# Classes réalisables d'extensions non abéliennes de degré p3

Maya Farhat, Bouchaïb Sodaïgui

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

Maya Farhat, Bouchaïb Sodaïgui *

*Université de Valenciennes, Département de Mathématiques, Le Mont Houy, 59313 Valenciennes Cedex 9, France*

R É S U M É

Soient $k$ un corps de nombres et $O_k$ son anneau d'entiers. Soit $p$ un nombre premier impair. Soit $\Gamma$ un groupe non abélien d'ordre $p^3$. Soient $\mathcal{M}$ un $O_k$-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$, et $Cl(\mathcal{M})$ le groupe des classes des $\mathcal{M}$-modules localement libres. On définit l'ensemble $\mathcal{R}(\mathcal{M})$ des classes réalisables comme étant l'ensemble des classes $c \in Cl(\mathcal{M})$ telles qu'il existe une extension $N/k$ modérément ramifiée, à groupe de Galois isomorphe à $\Gamma$, avec la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ égale $c$, où $O_N$ est l'anneau des entiers de $N$. Soit $\xi$ (resp. $\xi_{p^2}$) une racine primitive $p$-ième (resp. $p^2$-ième) de l'unité. Dans cet article, sous l'hypothèse que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes et $k(\xi_{p^2})/k(\xi)$ non ramifiée lorsque $\Gamma$ est d'exposant $p^2$, on définit un sous-ensemble de $Cl(\mathcal{M})$ par l'intermédiaire d'un idéal de Stickelberger, et on montre qu'il est un sous-groupe de $Cl(\mathcal{M})$ contenu dans $\mathcal{R}(\mathcal{M})$.

A B S T R A C T

Let $k$ be a number field and $O_k$ its ring of integers. Let $p$ be an odd prime number. Let $\Gamma$ be a non-abelian group of order $p^3$. Let $\mathcal{M}$ be a maximal $O_k$-order in the semi-simple algebra $k[\Gamma]$ containing $O_k[\Gamma]$, and let $Cl(\mathcal{M})$ be its locally free classgroup. We define the set $\mathcal{R}(\mathcal{M})$ of realizable classes to be the set of classes $c \in Cl(\mathcal{M})$ such that there exists a Galois extension $N/k$ which is tame, with Galois group isomorphic to $\Gamma$, and for which the class of $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ is equal to $c$, where $O_N$ is the ring of integers of $N$. Let $\xi$ (resp. $\xi_{p^2}$) be a primitive $p$th (resp. $p^2$th) root of unity. In the present article, under the hypothesis that $k/\mathbb{Q}$ and $\mathbb{Q}(\xi)/\mathbb{Q}$ are linearly disjoint and $k(\xi_{p^2})/k(\xi)$ is not ramified when $\Gamma$ has exponent $p^2$, we define a subset of $\mathcal{R}(\mathcal{M})$ by means of a Stickelberger ideal, and prove that it is a subgroup of $Cl(\mathcal{M})$ contained in $\mathcal{R}(\mathcal{M})$.

## 1. Introduction et énoncé des principaux résultats

Dans tout ce t 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 et $\Gamma$ un groupe fini. Soient $\mathcal{M}$ un $O_k$-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$. Soit $Cl(O_k[\Gamma])$ (resp. $Cl(\mathcal{M})$) le groupe des classes des $O_k[\Gamma]$-modules (resp. $\mathcal{M}$-modules) localement libres (voir [10, Chap. I]). Soit $M$ un $O_k[\Gamma]$-module localement libre. On peut associer à $M$ une classe, notée $[M]$, dans $Cl(O_k[\Gamma])$, et par extension des scalaires la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} M$, notée $[\mathcal{M} \otimes_{O_k[\Gamma]} M]$, dans $Cl(\mathcal{M})$. Ceci s'applique à $M = O_N$, où $N/k$ est une extension galoisienne, modérément ramifiée et à groupe de Galois isomorphe à $\Gamma$.

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

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

On conjecture (voir par exemple [5]) que $\mathcal{R}(O_k[\Gamma])$ et $\mathcal{R}(\mathcal{M})$ sont des sous-groupes respectifs de $Cl^\circ(O_k[\Gamma])$ et $Cl^\circ(\mathcal{M})$ ; signalons que cela est vrai lorsque $\Gamma$ est abélien (voir [13]). Cette conjecture (non abélienne) peut être considérée comme un complément à celle de Fröhlich sur les anneaux d'entiers de corps de nombres (la conjecture de Fröhlich est démontrée dans [20]).

Pour des résultats récents dans la direction de l'étude de la conjecture non abélienne sur les classes réalisables voir [3–7,14,19].

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

Lorsque $\Gamma$ est le groupe diédral $D_4$ (resp. quaternionien) d'ordre 8 et $k$ est un corps de nombres linéairement disjoint de $\mathbb{Q}(i)$ sur $\mathbb{Q}$, où $i^2 = -1$, on montre dans [17] (resp. [16]) que si le nombre de classes (resp. le nombre de classes au sens restreint) de $k$ est impair, alors $\mathcal{R}(\mathcal{M}) = Cl^\circ(\mathcal{M})$.

Dans [7] on montre que $\mathcal{R}(O_k[D_4]) = Cl^\circ(O_k[\Gamma])$ sous l'hypothèse que l'ordre du groupe de classes de rayon de $k$ modulo $4O_k$ est impair.

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

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

Pour ne pas alourdir les notations, on identifiera fréquemment des groupes isomorphes quand c'est faisable sans ambiguïté, et on indiquera l'isomorphisme si c'est nécessaire. Par exemple, si $G$ est un groupe, chaque fois qu'on indique $G \simeq C$ (resp. $H$), l'isomorphisme en question envoie le générateur apparent de $G$ vers $\sigma$ (resp. les deux générateurs apparents de $G$ vers $\tau_0, \nu_0$).

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

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

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

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

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

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

Le point de départ du présent article était la lecture des articles [2,8] et une tentative de la détermination de $\mathcal{R}(\mathcal{M})$ lorsque $\Gamma$ est un groupe non abélien d'ordre $p^3$. Nous n'avons pas réussi la détermination de $\mathcal{R}(\mathcal{M})$ à cause de grandes difficultés provenant d'un problème de plongement (voir Proposition 2.6 ci-dessous) en liaison avec la donnée d'éléments de l'ensemble $\mathcal{R}(\mathcal{M}(H))$ des classes réalisables des extensions modérées à groupe de Galois $H$, où $\mathcal{M}(H)$ est le $O_k$-ordre maximal dans $k[H]$ (on pourrait consulter Proposition 2.2(ii) ci-dessous pour avoir une idée de tels éléments). Mais sous l'hypothèse que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes et $k(\xi_{p^2})/k(\xi)$ est non ramifiée lorsque $\Gamma$ est d'exposant $p^2$, où $\xi_{p^2}$ est une racine $p^2$-ième de l'unité, nous avons déterminé à l'aide

d'un idéal de Stickelberger, pour chaque type de $\Gamma$, un sous-groupe de $Cl^\circ(\mathcal{M})$ contenu dans $\mathcal{R}(\mathcal{M})$ (voir une démarche analogue dans [14,18]).

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

Les caractères absolument irréductibles de $\Gamma$ sont (voir [11, Théorème 26.6, p. 302]) :

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

où pour pour tout $(r,s,t)$ :

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

et

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

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

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

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

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

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

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

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

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

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

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

**Pour simplifier les notations, posons**

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

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

Il est immédiat que la décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante (utiliser [9, p. 330 et §74]) :

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

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

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

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

D'où :

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

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

Soit

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

Soit l'élément de Stickelberger

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

et soit l'idéal de Stickelberger

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

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

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

Dans la Section 3, on démontre le théorème suivant :

**Théorème 1.1.** *Soient $k$ un corps de nombres, $p$ un nombre premier impair et $\xi$ (resp. $\xi_{p^2}$) une racine primitive $p$-ième (resp. $p^2$-ième) de l'unité. Soit $\Gamma$ un groupe non abélien d'ordre $p^3$. Supposons les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ linéairement disjointes. Identifions $Cl^\circ(\mathcal{M})$ et $\prod_{i=0}^{p+1} Cl(k(\xi))$.*

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

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

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

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

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

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

Si $K'/k'$ est une extension de corps de nombres de degré $s$, alors il existe un idéal $I$ de $O_{k'}$ tel que $O_{K'} \simeq O_{k'}^{s-1} \oplus I$ en tant que $O_{k'}$-module. La classe de $I$ dans $Cl(k')$ est appelée la classe de Steinitz de $K'/k'$ ; on la note $cl_{k'}(O_{K'})$.

Si $\Gamma'$ est un groupe fini, on désigne par $R_m(k', \Gamma')$ ($m$ pour modéré) l'ensemble des classes de Steinitz des extensions galoisiennes modérées de $k'$, dont le groupe de Galois est isomorphe à $\Gamma'$.

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

Nous verrons dans la section 3 au cours de la démonstration du théorème 1.1, sous-forme de deux remarques, qu'on a la proposition suivante comme application du théorème 1.1 :

**Proposition 1.2.** *Sous les hypothèses du théorème 1.1 et les notations précédentes, si* $\Gamma$ *est d'exposant* $p$*, alors*

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

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

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

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

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

Nous terminons cette section par une réponse aux critiques constructives du referee.

Le présent article est une suite naturelle de [2] vu le lien étroit—bien connu—entre les classes de Steinitz et celles galoisiennes. Son principal intérêt est de constituer une première étape pour comprendre le problème des classes galoisiennes réalisables pour les $p$-groupes, $p$ impair. Pour démontrer le principal résultat nous avons utilisé les théories du corps de classes et de Kummer, et des résultats connus de A. Fröhlich et d'un problème de plongement ; cette méthode est une variation de celle utilisée dans d'autres papiers du second auteur, mais ici la résolution du problème de plongement en lien avec des classes galoisiennes est nettement plus difficile. En ce qui concerne les perspectives : nous pensons posséder les principaux outils pour espérer dans un futur travail déterminer $\mathcal{R}(\mathcal{M})$ pour les groupes d'ordre $p^3$ sans aucune hypothèse sur le corps de base. Sachant que $\mathcal{R}(\mathcal{M})$ est une bonne approximation de $\mathcal{R}(O_k[\Gamma])$ (voir [6,7]), nous espérons ensuite déterminer ce dernier (à ce moment nous comparerons notre résultat avec celui de L.R. McCulloh dans le cas non abélien) et généraliser les résultats pour les $p$-groupes. Cette généralisation utilisera en partie une adaptation de la méthode de I.R. Shafarevich concernant la résolution du problème inverse de la théorie de Galois pour les groupes résolubles, et le théorème de Brauer qui permet d'écrire un caractère irréductible de $\Gamma$ comme combinaison linéaire à coefficients dans $\mathbb{Z}$ de caractères induits par des caractères de sous-groupes abéliens de $\Gamma$.

## 2. Préliminaires

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

Soient $k'$ un corps de nombres quelconque et $\Gamma'$ un groupe fini. Supposons qu'aucun caractère absolument irréductible de $\Gamma'$ ne soit symplectique (notre groupe $\Gamma$ du §1 vérifie cette condition) ; en particulier $k'[\Gamma']$ satisfait la condition d'Eichler. Soit $\mathcal{M}'$ un $O_{k'}$-ordre maximal dans $k'[\Gamma']$ contenant $O_{k'}[\Gamma']$. Ci-dessous, nous rappelons brièvement la Hom-description de Fröhlich du groupe des classes $Cl(\mathcal{M}')$ et la notion de résolvante de Fröhlich–Lagrange (voir [10]).

On désigne par $R_{\Gamma'}$ le groupe des caractères virtuels de $\Gamma'$. Soient $\overline{k'}$ une clôture algébrique de $k'$, $\overline{k'}^{\times} = \overline{k'} \setminus \{0\}$, $\Omega_{k'} = Gal(\overline{k'}/k')$, $J(\overline{k'})$ le groupe des idèles de $\overline{k'}$, et $U(\overline{k'})$ le sous-groupe des idèles unités de $J(\overline{k'})$. Alors

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

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

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

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

Soit $B$ une $k'$-algèbre commutative, 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 $\Gamma'$ de caractère $\chi'$. 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 :

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

où $Det$ désigne le déterminant.

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 $\mathfrak{p}$. Soient $N'_{\mathfrak{p}} = N' \otimes_{k'} k'_{\mathfrak{p}}$ et $O_{N',\mathfrak{p}} = O_{N'} \otimes_{O_{k'}} O_{k',\mathfrak{p}}$.

Supposons $N'/k'$ modérée. On sait que $O_{N'}$ est un $O_{k'}[\Gamma']$-module localement libre de rang 1. 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 $O_{N',\mathfrak{p}}$. Soit $a$ une base (normale) du $k'[\Gamma']$-module $N'$. Nous rappelons aussi que d'après Fröhlich (voir [10]), un représentant de la classe de $\mathcal{M}' \otimes_{O_{k'}[\Gamma']} O_{N'}$ $(= \mathcal{M}' \otimes_{O_{k'}[\Gamma']} O_{N',\pi})$ dans $Cl(\mathcal{M}')$ est l'application $f$ définie par :

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

Soit $r$ le nombre des classes de conjugaison sur $k'$ des caractères absolument irréductibles de $\Gamma'$. Pour tout $i \in \{1, 2, \ldots, r\}$, notons $\chi_i$ un représentant de l'une de ces classes de conjugaison. On note $k'(\chi_i)$ l'extension de $k'$ obtenue par adjonction à $k'$ des valeurs de $\chi_i$. Comme pour tout $i$, $1 \leq i \leq r$, $\chi_i$ n'est pas symplectique, un résultat bien connu de Swan nous donne :

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

**Désormais $N/k$ désigne une extension modérément ramifiée à groupe de Galois isomorphe à $\Gamma$, où $k$ et $\Gamma$ vérifient les hypothèses du théorème 1.1 : $k \cap \mathbb{Q}(\xi) = \mathbb{Q}$ et $\Gamma$ est un groupe non abélien d'ordre $p^3$.**

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

$$Gal(N/E) = \langle\eta, \tau\rangle, \quad Gal(K/k) = \langle\tau|_K, \nu|_K\rangle \simeq H,$$
$$Gal(M/E) = \langle\eta|_M\rangle \simeq \langle\eta\rangle \simeq C,$$
$$Gal(E/k) = \langle\nu|_E\rangle \simeq C, \ \ Gal(F/k) = \langle\tau|_F\rangle \simeq \langle\tau\rangle \simeq C,$$

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

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

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

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

On a les isomorphismes de restriction :

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

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

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

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

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

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

Une démonstration similaire à celle de la proposition 4.1 dans [5, pp. 22–23] et la proposition 2.1 dans [14, p. 1824] nous donne :

**Proposition 2.1.** *Sous les hypothèses et notations ci-dessus, un représentant de la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ dans $Cl(\mathcal{M})$ est l'élément $f$ de $Hom_{\Omega_k}(R_\Gamma, J(\overline{k}))$ défini par :*

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

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

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

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

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

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

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

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

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

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

et donc

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

Soit $\mathcal{R}(\mathcal{M}(H))$ l'ensemble des classes réalisables par les anneaux d'entiers des extensions galoisiennes et modérées de $k$, dont le groupe de Galois est isomorphe à $H$. D'après [13], $\mathcal{R}(\mathcal{M}(H))$ est un sous-groupe de $Cl^\circ(\mathcal{M}(H))$ qu'on peut décrire par une correspondance de Stickelberger ; on l'identifiera souvent avec un sous-groupe de $\prod_{i=0}^{p} Cl(k(\xi))$.

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

Puisque $k/\mathbb{Q}$ (resp. $E/\mathbb{Q}$) et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes, les caractères absolument irréductibles de $C$ donnent deux classes de conjugaison sur $k$ (resp. $E$) ; pour ces dernières on choisit comme représentants le caractère trivial de $C$ et $\chi$.

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

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

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

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

Par conséquent :

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

Soit $\mathcal{R}(\mathcal{M}(C))$ (resp. $\mathcal{R}(\mathcal{M}_E(C))$) l'ensemble des classes réalisables par les anneaux d'entiers des extensions galoisiennes et modérées de $k$ (resp. $E$), dont le groupe de Galois est isomorphe à $C$. En identifiant $Cl^\circ(\mathcal{M}(C))$ (resp. $Cl^\circ(\mathcal{M}_E(C))$) et $Cl(k(\xi))$ (resp. $Cl(E(\xi))$) sous les isomorphismes précédents, le théorème 2.4 de [15] nous donne (attention : $\mathcal{R}(\mathcal{M}(C))$ est noté $\mathcal{R}(O_k[C])$ dans [15]) :

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

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

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

Soit $k'$ un corps de nombres. Si $I$ est un idéal fractionnaire de $k'$, on désigne par $cl(I)$ sa classe dans $Cl(k')$ le groupe de classes de $k'$.

**Proposition 2.2.** *Soient $c_i$, $-1 \leq i \leq p+1$, les composantes de $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $Cl(k) \times (\prod_{i=0}^{p} Cl(k(\xi))) \times Cl(k(\xi)(\simeq Cl(\mathcal{M}))$. Sous les notations précédentes on a :*
*(i) $c_{-1}$ est la classe triviale dans $Cl(k)$.*

*(ii)* $(c_0, c_1, \ldots, c_p)$ *est la classe de* $[\mathcal{M}(H) \otimes_{O_k[H]} O_K]$ *dans* $\prod_{i=0}^{p} Cl(k(\xi))$ *et pour tout* $i$, $0 \leq i \leq p$, $c_i = [\mathcal{M}(C) \otimes_{O_k[C]} O_{K_i}]$ *dans* $\mathcal{S}Cl(k(\xi))$.
*(iii)* $c_{p+1} = \phi_{k(\xi)/k}(cl_k(O_E))N_{E(\xi)/k(\xi)}([\mathcal{M}_E(C) \otimes_{O_E[C]} O_M])$ *dans* $Cl(k(\xi))$.

**Démonstration.** $(i)$ C'est évident.

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

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

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

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

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

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

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

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

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

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

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

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

$(iii)$ La preuve consiste en la détermination de la classe du contenu de l'idèle suivant, lequel est défini dans la proposition 2.1 :

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

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

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

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

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

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

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

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

Soit $I$ l'idéal fractionnaire de $k$ qui est le contenu de l'idèle $(e((k_1)_\mathfrak{p}/k_\mathfrak{p})/e(k_1/k))_\mathfrak{p}$. Un raisonnement similaire à celui de la fin de la preuve de la proposition 4.2$(iii)$ dans [5, p. 24] nous donne : $cl(I) = cl_k(O_E)$. Ceci permet d'achever la démonstration de $(iii)$. □

Soient $k'$ un corps de nombres et $I$ un idéal fractionnaire de $k'$. Il est clair qu'on peut écrire de façon unique

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

où $J_0$ est un idéal fractionnaire de $k'$, et les $J_i$, $1 \leq i \leq (p-1)$, sont des idéaux entiers de $O_{k'}$, sans facteur carré et premiers entre eux deux à deux. Dans la suite de l'article, l'expression « décomposition de façon unique » signifie cette écriture.

**Proposition 2.3.** *Sous les hypothèses et notations de la proposition 2.2, avec le rappel* $c_0 = [\mathcal{M}(C) \otimes_{O_k[C]} O_E]$ *et* $c_p = [\mathcal{M}(C) \otimes_{O_k[C]} O_F]$, *on a :*

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

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

**Démonstration.** Dans la démonstration de la proposition 2.2 on a défini $\overline{\overline{\chi_i}}$ pour tout $i$, $0 \leq i \leq p$ $(\overline{\chi_i} = Inf^H_{Gal(K_i/k)}(\overline{\overline{\chi_i}}))$. Pour simplifier les notations, posons

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

de sorte que

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

Comme $c_0 = [\mathcal{M}(C) \otimes_{O_k[C]} O_E]$, et en raisonnant comme dans le début de la partie (1) de la preuve du théorème 1.1 dans [5, p. 25] (on utilise le caractère de la représentation régulière de $C$) on obtient :

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

Nous adaptons maintenant la démonstration de [15, Lemmes 3.1 et 3.2] à notre situation tout en précisant quelques détails pour la convenance du lecteur.

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

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

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

Puisque $Gal(E/k)$, $Gal(F/k)$ et $Gal(K_i/k)$ sont isomorphes à $C$ et les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes, le théorème 2.2 (1) de [15] nous donne les décompositions de façon unique suivantes :

$$\begin{aligned}
\langle a_E, \varphi_0 \rangle_{E/k}^p O_{k(\xi)} &= (I(\varphi_0))^p \theta J(\varphi_0), \\
\langle a_F, \varphi_p \rangle_{F/k}^p O_{k(\xi)} &= (I(\varphi_p))^p \theta J(\varphi_p), \\
\langle a_{K_i}, \varphi_i \rangle_{K_i/k}^p O_{k(\xi)} &= (I(\varphi_i))^p \theta J(\varphi_i), \quad \text{pour tout } i, 1 \leq i \leq p-1.
\end{aligned}$$

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

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

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

Par conséquent

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

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

Soient

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

et $\theta_1$ l'élément de Stickelberger (voir Proposition 2.7)

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

On a

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

On en déduit la décomposition de façon unique :

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

Comme pour tout $i$, $0 \leq i \leq p$, $\varphi_i = \chi \circ \pi_i$, le théorème 2.3 (1) de [15] nous donne :

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

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

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

Supposons maintenant $E/k$ et $F/k$ arithmétiquement disjointes. D'après le théorème 2.2 (2) de [15] (ou par le rappel sur le discriminant d'une extension de Kummer de degré $p$ fait à la fin du présent pargraphe), $J_0 = O_{k(\xi)}$. Donc $c_i = c_0 s_i(c_p)$. □

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

**Proposition 2.4.** *L'extension $E'/k$ est galoisienne abélienne si, et seulement si, il existe $a' \in k(\xi)^\times$ tel que $L = k(\xi)((\theta a')^{1/p})$.*

**Démonstration.** La proposition découle de [2, Proposition 2.3]. □

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

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

**Proposition 2.5.** *Supposons $E'/k$ abélienne et posons $\alpha' = (1/p)\,Tr_{E'/E''}(\alpha)$. Alors $\langle \alpha', \chi\rangle_{E''/k} = \alpha$.*

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

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

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

Nous finissons ce paragraphe par rappeler des résultats bien connus qui seront utiles pour la démonstration de notre théorème 1.1.

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

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

On choisit la notation exponentielle pour cette action :

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

On pose

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

La proposition suivante (voir [8, Théorèmes 4 et 6, et la remarque suivant Théorème 6], ou [2, Théorème 2.5]) donne un critère de plongement de l'extension $E'/k(\xi)$ dans une extension $N'/k(\xi)$ galoisienne, non abélienne et de degré $p^3$.

**Proposition 2.6.** *Sous les notations précédentes, on a :*
*(1) Pour que $E'/k(\xi)$ soit plongeable dans une extension galoisienne $N'/k(\xi)$ à groupe de Galois $\Gamma$ d'exposant $p$, il faut et il suffit qu'il existe $e \in (E')^\times$ et $\kappa \in k(\xi)^\times$ tels que les classes de $b = e^{-\mathfrak{N}}$ et $c = \kappa e^{\hat{\theta}}$ dans $(E')^\times/(E')^{\times p}$ soient non triviales et engendrent deux sous-groupes distincts de $(E')^\times/(E')^{\times p}$.*
*(2) Pour que $E'/k(\xi)$ soit plongeable dans une extension galoisienne $N'/k(\xi)$ à groupe de Galois $\Gamma$ d'exposant $p^2$, il faut et il suffit qu'il existe $e \in (E')^\times$ et $\kappa \in k(\xi)^\times$ tels que les classes de $b = \xi e^{-\mathfrak{N}}$ et $c = \kappa \alpha e^{\hat{\theta}}$ dans $(E')^\times/(E')^{\times p}$ soient non triviales et engendrent deux sous-groupes distincts de $(E')^\times/(E')^{\times p}$.*

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

**Remarque.** (Voir [8, Théorème 6].) Sous les notations de la proposition précédente, supposons que le plongement soit possible. Soit $Gal(N'/k(\xi)) = \langle \eta,\ \tau,\ \nu \mid \eta^p = \tau^p = 1,\ \nu^p = \eta^q,\ \eta\tau = \tau\eta,\ \eta\nu = \nu\eta,\ \tau\nu\tau^{-1}\nu^{-1} = \eta \rangle$. Alors, en remplaçant éventuellement $e$ par $\xi^u e$ pour un certain entier $u$, on peut supposer que l'action de $Gal(N'/k(\xi))$ sur $N'$ est déterminée par :

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

**Proposition 2.7.** *Soit $\mathcal{S}'$ l'idéal de $\mathbb{Z}[S]$ engendré par les éléments de la forme $c - s_{\underline{c}}$, où $c \in \mathbb{Z}$ est premier avec $p$, $\underline{c} \equiv c \ mod\ p$ et $1 \leq \underline{c} \leq p-1$. Alors $\mathcal{S} = \frac{1}{p}\theta\mathcal{S}'$.*

**Démonstration.** Voir [21, Lemme 6.9, p. 93]. □

Soit $K'/k'$ une extension finie de corps de nombres. On désigne par $\Delta(K'/k')$ son discriminant et rappelons que $cl_{k'}(O_{K'})$ est sa classe de Steinitz. Un théorème d'Artin (voir [1]) nous dit que

$$cl_{k'}(O_{K'}) = cl\big((\Delta(K'/k')/d)^{1/2}\big),$$

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

Enfin, soient $k'$ un corps de nombres contenant $\xi$ et $k'(\alpha^{1/p})/k'$ une extension cyclique (de Kummer) de degré $p$.

Ecrivons de façon unique

$$\alpha O_{k'} = J_0^p \prod_{i=1}^{p-1} J_i^i.$$

D'après la théorie de Kummer (voir [12, §39])

$$\Delta(k'(\alpha^{1/p})/k') = \big(J \prod_{i=1}^{p-1} J_i\big)^{p-1},$$

où $J$ est un idéal entier de $O_{k'}$ dont les diviseurs premiers divisent $pO_{k'}$.

On rappelle que $mod^*$ est la notation usuelle de la congruence dans la théorie du corps de classes. L'extension $k'(\alpha^{1/p})/k'$ est modérément ramifiée si, et seulement si, il existe $b \in O_{k'}$ tel que

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

cette condition est équivalente à $J = O_{k'}$ et $\prod_{i=1}^{p-1} J_i$ est premier à $pO_{k'}$.

## 3. Démonstration des principaux résultats

Cette section est consacrée à la démonstration du théorème 1.1 ; dans cette dernière se trouve celle de la proposition 1.2.

**Démonstration du théorème 1.1.** Nous distinguons deux cas, selon l'exposant de $\Gamma$. Il est clair que, par sa définition, $A_p$ (resp. $A_{p^2}$) est un sous-groupe de $Cl^\circ(\mathcal{M})$.

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

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

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

D'après [15, Théorème 2.4] (Rappel : attention : $\mathcal{R}(\mathcal{M}(C))$ est noté $\mathcal{R}(O_k[C])$ dans [15]), $c_0$ est réalisable par une extension galoisienne modérée de degré $p$ ; nous reprenons, d'une façon légèrement différente, la seconde partie de la preuve de ce théorème [15, (2), p. 195] pour ajouter des précisions et construire une telle extension de façon convenable pour notre démonstration.

D'après la proposition 2.7, il existe un entier $j$, des idéaux fractionnaires $I_i$ de $k(\xi)$, $1 \leq i \leq j$, qu'on peut choisir premiers avec $pO_{k(\xi)}$ par le théorème de densité de Chebotarev, et des éléments $\mathfrak{s}'_i$, $1 \leq i \leq j$, de $\mathcal{S}'$ tels que :

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

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

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

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

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

Posons

$$a = \theta a'.$$

Alors

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

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

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

$$\alpha^p = a.$$

Posons

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

Alors $E_1'/k(\xi)$ est une extension cyclique (de Kummer) de degré $p$. Elle est modérée, car $\theta a' \equiv 1 \ mod^* \ (1-\xi)^{p^2} O_{k(\xi)}$ ; donc $E_1'/k$ est modérée car $k(\xi)/k$ l'est. L'extension $E_1'/k$ est galoisienne abélienne par la proposition 2.4, car $a = \theta a'$ ; elle admet une (unique) sous-extension $E_1/k$ galoisienne, de degré $p$ ; c'est clair que $E_1/k$ est modérée et $E_1' = E_1(\xi)$.

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

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

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

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

Posons $\alpha' = (1/p)\, Tr_{E_1(\xi)/E_1}(\alpha)$. Alors $\langle \alpha', \varphi_0 \rangle_{E_1/k} = \alpha$ par la proposition 2.5. Donc

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

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

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

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

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

D'après [15, Théorème 2.3 (1)]

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

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

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

En effet : Par la rappel sur la théorie de Kummer (voir fin §2)

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

Les extensions $E_1/k$ et $k(\xi)/k$ étant arithmétiquement disjointes et $E_1' = E_1k(\xi)$, on a

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

Des deux égalités précédentes on déduit

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

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

**Etape 2. Considérons maintenant $c_p$.** *Dans cette étape on construit une extension modérée $F_1/k$ de groupe de Galois $C$, arithmétiquement disjointe de $E_1/k$, avec $[\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1}] = c_p$ et $F_1(\xi) = k(\xi)(b^{1/p})$, où $b = e^{-\mathfrak{N}}$ pour un certain $e \in E_1(\xi)$ (voir la définition de $\mathfrak{N}$ ci-dessous ; la forme de $b$ est motivée par l'utilisation des conditions de plongement de la proposition 2.6 dans l'étape 3).*

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

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

par [21, Théorème 10.1, p. 400]. On en déduit que

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

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

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

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

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

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

$$I'^{\,p} = \theta J', \quad c'_p = cl(I').$$

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

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

Posons

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

Alors

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

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

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

et soit

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

Posons

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

On a

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

Soit

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

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

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

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

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

$$\alpha'^{\,p} = b.$$

Posons

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

On a

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

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

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

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

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

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

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

*Dans cette étape on construit un élément $c \in E_1(\xi)$ de sorte que les classes de $b$ et $c$ n'engendrent pas le même sous-groupe de $E_1(\xi)^\times/E_1(\xi)^{\times p}$, ce qui permet, grâce à la proposition 2.6, de plonger $E_1(\xi)/k(\xi)$ dans une extension $N_1'/k(\xi)$ ($N_1' = E_1(\xi)(b^{1/p}, c^{1/p})$) à groupe de Galois isomorphe à $\Gamma$. Puis on prouve que $N_1'$ contient une extension $N_1/k$ galoisienne modérée de groupe de Galois $\Gamma$, avec $E_1 \subset N_1$ et $F_1 \subset N_1$.*

Définissons $d \in \mathcal{S}Cl(k(\xi))$ par

$$x = dc_p^{p-1},$$

où $c_p$ apparait dans $Y$ ci-dessus. (Ce choix de décomposition de $x$ est motivée par le calcul de $x_{p+1}$ dans la fin de l'étape 4 ; $x_{p+1}$ est défini au début de l'étape 4.)

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

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

Soit

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

Posons

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

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

On a

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

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

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

On a

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

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

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

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

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

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

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

D'après la proposition 2.6, $E_1(\xi)/k(\xi)$ est plongeable dans une extension $N_1'/k(\xi)$ à groupe de Galois isomorphe à $\Gamma$, et on peut prendre

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

On a

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

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

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

D'après la remarque suivant la proposition 2.6, on peut supposer que l'action de $Gal(N_1'/k(\xi))$ sur $N_1'$ est déterminée par :

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

Considérons l'extension

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

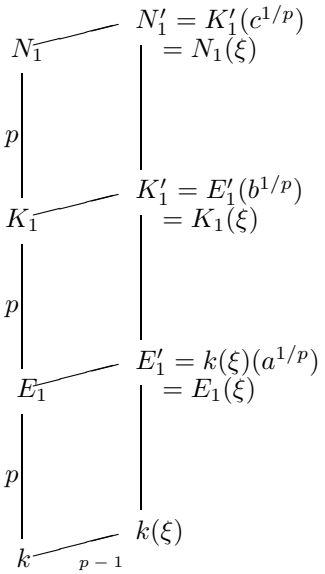
Puisque $b = \theta(\beta'^{\mathfrak{N}})$, la proposition 2.4 nous dit que $K'_1/E_1$ est abélienne, et comme elle est cyclique de degré $p(p-1)$ elle contient une unique sous-extension $K_1/E_1$ de degré $p$ ; c'est clair que $K'_1 = K_1(\xi)$. Mais la composée $E_1F_1$ est contenue dans $K'_1$. Il est immédiat que le degré de $E_1F_1/E_1$ est $p$, par conséquent $E_1F_1 = K_1$.

On a $N'_1 = K_1(\xi)(c^{1/p})/K_1(\xi)$ $(= K_1(\xi)(c^{-1/p})/K_1(\xi))$. Puisque

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

la proposition 2.4 nous dit que $N'_1/K_1$ est abélienne, et comme ci-dessus elle contient une unique sous-extension $N_1/K_1$ de degré $p$ ; c'est clair que $N'_1 = N_1(\xi)$

Nous résumons la situation dans le diagramme suivant :




Maintenant on remplace les diagrammes des pages 185 et 186 de [2] (qui sont les mêmes, puisque l'exposant $v$ de $\Gamma$ est $p$) par le nôtre ci-dessus. Sous nos notations, d'une façon très similaire à ce qu'est écrit dans [2, pp. 185–187] (on s'arrête à la ligne avant Etape 4), on montre que $N_1/k$ est galoisienne modérée ayant un groupe de Galois isomorphe à $\Gamma = Gal(N'_1/k(\xi)$ (isomorphisme de restriction). Ceci termine l'étape 3.

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

Considérons l'extension

$$M'_1 = E_1(\xi)(c^{-1/p})/E_1(\xi) \ (= E_1(\xi)(c^{1/p})/E_1(\xi)).$$

Puisque

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

la proposition 2.4 nous dit que $M_1'/E_1$ est abélienne, et comme ci-dessus elle contient une unique sous-extension $M_1/E_1$ de degré $p$ ; c'est clair que $M_1' = M_1(\xi)$ et $N_1 = M_1 K_1$.

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

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

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

Les extensions $E_1/k$ et $F_1/k$ étant arithmétiquement disjointes, puisque $[\mathcal{M}(C) \otimes_{O_k[C]} O_{E_1}] = c_0$ et $[\mathcal{M}(C) \otimes_{O_k[C]} O_{F_1}] = c_p$, d'après les propositions 2.2 et 2.3 on a :

$$x_0 = c_0, \quad x_p = c_p, \quad x_i = c_0 s_i(c_p), \quad \text{pour tout} \quad i, 1 \le i \le (p-1),$$
$$x_{p+1} = \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0)) N_{E_1(\xi)/k(\xi)}([\mathcal{M}_{E_1}(C) \otimes_{O_{E_1}[C]} O_{M_1}]).$$

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

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

Posons

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

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

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

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

On a donc :

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

Maintenant

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

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

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

D'où

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

Par la théorie de Kummer (voir le rappel dans §2)

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

Puisque $F_1(\xi)/k(\xi)$ est galoisienne de degré impair, le théorème d'Artin (voir le rappel dans §2) nous donne

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

Donc

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

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

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

Mais

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

par conséquent

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

D'où

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

Puisque $x = dc_p^{p-1}$, on conclut que

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

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

**Remarque.** L'objet de cette remarque est de montrer la proposition 1.2 lorsque $\Gamma$ est d'exposant $p$.

Ecrivons $X = [\mathcal{M} \otimes_{O_k[\Gamma]} O_{N_1}] = (x_0, x_1, \ldots, x_p, x_{p+1})$. En raisonnant comme dans le début de la partie (1) de la preuve du théorème 1.1 dans [5, p. 25] (on utilise le caractère de la représentation régulière de $C$) on obtient :

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

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

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

Par suite

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

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

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

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

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

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

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

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

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

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

d'en donner suffisamment afin de rendre notre démonstration aussi compréhensible que possible.

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

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

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

On pose

$$b' = \xi b.$$

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

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

et

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

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

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

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

$$\alpha'^{p} = b',$$

et on pose

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

Comme $b' = \theta(\xi^{-1}\beta'^{\mathfrak{N}})$, $F_1'/k$ est galoisienne abélienne par la proposition 2.4, elle admet une (unique) sous-extension $F_1/k$ galoisienne de degré $p$ et c'est clair que $F_1' = F_1(\xi)$.

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

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

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

Comme dans la partie (1), on obtient

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

**Considérons maintenant $x$.** Soit $d \in \mathcal{S}Cl(k(\xi))$ satisfaisant

$$x = dc_p^{p-1}.$$

On garde tout ce qu'il y a dans la partie (1), à partir de cette considération et on s'arrête avant le paragraphe débutant par [D'après la proposition 2.6...] ; mais on remplace $b$ par $b'$ et on ajoute (ajout facile à faire) la condition suivante dans le choix de $\mathfrak{r}$ : $\mathcal{N}(\mathfrak{r}O_{E_1(\xi)})$ est premier avec $\mathcal{N}(\mathfrak{p}O_{E_1(\xi)})$ (rappelons que $\mathcal{N} = \sum_{i=1}^{p-1} s_i$).

**Nous allons maintenant modifier l'élément $c$ de la partie (1).**

Rappelons qu'on a :

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

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

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

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

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

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

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

On a

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

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

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

Posons

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

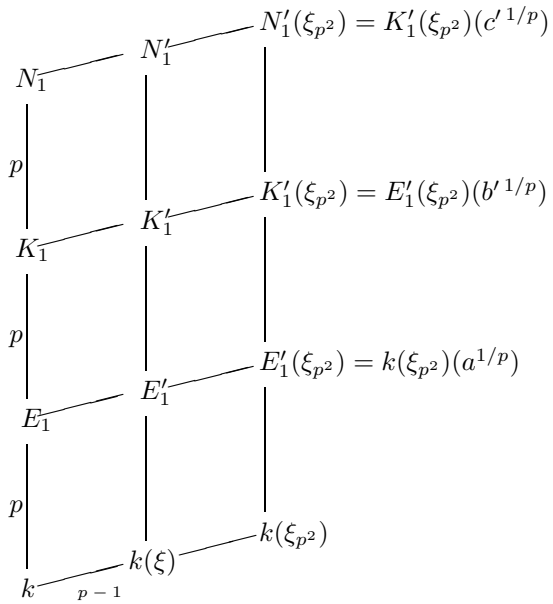
Comme $c = \theta(\kappa'{\beta'}^{\hat{\theta}})^{-1}$, on a

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

On vérifie facilement que $b'$ et $c'$ vérifient les conditions de l'assertion (2) de la proposition 2.6. Donc $E_1(\xi)/k(\xi)$ est plongeable dans une extension $N_1'/k(\xi)$ à groupe de Galois isomorphe à $\Gamma$, et on peut prendre

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

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




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

Considérons

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

Puisque ${c'}^{-1} = \theta(\kappa''\alpha\kappa'{\beta'}^{\hat{\theta}})$, la proposition 2.4 nous dit que $M_1'/E_1$ est abélienne, de plus elle contient une unique sous-extension $M_1/E_1$ de degré $p$ modérée ; c'est clair que $M_1' = M_1(\xi)$ et $N_1 = M_1K_1$.

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

On a

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

Par suite

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

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

$$\begin{aligned} {c'}^{-1}O_{E_1(\xi)} = &\Big({I''}^{-1}O_{E_1(\xi)}\hat{\theta}{I'}^{-1}\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{(ij-\underline{ij})/p}\Big)^p \\ &\times \theta\mathfrak{r}O_{E_1(\xi)}\Big(\prod_{i=1}^{p-1}\prod_{j=1}^{p-1}(s_i^{-1}\rho^j)(\mathfrak{q})^{\underline{ij}}\Big)\theta\mathfrak{p}_1 O_{E_1(\xi)}\theta^2\hat{\mathfrak{p}}. \end{aligned}$$

On a

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

en effet : écrivons $\theta = \sum_{i=1}^{p-1} i s_{i^*}$, où $ii^* \equiv 1 \ mod\ p$ ; d'après la proposition 2.7, $s_{i^*}\theta \equiv i^*\theta \ mod\ p\mathcal{S}$ et donc

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

Par suite :

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

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

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

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

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

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

Posons

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

Comme $E_1/k$ et $F_1/k$ sont arithmétiquement disjointes, $[\mathcal{M}(C)\otimes_{O_k[C]}O_{E_1}] = c_0$ et $[\mathcal{M}(C)\otimes_{O_k[C]}O_{F_1}] = c_p$, d'après les propositions 2.2 et 2.3 on a :

$$x_0 = c_0,\quad x_p = c_p,\quad x_i = c_0s_i(c_p),\quad \text{pour tout}\quad i, 1\le i\le (p-1),$$
$$x_{p+1} = \phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0))N_{E_1(\xi)/k(\xi)}([\mathcal{M}_{E_1}(C)\otimes_{O_{E_1}[C]}O_{M_1}]).$$

Posons

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

Alors

$$x_{p+1} = Zx^p\phi_{k(\xi)/k}(N_{k(\xi)/k}(c_0c_p))$$

Dans ce qui suit nous calculons $Z$.

On a

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

De

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

on déduit

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

Par conséquent

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

D'où

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

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

**Remarque.** Dans cette remarque on montre la proposition 1.2 lorsque $\Gamma$ est d'exposant $p^2$.

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

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

D'où

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

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

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

**Déclaration de conflits d'intérêts**

Rien à déclarer.

**Remerciements**

Les auteurs remercient le referee pour sa lecture très attentive et ses critiques constructives, lesquelles nous poussent à élargir nos horizons tout en gardant intacte la passion de faire des mathématiques.

**Références**

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

[2] C. Bruche, Classes de Steinitz d'extensions non abéliennes de degré $p^3$, Acta Arith. 137 (2) (2009) 177–191.
[3] C. Bruche, B. Sodaïgui, On realizable Galois module classes and Steinitz classes of nonabelian extensions, J. Number Theory 128 (2008) 954–978.
[4] N.P. Byott, B. Sodaïgui, Realizable Galois module classes over the group ring for non abelian extensions, Ann. Inst. Fourier (Grenoble) 63 (1) (2013) 303–371.
[5] N.P. Byott, C. Greither, B. Sodaïgui, Classes réalisables d'extensions non abéliennes, J. Reine Angew. Math. 601 (2006) 1–27.
[6] N.P. Byott, B. Sodaïgui, Realizable Galois module classes for tetrahedral extensions, Compos. Math. 141 (2005) 573–582.
[7] N.P. Byott, B. Sodaïgui, Galois module structure for dihedral extensions of degree 8: realizable classes over the group ring, J. Number Theory 112 (2005) 1–19.
[8] J.E. Carter, Characterisations of Galois extensions of prime cubed degree, Bull. Aust. Math. Soc. 55 (1997) 99–112.
[9] C.W. Curtis, I. Reiner, Methods of Representation Theory with Applications to Finite Groups and Orders, vol. II, Wiley–Interscience, New York, 1987.
[10] A. Fröhlich, Galois Module Structure of Algebraic Integers, Springer-Verlag, Berlin, 1983.
[11] J. Gordon, L. Martin, Representations and Characters of Groups, second ed., Cambridge University Press, New York, 2001.
[12] E. Hecke, Lectures on the Theory of Algebraic Numbers, Grad. Texts in Math., vol. 77, Springer-Verlag, New York, 1981.
[13] L.R. McCulloh, Galois module structure of abelian extensions, J. Reine Angew. Math. 375/376 (1987) 259–306.
[14] F. Sbeity, B. Sodaïgui, Classes réalisables d'extensions métacycliques de degré $lm$, J. Number Theory 130 (2010) 1818–1834.
[15] B. Sodaïgui, Structure galoisienne relative des anneaux d'entiers, J. Number Theory 28 (2) (1988) 189–204.
[16] B. Sodaïgui, "Galois module structure" des extensions quaternioniennes de degré 8, J. Algebra 213 (1999) 549–556.
[17] B. Sodaïgui, Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8, J. Algebra 223 (2000) 367–378.
[18] B. Sodaïgui, Realizable classes of quaternion extensions of degree 4l, J. Number Theory 80 (2000) 304–315.
[19] B. Sodaïgui, Relative Galois module structure of octahedral extensions, J. Algebra 312 (2007) 590–601.
[20] M.J. Taylor, On Fröhlich's conjecture for rings of integers of tame extensions, Invent. Math. 63 (1981) 41–79.
[21] L.C. Washington, Introduction to Cyclotomic Fields, second ed., Springer-Verlag, Berlin, 1996.