Classes réalisables d'extensions non abéliennes

Nigel P. Byott,
School of Mathematical Sciences, University of Exeter,
Exeter EX4 4QE, UK
E-mail : N.P.Byott@ex.ac.uk

Cornelius Greither,
Institut für Theoretische Informatik und Mathematik,
Fakultät für Informatik, Universität der Bundeswehr München,
85577 Neubiberg, F. R. Germany
E-mail : greither@informatik.unibw-muenchen.de

Bouchaïb Sodaïgui,
Département de Mathématiques, Université de Valenciennes,
Le Mont Houy, 59313 Valenciennes Cedex 9, France
E-mail : bouchaib.sodaigui@univ-valenciennes.fr
2000 Mathematics Subject Classification : 11R33

Résumé

Soient k un corps de nombres et O_k son anneau d'entiers. Soient Γ un groupe fini, N/k une extension galoisienne à groupe de Galois isomorphe à Γ et O_N l'anneau des entiers de N. Soient $\mathcal{M}$ un ordre maximal de O_k dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$, et $Cl(\mathcal{M})$ son groupe des classes (i.e., le groupe des classes des $\mathcal{M}$-modules localement libres). Lorsque N/k est modérément ramifiée, l'extension des scalaires permet d'associer à O_N 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 définit l'ensemble $\mathcal{R}(\mathcal{M})$ des classes réalisables comme étant l'ensemble des classes $c \in Cl(\mathcal{M})$ telles qu'il existe une extension N/k modérément ramifiée, à groupe de Galois isomorphe à Γ, avec $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$. Dans cet article, on montre, par l'intermédiaire d'une description assez explicite, que $\mathcal{R}(\mathcal{M})$ est un sous-groupe de $Cl(\mathcal{M})$ lorsque $\Gamma = V \rtimes_\rho C$, où V est un $\mathbb{F}_2$-espace vectoriel de dimension $r \geq 2$, C un groupe cyclique d'ordre $2^r - 1$, et ρ une représentation linéaire fidèle de C dans V ; un exemple est le groupe alterné A_4. La démonstration utilise des propriétés du code binaire de Hamming, et nécessite la résolution d'un problème de plongement en liason avec les classes de Steinitz. En outre, on détermine l'ensemble des classes de Steinitz des extensions galoisiennes modérées de k, ayant un tel groupe comme groupe de Galois, et on montre que c'est un sous-groupe du groupe des classes de k.

Abstract

Let k be a number field and O_k its ring of integers. Let Γ be a finite group, N/k a Galois extension with Galois group isomorphic to Γ, and O_N the ring of integers of N. 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. When N/k is tame (i.e., at most tamely ramified), extension of scalars allows us to assign to O_N the class of $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$, denoted $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$, in $Cl(\mathcal{M})$. We define the set $\mathcal{R}(\mathcal{M})$ of realizable classes to be the set of classes $c \in Cl(\mathcal{M})$ such that there exists a Galois extension N/k which is tame, with Galois group isomorphic to Γ, and for which $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$. In the present article, we prove, by means of a fairly explicit description, that $\mathcal{R}(\mathcal{M})$ is a subgroup of $Cl(\mathcal{M})$ when $\Gamma = V \rtimes_\rho C$, where V is an $\mathbb{F}_2$-vector space of dimension $r \geq 2$, C a cyclic group of order $2^r - 1$, and ρ a faithful representation of C in V ; an example is the alternating group A_4. In the proof, we use some properties of the binary Hamming code and solve an embedding problem connected with Steinitz classes. In addition, we determine the set of Steinitz classes of tame Galois extensions of k, with the above group as Galois group, and prove that it is a subgroup of the classgroup of k.

1 Introduction et énoncé des principaux résultats

Dans tout cet article, si K est un corps de nombres, O_K désigne son anneau d'entiers et $Cl(K)$ son groupe des classes.

Soient k un corps de nombres, $\overline{k}$ une clôture algébrique de k et $Gal(\overline{k}/k)$ son groupe de Galois. Soit Γ un groupe fini. A tout homomorphisme surjectif π défini sur $Gal(\overline{k}/k)$ et à valeurs dans Γ, 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 π, défini sur $Gal(N/k)$ et à valeurs dans Γ. A l'aide de π 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 $O_k[\Gamma]$ (i.e., le groupe des classes des $O_k[\Gamma]$-modules localement libres ; voir [F4], Chap. 1, §2, p. 17), 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 $\mathcal{M}$ (i.e., le groupe des classes des $\mathcal{M}$-modules localement libres).

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. $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$) ; 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 facile de voir que $\mathcal{R}(O_k[\Gamma]) \subset Cl^\circ(O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$) (voir le début de la preuve de (4.4) de [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. *L'ensemble $\mathcal{R}(O_k[\Gamma])$ est un sous-groupe de $Cl^\circ(O_k[\Gamma])$.*

Les tentatives de prouver cette conjecture se heurtent aux difficultés qui proviennent des unités locales des algèbres de groupes (voir la preuve d'une conjecture de Fröhlich dans [T] ; voir [BS1], [BS2]). Pour contourner ces problèmes on étudie la conjecture plus faible suivante :

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

La conjecture 1 entraîne la conjecture 2. En effet : l'extension des scalaires de $O_k[\Gamma]$ à $\mathcal{M}$ induit un morphisme surjectif $Ex : Cl(O_k[\Gamma]) \to Cl(\mathcal{M})$ et il est clair que $Ex(\mathcal{R}(O_k[\Gamma])) = \mathcal{R}(\mathcal{M})$.

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 fois, le caractère profond de ces questions, dans l'esprit des travaux de A. Fröhlich et M. J. Taylor (voir surtout [F4] et [T]).

Le cas où $k = \mathbb{Q}$ et Γ réalisable comme groupe de Galois d'une extension galoisienne modérée sur $\mathbb{Q}$ est assez bien compris grâce aux résultats de [T] et [F2]. Si Γ ne possède pas de caractère irréductible symplectique (c'est le cas par exemple de Γ abélien ou d'ordre impair), alors $\mathcal{R}(\mathbb{Z}[\Gamma])$ est le sous-groupe trivial de $Cl(\mathbb{Z}[\Gamma])$ (voir [T]), et la conjecture 1 est donc verifée. Quant à $\mathcal{R}(\mathcal{M})$, il est toujours trivial (voir [F4] corollaire du théorème 6, pp. 40–41, ou [F2], corollaire du théorème 11, p. 412).

Si k est un corps de nombres quelconque et Γ 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 Γ 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 sur $\mathbb{Q}$. On montre que la conjecture 2 est vraie en décrivant $\mathcal{R}(\mathcal{M})$ par deux idéaux de Stickelberger.

Lorsque Γ est le groupe diédral D_4 (resp. quaternionien) d'ordre 8 et k est un corps de nombres linéairement disjoint de $\mathbb{Q}(i)$ sur $\mathbb{Q}$, où $i^2 = -1$, on montre dans [So5] (resp. [So4]) 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 Γ est le groupe quaternionien 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 [GS2] on montre la conjecture 2 pour le groupe alterné A_4 sous les hypothèses : le nombre des classes de k est impair et $k/\mathbb{Q}$ est linéairement disjoint du $3^{\text{ième}}$ corps cyclotomique sur $\mathbb{Q}$.

Dans [BS1] on établit l'égalité $\mathcal{R}(O_k[A_4]) = Cl^\circ(O_k[A_4])$ pour tout corps de nombres k. Dans [BS2] on montre que $\mathcal{R}(O_k[D_4]) = Cl^\circ(O_k[D_4])$ sous l' hypothèse que l'ordre du groupe des classes de rayon de k modulo $4O_k$ est impair.

Une partie de cet article consiste en l'étude de la conjecture 2 pour Γ un certain produit semi-direct qu'on va maintenant définir.

Soit $\mathbb{F}_2$ le corps à deux éléments, qu'on identifiera souvent à $\mathbb{Z}/2\mathbb{Z}$. Soient V un $\mathbb{F}_2$-espace vectoriel de dimension $r \geq 2$, et C un groupe cyclique d'ordre $2^r - 1$. Soit

$$\rho : C \to Aut_{\mathbb{F}_2}(V)$$

une représentation linéaire de C dans V. On note $\Gamma = V \rtimes_\rho C$ le produit semi-direct défini par ρ.

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

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

où $n+1$ est le nombre des classes de conjugaison sur k des caractères absolument irréductibles de C (i.e., caractères de représentations irréductibles complexes), 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 par adjonction à k des valeurs de χ_i.

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

$$Cl(\mathcal{M}(C)) \simeq \prod_{i=0}^{n} Cl(k(\chi_i)),$$

et donc

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

Soit $\mathcal{R}(\mathcal{M}(C))$ 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 C. D'après [Mc2], $\mathcal{R}(\mathcal{M}(C))$ est un sous-groupe de $Cl^\circ(\mathcal{M}(C))$ qu'on peut décrire par une correspondance de Stickelberger ; on l'identifiera souvent avec un sous-groupe de $\prod_{i=1}^{n} Cl(k(\chi_i))$.

Maintenant, supposons ρ fidèle. Nous verrons au §4, après avoir déterminé les classes de conjugaison sur k des caractères absolument irréductibles de

Γ, que la décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante :

$$k[\Gamma] \simeq \prod_{i=0}^{n} k(\chi_i) \times M_{2^r-1}(k),$$

où $M_{2^r-1}(k)$ est l'anneau des matrices carrées d'ordre $2^r - 1$ à coefficients dans k.

Soit $\mathcal{M}$ un O_k-ordre maximal de $k[\Gamma]$ contenant $O_k[\Gamma]$. D'après un théorème de Swan (voir [Sw] ou [R], Theorem 35.14, p. 313)

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

et donc

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

Nous identifierons souvent $Cl^\circ(\mathcal{M})$ avec $\prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(k)$ sous l'isomorphisme de (1.1).

Fixons les notations suivantes pour toute la suite de l'article. Si K/k est une extension de corps de nombres, $N_{K/k}$ désigne la norme dans K/k. Si G est un groupe abélien et m un entier positif, G^m dénote le sous-groupe des puissances $m^{\text{ièmes}}$ des éléments de G.

Dans la section 4, on démontre le théorème suivant :

Théorème 1.1. *Soient k un corps de nombres quelconque et $\Gamma = V \rtimes_\rho C$. On suppose la représentation ρ fidèle. Identifions $Cl^\circ(\mathcal{M})$ avec $\prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(k)$. Alors $\mathcal{R}(\mathcal{M})$ est un sous-groupe de $Cl^\circ(\mathcal{M})$, égal au sous-groupe A suivant :*

$$A = \{(c_1, c_2, ..., c_n, x \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i))| \\ (c_1, c_2, ..., c_n) \in \mathcal{R}(\mathcal{M}(C)), x \in Cl(k)^{2^{r-2}}\}.$$

Remarque. Une conséquence immédiate de ce théorème est : $\mathcal{R}(\mathcal{M})$ est isomorphe au groupe produit $\mathcal{R}(\mathcal{M}(C)) \times Cl(k)^{2^{r-2}}$.

Nous verrons au §2 que le groupe alterné A_4 est un exemple de groupe Γ qui vérifie les hypothèses du théorème 1.1 (voir la remarque 2 qui suit la proposition 2. 3, dans ce cas $r = 2$).

Corollaire 1.2. *Avec les notations du théorème 1.1, soit k un corps de nombres quelconque et $\Gamma = A_4$. Alors $\mathcal{R}(\mathcal{M})$ est le sous-groupe $Cl^\circ(\mathcal{M})$. Dans ce cas, soit j une racine primitive $3^{ième}$ de l'unité, alors : $\mathcal{R}(\mathcal{M}) \simeq Cl(k) \times Cl(k) \times Cl(k)$ si $j \in k$, et $\mathcal{R}(\mathcal{M}) \simeq Cl(k(j)) \times Cl(k)$ sinon.*

Ce corollaire généralise, sans aucune hypothèse sur le corps de base k, le principal résultat suivant de [GS2] (voir [GS2], Theorem 1.1) : lorsque $\Gamma = A_4$, si $j \notin k$ et le nombre des classes de k est impair, alors $\mathcal{R}(\mathcal{M}) \simeq Cl(k(j)) \times Cl(k)$.

Ci-dessous, nous donnerons un autre exemple (relativement) explicite du théorème 1.1.

Supposons que $2^r - 1 = \ell$ est un nombre premier de Mersenne (on peut trouver une liste de ces nombres dans le Number Theory Web ; par exemple $r = 2, 3, 5, 7$ ou $r = 24036583$ –le dernier trouvé en Mai 2004– conviennent). Soit ξ_ℓ une racine primitive $\ell^{\text{ième}}$ de l'unité. Supposons k linéairement disjoint de $\mathbb{Q}(\xi_\ell)$ sur $\mathbb{Q}$. Soit $S = Gal(k(\xi_\ell)/k) = \{s_i \mid 1 \leq i \leq \ell-1\}$, avec $s_i(\xi_\ell) = \xi_\ell^i$. L'action naturelle de S sur les idéaux fractionnaires de $k(\xi_\ell)$ induit une structure de $\mathbb{Z}[S]$-module sur $Cl(k(\xi_\ell))$. Soient l'élément de Stickelberger $\theta = \sum_{i=1}^{\ell-1} i s_i^{-1}$ et l'idéal de Stickelberger $\mathcal{S}_\ell = (1/\ell)\theta\mathbb{Z}[S] \cap \mathbb{Z}[S]$.

Corollaire 1.3. *Sous les notations et les hypothèses ci-dessus on a :*
$Cl^\circ(\mathcal{M}) \simeq Cl(k(\xi_\ell)) \times Cl(k)$ *et*

$$\mathcal{R}(\mathcal{M}) \simeq A = \{(c, xN_{k(\xi_\ell)/k}(c)) \mid c \in \mathcal{S}_\ell Cl(k(\xi_\ell)), x \in Cl(k)^{2^{r-2}}\}.$$

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 $Cl(k)$, qui ne depend que de M, est appelée la classe de Steinitz de M, et on la note $cl_k(M)$ (voir [FT],Theorem 13, p. 95, ou [Co], Theorem 1.2.19, p. 9 et Corollary 1.2.24, p. 11). La structure de M en tant que O_k-module est complétement 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 aussi que $cl_k(O_K)$ est la classe de Steinitz de K/k.

Lorsque nous essayons d'étudier la conjecture 2, nous sommes confrontés au problème de plongement en liaison avec les classes de Steinitz (voir par exemple [GS2], [So5], [So6]).

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

Soient Γ un groupe fini et Δ un sous-groupe normal de Γ. 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 Γ/Δ. On désigne par $R_m(E/k, \Sigma)$ (m pour modéré) l'ensemble des classes $c \in Cl(k)$ vérifiant : il existe une extension galoisienne modérément ramifiée N/k dont la classe de Steinitz est c, contenant E, et dont le groupe de Galois est isomorphe à Γ, avec un isomorphisme π de $Gal(N/k)$ dans Γ

tel que E est le sous-corps de N fixe par $\pi^{-1}(\Delta)$, et l'action de Γ sur E correspond bien via π à l'action de Γ/Δ sur E qui est donnée.

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

Signalons un lien immédiat avec les deux conjectures précédentes. Notons 1 le sous-groupe trivial de Γ. L'anneau de groupe $O_k[1]$ étant identifié à O_k, d'après [F4], Chap. II, §3, pp. 62–63, l'injection $1 \to \Gamma$ induit le morphisme de restriction $res_1^\Gamma : Cl(O_k[\Gamma]) \to Cl(k)$ qui, à la classe d'un $O_k[\Gamma]$-module localement libre M, associe sa classe en tant que O_k-module dans $Cl(k)$; or cette dernière n'est autre chose que $cl_k(M)$ la classe de Steinitz de M. On en déduit que si N/k est une extension galoisienne modérée de k, à groupe de Galois isomorphe à Γ, alors $res_1^\Gamma([O_N]) = cl_k(O_N)$. Il en résulte que $res_1^\Gamma(\mathcal{R}(O_k[\Gamma]) = R_m(k, \Gamma)$. Il s'ensuit que la conjecture 1 implique la conjecture suivante :

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

Il découle de [Mc2] que cette conjecture est vraie lorsque Γ est abélien ; on peut voir [L] pour une description plus explicite de $R_m(k, \Gamma)$ dans le cas où Γ est un groupe cyclique d'ordre un nombre premier. Lorsque Γ n'est pas abélien, pour des travaux récents dans la direction de l'étude de $R_m(E/k, \Sigma)$ et la conjecture 3, on pourrait consulter [C1], [C2], [C3], [GS1], [GS3], [So3], [So4], [Sov].

Dans cet article, on s'interesse à la situation où $\Gamma = V \rtimes_\rho C$ et $\Delta = V$. On a $Gal(E/k) \simeq C$, donc E/k est une extension cyclique de degré $2^r - 1$. D'après [Mc2], l'ensemble $R_m(k, C)$ des classes de Steinitz des extensions modérées de k, à groupe de Galois isomorphe à C, est un sous-groupe de $Cl(k)$.

Dans la section 3, on démontre le résultat suivant :

Théorème 1.4. *Soient k un corps de nombres quelconque et E/k une extension cyclique modérée de degré $2^r - 1$. Soit $\Gamma = V \rtimes_\rho C$. On suppose la représentation ρ fidèle. Alors :*

(i) $$R_m(E/k, \Sigma) = cl_k(O_E)^{2^r} (N_{E/k}(Cl(E)))^{2^{r-2}(2^r-1)}.$$

(ii) $R_m(k, \Gamma)$ est un sous-groupe de $Cl(k)$ et

$$R_m(k, \Gamma) = R_m(k, C)^{2^r} (Cl(k))^{2^{r-2}(2^r-1)},$$

où le groupe $R_m(k, C)$ des classes de Steinitz des extensions modérées de k, à groupe de Galois isomorphe à C, est donné par la formule :

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

Ici, d parcourt l'ensemble des diviseurs positifs de 2^r-1 et ξ_d est une racine primitive $d^{ième}$ de l'unité.

Corollaire 1.5. *Sous les notations et hypothèses du théorème 1.4 on a les assertions suivantes :*

(1) Si O_E est un O_k-module libre, alors $R_m(E/k,\Sigma)$ est le sous-groupe $N_{E/k}(Cl(E))^{2^{r-2}(2^r-1)}$ de $Cl(k)$.

(2) Si $\xi_{2^r-1}\in k$ et le nombre des classes h de k est impair, alors $R_m(k,\Gamma)=Cl(k)$.

(3) Supposons $2^r-1=\ell$ est un nombre premier de Mersenne. Alors

$$R_m(k,\Gamma)=N_{k(\xi_\ell)/k}(Cl(k(\xi_\ell)))^{2^r(2^{r-1}-1)}(Cl(k))^{2^{r-2}\ell}.$$

En particulier, si h est impair, alors $R_m(k,\Gamma)=Cl(k)$.

Puisque le groupe alterné A_4 vérifie les hypothèses du théorème précédent, l'assertion (3) de ce corollaire généralise le résultat principal de [GS1] dans le cas de la ramification modérée (voir [GS1], Théorème 1.1 et Corollaire 1.2).

Enfin, signalons que le point de départ de cet article était une tentative de généralisation des arguments et résultats de [GS1], [GS2] concernant le groupe A_4 à d'autres groupes.

2 Préliminaires

Soient V un $\mathbb{F}_2$-espace vectoriel de dimension $r\geq 2$, et G un groupe commutatif d'ordre impair (alors $\mathbb{F}_2[G]$ est une algèbre semi-simple). Soit

$$\rho : G\to Aut_{\mathbb{F}_2}(V)$$

une représentation linéaire de G dans V. On note $\Gamma=V\rtimes_\rho G$ le produit semi-direct défini par ρ.

Si $g\in G$ et $v\in V$, on pose $gv=\rho(g)(v)$; ceci définit sur V une structure naturelle de $\mathbb{F}_2[G]$-module.

Dans la suite, pour ne pas alourdir les notations, on identifiera fréquemment des groupes isomorphes quand c'est faisable sans ambiguïté. Par exemple, on regardera souvent G et V comme des sous-groupes de Γ.

Soient E un corps de nombres et $E^\times=E\setminus\{0\}$. D'après la théorie de Kummer (voir par exemple [Co], §10.2), une extension N/E est galoisienne et à groupe de Galois V si et seulement s'il existe un sous-espace vectoriel W de dimension r du $\mathbb{F}_2$-espace vectoriel $E^\times/E^{\times 2}$ tel que $N=E(\sqrt{W})$, où $\sqrt{W}$ est l'ensemble de toutes les racines carrées des éléments de $E^\times$ appartenant aux classes de W, et tel que le couplage suivant soit parfait :

$$\langle , \rangle : V \times W \to \{1, -1\}$$
$$(v, w) \mapsto \langle v, w \rangle = v(\sqrt{w})/\sqrt{w},$$

où $\sqrt{w}$ est un abus de notation pour une racine carrée choisie d'un représentant choisi de la classe w.

Le groupe $\{1, -1\}$ étant isomorphe à $\mathbb{F}_2$ en tant que $\mathbb{F}_2$-espace vectoriel, le couplage précédent peut être considéré comme une forme bilinéaire non dégénérée de $V \times W$ dans $\mathbb{F}_2$. Les espaces V et W sont donc duaux :

$$W \simeq Hom(V, \{1, -1\}) \simeq Hom_{\mathbb{F}_2}(V, \mathbb{F}_2).$$

Par conséquent, il existe une représentation linéaire

$$\rho^* : G \to Aut_{\mathbb{F}_2}(W)$$

et une seule telle que pour tout $g \in G$, $v \in V$, $w \in W$

$$\langle \rho(g)(v), \rho^*(g)(w) \rangle = \langle v, w \rangle,$$

ce qui est équivalent à $\langle \rho(g^{-1})(v), w \rangle = \langle v, \rho^*(g)(w) \rangle$.

La représentation ρ^* s'appelle la contragrédiente de ρ. L'espace W a donc une structure de $\mathbb{F}_2[G]$-module défini par : pour tout $g \in G$, $gw = \rho^*(g)(w)$.

Si E/k est une extension galoisienne à groupe de Galois G, alors tout $g \in G$ induit un automorphisme du $\mathbb{F}_2$-espace vectoriel $E^\times/E^{\times 2}$, que l'on notera aussi par g. Le $\mathbb{F}_2$-espace $E^\times/E^{\times 2}$ a alors une structure naturelle de $\mathbb{F}_2[G]$-module.

Proposition 2.1. *Soient k un corps de nombres, E/k une extension galoisienne avec $Gal(E/k) = G$, W un $\mathbb{F}_2$-sous-espace de $E^\times/E^{\times 2}$ et $N = E(\sqrt{W})/E$ une extension galoisienne avec $Gal(N/E) = V$. Alors les deux assertions suivantes sont équivalentes :*

(i) N/k est galoisienne avec $Gal(N/k) \simeq \Gamma = V \rtimes_\rho G$.

(ii) L'espace W est stable sous l'action de G et la représentation naturelle de G dans $Aut_{\mathbb{F}_2}(W)$ qui en découle est la contragrédiente ρ^* de ρ.

Démonstration. Remarquons tout d'abord que N/k est galoisienne si et seulement si W est stable sous l'action de G. En effet, l'implication directe est une conséquence immédiate de la théorie de Kummer et sa réciproque est triviale.

a) Montrons l'implication $(i) \Rightarrow (ii)$. D'après la remarque ci-dessus, il reste à montrer que la représentation citée dans (ii) est la contragrédiente de ρ. Par définition du produit semi-direct défini par ρ, l'action de G sur V est l'action par conjugaison. Pour tout $g \in G$, $v \in V$ et $w \in W$, on a :

$$\begin{aligned}
\langle v, \rho^*(g)(w) \rangle &= \langle \rho(g^{-1})(v), w \rangle = \langle g^{-1}vg, w \rangle = g^{-1}vg(\sqrt{w})/\sqrt{w} \\
&= g^{-1}(v(g(\sqrt{w}))/g(\sqrt{w})) = g^{-1}(v(\sqrt{g(w)})/\sqrt{g(w)}) \\
&= v(\sqrt{g(w)})/\sqrt{g(w)} = \langle v, g(w) \rangle.
\end{aligned}$$

Le couplage étant parfait, on obtient $g(w) = \rho^*(g)(w)$. D'où l'implication.

b) Montrons maintenant l'implication $(ii) \Rightarrow (i)$. Puisque W est stable sous l'action de G, N/k est galoisienne et $Gal(N/k)$ s'insère dans la suite exacte $1 \to V \to Gal(N/k) \to G \to 1$. Cette suite est scindée car l'ordre de V est premier à celui de G. Il s'ensuit que $Gal(N/k)$ est un produit semi-direct : $V \rtimes_{\rho'} G$, où ρ' est une représentation de G dans $Aut_{\mathbb{F}_2}(V)$. Par le raisonnement de la partie a), l'action de G sur $Aut_{\mathbb{F}_2}(W)$ est la contragrédiente de ρ'. Puisque notre hypothèse dit que G agit sur $Aut_{\mathbb{F}_2}(W)$ via ρ^*, on trouve que ρ et ρ' sont isomorphes. Ce qui termine la démonstration. □

A partir de maintenant et jusqu'à la fin de l'article, on suppose que $G = C$ est un groupe cyclique d'ordre $2^r - 1$ dont on choisit un générateur σ.

Soit $\overline{\mathbb{F}_2}$ une clôture algébrique de $\mathbb{F}_2$. Dans ce qui suit, les extensions de $\mathbb{F}_2$ sont supposées incluses dans $\overline{\mathbb{F}_2}$.

La terminologie suivante est utilisée dans la théorie des codes (voir par exemple [Ro], p. 293).

Définition 2.2. *Soit $f \in \mathbb{F}_2[X]$ de degré $n \geq 1$. On dit que f est primitif s'il est le polynôme minimal d'un générateur du groupe cyclique $\mathbb{F}_{2^n}^\times (= \mathbb{F}_{2^n} \setminus \{0\})$.*

Exemples. Il existe des tables de polynômes primitifs, voir par exemple [Ro], p. 459 et p. 463. Citons-en un seul pour quelques valeurs de n :
$n = 1 : X + 1$; $n = 2 : X^2 + X + 1$; $n = 3 : X^3 + X^2 + 1$; $n = 30 : X^{30} + X^6 + X^4 + X + 1$.

Remarque. Les racines d'un polynôme irréductible de $\mathbb{F}_2[X]$ de degré n ont toutes le même ordre dans $\mathbb{F}_{2^n}^\times$ car elles sont conjuguées sous le Frobenius de $Gal(\mathbb{F}_{2^n}/\mathbb{F}_2)$. En particulier, chaque racine d'un polynôme primitif de degré n est un générateur du groupe $\mathbb{F}_{2^n}^\times$.

Proposition 2.3. *1) Sous les notations précédentes, si la représentation ρ est fidèle, alors elle est irréductible. De plus, le polynôme minimal de $\rho(\sigma) \in Aut_{\mathbb{F}_2}(V)$ est primitif de degré r et l'action de C sur $V \setminus \{1\}$ est simple et transitive.*
2) Réciproquement, à chaque polynôme primitif $f \in \mathbb{F}_2[X]$ de degré r, on peut associer une représentation fidèle de C dans $Aut_{\mathbb{F}_2}(V)$.

Démonstration. 1) Nous commençons par faire les remarques suivantes. On peut identifier l'algèbre $\mathbb{F}_2[C]$ au quotient $\mathbb{F}_2[X]/(X^{2^r-1} - 1)$, moyennant l'isomorphisme donné par $X \mapsto \sigma$. Les $\mathbb{F}_2[C]$-modules indécomposables correspondent aux $\mathbb{F}_2[X]$-modules indécomposables annulés par $X^{2^r-1} - 1$, et ces derniers sont tous de la forme $\mathbb{F}_2[X]/(g)$ avec g diviseur irréductible de $X^{2^r-1} - 1$, étant donné que ce polynôme n'a pas de facteur multiple. Si V est de la forme $\mathbb{F}_2[X]/(g)$, alors l'automorphisme $\rho(\sigma)$ de V n'est autre chose

que la multiplication par $\bar{X}$ dans l'anneau $\mathbb{F}_2[X]/(g)$; donc l'ordre de $\rho(\sigma)$ ne dépasse jamais $2^d - 1$, où d est le degré de g.

Supposons que notre représentation $\rho : C \to Aut_{\mathbb{F}_2}(V)$ soit réductible. Soit $V = \bigoplus_{i=1}^{t} V_i$, où $t > 1$ et les V_i sont des représentations indécomposables de dimension $d_i > 0$; on a donc $r = \sum_{i=1}^{t} d_i$ (rappelons que r est la dimension de V). Par les remarques precédentes, l'ordre de $\rho(\sigma)$ est borné par le ppcm des nombres $2^{d_i} - 1$. Mais $t > 1$, donc même le produit de ces nombres est strictement inferieur à $2^r - 1$. Par conséquent, l'ordre de $\rho(\sigma)$ n'est pas égal à $2^r - 1$ et donc ρ n'est pas fidèle.

Maintenant, supposons ρ fidèle. Alors ρ est irréductible d'après ce qui précède ; disons que V est de la forme $S = \mathbb{F}_2[X]/(f)$ avec f irréductible de degré r. L'anneau S est donc un corps (avec 2^r éléments). L'action de σ sur V correspond à la multiplication par $x = \bar{X}$ dans S. On en déduit que le polynôme minimal de $\rho(\sigma)$ est f, et que ρ est fidèle si et seulement si x est d'ordre $2^r - 1$. Puisque x est une racine de f, ceci revient à dire que f est primitif. De plus, dans ce cas $S \setminus \{0\}$ consiste exactement en $\{1, x, x^2, \ldots, x^{2^r-2}\}$, et on voit que C agit sur $S \setminus \{0\}$ de façon simplement transitive.

2) Si f est primitif de degré r, alors f est automatiquement irréductible et donc est un diviseur de $X^{2^r-1} - 1$. On prend $V = \mathbb{F}_2[X]/(f)$ avec l'action naturelle de σ (donc σ agit comme multiplication par $\bar{X}$). Comme ci-dessus, la primitivité de f est équivalente au fait que la représentation de C donnée par V est fidèle. En termes plus explicites : l'action de σ sur V est donnée, dans la base canonique $1, \bar{X}, \bar{X}^2, \ldots, \bar{X}^{r-1}$ de V, par la matrice compagnon attachée au polynôme f.

□

Remarques. 1) Les représentations irréductibles ρ de C dans V, à isomorphisme près, correspondent biunivoquement aux modules simples sur $\mathbb{F}_2[C]$, et ces derniers correspondent à leur tour aux diviseurs f irréductibles de $X^{2^r-1} - 1$. Dans cette bijection les représentations fidèles correspondent, on l'a vu, aux polynômes f primitifs.

2) Les tables des polynômes primitifs f (voir par exemple [Ro], p. 459 et p. 463) nous permettent de construire les groupes Γ définis par les représentations ρ fidèles ; il suffit d'utiliser la matrice compagnon associée à f. Ainsi, il est facile de vérifier que pour $r = 2$ on peut prendre (en fait on doit prendre) $f = 1 + X + X^2$ et Γ est isomorphe au groupe alterné A_4.

Dans toute la suite de l'article, on suppose ρ fidèle. On note f le polynôme minimal de $\rho(\sigma)$ et g l'élément de $\mathbb{F}_2[X]$ vérifiant

$$fg = X^{2^r-1} - 1.$$

Rappelons que si $P \in K[X]$ est de degré n, où K est un corps commutatif, on appelle polynôme réciproque de P le polynôme $\hat{P} = X^n P(X^{-1})$. Il est facile de voir que si P est irréductible et $n \geq 2$ alors $\hat{P}$ est aussi irréductible.

Proposition 2.4. *Sous les notations et hypothèses précédentes, les deux assertions suivantes sont équivalentes :*

(i) L'extension N/k est galoisienne et $Gal(N/k) \simeq \Gamma = V \rtimes_\rho C$.

(ii) Il existe $m \in E^\times / E^{\times 2}$ vérifiant $\hat{g}(\sigma)m \neq 1$ et $W = \mathbb{F}_2[C]\hat{g}(\sigma)m$.

Démonstration. a) Montrons l'implication $(i) \Rightarrow (ii)$. Comme ρ est irréductible, le $\mathbb{F}_2[C]$-module V est simple, et son contragrédient W est donc simple aussi. Comme tout module simple est monogéne et W n'est pas trivial, il existe $w \neq 1$ tel que $W = \mathbb{F}_2[C]w$.

Montrons que $\hat{f}(\sigma)w = 1$. La représentation de C dans W étant la contragrédiente de ρ (voir Prop. 2.1), pour tout i, $0 \leq i \leq 2^r - 2$, et tout $v \in V$ on a $\langle \sigma^{-i}v, w\rangle = \langle v, \sigma^i w\rangle$. Par linéarité du couplage $\langle , \rangle$ on déduit que pour tout $v \in V$ on a $\langle \hat{f}(\sigma^{-1})v, w\rangle = \langle v, \hat{f}(\sigma)w\rangle$. Or $\hat{f}(\sigma^{-1}) = \sigma^{-r}f(\sigma)$, d'où $\hat{f}(\sigma^{-1})v = 1$ et donc $\langle v, \hat{f}(\sigma)w\rangle = 1$. Comme $\langle , \rangle$ est parfait on obtient $\hat{f}(\sigma)w = 1$.

On a $\hat{f}\hat{g} = 1 - X^{2^r-1}$ $(= X^{2^r-1} - 1)$. Les racines de $1 - X^{2^r-1}$ (dans $\overline{\mathbb{F}_2}$) sont simples, par suite $\hat{f}$ et $\hat{g}$ sont premiers entre eux dans $\mathbb{F}_2[X]$. Donc il existe $h, k \in \mathbb{F}_2[X]$ tels que $h\hat{f} + k\hat{g} = 1$. On a $(k\hat{g})(\sigma)w = w$ car $\hat{f}(\sigma)w = 1$. Posons $m = k(\sigma)w$, alors $w = \hat{g}(\sigma)m$. Ce qui achève la preuve.

b) Montrons l'implication $(ii) \Rightarrow (i)$. Ecrivons $W = \mathbb{F}_2[C]w$, où $w = \hat{g}(\sigma)m$. Soit ρ' la représentation de C dans W corréspondante. Montrons que ρ' est isomorphe à ρ^*, ce qui termine la preuve grâce à la proposition 2.1. D'une part $\hat{f}(\sigma)w = (\hat{f}\hat{g})(\sigma)m = 1$. D'autre part $\hat{f}$ est irréductible car f l'est et le degré de f est ≥ 2. Donc le polynôme minimal de $\rho'(\sigma)$ est $\hat{f}$. Il est bien connu que $\rho^*(\sigma) = {}^t\rho(\sigma^{-1})$, où t désigne la transposée, il s'ensuit que le polynôme minimal de $\rho^*(\sigma)$ est $\hat{f}$. Donc ρ' est isomorphe à ρ^* d'après la première remarque qui suit la proposition 2.3. □

Soit s le morphisme surjectif naturel de $\mathbb{Z}[C]$ sur $\mathbb{F}_2[C]$. Dans toute la suite de cet article, nous ferons l'abus de notation suivant : nous noterons aussi $\hat{g}(\sigma)$ l'image réciproque, par s, de $\hat{g}(\sigma) \in \mathbb{F}_2[C]$, dont les coefficients appartiennent à $\{0, 1\}$; on dira qu'on considère $\hat{g}(\sigma)$ comme un élément de $\mathbb{N}[C]$, où $\mathbb{N} = \{0, 1, 2, \ldots\}$ est l'ensemble des entiers naturels.

Une conséquence immédiate de la proposition précédente est le résultat suivant qui est un critère de plongement d'une extension cyclique de degré $2^r - 1$ dans une extension à groupe de Galois isomorphe à Γ. Ce résultat est une généralisation du lemme 3.1 de [GS1] dont l'origine se trouve dans [M2], p. 365. Il sera utile pour la preuve des principaux résultats.

Proposition 2.5. *Soient k un corps de nombres, E/k une extension cyclique de degré 2^r-1, et L/E une extension quadratique. 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 Γ.

(ii) Il existe $m \in E$ tel que $L = E(\sqrt{\hat{g}(\sigma)m})$, où l'on a considéré $\hat{g}(\sigma)$ comme un élément de $\mathbb{N}[C]$.

De plus si (ii) est vérifiée, on peut choisir N égale à la composée des extensions $E(\sqrt{\sigma^i \hat{g}(\sigma)m})$, $0 \leq i \leq 2^r-2$.

Ci-dessous on donne quelques définitions qui seront utiles pour les sections suivantes.

Soit $\alpha(\sigma) = \sum_{i=0}^{2^r-2} a_i \sigma^i$ un élément de l'anneau de groupe $\mathbb{Z}[C]$, où $a_i \in \mathbb{Z}$.

On définit le poids entier de $\alpha(\sigma)$ et l'on note $p_e(\alpha(\sigma))$ par $p_e(\alpha(\sigma)) = \sum_{i=0}^{2^r-2} a_i$; autrement dit, c'est l'image de $\alpha(\sigma)$ par le morphisme d'augmentation $\mathbb{Z}[C] \to \mathbb{Z}$.

On définit le poids modulaire de $\alpha(\sigma)$ et l'on note $p_m(\alpha(\sigma))$ comme étant le nombre des coefficients a_i qui sont impairs.

Soient k un corps de nombres et I un idéal fractionnaire (non nul) de O_k. On appelle poids entier de I le nombre $p_e(I)$ défini comme $\sum_{\mathfrak{p}} v_{\mathfrak{p}}(I)$, où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de O_k et $v_{\mathfrak{p}}$ est la valuation $\mathfrak{p}$-adique corréspondante. Immédiatement on a $p_e(IJ) = p_e(I) + p_e(J)$ pour tout idéal fractionnaire J.

Il est clair qu'on peut écrire de façon unique : $I = I_1^2 I_2$, où I_1 est un idéal fractionnaire de O_k et I_2 est un idéal entier de O_k sans facteur carré. L'idéal I_1 est appelé la partie quadratique de I.

Nous rappelons la définition (la plus simple) d'un code cyclique (voir par exemple [Ro], p. 320) : c'est un idéal de $\mathbb{F}_q[X]/(X^n-1)$, où $\mathbb{F}_q$ est un corps fini à q éléments et n un entier naturel non nul ; ses éléments sont appelés des mots du code.

On appelle code (binaire) de Hamming (voir [Ro], p. 253 ; Theorem 7.41, p. 329) un code cyclique dans $\mathbb{F}_2[X]/(X^{2^r-1}-1)$, qui est engendré par la classe d'un polynôme primitif de $\mathbb{F}_2[X]$.

Dans notre situation, puisque $\mathbb{F}_2[C] \simeq \mathbb{F}_2[X]/(X^{2^r-1}-1)$, on définit un code cyclique de $\mathbb{F}_2[C]$ comme un idéal de $\mathbb{F}_2[C]$. Soit $\overline{\alpha(\sigma)}$ l'image d'un élément $\alpha(\sigma) \in \mathbb{Z}[C]$ dans $\mathbb{F}_2[C]$ par réduction des coefficients de $\alpha(\sigma)$ modulo 2. Dans la terminologie de la théorie des codes (voir par exemple [Ro], p. 146), $p_m(\alpha(\sigma))$ est en fait le poids du mot $\overline{\alpha(\sigma)}$ comme élément d'un code cyclique quelconque.

3 Classes de Steinitz

L'objectif de cette section est la preuve du théorème 1.4. Rappelons que $\Gamma = V \rtimes_\rho C$, où V est un $\mathbb{F}_2$-espace vectoriel de dimension $r \geq 2$, $C = \langle \sigma \rangle$ est un groupe cyclique d'ordre $2^r - 1$, et ρ est une représentation fidèle de C dans V. Rappelons aussi que f est le polynôme minimal de $\rho(\sigma)$ et g est l'élément de $\mathbb{F}_2[X]$ vérifiant $fg = X^{2^r-1} - 1$.

Nous commençons par fixer quelques notations et rappeler des résultats bien connus qui seront utilisés pour la preuve du théorème 1.4.

Soit k un corps de nombres. Si I est un idéal fractionnaire de k, on note $cl(I)$ sa classe dans $Cl(k)$. Soient $\mathcal{C}$ un cycle de k et $x \in k^\times$; l'écriture $x \equiv 1 \, mod^* \, \mathcal{C}$ est la notation de la congruence mod^* usuelle de la théorie du corps de classes (voir [N]). Si K/k est une extension finie de corps de nombres, on désigne par $[K : k]$ son degré, $\Delta(K/k)$ son discriminant et $N_{K/k}$ (resp. $Tr_{K/k}$) sa norme (resp. trace). On rappelle que $cl_k(O_K)$ est la classe de Steinitz de K/k.

Proposition 3.1. *Soit $k \subset K \subset M$ une tour de corps de nombres. Alors :*

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

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

Démonstration. L'assertion (i) est un théorème d'Artin (voir [A]) ; on peut trouver une preuve plus récente dans [M1], Théorème 1.4, p. 9. Le résultat (ii), qu'on peut lire comme la transitivité de la classe de Steinitz dans une tour de corps de nombres, est le théorème 4.1 de [F1]. □

Soit K/k une extension quadratique et soit $m \in k$ tel que $K = k(\sqrt{m})$. On a vu à la fin du §2 qu'on peut écrire de manière unique

$$mO_k = I(m)^2 J, \tag{3.1}$$

où $I(m)$ est la partie quadratique de mO_k, et J est un idéal entier sans facteur carré.

La proposition suivante découle immédiatement de la théorie de Kummer (voir [H], §39, ou [Co], §10.2) et du théorème d'Artin ci-dessus.

Proposition 3.2. *Soit $K = k(\sqrt{m})$ une extension quadratique de k. Sous les notations précédentes on a :*

(i) $\Delta(K/k) = JJ'^2$, 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 $J' = O_k$.

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

Remarque. Dans le cas de la ramification modérée, la partie quadratique de mO_k détermine la classe de Steinitz de K/k.

Dans ce paragraphe, N/k est une extension galoisienne dont le groupe de Galois est isomorphe à Γ. Si π est un isomorphisme de $Gal(N/k)$ dans Γ et $\gamma \in \Gamma$, on identifiera $\pi^{-1}(\gamma)$ et γ. Soit E/k la sous-extension de N fixe par V, alors E/k est cyclique de degré $2^r - 1$ et $Gal(E/k) \simeq C$. L'extension N/E contient $2^r - 1$ extensions quadratiques de E ; si L/E est l'une d'entre elles, alors les autres sont $\sigma^i(L)$, $1 \leq i \leq 2^r - 2$.

Proposition 3.3. *On a :*

$$cl_k(O_N) = (cl_k(O_E))^{2^r} (N_{E/k}(cl_E(O_L)))^{2^r-1}.$$

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

Lemme 3.4. *Soient K un corps de nombres, M/K une extension à groupe de Galois V, et K_i/K, $1 \leq i \leq 2^r - 1$, les sous-corps quadratiques de M/K. Alors*

$$cl_K(O_M) = \prod_{i=1}^{2^r-1} cl_K(O_{K_i}).$$

Preuve du lemme. Notons Δ le discriminant de M/K et Δ_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 [Se2], Chap. VI, §3, Cor. 2 et Prop. 6, pp. 111–112) est $\Delta = \prod_{i=1}^{2^r-1} \Delta_i$. Soient m_i, $1 \leq i \leq 2^r - 1$, des éléments de K tels que $K_i = K(\sqrt{m_i})$. Les familles $(1, \sqrt{m_i})$, $(1, \sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_{2^r-1}})$ sont des bases respectives des K-espaces vectoriels K_i et M, dont les discriminants respectifs d_i et d sont : $4m_i$ et $2^{r2^r} \prod_{i=1}^{2^r-1} m_i$. On en déduit que

$$\Delta/d = 2^{2((2-r)2^{r-1}-1)} \prod_{i=1}^{2^r-1} (\Delta_i/d_i).$$

On a alors le lemme car d'après le théorème d'Artin (voir Prop. 3.1 (i)), $cl_K(O_M) = cl(\sqrt{\Delta/d})$ et $cl_K(O_{K_i}) = cl(\sqrt{\Delta_i/d_i})$. □

Preuve de la proposition 3.3. Par la transitivité de la classe de Steinitz dans une tour de corps de nombres (voir Prop. 3.1 (ii)) on a :

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

Soient $\sigma^i(L)/E$, $0 \leq i \leq 2^r - 2$, les sous-corps quadratiques de N/E. Le lemme 3.4 nous affirme que :

$$cl_E(O_N) = \prod_{i=0}^{2^r-2} cl_E(O_{\sigma^i(L)}).$$

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 le résultat d'Artin ou par transport de structure) :

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

D'où

$$N_{E/k}(cl_E(O_N)) = (N_{E/k}(cl_E(O_L)))^{2^r-1},$$

ce qui termine la preuve de la proposition. □

Le groupe I_E des idéaux fractionnaires de E est, d'une façon naturelle, un $\mathbb{Z}[C]$-module. On choisit la notation exponentielle pour l'action de $\mathbb{Z}[C]$ sur I_E : si $I \in I_E$ et $\alpha(\sigma) = \sum_{i=0}^{2^r-2} a_i\sigma^i \in \mathbb{Z}[C]$, alors

$$I^{\alpha(\sigma)} = \prod_{i=0}^{2^r-2} \sigma^i(I)^{a_i}.$$

Il est facile de voir que $p_e(I^{\alpha(\sigma)}) = p_e(\alpha(\sigma))p_e(I)$.

Proposition 3.5. *Soit $\mathfrak{P}$ un idéal premier de O_E. Alors pour tout $e(\sigma) \in \mathbb{Z}[C]$, le poids entier de la partie quadratique de $\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)}$ est divisible par 2^{r-2}, où l'on a considéré $\hat{g}(\sigma)$ comme un élément de $\mathbb{N}[C]$.*

Le lemme suivant, qui servira dans la preuve de la proposition 3.5, est bien connu.

Lemme 3.6. *L'idéal de l'anneau $\mathbb{F}_2[C]$ (identifié à $\mathbb{F}_2[X]/(X^{2^r-1}-1)$) engendré par $f(\sigma)$ est un code binaire de Hamming. Son dual est le code de $\mathbb{F}_2[C]$ engendré par $\hat{g}(\sigma)$; les mots non nuls de ce dernier ont tous le même poids 2^{r-1}.*

Preuve du lemme. Le polynôme f étant primitif, le code engendré par $f(\sigma)$ est un code binaire de Hamming. Dans la terminologie de la théorie des codes linéaires, le dual (pour la forme bilinéaire usuelle) d'un code de Hamming est le code simplexe (voir [Ro], p. 256), et les mots non nuls de ce dernier ont tous le même poids 2^{r-1} (voir [Ro], Th. 6.1.1, p. 257). Le fait que ce dual est engendré par $\hat{g}(\sigma)$ découle de [Ro], Th. 7.4.4. 3), p. 325. □

Preuve de la proposition 3.5. Nous distinguons deux cas, selon que $\mathfrak{P} \cap O_k$ est, ou non, totalement décomposé dans E/k.

1) Supposons $\mathfrak{P} \cap O_k$ totalement décomposé dans E/k. Posons $\alpha(\sigma) = e(\sigma)\hat{g}(\sigma)$. Clairement on peut écrire $\alpha(\sigma) = 2q(\sigma) + r(\sigma)$, où les coefficients dans la base C de $r(\sigma)$ appartiennent à $\{0, 1\}$. Comme $\mathfrak{P}^{\alpha(\sigma)} = (\mathfrak{P}^{q(\sigma)})^2\mathfrak{P}^{r(\sigma)}$ et $\mathfrak{P} \cap O_k$ est totalement décomposé dans E/k, la partie quadratique de $\mathfrak{P}^{\alpha(\sigma)}$ est $\mathfrak{P}^{q(\sigma)}$, et donc son poids entier est $p_e(q(\sigma)) = [p_e(\alpha(\sigma)) - p_e(r(\sigma))]/2$. On a $p_e(q(\sigma)) = [p_e(\alpha(\sigma)) - p_m(r(\sigma))]/2$ car il est évident que $p_m(r(\sigma)) = p_e(r(\sigma))$.

D'une part, $p_e(\alpha(\sigma)) = e(1)\hat{g}(1) = e(1)2^{r-1}$; car $\hat{g}(1) = p_m(\hat{g}(\sigma))$ et, d'après le lemme 3.6, $p_m(\hat{g}(\sigma)) = 2^{r-1}$. D'autre part, l'image $\overline{\alpha(\sigma)}$ dans $\mathbb{F}_2[C]$ est un mot du code de $\mathbb{F}_2[C]$ engendré par $\hat{g}(\sigma)$. Il s'ensuit que $p_m(r(\alpha))$ $= 2^{r-1}$ ou 0 selon que $r(\sigma) \neq 0$ ou non. Donc $p_e(q(\sigma)) = 2^{r-2}(e(1)-1)$ ou $2^{r-2}e(1)$. Ce qui termine la preuve du premier cas.

2) Supposons maintenant $\mathfrak{P} \cap O_k$ non totalement décomposé dans E/k. Nous montrons que $\mathfrak{P}^{\hat{g}(\sigma)}$ est un carré.

Puisque C est cyclique d'ordre 2^r-1, le groupe de décomposition de $\mathfrak{P}$ est engendré par σ^d, où d est un diviseur de 2^r-1 et $d \neq 2^r-1$. De d divise 2^r-1 on tire X^d-1 divise $X^{2^r-1}-1$ dans $\mathbb{F}_2[X]$. Les racines de $\hat{f}$ sont les inverses de celles de f et f est primitif entraînent que $\hat{f}$ est primitif. Les racines de $\hat{f}$ étant d'ordre 2^r-1 et $d \neq 2^r-1$, on a $\hat{f}$ est premier avec X^d-1. Par conséquent X^d-1 divise $\hat{g}$. Soit $h \in \mathbb{F}_2[X]$ tel que $\hat{g} = h(X^d-1)$. On déduit l'égalité suivante dans $\mathbb{Z}[X]$ (l'abus de notation est justifié par $\mathbb{Z}[X]/2\mathbb{Z}[X] \simeq \mathbb{F}_2[X]$) : il existe $k \in \mathbb{Z}[X]$ tel que $\hat{g} = h(X^d-1) + 2k$. Mais $\mathfrak{P}^{\sigma^d-1} = O_E$, d'où $\mathfrak{P}^{\hat{g}(\sigma)} = (\mathfrak{P}^{k(\sigma)})^2$. Donc la partie quadratique de $\mathfrak{P}^{\alpha(\sigma)}$ est $\mathfrak{P}^{e(\sigma)k(\sigma)}$, et son poids entier est $p_e(e(\sigma)k(\sigma)) = e(1)2^{r-2}$, car $p_e(\hat{g}(\sigma)) = 2p_e(k(\sigma))$ et $p_e(\hat{g}(\sigma)) = p_m(\hat{g}(\sigma)) = 2^{r-1}$. Ce qui termine la preuve de 2). □

Démonstration de l'assertion (i) du théorème 1.4. Montrons la première inclusion

$$R_m(E/k, \Sigma) \subset cl_k(O_E)^{2^r} (N_{E/k}(Cl(E)))^{2^{r-2}(2^r-1)}. \tag{3.2}$$

Soit N/k une extension galoisienne modérément ramifiée à groupe de Galois isomorphe à Γ. Soit $L = E(\sqrt{\hat{g}(\sigma)m})/E$ une sous-extension quadratique de N/E (voir Prop. 2.5). Comme en (3.1), soit la décomposition :

$$\hat{g}(\sigma)mO_E = I(\hat{g}(\sigma)m)^2 J,$$

où $I(\hat{g}(\sigma)m)$ est la partie quadratique de $\hat{g}(\sigma)mO_E$, et J est un idéal entier de O_E sans facteur carré. D'après la proposition 3.2, $cl_E(O_L) = cl(I(\hat{g}(\sigma)m)^{-1})$ car L/E est modérée.

On peut écrire :

$$mO_E = \prod_{i=1}^{s} \mathfrak{P}_i^{e_i(\sigma)},$$

où $s \geq 1$, les $e_i \in \mathbb{Z}[C]$, et les $\mathfrak{P}_i$ sont des idéaux premiers de O_E au dessus d'idéaux premiers distincts de O_k ; par conséquent, les idéaux $\mathfrak{P}_i^{e_i(\sigma)}$ sont premiers entre eux deux à deux. (Signalons que les $e_i(\sigma)$ ne sont pas uniques, sauf dans le cas où tous les $\mathfrak{P}_i \cap O_k$ sont totalement décomposés dans E/k.) D'où :

$$\hat{g}(\sigma)mO_E = \prod_{i=1}^{s} \mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}.$$

Pour tout i, $1 \leq i \leq s$, il existe $q_i(\sigma), r_i(\sigma) \in \mathbb{Z}[C]$ tels que :

$$\mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)} = (\mathfrak{P}_i^{q_i(\sigma)})^2 \mathfrak{P}_i^{r_i(\sigma)},$$

où $\mathfrak{P}_i^{q_i(\sigma)}$ est la partie quadratique de $\mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}$, et $\mathfrak{P}_i^{r_i(\sigma)}$ est un idéal entier de O_E sans facteur carré . On en déduit :

$$I(\hat{g}(\sigma)m) = \prod_{i=1}^{s} \mathfrak{P}_i^{q_i(\sigma)},$$

et donc :

$$N_{E/k}(I(\hat{g}(\sigma)m)) = \prod_{i=1}^{s} N_{E/k}(\mathfrak{P}_i)^{p_e(\mathfrak{P}_i^{q_i(\sigma)})}.$$

Par la proposition 3.5, $p_e(\mathfrak{P}_i^{q_i(\sigma)})$ est divisible par 2^{r-2}. Par conséquent :

$$N_{E/k}(I(\hat{g}(\sigma)m)) = N_{E/k}(I'(\hat{g}(\sigma)m))^{2^{r-2}},$$

où $I'(\hat{g}(\sigma)m)$ est un idéal fractionnnaire de O_E. On en déduit l'existence de $c \in Cl(E)$ vérifiant :

$$N_{E/k}(cl_E(O_L)) = N_{E/k}(c)^{2^{r-2}}. \tag{3.3}$$

La proposition 3.3 et (3.3) nous donnent :

$$cl_k(O_N) = (cl_k(O_E))^{2^r} (N_{E/k}(c))^{2^{r-2}(2^r-1)},$$

ce qui entraîne (3.2).

Montrons maintenant la seconde inclusion :

$$cl_k(O_E)^{2^r} (N_{E/k}(Cl(E)))^{2^{r-2}(2^r-1)} \subset R_m(E/k, \Sigma). \tag{3.4}$$

Soit $c \in Cl(E)$. D'après le théorème de densité de Tchebotarev (voir [N], Chap. V, Th. 6.4, p. 132), il existe un idéal premier $\mathfrak{P}$ de O_E, totalement décomposé dans E/k, premier à $2O_E$ et tel que $c^{-1} = cl(\mathfrak{P})$. Il est clair que $\mathfrak{P}^{1+\sigma}$ est premier à $2O_E$. Considérons maintenant $cl(\mathfrak{P}^{1+\sigma})^{-1}$. Notons $Cl(E, 4O_E)$ le groupe des classes de rayon modulo $4O_E$. Par la surjection canonique de $Cl(E, 4O_E)$ sur $Cl(E)$ et le théorème de Tchebotarev, il existe un idéal premier $\mathfrak{Q}$ de O_E, premier à $2O_E$ et à tous les conjugués de $\mathfrak{P}$ sous $Gal(E/k)$, satisfaisant $\mathfrak{Q} \cap O_k$ totalement décomposé dans E/k et tel que

$cl(\mathfrak{P}^{1+\sigma})^{-1} = cl(\mathfrak{Q})$ dans $Cl(E, 4O_E)$. Par conséquent, il existe $m \in E^{\times}$ tel que

$$mO_E = \mathfrak{P}^{1+\sigma}\mathfrak{Q}, \text{ et } m \equiv 1 \ mod^* \ 4O_E.$$

En considérant $\hat{g}(\sigma)$ comme un élément de $\mathbb{N}[C]$ on en déduit l'égalité :

$$\hat{g}(\sigma)mO_E = \mathfrak{P}^{(1+\sigma)\hat{g}(\sigma)}\mathfrak{Q}^{\hat{g}(\sigma)}.$$

Il est clair que $\hat{g}(\sigma)m$ n'est pas un carré dans E (par exemple $v_{\mathfrak{Q}}(\hat{g}(\sigma)m) \equiv 1 \ mod \, 2$). On considère l'extension quadratique $L = E(\sqrt{\hat{g}(\sigma)m})/E$. D'après la proposition 2.5, la clôture galoisienne de L/k est une extension N/k à groupe de Galois isomorphe à Γ, et on peut prendre $N = E(\sqrt{\sigma^i\hat{g}(\sigma)m}), 0 \leq i \leq 2^r - 2)$. De $m \equiv 1 \ mod^* \ 4O_E$ on déduit que pour tout i, $0 \leq i \leq 2^r - 2$, $\sigma^i(m) \equiv 1 \ mod^* \ 4O_E$. Par suite $\hat{g}(\sigma)m \equiv 1 \ mod^* \ 4O_E$ et $\sigma^i\hat{g}(\sigma)m \equiv 1 \ mod^* \ 4O_E$. Par la proposition 3.2 (i), les extensions $E(\sqrt{\sigma^i\hat{g}(\sigma)m})/E$ sont modérées et donc N/E est modérée. Supposons E/k modérée, il s'ensuit que N/k l'est aussi.

Calculons maintenant $N_{E/k}(cl_E(O_L))$. Puisque $\mathfrak{Q}$ est totalement décomposé dans E/k, premier à tous les conjugués de $\mathfrak{P}$ et les coefficients de $\hat{g}(\sigma)$ appartiennent à $\{0, 1\}$, la partie quadratique de $\hat{g}(\sigma)mO_E$ est égale à celle de $\mathfrak{P}^{(1+\sigma)\hat{g}(\sigma)}$.

Comme dans la démonstration de la première inclusion, écrivons

$$\mathfrak{P}^{(1+\sigma)\hat{g}(\sigma)} = (\mathfrak{P}^{q(\sigma)})^2\mathfrak{P}^{r(\sigma)},$$

où la partie quadratique $I(\hat{g}(\sigma)m)$ de $\hat{g}(\sigma)mO_E$ est $\mathfrak{P}^{q(\sigma)}$. Alors

$$N_{E/k}(I(\hat{g}(\sigma)m)) = N_{E/k}(\mathfrak{P})^{p_e(q(\sigma))}.$$

Comme on l'a vu dans la preuve de la première partie de la proposition 3.5 :

$$p_e(q(\sigma)) = [p_e((1+\sigma)\hat{g}(\sigma)) - p_m((1+\sigma)\hat{g}(\sigma))]/2.$$

Un calcul simple utilisant le lemme 3.6 nous donne $p_e(q(\sigma)) = 2^{r-2}$. Par conséquent

$$N_{E/k}(cl_E(O_L)) = N_{E/k}(cl(\mathfrak{P})^{-1})^{2^{r-2}} = N_{E/k}(c)^{2^{r-2}}.$$

Par la proposition 3.3 :

$$cl_k(O_N) = (cl_k(O_E))^{2^r} N_{E/k}(c)^{2^{r-2}(2^r-1)},$$

d'où (3.4), ce qui termine la preuve de l'assertion (i) du théorème 1.4. □

Démonstration de l'assertion (ii) *du théorème 1.4.* Montrons tout d'abord l'égalité :

$$R_m(k,\Gamma) = R_m(k,C)^{2^r}(Cl(k))^{2^{r-2}(2^r-1)}. \tag{3.5}$$

Par l'assertion (i) du théorème 1.4 on a l'inclusion :

$$R_m(k,\Gamma) \subset R_m(k,C)^{2^r}(Cl(k))^{2^{r-2}(2^r-1)}.$$

Dans ce qui suit nous montrons l' inclusion :

$$R_m(k,C)^{2^r}(Cl(k))^{2^{r-2}(2^r-1)} \subset R_m(k,\Gamma). \tag{3.6}$$

Soit 1 le sous-groupe trivial de C. Comme on l'a vu au §1, l'injection $1 \to C$ induit le morphisme de restriction $res_1^C : Cl(O_k[C]) \to Cl(k)$, et l'on a $res_1^C(\mathcal{R}(O_k[C]) = R_m(k,C)$.

Soit $c \in R_m(k,C)$. D'après l'égalité précédente et les assertions $(a),(b)$ de [Mc2], Theorem. 6. 17, p. 289, il existe une extension modérée E/k, à groupe de Galois isomorphe à C, telle que $cl_k(O_E) = c$, et la seule sous-extension de E/k non ramifiée sur k est k lui-même. Ce dernier fait entraîne que $N_{E/k} : Cl(E) \to Cl(k)$ est surjective grâce à [W], Theorem 10. 1, p. 400. Il est clair que $R_m(E/k,\Sigma) \subset R_m(k,\Gamma)$. D'où $c^{2^r}(Cl(k))^{2^{r-2}(2^r-1)} \subset R_m(k,\Gamma)$, par l'assertion (i) du théorème 1.4 et l'égalité $N_{E/k}(Cl(E)) = Cl(k)$. Donc on a (3.6), ce qui achève la preuve de (3.5).

L'entier $2^r - 1$ étant impair, l'égalité suivante, citée dans l'énoncé du théorème 1.4, et dans ses notations, découle de [E], Theorem 1.3, p. 29 :

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

□

Preuve du corollaire 1.5. (1) Par définition de la classe de Steinitz, O_E est un O_k-module libre si et seulement si $cl_k(O_E) = 1$, d'où (1) par la partie (i) du théorème 1.4.

(2) Pour $d = 2^r - 1$ on a $(d-1)(2^r-1)/2d = 2^{r-1} - 1$; d'après l'assertion (ii) du théorème 1.4, $H = (Cl(k))^{2^r(2^{r-1}-1)}(Cl(k))^{2^{r-2}(2^r-1)} \subset R_m(k,\Gamma)$ car $\xi_d \in k$. On a immédiatement $H = Cl(k)$, car le nombre des classes h de k est supposé impair (donc $Cl(k)^{2^r} = Cl(k)^{2^{r-2}} = Cl(k)$) et les entiers $2^{r-1} - 1$ et $2^r - 1$ sont premiers entre eux.

(3) La formule donnant $R_m(k,\Gamma)$ provient de l'assertion (ii) du théorème 1.4. Soit $H' = N_{k(\xi_\ell)/k}(Cl(k(\xi_\ell))$. Il faut montrer que l'inclusion $H'^{2^r(2^{r-1}-1)}$ $Cl(k)^{2^{r-2}\ell} \subset Cl(k)$ est une égalité. Nous pouvons aussitôt oublier les 2-puissances dans les exposants, car $Cl(k)$ est un groupe d'ordre impair. Le sous-groupe H' contient $Cl(k)^{\ell-1}$ puisque le degré de $k(\xi_\ell)/k$ divise $\ell - 1$.

Il suffit donc de voir que $Cl(k)^{(\ell-1)(2^{r-1}-1)}Cl(k)^{\ell} = Cl(k)$. Or $2^{r-1}-1$ et $\ell = 2^r - 1$ sont premiers entre eux. Donc les deux exposants $(\ell-1)(2^{r-1}-1)$ et ℓ sont premiers entre eux, et cela suffit.

□

4 Classes réalisables

Le but de cette section est la preuve du théorème 1.1. Rappelons que la situation est la suivante : $\Gamma = V \rtimes_\rho C$, où V est un $\mathbb{F}_2$-espace vectoriel de dimension $r \geq 2$, $C = \langle\sigma\rangle$ est un groupe cyclique d'ordre $2^r - 1$, et ρ est une représentation fidèle de C dans V.

Le groupe dérivé (engendré par les commutateurs) $[\Gamma, \Gamma]$ de Γ s'identifie à $(\sigma-1)V$. Mais $(\sigma-1)V = V$ car V est un $\mathbb{F}_2[C]$-module simple. Pareillement $(\sigma^i - 1)V = V$ pour tout i, $1 \leq i \leq 2^r - 2$. On en déduit que pour tout i dans cet intervalle, l'élément $\sigma^i v$ est conjugué à σ^i, quel que soit $v \in V$. D'autre part, les éléments σ^i et σ^j ne sont pas conjugués pour $i \neq j$, car leurs images dans le groupe abélien $\Gamma/V = C$ sont distincts. Les $v \neq 1$ sont tous conjugués puisque l'action de C sur $V \setminus \{1\}$ est transitive. On conclut que le groupe Γ possède exactement les 2^r classes de conjugaison suivantes : la classe $\{1\}$, la classe $V \setminus \{1\}$, et les classes $\{\sigma^i v, v \in V\}$ avec $1 \leq i \leq 2^r - 2$. Donc (voir [Se1]), Γ a 2^r caractères absolument irréductibles. Parmi eux il y a exactement $2^r - 1$ caractères de degré 1 (linéaires). Ce sont les caractères qui proviennent de $\Gamma/[\Gamma, \Gamma]$, groupe qui s'identifie à C, et on peut les noter φ_i, $0 \leq i \leq 2^r - 2$, avec φ_i défini par :

$$\varphi_i(\sigma) = \xi_{2^r-1}^i, \varphi_i(v) = 1 \text{ pour tout } v \in V,$$

où ξ_{2^r-1} est une racine primitive $(2^r - 1)^{\text{ième}}$ de l'unité.

Il en reste un seul qu'on note χ. Par la formule $\sum_{i=0}^{2^r-2} \varphi_i(1)^2 + \chi(1)^2 = |\Gamma| = 2^r(2^r - 1)$ (voir [Se1], §2. 4, Corollaire 2, p. 31), le degré de χ est $2^r - 1$. Soit ψ un caractère complexe, irréductible et non trivial de V. Montrons que χ est induit par ψ, i.e., $\chi = Ind_V^\Gamma \psi$.

Comme pour tout $i, 0 \leq i \leq 2^r - 2$, φ_i est trivial sur V et $\sum_{v \in V} \psi(v) = 0$, par la formule de réciprocité de Frobenius (voir [Se1], Théorème 13, p. 73, et la remarque 2 qui le suit) $Ind_V^\Gamma \psi$ est orthogonal à tous les φ_i. Puisque le degré de $Ind_V^\Gamma \psi$ est égal à $|\Gamma/V| = 2^r - 1$, $\chi = Ind_V^\Gamma \psi$.

Remarque. On vérifie facilement que pour tout i, $1 \leq i \leq 2^r - 2$, $Ind_V^\Gamma \psi(\sigma^i) = 0$, et pour tout $v \in V \setminus \{1\}$, $Ind_V^\Gamma \psi(v) = -1$. On en déduit que χ est à valeurs dans $\{0, -1, 2^r - 1\}$.

Soient $n+1$ le nombre des classes de conjugaison sur k des caractères φ_i, et $\{\psi_i, 0 \leq i \leq n\}$ un système de leurs représentants avec ψ_0 le caractère trivial.

Alors Γ possède $n+2$ classes de conjugaison sur k de caractères absolument irréductibles dont les représentants sont ψ_i, $0 \leq i \leq n$, et $\psi_{n+1} = \chi$.

Pour tout i, $0 \leq i \leq n$, la restriction de ψ_i à C définit un caractère non trivial de C, car $Ker(\psi_i) = V$, 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 C (c'est la notation de l'introduction). 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, $0 \leq i \leq n$.

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

$$k[\Gamma] = \prod_{i=0}^{n+1} M_{n_i}(D_i),$$

où D_i est un corps gauche de centre $k(\psi_i)$ 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 $k(\psi_i)$ 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 $0 \leq i \leq n$. Aussi, $m_{n+1} = 1$ car χ est réalisable sur k : rappelons que χ est induit par ψ et ce dernier est réalisable sur k car V est d'exposant 2. On en déduit immédiatement que :

$$k[\Gamma] \simeq \prod_{i=0}^{n} k(\psi_i) \times M_{2^r-1}(k) = \prod_{i=0}^{n} k(\chi_i) \times M_{2^r-1}(k).$$

Soit $\mathcal{M}$ un O_k-ordre maximal de $k[\Gamma]$ contenant $O_k[\Gamma]$. Puisque la dimension de chaque composante simple de $k[\Gamma]$ sur son centre est différente de 4, $k[\Gamma]$ vérifie la condition d'Eichler (voir [R], Definition 38. 1, pp. 343–344 ; Remarque (34.4), p. 294). Par conséquent, par un résultat de Swan (voir [Sw] ou [R], Theorem 35. 14, p. 313) on a :

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

D'où

$$Cl^\circ(\mathcal{M}) \simeq \prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(k) \simeq Cl^\circ(\mathcal{M}(C)) \times Cl(k). \tag{4.1}$$

Soit K un corps de nombres quelconque et Γ' un groupe fini tel que $K[\Gamma']$ satisfait la condition d'Eichler. Soit $\mathcal{M}'$ un O_K-ordre maximal de $K[\Gamma']$ contenant $O_K[\Gamma']$. Ci-dessous, nous rappelons la Hom-description de Fröhlich du groupe des classes $Cl(\mathcal{M}')$ (voir [F2], [F4] ou [CR], §52).

On désigne par $R_{\Gamma'}$ le groupe des caractères virtuels de Γ'. Soient $\overline{K}$ une clôture algébrique de K, $\Omega_K = Gal(\overline{K}/K)$, $J(\overline{K})$ le groupe des idèles de $\overline{K}$, et $U(\overline{K})$ le sous-groupe des idèles unités de $J(\overline{K})$. Alors

$$Cl(\mathcal{M}') \simeq \frac{Hom_{\Omega_K}(R_{\Gamma'}, J(\overline{K}))}{Hom_{\Omega_K}(R_{\Gamma'}, \overline{K}^{\times}) \times Hom_{\Omega_K}(R_{\Gamma'}, U(\overline{K}))}.$$

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'.

La notion de résolvante de Fröhlich-Lagrange, dont nous rappelons la définition ci-dessous (voir [F4], pp. 28–29), est un outil fondamental pour étudier le problème des classes réalisables.

Soit M/K une extension galoisienne à groupe de Galois isomorphe à Γ'. Si π est un isomorphisme défini sur $Gal(M/K)$ et à valeurs dans Γ', alors tout caractère χ' de Γ' induit un caractère $\chi' \circ \pi$ de $Gal(M/K)$ que l'on notera aussi χ'. Si $\gamma \in \Gamma'$, nous noterons $\pi^{-1}(\gamma) \in Gal(M/K)$ simplement par γ. Soit B une K-algèbre commutative, alors $N \otimes_K B$ est un $B[\Gamma']$-module libre de rang 1 ; soit $a \in N \otimes_k B$ une base de ce module. Soit $T : \Gamma' \to GL_n(\overline{K})$ une représentation linéaire de Γ' de caractère χ'. On appelle résolvante de Fröhlich-Lagrange de a et de χ', l'élément de $\overline{K} \otimes_K B$, noté $\langle a, \chi' \rangle_{M/K}$ (ou $\langle a, \chi' \rangle$ si aucune confusion n'est possible), défini par :

$$\langle a, \chi' \rangle_{M/K} = Det(\sum_{\gamma \in \Gamma'} \gamma(a) T(\gamma^{-1})),$$

où Det désigne le déterminant.

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 : $M_{\mathfrak{p}} = M \otimes_K K_{\mathfrak{p}}$ et $O_{M,\mathfrak{p}} = O_M \otimes_{O_K} O_{K,\mathfrak{p}}$.

Supposons M/K modérée. On sait que O_M est un $O_K[\Gamma']$-module localement libre de rang 1 (voir [No] ou [F4], Chap. I, §3, pp. 26–28). Pour tout idéal premier $\mathfrak{p}$ de O_K, soit $\alpha_{\mathfrak{p}}$ une base (normale locale entière) du $O_{K,\mathfrak{p}}[\Gamma]$-module $O_{M,\mathfrak{p}}$. Soit a une base (normale) du $K[\Gamma']$-module M. D'après Fröhlich (voir [F4]), un représentant de la classe de $\mathcal{M}' \otimes_{O_K[\Gamma']} O_M$ dans $Cl(\mathcal{M}')$ est l'application f définie par :

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

A partir de maintenant N/k désigne une extension modérément ramifiée à groupe de Galois isomorphe à Γ. Nous notons par E le sous-corps de N fixe par V. Dans ce qui suit, on va déterminer un élément f de $Hom_{\Omega_k}(R_\Gamma, J(\overline{k}))$ qui représente $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ dans $Cl(\mathcal{M})$ en donnant les valeurs qu'il prend en ψ_i, $0 \leq i \leq n$, et χ.

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 $\langle \alpha_{\mathfrak{p}}, \psi_0 \rangle = Tr_{N_{\mathfrak{p}}/k_{\mathfrak{p}}}(\alpha_{\mathfrak{p}})$ et $\langle a, \psi_0 \rangle = Tr_{N/k}(a)$, où Tr désigne la trace. On peut supposer que $Tr_{N/k}(a) = 1$ (sinon prendre

$a/Tr_{N/k}(a)$). 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 :

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

Soit i, $1 \leq i \leq n$. Les égalités suivantes découlent facilement de la définition des résolvantes de Fröhlich-Lagrange (on peut voir aussi [F3], Theorem 10, p. 162) :

$$\langle \alpha_{\mathfrak{p}}, \psi_i \rangle = \langle Tr_{N_{\mathfrak{p}}/E_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}), \chi_i \rangle_{E/k}, \tag{4.2}$$

$$\langle a, \psi_i \rangle = \langle Tr_{N/E}(a), \chi_i \rangle_{E/k}. \tag{4.3}$$

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

On pose :

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

Soient b et $b_{\mathfrak{p}}$ des bases respectives du $E[V]$-module N et du $O_{E,\mathfrak{p}}[V]$-module $O_{N,\mathfrak{p}}$. Puisque $\chi = Ind_V^{\Gamma}\psi$, par un résultat de Fröhlich (voir [F2], Theorem 7, ou [F3], Theorem 12, p. 165), il existe λ et $\lambda_{\mathfrak{p}}$ des éléments inversibles respectifs des anneaux $k[V]$ et $O_{k,\mathfrak{p}}[V]$ tels que :

$$\langle a, \chi \rangle \psi(\lambda) = \mathfrak{N}_{E/k}(\langle b, \psi \rangle_{N/E}) e(E/k), \tag{4.4}$$

et

$$\langle \alpha_{\mathfrak{p}}, \chi \rangle \psi(\lambda_{\mathfrak{p}}) = \mathfrak{N}_{E/k}(\langle b_{\mathfrak{p}}, \psi \rangle_{N/E}) e(E_{\mathfrak{p}}/k_{\mathfrak{p}}), \tag{4.5}$$

où ψ a été prolongée par linéarité à $k_{\mathfrak{p}}[V]$, $e(E/k)^2$ 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

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

Dans notre situation :

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

car ψ est à valeurs dans $\{1, -1\}$. Ainsi $\mathfrak{N}_{E/k} = N_{E/k}$. Les égalités (4.4) et (4.5) impliquent :

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

D'une part, l'application définie sur R_Γ et à valeurs dans $\overline{k}^\times$ qui à ψ_i, $0 \leq i \leq n$, associe 1, et qui à χ associe $\psi(\lambda)$, est un élément de $Hom_{\Omega_k}(R_\Gamma, \overline{k}^\times)$. D'autre part, l'application définie sur R_Γ et à valeurs dans $U(\overline{k})$ qui à ψ_i, $0 \leq i \leq n$, associe 1, et qui a χ associe $\psi(\lambda_\mathfrak{p})^{-1}$, est un élément de $Hom_{\Omega_k}(R_\Gamma, U(\overline{k}))$.

On pose :

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

En résumé on a donc la proposition suivante :

Proposition 4.1. *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 :*

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

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

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

Rappelons que (dans les notations du §1) $\mathcal{M}(C)$ est l'ordre maximal de O_k dans $k[C]$, $\mathcal{R}(\mathcal{M}(C))$ est 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 C, et $\mathcal{R}(\mathcal{M}(C))$ est un sous-groupe de $Cl^\circ(\mathcal{M}(C)) \simeq \prod_{i=1}^n Cl(k(\chi_i))$. Dans la suite, nous identifierons souvent $Cl^\circ(\mathcal{M}(C))$ avec $\prod_{i=1}^n Cl(k(\chi_i))$ sous l'isomorphisme précédent.

Proposition 4.2. *Soient c_i, $0 \leq i \leq n+1$, les composantes de $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $\prod_{i=0}^n Cl(k(\chi_i)) \times Cl(k))$. Alors*

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

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

(iii) $c_{n+1} = cl_k(O_E) N_{E/k}(cl_E(O_L))$ dans $Cl(k)$, où L/E est une sous-extension quadratique de N/E.

Démonstration. (i) C'est est évident. On peut voir (i) comme l'assertion qui entraîne l'inclusion : $\mathcal{R}(\mathcal{M}) \subset Cl^\circ(\mathcal{M})$.

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

D'après les égalités (4.2), (4.3) et la remarque qui les suit, il est clair que l'élément f_1 de $Hom_{\Omega_k}(R_C, J(\overline{k}))$, qui au caractère trivial de C associe 1 et à χ_i, $1 \leq i \leq n$, associe $f_1(\chi_i) = f(\psi_i)$, est un représentant de $[\mathcal{M}(C) \otimes_{O_k[C]} O_E]$ dans la Hom-description de $Cl(\mathcal{M}(C))$. On en déduit que les composantes de $[\mathcal{M}(C) \otimes_{O_k[C]} O_E]$ dans $\prod_{i=1}^n Cl(k(\chi_i))$ sont celles de $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $\prod_{i=1}^n Cl(k(\chi_i))$. D'où (ii).

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

$$k[V] \simeq \prod_{i=0}^{2^r-1} E \text{ et } Cl(\mathcal{M}_2) \simeq \prod_{i=0}^{2^r-1} Cl(E).$$

Posons $\Omega_E = Gal(\overline{k}/E)$. Soit f_2 l'élément de $Hom_{\Omega_E}(R_V, J(\overline{k}))$ qui au caractère trivial de V fait correspondre 1, et pour tout caractère absolument irréductible non trivial χ' de V 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 $[\mathcal{M}_2 \otimes_{O_E[V]} O_N]$ dans la Hom-description de $Cl(\mathcal{M}_2)$, et les composantes de $[\mathcal{M}_2 \otimes_{O_E[V]} O_N]$ dans $\prod_{i=0}^{2^r-1} Cl(E)$, identifié à $Cl(\mathcal{M}_2)$, sont les classes des contenus des idèles $f_2(\chi')$.

Soit L/E la sous-extension quadratique de N/E fixe par $Ker(\psi)$. Le caractère ψ définit par restriction un caractère $\underline{\psi}$ de $Gal(L/E)$. Il est facile de vérifier (comme dans (4.2) et (4.3)) qu'on a :

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

D'après [F4], Note 4, pp. 50–51, la classe dans $Cl(E)$ du contenu de l'idèle dont les composantes sont écrites dans le membre de droite de l'égalité précédente est la classe de l'idéal fractionnaire $\frac{\langle O_L, \underline{\psi} \rangle_{L/E}}{\langle Tr_{N/L}(b), \underline{\psi} \rangle_{L/E}}$. La classe de ce dernier est égale à $cl_E(O_L)$ par la proposition 2.3 et [So1], Théorèmes 2.2 et 2.3, cas $l = 2$.

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 Proposition 3.1). On en déduit que $cl_k(O_E) = cl(I)$. Donc la classe du contenu de l'idèle $f(\chi)$ dans $Cl(k)$ est égale à $cl_k(O_E) N_{E/k}(cl_E(O_L))$. Ce qui termine la preuve de (*iii*). □

Démonstration de du théorème 1.1. La proposition 4.2 nous permet d'identifier $\mathcal{R}(\mathcal{M})$ avec un sous-ensemble de $\prod_{i=1}^{n} Cl(k(\chi_i)) \times Cl(k))$. Dans la suite nous montrerons les inclusions : $\mathcal{R}(\mathcal{M}) \subset A$ et $A \subset \mathcal{R}(\mathcal{M})$, où A est l'ensemble défini dans l'énoncé du théorème 1.1.

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

On utilise les hypothèses et notations de la proposition 4.2. Tout d'abord $(c_1, c_2, \ldots, c_n) \in \mathcal{R}(\mathcal{M}(C))$ par cette dernière. Soient f un représentant de $[\mathcal{M}(C) \otimes_{O_k[C]} O_E]$ dans la Hom-description de $Cl(\mathcal{M}(C))$ et r_C le caractère de la représentation régulière de C. D'après [Mc3], Proposition 12, $cl_k(O_E)$ est représentée par le contenu de l'idèle $f(r_C) \in J(k)$ (on pourrait voir [F4], pp. 62–63, pour reconstruire la preuve). On en déduit :

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

Soit $x = N_{E/k}(cl_E(O_L))$. L'égalité (3.3) (voir §3) implique $x \in Cl(k)^{2^{r-2}}$. Comme $c_{n+1} = x \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)$, on conclut que $(c_1, c_2, \ldots, c_{n+1}) \in A$. Par suite $\mathcal{R}(\mathcal{M}) \subset A$.

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

Soit $X = (c_1, c_2, \ldots, c_n, c_{n+1} = x \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)) \in A$, où x est un élément de $Cl(k)^{2^{r-2}}$. Tout d'abord on considère l'élément $(c_1, c_2, \ldots, c_n)$ de $\mathcal{R}(\mathcal{M}(C))$. Soit $Ex : Cl(O_k[C]) \to Cl(\mathcal{M}(C))$ la surjection induite par l'extension des scalaires de $O_k[C]$ à $\mathcal{M}(C)$. Puisque $Ex(\mathcal{R}(O_k[C])) = \mathcal{R}(\mathcal{M}(C))$, les assertions $(a), (b)$ de [Mc2], Theorem. 6. 17, p. 289, nous affirment l'existence d'une extension modérée E/k, à groupe de Galois isomorphe à C, telle que $[\mathcal{M}(C) \otimes_{O_k[C]} O_E] = (c_1, c_2, \ldots, c_n)$ et la seule sous-extension de E/k non ramifiée sur k est k lui-même. Ce dernier fait entraîne que $N_{E/k} : Cl(E) \to Cl(k)$ est surjective grâce à [W], Theorem 10. 1, p. 400.

Ensuite on considère l'élément x de $Cl(k)^{2^{r-2}}$. Soit $y \in Cl(k)$ tel que $x = y^{2^{r-2}}$. Choisissons $c \in Cl(E)$ tel que $N_{E/k}(c) = y$. Maintenant on copie la preuve de l'inclusion (3.4) (voir §3). Dans les notations de cette preuve, on construit une extension modérée N/k contenant E, à groupe de Galois isomorphe à Γ et vérifiant

$$N_{E/k}(cl_E(O_L)) = N_{E/k}(c)^{2^{r-2}}.$$

D'où :

$$N_{E/k}(cl_E(O_L)) = y^{2^{r-2}} = x.$$

En vertu de la proposition 4.2, $X \in \mathcal{R}(\mathcal{M})$. Donc $A \subset \mathcal{R}(\mathcal{M})$. □

Preuve du corollaire 1.2. Nous avons vu au §2 (voir la remarque 2 qui suit la proposition 2.3) que le groupe alterné A_4 est un exemple de groupe Γ qui vérifie les hypothèses du théorème 1.1 ; dans ce cas C est un groupe cyclique d'ordre 3. D'après [Mc1], Theorem, p. 103, ou Corollary 5.11, on a $\mathcal{R}(\mathcal{M}(C)) = Cl^{\circ}(\mathcal{M}(C))$, car il est facile de vérifier que l'idéal de Stickelberger de [Mc1] défini dans $\mathbb{Z}[Aut(C)]$ est $\mathbb{Z}[Aut(C)]$ tout entier. L'assertion (4.1) nous donne $Cl^{\circ}(\mathcal{M}) \simeq Cl^{\circ}(\mathcal{M}(C)) \times Cl(k)$. Le reste découle de la table des caractères d'un groupe cyclique d'ordre 3. □

Preuve du corollaire 1.3. La preuve est immédiate. En effet : d'après le théorème 2.4 de [So1] (Attention : dans [So1], $\mathcal{R}(\mathcal{M})$ est noté $\mathcal{R}(O_k[\Gamma])$), $\mathcal{R}(\mathcal{M}(C)$ est isomorphe à $\mathcal{S}_\ell Cl(k(\xi_\ell))$. □

Références

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

[BS1] N. P. Byott and B. Sodaïgui, *Realizable Galois module classes for tetrahedral extensions*, Compositio Math. (2004), à paraître.

[BS2] N. P. Byott and B. Sodaïgui, *Galois module structure for dihedral extensions of degree 8 : realizable classes over the group ring* , soumis.

[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.

[Co] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer-Verlag, GTM 193, New York, 2000.

[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, *Arithmetic and Galois module structure for tame extensions*, J. Reine Angew. Math. 286/287 (1976), 380–440.

[F3] A. Fröhlich, *Galois Module Structure*, in "Algebraic Number Fields", Proceedings of the Durham Symposium, 1975, pp. 133–191, Academic Press, London, 1977.

[F4] 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.

[GS1] M. Godin et B. Sodaïgui, *Classes de Steinitz d'extensions à groupe de Galois* A_4, J. Théor. Nombres Bordeaux 14 (2002), 241–248.

[GS2] M. Godin et B. Sodaïgui, *Realizable classes of tetrahedral extensions*, J. Number Theory 98 (2003), 320–328.

[GS3] M. Godin et B. Sodaïgui, *Module structure of rings of integers in octahedral extensions,* Acta Arith. 109.4 (2003), 321–327.

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

[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*, Ann. Inst. Fourier (1969), 1–80.

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

[Mc1] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra 82 (1983), 102–134.

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

[Mc3] L. R. McCulloh, *From Galois module classes to Steinitz classes* , Informal report (2002), Oberwolfach (Orders in arithmetic and geometry).

[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.

[Ro] S. Roman, *Coding and Information Theory*, GTM 134, Springer-Verlag, New York, 1992.

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

[So5] B. Sodaïgui, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, J. Algebra 223 (2000), 367–378.

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

[Sov] E. Soverchia, *Steinitz classes of metacyclic extensions*, J. London Math. Soc. (2) 66 (2002), no.1, 61–72.

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

[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*, 2ème édition, Springer-Verlag, Berlin, 1996.