

JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

FLORENCE SORIANO

Familles d'extensions de corps de nombres l -rationnels

Journal de Théorie des Nombres de Bordeaux, tome 8, n° 2 (1996),
p. 461-479

http://www.numdam.org/item?id=JTNB_1996__8_2_461_0

© Université Bordeaux 1, 1996, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/*

Familles d'extensions de corps de nombres \mathfrak{l} -rationnels

par FLORENCE SORIANO

RÉSUMÉ. Dans cet article, nous déterminons et classifions toutes les extensions cycliques de degré l de corps de nombres \mathbb{L} -rationnels contenant une racine primitive l -ième de l'unité. (Cette notion est plus générale que celle de l -régularité étudiée dans un travail antérieur).

ABSTRACT. In this paper we characterise and classify all the cyclic extensions of degree l of the \mathbb{L} -rational number fields which contain the l -roots of unity for an odd prime l . (Note that the concept of \mathbb{L} -rationality for number fields is more general than the l -rationality).

§1. Introduction

1.1 PRÉSENTATION DU PROBLÈME.

Soient ℓ un nombre premier, K un corps de nombres (totalement réel lorsque $\ell = 2$) contenant une racine primitive $\ell^{ième}$ de l'unité ζ . Tout récemment J.-F JAULENT et O. SAUZET (cf. [JS], déf. 1.1) ont généralisé comme suit la notion de corps ℓ -rationnel (ou ℓ -régulier) considérée dans notre travail précédent (cf. [So]) :

DÉFINITION 1. Soient K un corps de nombres contenant les racines primitives $\ell^{ièmes}$ de l'unité et \mathfrak{l} une place de K au dessus du nombre premier ℓ . Le corps de nombres K est dit \mathfrak{l} -rationnel lorsque la ℓ -extension abélienne ℓ -ramifiée \mathfrak{l} -décomposée (i.e. non ramifiée aux places finies en dehors de celles au-dessus de ℓ et complètement décomposée en \mathfrak{l}) maximale de K est triviale.

Lorsque le corps K ne possède qu'une seule place sauvage (i.e. au dessus de ℓ), les notions de \mathfrak{l} -rationalité, de ℓ -rationalité ou encore de ℓ -régularité se trouvent coïncider puisque nous supposons ici que K contient les racines primitives $\ell^{ièmes}$ de l'unité.

Le but de ce travail est ainsi de généraliser la classification des extensions cycliques de degré ℓ de corps de nombres ℓ -réguliers présentée dans [So]

(lorsque ℓ est impair) ou $[B_2]$ (lorsque $\ell = 2$). Plus précisément, nous proposons de déterminer ici toutes les extensions L d'un corps \mathfrak{l} -rationnel K , cycliques de degré ℓ et \mathfrak{L} -rationnelles en une place \mathfrak{L} au dessus de \mathfrak{l} , puis de les classifier en fonction de l'indice de ramification de la place sauvage \mathfrak{l} de K dans L/K et de la ℓ -valuation du nombre relatif $h_{L/K}$ de classes d'idéaux de L/K .

Dans toute la suite, nous notons G le groupe de Galois de l'extension L/K .

Notre point de départ est le résultat suivant établi dans [JS] (cf. th. 3.4) :

THÉORÈME 2. *Soient ℓ un nombre premier impair, K un corps de nombres contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité, \mathfrak{l} une place de K au-dessus de ℓ , puis L une ℓ -extension galoisienne de K et \mathfrak{L} une place de L au-dessus de \mathfrak{l} . Les propriétés suivantes sont équivalentes :*

- (i) *le corps L est \mathfrak{L} -rationnel;*
- (ii) *le corps K est \mathfrak{l} -rationnel, et l'ensemble X des places de K qui se ramifient modérément dans l'extension L/K est \mathfrak{l} -primitif. (Autrement dit les logarithmes de Gras $\ell g(p)$ des places de X forment une \mathbb{Z}_ℓ -base d'un supplémentaire de $K'_\mathfrak{l}/\mu'_\mathfrak{l}$ dans le groupe de Galois de la composée Z des \mathbb{Z}_ℓ -extensions de K , où $K'_\mathfrak{l}$ est le produit des ℓ -adiés des groupes multiplicatifs $K_\mathfrak{l}^\times$ des complétés de K en les places sauvages \mathfrak{l}' autres que \mathfrak{l} et $\mu'_\mathfrak{l}$ son groupe de torsion).*

Dans une telle extension, la place \mathfrak{l} ne peut se décomposer.

REMARQUE : les places p de la caractérisation (ii) ci-dessus sont donc nécessairement des places ultramétriques étrangères à ℓ . Nous les appelons *modérées* dans ce qui suit, par opposition avec les places au dessus de ℓ que nous disons *sauvages*.

Le théorème 2 imposant la condition ℓ impair, nous avons besoin pour ce qui suit de nous affranchir de cette restriction dans la situation particulière que nous considérons des extensions cycliques de degré ℓ . Nous pouvons ainsi énoncer :

THÉORÈME 3. *Soient ℓ un nombre premier quelconque, K un corps de nombres contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité, puis L une extension cyclique de degré ℓ sur K , que nous supposons totalement réelle lorsque ℓ vaut 2. Si l'on note \mathfrak{L} une place (sauvage) de L au-dessus de \mathfrak{l} , les propriétés suivantes sont équivalentes :*

- (i) *le corps L est \mathfrak{L} -rationnel;*

(ii) le corps K est \mathfrak{l} -rationnel, et l'ensemble X des places de K qui se ramifient modérément dans l'extension L/K est \mathfrak{l} -primitif.

La démonstration du théorème 3 repose sur le lemme suivant qui précise le cas $\ell = 2$:

LEMME 4. *Soit L/K une 2-extension de corps de nombres totalement réels. Si le corps L est rationnel en une place paire \mathfrak{L} , cette place est nécessairement fixe par les K -automorphismes de L .*

PREUVE : comme le corps L est totalement réel, il ne peut être 2-birationnel (cf. [JS], Prop. 1.9). Autrement dit, \mathfrak{L} est l'unique place divisant 2 en laquelle L est rationnelle. Si donc σ désigne un élément du groupe de Galois de l'extension L/K , la conjuguée \mathfrak{L}^σ est l'unique place en laquelle $L^\sigma = L$ est rationnelle; elle coïncide donc avec la place \mathfrak{L} .

PREUVE DU THÉORÈME 3 : il suffit pour cela d'adapter au cas $\ell = 2$ la démonstration écrite par J.-F JAULENT et O. SAUZET dans [JS] pour établir le théorème 3.4 qui s'appuie principalement sur le théorème 2.10 du même article. Ce dernier résultat suppose la non-décomposition de la place \mathfrak{l} dans les extensions que l'on est amené à considérer ; et celle-ci résulte ici du lemme 4 ci-dessus : c'est immédiat pour le sens direct (i) \Rightarrow (ii) ; quant au sens réciproque (ii) \Rightarrow (i), il s'obtient sans difficulté à partir des arguments de [JS] en plongeant L dans une 2-extension réelle X -modérément ramifiée maximale de K après avoir complété X en un ensemble \mathfrak{l} -primitif maximal de places modérées.

DÉFINITION 5. *Lorsque l'ensemble des places de K qui se ramifient modérément dans l'extension L/K est \mathfrak{l} -primitif, on dit que L/K est \mathfrak{l} -primitivement ramifiée.*

En résumé, nous considérons dans ce qui suit un corps de nombres K contenant une racine ℓ -ième de l'unité ζ , rationnel en une place sauvage \mathfrak{l} et totalement réel pour $\ell = 2$. Puisqu'une extension L/K cyclique de degré ℓ est \mathfrak{L} -rationnelle en une place \mathfrak{L} au dessus de \mathfrak{l} si et seulement s'il existe un ensemble \mathfrak{l} -primitif maximal X tel que L soit incluse dans la ℓ -extension \overline{M}^X ℓ -élémentaire X -modérément ramifiée ∞ -décomposée maximale de K , nous allons nous intéresser aux ℓ -extensions cycliques L de K qui sont \mathfrak{l} -primitivement ramifiées.

1.2 INDEX DES PRINCIPALES NOTATIONS.

Nous rassemblons ci-dessous les principales notations utilisées dans l'article.

Notations attachées à un corps local K_p :

- μ_p le groupe de torsion de K_p^\times ,
- μ_p° le sous-groupe des éléments de torsion d'ordre $Np - 1$,
- π_p une uniformisante de K_p ,
- $\mathcal{K}_p^\times = \varprojlim K_p^\times / K_p^{\times p^n}$ le compactifié ℓ -adique de K_p^\times ,
- \mathcal{U}_p le groupe des unités principales de \mathcal{K}_p^\times .

Notations attachées à un corps de nombres K :

- r, c, s le nombre de places réelles, complexes ou sauvages (i.e divisant ℓ),
- Pl_K l'ensemble de places de K ,
- h_K le nombre de classes (au sens ordinaire),
- E_K le groupe des unités (au sens ordinaire),
- E'_K le groupe des ℓ -unités (i.e. des unités en dehors ℓ),
- $\mathcal{I}_K = \prod_p^{res} \mathcal{K}_p^\times$ le ℓ -adifié du groupe des idèles,
- $\mathcal{R}_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$ le sous-groupe des idèles principaux,
- $\mathcal{E}_K, \mathcal{E}'_K$ les tensorisés ℓ -adiques de E_K, E'_K .

Notations attachées à une extension L/K :

- $G = \text{Gal}(L/K)$ le groupe de Galois,
- $N_{L/K}$ le groupe des normes,
- $\mathcal{N}_{L/K}$ le tensorisé ℓ -adique de $N_{L/K}$,
- $e_p(L/K)$ l'indice de ramification de la place finie p ,
- $d_p(L/K)$ le degré de l'extension locale $L_{\mathfrak{P}}/K_p$,
- $t_{L/K}$ le nombre de places modérées ramifiées dans L/K ,
- $m_{L/K}$ le nombre de places sauvages non décomposées dans L/K .

Notations attachées à une place sauvage \mathfrak{l} de K :

- X un ensemble \mathfrak{l} -primitif maximal de places modérées,
- d le degré de l'extension locale $K_{\mathfrak{l}}/\mathbb{Q}_\ell$,
- $x = d - r - c - s + 2$ le cardinal de X ,
- M^X la ℓ -extension abélienne X -modérément ramifiée ∞ -décomposée maximale de K (M^X/K est non ramifiée en dehors des places modérées $p \in X$ et des places sauvages, et non complexifiée aux places réelles),
- \overline{M}^X la sous-extension ℓ -élémentaire de M^X ,
- \mathfrak{L} une place de L contenant \mathfrak{l} ,
- E'_X le groupe des $X\ell$ -unités (i.e. des unités globales en dehors des places sauvages et des places de X),
- $f_{L/K}$ le nombre de places sauvages inertes dans l'extension L/K .

§2. Description de $\text{Gal}(\overline{M}^X/K)$ et de $\text{Rad}(\overline{M}^X/K)$:

Désormais, K désigne un corps de nombres \mathfrak{l} -rationnel contenant les racines $\ell^{ièmes}$ de l'unité et X un ensemble \mathfrak{l} -primitif maximal de places de K .

2.1 STRUCTURE DU GROUPE DE GALOIS.

Comme $\text{Gal}(\overline{M}^X/K) \simeq \text{Gal}(M^X/K)/\text{Gal}(M^X/K)^\ell$, nous avons d'après [JS], th. 2.6 :

$$\text{Gal}(\overline{M}^X/K) \simeq \prod_{p \in X} (\mathcal{K}_p^\times / \mathcal{K}_p^{\times \ell}) \prod_{\ell' \mid \ell, \ell' \neq \mathfrak{l}} (\mathcal{K}_{\ell'}^\times / \mathcal{K}_{\ell'}^{\times \ell})$$

La décomposition $K_p^\times \simeq \mu_p^\circ \times (1+p) \times \pi_p^{\mathbb{Z}}$ pour chaque place finie p , nous donne alors l'isomorphisme :

$$\text{Gal}(\overline{M}^X/K) \simeq \prod_{p \in X} \left(\frac{\mu_p^\circ}{\mu_p^{\circ \ell}} \times \frac{(1+p)}{(1+p)^\ell} \times \pi_p^{\mathbb{Z}/\ell\mathbb{Z}} \right) \prod_{\ell' \mid \ell, \ell' \neq \mathfrak{l}} \left(\frac{\mu_{\ell'}^\circ}{\mu_{\ell'}^{\circ \ell}} \times \frac{(1+\ell')}{(1+\ell')^\ell} \times \pi_{\ell'}^{\mathbb{Z}/\ell\mathbb{Z}} \right).$$

Dans le premier produit (i.e. pour $p \nmid \ell$), le facteur médian $\frac{(1+p)}{(1+p)^\ell}$ est trivial, et dans le second (i.e. pour $\ell' \mid \ell$) il en est de même du quotient $\mu_{\ell'}^\circ / \mu_{\ell'}^{\circ \ell}$. Il vient donc :

$$\text{Gal}(\overline{M}^X/K) \simeq \prod_{p \in X} \left(\frac{\mu_p^\circ}{\mu_p^{\circ \ell}} \times \pi_p^{\mathbb{Z}/\ell\mathbb{Z}} \right) \prod_{\ell' \mid \ell, \ell' \neq \mathfrak{l}} \left(\frac{(1+\ell')}{(1+\ell')^\ell} \times \pi_{\ell'}^{\mathbb{Z}/\ell\mathbb{Z}} \right).$$

Et puisque le logarithme ℓ' -adique envoie le groupe multiplicatif $1 + \ell'$ sur un \mathbb{Z}_ℓ -module libre de dimension $[K_{\ell'} : \mathbb{Q}_\ell]$, nous obtenons finalement :

$$\text{Gal}(\overline{M}^X/K) \simeq \prod_{p \in X} \mathbb{F}_\ell^2 \times \prod_{\ell' \mid \ell, \ell' \neq \mathfrak{l}} \mathbb{F}_\ell^{2+[K_{\ell'} : \mathbb{Q}_\ell]},$$

puisque μ_p° contient évidemment les racines $\ell^{ièmes}$ de l'unité lorsque p est modérée.

Compte tenu de l'identité $(\sum_{\ell' \mid \ell, \ell' \neq \mathfrak{l}} [K_{\ell'} : \mathbb{Q}_\ell] = r + 2c - [K_\mathfrak{l} : \mathbb{Q}_\ell])$, il en résulte que $\text{Gal}(\overline{M}^X/K)$ est un \mathbb{F}_ℓ -espace vectoriel de dimension :

$$\dim_{\mathbb{F}_\ell} \text{Gal}(\overline{M}^X/K) = 2(x + s - 1) + r + 2c - [K_\mathfrak{l} : \mathbb{Q}_\ell] = d + 2 - r.$$

PROPOSITION 16. *Si K est un corps de nombres \mathfrak{l} -rationnel qui contient les racines $\ell^{ièmes}$ de l'unité, pour tout ensemble \mathfrak{l} -primitif maximal X de places modérées, le groupe de Galois $\text{Gal}(\overline{M}^X / K)$ de la ℓ -extension abélienne X -modérément ramifiée ∞ -décomposée ℓ -élémentaire maximale de K est un \mathbb{F}_ℓ -espace vectoriel de dimension $d + 2 - r$, isomorphe au produit direct des ℓ -groupes de Galois locaux $G_p = \text{Gal}(K_p^\text{ét}/K_p)$ attachées aux ℓ -extensions abéliennes ℓ -élémentaires maximales des complétés K_p de K pour $p|X\ell$, $p \neq \mathfrak{l}$.*

2.2 STRUCTURE DU RADICAL POUR ℓ IMPAIR.

Dans ce sous-paragraphe, le nombre premier ℓ est supposé impair.

Le quotient du groupe E'_X par sa puissance $\ell^{ième}$ est d'après le théorème de DIRICHLET, un \mathbb{F}_ℓ -espace vectoriel de dimension $c + s + x = d + 2 - r$.

Lorsque x est un représentant du groupe quotient E'_X/E'_X^ℓ , l'extension $K(\sqrt[\ell]{x})$ est non ramifiée en dehors des places de X et de celles divisant ℓ , et ne se complexifie pas en les places réelles. Le quotient E'_X/E'_X^ℓ est donc un sous-groupe du radical de l'extension \overline{M}^X / K . La théorie de KUMMER établissant une dualité entre les groupes $\text{Gal}(\overline{M}^X / K)$ et $\text{Rad}(\overline{M}^X / K)$, de l'égalité des ordres il vient ainsi :

$$\text{Rad}(M^X / K) \simeq E'_X / E'_X^\ell.$$

PROPOSITION 7. *Soient ℓ un nombre premier impair, K un corps de nombres \mathfrak{l} -rationnel contenant une racine primitive $\ell^{ième}$ de l'unité, \mathfrak{l} l'une de ses places sauvages, X un ensemble \mathfrak{l} -primitif maximal de places de K . La théorie de KUMMER établit l'isomorphisme :*

$$\text{Rad}(M^X / K) \simeq E'_X / E'_X^\ell \simeq \prod_{p \in X} (K_p^\times / K_p^{\times\ell}) \prod_{\mathfrak{v}|\ell, \mathfrak{v} \neq \mathfrak{l}} (\mathcal{K}_{\mathfrak{v}}^\times / \mathcal{K}_{\mathfrak{v}}^{\times\ell})$$

entre le radical kummérien de la ℓ -extension abélienne X -modérément ramifiée ∞ -décomposée ℓ -élémentaire maximale et le produit des radicaux locaux associés aux ℓ -extensions abéliennes ℓ -élémentaires maximales des complétés K_p de K aux places modérées de X ou sauvages autres que \mathfrak{l} .

COROLLAIRE 8. *Sous les hypothèses de la proposition 7, il existe exactement*

$(\ell^{d+2} - 1)/(\ell - 1)$ *sous-extensions non triviales \mathfrak{l} -rationnelles de degré ℓ de \overline{M}^X .*

Ce sont les extensions de la forme $K(\sqrt[\ell]{\sigma})$ où σ est un représentant de l'une quelconque des $(\ell^{d+2} - 1)$ classes non triviales de E'_X / E'_X^ℓ .

Plus précisément, si \mathfrak{l} est la place sauvage donnée de K , si les $\{\pi_j; j = 1, \dots, d - c + 2\}$ sont des uniformisantes associées aux places sauvages étrangères à \mathfrak{l} ou modérées de X , puis si $\{u_j; j = 1, \dots, c - 1\}$ est un système de $(c - 1)$ unités fondamentales de K , les extensions L cherchées sont les extensions de la forme :

$$L = K \left(\sqrt[\ell]{\zeta^i \times \left(\prod_{j=1}^{d-c+2} \pi_j^{k_j} \right) \times \left(\prod_{j=1}^{c-1} u_j^{l_j} \right)} \right)$$

où les entiers i, k_j et l_j sont pris non tous nuls dans $\{0, \dots, \ell - 1\}^{d+2}$.

2.3 Structure du radical pour $\ell = 2$

A présent ℓ est pair. Notons $E_{\mathfrak{l}}^{\text{ord}}$ (resp. $E_{\mathfrak{l}}^{\text{res}}$) le groupe des \mathfrak{l} -unités (i.e des éléments de K qui sont unités, au sens ordinaire (resp. au restreint) en dehors de la place \mathfrak{l}). Nous avons ici :

LEMME 9. Si K est \mathfrak{l} -rationnel pour une place \mathfrak{l} au dessus de 2, il contient des \mathfrak{l} -unités (au sens ordinaire) de toutes signatures.

PREUVE : comme K est \mathfrak{l} -rationnel, on a l'identité entre les groupes d'idèles :

$$\mathcal{I}_K = \mathcal{R}_K \mathcal{K}_{\mathfrak{l}}^{\times} \prod_{p \neq \infty} \mu_p$$

si bien que la 2-partie du quotient du groupe des classes au sens restreint par son sous-groupe engendré par la classe de \mathfrak{l} est triviale. En d'autres termes, la 2-partie du groupe des \mathfrak{l} -classes de K est triviale.

Considérons par ailleurs le diagramme

$$\begin{array}{ccccccc} & 1 & & 1 & & 1 & \\ & \downarrow & & \downarrow & & \downarrow & \\ 1 & \longrightarrow & \mathcal{E}_{\mathfrak{l}}^{\text{res}} & \longrightarrow & \mathcal{E}_{\mathfrak{l}}^{\text{ord}} & \longrightarrow & sg(\mathcal{E}_{\mathfrak{l}}^{\text{ord}}) \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 1 & \longrightarrow & K^+ & \longrightarrow & K^{\times} & \longrightarrow & sg(K^{\times}) \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 1 & \longrightarrow & P_{\mathfrak{l}}^+ & \longrightarrow & P_{\mathfrak{l}} & \longrightarrow & P_{\mathfrak{l}}/P_{\mathfrak{l}}^+ \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ & 1 & & 1 & & 1 & \end{array}$$

où sg est le morphisme signature, K^+ est le sous-groupe des éléments totalement positifs de K^\times et P_ℓ (resp. P_ℓ^+) est l'image de K^\times (resp. K^+) dans $\bigoplus_{\mathfrak{p} \in X\ell} \mathfrak{p}^\mathbb{Z}$.

Comme P_ℓ/P_ℓ^+ est un 2-groupe et que la 2-partie du groupe des ℓ -classes au sens restreint est triviale, le quotient P_ℓ/P_ℓ^+ l'est aussi. On a finalement :

$$sg(\mathcal{E}_\ell^{ord}) = sg(K^\times) = \{\pm 1\}^r.$$

En particulier, si l'on désigne par π_p une uniformisante attachée à une place de $X\ell$ (i.e. sauvage ou modérée de X), il existe une ℓ -unité u_p telle que le produit $\pi'_p = \pi_p u_p$ soit totalement positif. Comme les extensions totalement réelles

$$L = K \left(\sqrt{\prod_{p \in X\ell} \pi'_p^{n_p}} \right)$$

(où les entiers n_p valent 0 ou 1 et ne sont pas simultanément nuls), sont non ramifiées en dehors des places de $X\ell$, le groupe $\bigoplus_{p \in X\ell} \pi'_p^{\mathbb{Z}/2\mathbb{Z}}$ est un sous-groupe du radical de l'extension \overline{M}^\times/K . La théorie de KUMMER établissant une dualité entre les groupes $\text{Gal}(\overline{M}^\times/K)$ et $\text{Rad}(\overline{M}^\times/K)$, de l'égalité des ordres donnée par la proposition 6 nous donne :

$$\text{Rad}(M^\times/K) \simeq \bigoplus_{p \in X\ell} \pi'_p^{\mathbb{Z}/2\mathbb{Z}}.$$

PROPOSITION 10. *Soient K un corps de nombres ℓ -rationnel en une place sauvage ℓ puis X un ensemble ℓ -primitif maximal de places de K .*

Il existe $2^{d-r+2}-1$ sous-extensions non triviales non triviales ℓ -rationnelles de degré 2 de \overline{M}^\times . Ce sont les extensions de la forme $K(\sqrt{\sigma})$ où σ est un représentant de l'une quelconque des $2^{d-r+2}-1$ classes non triviales de E'_X/E_X^{ℓ} .

Plus précisément, si ℓ est la place sauvage donnée de K , si les $\{\pi'_j; j = 1, \dots, d - c + 2\}$ sont des uniformisantes associées aux places sauvages étrangères à ℓ ou modérées de X , il existe pour tout indice j une ℓ -unité u_j telle que le produit $\pi_j = \pi'_j u_j$ soit totalement positif. Les extensions cherchées sont de la forme :

$$L = K \left(\sqrt{\prod_{j=1}^{d-r+2} \pi_j^{k_j}} \right)$$

où les entiers k_j prennent les valeurs 0 ou 1 et ne sont pas simultanément nuls.

Lorsque ($\ell = 2$), R. BERGER s'est attachée à l'étude de la propagation de la surjectivité de la restriction de la signature au groupe des unités. Dans ce cadre plus général, il vient le résultat analogue :

LEMME 11. *Soit L une extension cyclique de degré ℓ , rationnelle en une place sauvage \mathfrak{L} , d'un corps de nombres K contenant les racines ℓ ièmes de l'unité. Toutes les unités de K normes dans l'extension L/K sont normes d'unités. Autrement dit,*

$$\mathcal{E}_K \cap \mathcal{N}_{L/K} = N_{L/K}(\mathcal{E}_L).$$

PREUVE : comme l'établit le début de la démonstration du lemme 9, l'identité entre les groupes d'idèles :

$$\mathcal{I}_L = \mathcal{R}_L \mathcal{K}_{\mathfrak{L}}^{\times} \prod_{p \nmid \ell\infty} \mu_p$$

traduit la trivialité du ℓ -groupe des \mathfrak{L} -classes (au sens ordinaire) de L . Le ℓ -groupe des classes (au sens ordinaire) de L est donc engendré par la classe de \mathfrak{L} . Or, comme nous l'avons vu dans la preuve du théorème 3 (pour ℓ impair) ou du lemme 4 (pour ℓ pair), la place \mathfrak{L} est fixe par les K -automorphismes de L . Autrement dit, les classes ambiguës sont d'ambigues. Et d'après l'isomorphisme de CHEVALLEY, le ℓ -groupe des unités normes dans l'extension L/K est le ℓ -groupe des normes d'unités.

La situation particulière suivante se révèle intéressante puisque le radical s'explique plus facilement :

COROLLAIRE 12. *Sous les hypothèses de la proposition 10, lorsque le corps K est totalement réel et admet des unités de toutes signatures, il existe une uniformisante totalement positive associée à chacune des places de $X\ell$. Les notant π_i pour $i = 1, \dots, d+2-r$, on voit que les extensions L considérées sont de la forme :*

$$L = K \left(\sqrt{\prod_{j=1}^{d+2-r} \pi_j^{k_j}} \right),$$

où les entiers k_j prennent la valeur 0 ou 1 et ne sont pas simultanément nuls.

De plus, la restriction de la signature au groupe des unités de L est alors surjective.

PREUVE : la proposition 1.2 dans [B₁] montre que la restriction de la signature au groupe des unités de L est surjective dès que celle de K l'est aussi et que toutes les unités sont normes dans l'extension L/K . Le premier point est satisfait par hypothèse, le second grâce au lemme 11.

§4. Cas des ℓ -extensions non ramifiées aux places modérées :

4.1 RAMIFICATION SAUVAGE.

Désormais, K désigne un corps de nombres contenant une racine primitive $\ell^{i\text{ème}}$ ζ de l'unité, puis L/K une ℓ -extension cyclique de degré ℓ sur K , réputée totalement réelle lorsque ℓ vaut 2. Fixant une place \mathfrak{L} de L au-dessus de \mathfrak{l} , nous supposons dans ce qui suit que L est \mathfrak{L} -rationnelle. Nous disons que l'extension L/K est \mathfrak{L} -rationnelle. L'ensemble des places de K qui se ramifient sur L est alors \mathfrak{l} -primitif et peut donc être complété en un ensemble \mathfrak{l} -primitif maximal X . Nous nous intéressons plus particulièrement dans cette section au cas où l'extension considérée L est ℓ -ramifiée (i.e. non ramifiée aux places étrangères à ℓ).

Enonçons la loi de réciprocité primitive établie dans [JS], corollaire 3.2 :

LEMME 13. (*Lemme d'approximation par les X -unités*). *Soient K un corps de nombres \mathfrak{l} -rationnel contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité et X un ensemble \mathfrak{l} -primitif maximal de places de K . Nous avons alors les isomorphismes suivants :*

$$E'_X/E'_X^{\times \ell} \simeq K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times \ell}.$$

Ce lemme permet d'identifier le quotient $E'_X/E'_X^{\times \ell}$ du groupe des $X\ell$ -unités par le sous-groupe de ses puissances $\ell^{i\text{èmes}}$ avec le quotient $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times \ell}$ du groupe multiplicatif du complété en \mathfrak{l} de K par le sous-groupe formé de ses puissances $\ell^{i\text{èmes}}$ et donc de regarder le quotient $E'_K/E'_K^{\times \ell}$ du groupe des ℓ -unités de K comme un sous-groupe de $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times \ell}$.

Il existe donc une classe $\beta = cl(\sigma)$ de $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times \ell}$ telle que l'on ait : $L = K(\sqrt[\ell]{\sigma})$. En particulier, lorsque l'extension est modérément ramifiée, la classe $\beta = cl(\sigma)$ appartient à $(K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times \ell} - E'_K/E'_K^{\times \ell})$. Enfin, dans le cas de ramification non modérée, l'extension L s'écrit sous la forme $K(\sqrt[\ell]{\tau})$ où τ est un représentant d'une classe de $E'_K/E'_K^{\times \ell}$.

PROPOSITION 14. *Si h_K désigne le nombre de classes d'idéaux de K , deux cas se présentent suivant sa divisibilité par le nombre premier ℓ :*

- ou bien ($\ell \nmid h_K$), et toutes les extensions L/K sont alors ramifiées,
- ou bien ($\ell \mid h_K$), et l'une et seulement l'une des extensions L est non ramifiée.

PREUVE : le groupe de Galois de la ℓ -extension C abélienne non ramifiée maximale (cf. [Ja], p.30, Exemple I.1.20.) est isomorphe à $\mathcal{I}_K / \prod_{v \nmid \ell} \mathcal{U}_v \prod_{q \nmid \ell} \mu_q \mathcal{R}_K$.

Comme K est supposé \mathfrak{l} -rationnel, le ℓ -adifié du groupe de ses idèles vérifie $\mathcal{I}_K = \prod_{q \nmid \ell} \mu_q \mathcal{K}_{\mathfrak{l}}^{\times} \mathcal{R}_K$, de sorte qu'il vient :

$$\begin{aligned} \text{Gal}(C/K) &\simeq \mathcal{I}_K / \prod_{q \nmid \ell} \mu_q \prod_{v \nmid \ell} \mathcal{U}_v \mathcal{R}_K \simeq \mathcal{K}_{\mathfrak{l}}^{\times} / \mathcal{K}_{\mathfrak{l}}^{\times} \cap (\prod_{q \nmid \ell} \mu_q \prod_{v \nmid \ell} \mathcal{U}_v \mathcal{R}_K), \\ (*) \quad \text{Gal}(C/K) &\simeq \mathcal{K}_{\mathfrak{l}}^{\times} / s_{\mathfrak{l}}(\mathcal{E}_{\mathfrak{l}}) \mathcal{U}_{\mathfrak{l}} \simeq \mathbb{Z}_{\ell} / v_{\mathfrak{l}}(\mathcal{E}_{\mathfrak{l}}) \end{aligned}$$

où $s_{\mathfrak{l}}(\mathcal{E}_{\mathfrak{l}})$ est la projection du groupe des \mathfrak{l} -unités (i.e. des unités en dehors de \mathfrak{l}) sur le tensorisé $\mathcal{K}_{\mathfrak{l}}^{\times}$ puis $v_{\mathfrak{l}}(\mathcal{E}_{\mathfrak{l}})$ le sous-groupe des valuations des \mathfrak{l} -unités pour la place \mathfrak{l} .

Lorsque h_K est étranger à ℓ , le groupe de Galois $\text{Gal}(C/K)$ qui s'identifie au ℓ -groupe fini des classes de diviseurs de K est trivial, si bien que les extensions C et K coïncident. Dans le cas contraire, le groupe de Galois $\text{Gal}(C/K) \simeq \mathbb{Z}_{\ell} / v_{\mathfrak{l}}(\mathcal{E}_{\mathfrak{l}})$ est cyclique non trivial et il existe une unique ℓ -extension non ramifiée L de K .

PROPOSITION 15. *Si $\mathcal{E}'_{\mathfrak{l}}$ désigne le noyau de la surjection canonique du tensorisé ℓ -adique $\mathcal{E}'_K = \mathbb{Z}_{\ell} \otimes_{\mathbb{Z}} E'_K$ du groupe des ℓ -unités (au sens ordinaire) de K dans le produit des complétés profinis $\mathcal{K}'_{\mathfrak{l}} = \prod_{v \neq \mathfrak{l}} \mathcal{K}_v^{\times}$ induite par les plongements diagonaux du groupe multiplicatif de K dans ses complétés aux places sauvages $v \neq \mathfrak{l}$, deux cas se présentent :*

- ou bien il existe une ℓ -unité de $\mathcal{E}'_{\mathfrak{l}}$ uniformisante locale (en \mathfrak{l}), auquel cas toutes les extensions L non ramifiées aux places modérées se ramifient en la place sauvage \mathfrak{l} ,
- ou bien il n'en existe pas, auquel cas l'une et seulement l'une des extensions L non ramifiées aux places modérées ne se ramifie pas en \mathfrak{l} . Les autres sont donc ramifiées en cette place.

PREUVE : le groupe de Galois de la ℓ -extension $M_{\mathfrak{l}}$ abélienne maximale qui est non ramifiée en dehors des places sauvages autres que \mathfrak{l} est isomorphe à $\mathcal{I}_K / (\mathcal{U}_{\mathfrak{l}} \prod_{q \nmid \ell} \mu_q \mathcal{R}_K)$ avec les notations de la preuve précédente. Comme K

est supposé \mathfrak{l} -rationnel, le ℓ -adifié du groupe de ses idèles est donné par $\mathcal{I}_K \simeq \mathcal{R}_K \prod_{\mathfrak{q} \neq \ell} \mu_{\mathfrak{q}} \mathcal{K}_{\mathfrak{l}}^{\times}$, de sorte qu'il vient :

$$\text{Gal}(M_{\mathfrak{l}}/K) \simeq \mathcal{I}_K / \mathcal{U}_{\mathfrak{l}} \left(\prod_{\mathfrak{q} \neq \ell} \mu_{\mathfrak{q}} \right) \mathcal{R}_K \simeq \mathcal{K}_{\mathfrak{l}}^{\times} / \mathcal{K}_{\mathfrak{l}}^{\times} \cap \left(\mathcal{U}_{\mathfrak{l}} \left(\prod_{\mathfrak{q} \neq \ell} \mu_{\mathfrak{q}} \right) \mathcal{R}_K \right),$$

$$(**) \quad \text{Gal}(M_{\mathfrak{l}}/K) \simeq \mathcal{K}_{\mathfrak{l}}^{\times} / s_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) \mathcal{U}_{\mathfrak{l}} \simeq \mathbb{Z}_{\ell} / v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}).$$

Et $\text{Gal}(M_{\mathfrak{l}}/K)$ est un ℓ -groupe cyclique, trivial sous la seule condition ($v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) = \mathbb{Z}_{\ell}$).

4.2 APPLICATION DE LA FORMULE DES CLASSES AMBIGES.

Le nombre de classes ambiguës (i.e. invariantes par G) de L est donné par la formule bien connue (cf. [Ja], p177, th. III.1.9) :

$$h_L^G = h_K \times \frac{\prod_{p \nmid \infty} e_p(L/K) \times \prod_{p \mid \infty} d_p(L/K)}{[L : K] \times (E_K : E_K \cap N_{L/K})}$$

qui devient ici

$$h_L^G = h_K \times \frac{\ell^{t-1} \times \prod_{\mathfrak{p} \mid \ell} e_{\mathfrak{p}}(L/K)}{(E_K : E_K \cap N_{L/K})}$$

si $t = t_{L/K}$ désigne le nombre de premiers modérés de K ramifiés dans l'extension L/K .

REMARQUES :

1/ Lorsque L/K désigne une extension cyclique de degré ℓ de corps de nombres ℓ -rationnels, les classes d'idéaux de L sont engendrées par la classe de la seule place sauvage, et sont ainsi des classes d'ambigues donc ambiguës (i.e. $h_L^G = h_L$).

2/ Comme l'extension L/K est de degré premier, le nombre relatif de classes est un entier (i.e. $h_K | h_L$) dès que l'extension est ramifiée.

De cette seconde remarque, découle immédiatement le résultat suivant :

SCOLIE 16. *Si K contient une racine primitive $\ell^{ième}$ de l'unité et si L/K désigne une extension ramifiée cyclique de degré ℓ de corps de nombres \mathfrak{L} -rationnels, alors le nombre h_L de classes de L est divisible par ℓ dès que le nombre h_K de classes de K l'est aussi.*

Afin d'évaluer l'indice normique $(E_K : E_K \cap N_{L/K})$, nous examinons tout d'abord l'indice $(E'_K : E'_K \cap N_{L/K})$.

LEMME 17. *Sous les mêmes hypothèses, si t désigne le nombre de places modérées ramifiées dans l'extension L/K et m le nombre de places sauvages non décomposées, l'indice normique $(E'_K : E'_K \cap N_{L/K})$ est ℓ^{t+m-1} .*

PREUVE : désignons par Cl'_L (resp. Cl'_K) le groupe des ℓ -classes de L (resp. K), c'est à dire le quotient du groupe des classes par son sous-groupe engendré par les classes des places sauvages. Le groupe des ℓ -classes d'un corps ℓ -rationnel étant trivial (cf. [JS], th. 1.7, (2')), la formule des ℓ -classes ambiguës qui s'écrit (cf. [Ja], p. 177, th. III.1.9) :

$$|Cl'_L|^G = |Cl'_K| \times \frac{\prod_{p \nmid \ell} e_p(L/K) \times \prod_{\nu \mid \ell} d_\nu(L/K)}{[L : K] \times (E'_K : E'_K \cap N_{L/K})}$$

donne immédiatement :

$$(E'_K : E'_K \cap N_{L/K}) = \ell^{t+m-1}$$

où $m = \sum_{\nu \mid \ell} v_\nu(d_\nu(L/K))$ est bien le nombre de places sauvages non décomposées dans l'extension L/K .

DÉFINITION 18. *Un nombre α est dit "norme à une unité près" dans l'extension L/K s'il existe une unité (globale) u de K telle que le produit αu soit effectivement norme dans l'extension L/K , en d'autres termes lorsque l'idéal principal (α) est norme d'un idéal principal de L .*

Ecrivons $(E'_K : E'_K \cap N_{L/K}) = (E'_K : E_K(E'_K \cap N_{L/K}))(E_K : E_K \cap N_{L/K})$. Nous obtenons ainsi :

LEMME 19. *L'indice normique $(E_K : E_K \cap N_{L/K})$ est égal à $\ell^{t+m-q-1}$, où q est la dimension sur \mathbb{F}_ℓ du quotient du groupe des ℓ -unités E'_K par le sous-groupe $E_K(E'_K \cap N_{L/K})$ des ℓ -unités qui sont normes à une unité près.*

La formule des classes ambiguës devient donc :

$$h_L^G = h_K \times \ell^{q-f}$$

où $f = f_{L/K}$ est le nombre de places sauvages inertes dans l'extension L/K . Deux cas se présentent alors :

- ou bien $v_\ell(\mathcal{E}_\ell) \neq \mathbb{Z}_\ell$, auquel cas $\ell|h_K$ (d'après (*)). Il existe alors une unique ℓ -extension cyclique L/K non ramifiée. Comme $C \subset M_\ell$, il vient de (**) et de l'hypothèse $v_\ell(\mathcal{E}_\ell) \neq \mathbb{Z}_\ell$ l'inégalité

$v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) \neq \mathbb{Z}_{\ell}$. Et l'extension non ramifiée L/K est la seule qui ne se ramifie pas en \mathfrak{l} . Or par la théorie du corps de classes locale, le groupe d'inertie de chacune des places finies p dans l'extension L/K est isomorphe au quotient du groupe des unités U_p de K_p par le sous-groupe de ses normes dans l'extension locale $L_{\mathfrak{p}}/K_p$. Par conséquent, si l'on considère l'extension non ramifiée L/K , les indices normiques $(U_p : U_p \cap N_{L_{\mathfrak{p}}/K_p})$ attachés aux places finies valent tous +1. Comme en les places infinies l'extension locale $L_{\mathfrak{p}}/K_p$ est triviale, les unités de K sont partout normes locales donc normes globales. La formule des classes ambiguës $h_L^G = h_K/\ell$ nous donne les équivalences successives :

$$(\ell|h_L) \iff (\ell|h_L^G) \iff (\ell^2|h_K).$$

Toutes les autres extensions L sont ramifiées en \mathfrak{l} . Dans ce cas, nous avons évidemment : $\ell|h_L$.

- ou bien $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) = \mathbb{Z}_{\ell}$, auquel cas $\ell \nmid h_K$. L'isomorphisme donné par (**)) impose alors deux cas :

- lorsque $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) = \mathbb{Z}_{\ell}$, elles sont toutes ramifiées en \mathfrak{l} . Comme ℓ ne divise pas h_K , ℓ divise h_L si et seulement si on a $q - f \geq 1$.

- sinon, parmi toutes les extensions L/K qui sont ℓ -ramifiées, une seule d'entre elles ne se ramifie pas en \mathfrak{l} . Toutes les autres sont ramifiées en la place sauvage \mathfrak{l} . Pour chacune d'elles, la formule des classes ambiguës donne :

$$(\ell|h_L) \iff (q - f \geq 1).$$

En résumé, il vient :

THÉORÈME 20. *Soit L une extension cyclique de degré ℓ , non ramifiée en dehors des places sauvages, d'un corps de nombres \mathfrak{l} -rationnel K , contenant les racines $\ell^{ièmes}$ de l'unité, totalement réelle si ℓ vaut 2. Si L est \mathfrak{l} -rationnelle, il existe alors une classe $c\ell(\tau)$ non triviale de E'_K/E_K^{ℓ} , telle qu'on ait $L = K(\sqrt[\ell]{\tau})$.*

Trois cas se présentent :

(i) *Pour $\ell \nmid h_K$ et $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) = \mathbb{Z}_{\ell}$, la place sauvage \mathfrak{l} est ramifiée dans L/K et l'ordre h_L du groupe des classes de L est divisible par ℓ si et seulement si on a $q - f \geq 1$.*

(ii) *Pour $\ell \nmid h_K$ et $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) \neq \mathbb{Z}_{\ell}$, il existe une unique extension L/K non ramifiée en \mathfrak{l} . L'ordre h_L de son groupe des classes est divisible par ℓ si et seulement si on a $q - f \geq 1$. Les autres telles extensions sont donc ramifiées en la place sauvage \mathfrak{l} et on a $\ell|h_L$ si et seulement si on a $q - f \geq 1$.*

(iii) *Pour $\ell|h_K$, il existe une unique extension L/K non ramifiée. L'ordre h_L de son groupe des classes est divisible par ℓ si et seulement si on a*

$\ell^2|h_K$. Les autres telles extensions sont donc ramifiées en la place sauvage \mathfrak{l} et $\ell|h_L$.

§5. Familles d'extensions de degré ℓ de corps de nombres \mathfrak{L} -rationnels :

5.1 CONSTRUCTION DES FAMILLES.

Nous rappelons que le lemme d'approximation par les X -unités nous permet de considérer le groupe $E'_K/E_K^{\times\ell}$ comme un sous-groupe de $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times\ell}$.

Définition 21. Soient K un corps de nombres \mathfrak{l} -rationnel contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité ζ , et totalement réel lorsque ℓ vaut 2, puis β une classe de $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times\ell} \setminus E'_K/E_K^{\times\ell}$.

Un corps de nombres L est dit “être membre de la famille β (notée $\text{Fam}(\beta)$)” si et seulement si $L = K(\sqrt[\ell]{\sigma})$, où σ est un représentant de la classe β dans $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times\ell}$, est une extension de degré ℓ dans laquelle au moins une place modérée p de K se ramifie.

Théorème 22. Soit K un corps de nombres \mathfrak{l} -rationnel et contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité ζ , et totalement réel lorsque ℓ vaut 2. Pour chaque classe β de $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times\ell} \setminus E'_K/E_K^{\times\ell}$, il existe une infinité de corps de nombres qui sont membres de la famille $\text{Fam}(\beta)$.

La clé de la preuve du résultat précédent est le résultat suivant :

Lemme 23. Soit K un corps de nombres \mathfrak{l} -rationnel contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité ζ et totalement réel lorsque ℓ est pair. Il existe un épimorphisme ϕ , de $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times\ell}$ dans le groupe de Galois $\text{Gal}(\overline{Z}'/K)$ de la sous-extension ℓ -élémentaire de la pro- ℓ -extension abélienne maximale de K , qui est ℓ -ramifiée et complètement décomposée aux places sauvages autres que \mathfrak{l} . De plus, le noyau de ϕ est $E'_K/E_K^{\times\ell}$. Autrement dit, on a la suite exacte courte canonique :

$$1 \longrightarrow E'_K/E_K^{\times\ell} \longrightarrow K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times\ell} \xrightarrow{\phi} \text{Gal}(\overline{Z}'/K) \longrightarrow 1.$$

PREUVE : le groupe de Galois de la ℓ -extension M^{ab} abélienne ℓ -ramifiée maximale (cf. [Ja], p.29, Exemple I.1.17.) est isomorphe à $G^{ab} = \text{Gal}(M^{ab}/K) \simeq \mathcal{I}_K / (\prod_{q \neq \ell} \mu_q) \mathcal{R}_K$. Comme K est supposé \mathfrak{l} -rationnel, le ℓ -adifié du groupe de

ses idèles est donné par l'isomorphisme $\mathcal{I}_K \simeq (\prod_{q \neq \ell} \mu_q) \mathcal{K}_{\mathfrak{l}}^{\times} \mathcal{R}_K$, de sorte qu'il

vient :

$$G^{ab} = \text{Gal}(M^{ab}/K) \simeq \mathcal{K}_l^\times / \mathcal{K}_l^\times \cap (\prod_{q \neq l} \mu_q \mathcal{R}_K) \simeq \mathcal{K}_l^\times / s_l(\mathcal{E}'_K).$$

De l'injectivité du morphisme (cf. [JS], th. 1.7, (3')), nous concluons : $\mathcal{K}_l' \cap \mathcal{R}_K \prod_{p \neq l} \mu_p = 1$ si bien que \mathcal{K}_l' s'injecte dans G^{ab} . Le quotient correspondant

$$G^{ab} / \mathcal{K}_l' \simeq \mathcal{I}_K / \mathcal{R}_K (\prod_{q \neq l} \mu_q) \mathcal{K}_l' \simeq K_l^\times / s_l(\mathcal{E}'_K) \simeq \mathbb{Z}_\ell^x$$

est sans torsion, si bien qu'il est isomorphe au groupe de Galois de la sous-extension Z' de la composée des \mathbb{Z}_ℓ -extensions, qui est l' -décomposée en toutes places sauvages autres que l . Finalement, il vient :

$$\text{Gal}(Z'/K) \simeq \mathcal{K}_l^\times / s_l(\mathcal{E}'_K) \quad \text{donc} \quad \text{Gal}(\overline{Z}'/K) \simeq \mathcal{K}_l^\times / s_l(\mathcal{E}'_K) \mathcal{K}_l^{\times \ell}$$

où \mathcal{E}'_K est le tensorisé ℓ -adique du groupe des ℓ -unités, $s_l(\mathcal{E}'_K)$ sa projection sur le tensorisé \mathcal{K}_l^\times et \overline{Z}' la sous-extension ℓ -élémentaire de Z' . Il existe donc un épimorphisme canonique de $K_l^\times / K_l^{\times \ell}$ dans le groupe de Galois de la ℓ -extension \overline{Z}' dont le noyau est clairement le quotient $s_l(\mathcal{E}'_K) \mathcal{K}_l^{\times \ell} / \mathcal{K}_l^{\times \ell}$ et est en particulier isomorphe à $\mathcal{E}'_K / \mathcal{E}'_K^\ell \simeq E'_K / E'_K^\ell$.

PREUVE DU THÉORÈME 22 : soit β une classe du groupe quotient $K_l^\times / K_l^{\times \ell}$; il résulte de l'uniforme répartition des automorphismes de Frobenius $\left(\frac{\overline{Z}'/K}{p} \right)$ dans le groupe de Galois de l'extension \overline{Z}'/K , et de l'épimorphisme donné par le lemme 23, qu'à la classe $\phi(\beta)$ correspond une infinité de places modérées p . Si de plus β n'appartient pas à E'_K / E'_K^ℓ , son image dans le groupe de Galois $\text{Gal}(\overline{Z}'/K) \simeq \mathcal{K}_l^\times / s_l(\mathcal{E}'_K) \mathcal{K}_l^{\times \ell}$ n'est pas triviale. Par suite, l'automorphisme de Frobenius $\left(\frac{\overline{Z}'/K}{p} \right)$ ne fixe pas la ℓ -extension \overline{Z}' , si bien que le premier modéré p est l -primitif et peut être complété en un ensemble l -primitif maximal de K .

5.2 CLASSIFICATION DES EXTENSIONS CYCLIQUES DE DEGRÉ ℓ .

On considère à présent les extensions L/K cycliques de degré ℓ , de corps de nombres l -rationnels contenant ζ une racine primitive $\ell^{i\text{ème}}$ de l'unité, totalement réels lorsque ℓ vaut 2, ramifiées en au moins une place modérée de K .

PROPOSITION 24. Soit K un corps de nombres \mathfrak{l} -rationnel contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité ζ ,

- si $\ell \nmid h_K$ et $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) = \mathbb{Z}_{\ell}$, alors la place \mathfrak{l} est non ramifiée dans les membres L de l'une de ces familles, et se ramifie dans toute autre famille.
- si $\ell|h_K$ ou $(\ell \nmid h_K \text{ et } v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) \neq \mathbb{Z}_{\ell})$, alors la place \mathfrak{l} se ramifie dans les membres de toutes les familles d'extensions.

PREUVE : notons S l'ensemble des places de X jointes aux places sauvages distinctes de \mathfrak{l} et désignons par E_K^S le groupe des S -unités (i.e. des unités globales en dehors des places de S). En considérant $E_K^S/E_K^{S,\ell}$ comme un hyperplan de l'espace vectoriel $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times,\ell}$, nous sommes assurés de l'existence de ℓ applications linéaires de $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times,\ell}$, triviales sur l'hyperplan $E_K^S/E_K^{S,\ell}$ et à valeurs dans le groupe μ_{ℓ} des racines $\ell^{i\text{èmes}}$ de l'unité. Par suite, si $[.,.]_{\mathfrak{l}}$ désigne la puissance $(m_{\mathfrak{l}}/\ell) - i\text{ème}$ du symbole de Hilbert en la place sauvage \mathfrak{l} , $m_{\mathfrak{l}}$ étant l'ordre du groupe $\mu_{\mathfrak{l}}$ des racines de l'unité de $K_{\mathfrak{l}}$ d'ordre une puissance de ℓ , $[\beta, .]_{\mathfrak{l}}$ est l'une des ℓ applications linéaires cherchées et est de plus, non partout triviale. Les autres applications linéaires sont clairement les symboles $[\beta^i, .]$. La recherche de ces ℓ applications linéaires nous caractérise donc la seule extension L/K non ramifiée en \mathfrak{l} .

• Plaçons nous d'abord dans le cas où $(\ell \mid h_K)$; il existe alors une unique extension L/K non ramifiée, si bien que la place sauvage \mathfrak{l} est ramifiée dans les membres de toutes familles d'extensions.

• Supposons à présent que $(\ell \nmid h_K)$; deux cas s'imposent alors :

- ou bien $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) = \mathbb{Z}_{\ell}$, auquel cas toutes les extensions L/K ℓ -ramifiées se ramifient en la place \mathfrak{l} qui est donc non ramifiée dans l'une de ces familles, mais ramifiée dans toutes les autres.

- ou bien $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) \neq \mathbb{Z}_{\ell}$, auquel cas \mathfrak{l} est non ramifiée dans une seule extension non triviale de la forme $L = K(\sqrt[\ell]{\tau})$ où τ est un représentant d'une classe de $E'_K/E_K'^{\ell}$, si bien que les membres de toutes les familles d'extensions sont ramifiées en \mathfrak{l} .

THÉORÈME 25. Soit K un corps de nombres contenant une racine primitive $\ell^{i\text{ème}}$ de l'unité et dont une place sauvage est notée \mathfrak{l} .

Si L désigne une extension cyclique de degré ℓ de corps de nombres \mathfrak{L} -rationnels ($\mathfrak{L}|\mathfrak{l}$), alors il existe une classe $cl(\sigma) = \beta$ de $E'_X/E_X'^{\ell} \simeq K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times,\ell}$, telle qu'on ait $L = K(\sqrt[\ell]{\sigma})$.

Le nombre q de représentants du quotient E'_K/E_K du groupe des ℓ -unités par son sous-groupe des unités globales, qui ne sont pas normes à unité près dans l'extension L/K , et le nombre f de places sauvages inertes dans l'extension, ne dépendent que de l'image β de σ dans $K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times,\ell}$ (et

par conséquent, sont indépendants du choix de l'ensemble \mathfrak{l} -primitif maximal X). Autrement dit, les extensions d'une même famille ont les mêmes indices q et f .

PREUVE : l'isomorphisme de dualité joint au lemme d'approximation par les X -unités nous donne les isomorphismes compatibles avec la structure (symplectique pour $\ell \neq 2$) définie par les symboles de Hilbert :

$$E'_X/E'_X{}^\ell \simeq K_{\mathfrak{l}}^\times/K_{\mathfrak{l}}^{\times\ell} \simeq \prod_{p \in X} (K_p^\times/K_p^{\times\ell}) \prod_{v|\ell, v \neq \mathfrak{l}} (K_v^\times/K_v^{\times\ell})$$

et montre qu'effectivement les images de $(\sigma \in E'_X)$ dans le ℓ -groupe quotient $K_{\mathfrak{l}}^\times/K_{\mathfrak{l}}^{\times\ell}$ sont indépendantes du choix de X . Ce qui établit que d'une part f , et d'autre part q (puisque une ℓ -unité est norme globale dès qu'elle l'est localement partout) ne dépendent que de l'image de σ dans $K_{\mathfrak{l}}^\times/K_{\mathfrak{l}}^{\times\ell}$.

THÉORÈME 26. Soit K un corps de nombres \mathfrak{l} -rationnel contenant une racine primitive $\ell^{\text{ème}}$ de l'unité.

La liste complète des extensions L cycliques \mathfrak{L} -rationnelles et de degré ℓ sur K comprend :

- d'une part les $\frac{\ell^{c+s}-1}{\ell-1}$ extensions $L = K(\sqrt[\ell]{\tau})$ où τ est un représentant d'une classe du groupe $E'_K/E'_K{}^\ell$, dans lesquelles aucun premier modéré de K se ramifie.

- d'autre part $\frac{\ell^{d+2-r}-\ell^{c+s}}{\ell-1}$ familles infinies d'extensions, dont les membres L se ramifient en au moins un premier modéré de K .

- Pour $\ell \nmid h_K$ et $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) = \mathbb{Z}_\ell$, les extensions $L = K(\sqrt[\ell]{\tau})$ où τ est un représentant d'une classe du groupe $E'_K/E'_K{}^\ell$ sont telles que la place sauvage \mathfrak{l} est ramifiée et que l'ordre h_L du groupe des classes de L est divisible par ℓ si et seulement si on a $q - f \geq 1$. De plus, il n'existe qu'une seule famille d'extensions dont les membres L ne se ramifient pas en \mathfrak{l} et dont l'ordre du groupe des classes est divisible par ℓ si et seulement si on a $q - f \geq 1$. Pour toute autre famille, la place sauvage \mathfrak{l} est ramifiée et l'ordre h_L associé aux membres est multiple de ℓ si et seulement si on a $q - f \geq 1$.

- Pour $\ell \nmid h_K$ et $v_{\mathfrak{l}}(\mathcal{E}'_{\mathfrak{l}}) \neq \mathbb{Z}_\ell$, il existe une seule extension $L = K(\sqrt[\ell]{\tau})$ (où τ est nécessairement un représentant d'une classe du groupe $E'_K/E'_K{}^\ell$) non triviale et non ramifiée en \mathfrak{l} . L'ordre h_L de son groupe des classes est divisible par ℓ si et seulement si on a $q - f \geq 1$. Les autres extensions cycliques ℓ -ramifiées de degré ℓ , sont ramifiées en la place sauvage \mathfrak{l} et ont pour ordre h_L un multiple de ℓ si et seulement si on a $q - f \geq 1$. Enfin, les membres de toutes les familles se ramifient en

la place sauvage ℓ et eux aussi, ont pour ordre un multiple h_L de ℓ si et seulement si on a $q - f \geq 1$.

• Pour $\ell|h_K$, il existe une unique extension non triviale et non ramifiée $L = K(\sqrt[\ell]{\tau})$ où τ est nécessairement un représentant d'une classe du groupe E'_K/E_K^{ℓ} . Et l'ordre h_L de son groupe des classes est divisible par ℓ si et seulement si l'ordre h_K l'est par ℓ^2 . Les autres extensions cycliques ℓ -ramifiées de degré ℓ , sont ramifiées en la place sauvage ℓ et ont pour ordre h_L un multiple de ℓ . Enfin, les membres de toutes les familles se ramifient en la place sauvage ℓ et eux aussi, ont pour ordre un multiple h_L de ℓ .

BIBLIOGRAPHIE

- [B₁] R. BERGER, *Quadratic extensions of number fields with elementary abelian 2-prim $K_2(\mathbb{M}_F)$ of smallest rank*, J. Number Theory **34** (1990), 284-292.
- [B₂] R. BERGER, *Class number parity and unit signature*, Arch. Math. **59** (1993), 427-435.
- [Ja] J.-F. JAULENT, *L'arithmétique des ℓ -extensions* (Thèse), Publ. Math. Fac. Sci. Besançon, Théor. Nombres, 13-43, 163-178, 1984/1985, 1985/1986 (1986).
- [JN] J.-F. JAULENT & T. NGUYEN QUANG DO, *Corps p -rationnels, corps p -réguliers, et ramification restreinte*, J. Théor. Nombres Bordeaux **5** (1994), 343-363.
- [JS] J.-F. JAULENT & O. SAUZET, *Pro- ℓ -extensions de corps de nombres ℓ -réguliers*, Prépublication.
- [GJ] G. GRAS et J.-F. JAULENT, *Sur les corps de nombres réguliers*, Math.Z.202 (1989), 343-365.
- [Se] J.-P. SERRE, *Corps Locaux*, Hermann, Paris (1968), 17-34, 211-238.
- [So] F. SORIANO, *Extensions cycliques de degré ℓ de corps de nombres ℓ -réguliers*, J. Théor. Nombres Bordeaux **4** (1994), 407-420.

Florence SORIANO
 Laboratoire de Mathématiques
 U.F.R. / S.F.A.
 40 avenue du Recteur Pineau
 86 022 POITIERS CEDEX, FRANCE
 e-mail : soriano@matpts.univ-poitiers