ACTA ARITHMETICA
137.2 (2009)

Classes de Steinitz d'extensions non abéliennes de degré p^3

par

Clément Bruche (Valenciennes)

1. Introduction. Dans cet article, si K est un corps de nombres, O_K désigne son anneau d'entiers et $\mathrm{Cl}(K)$ son groupe des classes.

Soit k un corps de nombres. 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 $\mathrm{Cl}(k)$ est appelée la *classe de Steinitz de* M, et on la note $\mathrm{cl}_k(M)$ (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 complètement déterminée par son rang et sa classe de Steinitz. Ceci s'applique en particulier à $M = O_K$, où K/k est une extension finie de corps de nombres de degré s ; on dira alors que $\mathrm{cl}_k(O_K)$ est la *classe de Steinitz de* K/k.

Soient Γ un groupe fini et $\mathrm{Cl}(O_k[\Gamma])$ le groupe des classes de $O_k[\Gamma]$ (i.e. le groupe des classes des $O_k[\Gamma]$-modules localement libres ; voir [F2, Chap. I, §2, p. 17]). On désigne par $\mathcal{R}(O_k[\Gamma])$ (resp. $R_m(k,\Gamma)$; m pour modéré) l'ensemble des classes c de $\mathrm{Cl}(O_k[\Gamma])$ (resp. $\mathrm{Cl}(k)$) telles qu'il existe une extension N/k modérément ramifiée, à groupe de Galois isomorphe à Γ, avec $[O_N] = c$ (resp. $\mathrm{cl}_k(O_N) = c$), où $[O_N]$ est la classe de O_N dans $\mathrm{Cl}(O_k[\Gamma])$.

Les travaux de McCulloh (voir [M]) et les résultats de [BS1] et [BS2] vont dans le sens de la conjecture suivante :

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

Notons 1 le sous-groupe trivial de Γ. L'anneau de groupe $O_k[1]$ étant identifié à O_k, d'après [F2, Chap. II, §3, pp. 62–65], l'injection $1 \to \Gamma$ induit le morphisme de restriction $\mathrm{res}_1^\Gamma : \mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(k)$ qui, à la classe d'un $O_k[\Gamma]$-module localement libre M, associe sa classe en tant que O_k-module dans $\mathrm{Cl}(k)$; or cette dernière n'est autre chose que $\mathrm{cl}_k(M)$, la classe de Steinitz de M. On en déduit que si N/k est une extension ga-

2000 *Mathematics Subject Classification*: Primary 11R33.
Key words and phrases: rings of integers, relative module structure, Steinitz classes, realizable classes.

DOI: 10.4064/aa137-2-6

loisienne modérément ramifiée, à groupe de Galois isomorphe à Γ, alors $\mathrm{res}_1^\Gamma([O_N]) = \mathrm{cl}_k(O_N)$. Il en résulte que $\mathrm{res}_1^\Gamma(\mathcal{R}(O_k[\Gamma])) = R_m(k,\Gamma)$. Il s'ensuit que la conjecture 1 implique la conjecture suivante :

CONJECTURE 2. *L'ensemble $R_m(k,\Gamma)$ est un sous-groupe de* $\mathrm{Cl}(k)$.

Il vient de [M] que ces conjectures sont vraies lorsque Γ est abélien ; on peut voir [L1, L2] pour une description plus explicite de $R_m(k,\Gamma)$ dans le cas où Γ est un groupe cyclique d'ordre une puissance d'un nombre premier impair, et [E] pour tout groupe abélien d'ordre impair. Pour des travaux récents dans la direction de l'étude de ces conjectures, on pourra consulter [BGS, BrS, BS1, BS2, C3, CS, GS1, GS2, So1–So4, Sov].

Dans cet article, on s'intéresse à l'étude de la conjecture 2 dans la situation où Γ est un groupe non abélien d'ordre p^3, où p désigne un premier impair. Dans la suite, si $n \in \mathbb{N}^*$, on désigne par ζ_n une racine primitive $n^{\text{ième}}$ de l'unité. Le principal résultat de ce papier est le théorème suivant.

THÉORÈME 1.1. *Soient k un corps de nombres et Γ un groupe non abélien d'ordre $p^3 = uv$, où p est un nombre premier impair et où v désigne l'exposant de Γ. On suppose que l'extension $k(\zeta_v)/k(\zeta_p)$ est non ramifiée. Alors*

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

On en déduit immédiatement le corollaire suivant :

COROLLAIRE 1.2. *Sous les notations du théorème précédent, on a* :

(i) *Si l'exposant de Γ est p, alors, pour tout corps de nombres k,*

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

(ii) *Si $\zeta_v \in k$, alors*

$$R_m(k,\Gamma) = \mathrm{Cl}(k)^{u(p-1)/2}.$$

REMARQUE. Le théorème 1.1 généralise le résultat principal de [C2], dont l'énoncé est l'assertion (ii) du corollaire précédent.

2. Préliminaires. Dans cette section, on fixe des notations et on donne quelques résultats qui seront utiles à la démonstration du théorème 1.1.

Dorénavant, p désigne un nombre premier impair. 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 O_k, et les J_i, $1 \le i \le p-1$, sont des idéaux entiers de O_k sans facteur carré, et premiers entre eux deux à deux. L'idéal J_0 est appelé la *p-partie* de I, et l'idéal $\prod_{i=1}^{p-1} J_i$, que l'on notera

$\mathcal{F}(I)$, le *p-conducteur* de I, ou tout simplement le *conducteur* de I si aucune confusion n'est possible.

Le théorème suivant découle de la théorie de Kummer (voir [H, §39], ou [Co, §10.2]). On rappelle que "mod*" est la notation usuelle de la congruence dans la théorie du corps de classes, et on note $\Delta(K/k)$ le discriminant d'une extension de corps de nombres K/k.

THÉORÈME 2.1. *Soient $m \in k^\times$ et $K = k(\sqrt[p]{m})$ une extension cyclique de k de degré p. On suppose $\zeta_p \in k$. Sous les notations précédentes on a :*

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

(ii) *Soit $\mathfrak{p}$ un idéal premier de O_k divisant $(1-\zeta_p)O_k$. Soit ensuite $w = v_\mathfrak{p}((1-\zeta_p)O_k)$. Supposons que $\mathfrak{p}$ ne divise pas mO_k. Alors $\mathfrak{p}$ est ramifié dans K/k si et seulement si la congruence $x^p \equiv m \bmod^* \mathfrak{p}^{wp}$ n'a pas de solution dans $k^\times$.*

Rappelons que deux extensions K_1/k et K_2/k sont dites *arithmétiquement disjointes* si elles sont linéairement disjointes et si leurs discriminants $\Delta(K_1/k)$ et $\Delta(K_2/k)$ sont premiers entre eux ; dans ce cas on vérifie facilement que $\Delta(K_1K_2/K_2) = \Delta(K_1/k)O_{K_2}$.

Fixons les notations suivantes pour la suite de cet article. On note l le degré de l'extension $k(\zeta_p)/k$ (rappelons que l divise $p-1$), et on choisit un générateur σ du groupe $H = \mathrm{Gal}(k(\zeta_p)/k)$. Soit s l'entier naturel vérifiant $\sigma(\zeta_p) = \zeta_p^s$ et $1 \le s \le p-1$.

Le groupe quotient $k(\zeta_p)^\times / k(\zeta_p)^{\times p}$ (resp. l'ensemble des idéaux fractionnaires de $k(\zeta_p)$) est d'une façon naturelle un $\mathbb{F}_p[H]$-module (resp. $\mathbb{Z}[H]$-module).

DÉFINITION 2.2. On définit $A \in \mathbb{F}_p[H]$ par

$$A = \sum_{i=0}^{l-1} (\bar{s})^{-i} \sigma^i,$$

où $\bar{s}$ est la classe de s dans $\mathbb{Z}/p\mathbb{Z}$. Si $x \in k(\zeta_p)^\times$ et si I est un idéal fractionnaire de $k(\zeta_p)$, on pose $x^A = \prod_{i=0}^{l-1} \sigma^i(x)^{s^{-i}}$ et $I^A = \prod_{i=0}^{l-1} \sigma^i(I)^{s^{-i}}$, où s^{-i} est, par abus de notation, l'entier compris entre 1 et $p-1$ tel que sa classe dans $\mathbb{Z}/p\mathbb{Z}$ soit $(\bar{s})^{-i}$.

PROPOSITION 2.3 ([L1, Corollary 1.3, p. 89]). *Soit $E/k(\zeta_p)$ une extension cyclique de degré p. L'extension E/k est abélienne si et seulement si il existe $m \in k(\zeta_p)^\times$ tel que $E = k(\zeta_p)((m^A)^{1/p})$.*

REMARQUE. Avec les hypothèses et notations de la proposition précédente, supposons E/k abélienne. Comme son degré est pl, elle admet une sous-extension L/k de degré p. Puisque p est premier à l, les extensions L/k et $k(\zeta_p)/k$ sont linéairement disjointes. On en déduit $E = Lk(\zeta_p) = L(\zeta_p)$ et $\mathrm{Gal}(E/k) \simeq \mathrm{Gal}(L/k) \times \mathrm{Gal}(k(\zeta_p)/k)$ ($\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \simeq \mathbb{Z}/pl\mathbb{Z}$). Donc E/k est cyclique et L est unique.

PROPOSITION 2.4. *Soit $\mathfrak{p}$ un idéal premier de O_k ne divisant pas pO_k. Si $\mathfrak{p}$ est ramifié dans une extension K/k cyclique de degré p, alors il vérifie les conditions équivalentes suivantes* :

(i) $\mathfrak{p}$ *est totalement décomposé dans* $k(\zeta_p)/k$,
(ii) $N_{k/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \bmod p$,
(iii) $\mathrm{cl}(\mathfrak{p}) \in N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))$.

Preuve. D'après [L2, Lemma, p. 298], si K/k est (modérément) ramifiée en $\mathfrak{p}$, alors $N_{k/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \bmod p$.

(i)⇔(ii). Voir [L1, Proposition 2.4, p. 89] (surtout la dernière phrase de la proposition).

(i)⇔(iii). C'est une conséquence du résultat plus général suivant, qui découle du théorème de densité de Chebotarev (voir [N, Chap. VII, Theorem (13.4), p. 545]) : pour toute extension de corps de nombres K/k, l'ensemble $N_{K/k}(\mathrm{Cl}(K))$ est le sous-groupe de $\mathrm{Cl}(k)$ engendré par les classes contenant des idéaux premiers de O_k totalement décomposés dans K/k. ∎

La structure des groupes non-abéliens d'ordre p^3 est bien connue (voir par exemple [C1]). On peut les définir par la présentation suivante :

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

avec $q = 0$ ou $q = 1$. Le groupe Γ est donc, à isomorphisme près, l'un des deux groupes suivants :

(i) Si $q = 0$, alors $\Gamma \simeq (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$; dans ce cas l'exposant de Γ est égal à p.
(ii) Si $q \neq 0$, alors $\Gamma \simeq (\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$; dans ce cas l'exposant de Γ est égal à p^2.

Soit $a \in k(\zeta_p)$ tel que a n'est pas une puissance $p^{\text{ième}}$ dans $k(\zeta_p)$. On considère l'extension de Kummer $E = k(\zeta_p)(\alpha)/k(\zeta_p)$, où α vérifie $\alpha^p = a$. On note ϱ un générateur du groupe $\mathrm{Gal}(E/k(\zeta_p))$. L'anneau de groupe $\mathbb{Z}[\langle\varrho\rangle]$ agit sur $E^\times$ d'une façon naturelle. On choisit la notation exponentielle pour cette action :

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

On pose $\mathfrak{N} = \sum_{i=0}^{p-1} \varrho^i$ et $\theta = \sum_{i=0}^{p-1} i\varrho^i$.

Le théorème suivant (voir [C1, Theorem 4, Theorem 6, et la remarque qui suit la preuve du Theorem 6]) donne un critère de plongement de l'extension $E/k(\zeta_p)$ dans une extension $K/k(\zeta_p)$ galoisienne, non abélienne et de degré p^3.

THÉORÈME 2.5. *Sous les notations précédentes, pour que $E/k(\zeta_p)$ soit plongeable dans une extension $K/k(\zeta_p)$ non abélienne de degré p^3, il faut et il suffit qu'il existe $e \in E^\times$, $\kappa \in k(\zeta_p)^\times$ et $\varepsilon \in \{0,1\}$ tels que les classes de $b = \zeta_p^\varepsilon e^{-\mathfrak{N}}$ et $c = \kappa\alpha^\varepsilon e^\theta$ dans $E^\times/E^{\times p}$ soient non triviales et engendrent deux sous-groupes distincts de $E^\times/E^{\times p}$. L'exposant de $\mathrm{Gal}(K/k(\zeta_p))$ est alors p si $\varepsilon = 0$, et p^2 si $\varepsilon = 1$. Lorsque le plongement est possible, on peut choisir $K = E(b^{1/p}, c^{1/p})$.*

3. Démonstration du théorème 1.1. Soit Γ un groupe non abélien d'ordre p^3 et d'exposant v. Soit k un corps de nombres tel que $k(\zeta_v)/k(\zeta_p)$ est non ramifié. Dans ce paragraphe, on montre l'égalité suivante :

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

3.1. *Première inclusion.* L'objectif de ce sous-paragraphe est de montrer l'inclusion suivante :

$$R_m(k,\Gamma) \subset N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))^{u(p-1)/2}.$$

Soit N/k une extension galoisienne, modérée, avec $\mathrm{Gal}(N/k) \simeq \Gamma$. Soit $\mathfrak{p}$ un idéal premier de O_k ramifié dans N/k. On voit facilement, en utilisant la proposition 2.4, que $\mathrm{cl}(\mathfrak{p}) \in N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))$. On note $e_\mathfrak{p}$ (resp. $f_\mathfrak{p}$) l'indice de ramification (resp. le degré résiduel) de $\mathfrak{p}$ dans N/k et $g_\mathfrak{p}$ le nombre d'idéaux premiers de O_N au dessus de $\mathfrak{p}$. La ramification dans N/k étant modérée, on a $v_\mathfrak{p}(\Delta(N/k)) = f_\mathfrak{p} g_\mathfrak{p}(e_\mathfrak{p} - 1)$, où $v_\mathfrak{p}$ désigne la valuation $\mathfrak{p}$-adique. Or, l'entier $u(p-1)$ est un diviseur de $f_\mathfrak{p} g_\mathfrak{p}(e_\mathfrak{p} - 1)$ car u divise $f_\mathfrak{p} g_\mathfrak{p}$ et $(p-1)$ divise $(e_\mathfrak{p} - 1)$. Ainsi, $\mathrm{cl}(\mathfrak{p}^{f_\mathfrak{p} g_\mathfrak{p}(e_\mathfrak{p}-1)}) \in N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))^{u(p-1)}$.

Comme $\Delta(N/k) = \prod_\mathfrak{p} \mathfrak{p}^{f_\mathfrak{p} g_\mathfrak{p}(e_\mathfrak{p}-1)}$, où $\mathfrak{p}$ parcourt l'ensemble des premiers de O_k ramifiés dans N/k, on a $\mathrm{cl}(\Delta(N/k)) \in N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))^{u(p-1)}$.

L'extension N/k étant galoisienne de degré impair, un théorème d'Artin (voir [A]) nous donne

$$\mathrm{cl}_k(O_N) = \mathrm{cl}(\Delta(N/k)^{1/2}) \in N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))^{u(p-1)/2},$$

ce qui termine la démonstration de la première inclusion.

3.2. *Deuxième inclusion.* Le but de ce sous-paragraphe est de prouver l'inclusion suivante :

$$N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))^{u(p-1)/2} \subset R_m(k,\Gamma).$$

REMARQUE. La démonstration qui suit peut être considérablement simplifiée lorsque k contient ζ_v. Dans ce cas, $k(\zeta_p) = k$, σ et A sont triviaux,

et la preuve se réduit essentiellement à un argument similaire à celui donné par Carter dans [C2].

Soit $c_0 \in N_{k(\zeta_p)/k}(\mathrm{Cl}(k(\zeta_p)))$. La démonstration se fera en quatre étapes. Le but est de construire une extension N/k modérée, à groupe de Galois isomorphe à Γ et de classe de Steinitz $c_0^{u(p-1)/2}$.

Étape 1 : *On construit une extension L/k cyclique de degré p, modérée, et dont la classe de Steinitz est $c_0^{(p-1)/2}$.* Soit l'idéal $\mathfrak{m} = (1-\zeta_p)^{p^2} O_{k(\zeta_p)}$. Soit t un entier impair tel que $t > 3$ et $c_0^t = c_0$. Soient $h_1, \dots, h_t$ des entiers naturels premiers à p et tels que $\sum_{i=1}^t h_i = p^2 t$; par exemple

$$h_i = \begin{cases} p^2 - 1 & \text{si } 1 \le i \le (t+1)/2, \\ p^2 + 1 & \text{si } (t+3)/2 \le i \le t-1, \\ p^2 + 2 & \text{si } i = t. \end{cases}$$

Soit $\mathrm{Cl}(k(\zeta_p), \mathfrak{m})$ le groupe des classes de rayon de $k(\zeta_p)$ modulo $\mathfrak{m}$. D'après la surjection $\mathrm{Cl}(k(\zeta_p), \mathfrak{m}) \to \mathrm{Cl}(k(\zeta_p))$ et le théorème de densité de Chebotarev, il existe une classe $c_{\mathfrak{m}} \in \mathrm{Cl}(k(\zeta_p), \mathfrak{m})$ telle que pour chaque $i = 1, \dots, t$, il existe un idéal premier $\mathfrak{p}_i \in c_0$, totalement décomposé dans $k(\zeta_p)/k$, ayant un diviseur premier $\mathfrak{P}_i \in c_{\mathfrak{m}}$ dans $O_{k(\zeta_p)}$. De plus, tous les idéaux $\mathfrak{p}_i$ sont distincts.

Soit $\mathfrak{P}_{t+1}$ un idéal de $O_{k(\zeta_p)}$ appartenant à $c_{\mathfrak{m}}^{-1}$. Soit $\mathfrak{a} = \prod_{i=1}^t \mathfrak{P}_i^{h_i} \mathfrak{P}_{t+1}^{p^2 t}$. Alors $\mathrm{cl}(\mathfrak{a}) = 1$ dans $\mathrm{Cl}(k(\zeta_p), \mathfrak{m})$. Donc il existe $a' \in O_{k(\zeta_p)}$ tel que

$$a' O_{k(\zeta_p)} = \mathfrak{a} = \prod_{i=1}^{t} \mathfrak{P}_i^{h_i} \mathfrak{P}_{t+1}^{p^2 t}, \quad \text{et} \quad a' \equiv 1 \bmod^* \mathfrak{m}.$$

Posons $a = a'^A$. Alors

$$a O_{k(\zeta_p)} = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{h_i} \mathfrak{P}_{t+1}^{p^2 t} \Big)^A = \prod_{j=0}^{l-1} \prod_{i=1}^{t} \sigma^j (\mathfrak{P}_i^{h_i s^{-j}}) (\mathfrak{P}_{t+1}^{At})^{p^2}, \text{ et } a \equiv 1 \bmod^* \mathfrak{m}.$$

L'élément a n'est pas une puissance $p^{\text{ième}}$ dans $k(\zeta_p)$ car $v_{\mathfrak{P}_1}(a) \equiv h_1 \bmod p$, et h_1 est premier à p. On considère l'extension $E = k(\zeta_p)(a^{1/p})/k(\zeta_p)$. C'est une extension cyclique de degré p. D'après la proposition 2.3 et la remarque qui la suit, E/k est abélienne et contient une unique sous-extension L/k cyclique de degré p.

L'extension $E/k(\zeta_p)$ est modérée car $a \equiv 1 \bmod^* (1-\zeta_p)^{p^2} O_{k(\zeta_p)}$ (voir le théorème 2.1(i)). On en déduit que L/k est modérément ramifiée. Ceci implique que L/k et $k(\zeta_p)/k$ sont arithmétiquement disjointes. Ainsi on a $\Delta(L/k) O_{k(\zeta_p)} = \Delta(E/k(\zeta_p))$, d'où

$$\Delta(L/k)^l = N_{k(\zeta_p)/k}(\Delta(E/k(\zeta_p))).$$

Comme les $h_i, 1 \le i \le t$, sont premiers à p et que les $\mathfrak{P}_i$ ne sont pas conjugués sous $\mathrm{Gal}(k(\zeta_p)/k)$, on obtient $\mathcal{F}(aO_{k(\zeta_p)}) = \prod_{i=1}^{t}\prod_{j=0}^{l-1}\sigma^j(\mathfrak{P}_i)$. On a donc, d'après le théorème 2.1(i), $\Delta(E/k(\zeta_p)) = (\prod_{i=1}^{t}\prod_{j=0}^{l-1}\sigma^j(\mathfrak{P}_i))^{p-1}$. Mais les $\mathfrak{p}_i$ sont totalement décomposés dans $k(\zeta_p)/k$, d'où

$$\Delta(E/k(\zeta_p)) = \Big(\prod_{i=1}^{t}\mathfrak{p}_i O_{k(\zeta_p)}\Big)^{p-1}.$$

Par conséquent,

$$\Delta(L/k) = \Big(\prod_{i=1}^{t}\mathfrak{p}_i\Big)^{p-1}.$$

L'extension L/k étant de degré impair, le théorème d'Artin (voir [A]) donne $\mathrm{cl}_k(O_L) = c_0^{t(p-1)/2} = c_0^{(p-1)/2}$.

On se fixe ϱ un générateur de $\mathrm{Gal}(E/k(\zeta_p))$, et on note $\mathfrak{N} = \sum_{i=0}^{p-1}\varrho^i$ et $\theta = \sum_{i=0}^{p-1} i\varrho^i$.

Puisque les extensions L/k et $k(\zeta_p)/k$ sont linéairement disjointes et que E est la composée de L et $k(\zeta_p)$ ($E = L(\zeta_p)$), on a l'isomorphisme de restriction $\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(k(\zeta_p)/k)$ ($= \langle\sigma\rangle$). Dans la suite, pour ne pas alourdir les notations, on identifiera $\mathrm{Gal}(E/L)$ avec $\mathrm{Gal}(k(\zeta_p)/k)$ sous cet isomorphisme, et donc on pourra considérer A comme un élément de $\mathbb{F}_p[\mathrm{Gal}(E/L)]$.

On choisit un élément α de $E^\times$ tel que $\alpha^p = a$.

Étape 2 : *On plonge l'extension L/k dans une extension non abélienne de degré p^3.* On pose $\varepsilon = 0$ si $v = p$ et $\varepsilon = 1$ si $v = p^2$.

Soient u_i, $1 \le i \le t$, des entiers naturels premiers à p et tels que $\sum_{i=1}^{t} u_i = pt$. D'après la surjection $\mathrm{Cl}(k(\zeta_p), \mathfrak{m}) \to \mathrm{Cl}(k(\zeta_p))$ et le théorème de densité de Chebotarev, il existe une classe $c'_{\mathfrak{m}}$ de $\mathrm{Cl}(k(\zeta_p), \mathfrak{m})$ telle que pour chaque $i = 1, \ldots, t$, il existe un idéal premier $\mathfrak{q}_i \in c_0^{-1}$, totalement décomposé dans $k(\zeta_p)/k$, ayant un diviseur premier $\mathfrak{Q}_i \in c'_{\mathfrak{m}}$ dans $O_{k(\zeta_p)}$. De plus, tous les idéaux $\mathfrak{q}_i$ sont distincts et premiers à aO_k.

Soit $\mathfrak{Q}_{t+1}$ un idéal premier de $O_{k(\zeta_p)}$ appartenant à $c'^{-1}_{\mathfrak{m}}$ et premier à $aO_{k(\zeta_p)}$.

Soit $\mathfrak{K} = \prod_{i=1}^{t}\mathfrak{Q}_i^{u_i}\mathfrak{Q}_{t+1}^{pt}$. Alors $\mathrm{cl}(\mathfrak{K}) = 1$ dans $\mathrm{Cl}(k(\zeta_p), \mathfrak{m})$. Donc il existe $\kappa' \in O_{k(\zeta_p)}$ tel que

$$\kappa' O_{k(\zeta_p)} = \mathfrak{K} = \prod_{i=1}^{t}\mathfrak{Q}_i^{u_i}\mathfrak{Q}_{t+1}^{pt}, \quad \text{et} \quad \kappa' \equiv 1 \bmod^* \mathfrak{m}.$$

Posons $\kappa = \kappa'^A$. Alors

$$\kappa O_{k(\zeta_p)} = \Big(\prod_{i=1}^{t}\mathfrak{Q}_i^{h_i}\mathfrak{Q}_{t+1}^{pt}\Big)^A = \prod_{j=0}^{l-1}\prod_{i=1}^{t}\sigma^j(\mathfrak{Q}_i^{h_i s^{-j}})(\mathfrak{Q}_{t+1}^{At})^p, \text{ et } \kappa \equiv 1 \bmod^* \mathfrak{m}.$$

On note $\mathrm{Cl}(E, \mathfrak{m}O_E)$ le groupe des classes de rayon de E modulo $\mathfrak{m}O_E$. D'après le théorème de densité de Chebotarev, il existe un idéal premier $\mathfrak{E}$ de O_E dans la classe triviale de $\mathrm{Cl}(E, \mathfrak{m}O_E)$ tel que $\mathfrak{E} \cap O_k$ est totalement décomposé dans E/k, et tel que $\mathfrak{E}$ et tous ses conjugués sous $\mathrm{Gal}(E/k)$ sont premiers à $\kappa\alpha O_E$.

Puisque $\mathrm{cl}(\mathfrak{E}) = 1$ dans $\mathrm{Cl}(E, \mathfrak{m}O_E)$, il existe $e' \in O_E$ tel que $e'O_E = \mathfrak{E}$ et $e' \equiv 1 \bmod^* \mathfrak{m}O_E$.

Posons $e = e'^A$, $b = \zeta_p^{\varepsilon} e^{-\mathfrak{N}}$ et $c = \kappa^{\varepsilon}\alpha^{\varepsilon}e^{\theta}$.

Montrons que b et c satisfont les conditions du théorème 2.5. On a

$$bO_E = \zeta_p^{\varepsilon} e^{-\mathfrak{N}} O_E = \prod_{j=0}^{l-1} \sigma^j(\mathfrak{E})^{-s^{-j}\mathfrak{N}} = \prod_{i=0}^{p-1}\prod_{j=0}^{l-1} \varrho^i\sigma^j(\mathfrak{E})^{-s^{-j}},$$

ainsi $v_{\mathfrak{E}}(b) \equiv -1 \bmod p$. Par suite, la classe de b dans $E^\times/E^{\times p}$ est non triviale.

De même, on a

$$cO_E = (\kappa\alpha)^{\varepsilon}e^{\theta}O_E = \prod_{j=0}^{l-1} \sigma^j(\mathfrak{E})^{s^{-j}\theta}(\kappa\alpha)^{\varepsilon}O_E = \prod_{i=0}^{p-1}\prod_{j=0}^{l-1} \varrho^i\sigma^j(\mathfrak{E})^{is^{-j}}(\kappa\alpha)^{\varepsilon}O_E.$$

Mais $\varrho(\mathfrak{E})$ est premier à $(\kappa\alpha)^{\varepsilon}O_E$, d'où $v_{\varrho(\mathfrak{E})}(c) \equiv 1 \bmod p$, et on a donc $c \not\equiv 1 \bmod E^{\times p}$.

Supposons qu'il existe $u \in \{1, \dots, p-1\}$ tel que $c \equiv b^u \bmod E^{\times p}$. Alors $cb^{-u} \equiv 1 \bmod E^{\times p}$. Or

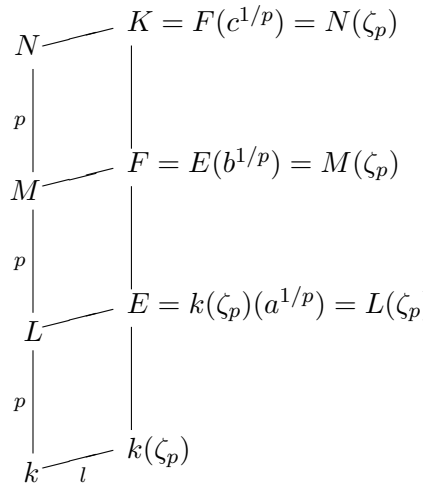
$$cb^{-u}O_E = \prod_{i=0}^{p-1}\prod_{j=0}^{l-1} \varrho^i\sigma^j(\mathfrak{E})^{(i+u)s^{-j}}(\kappa\alpha)^{\varepsilon}O_E,$$

ainsi $v_{\mathfrak{E}}(cb^{-u}) \equiv u \bmod p$, ce qui contredit $cb^{-u} \equiv 1 \bmod E^{\times p}$. Donc les sous-groupes $\langle cE^{\times p}\rangle$ et $\langle bE^{\times p}\rangle$ de $E^\times/E^{\times p}$ sont distincts.

D'après le théorème 2.5, l'extension $E/k(\zeta_p)$ est plongeable dans une extension $K/k(\zeta_p)$ à groupe de Galois isomorphe à Γ, et on peut prendre $K = E(b^{1/p}, c^{1/p}) = k(\zeta_p, a^{1/p}, b^{1/p}, c^{1/p})$.

Posons $F = E(b^{1/p})$ et rappelons que $E = L(\zeta_p)$. Puisque ϱ et σ commutent, $b = e^{-\mathfrak{N}} = (e'^{-\mathfrak{N}})^A$ et $c = e^{\theta} = (e'^{\theta})^A$. D'après la proposition 2.3, F/L est abélienne. Son degré est pl, elle contient donc une unique sous-extension M/L cyclique de degré p ; de plus, $F = M(\zeta_p)$. De même, en considérant K/F, l'extension K/M est abélienne de degré pl et contient une unique sous-extension N/M cyclique de degré p. Signalons que $K = N(\zeta_p)$. On a les isomorphismes de restrictions et le diagramme suivants :

$$\mathrm{Gal}(K/N) \simeq \mathrm{Gal}(F/M) \simeq \mathrm{Gal}(E/L) \simeq \mathrm{Gal}(k(\zeta_p)/k) = \langle\sigma\rangle.$$



Montrons que K/k est galoisienne. Soit $x \in K$ invariant sous l'action de $G = \{k\text{-automorphismes de } K\}$. Comme $\mathrm{Gal}(K/k(\zeta_p))$ et $\mathrm{Gal}(K/N)$ sont inclus dans G, $x \in k(\zeta_p) \cap N$. Mais $k(\zeta_p) \cap N = k$ car $l = [k(\zeta_p) : k]$ et $p^3 = [N : k]$ sont premiers entre eux. Donc K/k est galoisienne. Il est immédiat que $\mathrm{Gal}(K/k) = \mathrm{Gal}(K/N) \rtimes \mathrm{Gal}(K/k(\zeta_p))$.

Maintenant prouvons que N/k est galoisienne. Pour cela, nous montrons que $\mathrm{Gal}(K/N)$, identifié à $\langle\sigma\rangle$, est un sous-groupe normal de $\mathrm{Gal}(K/k)$. Soient $\gamma \in \mathrm{Gal}(K/k)$ et $H' = \gamma\langle\sigma\rangle\gamma^{-1}$. Soit $N' = K^{H'}$ le sous-corps de K fixe par H'. Ci-dessous nous démontrons que $N' = N$. Comme $N = K^{\langle\sigma\rangle}$, d'après la théorie de Galois, $H' = \langle\sigma\rangle$, et donc $\mathrm{Gal}(K/N)$ est un sous-groupe normal de $\mathrm{Gal}(K/k)$.

Considérons $N' \cap L$. D'après les inclusions $k \subset N' \cap L \subset L$, il vient $N' \cap L = L$ ou bien $N' \cap L = k$. On a $N' \cap L = L$: en effet, sinon, comme L/k est galoisienne, les extensions N'/k et L/k sont linéairement disjointes ; on obtient alors $[N'L : k] = [N' : k][L : k] = p^4$, ce qui est impossible puisque $N'L \subset K$ et $[K : k] = p^3 l < p^4$. De même, en considérant $N' \cap M$, les inclusions $L \subset N' \cap M \subset M$ impliquent $N' \cap M = M$ ou bien $N' \cap M = L$; si l'on suppose $N' \cap M = L$, alors les extensions N'/L et M/L sont linéairement disjointes car M/L est galoisienne ; on obtient $[N'M : L] = [N' : L][M : L] = p^3$, ce qui est impossible puisque $N'M \subset K$ et $[K : L] = p^2 l < p^3$. On en déduit que $M \subset N'$. Ainsi, N'/M est une sous-extension de K/M de degré $p = [N' : k]/[M : k]$. Or l'extension K/M admet N/M comme unique sous-extension cyclique de degré p, d'où $N' = N$. On conclut que N/k est galoisienne.

On a $\mathrm{Gal}(N/k) \simeq \mathrm{Gal}(K/k(\zeta_p))$ car les extensions N/k et $k(\zeta_p)/k$ sont linéairement disjointes et K est la composée de N et $k(\zeta_p)$. Par conséquent, N/k est une extension à groupe de Galois isomorphe à Γ.

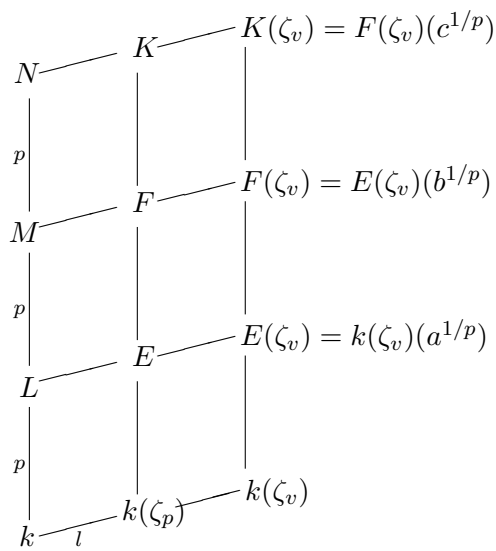
Remarque. Les extensions N/k et $k(\zeta_p)/k$ étant galoisiennes, linéairement disjointes, avec $Nk(\zeta_p) = K$, on a

$$\mathrm{Gal}(K/k) \simeq \mathrm{Gal}(k(\zeta_p)/k) \times \mathrm{Gal}(N/k) \simeq \mathrm{Gal}(K/N) \times \mathrm{Gal}(K/k(\zeta_p)).$$

Donc $\mathrm{Gal}(K/k)$ est un produit direct de ses sous-groupes $\mathrm{Gal}(K/N)$ et $\mathrm{Gal}(K/k(\zeta_p))$. On en déduit que σ appartient au centre de $\mathrm{Gal}(K/k)$.

Étape 3 : *On montre que N/k est modérément ramifiée.* Faisons les observations suivantes. Les extensions $E/k(\zeta_p)$, F/E et K/F sont ramifiées en au moins un idéal premier, premier respectivement à $pO_{k(\zeta_p)}$, pO_E et pO_F (on le voit en utilisant la décomposition de $aO_{k(\zeta_p)}$, bO_E et cO_F). Elles sont donc respectivement linéairement disjointes de $k(\zeta_v)/k(\zeta_p)$, $E(\zeta_v)/E$ et $F(\zeta_v)/F$ (puisque ces dernières ne peuvent se ramifier qu'en des idéaux premiers au dessus de p) ; en particulier, le degré des extensions $E(\zeta_v)/k(\zeta_v)$, $F(\zeta_v)/E(\zeta_v)$ et $K(\zeta_v)/F(\zeta_v)$ est égal à p.

On a le diagramme suivant :



Pour voir que N/k est modérée, nous commençons par montrer que $K(\zeta_v)/k(\zeta_v)$ l'est. Ensuite, en supposant que $k(\zeta_v)/k(\zeta_p)$ est non ramifiée (c'est le seul endroit de l'article où l'on utilise cette hypothèse), on en déduit que $K(\zeta_v)/k$ est modérée ; il en est donc de même de N/k. On rappelle que $\varepsilon = 0$ lorsque $v = p$, et $\varepsilon = 1$ lorsque $v = p^2$.

Puisque $E/k(\zeta_p)$ est modérée (voir Étape 1) et $Ek(\zeta_v) = E(\zeta_v)$, l'extension $E(\zeta_v)/k(\zeta_v)$ est modérée. Donc pour que $K(\zeta_v)/k(\zeta_v)$ soit modérée, il faut et il suffit que $F(\zeta_v)/E(\zeta_v)$ et $K(\zeta_v)/F(\zeta_v)$ le soient.

Considérons l'extension $F(\zeta_v)/E(\zeta_v)$. Rappelons que $b = \zeta_p^{\varepsilon} e^{-\mathfrak{N}}$, $e = e'^A$, et $e' \equiv 1 \bmod^* \mathfrak{m}O_E$. Immédiatement, on a $e^{-\mathfrak{N}} \equiv 1 \bmod^* \mathfrak{m}O_E$. On en

déduit que $b \equiv \zeta_p^{\varepsilon} \bmod^* \mathfrak{m}O_{E(\zeta_v)}$. Mais ζ_p^{ε} est une puissance $p^{\text{ième}}$ dans $E(\zeta_v)$. Par suite $F(\zeta_v)/E(\zeta_v)$ est modérément ramifiée par le théorème 2.1(i).

Montrons que $K(\zeta_v)/F(\zeta_v)$ est modérée. Soient $\mathfrak{p}$ un idéal premier de $O_{F(\zeta_v)}$ divisant $(1-\zeta_p)O_{F(\zeta_v)}$ et $w = v_{\mathfrak{p}}((1-\zeta_p)O_{F(\zeta_v)})$. Rappelons que $\kappa \equiv 1 \bmod^* (1-\zeta_p)^{p^2}O_{k(\zeta_p)}$, d'où $\kappa \equiv 1 \bmod^* (1-\zeta_p)^{p^2}O_{F(\zeta_v)}$ et donc $\kappa \equiv 1 \bmod^* \mathfrak{p}^{wp^2}$. De même, $e^{\theta} \equiv 1 \bmod^* \mathfrak{p}^{wp^2}$, et $a \equiv 1 \bmod^* \mathfrak{p}^{wp^2}$. La dernière congruence implique $v_{\mathfrak{p}}(a-1) \geq wp^2$, soit $v_{\mathfrak{p}}(\prod_{i=0}^{p-1}(\alpha - \zeta_p^i)) \geq wp^2$. Il s'ensuit qu'il existe $i \in \{0, \ldots, p-1\}$ tel que $v_{\mathfrak{p}}(\alpha - \zeta_p^i) \geq wp$, d'où $\alpha \equiv \zeta_p^i \bmod^* \mathfrak{p}^{wp}$. Enfin, $c = \kappa^{\varepsilon}\alpha^{\varepsilon}e^{\theta} \equiv (\zeta_p^i)^{\varepsilon} \bmod^* \mathfrak{p}^{wp}$. Comme $(\zeta_p^i)^{\varepsilon}$ est une puissance $p^{\text{ième}}$ dans $F(\zeta_v)$, le théorème 2.1(ii) implique que $\mathfrak{p}$ est non ramifié dans $K(\zeta_v)/F(\zeta_v)$. Ainsi, aucun diviseur premier de $(1-\zeta_p)O_{F(\zeta_v)}$ ne se ramifie dans $K(\zeta_v)/F(\zeta_v)$, donc l'extension $K(\zeta_v)/F(\zeta_v)$ est modérément ramifiée.

On conclut que N/k est modérée. Par suite, les extensions N/k et $k(\zeta_p)/k$ sont arithmétiquement disjointes.

Étape 4 : *On calcule* $\mathrm{cl}_k(O_N)$. D'après la transitivité de la classe de Steinitz dans une tour de corps de nombres (voir [F1, Theorem 4.1]), on a $\mathrm{cl}_k(O_N) = \mathrm{cl}_k(O_L)^{[N:L]}N_{L/k}(\mathrm{cl}_L(O_N))$.

Comme N/L est galoisienne de degré impair, le théorème d'Artin implique que $\mathrm{cl}_L(O_N) = \mathrm{cl}(\Delta(N/L)^{1/2})$. Puisque E/L et N/L sont arithmétiquement disjointes et que $K = EN$, on a $\Delta(N/L)O_E = \Delta(K/E)$.

Calculons $\Delta(K/E)$. On a $\Delta(K/E) = \Delta(F/E)^{[K:F]}N_{F/E}(\Delta(K/F))$.

D'une part, d'après le théorème 2.1(i), $\Delta(F/E) = (\mathcal{F}(bO_E))^{p-1}$. Mais

$$bO_E = \prod_{i=0}^{p-1}\prod_{j=0}^{l-1} \varrho^i\sigma^j(\mathfrak{E})^{-s^{-j}},$$

où, pour tout j, $0 \leq j \leq l-1$, on a $s^{-j} \not\equiv 0 \bmod p$, et $\mathfrak{E} \cap O_k$ est totalement décomposé dans E/k. Alors

$$\Delta(F/E) = \Big(\prod_{i=0}^{p-1}\prod_{j=0}^{l-1} \varrho^i\sigma^j(\mathfrak{E})\Big)^{p-1}.$$

D'autre part, $\Delta(K/F) = (\mathcal{F}(cO_F))^{p-1}$ et $c = (\kappa\alpha)^{\varepsilon}e^{\theta}$. Pour déterminer la décomposition de l'idéal cO_F en un produit d'idéaux premiers, trouvons d'abord celle de αO_F. On a

$$aO_E = \alpha^p O_E = \prod_{j=0}^{l-1}\prod_{i'=1}^{t} \sigma^j(\mathfrak{P}_{i'}^{h_{i'}s^{-j}})(\mathfrak{P}_{t+1}^{At})^{p^2}O_E,$$

et les seuls idéaux premiers de $O_{k(\zeta_p)}$ ramifiés dans $E/k(\zeta_p)$ sont les $\sigma^j(\mathfrak{P}_{i'})$,

avec $1 \leq i' \leq t$, $0 \leq j \leq l-1$. Donc

$$\alpha O_E = \prod_{j=0}^{l-1} \prod_{i'=1}^{t} \sigma^j(\mathfrak{L}_{i'}^{h_{i'} s^{-j}})(\mathfrak{P}_{t+1}^{At} O_E)^p,$$

où pour tout i', $1 \leq i' \leq t$, $\mathfrak{L}_{i'}$ est l'idéal premier de O_E tel que $\mathfrak{P}_{i'} O_E = \mathfrak{L}_{i'}^p$. Ceci nous donne

$$\alpha O_F = \prod_{j=0}^{l-1} \prod_{i'=1}^{t} \sigma^j(\mathfrak{L}_{i'}^{h_{i'} s^{-j}})(\mathfrak{P}_{t+1}^{At})^p O_F.$$

On a aussi

$$\kappa O_F = \prod_{j=0}^{l-1} \prod_{i'=1}^{t} \sigma^j(\mathfrak{Q}_{i'}^{h_{i'} s^{-j}})(\mathfrak{Q}_{t+1}^{At})^p O_F.$$

On rappelle que les $\sigma^j(\mathfrak{Q}_{i'})$, $1 \leq i' \leq t$, $0 \leq j \leq l-1$, ne sont pas ramifiés dans $E/k(\zeta_p)$, car on les a choisis premiers à $aO_{k(\zeta_p)}$. Enfin, on a

$$e^\theta O_F = \prod_{i=0}^{p-1} \prod_{j=0}^{l-1} \varrho^i \sigma^j(\mathfrak{E})^{is^{-j}} O_F.$$

Par conséquent,

$$cO_F = \prod_{j=0}^{l-1} \sigma^j \Big(\prod_{i=1}^{p-1} \varrho^i(\mathfrak{E})^{is^{-j}} \Big(\prod_{i'=1}^{t} \mathfrak{L}_{i'}^{h_{i'} s^{-j}} \mathfrak{Q}_{i'}^{h_{i'} s^{-j}} \Big)^{\varepsilon} \Big) (\mathfrak{Q}_{t+1}^{At})^{\varepsilon p} (\mathfrak{P}_{t+1}^{At})^{\varepsilon p} O_F.$$

Rappelons que nous avons montré que les seuls idéaux premiers de O_E ramifiés dans F/E sont les $\sigma^j \varrho^i(\mathfrak{E})$, $0 \leq i \leq p-1$, $0 \leq j \leq l-1$ (voir $\Delta(F/E)$). Donc $\sigma^j \varrho^i(\mathfrak{E}) O_F$ est la puissance $p^{\text{ième}}$ d'un idéal premier de O_F ; et les idéaux $\sigma^j(\mathfrak{L}_{i'})$ (resp. $\sigma^j(\mathfrak{Q}_{i'})$), pour tout i', j, $1 \leq i' \leq t$, $0 \leq j \leq l-1$, ne sont pas ramifiés dans F/E (resp. $F/k(\zeta_p)$). En effet, on a pris soin de choisir $\mathfrak{E}$ tel que tous les $\sigma^j \varrho^i(\mathfrak{E})$ sont premiers avec $\kappa\alpha O_E$.

Comme les $\sigma^j(\mathfrak{P}_{i'})$ et les $\sigma^j(\mathfrak{Q}_{i'})$ sont premiers entre eux deux à deux, les $\sigma^j(\mathfrak{L}_{i'})$ et les $\sigma^j(\mathfrak{Q}_{i'}) O_E$ le sont également. Donc les $\sigma^j(\mathfrak{L}_{i'}) O_F$ et les $\sigma^j(\mathfrak{Q}_{i'}) O_F$ sont premiers entre eux deux à deux. Ce dernier point, conjugué au fait que $h_{i'} s^{-j} \not\equiv 0 \bmod p$, nous donne

$$\mathcal{F}(cO_F) = \prod_{j=0}^{l-1} \sigma^j \Big(\prod_{i'=1}^{t} \mathfrak{L}_{i'} \mathfrak{Q}_{i'} \Big)^{\varepsilon} O_F,$$

d'où

$$\Delta(K/F) = \Big(\prod_{j=0}^{l-1} \sigma^j \Big(\prod_{i'=1}^{t} \mathfrak{L}_{i'} \mathfrak{Q}_{i'} \Big)^{\varepsilon} O_F \Big)^{p-1}.$$

On a donc

$$\begin{aligned}\Delta(K/E) &= \Delta(F/E)^{[K:F]} N_{F/E}(\Delta(K/F)) \\ &= \Big(\prod_{i=0}^{p-1}\prod_{j=0}^{l-1} \varrho^i\sigma^j(\mathfrak{E})\Big)^{p(p-1)} N_{F/E}\Big(\prod_{j=0}^{l-1}\sigma^j\Big(\prod_{i'=1}^{t}\mathfrak{L}_{i'}\mathfrak{Q}_{i'}\Big)^{\varepsilon} O_F\Big)^{p-1} \\ &= \Big(\prod_{j=0}^{l-1}\sigma^j\Big(\prod_{i=0}^{p-1}\varrho^i(\mathfrak{E})\Big(\prod_{i'=1}^{t}\mathfrak{L}_{i'}\mathfrak{Q}_{i'}\Big)^{\varepsilon} O_E\Big)\Big)^{p(p-1)}.\end{aligned}$$

Ainsi,

$$\Delta(N/L)^l = N_{E/L}(\Delta(K/E)) = N_{E/L}\Big(\prod_{i=0}^{p-1}\varrho^i(\mathfrak{E})\Big(\prod_{i'=1}^{t}\mathfrak{L}_{i'}\mathfrak{Q}_{i'}\Big)^{\varepsilon} O_E\Big)^{p(p-1)l}.$$

Enfin, on rappelle que $\mathfrak{E}$ est principal dans O_E (donc $N_{E/k}(\mathfrak{E})$ est un idéal principal de O_k), que pour tout i', $1 \le i' \le t$, on a $N_{E/k(\zeta_p)}(\mathfrak{L}_{i'}) = \mathfrak{P}_{i'}$, $N_{k(\zeta_p)/k}(\mathfrak{P}_{i'}) = \mathfrak{p}_{i'}$, $N_{k(\zeta_p)/k}(\mathfrak{Q}_{i'}) = \mathfrak{q}_{i'}$, $\mathrm{cl}(\mathfrak{p}_{i'}) = c_0$, $\mathrm{cl}(\mathfrak{q}_{i'}) = c_0^{-1}$, et que $\mathrm{cl}_k(O_L) = c_0^{(p-1)/2}$ et $c_0^t = c_0$.

On obtient donc

$$\begin{aligned}\mathrm{cl}_k(O_N) &= \mathrm{cl}_k(O_L)^{[N:L]} N_{L/k}(\mathrm{cl}_L(O_N)) \\ &= c_0^{p^2(p-1)/2}\,\mathrm{cl}(N_{L/k}(\Delta(N/L)^{1/2})) \\ &= c_0^{p^2(p-1)/2}\,\mathrm{cl}\Big(N_{E/k}\Big(\prod_{i=0}^{p-1}\varrho^i(\mathfrak{E})\Big(\prod_{i'=1}^{t}\mathfrak{L}_{i'}\mathfrak{Q}_{i'}\Big)^{\varepsilon} O_E\Big)^{p(p-1)/2}\Big) \\ &= c_0^{p^2(p-1)/2}\,\mathrm{cl}\Big(\Big(N_{E/k}(\mathfrak{E})^p N_{E/k}\Big(\prod_{i'=1}^{t}\mathfrak{L}_{i'}\mathfrak{Q}_{i'}O_E\Big)^{\varepsilon}\Big)^{p(p-1)/2}\Big) \\ &= c_0^{p^2(p-1)/2}\,\mathrm{cl}\Big(N_{k(\zeta_p)/k}\Big(\prod_{i'=1}^{t}\mathfrak{P}_{i'}\mathfrak{Q}_{i'}^p\Big)^{\varepsilon}\Big)^{p(p-1)/2} \\ &= c_0^{p^2(p-1)/2}\,\mathrm{cl}\Big(\prod_{i'=1}^{t}\mathfrak{p}_{i'}\mathfrak{q}_{i'}^p\Big)^{\varepsilon p(p-1)/2} \\ &= c_0^{p^2(p-1)/2} c_0^{\varepsilon p(p-1)/2} c_0^{-\varepsilon p^2(p-1)/2} = c_0^{u(p-1)/2},\end{aligned}$$

ce qui achève la démonstration de la deuxième inclusion, et du théorème 1.1.

4. Appendice. Exemples d'extensions $k(\zeta_{p^2})/k(\zeta_p)$ non ramifiées. Supposons que $\zeta_{p^2} \notin k(\zeta_p)$, alors $[k(\zeta_{p^2}) : k(\zeta_p)] = p$. D'après le théorème 2.1(i), l'extension $k(\zeta_{p^2})/k(\zeta_p)$ est non ramifiée si et seulement si il existe $b \in k(\zeta_p)^\times$ tel que $\zeta_p \equiv b^p \bmod^* (1-\zeta_p)^p O_{k(\zeta_p)}$.

Supposons $p = 3$. On note j une racine primitive $3^{\text{ième}}$ de l'unité. On sait que l'extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ est totalement ramifiée. On en déduit que

l'extension de Kummer $\mathbb{Q}(\zeta_9)/\mathbb{Q}(j)$ est ramifiée. D'après le théorème 2.1(i), cela implique que

$$(*) \qquad \forall x \in \mathbb{Q}(j)^\times, \quad j \not\equiv x^3 \bmod^* (1-j)^3\ \mathbb{Z}[j].$$

Posons $a = j + (1-j)^3 = -3 - 5j$. On a $a \notin \mathbb{Q}(j)^3$ d'après $(*)$. On considère $E = \mathbb{Q}(j, a^{1/3})$; l'extension $E/\mathbb{Q}(j)$ est donc cyclique de degré 3. Le théorème 2.1(i) implique que $E(\zeta_9)/E(j)$ $(E(j) = E)$ est non ramifiée. D'après la théorie de Kummer, pour que cette dernière extension ne soit pas triviale, il faut et il suffit que $ja \notin E^3$ et $j^2a \notin E^3$. Mais $ja = j^2 + j(1-j)^3$, donc $ja \notin E^3$ d'après $(*)$. L'élément j^2a n'appartient pas à E^3 car il est immédiat que l'équation $j^2a = -2 + 3j = (x + yj)^3$ n'a pas de solutions x et y appartenant à $\mathbb{Z}$. On en déduit que $E(\zeta_9)/E(j)$ est une extension non triviale et non ramifiée.

Maintenant supposons que p est un nombre premier impair quelconque. D'une façon similaire, on montre que lorsqu'une extension $k(\zeta_{p^2})/k(\zeta_p)$ est ramifiée, l'extension $E = k(\zeta_p)(a^{1/p})$, où $a = \zeta_p + (1-\zeta_p)^p$, est telle que $E(\zeta_{p^2})/E(\zeta_p)$ soit non ramifiée. Par la théorie de Kummer, elle est non triviale si et seulement si pour tout $i \in \mathbb{Z}$, $\zeta_p^i a$ n'est pas une puissance $p^{\text{ième}}$ dans $k(\zeta_p)$. Cette dernière condition est équivalente à $\zeta_p^{-1}a \notin k(\zeta_p)^{\times p}$; en effet, si $i \not\equiv -1 \bmod p$, on a $\zeta_p^i a \equiv \zeta_p^{i+1} \bmod^* (1-\zeta_p)^p O_{k(\zeta_p)}$, mais la congruence $\zeta_p^{i+1} \equiv x^p \bmod^* (1-\zeta_p)^p O_{k(\zeta_p)}$ n'a pas de solution dans $k(\zeta_p)^\times$ car l'extension $k(\zeta_{p^2})/k(\zeta_p)$ est ramifiée.

Références

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

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

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

[BS1] N. P. Byott and B. Sodaïgui, *Realizable Galois module classes for tetrahedral extensions*, Compos. Math. 141 (2005), 573–582.

[BS2] —, —, *Galois module structure for dihedral extensions of degree 8 : realizable classes over the group ring*, J. Number Theory 112 (2005), 1–19.

[C1] J. E. Carter, *Characterisations of Galois extensions of prime cubed degree*, Bull. Austral. Math. Soc. 55 (1997), 99–112.

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

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

[CS] J. E. Carter et B. Sodaïgui, *Classes de Steinitz d'extensions quaternioniennes généralisées de degré $4p^r$*, J. London Math. Soc. 76 (2007), 331–344.

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

[E] L. P. Endo, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, thèse, Univ. 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] —, *Galois Module Structure of Algebraic Integers*, Springer, Berlin, 1983.

[FT] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 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] —, —, *Module structure of rings of integers in octahedral extensions,* Acta Arith. 109 (2003), 321–327.

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

[L1] R. Long, *Steinitz classes of cyclic extensions of prime degree*, J. Reine Angew. Math. 250 (1971), 87–98.

[L2] —, *Steinitz classes of cyclic extensions of degree l^r*, Proc. Amer. Math. Soc. 49 (1975), 297–304.

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

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

[So1] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement*, Illinois J. Math. 43 (1999), 47–60.

[So2] —, *"Galois module structure" des extensions quaternioniennes de degré 8*, J. Algebra 213 (1999), 549–556.

[So3] —, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, ibid. 223 (2000), 367–378.

[So4] —, *Relative Galois module structure of octahedral extensions*, ibid. 312 (2007), 590–601.

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

LAMAV–ISTV2
Université de Valenciennes
Le Mont-Houy
59313 Valenciennes Cedex 9, France
E-mail: clement.bruche@univ-valenciennes.fr

Reçu le 13.5.2008
et révisé le 22.10.2008 (5705)