Extensions quadratiques 2-birationnelles de corps totalement réels*

Jean-François JAULENT et Odile SAUZET

Résumé. Nous caractérisons entièrement en termes de ramification les extensions quadratiques d'un corps de nombres totalement réel qui sont birationnelles. Cette étude complète un cas resté ouvert dans un travail antérieur sur les pro-ℓ-extensions de corps de nombres ℓ-rationnels.

Abstract. we characterize 2-birational CM-extensions of totally real number fields in terms of tame ramification. This result completes in this case a previous work on pro-ℓ-extensions over 2-rational number fields.

1. Position du problème

La notion de corps S-rationnel a été introduite dans [JSa], en liaison avec les résultats de [W1] et [W2], pour généraliser la notion de corps de nombres ℓ-rationnel rencontrée implicitement dans des contextes variés par plusieurs auteurs puis explicitement définie et étudiée par [MN] d'une part et [GJ] d'autre part (cf. [JN]). Rappelons ce dont il s'agit : si ℓ est un nombre premier et S un sous-ensemble non vide de l'ensemble Pl_K^ℓ des places de K au-dessus de ℓ, on dit que le corps de nombres K est S-rationnel lorsque le groupe de Galois $G_K = Gal(K'/K)$ de sa pro-ℓ-extension (galoisienne) ℓ-ramifiée maximale est le pro-ℓ-produit libre

$$G_K \simeq (\mathop{*}_{\substack{\mathfrak{p}|\ell\infty \\ \mathfrak{p}\notin S}} \mathcal{G}_\mathfrak{p}) * \mathcal{F}$$

des groupes de Galois locaux $\mathcal{G}_\mathfrak{p} = Gal(\bar{K}_\mathfrak{p}/K_\mathfrak{p})$ respectivement attachés aux pro-ℓ-extensions maximales $\bar{K}_\mathfrak{p}$ des completés $K_\mathfrak{p}$ de K aux places réelles ou ℓ-adiques qui ne sont pas dans S, et d'un pro-ℓ-groupe libre $\mathcal{F}$; dans ce cas, le nombre f de générateurs de $\mathcal{F}$ est donné par la formule

$$(ii) \qquad f = d - r - c - l + s + 1,$$

où d est la somme des degrés locaux $d = \sum_{\mathfrak{l}\in S}[K_\mathfrak{l} : \mathbb{Q}_\ell]$ et r, c, l, s sont respectivement les nombres de places réelles , complexes, ℓ-adiques ou dans S de K (cf [JSa]), th 2.7). Lorsque S est un singleton $\{\mathfrak{l}\}$, on parle de corps $\mathfrak{l}$-rationnel et si Pl_K^ℓ est lui même un singleton, on dit tout simplement que K est ℓ-rationnel. Dans ce dernier cas, si K contient en outre les racines ℓ-ièmes de l'unité, la condition (i) ci-dessus a lieu si et seulement si le ℓ-groupe

*J. Number Theory **65** (1997), 240–267.

$C\ell'_K$ des ℓ-classes de diviseurs de K (i.e. ici le quotient du ℓ-groupe des classes d'idéaux prises au sens restreint par le sous-groupe engendré par la classe de l'idéal premier au dessus de ℓ) est trivial, ce qui s'écrit

$$(iii) \qquad C\ell'_K = 1,$$

de sorte que la notion de ℓ-rationalité coïncide alors avec celle de ℓ-régularité introduite par Kummer dans l'étude des corps cyclotomiques $\mathbb{Q}[\zeta_\ell]$.

La question de la propagation de la S-rationalité dans une ℓ-extension L/K de corps de nombres a été complètement résolue dans [JSa] pour les ℓ impairs. Pour $\ell = 2$, en revanche, et L/K quadratique, il peut arriver que le corps de base K soit $\mathfrak{l}$-rationnel en une place 2-adique décomposée dans l'extension L/K et que L soit $\mathfrak{l}$-rationnel pour chacune des deux places au-dessus de $\mathfrak{l}$ (on dit alors qu'il est birationnel), situation que les arguments de [JSa] ne permettent pas de traiter complètement.

L'objet de ce travail est précisement d'éclaircir ce point plus délicat, dans le cas particulier où le corps de base K est totalement réel, en prenant appui sur la notion de classes logarithmiques exposée dans [J1].

2. Index des notations

Nous utiliserons dans tout ce qui suit les notations de la théorie ℓ-adique du corps de classes (avec ici $\ell = 2$) telle qu'exposée dans [J2]. En particulier si K est un corps de nombres et $\mathfrak{p}$ une place de K, nous notons :

- $K_\mathfrak{p}$ le complété de K en la place $\mathfrak{p}$;
- $\mathcal{R}_\mathfrak{p} = \varprojlim K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2^n}$ le compactifié 2-adique de $K_\mathfrak{p}^\times$;
- $\tilde{\mathcal{U}}_\mathfrak{p}$ le sous-groupe des unités logarithmiques de $\mathcal{R}_\mathfrak{p}$, i.e. le noyau dans $\mathcal{R}_\mathfrak{p}$ de la valeur absolue 2-adique $|.|_\mathfrak{p}$;
- $\mu_\mathfrak{p}$ le sous-groupe de torsion de $\mathcal{R}_\mathfrak{p}$, i.e. le 2-groupe des racines de l'unité dans $K_\mathfrak{p}$;
- $\mathcal{J}_K = \prod_\mathfrak{p}^{res} \mathcal{R}_\mathfrak{p}$ le 2-groupe des idèles de K ;
- $\tilde{\mathcal{J}}_K$ le noyau dans $\mathcal{J}_K$ de la formule du produit pour les valeurs absolues 2-adiques ;
- $\tilde{\mathcal{U}}_K = \prod_\mathfrak{p} \tilde{\mathcal{U}}_\mathfrak{p}$ le sous-groupe des unités logarithmiques semi-locales ;
- $\mathcal{R}_K = \mathbb{Z}_2 \otimes_\mathbb{Z} K^\times$ le 2-groupe des idèles principaux (plongé dans $\mathcal{J}_K$) ;
- $\tilde{\mathcal{E}}_K = \mathcal{R}_K \cap \tilde{\mathcal{U}}_K$ le sous-groupe des unités logarithmiques globales ;
- $\mathcal{E}'_K = \mathbb{Z}_2 \otimes_\mathbb{Z} E'_K$ le sous-groupe construit sur les 2-unités (au sens ordinaire) ;
- $\mathcal{D}_K = \mathcal{J}_K / \tilde{\mathcal{U}}_K$ le 2-groupe des diviseurs logarithmiques de K ;
- $\tilde{\mathcal{D}}_K = \tilde{\mathcal{J}}_K / \tilde{\mathcal{U}}_K$ le sous-groupe des diviseurs logarithmiques de degré nul ;
- $\tilde{\mathcal{P}}_K$ le sous-groupe des diviseurs logarithmiques principaux , i.e. l'image canonique de $\mathcal{R}_K$ dans $\tilde{\mathcal{D}}_K$;
- $\tilde{C\ell}'_K = \tilde{\mathcal{D}}_K / \tilde{\mathcal{P}}_K = \tilde{\mathcal{J}}_K / \mathcal{R}_K \tilde{U}_K$ le 2-groupe des classes logarithmiques ;
- $C\ell'_K = \mathcal{J}_K / \mathcal{R}_K \prod_{\mathfrak{p} \nmid 2\infty} \mu_\mathfrak{p} \prod_{\mathfrak{l} | 2} \mathcal{R}_\mathfrak{l}$ le 2-groupe des 2-classes (au sens restreint).

Enfin pour une extension L/K de corps de nombres, nous écrivons :

- $\mathcal{N}_{L/K}$ le sous-groupe de $\mathcal{R}_K$ formé des éléments qui sont une norme locale dans L/K (lorsque L/K est cyclique, c'est tout simplement le groupe $N_{L/K}(\mathcal{R}_L)$ des normes globales).

Conformément aux conventions de [J2] nous réservons aux places finies le concept de ramification ; si $\mathfrak{p}$ est une place réelle, nous parlons, s'il y a lieu, de complexification. De plus, toutes les extensions considérées ici étant des 2-extensions, la ramification est ipso facto modérée aux places étrangères à 2 et sauvage aux places 2-adiques.

3. Enoncé du résultat principal

Nous supposons désormais que ℓ vaut 2 et que L est une extension quadratique
totalement imaginaire d'un corps K totalement réel. Notre propos est de relier la 2-rationalité de K avec la 2-birationalité de L. Rappelons ce que nous entendons pas là :

Définition 1. (cf. [JN] th. 1.2) Un corps totalement réel K est dit *2-rationnel* lorsque sa 2-extension (galoisienne) 2-ramifiée ∞-décomposée maximale K' coïncide avec sa $\mathbb{Z}_2$-extension cyclotomique K^c, ce qui a lieu si et seulement si les deux conditions suivantes sont réunies :

(1a) K admet une unique place 2-adique $\mathfrak{l}$;

(1b) le 2-groupe $\mathcal{C}\ell'_K$ des 2-classes est trivial (en d'autres termes ici le 2-sous-groupe de Sylow du groupe des classes d'idéaux au sens restreint de K est engendré par l'image de la classe de $\mathfrak{l}$).

Définition 2. (cf. [JSa] th. 1.11). Un corps totalement imaginaire L est dit *2-birationnel* lorsqu'il est $\mathfrak{l}$-rationnel en chacune des places 2-adiques (en ce sens qu'il n'admet pas de 2-extension 2-ramifiée $\mathfrak{l}$-décomposée non triviale), ce qui a lieu si et seulement si les trois conditions suivantes sont vérifiées :

(2a) L admet exactement 2 places 2-adiques $\mathfrak{l}$ et $\mathfrak{l}'$;

(2b) le 2-groupe $C\ell'_L$ des 2-classes de diviseurs de L est trivial (en d'autres termes ici le 2-sous-groupe de Sylow du groupe des classes d'idéaux de L (au sens ordinaire comme au sens restreint) est engendré par les images de $\mathfrak{l}$ et de $\mathfrak{l}'$.

(2c) les plongements canoniques de $L^\times$ dans $L_\mathfrak{l}^\times$ et $L_{\mathfrak{l}'}^\times$ induisent des isomorphismes $\mathcal{E}'_L \simeq \mathcal{R}_{\mathfrak{l}'} \simeq \mathcal{R}_\mathfrak{l}$ du tensorisé 2-adique du groupe des 2-unités de L sur les compactifiés des groupes multiplicatifs des complétés de L aux places 2-adiques.

Introduisons maintenant la notion de place primitive : étant donné un corps de nombres K, notons provisoirement K^z le compositum des $\mathbb{Z}_2$-extensions de K et K^c la $\mathbb{Z}_2$-extension cylotomique de K ; dans [GJ] (cf. déf. 1.1) une place modérée de K (i.e. une place finie étrangère à 2) est dite primitive lorsque son image dans $Gal(K^z/K)$ par l'application d'Artin n'est pas un carré ; elle est dite dans [J1] (cf. déf. 4.4) logarithmiquement primitive lorsque c'est son image dans $Gal(K^c/K)$ qui n'est pas un carré. Il se trouve que, lorsque K

est totalement réel et vérifie la conjecture de Leopoldt en 2, le compositum K^z des $\mathbb{Z}_2$-extensions se réduit à la $\mathbb{Z}_2$-extension cyclotomique K^c, de sorte que les deux notions coïncident. Nous adopterons donc dans ce qui suit la convention suivante :

Définition 3. Soit K un corps de nombres totalement réel qui satisfait la conjecture de Leopoldt en $\ell = 2$. Nous dirons qu'une place modérée $\mathfrak{p}$ de K (i.e. une place finie ne divisant pas 2) est (relativement au nombre premier 2)

- *primitive*, lorsque son image dans le groupe procyclique $Gal(K^c/K)$ n'est pas un carré, autrement dit lorsqu'elle n'est pas décomposée dans la $\mathbb{Z}_2$-extension cyclotomique K^c/K ;

- *semi-primitive*, lorsque son image est un carré mais non une puissance 4-ième, autrement dit lorsqu'elle se décompose dans le premier étage de la $\mathbb{Z}_2$-extension cyclotomique K^c/K mais pas au-delà.

Cela étant posé, le résultat principal de cet article est le suivant :

Théorème 4. *Soit L/K une extension quadratique totalement imaginaire d'un corps de nombres totalement réel. Les assertions suivantes sont équivalentes :*

(i) le corps L est 2-birationnel ;

(ii) le corps K est 2-rationnel, son unique place 2-adique est décomposée dans L/K et l'extension L/K est ramifiée modérément soit en une place semi-primitive $\mathfrak{p}$ soit en deux places primitives $\mathfrak{p}$ et $\mathfrak{q}$.

Exemple. Pour $K = \mathbb{Q}$ et $L = \mathbb{Q}[\sqrt{-d}]$, on retrouve ainsi la classification des corps quadratiques imaginaires 2-birationnels donnée dans [JSa] (cf. cor. 1.12) : ce sont les corps $\mathbb{Q}[\sqrt{-p}]$ avec $p \equiv 7$ [mod 16] premier et les corps $\mathbb{Q}[\sqrt{-pq}]$ avec $p \equiv -q \equiv 3$ [mod 8] premiers.
Remarque. Le théorème de densité de Čebotarev montre alors que tout corps de nombres 2-birationnel totalement réel possède une infinité d'extensions quadratiques totalement imaginaires qui sont 2-birationnelles.

4. Interprétation logarithmique de la 2-rationalité

Commençons par rappeler la construction du 2-groupe des classes logarithmiques (cf. [J1] pour plus de détails). Soit

$$\tilde{\mathcal{J}}_L = \{\mathfrak{x} = (x_{\mathfrak{P}})_{\mathfrak{P}} \in \mathcal{J}_L \mid \prod_{\mathfrak{P}} |x_{\mathfrak{P}}|_{\mathfrak{P}} = 1\}$$

le noyau dans le 2-groupe des idèles $\mathcal{J}_L = \prod_{\mathfrak{P}}^{res} \mathcal{R}_{\mathfrak{P}}$ de la formule du produit pour les valeurs absolues 2-adiques et

$$\tilde{\mathcal{U}}_L = \{\mathfrak{x} = (x_{\mathfrak{P}})_{\mathfrak{P}} \in \mathcal{J}_L \mid |x_{\mathfrak{P}}|_{\mathfrak{P}} = 1, \ \forall\, \mathfrak{P} \in Pl_L\}$$

le sous-groupe des *unités logarithmiques locales ;* le quotient $\tilde{\mathcal{D}}_L = \tilde{\mathcal{J}}_L/\tilde{\mathcal{U}}_L$ est par définition, le 2-groupe des *diviseurs logarithmiques* de L et son quotient $\tilde{C\ell}'_L =$

$\tilde{\mathcal{D}}_L/\tilde{\mathcal{P}}_L = \tilde{\mathcal{J}}_L/\mathcal{R}_L\tilde{U}_L$ par l'image canonique $\tilde{\mathcal{P}}_L$ du 2-groupe $\mathcal{R}_L = \mathbb{Z}_2 \otimes_{\mathbb{Z}} L^\times$ des idèles principaux est le 2-groupe des classes logarithmiques du corps L.

Dans la correspondance du corps de classes, le groupe d'idèles $\tilde{\mathcal{J}}_L$ est le groupe de normes associé à la $\mathbb{Z}_2$-extension cyclotomique L^c de L et son sous-groupe $\tilde{\mathcal{U}}_L\mathcal{R}_L$ est, lui, le sous-groupe de normes associé à la pro-2-extension abélienne *localement cyclotomique maximale* L^{lc} de L (i.e. à la plus grande 2-extension abélienne de L qui est complètement décomposée sur L^c en chacune des ses places), de sorte que le quotient $\tilde{C\ell}_L$ s'identifie au groupe de Galois $Gal(L^{lc}/L^c)$. Lorsque $\tilde{C\ell}_L$ est trivial, L^{lc} coïncide avec L^c et on dit que L est *2-logarithmiquement principal.*

Cela étant nous allons déduire le théorème 4 du critère suivant de birationalité :

Proposition 5. *Soit L/K une extension quadratique totalement imaginaire d'un corps de nombres totalement réel. Il a alors équivalence entre :*

(i) le corps L est 2-birationnel ;

(ii) le corps K est 2-rationnel, l'extension L/K est 2-décomposée mais ramifiée modérement en au moins une place finie et le corps L est 2-logarithmiquement principal.

Commençons pour cela par établir un lemme :

Lemme 6. *Si L est un corps 2-birationnel extension quadratique d'un sous-corps K totalement réel, celui-ci est 2-rationnel et l'extension L/K est décomposée au-dessus de 2 et ramifiée modérément en au moins une place finie.*

Preuve du lemme. Vérifions d'abord que les places 2-adiques sont décomposée dans L/K. Dans le cas contraire, puisque L supposé 2-birationnel possède exactement deux places 2-adiques, disons $\mathfrak{L}$ et $\mathfrak{L}'$, le sous-corps K posséderait aussi deux places 2-adiques disons $\mathfrak{l}$ et $\mathfrak{l}'$, et les résultats de [JSa] (cf. cor. 2.11) montrent que, puisque L est rationnel en $\mathfrak{L}$ comme en $\mathfrak{L}'$, il en résulterait que K serait lui même rationnel en $\mathfrak{l}$ et $\mathfrak{l}'$, donc 2-birationnel, ce qui est exclu puisqu'un tel corps est nécessairement totalement imaginaire. En résumé L possède donc deux places 2-adiques $\mathfrak{L}$ et $\mathfrak{L}'$, et K une unique place 2-adique $\mathfrak{l}$, laquelle se décompose dans l'extension quadratique L/K.

Ce point acquis, écrivant la formule des classes ambiges pour les 2-classes (au sens restreint) $\mathcal{C}\ell'$ dans l'extension 2-décomposée L/K, nous obtenons :

$$1 = |\mathcal{C}\ell'^{\,\mathrm{Gal}(L/K)}_L| = |\mathcal{C}\ell'_K| \; \frac{2^n \prod_{\mathfrak{p}\nmid 2} e_{\mathfrak{p}}}{[L:K](\mathcal{E}'_K : \mathcal{E}'_K \cap \mathcal{N}_{L/K})} = |\mathcal{C}\ell'_K| \; \frac{2^{n+t-1}}{(\mathcal{E}'_K : \mathcal{E}'_K \cap \mathcal{N}_{L/K})}$$

où $n = [K:\mathbb{Q}]$ est le nombre de places réelles qui se complexifient, t le nombre de places finies qui se ramifient, $\mathcal{E}'_K$ le groupe des 2-unités (au sens restreint) et $\mathcal{N}_{L/K}$ le groupe des normes locales. Si donc l'extension L/K était 2-ramifiée, nous aurions simultanément $t = 0$ (par hypothèse), $|\mathcal{C}\ell'_K| \geq 2$ (puisque K posséderait une 2-extension non ramifiée (aux places finies) 2-décomposée non triviale : L), et $(\mathcal{E}'_K : \mathcal{E}'_K \cap \mathcal{N}_{L/K}) = (\mathcal{E}'_K : \mathcal{E}^+_K) \leq 2^n$ (puisque les 2-unités normes locales seraient tout simplement celles totalement positives), donc finalement :

$|\mathcal{C}\ell'_K| = 2$ & $(\mathcal{E}'_K : \mathcal{E}^+_K) = 2^n$($K$ possèderait des 2-unités de toutes signatures).

En particulier le 2-groupe des 2-classes de K au sens ordinaire serait encore d'ordre 2, et l'extension L/K non complexifiée aux places réelles, contrairement au fait que L est totalement imaginaire.

En fin de compte, il vient donc $t \geq 1$; chacun des deux facteurs $|\mathcal{C}\ell'_K|$ et $\frac{2^{n+t-1}}{\mathcal{E}'_K : \mathcal{E}'_K \cap \mathcal{N}_{L/K}}$ dans la formule des classes ambiges est entier donc vaut 1 ; et il suit $|\mathcal{C}\ell'_K| = 1$, comme attendu. □

Preuve de la proposition. D'après le lemme, nous pouvons supposer K 2-rationnel et L/K 2-décomposée. Ecrivons donc $\mathfrak{L}$ et $\mathfrak{L}'$ les deux places 2-adiques de L, notons 2^a l'ordre du diviseur logarithmique de degré nul $\mathfrak{l} - \mathfrak{l}'$ dans le groupe $\tilde{C}\ell_L$, et posons $2^a(\mathfrak{L} - \mathfrak{L}') = \tilde{div}(\pi_L)$, pour un π_L de $\mathcal{R}_L$. Nous pouvons alors écrire le groupe $\mathcal{E}'_L$ des 2-unités dans $\mathcal{R}_L$ comme produit direct

$$\mathcal{E}'_L = \tilde{\mathcal{E}}_L \pi_L^{\mathbb{Z}_2}$$

du sous-groupe $\tilde{\mathcal{E}}_L$ des unités logarithmiques de L et du $\mathbb{Z}_2$-module monogène engendré par π_L.

Maintenant, puisque L est totalement imaginaire et possède $n = [K : \mathbb{Q}]$ places complexes, $\tilde{\mathcal{E}}_L$ est le produit du groupe μ_L des racines de l'unité dans L et d'un $\mathbb{Z}_2$-module libre de dimension n (cf. [J1], prop 3.4) ; en particulier il contient $\tilde{\mathcal{E}}_K$ avec un indice fini. Mais comme le quotient $\tilde{\mathcal{E}}_L/\tilde{\mathcal{E}}_K$ est sans torsion (sans quoi nous pourions écrire $L = K[\sqrt{\eta}]$ avec une unité logarithmique η de K et l'extension L/K serait 2-ramifiée contrairement aux hypothèses faites), il suit que l'on a l'égalité $\tilde{\mathcal{E}}_L = \tilde{\mathcal{E}}_K$ (donc en fait $\tilde{\mathcal{E}}_L = \mathcal{E}'_K$ puisque , K n'ayant qu'une seule place 2-adique, les unités logarithmiques de K sont les 2-unités). En résumé nous avons obtenu la décomposition directe :

$$\mathcal{E}'_L = \tilde{\mathcal{E}}_K \pi_L^{\mathbb{Z}_2}$$

Considérons maintenant le compactifié $\mathcal{R}_{\mathfrak{L}} = \mathcal{R}_{\mathfrak{l}}$ du groupe multiplicatif $L^\times_{\mathfrak{L}} = K^\times_{\mathfrak{l}}$ d'un complété 2-adique de L. Le choix d'une uniformisante logarithmique $\pi_{\mathfrak{L}}$ nous permet d'écrire de même $\mathcal{R}_{\mathfrak{L}} = \tilde{\mathcal{U}}_{\mathfrak{L}} \pi_{\mathfrak{l}}^{\mathbb{Z}_2}$ à partir cette fois du groupe $\tilde{\mathcal{U}}_{\mathfrak{L}} = \tilde{\mathcal{U}}_{\mathfrak{l}}$ des unités logarithmiques locales. Ici encore, l'application de localisation identifie $\tilde{\mathcal{E}}_K$ à un module d'indice fini de $\tilde{\mathcal{U}}_L$ (du fait de l'égalité des rangs) et finalement à $\tilde{\mathcal{E}}_K$ lui même (sans quoi K possèderait une extension 2-décomposée $K[\sqrt{\eta}]$ non triviale engendrée par la racine carré d'une unité logarithmique, i.e. une extension quadratique 2-ramifiée et 2-décomposée, contrairement à la trivialité du groupe $C\ell'_K$).

En fin de compte, on voit que l'application de localisation de $\mathcal{E}'_L$ dans $\mathcal{R}_{\mathfrak{l}}$ est bijective si et seulement si π_L est une uniformisante logarithmique ; autrement dit que L est 2-birationnel si et seulement si le diviseur logarithmique $\mathfrak{L} - \mathfrak{L}'$ est principal :

- si ce n'est pas le cas, le corps L n'est ni 2-birationnel ni logarithmiquement principal ;

- si c'est le cas, L est birationnel, le groupe $C\ell'_L$ est trivial et le groupe $\tilde{C}\ell_L$ qui est alors engendré par la classe de $\mathfrak{L} - \mathfrak{L}'$ l'est aussi, de sorte que L est logarithmiquement principal. $\square$

5. Démonstration du théorème principal dans le cas modérement ramifié.

Soit L une extension totalement imaginaire d'un corps de nombres totalement réel, ramifiée modérément en au moins une place (finie). D'après la proposition 5 et le lemme 6, nous pouvons supposer K 2-rationnel et L/K 2-décomposée, et notre problème est de déterminer sous quelles conditions portant sur la ramification le corps L est logarithmiquement 2-principal.

Notons G le groupe de Galois $Gal(L/K)$ et écrivons la formule des classes logarithmiques ambiges dans l'extension L/K (cf. [J1], th. 4.5 et th. 5.3). Nous obtenons :

$$|\tilde{C}\ell_L^G| = |\tilde{C}\ell_K| \frac{2^n \prod \tilde{e}_{\mathfrak{p}}(L/K)}{[L^c : K^c](\tilde{\mathcal{E}}_K : \tilde{\mathcal{E}}_K \cap \mathcal{N}_{L/K})} (\mathcal{D}_L^{I_G} \tilde{\mathcal{P}}_L : \tilde{\mathcal{D}}_L^{I_G} \tilde{\mathcal{P}}_L),$$

où $|\tilde{C}\ell_K|$ vaut 1 puisque K est 2-rationnel ; $n = [K : \mathbb{Q}]$ est le nombre de places réelles de K complexifiées dans L (elles le sont toutes !) ; $\tilde{e}_{\mathfrak{p}}(L/K)$ désigne l'indice de ramification logarithmique de la place $\mathfrak{p}$ dans l'extension L/K (lequel coïncide avec l'indice de ramification au sens ordinaire $e_{\mathfrak{p}}(L/K)$, puisque les places 2-adiques, décomposées par hypothèse, sont non ramifiées) ; le degré $[L^c : K^c] = [L : K]$ est égal à 2 ; l'indice normique $(\tilde{\mathcal{E}}_K : \tilde{\mathcal{E}}_K \cap \mathcal{N}_{L/K})$ des unités logarithmiques modulo les normes est majoré par 2^{n+1} (puisque $\tilde{\mathcal{E}}_K$ est le produit de $\{\pm 1\}$ par un $\mathbb{Z}_2$-module libre de rang n) ; et le terme correctif $(\mathcal{D}^{I_G} \tilde{\mathcal{P}}_L : \tilde{\mathcal{D}}^{I_G} \tilde{\mathcal{P}}_L)$ vaut 1 ou 2 (et on sait qu'il vaut 1 lorsque l'extension L/K est primitivement ramifiée).

Il en résulte que si L est 2-logarithmiquement principal, l'extension quadratique L/K n'est ramifiée qu'en une ou deux places.

Reprenons maintenant le même raisonnement à un étage fini L_n/K_n de la tour cyclotomique : notons K_m le m-ième étage de la $\mathbb{Z}_2$-extenion cyclotomique K^c de K (c'est encore un corps totalement réel qui est 2-ramifié sur K donc 2-rationnel) et considérons le compositum $L_m = K_m L$ (qui est le m-ième étage de la $\mathbb{Z}_2$-extenion cyclotomique L^c de L). Observant que L et L_m sont simultanément 2-logarithmiquement principaux ou pas (la principalité logarithmique de L comme de L_m équivalant à la trivialité du 2-groupe des 2-classes $C\ell'_{L^c}$ du corps surcirculaire L^c (cf. par exemple [JSo])), nous concluons comme précédemment que si L est 2-logarithmiquement principal, l'extension L_m/K_m n'est ramifiée qu'en une ou deux places.

- Supposons donc L 2-logarithmiquement principal et examinons les deux éventualités :

(i) cas monoramifié : s'il existe une unique place finie ramifiée (modérément) dans L/K, elle est forcément imprimitive (sans quoi L/K serait primitivement ramifiée, et L 2-rationnel en vertu du résultat de [GJ], ce qui est exclu L ayant exactement deux places 2-adiques), i.e. décomposée dans K_1/K ; et, quitte à remplacer K par K_1 et L par L_1 nous sommes ramenés au :

(ii) cas biramifié : s'il existe exactement deux places finies $\mathfrak{p}$ et $\mathfrak{q}$ ramifiées dans L/K, elles sont forcément toutes deux primitives (sans quoi l'une au moins serait décomposée dans K_1/K et L_1/K_1 serait ramifiée en trois places au moins).

- Inversement, supposons L/K ramifiée modérément en une unique place $\mathfrak{p}$ semi-primitive, soit en deux places exactement $\mathfrak{p}$ et $\mathfrak{q}$ toutes deux primitives. Alors, quitte à remplacer L/K par K_1/L_1, nous pouvons nous placer dans le second cas. Cela étant, le terme correctif de la formule des classes logarithmique ambiges disparait (l'extension considérée est primitivement ramifiée), et la formule s'écrit :

$$|\tilde{C}\ell_L^G| = \frac{2^{n+1}}{(\tilde{\mathcal{E}}_K : \tilde{\mathcal{E}}_K \cap N_{L/K})} = \frac{2^{n+1}}{(\mathcal{E}'_K : \mathcal{E}'_K \cap N_{L/K})}.$$

D'autre part nous savons déjà, puisque K est 2-rationnel, qu'il contient des 2-unités de toutes signatures. En d'autres termes, les 2-unités totalement positives (i.e. celles qui sont normes locales aux places infinies dans l'extension L/K) forment un sous-groupe d'indice 2^n dans $\mathcal{E}'_K$. Montrer que $\tilde{C}\ell_L$ est trivial revient donc à trouver une 2-unité totalement positive qui ne soit pas norme locale en $\mathfrak{p}$ (ou en $\mathfrak{q}$, ce qui est équivalent d'après la formule du produit). Or nous connaissons une telle 2-unité ε : le premier étage K_1 de la $\mathbb{Z}_2$-extension cyclotomique K^c de K est précisément de la forme $K[\sqrt{\varepsilon}]$ pour une 2-unité $\varepsilon >> 0$ qui n'est pas un carré dans $K_{\mathfrak{p}}^{\times}$ (puisque $\mathfrak{p}$ ne se décompose pas dans K_1/K) donc qui n'est pas norme locale en $\mathfrak{p}$ dans l'extension quadratique L/K ramifiée en $\mathfrak{p}$; ce qui achève la démonstration.

Remarque. Pour $K = \mathbb{Q}$, le résultat obtenu redonne naturellement la classification des corps quadratiques imaginaires 2-logarithmiquement principaux $\mathbb{Q}[\sqrt{-d}]$ (avec ici $d \equiv -1[\text{mod } 8]$ compte tenu de la contrainte de 2-décomposition) établie dans [So].

Bibliographie

[GJ] G. Gras & J.-F. Jaulent, *Sur les corps de nombres réguliers*, Math. Z. **202** (1989), 343–365.

[J1] J.-F. Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1995), 301–325.

[J2] J.-F. Jaulent, *Théorie ℓ-adique globale du corps de classes*, J. Théor. Nombres Bordeaux **10** (1999), 355–397.

[JN] J.-F. Jaulent & T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers et ramification restreinte*, J. Théor. Nombres. Bordeaux **5** (1993), 343–365.

[JSa] J.-F. Jaulent & O. Sauzet, *pro-ℓ-extension de corps $\mathfrak{l}$-rationnels*, J. Numb. Th. **65**, 240–267.

[JSo] J.-F. Jaulent & F. Soriano, *Sur les tours localement cyclotomiques*, Archiv. der Math. **73** (1999), 132–140.

[So] F. Soriano, *Classes logarithmiques ambiges des corps quadratiques*, Acta Arith. **78** (1997), 201–219.

[MN] A. Movahhedi, T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Sém. Th. Nombres Paris (1987/1988), Prog. in Math. **89** (1990), 155–200.

[W1] K. Wingberg, *On Galois groups of p-closed algebraic number fields with restricted ramification*, J. reine angew. Math. **400** (1989), 185–202.

[W2] K. Wingberg, *On Galois groups of p-closed algebraic number fields with restricted ramification II*, J. reine angew. Math. **416** (1991), 187–194.

Jean-François Jaulent
Institut de Mathématiques
Université Bordeaux I
351, cours de la libération
F-33405 Talence Cedex
email : jaulent@math.u-bordeaux.fr

Odile Sauzet
Institut de Mathématiques
Université Bordeaux I
351, cours de la libération
F-33405 Talence Cedex
email : sauzet@math.u-bordeaux.fr