Functiones et Approximatio
48.2 (2013), 183–196
doi: 10.7169/facm/2013.48.2.2

CLASSES DE STEINITZ D'EXTENSIONS GALOISIENNES À GROUPE DE GALOIS UN 2-GROUPE

Bouchaïb Sodaïgui

Abstract: Let k be a number field and $Cl(k)$ its class group. Let Γ be a non trivial finite 2-group. Let $R_m(k,\Gamma)$ be the subset of $Cl(k)$ consisting of those classes which are realizable as Steinitz classes of tame Galois extensions of k with Galois group isomorphic to Γ. In the present article, we show that $R_m(k,\Gamma)$ is the full group $Cl(k)$, if the class number of k is odd. We study an embedding problem connected with Steinitz classes in the perspective of studying realizable Galois module classes, when Γ is defined by certain central non-split group extensions, examples of which are certain groups of order 32 or 64. For such groups Γ, We prove that for all $c \in Cl(k)$, there exist a tame quadratic extension of k, with Steinitz class c, and which is embeddable in a Galois extension of k with Galois group isomorphic to Γ.

Keywords: 2-groups, Galois module structure, ring of integers, realizable Steinitz classes, embedding problem, central extensions, local symbols, Brauer group.

Résumé: Soient k un corps de nombres et $Cl(k)$ son groupe de classes. Soit Γ un 2-groupe fini non trivial. Soit $R_m(k,\Gamma)$ le sous-ensemble de $Cl(k)$ formé par les éléments qui sont réalisables par les classes de Steinitz d'extensions galoisiennes de k, modérément ramifiées et dont le groupe de Galois est isomorphe à Γ. Dans cet article, on montre que $R_m(k,\Gamma)$ est le groupe $Cl(k)$ tout entier, si le nombre de classes de k est impair. On étudie un problème de plongement en liaison avec les classes de Steinitz, dans la perspective de l'étude des classes galoisiennes réalisables, lorsque Γ est défini par certaines extensions centrales non scindées, dont des exemples sont certains groupes d'ordre 32 ou 64. Pour de tels groupes Γ, on prouve que pour tout $c \in Cl(k)$, il existe une extension quadratique de k, modérée, dont la classe de Steinitz est c, et qui est plongeable dans une extension galoisienne de k, à groupe de Galois isomorphe à Γ.

Mots clés: 2-groupes, structure de module galoisien, anneaux d'entiers, classes de Steinitz réalisables, problème de plongement, extensions centrales, symboles locaux, groupe de Brauer.

1. Introduction et énoncé des principaux résultats

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

2010 Mathematics Subject Classification: primary: 11R33

Soit k un corps de nombres. Soit M un O_k-module de type fini, sans torsion et de rang n. Alors, il existe un idéal I de O_k tel que $M \simeq O_k^{n-1} \oplus I$ en tant que O_k-module. La classe de I dans $Cl(k)$, qui ne dépend que de M, est appelée la classe de Steinitz de M, et on la note $cl_k(M)$.

La structure de M, en tant que O_k-module, est complètement déterminée par son rang et sa classe de Steinitz ; par exemple, M est un O_k-module libre si, et seulement si, $cl_k(M) = 1$. Ceci s'applique en particulier à $M = O_K$, où K/k est une extension finie de corps de nombres de degré n ; on dira aussi que $cl_k(O_K)$ est la classe de Steinitz de K/k.

Soit Γ un groupe fini. On désigne par $R_m(k, \Gamma)$ (m pour modéré) l'ensemble des classes c de $Cl(k)$ telles qu'il existe une extension galoisienne modérément ramifiée N/k, à groupe de Galois isomorphe à Γ, avec $cl_k(O_N) = c$. Nous dirons que $R_m(k, \Gamma)$ est l'ensemble des classes de Steinitz réalisables.

On conjecture que $R_m(k, \Gamma)$ est un sous-groupe de $Cl(k)$ (voir par exemple [2, Conjecture 3, p. 6], ou [3, Conjecture 1.2]). Signalons que cette conjecture est vraie lorsque Γ est abélien, car, dans ce cas, c'est une conséquence de [16, Théorème 6.17, p. 289]. Signalons aussi que l'étude de $R_m(k, \Gamma)$ est étroitement liée à celle de l'ensemble des classes galoisiennes réalisables (voir [2, §1], ou [3, §1]).

Le but du présent article est la poursuite de l'étude de $R_m(k, \Gamma)$ et d'un problème de plongement en liaison avec la donnée de classes de Steinitz, dans la situation non abélienne, dans le cas où Γ est un 2-groupe fini non trivial. Le point de départ était la lecture des articles [8, 9, 10, 11], en vue de généraliser les résultats de [19] aux groupes non abéliens d'ordre 32 ou 64.

Le premier résultat principal est le théorème suivant.

Théorème 1.1. *Soient k un corps de nombres et Γ un 2-groupe fini non trivial (abélien ou non). Si le nombre de classes de k est impair, alors $R_m(k, \Gamma)$ est égal au groupe $Cl(k)$.*

Dans la situation où Γ est un 2-groupe non abélien, ce théorème généralise des résultats antérieurs dans [21, Théorème 1.1(ii), p. 48], [22, Théorème 1.3(ii), p. 369], [19, Théorème 1.2, p. 1772], dans les cas respectifs où Γ est un groupe quaternionien d'ordre 8, ou diédral d'ordre 8, ou un groupe non abélien d'ordre 16 ou un groupe extraspécial d'ordre 32.

Le but de ce qui suit est de motiver l'énoncé d'un corollaire du théorème 1.1. Supposons maintenant Γ abélien fini quelconque. En ce qui concerne la description explicite de $R_m(k, \Gamma)$, il est difficile de la déduire de [16, Théorème 6.17]. Il y en a une seule connue pour les 2-groupes, c'est celle donnée par L. P. Endo, dans le cas d'un 2-groupe cyclique d'ordre 2^n, sous l'hypothèse que $Gal(k(\zeta_{2^n})/k)$ est cyclique, où ζ_{2^n} est une racine primitive 2^n-ième de l'unité (voir [3, Appendice, Théorème A.7(1), p. 343] ou [4, Théorème 1.1]) ; notons qu'on en peut déduire, pour k quelconque, que $R_m(k, \mathbb{Z}/2\mathbb{Z}) = Cl(k)$ (c'est immédiat), et $R_m(k, \mathbb{Z}/4\mathbb{Z}) = Cl(k)$ (voir [3, Proposition 2.6]). L. P. Endo a donné aussi une description explicite de $R_m(k, \Gamma)$ lorsque l'ordre de Γ est impair (voir [3, Appendice, Théorème A.7 (2)]

ou [4, Théorème 4.1]). Dans la dernière section de [4], on montre que la description explicite de $R_m(k,\Gamma)$, lorsque Γ est d'ordre pair, se ramène à celle où Γ est un 2-groupe cyclique (voir [4, Théorèmes 4.2 et 4.3]). Notre corollaire du théorème 1.1 est le suivant:

Corollaire 1.2. *Soient k un corps de nombres et Γ un groupe abélien fini. Si l'ordre de Γ est pair et est premier avec le nombre de classes de k, alors $R_m(k,\Gamma) = Cl(k)$.*

Remarques.

(a) Par la théorie du corps de classes, l'ordre o de Γ est premier avec le nombre de classes h de k si, et, seulement si, pour tout diviseur premier p de o, toute extension cyclique de k de degré p est ramifiée en au moins une place (finie ou infinie) ; pour le voir, il suffit d'utiliser le corps de classes de Hilbert de k.

(b) Si l'on remplace, dans le corollaire 1.2, pair par impair, l'assertion résultante n'est pas vraie. En effet: Soit p un nombre premier impair. Un cas particulier du résultat d'Endo [3, Théorème A.7 (2)] est: $R_m(k,\mathbb{Z}/p\mathbb{Z}) = N_{k(\zeta_p)/k}(Cl(k(\zeta_p))^{(p-1)/2}$, où ζ_p est une racine primitive p-ième de l'unité (en fait, ce cas est un ancien théorème de R. Long paru dans Crelle (250), 1971, pp. $87-98$). Si p est non ramifié dans $k/\mathbb{Q}$, alors toute sous-extension de $k(\zeta_p)/k$, différente de k, est ramifiée, et donc $N_{k(\zeta_p)/k}(Cl(k(\zeta_p)) = Cl(k)$ par [23, Théorème 10.1, p. 400] ; d'où (dans ce cas): $R_m(k,\mathbb{Z}/p\mathbb{Z}) = Cl(k)$ si, et seulement si, h est premier avec $(p-1)/2$. Prenons $p = 5$ et $k = \mathbb{Q}(\sqrt{-13})$, alors $h = 2$ (par une table dans la littérature) et $R_m(k,\mathbb{Z}/5\mathbb{Z}) = \{1\} \neq Cl(k)$.

Dans toute la suite, on identifiera fréquemment des groupes isomorphes quand il n'y a aucune confusion possible, et l'on désignera par C_2, C_4, les groupes cycliques d'ordres respectifs 2, 4, et D_4 le groupe diédral d'ordre 8.

Si Γ est un 2-groupe fini d'ordre o, on note $\Gamma = \Gamma_{(o,m,n)}$, où m est le numéro de Γ dans la liste de Hall-Senior (voir [12]), et n est celui de Γ dans la liste des petits groupes de GAP (voir [6]).

Dans la perspective de l'étude des classes galoisiennes réalisables lorsque Γ est un 2-groupe fini, et en vue de généraliser le théorème 1.1 de [19] pour une famille infinie de 2-groupes, le deuxième résultat principal est le théorème suivant.

Théorème 1.3. *Soit k un corps de nombres. Soit Γ un 2-groupe défini par l'une des extensions centrales non scindées suivantes:*

$$1 \to C_2 \to \Gamma \to (C_2)^r \times (C_4)^s \times (D_4)^t \to 1, \tag{1}$$

$$1 \to C_2 \times C_2 \to \Gamma \to (C_2)^r \times (C_4)^s \times (D_4)^t \to 1, \tag{2}$$

$$1 \to C_4 \to \Gamma \to D_4 \to 1, \tag{3}$$

où r, s et t sont des entiers naturels, et dans (3), $\Gamma = \Gamma_{(32,32,15)}$. Alors, pour tout $c \in Cl(k)$, il existe une extension quadratique de k, modérément ramifiée dont la classe de Steinitz est c, et qui est plongeable dans une extension galoisienne N/k à groupe de Galois isomorphe à Γ.

Remarques.

(a) Nous savons dire, pour une bonne proportion de ces groupes Γ, qu'on peut choisir N/k modérée. Pour ne pas alourdir l'énoncé du théorème 1.3, nous avons préféré le préciser dans la section 2.

(b) Soit Γ un groupe fini. Soient $\mathcal{M}$ un O_k-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$ et $Cl(\mathcal{M})$ son groupe des classes. Soit $\mathcal{R}(\mathcal{M})$ l'ensemble des classes galoisiennes réalisables $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ dans $Cl(\mathcal{M})$, où N/k est modérée à groupe de Galois isomorphe à Γ. La classe de $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ se calcule à l'aide des classes de Steinitz d'extensions intermédiaires de N/k, et la determination de la structure de $\mathcal{R}(\mathcal{M})$ se fait grâce à la résolution d'un problème de plongement en lien avec la donnée de classes de Steinitz (voir par exemple [2]).

(c) Le but principal de l'article [9] est l'étude de la réalisabilité de $\Gamma_{(32,32,15)}$ comme groupe de Galois.

A isomorphisme près, il y a 51 groupes d'ordre 32 (dont 7 abéliens et 11 produits directs non abéliens) et 267 groupes d'ordre 64 (dont 11 abéliens et 56 produits directs non abéliens) (voir [6]).

Corollaire 1.4. *Le théorème 1.3 s'applique à* 22 *(resp.* 134*) groupes* Γ *d'ordre* 32 *(resp.* 64*) qui sont définis par des extensions centrales de la forme* (1) *ou* (2). *(Ces groupes sont dans les tables* 1 *et* 2 *de la section* 2.*)*

Remarque. Le but principal de l'article [8] est l'étude de 13 groupes satisfaisant (1) parmi les 22 ; les 9 restants, qui vérifient (2), sont étudiés dans [10]. Les 134 groupes d'ordre 64 sont ceux étudiés dans [11].

2. Démonstration des résultats principaux

Nous commençons par fixer quelques notations et rappeler, brièvement, des résultats connus qui seront utiles pour la démonstration de nos principaux théorèmes. Ces résultats se trouvent déjà dans [19] ; nous les rappelons ici rapidement pour la convenance du lecteur.

Soit k un corps de nombres. Si $\mathfrak{p}$ est un idéal premier de O_k, $v_\mathfrak{p}$ désigne la valuation en $\mathfrak{p}$.

Soit $\mathcal{C}$ un cycle de k ; $Cl(k, \mathcal{C})$ désigne le groupe de classes de rayon de k modulo $\mathcal{C}$. La classe d'un idéal fractionnaire I de O_k dans $Cl(k, \mathcal{C})$ est notée $cl(I)$. Le cycle $\prod_{\sigma(k)\subset\mathbb{R}} \sigma$, où σ parcourt l'ensemble des plongements réels de k , est noté $\mathcal{C}_\infty$. Soit $x \in k^\times = k\backslash\{0\}$; l'écriture $x \equiv 1 \ mod^* \ \mathcal{C}$ est la notation de la congruence mod^* usuelle de la théorie du corps de classes. Si K/k est une extension finie de

corps de nombres, on désigne par $[K : k]$ son degré, $\Delta(K/k)$ son discriminant et $N_{K/k}$ sa norme. On rappelle que $cl_k(O_K)$ est la classe de Steinitz de K/k.

Soit $k \subset K \subset M$ une tour de corps de nombres. On rappelle un théorème de Fröhlich concernant la transitivité de la classe de Steinitz dans une tour de corps de nombres (voir [5, Theorem 4.1]):

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

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

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

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

Soit K/k une extension quadratique. D'après la théorie de Kummer, K/k est modérée si, et seulement si, on peut choisir $x \in k^\times$ tel que:

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

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

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

et par un théorème d'Artin (voir[1]) on a:

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

Soient $a, b \in k^\times$; $(\frac{a,b}{k})$ est l'algèbre des quaternions sur k définie par a et b. On notera (a, b) sa classe dans le groupe de Brauer $Br(k)$ de k. Rappelons que $(a, b)^2 = 1$ dans $Br(k)$, et que $(a, b) = 1$ dans $Br(k)$, si, et seulement si, la forme quadratique $\langle a, b\rangle$ sur k représente 1 ; condition équivalente à b est une norme dans l'extension $k(\sqrt{a})/k$.

Soient v une place de k et $a, b \in k^\times$; $(a, b)_v$ est le symbole (local) de Hilbert (voir [20, Chapitre XIV, cas $n = 2$]). Rappelons que $(a, b)_v = 1$ ou -1, et pour que $(a, b)_v = 1$, il faut et il suffit que la forme quadratique $< a, b >$ sur le complété k_v de k représente 1 ; condition équivalente à b est une norme (locale) dans l'extension $k_v(\sqrt{a})/k_v$. La formule du produit nous dit qu'on a: $\prod_{v \text{ place de } k}(a, b)_v = 1$.

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

Si v est complexe, alors $(a, b)_v = 1$.

Si v est réelle, alors $(a, b)_v = 1$ si a ou b est totalement positif.

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

Soit

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

et soit $\overline{c}$ la classe de c dans $\overline{k_\mathfrak{p}}$.

Supposons que $\mathfrak{p}$ ne soit pas au dessus de 2. Alors (voir [20, Proposition 8 et son corollaire, p. 217]):

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

Supposons maintenant que $\mathfrak{p}$ soit au dessus de 2, et soit $e = v_{\mathfrak{p}}(2O_k)$ son indice de ramification absolu. Si $v_{\mathfrak{p}}(a-1) \geqslant 2e$, alors (voir [20, Proposition 6, p. 237]):

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

où Tr désigne la trace et $\overline{(a-1)/4}$ est la classe de $(a-1)/4$ dans $\overline{k_{\mathfrak{p}}}$.

Le théorème de Hasse-Minkowski nous dit qu'une forme quadratique $\langle a,b\rangle$ sur k représente un élément x de k si, et seulement si, pour toute place v de k, la forme quadratique $\langle a,b\rangle$ sur le complété k_v de k représente x. Donc: pour que $(a,b)=1$, il faut et il suffit que pour toute place v de k, $(a,b)_v = 1$.

Démonstration du théorème 1.1. Soit k un corps de nombres. Soit Γ un 2-groupe fini non trivial. Puisque Γ est résoluble, d'après le théorème de Shafarevich (voir [18, Théorème 9.6.1, p. 574, et Exercice (b), p. 597], ou [14, Théorème 6.1, p. 15]), il existe une extension galoisienne N/k, modérée dont le groupe de Galois est isomorphe à Γ. Soit $Z(\Gamma)$ le centre de Γ. Comme $Z(\Gamma)$ est non trivial (puisque Γ est un p-groupe) et 2 est un diviseur de son ordre, il existe $\sigma \in Z(\Gamma)$ d'ordre 2 (par le théorème de Cauchy). Soit E/k la sous-extension galoisienne de N/k fixe par σ.

Soit $c \in Cl(k)$. Considérons c^{-1} et le cycle $4O_k$. Par la surjection canonique de $Cl(k,4O_k)$ sur $Cl(k)$, qui à $cl(I)$ dans $Cl(k,4O_k)$ associe $cl(I)$ dans $Cl(k)$, il existe un idéal fractionnaire I de O_k, premier avec $4O_k$, qui est dans c^{-1} et donc on a une classe $cl(I)$ dans $Cl(k,4O_k)$. D'après le théorème de densité de Tchebotarev, il existe un idéal premier $\mathfrak{p}$ de O_k, premier avec $4O_k$ et le discriminant de N/k, et vérifiant $cl(I)^{-2} = cl(\mathfrak{p})$ dans $Cl(k,4O_k)$. Donc, il existe $r \in k$ tel que:

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

D'après les rappels, l'extension $k(\sqrt{r})/k$ est quadratique modérée de discriminant $\mathfrak{p}$ et classe de Steinitz c. Il est clair que N/k et $k(\sqrt{r})/k$ sont arithmétiquement disjointes (i.e., linéairement disjointes et leurs discriminants sont premiers entre eux).

Soit $N' = Nk(\sqrt{r})$ la composée de N/k et $k(\sqrt{r})/k$. Soit $\gamma \in E$ tel que $N = E(\sqrt{\gamma})$ (N/E est quadratique). L'extension N'/E étant biquadratique, elle contient une troisième sous-extension quadratique $N_r = E(\sqrt{r\gamma})/E$. Soit τ un générateur de $Gal(k(\sqrt{r})/k)$. Sous l'isomorphisme $Gal(N'/k) \simeq \Gamma \times Gal(k(\sqrt{r})/k)$ (N/k et $k(\sqrt{r})/k$ sont linéairement disjointes), N_r/k est la sous-extension de N'/k fixe par (σ,τ). Comme (σ,τ) appartient au centre de $Gal(N'/k)$, N_r/k est galoisienne. Il est immédiat que N_r/k et $k(\sqrt{r})/k$ sont linéairement disjointes et leur composée est N'/k. On en déduit que $Gal(N_r/k) \simeq \Gamma$. L'extension N'/k est modérée, car c'est une composée de deux extensions modérées. Par conséquent N_r/k est modérée, puisque c'est une sous-extension de N'/k.

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

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

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

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

On a la décomposition:

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

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

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

Par conséquent:

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

D'où $A = \{cl_k(O_N)c^{[E:k]} \mid c \in Cl(k)\} \subset R_m(k,\Gamma)$.

Supposons le nombre de classes de k impair. Alors $A = Cl(k)$, car $[E : k]$ est une puissance de 2, et donc $R_m(k,\Gamma) = Cl(k)$. Ceci termine la preuve du théorème 1.1. ∎

Démonstration du corollaire 1.2. Soient k un corps de nombres et Γ un groupe abélien fini. Supposons Γ d'ordre pair $o = 2^r s$, où s est impair. Si p est un diviseur premier de o, notons $\Gamma(p)$ le p-sous-groupe de Sylow de Γ. Rappelons que $R_m(k,\Gamma(p))$ est un sous-groupe de $Cl(k)$, car $\Gamma(p)$ est abélien. D'après [4, Corollaire 4.3], $R_m(k,\Gamma) = \prod_{p|o} R_m(k,\Gamma(p))^{o/p^{v_p(o)}}$, où p parcourt l'ensemble des diviseurs premiers de o. On en déduit que $R_m(k,\Gamma(2))^s \subset R_m(k,\Gamma)$.

Supposons o premier avec le nombre de classes h de k. L'entier h étant impair, le théorème 1.1 nous donne $R_m(k,\Gamma(2)) = Cl(k)$. Comme s est premier avec h, $Cl(k)^s = Cl(k)$. Donc $R_m(k,\Gamma) = Cl(k)$. ∎

Le lemme suivant sera utile pour la démonstration du théorème 1.3.

Lemme 2.1. *Soit k un corps de nombres. Soit $n > 0$ un entier naturel. Soient c_i, $1 \leqslant i \leqslant n$, des éléments de $Cl(k)$. Alors:*

(1) *Il existe n éléments a_i de k, n idéaux premiers $\mathfrak{p}_i$ de O_k deux à deux distincts et ne divisant pas $2O_k$, et n idéaux fractionnaires I_i de k satisfaisant:*

- *pour tout i et j, $1 \leqslant i,j \leqslant n$, $v_{\mathfrak{p}_i}(I_j) = 0$,*
- *pour tout i, $1 \leqslant i \leqslant n$, $a_i O_k = I_i^2 \mathfrak{p}_i$ et $c_i = cl(I_i)^{-1}$,*
- *$a_1 \equiv 1 \mod^* \mathcal{C}_\infty 8O_k$ et pour tout i, $2 \leqslant i \leqslant n$, $a_i \equiv 1 \mod^* \mathcal{C}_\infty 8 \prod_{j=1}^{i-1} \mathfrak{p}_j$.*

(2) *Les éléments a_i, $1 \leqslant i \leqslant n$, de (1) sont quadratiquement indépendants (i.e., $\{\overline{a_i}, 1 \leqslant i \leqslant n\} \subset$ le $\mathbb{F}_2$-espace vectoriel $k^\times/(k^\times)^2$ est $\mathbb{F}_2$-libre) et vérifient: pour tout i et j, $1 \leqslant i,j \leqslant n$, $(a_i,a_j) = 1$ et $(2,a_i) = 1$.*

Démonstration. (1) Soient k un corps de nombres, n un entier naturel non nul et c_i, $1 \leqslant i \leqslant n$, des éléments de $Cl(k)$.

Considérons c_1^{-1} et le cycle $\mathcal{C}_\infty 8O_k$. Par la surjection canonique de $Cl(k, \mathcal{C}_\infty 8O_k)$ sur $Cl(k)$, qui à $cl(I)$ dans $Cl(k, \mathcal{C}_\infty 8O_k)$ associe $cl(I)$ dans $Cl(k)$, il existe un idéal fractionnaire I_1 de O_k, premier avec $8O_k$, qui est dans c_1^{-1} et donc on a une classe $cl(I_1)$ dans $Cl(k, \mathcal{C}_\infty 8O_k)$. D'après le théorème de densité de Tchebotarev, il existe un idéal premier $\mathfrak{p}_1$ de O_k tel que $v_{\mathfrak{p}_1}(2O_k) = v_{\mathfrak{p}_1}(I_1) = 0$, et vérifiant $cl(I_1)^{-2} = Cl(\mathfrak{p}_1)$ dans $Cl(k, \mathcal{C}_\infty 8O_k)$. Par conséquent, il existe $a_1 \in k$ tel que:

$$a_1 O_k = I_1^2 \mathfrak{p}_1, \qquad a_1 \equiv 1 \ mod^*\ \mathcal{C}_\infty 8O_k, \qquad c_1 = cl(I_1)^{-1}.$$

En considérant c_2^{-1} et le cycle $\mathcal{C}_\infty 8\mathfrak{p}_1$, et en procédant comme ci-dessus, on obtient: Il existe un idéal fractionnaire I_2 de O_k, premier avec $8\mathfrak{p}_1$ (donc $v_{\mathfrak{p}_1}(I_2) = 0$), appartenant à c_2^{-1} et on a une classe $cl(I_2) \in Cl(k, \mathcal{C}_\infty 8\mathfrak{p}_1)$. Il existe un idéal premier $\mathfrak{p}_2$ de O_k avec $v_{\mathfrak{p}_2}(2\mathfrak{p}_1) = v_{\mathfrak{p}_2}(I_1) = v_{\mathfrak{p}_2}(I_2) = 0$, et satisfaisant $cl(I_2)^{-2} = Cl(\mathfrak{p}_2)$ dans $Cl(k, \mathcal{C}_\infty 8\mathfrak{p}_1)$. Donc il existe un élément a_2 de $k^\times$ tel que:

$$a_2 O_k = I_2^2 \mathfrak{p}_2, \qquad a_2 \equiv\ 1 \ mod^*\ \mathcal{C}_\infty 8\mathfrak{p}_1, \qquad c_2 = cl(I_2)^{-1}.$$

Notons qu'on a $\mathfrak{p}_1 \neq \mathfrak{p}_2$, et pour tout i et j, $1 \leqslant i, j \leqslant 2$, $v_{\mathfrak{p}_i}(I_j) = 0$.

En réitérant ce procédé, qui s'arrête au bout d'un nombre fini de n étapes, on obtient la partie (1) du lemme.

(2) Soient e_i, $1 \leqslant i \leqslant n$, des éléments de $\mathbb{Z}$, et $x = \prod_{i=1}^n a_i^{e_i}$. Supposons que x soit un carré dans k. Comme $v_{\mathfrak{p}_i}(I_j) = 0$ (par (1)), il est immédiat que $v_{\mathfrak{p}_i}(a_j) = v_{\mathfrak{p}_i}(\mathfrak{p}_\mathfrak{j})$; de plus $v_{\mathfrak{p}_i}(\mathfrak{p}_\mathfrak{j}) = 1$, si $i = j$, et 0 sinon, car les $\mathfrak{p}_i$ sont distincts deux à deux. On en déduit que $v_{\mathfrak{p}_i}(x) = e_i \equiv 0 \bmod 2$. Donc les a_i, $1 \leqslant i \leqslant n$, sont quadratiquement indépendants.

Montrons maintenant la deuxième partie de l'assertion (2).

Soit v une place archimédienne de k. Soient i et j, $1 \leqslant i, j \leqslant n$.

Si v est complexe, alors

$$(a_i, a_j)_v = 1, \qquad (a_i, 2)_v = 1.$$

Si v est réelle, alors

$$(a_i, a_j)_v = 1, \qquad (a_i, 2)_v = 1,$$

car les a_i sont totalement positifs par les congruences $(mod^*\ \mathcal{C}_\infty)$ qu'ils vérifient.

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

Si $\mathfrak{p}$ est au dessus de 2 et e est son indice de ramification absolu, les congruences que vérifient les a_i entraînent: $v_\mathfrak{p}(a_i - 1) \geqslant v_\mathfrak{p}(8O_k) = 3e \geqslant 2e$. Donc:

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

Il est immédiat que $v_\mathfrak{p}((a_i - 1)/4) \geqslant e$. Par conséquent la classe de $(a_i - 1)/4$ dans le corps résiduel $\overline{k_\mathfrak{p}}$ est égale à 0. Par suite $m(a_i) = 0$ dans $\mathbb{F}_2$, et donc les deux symboles précédents sont égaux à 1.

Supposons maintenant que $\mathfrak{p}$ ne soit pas au dessus de 2.
Si $\mathfrak{p} \neq \mathfrak{p}_i$ et $\mathfrak{p} \neq \mathfrak{p}_j$, alors $(a_i, a_j)_{\mathfrak{p}} = 1$, car $v_{\mathfrak{p}}(a_i)$ et $v_{\mathfrak{p}}(a_j)$ sont paires.
Si $i = j$, alors $(a_i, a_i)_{\mathfrak{p}_i} = 1$ par la formule du produit. D'où $(a_i, a_i) = 1$.
Supposons $i \neq j$. Si $j < i$ et $\mathfrak{p} = \mathfrak{p}_j$, alors

$$(a_i, a_j)_{\mathfrak{p}_j} = (\overline{a_i})^{v_{\mathfrak{p}_j}(a_j)(N_{k/\mathbb{Q}}(\mathfrak{p}_j)-1)/2} = (\overline{a_i})^{(N_{k/\mathbb{Q}}(\mathfrak{p}_j)-1)/2}$$

dans $\overline{k_{\mathfrak{p}_j}}$, car $v_{\mathfrak{p}_j}(a_i) = 0$ et $v_{\mathfrak{p}_j}(a_j) = 1$ (rappelons que $v_{\mathfrak{p}_j}(a_i) = v_{\mathfrak{p}_j}(\mathfrak{p}_i)$). On a $(a_i, a_j)_{\mathfrak{p}_j} = 1$, parce que $\overline{a_i} = 1$ dans $\overline{k_{\mathfrak{p}_j}}$ par la congruence $(mod^*\ \mathfrak{p}_j)$ qu'il vérifie. La formule du produit nous donne $(a_i, a_j)_{\mathfrak{p}_i} = 1$. Il s'ensuit que $(a_i, a_j) = 1$, si $j < i$. Comme $(a_i, a_j) = (a_j, a_i)$, on en déduit que pour tout $i \neq j$, $(a_i, a_j) = 1$

Puisque $v_{\mathfrak{p}}(2) = 0$, on a

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

Si $\mathfrak{p} \neq \mathfrak{p}_i$, alors $(a_i, 2)_{\mathfrak{p}} = 1$, car $v_{\mathfrak{p}}(a_i)$ est paire. Par la formule du produit on a $(a_i, 2)_{\mathfrak{p}_i} = 1$. On conclut que $(a_i, 2) = 1$. Ceci termine la démonstration de (2). ■

Remarques.

(a) Si $x \in k^\times$, alors $(-x, x) = 1$ (c'est bien connu), d'où $(x, x) = (-1, x)$. Donc pour tout i, $1 \leqslant i \leqslant n$, $(-1, a_i) = (a_i, a_i) = 1$.
(b) Il est immédiat que pour tout i, $1 \leqslant i \leqslant n$, l'extension $k(\sqrt{a_i})/k$ est quadratique, modérée et de classes de Steinitz c_i.

Démonstration du théorème 1.3. Soient k un corps de nombres et Γ un 2-groupe.

(1) Dans cette partie, on traite le cas où Γ est une extension centrale non scindée du groupe produit $G = (C_2)^r \times (C_4)^s \times (D_4)^t$ par C_2, ou par $C_2 \times C_2$.

Soit E/k une extension galoisienne à groupe de Galois isomorphe à G. Soient E_i/k, $1 \leqslant i \leqslant 3$, les sous-extensions de E/k de groupes de Galois respectifs $(C_2)^r, (C_4)^s, (D_4)^t$, de sorte que E/k soit la composée des E_i/k. En utilisant le lemme 2.1 précédent, et convenablement [10, Théorème 2.1] et [8, Théorème 1], on obtient notre théorème 1.3 dans les deux cas considérés dans cette partie.

Précisons que [10, Théorème 2.1] est déduit d'un résultat dans [13], et [8, Théorème 1] est une application du [15, Corollaire 2.5].

Pour alléger la preuve, nous la faisons seulement dans le cas où $r = s = t = 1$; le cas général se traite d'une manière similaire.

Prenons $n = 4$ dans le lemme 2.1 ; soient c_i et a_i , $1 \leqslant i \leqslant 4$, les éléments respectifs de $Cl(k)$ et k définis dans ce lemme. Nous utiliserons ci-dessous le fait que $(-1, a_i) = 1$, $(a_i, a_j) = 1$ si $i \neq j$, et $(2, a_i) = 1$.

Posons $E_1 = k(\sqrt{a_1})$.

Puisque $(-1, a_2) = 1$ (condition équivalente à a_2 est somme de deux carrés dans k), l'extension quadratique $k(\sqrt{a_2})/k$ est plongeable dans une extension cyclique de degré 4 (voir par exemple [7]). Soient x, $y \in k^\times$ tels que $a_2 = x^2 + y^2$.

Posons $a_0 = a_2/x^2$. Il est bien connu que toute extension cyclique de k, de degré 4 et contenant $k(\sqrt{a_2})$, peut s'écrire sous la forme $k(\sqrt{q_2(a_0+\sqrt{a_0})}) := E_{2,q_2}$, où q_2 parcourt $k^\times$ (voir par exemple [7]). Il est clair que $k(\sqrt{a_2}) = k(\sqrt{a_0})$, et pour tout $z \in k^\times$, $(a_0, z) = (a_2, z)$.

Comme a_3 et a_4 sont quadratiquement indépendants en vertu du lemme 2.1, l'extension $k(\sqrt{a_3}, \sqrt{a_4})/k$ est biquadratique. De $(a_3, a_3) = (a_3, a_4) = 1$ et $(a_3, a_3a_4) = (a_3, a_3)(a_3, a_4)$ découle $(a_3, a_3a_4) = 1$ (condition équivalente à a_3a_4 est une norme dans $k(\sqrt{a_3})$). Par suite $k(\sqrt{a_3}, \sqrt{a_4})/k$ est plongeable dans une extension diédrale de degré 8 (cyclique sur $k(\sqrt{a_4})$). Il est bien connu que toutes les solutions de ce problème de plongement s'écrivent sous la forme: $k(\sqrt{q_3(\alpha_3+\beta_3\sqrt{a_3})}, \sqrt{a_4}) := E_{3,q_3}$, où q_3 parcourt $k^\times$, et α_3 et β_3 sont des éléments de k satisfaisant: $a_3a_4 = N_{k(\sqrt{a_3})/k}(\alpha_3+\beta_3\sqrt{a_3}) = \alpha_3^2 - a_3\beta_3^2$ (voir par exemple [7]).

On désigne par $E_{q_2,q_3}/k$ la composée des extensions galoisiennes E_1/k, E_{2,q_2} et E_{3,q_3}. Puisque les a_i, $1 \leqslant i \leqslant 4$, sont quadratiquement indépendants par le lemme 2.1, il est immédiat que $Gal(E_{q_2,q_3}/k) = C_2 \times C_4 \times D_4 = G$.

1.1. Supposons que Γ soit une extension centrale de G par C_2:

$$1 \to C_2 \to \Gamma \to G \to 1.$$

D'après [8, Théorème 1] et sa démonstration, l'extension $E_{q_2,q_3}/k$ est plongeable dans une extension N/k à groupe de Galois Γ si

$$(-1,a_1)^{d_1}[(2,a_2)(-1,q_2)]^{d_2}[(-2,a_3)(-a_4,2\alpha_3q_3)]^{d_3}(-1,a_4)^{e_3}(-1,a_3)^{f_3} \times \prod_{i<j\leqslant 3}(a_i,a_j)^{d_{ij}} \prod_{i<3}(a_i,a_4)^{e_{i3}} = 1, \quad (4)$$

où les entiers qui figurent dans les puissances sont déterminés par la structure de Γ, et $\alpha_3 \neq 0$ car $-a_4$ n'est pas un carré dans k ($v_{\mathfrak{p}_4}(-a_4) = 1$).

Prenons $q_2 = 1$, et $q_3 = (2\alpha_3)^{-1}$ (de sorte que $2\alpha_3q_3 = 1$). Par l'assertion (2) du lemme 2.1, il est alors immédiat que l'élément de $Br(k)$, figurant dans le membre de gauche de l'égalité (4) précédente, est égal à 1. Donc $E_{1,(2\alpha_3)^{-1}}/k$ est plongeable dans une extension N/k à groupe de Galois Γ, qui n'est pas nécessairement modérée à cause du choix de q_2 et q_3. Elle contient $k(\sqrt{a_1})/k$ de classe de Steinitz c_1, d'où le théorème 1.3 dans ce premier cas.

1.2. Supposons maintenant que Γ soit une extension centrale de G par $C_2 \times C_2$:

$$1 \to C_2 \times C_2 \to \Gamma \to G \to 1.$$

Notons $C_2 = \{1, -1\}$, et soient x et y les images respectifs des éléments $(-1, 1)$ et $(1, -1)$ de $C_2 \times C_2$ dans Γ. D'après [10, Théorème 2.1], l'extension $E_{q_2,q_3}/k$ est plongeable dans une extension N/k à groupe de Galois Γ si elle est, à la fois, plongeable dans une extension N_1/k à groupe de Galois $\Gamma/\langle x\rangle$ et dans une extension N_2/k à groupe de Galois $\Gamma/\langle y\rangle$. Les groupes $\Gamma/\langle x\rangle$ et $\Gamma/\langle y\rangle$ étant des extensions centrales de G par C_2, on est ramené à la situation 1.1. La condition de plongement est décrite par deux éléments de $Br(k)$, ayant exactement la mẹme

forme de décomposition que l'élément de $Br(k)$ figurant dans le membre de gauche de l'égalité (4) dans 1.1, mais avec des puissances éventuellement différentes. Avec le choix $q_2 = 1$ et $q_3 = (2\alpha_3)^{-1}$, on en déduit que ces deux éléments sont triviaux dans $Br(k)$ par le même calcul qu'en **1.1**. Du coup on conclut comme dans 1.1.

(2) Dans cette partie, on traite le cas où $\Gamma = \Gamma_{(32,32,15)}$ est une extension centrale non scindée du groupe D_4 par C_4:

$$1 \to C_4 \to \Gamma \to D_4 \to 1.$$

Reprenons l'extension diédrale de degré 8 de la partie (1):

$$E_{3,q_3} = k(\sqrt{q_3(\alpha_3 + \beta_3\sqrt{a_3})}, \sqrt{a_4})/k.$$

Notons $q_3 = q$, $E_{3,q_3} = E_q$, $\alpha_3 = \alpha$, $a_3 = a$ et $a_4 = b$.

2.1. Si i $(= \zeta_4) \in k$, où $i^2 = -1$, d'après l'assertion 1 du théorème 8 de [9] et sa démonstration, E_q/k est plongeable dans une extension N_q/k à groupe de Galois Γ, si $(a,2)(b,q\alpha) = 1$. Rappelons que $\alpha \neq 0$ et prenons $q = \alpha^{-1}$. Puisque $(a,2)(b,1) = 1$, $Gal(N_{\alpha^{-1}}/k) = \Gamma$. On a le théorème 1.3, car l'extension $k(\sqrt{a})/k$, de classe de Steinitz c_3, est contenue dans $N_{\alpha^{-1}}/k$.

2.2. Supposons que $i \notin k$. Il est immédiat que a, b et -1 sont quadratiquement indépendants. Par le lemme 2.1, $(b,-1) = 1$. D'après le premier point de l'assertion 2 du théorème 8 de [9] et sa démonstration, E_q/k est plongeable dans une extension N_q/k à groupe de Galois Γ, si $(a,2)(b,q\alpha) = 1$ dans $Br(k(i))$. Prenons $q = \alpha^{-1}$. Comme $(a,2) = 1$ dans $Br(k)$ (par le lemme 2.1), on a aussi $(a,2) = 1$ dans $Br(k(i))$. Donc $Gal(N_{\alpha^{-1}}/k) = \Gamma$ et on conclut comme dans 2.1. ■

Nous allons maintenant préciser la remarque (a), se trouvant juste après le théorème 1.3, dans la section 1. Revenons à la partie (1) de la démonstration précédente. Puisque les extensions $k(\sqrt{a_2})/k$ et $k(\sqrt{a_3}, \sqrt{a_4})/k$ sont modérées, et leurs problèmes de plongement respectifs correspondent à des extensions (de groupes) à noyaux abéliens, d'après [17, Théorème 6.6] il existe q_2 et q_3 tels que $E_{2,q_2}/k$ et $E_{3,q_3}/k$ soient modérées (i.e., il existe des plongements modérés). Donc $E_{q_2,q_3}/k$ est aussi modérée. Si Γ est tel que $d_2 = d_3 = 1$, alors l'élément de $Br(k)$ dans (4) de 1.1 est trivial. Donc $E_{q_2,q_3}/k$ est plongeable dans une extension à groupe de Galois Γ, qu'on peut choisir modérée, comme ci-dessus par [17, Théorème 6.6]. Il est facile de voir maintenant qu'à chaque fois que la condition de plongement ne contient pas d'éléments de $Br(k)$ définis à l'aide des q_i, le théorème 1.3 peut s'énoncer avec N/k modérée.

Notons aussi que dans la discussion précédente, avec l'hypothèse $i \in k$ on n'a pas besoin de supposer $d_2 = 1$, car $(-1,q_2) = (i^2,q_2) = 1$. On en déduit, comme ci-dessus, que lorsque le critère de plongement ne contient que des $(-1,q_j)$ comme éléments de $Br(k)$ définis à l'aide des q_j, et que $i \in k$, le théorème 1.3 peut s'énoncer avec N/k modérée.

Nous appliquons les précisions précédentes aux groupes d'ordre 32 ou 64 du corollaire 1.4, et nous donnons les résultats dans les deux tables suivantes.

Table 1: $\Gamma = \Gamma_{(64,m,n)} := (m, n)$

(30,57)*	(32,86)'	(106,199)*	(107,201)*	(108,200)*	(109,249)'	(105,266)*
(77,206)*	(78,213)*	(112,256)	(157,227)*	(158,231)*	(159,229)*	(160,228)*
(169,215)*	(170,216)*	(171,218)*	(172,217)*	(241,257)	(242,258)	(243,259)
(58,124)	(84,167)*	(85,71)*	(86,66)*	(88,70)*	(91,69)*	(92,68)*
(99,116)'	(100,117)'	(117,123)	(118,121)	(119,122)	(122,125)	.
(33,112)	(81,60)*	(82,65)*	(83,61)*	(87,72)*	(89,62)*	(90,63)*
(93,64)	(94,88)'	(95,104)'	(96,89)'	(97,105)'	(98,113)'	(101,127)'
(102,114)'	(79,214)*	(80,210)*	(161,235)	(162,238)*	(163,232)*	(164,234)*
(165,240)*	(166,236)*	(167,233)*	(168,237)*	(173,224)*	(174,225)*	(175,219)*
(176,221)*	(177,220)*	(178,223)*	(179,222)*	(183,242)*	(184,241)*	(185,243)*
(186,244)*	(187,245)*	(37,17)'	(38,3)'	(53,97)	(54,108)	(113,99)
(114,98)	(115,100)	(116,109)	(144,73)*	(145,76)*	(146,75)*	(147,74)*
(148,80)*	(149,79)*	(150,77)*	(151,78)	(152,81)	(188,174)	(189,173)
(190,181)	(191,179)	(192,175)	(193,167)	(194,168)	(195,147)	(196,146)
(197,148)	(198,176)	(199,180)	(200,169)	(201,128)	(202,131)	(203,129)
(204,132)	(205,140)	(206,141)	(207,155)	(208,142)	(209,157)	(210,156)
(211,143)	(212,158)	(213,161)	(214,162)	(215,164)	(216,165)	(217,130)
(218,133)	(219,144)	(220,145)	(221,159)	(222,160)	(223,163)	(224,166)
(225,177)	(226,178)	(227,182)	(228,150)	(229,149)	(230,151)	(231,171)
(232,170)	(233,172)					

Table 2: $\Gamma = \Gamma_{(32,m,n)} := (m, n)$

(16,24)*	(17,38)'	(19,4)'	(26,42)	(33,27)*	(34,34)*	(35,35)*
(36,28)*	(37,29)*	(38,30)*	(39,31)*	(44,43)	(45,44)	.
(18,2)*	(20,5)'	(21,12)'	(27,9)	(28,10)	(29,14)	(30,13)
(40,32)*	(41,33)*					

Pour les groupes d'ordre 32 (resp. 64) des conditions suffisantes de plongements se trouvent dans les tables [8, Table 2, p. 430] et [10, Table 3, p. 247] (resp. [11, Tables 1–8, pp. 850–853]). L'étoile * (resp. l'accent ') signifie qu'on peut énoncer le théorème 1.3 avec N/k modérée pour k quelconque (resp. contenant i).

Les 134 groupes d'ordre 64 de la table 1 sont ceux étudiés dans [11]. Les groupes des cinq premières lignes sont des extensions centrales par C_2, le reste par $C_2 \times C_2$. Il y a 55 groupes signalés par *, et 13 autres par '.

Les 13 groupes de [8] se trouvent dans les deux premières lignes de la table 2, et les 9 restants de [10] sont dans les deux dernières lignes. Il y a 11 groupes signalés par *, et 4 autres par '.

Références

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

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

[3] J. E. Carter, B. Sodaïgui, *Classes de Steinitz d'extensions quaternioniennes généralisées de degré* $4p^r$, J. London Math. Soc. (2) **76** (2007), 331–344.

[4] A. Cobbe, *Steinitz classes of some abelian and nonabelian extensions of even degree*, J. Théor. Nombres Bordeaux **22** (2010), no. 3, 607–628.

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

[6] GAP group, Algorithms and Programming, Version 4.4.9, 2006, http://www.gap-system.org.

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

[8] H.G. Grundman, G.L. Stewart, *Galois realizability of non-split group extensions of* C_2 *by* $(C_2)^r \times (C_4)^s \times (D_4)^t$, J. Algebra **272** (2004), 425–435.

[9] H.G. Grundman, T.L. Smith, *Galois realizability of a central* C_4*-extension of* D_8, J. Algebra **322** (2009), 3492–3498.

[10] H.G. Grundman, T.L. Smith, *Realizability and automatic realizability of Galois groups of order* 32, Cent. Eur. J. Math. **8** (2) (2010), 244–260.

[11] H.G. Grundman, T.L. Smith, *Galois Realizability of groups of order* 64, Cent. Eur. J. Math. **8** (5) (2010), 846–854.

[12] J.M. Hall, J.K. Senior, *The Groups of Order* 2^n *(*$n \leqslant 6$*)*, Macmillan, New York, 1964.

[13] V.V. Ishkhanov, B.B. Lur'e, D.K. Faddeev, *The Embedding Problem in Galois Theory*, Translations of Mathematical Monographs **165**, AMS, Providence, 1997.
[14] J. Klüners, G. Malle, *Counting nilpotent Galois extensions*, J. reine angew. Math. **572** (2004), 1–26.
[15] A. Ledet, *On* 2*-groups as Galois groups*, Can. J. Math. **47**(6) (1995), 1253–1273.
[16] L.R. McCulloh, *Galois module structure of abelian extensions*, J. reine angew. Math. **375/376** (1987), 259–306.
[17] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–16.
[18] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, second ed., Springer, Berlin-Heidelberg-New York, 2008.
[19] F. Sbeity, B. Sodaïgui, *Classes de Steinitz d'extensions non abéliennes à groupe de Galois d'ordre* 16 *ou extraspécial d'ordre* 32 *et problème de plongement*, Inter. J. Number Theory **6**, no. 8 (2010), 1769–1783.
[20] J.-P. Serre, *Corps Locaux*, 3ème édition, Hermann, Paris, 1980.
[21] 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.
[22] B. Sodaïgui, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, J. Algebra **223** (2000), 367–378.
[23] L.C. Washington, *Introduction to Cyclotomic Fields*, second ed., Springer-Verlag, Berlin, 1996.

Address: Bouchaïb Sodaïgui: Département de Mathématiques, Université de Valenciennes, Le Mont Houy, 59313 Valenciennes Cedex 9, France.

E-mail: bouchaib.sodaigui@univ-valenciennes.fr

Received: 3 July 2012