théorème 1.3.3.** ***(Théorème de densité de Chebotarev)****(voir [N, Chap. V, §6, Theorem 6.2 et 6.4, p. 132]) Soit $c \in Cl(k, \mathfrak{M})$. 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 $Cl(k, \mathfrak{M})$ est $c$.*

On en déduit facilement :

**Proposition 1.3.4.** *Il existe une surjection canonique de $Cl(k, \mathfrak{M}) \to Cl(k)$.*

**Théorème 1.3.5.** *(voir [W, Theorem 10.1, p. 400]) 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, où $N_{E/k}$ est la norme dans $E/k$.*

## 1.4 Classes de Steinitz et Discriminant

Dans la suite, si $I$ est un idéal fractionnaire d'un corps de nombres $k$, on note $cl(I)$ sa classe dans $Cl(k)$.

Rappelons la définition de la classe de Steinitz. Soit $K/k$ une extension finie de corps de nombres de degré $n$. L'anneau $O_K$ est un $O_k$-module sans torsion de rang $n$, donc il existe un idéal $I$ de $O_k$ tel que $O_K \simeq O_k^{n-1} \oplus I$ en tant que $O_k$-modules. La classe de $I$ dans $Cl(k)$ est appelée la classe de Steinitz de l'anneau $O_K$ ou de l'extension $K/k$, et on la note $cl_k(O_K)$ (voir [FT, Theorem 13, p. 95]). Le théorème suivant est dû à Artin (voir [A], on peut trouver une preuve plus récente de ce résultat dans [M1]), il permet de calculer une telle classe.

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

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

*où $\Delta(K/k)$ est le discriminant de $K/k$ et $d$ le discriminant d'une base du $k$-espace vectoriel $K$.*

*De plus si $K/k$ est galoisienne de degré impair, alors $cl_k(O_K) = cl(\Delta(K/k)^{1/2})$.*

La proposition suivante découle immédiatement de la théorie de Kummer (voir [H, §39]) et du théorème d'Artin ci-dessus.

**Proposition 1.4.2.** *Soient $K/k$ une extension quadratique et $m \in k$ tel que $K = k(\sqrt{m})$.*

*(i) On peut écrire de manière unique $mO_k = I(m)^2 J$, où $I(m)$ est un idéal fractionnaire de $O_k$ et $J$ un idéal entier de $O_k$ sans facteur carré.*

*(ii) On a* $\Delta(K/k) = JJ'^2$ *où* $J'$ *est un idéal entier de* $O_k$ *dont les diviseurs premiers divisent* $2O_k$. *L'extension* $K/k$ *est modérément ramifiée si et seulement si on peut choisir* $m \equiv 1 \ mod^*(4O_k)$, *dans ce cas* $J' = O_k$.

*(iii)* $cl_k(O_K) = cl(I(m)^{-1}J')$.

Soient $K/k$ une extension galoisienne finie de groupe de Galois $G$, $\chi$ un caractère de $G$ et $f(\chi, K/k)$ le conducteur d'Artin de $\chi$. Rappelons la décomposition d'Artin et Hasse du discriminant en un produit de conducteurs (voir [Se2, p. 111–112]) :

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

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

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

**Proposition 1.4.3.** *Soient* $k$, $K$ *et* $M$ *des corps de nombres tels que* $k \subset K \subset M$. *Soient* $[M : K]$ *le degré de l'extension* $M/K$ *et* $N_{K/k}$ *la norme de l'extension* $K/k$. *Alors :*

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

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

L'assertion $(i)$ résulte de la transitivité de la différente (voir par exemple [FT]). L'assertion $(ii)$ est le théorème 4.1 de [F1].

# Chapitre 2

# Classes de Steinitz

## 2.1 Introduction

Soient $\Gamma$ un groupe fini et $\Delta$ un sous-groupe normal de $\Gamma$. On a donc la suite exacte de groupes suivante :

$$\Sigma : 1 \longrightarrow \Delta \longrightarrow \Gamma \longrightarrow \Gamma/\Delta \longrightarrow 1.$$

Soit $k$ un corps de nombres. Fixons $E/k$ une extension galoisienne dont le groupe de Galois est isomorphe à $\Gamma/\Delta$. On désigne par $R(E/k,\Sigma)$ (resp. $R_m(E/k,\Sigma)$) l'ensemble des classes $c \in Cl(k)$ vérifiant : il existe une extension galoisienne (resp. galoisienne et modérément ramifiée) $N/k$ dont la classe de Steinitz est $c$, contenant $E$, et dont le groupe de Galois est isomorphe à $\Gamma$, avec un isomorphisme $\pi$ de $Gal(N/k)$ dans $\Gamma$ satisfaisant $E$ est le sous-corps de $N$ fixe par $\pi^{-1}(\Delta)$.

Lorsque $\Delta = \Gamma$, $R(E/k,\Sigma)$ (resp. $R_m(E/k,\Sigma)$) est tout simplement l'ensemble des classes de Steinitz des extensions galoisiennes (resp. galoisiennes et modérées) de $k$, dont le groupe de Galois est isomorphe à $\Gamma$ ; on note $R(k,\Gamma)$ et $R_m(k,\Gamma)$ au lieu de $R(E/k,\Sigma)$ et $R_m(E/k,\Sigma)$.

## 2.2 Classes de Steinitz d'extensions tétraédrales

On s'intéresse ici à la situation où $\Gamma$ est le groupe alterné $A_4$ défini par la présentation :

$$A_4 = \langle \sigma,\tau,\nu : \sigma^3 = \tau^2 = \nu^2 = 1, \tau\nu = \nu\tau, \sigma\tau\sigma^{-1} = \nu, \sigma\nu\sigma^{-1} = \tau\nu \rangle,$$

et

$$\Delta = \langle \tau, \nu \rangle.$$

Une extension galoisienne de $k$ est appelée tétraédrale si son groupe de Galois est isomorphe à $A_4$.

On a $Gal(E/k) \simeq \langle \sigma \rangle$, donc $E/k$ est une extension cyclique de degré 3.

Dans cette section, nous démontrons les principaux résultats suivants :

**Théorème 2.2.1.** *Soient $k$ un corps de nombres et $E/k$ une extension cyclique de degré 3. Alors :*

*(i)* $$R(E/k, \Sigma) = cl_k(O_E)(N_{E/k}(Cl(E)))^3,$$

*où $N_{E/k}$ est la norme dans $E/k$ et $(N_{E/k}(Cl(E)))^3$ est le sous-groupe des puissances $3^{ième}$ des éléments du groupe $N_{E/k}(Cl(E))$.*

*De plus, si $E/k$ est modérée alors $R_m(E/k, \Sigma) = R(E/k, \Sigma)$.*

*(ii) Soit $j$ une racine primitive troisième de l'unité. Soit $W$ le sous-groupe de $Cl(k)$ engendré par $N_{k(j)/k}(Cl(k(j)))$ et les classes des idéaux premiers de $O_k$ au-dessus de 3, où $N_{k(j)/k}$ désigne la norme dans $k(j)/k$. Alors*

$$R(k, A_4) = WCl(k)^3,$$

$$R_m(k, A_4) = N_{k(j)/k}(Cl(k(j)))Cl(k)^3.$$

**Corollaire 2.2.2.** *Sous les hypothèses et notations du théorème 2.2.1 on a les assertions suivantes :*

*(i) Si le nombre des classes de $k$ est impair alors $R(k, A_4) = R_m(k, A_4) = Cl(k)$.*

*(ii) Si 3 ne divise pas le nombre des classes de $k$ alors $R(E/k, \Sigma) = Cl(k)(= R_m(E/k, \Sigma)$ si $E/k$ est modérée).*

*(iii) Si $O_E$ est un $O_k$-module libre alors $R(E/k, \Sigma)$ est un sous-groupe de $Cl(k)$ égal à $(N_{E/k}(Cl(E)))^3$ $(= R_m(E/k, \Sigma)$ si $E/k$ est modérée); de plus si $E/k$ est ramifiée alors il est égal à $Cl(k)^3$.*

Soit $N/k$ une extension galoisienne dont le groupe de Galois est isomorphe à $A_4$. Si $\pi$ est un isomorphisme de $Gal(N/k)$ dans $A_4$ et $\gamma \in A_4$, on identifiera $\pi^{-1}(\gamma)$ et $\gamma$. Soit $E/k$ la sous-extension de $N$ fixe par $\langle \tau, \nu \rangle$ : c'est l'unique sous-extension cyclique de degré 3, et on a $Gal(E/k) \simeq \langle \sigma \rangle$. L'extension $N/E$ est biquadratique, elle contient donc trois sous-extensions quadratiques de $E$ ; si $L/E$ est l'une d'entre elles alors les deux autres sont $\sigma(L)$ et $\sigma^2(L)$.

**Proposition 2.2.3.** *On a :*

$$cl_k(O_N) = (cl_k(O_E))^4 (N_{E/k}(cl_E(O_L)))^3.$$

Le lemme suivant sera utile pour la preuve de la proposition précédente.

**Lemme 2.2.4.** *Soient $K$ un corps de nombres, $M/K$ une extension biquadratique et $K_i/K$, $1 \leq i \leq 3$, les trois sous-corps quadratiques de $M$. Alors*

$$cl_K(O_M) = cl_K(O_{K_1}) cl_K(O_{K_2}) cl_K(O_{K_3}).$$

*Preuve du lemme.* Notons $\Delta_0$ le discriminant de $M/K$ et $\Delta_i$ les discriminants des $K_i/K$. Une conséquence immédiate de la décomposition d'Artin et Hasse du discriminant en un produit de conducteurs et la propriété de ces derniers relative au passage au quotient (voir Chap. 1, §4) est $\Delta_0 = \Delta_1 \Delta_2 \Delta_3$. Soient $m_i$, $1 \leq i \leq 2$, des éléments de $K$ tels que $K_i = K(\sqrt{m_i})$. Posons $m_3 = m_1 m_2$, il est clair que $K_3 = K(\sqrt{m_3})$. Les familles $(1, \sqrt{m_1}), (1, \sqrt{m_2}), (1, \sqrt{m_3}), (1, \sqrt{m_1}, \sqrt{m_2}, \sqrt{m_3})$ sont des bases respectives des $K$-espaces vectoriels $K_i$ et $M$, dont les discriminants respectifs $d_i$ et $d$ sont : $4m_i$ et $(16m_3)^2$. On en déduit que

$$\Delta_0/d = (\Delta_1/d_1)(\Delta_2/d_2)(\Delta_3/d_3)2^{-2}.$$

On a alors le lemme car d'après le théorème d'Artin (voir Théorème 1.4.1), $cl_K(O_M) = cl(\sqrt{\Delta_0/d})$ et $cl_K(O_{K_i}) = cl(\sqrt{\Delta_i/d_i})$. □

*Preuve de la proposition 2.2.3.* Par la transitivité de la classe de Steinitz dans une tour de corps de nombres (voir Proposition 1.4.3, $(ii)$) on a :

$$cl_k(O_N) = (cl_k(O_E))^4 N_{E/k}(cl_E(O_N)).$$

Soient $\sigma^i(L)/E$, $0 \leq i \leq 2$, les trois sous-corps quadratiques de $N/E$. Le lemme 2.2.1 nous affirme que :

$$cl_E(O_N) = cl_E(O_L)cl_E(O_{\sigma(L)})cl_E(O_{\sigma^2(L)}).$$

Ecrivons $L = E(\sqrt{m})$. Comme $\sigma^i(L) = E(\sqrt{\sigma^i(m)})$, et $\sigma^i(\Delta(L/E)) = \Delta(\sigma^i(L)/E)$, on a (par Artin) :

$$cl_E(O_{\sigma^i(L)}) = \sigma^i(cl_E(O_L)).$$

D'où

$$N_{E/k}(cl_E(O_N)) = (N_{E/k}(cl_E(O_L)))^3.$$

Ce qui termine la preuve de la proposition. □

Pour la démonstration du théorème 2.2.1, nous avons besoin du lemme suivant qui est un critère de plongement d'une extension cubique cyclique dans une extension à groupe de Galois $A_4$ . Ce lemme est bien connu, il est cité dans [K, p. 21] de la thèse mais sans démonstration complète (on peut voir aussi [M2, p. 365]).

**Lemme 2.2.5.** *Soient $k$ un corps de nombres, $K/k$ une extension cyclique de degré 3, $L = K(\sqrt{a})/K$ une extension quadratique de $K$. Alors les deux assertions suivantes sont équivalentes :*

*(i) La clôture galoisienne de $L/k$ est une extension $N/k$ à groupe de Galois isomorphe à $A_4$.*

*(ii) $N_{K/k}(a)$ est un carré dans $k$, où $N_{K/k}$ est la norme dans $K/k$.*
*De plus si (ii) est vérifiée, on peut choisir $N = K(\sqrt{a}, \sqrt{\sigma(a)})$.*

*Démonstration.* L'implication $(i) \Rightarrow (ii)$ résulte de la théorie de Kummer. On a $\sigma(L) = K(\sqrt{\sigma(a)})$. Le troisième sous-corps quadratique de $N/K$ est $\sigma^2(L) = K(\sqrt{\sigma^2(a)})$ qui est aussi égal à $K(\sqrt{a\sigma(a)})$. D'après la théorie de Kummer, il existe $b \in K$ tel que $a\sigma(a) = b^2\sigma^2(a)$. D'où $N_{K/k}(a) = (b\sigma^2(a))^2$ ; $b\sigma^2(a) \in k$ sinon $K/k$ contiendrait une sous-extension quadratique, ce qui est impossible.

Montrons maintenant que $(ii) \Rightarrow (i)$. Notons par $\sigma$ un générateur de $Gal(K/k)$. Puisque $a$ n'est pas un carré dans $K$, il en est de même pour $\sigma(a)$. Soient $N$ l'extension biquadratique $K(\sqrt{a}, \sqrt{\sigma(a)})/K$, $\sigma_1$ et $\sigma_2$ les générateurs de $Gal(N/K)$

définis par : $\sigma_1(\sqrt{a}) = -\sqrt{a}$ et $\sigma_1(\sqrt{\sigma(a)}) = \sqrt{\sigma(a)}$, $\sigma_2(\sqrt{\sigma(a)}) = -\sqrt{\sigma(a)}$ et $\sigma_2(\sqrt{a}) = \sqrt{a}$. Notons $\overline{\sigma}$ un prolongement de $\sigma$ à $N$. On a $(\sqrt{a})^2 = a$, d'où $(\overline{\sigma}(\sqrt{a}))^2 = \overline{\sigma}(a) = \sigma(a)$ ; par suite $\overline{\sigma}(\sqrt{a}) = \pm\sqrt{\sigma(a)}$. De $(\sqrt{\sigma(a)})^2 = \sigma(a)$ on déduit que $(\overline{\sigma}(\sqrt{\sigma(a)}))^2 = \sigma^2(a)$. Soit $x \in k$ tel que $N_{K/k}(a) = x^2$, alors $\sigma^2(a) = (x/\sqrt{a} \cdot \sqrt{\sigma(a)})^2$, i.e. $\sigma^2(a)$ admet une racine carrée dans $N$, d'où $\overline{\sigma}(\sqrt{\sigma(a)}) = \pm\sqrt{\sigma^2(a)}$. Donc $\overline{\sigma}(N) \subset N$, par suite $N/k$ est galoisienne de degré 12.

On vérifie facilement que $Gal(N/k) = \langle \overline{\sigma}, \sigma_1, \sigma_2 \rangle$, où, par exemple, $\overline{\sigma}$ est défini par $\overline{\sigma}(\sqrt{a}) = \sqrt{\sigma(a)}$ et $\overline{\sigma}(\sqrt{\sigma(a)} = \sqrt{\sigma^2(a)}$, et que $Gal(N/k) \simeq A_4$. □

*Preuve du théorème 2.2.1.* (*i*) Nous commençons par montrer l'égalité

$$cl_k(O_E)(N_{E/k}(Cl(E)))^3 = (cl_k(O_E))^4(N_{E/k}(Cl(E)))^3. \tag{2.1}$$

Pour cela il suffit de montrer que $cl_k(O_E) \in N_{E/k}(Cl(E))$. Soit $\Delta(E/k)$ (resp. $\mathfrak{D}(E/k)$) le discriminant (resp. la différente) de $E/k$. Comme $E/k$ est normale de degré impair, il découle du théorème d'Artin (voir Théorème 1.4.1) que

$$cl_k(O_E) = cl((\Delta(E/k))^{1/2}).$$

La différente de $E/k$ étant un carré (on le voit facilement par la formule de Hilbert, voir [Se2, Chap. IV, Prop. 4, p. 72]), on en déduit que

$$cl_k(O_E) = N_{E/k}(cl(\mathfrak{D}(E/k)^{1/2})).$$

L'inclusion :

$$R(E/k, \Sigma) \subset cl_k(O_E)(N_{E/k}(Cl(E)))^3, \tag{2.2}$$

est donc une conséquence de (2.1) et de la proposition 2.2.3. Montrons maintenant qu'on a :

$$(cl_k(O_E))^4(N_{E/k}(Cl(E)))^3 \subset R(E/k, \Sigma). \tag{2.3}$$

Soient $c \in N_{E/k}(Cl(E))$ et $d \in Cl(E)$ telle que $N_{E/k}(d) = c$.

Considérons la classe $\sigma^2(d)^{-1}$. D'après le théorème de densité de Tchebotarev (voir Théorème 1.3.3), il existe un idéal premier $\beta$ de $O_E$, premier à $2O_E$, vérifiant $\beta \cap O_k$ totalement décomposé dans $E/k$ et tel que $\sigma^2(d)^{-1} = cl(\beta)$.

Considérons maintenant $cl(\beta\sigma(\beta))^{-1}$. Notons $Cl(E, 4O_E)$ le groupe des classes de rayon modulo $4O_E$. Par la surjection canonique de $Cl(E, 4O_E)$ sur $Cl(E)$ (voir Proposition 1.3.4) et le théorème de Tchebotarev, il existe un idéal premier $\beta'$ de $O_E$, premier à $2O_E$, satisfaisant $\beta' \cap O_k$ totalement décomposé dans $E/k$ et tel que $cl(\beta\sigma(\beta))^{-1} = cl(\beta')$ dans $Cl(E, 4O_E)$ . Par conséquent, il existe $m \in E^\times$ tel que

$$mO_E = \beta\sigma(\beta)\beta', \text{ et } m \equiv 1 \ mod^* \ 4O_E$$

où $mod^*$ est la notation usuelle de la théorie du corps de classes (voir Définition 1.3.2). On a :

$$m\sigma(m)O_E = (\sigma(\beta))^2\beta\sigma^2(\beta)\beta'\sigma(\beta').$$

Il est clair que $m\sigma(m)$ n'est pas un carré dans $E$ ($v_{\beta'}(m\sigma(m)) \equiv 1 \ mod \ 2$). On considère l'extension quadratique $L = E(\sqrt{m\sigma(m)})/E$. On a $N_{E/k}(m\sigma(m)) = (N_{E/k}(m))^2$. D'après le lemme 2.1.2, la clôture galoisienne de $L/k$ est une extension $N/k$ à groupe de Galois isomorphe à $A_4$, et on peut prendre $N = E(\sqrt{m\sigma(m)}, \sqrt{\sigma(m\sigma(m))})/k$. De $m \equiv 1 \ mod^* \ 4O_E$ on déduit $\sigma(m) \equiv 1 \ mod^* \ 4O_E$, par suite $m\sigma(m) \equiv 1 \ mod^* \ 4O_E$. Par la proposition 1.4.2, $L/E$ est modérée et $cl_E(O_L) = cl(\sigma(\beta))^{-1}$ ; comme $\sigma^2(d)^{-1} = cl(\beta)$, on en déduit immédiatement

$$cl_E(O_L) = d.$$

La proposition 2.2.3 nous donne :

$$cl_k(O_N) = (cl_k(O_E))^4(N_{E/k}(d))^3.$$

Par suite

$$cl_k(O_N) = (cl_k(O_E))^4c^3.$$

On conclut qu'on a (2.3). On a donc la première partie de ($i$) du théorème 2.2.1 grâce à (2.1), (2.2) et (2.3).

Il est clair que $E(\sqrt{m\sigma(m)})/E$ et $E(\sqrt{\sigma(m\sigma(m))})/E$ sont modérées (voir Proposition 1.4.2, ($ii$)). Il s'en suit que $N/E$ est modérée. Si $E/k$ est modérée alors $N/k$ l'est aussi et donc

$$(cl_k(O_E))^4(N_{E/k}(Cl(E)))^3 \subset R_m(E/k, \Sigma).$$

D'où $R(E/k, \Sigma) = R_m(E/k, \Sigma)$. Ce qui termine la preuve de ($i$) du théorème 2.2.1.

$(ii)$ Soient $C_3$ un groupe cyclique d'ordre 3, $j$ une racine primitive $3^{\text{ième}}$ de l'unité. Alors $R(k, C_3)$ (voir [L, Theorem 4.7, p. 97]) est le sous-groupe de $Cl(k)$ égal à $W$.

D'après (i), l'inclusion $R(k, A_4) \subset WCl(k)^3$ est évidente.

Montrons l'autre inclusion. Soit $c \in WCl(k)^3$, alors il existe $(c_1, c_2) \in W \times Cl(k)$ tel que $c = c_1 c_2^3$. Comme $c_1 \in W$, il existe une extension $E/k$ cyclique de degré 3 telle que $c_1 = cl_k(O_E)$. De plus on peut supposer (d'après [L]) que $E/k$ est ramifiée au moins en une place. Par suite $N_{E/k} : Cl(E) \to Cl(k)$ est surjective (voir Théorème 1.3.5) et $N_{E/k}(Cl(E)) = Cl(k)$, d'où $c_1 c_2^3 \in cl_k(O_E)(N_{E/k}(Cl(E)))^3$ et donc $c \in R(k, A_4)$ d'après (i). Par conséquent $WCl(k)^3 \subset R(k, A_4)$.

L'égalité $R_m(k, A_4) = N_{k(j)/k}(Cl(k(j))Cl(k)^3$ provient du fait qu'on a (voir [L, Theorem 2.6, p. 90]) : $R_m(k, C_3) = N_{k(j)/k}(Cl(k(j))$. □

**Remarque.** A l'origine, dans l'énoncé du théorème 2.2.1, on supposait le nombre des classes de $k$ impair. C'est grâce à une idée de C. Greither que nous avons pu enlever cette hypothèse. Nous donnons ci-dessous les principales idées de l'ancienne démonstration de $(i)$ (sous cette hypothèse).

Soit $c \in N_{E/k}(Cl(E))$. L'ensemble $N_{E/k}(Cl(E))$ étant un sous-groupe de $Cl(k)$, son ordre est impair. Par suite il existe $c' \in N_{E/k}(Cl(E))$ telle que $c = c'^2$. Soit $d \in Cl(E)$ telle que $c' = N_{E/k}(d)$. D'après le théorème de Tchebotarev, il existe un idéal $I$ de $O_E$ premier à $2O_E$ tel que $d^{-1} = cl(I)$. D'après la surjection canonique de $Cl(E, 4O_E)$ sur $Cl(E)$ et le théorème de Tchebotarev, il existe un idéal premier $\beta$ de $O_E$ satisfaisant $\beta \cap O_k$ totalement décomposé dans $E/k$ tel que $cl(I)^{-2} = cl(\beta)$ dans $Cl(E, 4O_E)$. Par conséquent, il existe $m \in E^\times$ tel que :

$$mO_E = I^2\beta, \quad m \equiv 1 \ mod^* \ 4O_E, \quad \text{et} \quad cl(I^{-1}) = d.$$

La suite de la démonstration est analogue à celle du théorème 2.2.1. $(i)$. On considére de nouveau l'élément $m\sigma(m)$, l'extension quadratique $L = E(\sqrt{m\sigma(m)})/E$ et l'extension tétraédrale $N = E(\sqrt{m\sigma(m)}, \sqrt{\sigma(m\sigma(m))})/k$. On obtient $cl_E(O_L) = d\sigma(d)$ et $cl_k(O_N) = cl_k(O_E)^4 c^3$.

*Preuve du corollaire 2.2.2.* $(i)$ Si le nombre des classes de $k$ est impair on a $N_{k(j)/k}(Cl(k(j)) = Cl(k)$ grâce au théorème 1.3.5, en effet : si $j$ n'appartient pas à $k$, $k(j)/k$ est de degré 2, donc elle est ramifiée au moins en une place de

$k$ (car elle ne peut être contenue dans le corps de classes de Hilbert de $k$). Par suite $R(k, C_3) = R_m(k, C_3) = Cl(k)$.
$(ii)$ Si 3 ne divise pas le nombre des classes de $k$ alors $(N_{E/k}(Cl(E)))^3 = N_{E/k}(Cl(E))$. D'autre part $E/k$ est nécessairement ramifiée au moins en une place de $k$ et comme $E$ est la seule sous-extension abélienne non triviale de $E/k$, $N_{E/k} : Cl(E) \longrightarrow Cl(k)$ est surjective (voir Théorème 1.3.5), et donc $N_{E/k}(Cl(E)) = Cl(k)$. D'où $R(E/k, \Sigma) = cl_k(O_E)Cl(k) = Cl(k)$.
$(iii)$ Par définition de la classe de Steinitz, on a $O_E$ est un $O_k$-module libre si et seulement si $Cl_k(O_E) = 1$. Si $E/k$ est ramifiée, comme ci-dessus on a $N_{E/k}(Cl(E)) = Cl(k)$. Donc on a $(iii)$.

□

## 2.3 Classes de Steinitz d'extensions octaédrales

On s'intéresse maintenant à la situation où $\Gamma$ est le groupe symétrique $S_4$ défini par la présentation :

$$S_4 = \langle \sigma, \tau, \nu, \mu : \sigma^3 = \tau^2 = \nu^2 = \mu^2 = 1, \tau\nu = \nu\tau, \sigma\tau\sigma^{-1} = \nu, \sigma\nu\sigma^{-1} = \tau\nu, \mu\tau\mu = \nu, \mu\sigma\mu = \sigma^{-1} \rangle,$$

et

$$\Delta = \langle \tau, \nu \rangle.$$

Le groupe $S_4$ est un produit semi-direct de $\Delta$ et $\langle \sigma, \mu \rangle$, où $\Delta \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\langle \sigma, \mu \rangle \simeq D_3$ (ou $S_3$), $D_3$ étant le groupe diédral d'ordre 6. Une extension galoisienne de $k$ est appelée octaédrale si son groupe de Galois est isomorphe à $S_4$.

On a $Gal(E/k) \simeq \langle \sigma, \mu \rangle$, par suite $E/k$ est une extension diédrale de degré 6.

Dans cette section nous montrons le résultat principal suivant :

**Théorème 2.3.1.** *Soient $k$ un corps de nombres et $E/k$ une extension diédrale de degré 6. Supposons le nombre des classes de $k$ impair. Alors*

*(i)* $$R(E/k,\Sigma) = cl_k(O_E)(Cl(k))^3,$$

*où* $Cl(k)^3$ *est le sous-groupe des puissances 3-ième des éléments de* $Cl(k)$.
*De plus si* $E/k$ *est modérée alors* $R_m(E/k,\Sigma) = R(E/k,\Sigma)$.

*(ii)* $$R(k,S_4) = R_m(k,S_4) = Cl(k).$$

**Remarques.** 1) L'hypothèse "le nombre des classes de $k$ impair" provient d'un problème de plongement.
2) Soit $k = \mathbb{Q}(\sqrt{d})/\mathbb{Q}$ une extension quadratique. D'après [CH], le nombre des classes de $k$ est impair si et seulement si $d = -1, \pm 2, p, -p, 2p$ ou $qr$, où p est un nombre premier, q et r sont des nombres premiers congrus à 3 modulo 4.

Si le nombre des classes de $k$ n'est pas divisible par 3 alors $Cl(k)^3 = Cl(k)$. D'après la définition de la classe de Steinitz, $O_E$ est un $O_k$-module libre si et seulement si $Cl_k(O_E) = 1$. On a immédiatement le résultat suivant :

**Corollaire 2.3.2.** *Sous les hypothèses et notations du théorème 2.3.1 on a les assertions suivantes :*

*(i) Si 3 ne divise pas le nombre des classes de* $k$ *alors* $R(E/k,\Sigma) = Cl(k) (= R_m(E/k,\Sigma)$ *si* $E/k$ *est modérée).*

*(ii) Si* $O_E$ *est un* $O_k$*-module libre alors* $R(E/k,\Sigma)$ *est un sous-groupe de* $Cl(k)$ *égal à* $Cl(k)^3$ $(= R_m(E/k,\Sigma)$ *si* $E/k$ *est modérée).*

Soit $N/k$ une extension octaédrale. Si $\pi$ est un isomorphisme de $Gal(N/k)$ dans $S_4$ et $\gamma \in S_4$, on identifiera $\pi^{-1}(\gamma)$ et $\gamma$. Soit $E$ le sous-corps de $N$ fixe par $\Delta$. Alors $E/k$ est une extension diédrale de degré 6. Soit $k'/k$ la sous-extension quadratique de $E/k$. Alors l'extension $N/k'$ est galoisienne à groupe de Galois isomorphe à $A_4$. L'extension $N/E$ est biquadratique, elle contient donc trois sous-extensions quadratiques de $E$ ; si $L/E$ est l'une d'entre elles alors les deux autres sont $\sigma(L)$ et $\sigma^2(L)$.

**Proposition 2.3.3.** *Sous les notations précédentes, on a :*

$$cl_k(O_N) = (cl_k(O_E))^4(N_{E/k}(cl_E(O_L)))^3.$$

*Démonstration.* Elle est analogue à la preuve de la proposition 2.2.3 car $Gal(N/k') \simeq A_4$. En vertu de la transitivité de la classe de Steinitz dans une tour de corps de nombres (voir Proposition 1.4.3, $(ii)$), on a :

$$cl_k(O_N) = (cl_k(O_E))^4 N_{E/k}(cl_E(O_N)).$$

On sait d'après le lemme 2.2.4 que la classe de Steinitz d'une extension biquadratique est le produit des classes de Steinitz de ses trois sous-extensions quadratiques. Ainsi :

$$cl_E(O_N) = cl_E(O_L)cl_E(O_{\sigma(L)})cl_E(O_{\sigma^2(L)}).$$

Comme dans la preuve de la proposition 2.2.3, si $L = E(\sqrt{m})$ alors, puisque $\sigma^i(L) = E(\sqrt{\sigma^i(m)})$ et $\sigma^i(\Delta(L/E)) = \Delta(\sigma^i(L)/E)$, on a par le théorème d'Artin (voir Théorème 1.4.1) :

$$cl_E(O_{\sigma^i(L)}) = \sigma^i(cl_E(O_L)).$$

D'où,

$$N_{E/k}(cl_E(O_N)) = (N_{E/k}(cl_E(O_L)))^3.$$

Ce qui achève la démonstration. □

Pour prouver le théorème 2.3.1, nous avons besoin du lemme suivant qui est un critère de plongement. Son origine est un énoncé dans [M2, p. 365, application pour n=4, (ii)] sans preuve. Une partie de ce lemme est le théorème I.2 de [J].

**Lemme 2.3.4.** *Soit $k$ un corps de nombres. Soient $E/k$ une extension diédrale de degré 6 de groupe de Galois $\langle \sigma, \mu \rangle$ et $K/k$ sa sous-extension (cubique non galoisienne) fixe par $\mu$. Soit $a \in K$ un élément qui n'est pas un carré dans $E$, et soit $M$ l'extension quadratique de $K(\sqrt{a})/K$. Alors les assertions suivantes sont équivalentes :*

*(i) $E/k$ est plongeable dans une extension octaédrale $N/k$ contenant $M$ et telle que $N/E$ soit biquadratique.*

*(ii)* $N_{K/k}(a)$ *est un carré dans* $k$, *où* $N_{K/k}$ *désigne la norme dans* $K/k$. *Lorsque ce plongement est possible, on peut choisir* $N = E(\sqrt{a}, \sqrt{\sigma(a)})$.

*Démonstration.* L'implication $(i) \Rightarrow (ii)$ est le théorème I.2 de [J].

Prouvons maintenant l'implication $(ii) \Rightarrow (i)$. Puisque $a$ n'est pas un carré dans $E$, $\sigma(a)$ non plus. Soient $N/E$ l'extension biquadratique $N = E(\sqrt{a}, \sqrt{\sigma(a)})/E$, $\sigma_1$ et $\sigma_2$ des générateurs de $Gal(N/E)$. Notons par $\overline{\sigma}$ (resp. $\overline{\mu}$) un $k$-plongement de $N$ qui prolonge $\sigma$ (resp. $\mu$). Il est immédiat que $\overline{\sigma}(\sqrt{a}) = \pm\sqrt{\sigma(a)}$. Comme $N_{K/k}(a) = a\sigma(a)\sigma^2(a)$ est un carré dans $k$, on en déduit que $\sigma^2(a)$ a une racine carré dans $N$. D'où $\overline{\sigma}(\sqrt{\sigma(a)}) = \pm\sqrt{\sigma^2(a)}$ et $\overline{\sigma}(N) \subset N$. De $(\sqrt{a})^2 = a$ on tire $(\overline{\mu}(\sqrt{a}))^2 = \mu(a) = a$, et donc $\overline{\mu}(\sqrt{a}) = \pm\sqrt{a}$. De même, on a $(\overline{\mu}(\sqrt{\sigma(a)}))^2 = \mu\sigma(a) = \sigma^2\mu(a) = \sigma^2(a)$, par conséquent $\overline{\mu}(\sqrt{\sigma(a)}) = \pm\sqrt{\sigma^2(a)}$ et $\overline{\mu}(N) \subset N$. On conclut que $N/k$ est une extension galoisienne de degré 24 et que $Gal(N/k) = \langle \sigma_1, \sigma_2, \overline{\sigma}, \overline{\mu} \rangle$. Choisissons par exemple $\sigma_1, \sigma_2, \overline{\sigma}, \overline{\mu}$ definis par :

$$\sigma_1(\sqrt{a}) = -\sqrt{a}, \quad \sigma_1(\sqrt{\sigma(a)}) = \sqrt{\sigma(a)}, \quad \sigma_1(\sqrt{\sigma^2(a)}) = -\sqrt{\sigma^2(a)},$$

$$\sigma_2(\sqrt{a}) = -\sqrt{a}, \quad \sigma_2(\sqrt{\sigma(a)}) = -\sqrt{\sigma(a)}, \quad \sigma_2(\sqrt{\sigma^2(a)}) = \sqrt{\sigma^2(a)},$$

$$\overline{\sigma}(\sqrt{a}) = \sqrt{\sigma(a)}, \quad \overline{\sigma}(\sqrt{\sigma(a)}) = \sqrt{\sigma^2(a)}, \quad \overline{\sigma}(\sqrt{\sigma^2(a)}) = \sqrt{a},$$

$$\overline{\mu}(\sqrt{a}) = \sqrt{a}, \quad \overline{\mu}(\sqrt{\sigma(a)}) = \sqrt{\sigma^2(a)}, \quad \overline{\mu}(\sqrt{\sigma^2(a)}) = \sqrt{\sigma(a)}.$$

Il est facile de voir que $Gal(N/k) \simeq S_4$. Ce qui termine la preuve du lemme. □

*Preuve du théorème 2.3.1.* $(i)$ Nous commençons par prouver les égalités suivantes :

$$R(E/k, \Sigma) = (cl_k(O_E))^4 (N_{E/k}(Cl(E)))^3, \tag{2.4}$$

$$R_m(E/k, \Sigma) = R(E/k, \Sigma) \text{ si } E/k \text{ est ramifiée.} \tag{2.5}$$

L'inclusion (pour tout corps de nombres $k$) :

$$R(E/k, \Sigma) \subset (cl_k(O_E))^4 (N_{E/k}(Cl(E)))^3, \tag{2.6}$$

est une conséquence immédiate de la proposition 2.3.3. Montrons maintenant l'inclusion :

$$(cl_k(O_E))^4(N_{E/k}(Cl(E)))^3 \subset R(E/k,\Sigma). \tag{2.7}$$

Supposons que l'ordre du groupe des classes de $k$ est impair. Soit $c \in N_{E/k}(Cl(E))$, puisque $N_{E/k}(Cl(E))$ est un sous-groupe de $Cl(k)$, il est aussi d'ordre impair. Il existe donc $c' \in N_{E/k}(Cl(E))$ tel que $c = c'^4$. Soit $d \in Cl(E)$ tel que $c' = N_{E/k}(d)$.

D'après la surjection canonique de $Cl(E, 4O_E)$ sur $Cl(E)$ (voir Proposition 1.3.4) et le théorème de densité de Tchebotarev (voir Théorème 1.3.3) : il existe $m \in E^\times$, un idéal fractionnaire $I$ de $O_E$ et un idéal premier $\beta$ de $O_E$ satisfaisant $\beta \cap O_k$ totalement décomposé dans $E/k$ tels que :

$$mO_E = I^2\beta, \quad m \equiv 1 \ mod^* \ 4O_E, \quad \text{et} \quad Cl(I^{-1}) = d.$$

On a alors :

$$m\sigma(m)\mu(m\sigma(m))O_E = (I\sigma(I)\mu(I)\mu\sigma(I))^2\beta\sigma(\beta)\mu(\beta)\mu\sigma(\beta).$$

Posons $a = m\sigma(m)\mu(m\sigma(m))$. Il est clair que $a$ n'est pas un carré dans $E$ ($v_\beta(a) \equiv 1 \ mod \ 2$). Soit $K/k$ la sous-extension cubique non galoisienne de $E/k$ fixe par $\mu$. Puisque $Gal(E/K) = \langle\mu\rangle$, $a = N_{E/K}(m\sigma(m)) \in K$. Soit $M$ l'extension quadratique $K(\sqrt{a})/K$. On a $N_{K/k}(a) = (N_{E/k}(m))^2$. Par le lemme 2.3.4, $E/k$ est plongeable dans l'extension octaédrale $N = E(\sqrt{a}, \sqrt{\sigma(a)})/k$.

Soit $L$ l'extension quadratique $E(\sqrt{a})/E$. On déduit de $m \equiv 1 \ mod^* \ 4O_E$ que $\gamma(m) \equiv 1 \ mod^* \ 4O_E$, pour $\gamma = \sigma$, $\mu$ ou $\mu\sigma$, par suite $a \equiv 1 \ mod^* \ 4O_E$. Par la proposition 1.4.2,

$$\Delta(L/E) = \beta\sigma(\beta)\mu(\beta)\mu\sigma(\beta),$$

et

$$cl_E(O_L) = cl(I\sigma(I)\mu(I)\mu\sigma(I))^{-1},$$

d'où

$$cl_E(O_L) = d\sigma(d)\mu(d)\mu\sigma(d).$$

La proposition 2.3.3 nous donne :

$$cl_k(O_N) = (cl_k(O_E))^4(N_{E/k}(d\sigma(d)\mu(d)\mu\sigma(d)))^3.$$

Par suite

$$cl_k(O_N) = (cl_k(O_E))^4(c'^4)^3 = (cl_k(O_E))^4c^3.$$

On conclut qu'on a l'égalité (2.7). L'égalité (2.4) découle alors de (2.6) et (2.7).

Clairement $E(\sqrt{a})/E$ et $E(\sqrt{\sigma(a)})/E$ sont modérées, il s'en suit que $N/E$ est modérée. Si $E/k$ est modérée alors $N/k$ l'est aussi, donc

$$(cl_k(O_E))^4(N_{E/k}(Cl(E)))^3 \subset R_m(E/k,\Sigma).$$

D'où $R(E/k,\Sigma) = R_m(E/k,\Sigma)$, ce qui termine la preuve de (2.5).

Maintenant nous terminons la preuve de $(i)$. Soit $k'/k$ la sous-extension quadratique de $E/k$. Parce que l'ordre du groupe des classes de $k$ est impair, $k'/k$ est ramifiée. Puisque $k'/k$ est l'unique sous-extension abélienne non triviale de $E/k$, l'application $N_{E/k} : Cl(E) \longrightarrow Cl(k)$ est surjective (voir Théorème 1.3.5). D'où $N_{E/k}(Cl(E)) = Cl(k)$. En utilisant (2.4) on obtient :

$$R(E/k,\Sigma) = (cl_k(O_E))^4(Cl(k))^3 = cl_k(O_E)(Cl(k))^3.$$

Ce qui achève la preuve de $(i)$.

$(ii)$ Soit $D_3$ le groupe diédral d'ordre 6. Pour tout corps de nombres $k$ (voir [E, Chap. III, §3, 3.1, p. 59]) :

$$R_m(k, D_3) = Cl(k).$$

Soit $c \in Cl(k)$, il existe donc une extension diédrale $E/k$ de degré 6 modérée, et telle que $c = cl_k(O_E)$. D'autre part, par l'assertion $(i)$ du théorème 2.3.1 $c \in R_m(E/k,\Sigma)$ ; ainsi $Cl(k) \subset R_m(k, S_4)$, d'où $R_m(k, S_4) = Cl(k)$. Maintenant l'égalité $R(k, S_4) = R_m(k, S_4)$ est claire. □

# Chapitre 3

# Classes réalisables d'extensions tétraédrales

## 3.1 Introduction

Soient $k$ un corps de nombres et $O_k$ son anneau d'entiers. Soient $\Gamma$ un groupe fini, $N/k$ une extension galoisienne à groupe de Galois isomorphe à $\Gamma$, et $O_N$ l'anneau d'entiers de $N$. Soit $\mathcal{M}$ un ordre maximal de $O_k$ dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$. 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 $Cl(\mathcal{M})$ le groupe des classes de $\mathcal{M}$. On désigne par $\mathcal{R}(\mathcal{M})$ l'ensemble des classes $c$ de $Cl(\mathcal{M})$ telle qu'il existe une extension $N/k$ modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$, avec $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$; on dira que $c$ est réalisable par l'extension $N/k$ et $\mathcal{R}(\mathcal{M})$ est l'ensemble des classes réalisables. Il est bien connu que $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$, où $Cl^\circ(\mathcal{M})$ est le noyau du morphisme $Cl(\mathcal{M}) \to Cl(k)$ induit par l'augmentation $\mathcal{M} \to O_k$.

Dans ce chapitre, le principal résultat est le théorème suivant :

**Théorème 3.1.1.** *Soit $\Gamma$ le groupe alterné $A_4$. Soient $j$ une racine primitive $3^{ième}$ de l'unité et $k$ un corps de nombres linéairement disjoint de $\mathbb{Q}(j)$ sur $\mathbb{Q}$. Alors $\mathcal{R}(\mathcal{M})$ est le groupe $Cl^\circ(\mathcal{M})$. Dans ce cas, $\mathcal{R}(\mathcal{M}) \simeq Cl(k(j)) \times Cl(k)$.*

## 3.2 Description d'un représentant de la classe de $\mathcal{M} \otimes_{O_k[A_4]} O_N$ dans $Cl(\mathcal{M})$

Rappelons que le groupe $A_4$ peut être défini par la présentation suivante :

$$A_4 = \langle \sigma, \tau, \nu : \sigma^3 = \tau^2 = \nu^2 = 1, \tau\nu = \nu\tau, \sigma\tau\sigma^{-1} = \nu, \sigma\nu\sigma^{-1} = \tau\nu \rangle.$$

Dorénavant, on pose :

$$\Delta = \langle \tau, \nu \rangle \text{ et } C_3 = \langle \sigma \rangle.$$

Le groupe $\Delta$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $C_3$ est cyclique d'ordre 3. Le groupe $A_4$ est le produit semi-direct de $C_3$ par le sous-groupe distingué $\Delta$.

Le groupe $A_4$ a quatre caractères absolument irréductibles qui sont définis de la manière suivante (voir [Se1, §5.7, p. 57]) :

| | 1 | $\tau$ | $\sigma$ | $\sigma^2$ |
|---|---|---|---|---|
| $\chi_0$ | 1 | 1 | 1 | 1 |
| $\chi_1$ | 1 | 1 | $j$ | $j^2$ |
| $\chi_1'$ | 1 | 1 | $j^2$ | $j$ |
| $\chi_2$ | 3 | -1 | 0 | 0 |

Dans toute la suite du chapitre, on suppose que $k$ est linéairement disjoint de $\mathbb{Q}(j)$ sur $\mathbb{Q}$. Alors $A_4$ possède trois classes de conjugaison de caractères absolument irréductibles dont les représentants sont les suivants :

a) $\chi_0$ le caractère trivial de $\Gamma$.

b) $\chi_1$ un caractère non trivial, de degré 1, dont le noyau est $\Delta$.

c) $\chi_2$ un caractère de degré 3, qui est induit par un caractère non trivial $\varphi$ de $\Delta$, de degré 1, i.e. $\chi_2 = Ind_\Delta^\Gamma \varphi$.

La décomposition de Wedderburn de $k[A_4]$ en un produit d'algèbres simples est (voir Chap. 1, §1) :

$$k[A_4] = \prod_{i=0}^{2} M_{n_i}(D_i),$$

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 $D_i$. On rappelle que la dimension de $D_i$ sur $k(\chi_i)$ est un carré $m_i^2$, où l'entier $m_i$ est l'indice de Schur relatif à $k$. Ainsi $\chi_i(1) = n_i m_i$.

Il est clair que $m_i = 1$ pour $i$ =0, 1. Aussi, $m_2 = 1$ car $\chi_2$ est à valeurs dans $k$ (i.e. réalisable sur $k$). On en déduit immédiatement que :

$$k[A_4] \simeq k \times k(j) \times M_3(k).$$

Puisque la dimension de chaque composante simple de $k[A_4]$ sur son centre est différente de 4, $k[A_4]$ vérifie la condition d'Eichler (voir Chap. 1, §1). Par conséquent (voir Théorème 1.1.2) :

$$Cl(\mathcal{M}) \simeq Cl(k) \times Cl(k(j)) \times Cl(k),$$

D'où

$$Cl^{\circ}(\mathcal{M}) \simeq Cl(k(j)) \times Cl(k).$$

A partir de maintenant $N/k$ désigne une extension tétraédrale modérément ramifiée. Nous notons par $E$ le sous-corps de $N$ fixe par $\Delta$. Ainsi l'extension $E/k$ est cyclique de degré 3 et l'extension $N/E$ est biquadratique.

Dans ce qui suit, on va déterminer un élément $f$ de $Hom_{\Omega_k}(R_{A_4}, J(\overline{k}))$ (voir Théorème 1.2.2) qui représente $\mathcal{M} \otimes_{O_k[A_4]} O_N$ dans $Cl(\mathcal{M})$ en donnant les valeurs qu'il prend en $\chi_0$, $\chi_1$ et $\chi_2$.

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 $O_{N,\mathfrak{p}}$.

Il est clair que $\langle \alpha_{\mathfrak{p}}, \chi_0 \rangle = Tr_{N_{\mathfrak{p}}/k_{\mathfrak{p}}}(\alpha_{\mathfrak{p}})$ et $\langle a, \chi_0 \rangle = Tr_{N/k}(a)$, où $Tr$ désigne la trace. On peut supposer que $Tr_{N/k}(a) = 1$ (sinon prendre $a(Tr_{N/k}(a))^{-1}$). Comme $\alpha_{\mathfrak{p}}$ est une base normale locale d'entiers, $Tr_{N_{\mathfrak{p}}/k_{\mathfrak{p}}}(\alpha_{\mathfrak{p}})$ est une unité de $O_{k,\mathfrak{p}}$. Donc on peut choisir $\alpha_{\mathfrak{p}}$ de sorte que $Tr_{N_{\mathfrak{p}}/k_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}) = 1$.

On pose alors :

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

La restriction de $\chi_1$ à $C_3$ définit un caractère non trivial de $C_3$ (car $ker(\chi_1) = \Delta$) qu'on note $\underline{\chi_1}$. Les égalités suivantes découlent facilement de la définition 1.2.1 des résolvantes de Fröhlich-Lagrange (on peut voir aussi [F2, Theorem 10, p. 162]) :

$$\langle \alpha_{\mathfrak{p}}, \chi_1 \rangle = \langle Tr_{N_{\mathfrak{p}}/E_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}), \underline{\chi_1} \rangle_{E/k}, \tag{3.1}$$

$$\langle a, \chi_1 \rangle = \langle Tr_{N/E}(a), \underline{\chi_1} \rangle_{E/k}. \tag{3.2}$$

Signalons que $Tr_{N_{\mathfrak{p}}/E_{\mathfrak{p}}}(\alpha_{\mathfrak{p}})$ et $Tr_{N/E}(a)$ sont des bases respectives du $O_{k,\mathfrak{p}}[C_3]$-module $O_{E,\mathfrak{p}}$ et du $k[C_3]$-module $E$.

On pose :

$$f(\chi_1) = \left( \frac{\langle Tr_{N_{\mathfrak{p}}/E_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}), \underline{\chi_1} \rangle_{E/k}}{\langle Tr_{N/E}(a), \underline{\chi_1} \rangle_{E/k}} \right).$$

Soient $b$ et $b_{\mathfrak{p}}$ des bases respectives du $E[\Delta]$-module $N$ et du $O_{E,\mathfrak{p}}[\Delta]$-module $O_{N,\mathfrak{p}}$. Puisque $\chi_2 = Ind_{\Delta}^{\Gamma}\varphi$, par un résultat de Fröhlich (voir [F2, Theorem 12, p. 165]) il existe $\lambda$ et $\lambda_{\mathfrak{p}}$ des éléments inversibles respectifs des anneaux $k[\Delta]$ et $O_{k,\mathfrak{p}}[\Delta]$ tels que :

$$\langle a, \chi_2 \rangle \varphi(\lambda) = \mathfrak{N}_{E/k}(\langle b, \varphi \rangle_{N/E}) e(E/k), \tag{3.3}$$

et

$$\langle \alpha_{\mathfrak{p}}, \chi_2 \rangle \varphi(\lambda_{\mathfrak{p}}) = \mathfrak{N}_{E/k}(\langle b_{\mathfrak{p}}, \varphi \rangle_{N/E}) e(E_{\mathfrak{p}}/k_{\mathfrak{p}}); \tag{3.4}$$

où $\varphi$ a été prolongée par linéarité à $k_{\mathfrak{p}}[\Delta]$, $e(E/k)^2$ est le discriminant d'une base du $k$-espace vectoriel $E$, $e(E_{\mathfrak{p}}/k_{\mathfrak{p}})^2 O_{k,\mathfrak{p}}$ est le discriminant de $E_{\mathfrak{p}}/k_{\mathfrak{p}}$, et

$$\mathfrak{N}_{E/k}(\langle x, \varphi \rangle_{N/E}) = \prod_{\gamma \in Gal(E/k)} \gamma(\langle x, \gamma^{-1}\varphi \rangle_{N/E}).$$

Dans notre situation :

$$\mathfrak{N}_{E/k}(\langle x,\varphi\rangle_{N/E}) = \prod_{\gamma\in Gal(E/k)} \gamma(\langle x,\varphi\rangle_{E/k})$$

car $\varphi$ est à valeurs dans $\{1,-1\}$. Ainsi $\mathfrak{N}_{E/k} = N_{E/k}$. Les égalités (3.3) et (3.4) impliquent :

$$\frac{\langle \alpha_{\mathfrak{p}},\chi_2\rangle}{\langle a,\chi_2\rangle} = \varphi(\lambda_{\mathfrak{p}})^{-1}\varphi(\lambda)\frac{e(E_{\mathfrak{p}}/k_{\mathfrak{p}})}{e(E/k)}N_{E/k}\left(\frac{\langle b_{\mathfrak{p}},\varphi\rangle_{N/E}}{\langle b,\varphi\rangle_{N/E}}\right).$$

D'une part, l'application définie sur $R_{A_4}$ et à valeurs dans $\overline{k}^*$ qui a $\chi_0$ et $\chi_1$ associe 1, et qui a $\chi_2$ associe $\varphi(\lambda)$, est un élément de $Hom_{\Omega_k}(R_{A_4},\overline{k}^*)$. D'autre part, l'application définie sur $R_{A_4}$ et à valeurs dans $U(\overline{k})$ qui a $\chi_0$ et $\chi_1$ associe 1, et qui a $\chi_2$ associe $\varphi(\lambda_{\mathfrak{p}})^{-1}$, est un élément de $Hom_{\Omega_k}(R_{A_4},U(\overline{k}))$.

On pose :

$$f(\chi_2) = \left(\frac{e(E_{\mathfrak{p}}/k_{\mathfrak{p}})}{e(E/k)}N_{E/k}\left(\frac{\langle b_{\mathfrak{p}},\varphi\rangle_{N/E}}{\langle b,\varphi\rangle_{N/E}}\right)\right).$$

En résumé on a donc la proposition suivante :

**Proposition 3.2.1.** *Sous les hypothèses et notations définies ci-dessus, un représentant de la classe de $\mathcal{M}\otimes_{O_k[A_4]}O_N$ dans $Cl(\mathcal{M})$ est l'élément $f$ de $Hom_{\Omega_k}(R_{A_4},J(\overline{k}))$ défini par :*

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

$$f(\chi_1) = \left(\frac{\langle Tr_{N_{\mathfrak{p}}/E_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}),\underline{\chi_1}\rangle_{E/k}}{\langle Tr_{N/E}(a),\underline{\chi_1}\rangle_{E/k}}\right),$$

$$f(\chi_2) = \left(\frac{e(E_{\mathfrak{p}}/k_{\mathfrak{p}})}{e(E/k)}N_{E/k}\left(\frac{\langle b_{\mathfrak{p}},\varphi\rangle_{N/E}}{\langle b,\varphi\rangle_{N/E}}\right)\right).$$

On va maintenant déterminer effectivement les composantes $c_i$, $0\leq i\leq 2$, de $[\mathcal{M}\otimes_{O_k[A_4]}O_N]$ dans $Cl(k)\times Cl(k(j))\times Cl(k)$, grâce à la proposition ci-dessus et à [Sol].

Notons $S_3 = \{s_1, s_2\}$ le groupe de Galois de $k(j)/k$, où $s_1(j) = j$ et $s_2(j) = j^2$. Soit $\theta_3$ l'élément de Stickelberger $\theta_3 = s_1 + 2s_2$. On peut écrire de manière unique (voir [So1, Théorème 2.2, (1)]) :

$$\langle Tr_{N/E}(a), \underline{\chi_1}\rangle_{E/k}^3 O_{k(j)} = I(\underline{\chi_1})^3 \theta_3 J(\underline{\chi_1}),$$

où $I(\underline{\chi_1})$ est un idéal fractionnaire de $O_{k(j)}$ et $J(\underline{\chi_1})$ un idéal entier de $O_{k(j)}$ sans facteur carré, tel que $J(\underline{\chi_1})$ et $s_2(J(\underline{\chi_1}))$ soient premier entre eux.

**Proposition 3.2.2.** *Sous les notations précédentes, on a :*

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

*(ii)* $c_1$ *est la classe de* $(I(\underline{\chi_1}))^{-1}$ *dans* $Cl(k(j))$.

*(iii)* $c_2 = cl_k(O_E)N_{E/k}(cl_E(O_L))$ *dans* $Cl(k)$, *où* $L/E$ *est une sous-extension quadratique de* $N/E$.

*Démonstration.* *(i)* Il est évident que la classe de $\mathcal{M} \otimes_{O_k[A_4]} O_N$ dans $Cl(\mathcal{M})$ est représentée par la classe triviale dans $Cl(k)$.

*(ii)* Les extensions $N/E$ et $E/k$ sont modérées car $N/k$ est modérée.

Soit $\mathcal{M}_1$ l'ordre maximal de $O_k$ dans $k[C_3]$. Puisque $k[C_3]$ vérifie la condition d'Eichler (voir Chap. 1, §1) et $k$ est linéairement disjoint de $\mathbb{Q}(j)$, on a immédiatement

$$Cl(\mathcal{M}_1) \simeq Cl(k) \times Cl(k(j)).$$

Il est clair que de l'élément $f_1$ de $Hom_{\Omega_k}(R_{C_3}, J(\overline{k}))$, qui au caractère trivial de $C_3$ associe 1 et à $\underline{\chi_1}$ associe $f_1(\underline{\chi_1}) = f(\chi_1)$, est un représentant de $[\mathcal{M}_1 \otimes_{O_k[C_3]} O_E]$ dans la Hom-description de $Cl(\mathcal{M}_1)$. D'aprés [So1, Théorème 2.3] (Attention : dans [So1] $\mathcal{R}(\mathcal{M}_1)$ est noté $\mathcal{R}(O_k[C_3])$), la composante de $[\mathcal{M}_1 \otimes_{O_k[C_3]} O_E]$ dans $Cl(k(j))$ est égale à la classe de $I(\underline{\chi_1})^{-1}$. On déduit de $f_1(\underline{\chi_1}) = f(\chi_1)$ que la composante de $[\mathcal{M}_1 \otimes_{O_k[C_3]} O_E]$ dans $Cl(k(j))$ est égale à la composante de $[\mathcal{M} \otimes_{O_k[A_4]} O_N]$ dans $Cl(k(j))$. D'où *(ii)*.

*(iii)* Soit $\mathcal{M}_2$ l'ordre maximal de $O_E$ dans $E[\Delta]$. On vérifie facilement que

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

Posons $\Omega_E = Gal(\overline{k}/E)$. Soit $f_2$ l'élément de $Hom_{\Omega_E}(R_\Delta, J(\overline{k}))$ qui au caractère trivial de $\Delta$ fait correspondre 1, et pour tout caractère absolument irréductible

non trivial $\chi$ de $\Delta$ fait correspondre $f_2(\chi)$ défini par : pour tout idéal premier $\mathfrak{p}$ de $O_k$, $f_2(\chi)_\mathfrak{p} = \dfrac{\langle b_\mathfrak{p}, \chi\rangle_{N/E}}{\langle b, \chi\rangle_{N/E}}$. Alors $f_2$ est un représentant de $[\mathcal{M}_2 \otimes_{O_E[\Delta]} O_N]$ dans la Hom-description de $Cl(\mathcal{M}_2)$.

Soit $L/E$ la sous-extension quadratique de $N/E$ fixe par $Ker\varphi$. Le caractère $\varphi$ définit par restriction un caractère $\underline{\varphi}$ de $Gal(L/E)$. Il est facile de vérifier (comme dans (3.1) et (3.2)) :

$$\frac{\langle b_\mathfrak{p}, \varphi\rangle_{N/E}}{\langle b, \varphi\rangle_{N/E}} = \frac{\langle Tr_{N_\mathfrak{p}/L_\mathfrak{p}}(b_\mathfrak{p}), \underline{\varphi}\rangle_{L/E}}{\langle Tr_{N/L}(b), \underline{\varphi}\rangle_{L/E}}.$$

Il est montré dans [So3, Preuve du théorème 1.3, p. 52–53], que la classe du contenu de l'idèle dont les composantes sont écrites dans le membre de droite de l'égalité précédente est $cl_E(O_L)$.

Soit $I$ l'idéal de $O_k$ qui est le contenu de l'idèle $\left(\dfrac{e(E_\mathfrak{p}/k_\mathfrak{p})}{e(E/k)}\right)$. Puisque $(e(E_\mathfrak{p}/k_\mathfrak{p}))^2 O_{k,\mathfrak{p}}$ est égal au discriminant local $\Delta(E_\mathfrak{p}/k_\mathfrak{p})$, on a

$$I^2 = \frac{\Delta(E/k)}{e(E/k)^2},$$

où $\Delta(E/k)$ est le discriminant de $E/k$. Comme $d = e(E/k)^2$ est le discriminant d'une base de $E/k$, on a $cl_k(O_E) = cl(\sqrt{\Delta/d})$ par le théorème d'Artin (voir Théorème 1.4.1). On en déduit que $cl_k(O_E) = cl(I)$. Donc la classe du contenu de l'idèle $f(\chi_2)$ dans $Cl(k)$ est égal à $cl_k(O_E)N_{E/k}(cl_E(O_L))$. Ce qui termine la preuve de $(iii)$. □

## 3.3 Démonstration du théorème 3.1.1

La proposition 3.2.2 nous permet d'identifier $\mathcal{R}(\mathcal{M})$ avec un sous-ensemble de $Cl(k(j)) \times Cl(k)$. Dans la suite nous montrerons l'inclusion :

$$Cl(k(j)) \times Cl(k) \subset \mathcal{R}(\mathcal{M}).$$

Soit $(x, y) \in Cl(k(j)) \times Cl(k)$.

On considère tout d'abord $x$. Soit $\mathcal{S}_3$ l'idéal de Stickelberger défini par

$$\mathcal{S}_3 = 3^{-1}\theta_3\mathbb{Z}[S_3] \cap \mathbb{Z}[S_3].$$

On a que $3^{-1}\theta_3(2s_2 - s_1) = s_1$, d'où $\mathcal{S}_3 = \mathbb{Z}[S_3]$. Il s'en suit de [So1, Théorème 2.4, p. 194] (Attention : $\mathcal{R}(\mathcal{M})$ est noté $\mathcal{R}(O_k[\Gamma])$), qu'on peut identifier $\mathcal{R}(\mathcal{M}_1)$

à $Cl(k(j))$ (où $\mathcal{M}_1$ est l'ordre maximal de $O_k$ dans $k[C_3]$). Donc il existe une extension galoisienne $E/k$, à groupe de Galois isomorphe à $C_3$, modérément ramifiée et telle que la composante de $[\mathcal{M}_1 \otimes_{O_k[C_3]} O_E]$ dans $Cl(k(j))$ est égale à $x$. De plus on peut supposer que $E/k$ est ramifiée au moins en une place (voir [So1, Preuve du théorème 2.4, p. 195], dans cette preuve remplacer $l$ par 3 et $N$ par $E$).

On considère maintenant $y$. Soit $c \in Cl(k)$ tel que $y = cl_k(O_E)c$. Puisque $E/k$ est ramifiée, $N_{E/k} : Cl(E) \to Cl(k)$ est surjective (voir Théorème 1.3.5). Par suite, il existe $d \in Cl(E)$ tel que $N_{E/k}(d) = c$. Comme dans la preuve de l'inclusion (2.3) (voir Chap. 2, preuve du théorème 2.2.1), il existe une extension quadratique $L/E$ satisfaisant : la clôture galoisienne de $L/k$ est une extension tétraédrale modérée $N/k$, et $cl_E(O_L) = d$. On a :

$$N_{E/k}(cl_E(O_L)) = N_{E/k}(d) = c.$$

D'où

$$y = cl_k(O_E)N_{E/k}(cl_E(O_L)).$$

En vertu de la Proposition 3.2.2, on conclut que les composantes de $[\mathcal{M} \otimes_{O_k[A_4]} O_N]$ dans $Cl(k(j)) \times Cl(k)$ sont $x$ et $y$. Ce qui achève la preuve du théorème 3.1.1.

# Bibliographie


[A] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, Colloq. Internat. CNRS 24, Paris (1950), 19–20.

[C1] J.E. Carter, *Steinitz classes of a nonabelian extension of degree $p^3$*, Colloq. Math. 71 (1996), 297–303.

[C2] J.E. Carter, *Steinitz classes of nonabelian extensions of degree $p^3$*, Acta Arith. 78 (1997), 297–303.

[C3] J.E. Carter, *Module structure of integers in metacyclic extensions*, Colloq. Math. 76 (1998), 191–199.

[CH] P.E. Conner, J. Hurrelbrink, *Class Number Parity*, Series in Pures Math. 8, Singapore, 1988.

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

[E] L.P. Endo, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, Thesis, University of Illinois at Urbana-Champaign (1975).

[F1] A. Fröhlich, *The discriminant of relative extensions and the existence of integral bases*, Mathematika 7 (1960), 15–22.

[F2] A. Fröhlich *Galois Module Structure*, in "Algebraic Number Fields, Proceedings of the Durham Symposium,1975", 133–191, Academic Press, London, 1977.

[F3] A. Fröhlich *Galois Module Structure of Algebraic Integers*, Springer-Verlag, Berlin, 1983.

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

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

[J] A. Jehanne, *Sur les extensions de $\mathbb{Q}$ à groupe de Galois $S_4$ ou $\tilde{S}_4$*, Acta. Arith. LXIX.3 (1995), 259–276.

[K] S.-H. Kwon, *Extensions à groupes de Galois $A_4$*, Thèse, Université Bordeaux I, 1984.
*Corps de nombres de degré 4 de type alterné*, C.R.Acad.Sci. 299 (2) (1984), 41–43.

[L] R. Long, *Steinitz classes of cyclic extensions of prime degree*, J. Reine Angew. Math. 250 (1971), 87–98.

[M1] J. Martinet, *Sur l'arithmétique d'une extension galoisienne à groupe de Galois diédral d'ordre 2p*, An. Inst. Fourier (1969), 1–80.

[M2] J. Martinet, *Discriminants and permutation groups*, Number Theory, Walter de Gruyter (Richard A. Molin, ed.), Berlin - New York (1990), 359–385.

[Mc1] 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", 561–588, Academic Press, London, 1977.

[Mc2] L.R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. 375/376 (1987), 259–306.

[N] J. Neukirch, *Class Field Theory*, Springer-Verlag, Berlin, 1986.

[No] E. Noether, *Normalbasis bei Körpen ohne höhere Verzweigung*, J. Reine Angew. Math. 167 (1931), 147–152.

[R] I. Reiner, *Maximal Orders*, Academic Press, 1975.

[Se1] J.-P. Serre, *Représentations linéaires des groupes finis*, 3ème édition, Hermann, Paris, 1978.

[Se2] J.-P. Serre, *Corps Locaux*, 3ème édition, Hermann, Paris, 1980.

[Se3] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Vol. 1, Boston, 1992.

[So1] B. Sodaïgui *Structure galoisiennes relative des anneaux d'entiers*, J. Number Theory 28, no.2 (1988), 189–204.

[So2] B. Sodaïgui, *Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger*, J. Number Theory 65 (1997), 87–95.

[So3] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement*, Illinois J. Math. 43, no.1 (1999), 47–60.

[So4] B. Sodaïgui, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, J. Algebra 223 (1999), 367–378.

[So5] B. Sodaïgui, *"Galois module structure" des extensions quaternioniennes de degre 8*, J. Algebra 213 (1999), 549–556.

[So6] B. Sodaïgui, *Realizables Classes of quaternion extensions of degree 4l*, J. Number Theory 80 (2000), 304–315.

[T] M.J. Taylor, *On Fröhlich's conjecture for rings of tame extensions*, Invent. Math. 63 (1981), 41–79.

[W] L.C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Springer-Verlag, Berlin, 1996.

# Structure galoisienne d'anneaux d'entiers

Soient $k$ un corps de nombres et $O_k$ son anneau d'entiers. Soient $\Gamma$ un groupe fini, $N/k$ une extension galoisienne à groupe de Galois isomorphe à $\Gamma$ et $O_N$ l'anneau d'entiers de $N$. Soit $\mathcal{M}$ un ordre maximal de $O_k$ dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$. Lorsque $N/k$ est modérément ramifiée, on peut associer à $O_N$ par extension des scalaires, une classe notée $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $Cl(\mathcal{M})$, le groupe des classes de $\mathcal{M}$. On désigne par $\mathcal{R}(\mathcal{M})$ l'ensemble des classes réalisables, c'est-à-dire l'ensemble des classes $c \in Cl(\mathcal{M})$ telle qu'il existe une extension $N/k$ modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$, avec $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$. Il est bien connu que $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$, où $Cl^\circ(\mathcal{M})$ est le noyau du morphisme $Cl(\mathcal{M}) \to Cl(k)$ induit par l'augmentation $\mathcal{M} \to O_k$. Les résultats de McCulloh vont dans le sens de la conjecture suivante :
**Conjecture :** $\mathcal{R}(\mathcal{M})$ est un sous-groupe de $Cl^\circ(\mathcal{M})$.
Lorsque $\Gamma$ est abélien et $k$ un corps de nombres quelconque, les travaux de McCulloh entraînent que cette conjecture est vraie. Dans cette thèse, nous vérifions la conjecture dans le cas où $\Gamma$ est le groupe alterné $A_4$ et $k$ est linéairement disjoint du troisième corps cyclotomique de $\mathbb{Q}$. Par ailleurs, lorsque nous essayons d'étudier cette conjecture, nous sommes confrontés au problème de plongement en liaison avec les classes de Steinitz. Une autre partie de cette thèse est l'étude des classes de Steinitz d'extensions à groupe de Galois isomorphe à $A_4$ ou au groupe symétrique $S_4$.

**Mots clés :** Structure galoisienne, Hom-description de Fröhlich, Résolvante de Fröhlich-Lagrange, Ordre maximal, Classes réalisables, Classes de Steinitz.

# Galois module structure of rings of integers

Let $k$ be a number field and $O_k$ its ring of integers. Let $\Gamma$ be a finite group, $N/k$ a Galois extension with Galois group isomorphic to $\Gamma$ and $O_N$ the ring of integers of $N$. Let $\mathcal{M}$ be a maximal $O_k$-order in $k[\Gamma]$ containing $O_k[\Gamma]$. When $N/k$ is at most tamely ramified, we can associate to $O_N$ by extension of scalars, a class denote by $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ in $Cl(\mathcal{M})$, the classgroup of $\mathcal{M}$. We denote by $\mathcal{R}(\mathcal{M})$ the set of realizable classes, that is the set of $c \in Cl(\mathcal{M})$ such that there exists a Galois extension $N/k$ at most tamely ramified, with Galois group isomorphic to $\Gamma$, for which $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$. It is well known that $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$, where $Cl^\circ(\mathcal{M})$ is the kernel of the morphism $Cl(\mathcal{M}) \to Cl(k)$ induced by the augmentation $\mathcal{M} \to O_k$. The results of McCulloh lead to the following conjecture :
**Conjecture :** $\mathcal{R}(\mathcal{M})$ is a subgroup of $Cl^\circ(\mathcal{M})$.
If $\Gamma$ is abelian and $k$ is any number field, it follows from McCulloh that this conjecture is true. In this thesis, we verify the conjecture when $\Gamma$ is the alternating group $A_4$ and $k$ and the third cyclotomic field of $\mathbb{Q}$ are linearly disjoint. When we attempt to study this conjecture, we are faced with the embedding problem connected with the Steinitz classes. The second part of this thesis is the study of Steinitz classes of extensions with Galois group isomorphic to $A_4$ or to the symetric group $S_4$.

**Key words :** Galois module structure, Fröhlich's Hom-description, Fröhlich-Lagrange resolvent, Maximal order, Realizable classe, Steinitz classes.

MATHEMATIQUES PURES

Laboratoire de Mathématiques, LAMATH, Université de Valenciennes et du Hainaut Cambrésis, Le Mont Houy, 59313 Valenciennes Cedex 9