Pro-ℓ-extensions de corps de nombres $\mathfrak{l}$-rationnels*

Jean-François JAULENT et Odile SAUZET

Version corrigée

Résumé. Nous introduisons ici la notion de corps de nombres $\mathfrak{l}$-rationnel K relativement à une place $\mathfrak{l}$ au-dessus d'un nombre premier ℓ, qui généralise celle de corps ℓ-rationnel (ou ℓ-régulier) déjà considérée par plusieurs auteurs en relation avec la K-théorie, et nous en discutons diverses propriétés. Nous définissons ensuite la notion d'ensemble de places $\mathfrak{l}$-primitif qui permet de décrire le groupe de Galois de la pro-ℓ-extension maximale d'un tel corps comme pro-ℓ-produit de groupe de Galois locaux et de caractériser les ℓ-extensions ℓ-ramifiées en termes de ramification modérée. Le tout est illustré par des exemples numériques obtenus par le système PARI.

Abstract. For a prime $\mathfrak{l}$ dividing a prime number ℓ, we define what it is for a number field K to be $\mathfrak{l}$-rational. We discuss a special case : the ℓ-birational fields, rational for two places over ℓ. We give a definition for a $\mathfrak{l}$-primitive set of tame primes, X, that let us write the Galois group of the maximal ℓ-ramified ℓ-extension of K as the free pro-ℓ-product of the decomposition groups of primes dividing $\ell X \infty$. This way we get a condition on the ramification for an ℓ-extension of K to be rational. Numerical exemples are given.

Sommaire

*J. Number Theory **65** (1997), 240–267 & **80** (2000), 318–319.

0. Introduction et Notations

0.a Position du problème

La notion de corps ℓ-régulier, déjà rencontrée implicitement sous forme d'une hypothèse technique par divers auteurs (notamment H. Miki [Mi] ou J.-F. Jaulent [J1]) à l'occasion de l'étude d'une condition suffisante de la conjecture de Leopoldt, a été explicitement définie par G. Gras et J.-F. Jaulent (cf [GJ]) par référence au ℓ-noyau $R_2(K)$ des symboles réguliers dans le groupe universel $K_2(K)$: en présence des racines ℓ-ièmes de l'unité (en fait sous une hypothèse plus faible), les corps de nombres K pour lesquels le ℓ-sous-groupe de Sylow $R_2(K)$ du noyau régulier est trivial sont exactement ceux qui vérifient les deux conditions :

(a) K admet une unique place $\mathfrak{l}$ au dessus du premier ℓ et

(b) le ℓ-groupe $\mathcal{C}l'_K$ des ℓ-classes de diviseurs de K (i.e. le quotient du ℓ-groupe des classes d'idéaux prises au sens restreint par le sous groupe engendré par les classes d'idéaux construits sur les places au dessus de ℓ) est trivial ;

de sorte que la terminologie introduite généralise naturellement la notion de nombre premier régulier utilisée dans la classification des corps cyclotomiques $\mathbb{Q}[\zeta_\ell]$.

Toujours sous la même condition $\zeta_\ell \in K$, la notion de ℓ-régularité se trouve en outre (comme expliqué dans [JN]) coïncider avec celle de ℓ-rationalité introduite indépendamment par A. Movahhedi et T. Nguyen Quang Do (cf [MN]) si bien que les corps ℓ-réguliers sont aussi caractérisés par le fait que le groupe de Galois $G_S = Gal(K_S/K)$ attaché à leur pro-ℓ-extension ℓ-ramifiée ∞-décomposée maximale K_S a la structure la plus simple qui soit : c'est un pro-ℓ-groupe libre de rang $c_K + 1$ (où c_K désigne le nombre de places complexes de K). On retrouve là en particulier le fait qu'un corps ℓ-régulier satisfait évidemment la conjecture de Leopoldt puisqu'il possède bien exactement $(c_K + 1)$ $\mathbb{Z}_\ell$-extensions linéairement indépendantes.

Si l'on revient maintenant sur les deux conditions (a) et (b) données plus haut, une dissymétrie saute aux yeux : autant il parait naturel, si l'on souhaite seulement que l'arithmétique des ℓ-extensions d'un corps de nombre soit relativement simple, d'exiger qu'un certain ℓ-groupe de classes soit trivial, autant refuser toute décomposition dans K du premier ℓ considéré peut sembler exagérément sévère au regard du résultat attendu.

Notre propos dans cet article est donc clair : il s'agit d'introduire une nouvelle classe de corps de nombres, que nous proposons ici d'appeler $\mathfrak{l}$-rationnels, ne satisfaisant plus nécessairement la condition (a) jugée trop restrictive, mais vérifiant en revanche une hypothèse de trivialité, plus dure que la seule condition (b) mais moins dure que (a) et (b) réunies, et néanmoins suffisante pour autoriser une description particulièrement simple de la pro-ℓ-extension ℓX-ramifiée maximale d'un tel corps, pour tout ensemble fini X de places modérées de K satisfaisant une propriété convenable de primitivité.

Les résultats que nous obtenons, qui prennent appui sur les techniques de corps de classe ℓ-adique développées dans [J1], permettent ainsi de conserver la plupart des résultats récapitulés dans [JN] (au prix naturellement de quelques complications) et redonnent en particulier des théorèmes de propagation de la rationalité, via une généralisation convenable de la notion d'ensemble primitif de places modérées. Ils recoupent en outre plusieurs résultats de K. Winberg (cf [W1], [W2]) dont la parenté avec ceux de [GJ] ou [MN] était jusqu'ici partiellement passée inaperçue et permettent incidemment de compléter la classification des corps de nombres introduite par L.V. Kuz'min (cf [Ku]) puisque l'implantation récente du calcul des groupes de classes de rayons dans le système PARI de calcul formel développé à Bordeaux nous a permis d'illustrer numériquement les notions que nous introduisons ici.

Les corps $\mathfrak{l}$-rationnels ainsi construits constituent finalement une nouvelle classe de corps de nombres K qui satisfont pour des raisons purement algébriques les conjectures ℓ-adiques de Leopoldt et de Gross, dont la $\mathbb{Z}_\ell$-extension cyclotomique est un corps surcirculaire de genre nul (suivant la terminologie introduite dans [Jo] et discutée dans [JM]), et qui vérifient en outre une propriété galoisienne introduite par M. Yamagishi (cf [Ya]) : le rang ρ d'une extension pro-ℓ-libre d'un tel corps est en général majoré par le nombre de places complexes c de K; il est donc strictement plus petit que le rang $c+1$ de la composée des $\mathbb{Z}_\ell$-extensions.

0.b Index des principales notations

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

Notations attachées à un corps local $K_\mathfrak{p}$:

- $\bar{K}_\mathfrak{p}$: la pro-ℓ-extension (galoisienne) maximale de $K_\mathfrak{p}$,
- $\mathcal{G}_\mathfrak{p}$: le groupe de Galois $Gal(\bar{K}_\mathfrak{p}/K_\mathfrak{p})$,
- $\bar{K}_\mathfrak{p}^{ab}$: la pro-ℓ-extension abélienne maximale de $K_\mathfrak{p}$,
- $\mathcal{G}_\mathfrak{p}^{ab}$: le groupe de Galois $Gal(\bar{K}_\mathfrak{p}^{ab}/K_\mathfrak{p})$,
- $\mathcal{R}_\mathfrak{p} = \varprojlim K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times\ell^n} \simeq \mathcal{G}_\mathfrak{p}^{ab}$: le compactifié ℓ-adique de $K_\mathfrak{p}^\times$,
- $\mu_\mathfrak{p} = \mathcal{R}_\mathfrak{p}^{tor}$: le ℓ-groupe des racines de l'unité dans $K_\mathfrak{p}$,
- $\widetilde{v}_\mathfrak{p}$: la valuation logarithmique sur $\mathcal{R}_\mathfrak{p}$ à valeurs dans $\mathbb{Z}_\ell$,
- $\widetilde{\mathcal{U}}_\mathfrak{p} = ker\ \widetilde{v}_\mathfrak{p}$: le sous groupe des normes cyclotomiques dans $\mathcal{R}_\mathfrak{p}$.

Notations attachées à un corps de nombres K :

- Pl_r, Pl_c, Pl_ℓ : l'ensemble des places réelles, complexes ou ℓ-adiques,
- r, c, l : les nombres de places réelles, complexes ou ℓ-adique de K,
- S un sous-ensemble non vide des des places sauvages (i.e. ℓ-adiques) de K,
- s le nombre de places dans S,
- X un ensemble de places finies modérées (i.e. étrangères à ℓ) de K,
- $\mathcal{J} = \prod_\mathfrak{p}^{res} \mathcal{R}_\mathfrak{p}$: le ℓ-adifié du groupe des idèles de K,
- $\widetilde{\mathcal{J}}$: le noyau dans $\mathcal{J}$ de la formule du produit pour les valeurs absolues,
- $\mathcal{R} = \mathbb{Z}_\ell \otimes_\mathbb{Z} K^\times$: le sous-groupe des idèles principaux,
- $\widetilde{\mathcal{U}} = \prod_\mathfrak{p} \widetilde{\mathcal{U}}_\mathfrak{p}$: le groupe des normes cyclotomiques dans $\mathcal{J}$,
- $\widetilde{\mathcal{D}\ell} = \widetilde{\mathcal{J}}/\widetilde{\mathcal{U}}$: le ℓ-groupe des diviseurs logarithmiques,
- $\widetilde{\mathcal{P}\ell} = \mathcal{R}\widetilde{\mathcal{U}}/\widetilde{\mathcal{U}}$: le sous-groupe des diviseurs logarithmiques principaux,
- $\widetilde{\mathcal{C}\ell} = \widetilde{\mathcal{J}}/\widetilde{\mathcal{U}}\mathcal{R} = \widetilde{\mathcal{D}\ell}/\widetilde{\mathcal{P}\ell}$: le ℓ-groupe des classes logarithmiques,
- $\mathcal{U}' = \prod_{\mathfrak{l}|\ell} \mathcal{R}_\mathfrak{l} \prod_{\mathfrak{p}\nmid\ell} \mathcal{U}_\mathfrak{p}$: le groupe des ℓ-unités,

- $\mathcal{C}l' = \mathcal{J}/\mathcal{U}'\mathcal{R}$: le ℓ-groupe des ℓ-classes de diviseurs au sens ordinaire,
- $\mathcal{E}' = \mathcal{R} \cap \mathcal{U}' \simeq \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E'_K$: le ℓ-groupe des ℓ-unités,
- $\widetilde{\mu} = \prod_{\mathfrak{p}} \mu_{\mathfrak{p}}$: le sous groupe fermé des racines de l'unité dans $\mathcal{J}$,
- μ : le ℓ-groupe des racines de l'unité dans $\mathcal{R}$ ($= \widetilde{\mu} \cap \mathcal{R}$ sous Leopoldt).

Quelques pro-ℓ-extensions de K :

- K^c : $\mathbb{Z}_\ell$-extension cyclotomique,
- K^{lc} : pro-ℓ-extension abélienne localement cyclotomique maximale,
- K^z : compositum des $\mathbb{Z}_\ell$-extensions,
- K^{bp} : compositum des ℓ-extensions cycliques de K localement $\mathbb{Z}_\ell$-plongeables,
- K^{ab}_ℓ : pro-ℓ-extension abélienne ℓ-ramifiée maximale (i.e. non ramifiée aux places finies étrangères à ℓ, éventuellement complexifiée aux places réelles),
- $K^{ab}_{\ell X}$: pro-ℓ-extension abélienne ℓX-ramifiée maximale (i.e. non ramifiée aux places finies étrangères à ℓ non contenues dans X, éventuellement complexifiée aux places réelles)

1. Extensions $\mathfrak{l}$-rationnelles de $\mathbb{Q}[\zeta_\ell]$

Soit ℓ un nombre premier. La notion centrale de cet article est celle de corps $\mathfrak{l}$-rationnel que nous pouvons introduire comme suit :

Définition 1.1. *Nous disons qu'un corps de nombre K contenant les racines ℓ-ièmes de l'unité est $\mathfrak{l}$-rationnel en une place $\mathfrak{l}$ au dessus de ℓ lorsque la ℓ-extension (abélienne) ℓ-ramifiée $\mathfrak{l}$-décomposée maximale de K est triviale.*

Remarques.

(i) Il est indifférent dans la définition précédente de mettre ou non la condition d'abélianité.

(ii) Lorsque K possède une unique place $\mathfrak{l}$ au dessus de ℓ, la condition précédente postule la trivialité de la ℓ-extension abélienne maximale ℓ-ramifiée ℓ-décomposée de K , en d'autre termes , via la correspondance du corps de classes, la trivialité du ℓ-groupe des ℓ-classes d'idéaux au sens restreint du corps K ce qui est bien l'une des définitions équivalente de la ℓ-régularité (ou ℓ-rationalité) données par [GJ], [MN] et [JN].

Nous commençons par discuter dans ce qui suit diverses caractérisations de la $\mathfrak{l}$-rationalité, par la théorie ℓ-adique du corps de classes d'abord, par la théorie de Kummer ensuite. L'opposition entre ces caractérisations et leurs reflets respectifs dans le miroir de Leopoldt est, en effet, essentielle dans la généralisation de la $\mathfrak{l}$-rationalité au cas non kummérien étudié dans la section 2.

1.a Interprétation corps de classes de la $\mathfrak{l}$-rationalité

Proposition 1.2. *Un corps K contenant les racines ℓ-ièmes de l'unité est $\mathfrak{l}$-rationnel si et seulement si on a l'identité entre les groupes d'idèles :*

$$(1) \quad \mathcal{J} = \mathcal{R}\mathcal{R}_{\mathfrak{l}} \prod_{\mathfrak{p} \nmid \ell\infty} \mu_{\mathfrak{p}}$$

Preuve. Le membre de droite de l'égalité n'est autre, en effet, que le sous-groupe fermé de $\mathcal{J}$ attaché par la théorie ℓ-adique du corps de classes à la ℓ-extension abélienne ℓ-ramifiée $\mathfrak{l}$-décomposée maximale de K.

Théorème 1.3. *La condition (1) est satisfaite dans un corps de nombre K (contenant ou non les racines ℓ-ièmes de l'unité) si et seulement si les deux conditions suivantes se trouvent réunies :*

(2) le groupe des ℓ-classes d'idéaux (au sens ordinaire) Cl' du corps K est trivial ;

(3) et l'application de semi-localisation $s'_{\mathfrak{l}}$ induit une surjection du tensorisé $\mathcal{E}'$ du groupe des ℓ-unités (au sens ordinaire) de K sur le produit $\mathcal{R}'_{\mathfrak{l}} = \prod'_{\mathfrak{p}|\ell\infty} \mathcal{R}_{\mathfrak{p}}$ étendu aux places $\mathfrak{l}' \neq \mathfrak{l}$ divisant ℓ et aux places réelles.

Preuve. Introduisons le facteur semi-local $\mathcal{R}_{\ell\infty} = \prod_{\mathfrak{p}|\ell\infty} \mathcal{R}_{\mathfrak{p}} = \mathcal{R}_{\mathfrak{l}}.\prod'_{\mathfrak{p}|\ell\infty} \mathcal{R}_{\mathfrak{p}}$. Nous obtenons immédiatement l'équivalence annoncée par :

$$(1)\quad \mathcal{J} = \mathcal{R}\mathcal{R}_{\mathfrak{l}} \prod_{\mathfrak{p}\nmid\ell\infty} \mu_{\mathfrak{p}} \Leftrightarrow \begin{cases} (2)\quad \mathcal{J} = \mathcal{R}\mathcal{R}_{\ell\infty} \prod\limits_{\mathfrak{p}\nmid\ell\infty} \mu_{\mathfrak{p}},\ \textit{et} \\ (3)\quad \mathcal{R}\mathcal{R}_{\ell\infty} \prod\limits_{\mathfrak{p}\nmid\ell\infty} \mu_{\mathfrak{p}} = \mathcal{R}\mathcal{R}_{\mathfrak{l}} \prod\limits_{\mathfrak{p}\nmid\ell\infty} \mu_{\mathfrak{p}} \end{cases}$$

Scolie 1.4. *Lorsque la condition (3) est satisfaite il existe en particulier dans K des ℓ-unités de toutes signatures. La trivialité du ℓ-groupe des ℓ-classes d'idéaux exigé par la condition (2) peut donc être prise indifféremment au sens ordinaire ou au sens restreint.*

Corollaire 1.5. *Soit K satisfaisant la condition (1). Alors K est logarithmiquement principal, en ce sens que son ℓ-groupe des classes logarithmiques $\widetilde{Cl}$ est trivial. En d'autres termes une ℓ-extension de K est cyclotomique (i.e. contenue dans la $\mathbb{Z}_\ell$-extension cyclotomique K^c de K) dès qu'elle l'est localement. En particulier K vérifie banalement la conjecture de Gross généralisée (pour le premier ℓ).*

Preuve. Sous la condition (1), le noyau $\widetilde{\mathcal{J}}$ de la formule du produit pour les valeurs absolues ℓ-adiques est donné par : $\widetilde{\mathcal{J}} = \mathcal{R}\widetilde{\mathcal{R}}_{\mathfrak{l}} \prod_{\mathfrak{p}\nmid\ell\infty} \mu_{\mathfrak{p}}$ et $\widetilde{\mathcal{R}}_{\mathfrak{l}}$ n'est autre que le sous-groupe $\widetilde{\mathcal{U}}_{\mathfrak{l}}$ des normes cyclotomiques dans $\mathcal{R}_{\mathfrak{l}}$. Il vient donc comme annoncé $\widetilde{\mathcal{J}} \subset \mathcal{R}\widetilde{\mathcal{U}}$ i.e. $\widetilde{\mathcal{C}\ell} = \widetilde{\mathcal{J}}/\mathcal{R}\widetilde{\mathcal{U}} = 1$. En particulier le corps K vérifie évidemment la conjecture de Gross géneralisée qui postule la finitude du groupe $\widetilde{\mathcal{C}\ell}$. Enfin $\widetilde{\mathcal{C}\ell}$ s'interprète d'après [J2] comme étant le groupe de Galois $Gal(K^{lc}/K^c)$ où K^{lc} est la ℓ-extension localement cyclotomique maximale de K.

Remarque. Désignons par r, c et l les nombres respectifs de places réelles , complexes et ℓ-adiques de K . Si $d = [K_{\mathfrak{l}} : \mathbb{Q}_\ell]$ et $n = r + 2c = [K : \mathbb{Q}]$ sont respectivement les degrés local et global, nous concluons des isomorphismes $\mathcal{E}' \simeq \mu\mathbb{Z}_\ell^{r+c+l-1}$ et $\mathcal{R}'_{\mathfrak{l}} \simeq \mu'_{\mathfrak{l}}\mathbb{Z}_\ell^{r+2c-d+(l-1)}$ que l'application $s'_{\mathfrak{l}}$ ne peut envoyer $\mathcal{E}'$ sur $\mathcal{R}'_{\mathfrak{l}}$ que sous les conditions de rang $d \geq c$, si μ et $\mu'_{\mathfrak{l}}$ sont triviaux, et même $d \geq r + c + s - 2$ s'ils ne le sont pas .

1.b Interprétation kummérienne de la $\mathfrak{l}$-rationalité

Proposition 1.6. *Un corps de nombres K contenant μ_ℓ est $\mathfrak{l}$-rationnel pour une place $\mathfrak{l}$ au-dessus de ℓ si et seulement si l'application naturelle induite par la localisation des radicaux $\mathcal{R}/\mathcal{R}^\ell \to \mathcal{R}_\mathfrak{l}/{\mathcal{R}_\mathfrak{l}}^\ell \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p}{\mathcal{R}_\mathfrak{p}}^\ell)$ est injective , en d'autres termes si et seulement si le plongement naturel du sous-module principal $\mathcal{R}$ dans le groupe des idèles $\mathcal{J}$ induit une injection à conoyau $\mathbb{Z}_\ell$-libre de $\mathcal{R}$ dans $\mathcal{R}_\mathfrak{l} \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p})$, ce que nous résumons en écrivant :*

$$(1') \quad \mathcal{R} \rightarrowtail \mathcal{R}_\mathfrak{l} \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p}) \simeq \mathcal{R}_\mathfrak{l} \oplus \mathcal{I}d'.$$

Preuve. La première affirmation s'obtient en observant que le noyau de l'application naturelle $\mathcal{R}/\mathcal{R}^\ell \to \mathcal{R}_\mathfrak{l}/{\mathcal{R}_\mathfrak{l}}^\ell \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p}.{\mathcal{R}_\mathfrak{p}}^\ell)$ n'est autre que le radical kummérien attaché à la ℓ-extension abélienne élémentaire maximale de K qui est complè- tement décomposée en la place $\mathfrak{l}$ et non ramifiée aux places finies $\mathfrak{p} \nmid \ell$. Il en résulte immédiatement que $\mathcal{R}$ s'identifie à un sous-module pur de la somme $\mathcal{R}_\mathfrak{l} \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p}) \simeq \mathcal{R}_\mathfrak{l} \oplus \mathcal{I}d'$ où $\mathcal{I}d'$ désigne le $\mathbb{Z}_\ell$-module libre construit sur les idéaux premiers de K étranger à ℓ. En effet, puisque $\mathcal{R}$ contient par hypothèse les racines ℓ-ièmes de l'unité, son image dans $\mathcal{R}_\mathfrak{l} \oplus \mathcal{I}d'$ contient le sous groupe de torsion $\mu_\mathfrak{l}$ de $\mathcal{R}_\mathfrak{l}$ et le quotient correspondant est donc sans $\mathbb{Z}_\ell$-torsion.

Théorème 1.7. *Le plongement naturel du sous-module principal $\mathcal{R} = \mathbb{Z}_l \otimes_\mathbb{Z} K^\times$ dans le ℓ-adifié $\mathcal{J}$ du groupe des idèles de K induit une injection à conoyau $\mathbb{Z}_\ell$-libre de $\mathcal{R}$ dans la somme directe $\mathcal{R}_\mathfrak{l} \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p})$ (i.e. K vérifie la condition (1')) dès que les deux conditions suivantes se trouvent réunies :*

(2') le groupe des ℓ-classes d'idéaux (au sens ordinaire) $\mathcal{C}l'$ du corps K est trivial, et

(3') l'application de localisation $s_\mathfrak{l}$ induit une injection à conoyau $\mathbb{Z}_\ell$-libre du tensorisé $\mathcal{E}'$ du groupe des ℓ-unités (au sens ordinaire) de K dans le compactifié ℓ-adique $\mathcal{R}_\mathfrak{l}$ du groupe multiplicatif $K_\mathfrak{l}^\times$.

Ces conditions sont également nécessaires en présence des racines ℓ-ièmes de l'unité.

L'exemple suivant illustre la nécessité d'avoir une hypothèse sur les racines ℓ-ièmes de l'unité dans le théorème 1.7.

Exemple. Soient $k_0 = \mathbb{Q}[\sqrt{-1}]$, puis k l'unique extension de degré 5 sur k_0 contenue dans $\mathbb{Q}[\zeta_{124}]$ et k_1 le premier étage de la $\mathbb{Z}_5$-extension cyclotomique de k_0. Il est montré dans [W3] que les sous-corps K de kk_1 de degré 5 sur k_0 autre que k et k_1 vérifient la condition (1') pour $\mathfrak{l}$ au-dessus de $\ell = 5$ mais non la condition (2').

Preuve. Le groupe $\mathcal{E}'$ est, en effet, un sous-module pur de $\mathcal{R}$ d'image triviale dans la somme directe $\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p}$; c'est donc sous la condition (1') un sous-module pur du premier facteur $\mathcal{R}_\mathfrak{l}$. L'équivalence s'obtient alors en observant que la somme de droite $\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p}$ s'identifie au $\mathbb{Z}_\ell$-module libre construit sur les idéaux premiers étrangers à ℓ et qu'il contient comme sous-module d'indice fini l'image de $\mathcal{R}/\mathcal{E}'$ isomorphe au sous-module principal.

Remarque. La condition (3') impose en particulier l'isomorphisme $\mu \simeq \mu_\mathfrak{l}$ entre les ℓ-groupes de racines globales et locales de l'unité.

Corollaire 1.8. *Soit K satisfaisant (1'). Alors K vérifie banalement la conjecture de Leopoldt (pour le premier ℓ) et le groupe de Galois $Gal(K^h/K) \simeq \mathcal{J}/\mathcal{R}\prod_{\mathfrak{p}}\mu_{\mathfrak{p}}$ de la composée K^h des ℓ-extensions cycliques de K qui sont localement $\mathbb{Z}_\ell$-plongeables est un $\mathbb{Z}_\ell$-module libre de dimension $c+1$.*

Preuve. Par (3') le tensorisé $\mathcal{E}'$ du groupe des ℓ-unités s'injecte dans $\mathcal{R}_{\mathfrak{l}}$; il en va donc de même du sous module $\mathcal{E}$ construit sur les unités, et K vérifie la conjecture de Leopoldt. Ce point acquis, considérons la composée K^h des ℓ-extensions cycliques de K qui sont localement $\mathbb{Z}_\ell$-plongeables. Puisque le sous-module de torsion $\mu_{\mathfrak{p}}$ de $\mathcal{R}_{\mathfrak{p}}$ mesure précisément en la place $\mathfrak{p}$ l'obstruction locale à un $\mathbb{Z}_\ell$-plongement, le groupe d'idèles associé par le théorie du corps de classes est le produit $\mathcal{R}\prod_{\mathfrak{p}}\mu_{\mathfrak{p}}$. Le quotient correspondant $\mathcal{J}/\mathcal{R}\prod_{\mathfrak{p}}\mu_{\mathfrak{p}}$ est ainsi un $\mathbb{Z}_\ell$-module de type fini, de rang essentiel $c+1$ puisque K vérifie la conjecture de Leopoldt. Cela étant, d'après l'assertion (1') le groupe $\mathcal{R}$ des idèles principaux s'identifie à un sous-module pur du groupe d'idèles $\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_{\mathfrak{p}}/\mu_{\mathfrak{p}}$ et donc a fortiori du groupe $\mathcal{R}_\ell \oplus \mathcal{R}_\infty \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_{\mathfrak{p}}/\mu_{\mathfrak{p}})$. Le quotient modulo la torsion $\mathcal{J}/\mathcal{R}\prod_{\mathfrak{p}}\mu_{\mathfrak{p}}$ est ainsi un $\mathbb{Z}_\ell$-module sans torsion, donc libre de rang $c+1$ d'après ce qui précède.

Remarque. Des isomorphismes $\mathcal{E}' \simeq \mu\mathbb{Z}_\ell^{r+c+l-1}$ et $\mathcal{R}_{\mathfrak{l}} \simeq \mu_{\mathfrak{l}}\mathbb{Z}_\ell^{d+1}$, on conclut que $\mathcal{E}'$ ne peut s'injecter dans $\mathcal{R}_{\mathfrak{l}}$ que sous la condition de rang $r+c+l-1 \leq d+1$. On retrouve ainsi l'inégalité nécessaire $d \geq r+c+l-2$ déjà obtenue.

1.c Application aux corps ℓ-birationnels

Définition & Proposition 1.9. *Nous disons qu'un corps de nombres K contenant les racines ℓ-ièmes de l'unité est ℓ-birationnel lorsqu'il est rationnel pour au moins (et donc exactement) deux places au-dessus de ℓ. Un tel corps est totalement imaginaire et possède en tout et pour tout deux places au-dessus de ℓ.*

Preuve. Supposons K rationnel en, disons, $\mathfrak{l}$ et $\mathfrak{l}'$ au dessus de ℓ. L'assertion (3') du théorème 1.7 appliquée en la place $\mathfrak{l}$ nous dit que le tensorisé $\mathcal{E}'$ du groupe des ℓ-unités de K s'envoie injectivement dans le compactifié $\mathcal{R}_{\mathfrak{l}}$, et l'assertion (3) du théorème 1.3 appliquée en $\mathfrak{l}'$ que le même tensorisé s'envoie surjectivement sur le produit $\prod_{\mathfrak{p}|\ell\infty,\mathfrak{p}\neq\mathfrak{l}'}\mathcal{R}_{\mathfrak{p}}$. Il en résulte que $\mathfrak{l}$ et $\mathfrak{l}'$ sont les seules places de K au dessus de ℓ ; de plus, nous avons $\mathcal{R}_{\mathfrak{p}} = 1$, pour tout $\mathfrak{p}|\infty$ donc ou bien $\ell \neq 2$ et K, qui contient ζ_ℓ est totalement imaginaire, ou bien $\ell = 2$ et $r = 0$ auquel cas K est encore totalement imaginaire.

Remarque. Les corps birationnels sont exactement ceux du type B dans la classification de L.V. Kuz'min (cf [Ku] Fundamental Theorem) comme il résulte du théorème 1.11 ci-dessous.

Pour établir l'équivalence entre les diverses caractérisations de la ℓ-birationalité, nous avons besoin d'un résultat technique essentiellement bien connu (cf [MN], lemme 2.4 ou [JN], lemme 3.1) dont il peut être commode de donner une courte preuve :

Lemme 1.10. *Soient G et H deux pro-ℓ-groupes et $\phi : H \to G$ un morphisme surjectif . Pour que ϕ soit un isomorphisme il suffit que les conditions suivantes soient remplies :*

(i) L'application $H^{ab} \to G^{ab}$ induite par ϕ est un isomorphisme ;

(ii) $H^2(G, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 1$.

Preuve. Soit N le noyau de ϕ ; la suite exacte d'inflation-restriction à coefficients dans $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ s'écrit :

$$1 \to H^1(G, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \to H^1(H, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \to H^1(N, \mathbb{Q}_\ell/\mathbb{Z}_\ell)^G \to H^2(G, \mathbb{Q}_\ell/\mathbb{Z}_\ell).$$

Les conditions (i) et (ii) donnent alors $H^1(N, \mathbb{Q}_\ell/\mathbb{Z}_\ell)^G = 1$, donc $H^1(N, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 1$ et finalement $N = 1$, comme annoncé.

Théorème 1.11. *Soient K un corps de nombres contenant les racines ℓ-ièmes de l'unité et admettant au moins deux places $\mathfrak{l}$ et $\mathfrak{l}'$ au-dessus de ℓ, puis K_ℓ la pro-ℓ-extension maximale ℓ-ramifiée de K et K_ℓ^{ab} la sous-extension abélienne maximale de K_ℓ. Les assertions suivantes sont équivalentes :*

(i) K est ℓ-birationnel ;

(ii) K est totalement imaginaire, admet exactement deux places $\mathfrak{l}$ et $\mathfrak{l}'$ au-dessus de ℓ, son ℓ-groupe des ℓ-classes est trivial et les applications de localisation induisent des isomorphismes :

$$\mathcal{R}_\mathfrak{l} \simeq \mathcal{E}' \simeq \mathcal{R}_{\mathfrak{l}'}$$

(iii) Le groupe de Galois global $Gal(K_\ell^{ab}/K)$ coïncide avec les sous-groupes de décomposition $D_\mathfrak{l}(K_\ell^{ab}/K)$ et $D_{\mathfrak{l}'}(K_\ell^{ab}/K)$ et l'on a :

$$Gal(K_\ell^{ab}/K) \simeq Gal(\bar{K}_\mathfrak{l}^{ab}/K_\mathfrak{l}) \simeq Gal(\bar{K}_{\mathfrak{l}'}^{ab}/K_{\mathfrak{l}'})$$

(iv) Le groupe de Galois global $Gal(K_\ell/K)$ s'identifie de même aux groupes de Galois locaux :

$$Gal(K_\ell/K) \simeq Gal(\bar{K}_\mathfrak{l}/K_\mathfrak{l}) \simeq Gal(\bar{K}_{\mathfrak{l}'}/K_{\mathfrak{l}'}).$$

Preuve. Nous avons successivement :

(i)$\Leftrightarrow$(ii) en vertu de la discussion ci-dessus : en effet, la condition (2)=(2') exprime la trivialité du groupe $\mathcal{C}l'$ et les conditions (3) et (3') données plus haut (cf th. 1.3 et th. 1.7) montrent que les applications $s_\mathfrak{l} : \mathcal{E}' \to \mathcal{R}_\mathfrak{l}$ et $s'_\mathfrak{l} : \mathcal{E}' \to \mathcal{R}_{\mathfrak{l}'}$ sont simultanément injectives et surjectives ;

(ii)$\Rightarrow$(iii) d'après l'équivalence précédente : K étant $\mathfrak{l}$-rationnel (resp $\mathfrak{l}'$-rationnel) le groupe de Galois $Gal(K_\ell^{ab}/K)$ coïncide avec le sous-groupe de décomposition $D_\mathfrak{l}(K_\ell^{ab}/K)$ (resp $D_{\mathfrak{l}'}(K_\ell^{ab}/K)$) et la théorie ℓ-adique du corps de classes donne directement : $D_\mathfrak{l}(K_\ell^{ab}/K) \simeq \mathcal{R}_\mathfrak{l}/\mathcal{R}_\mathfrak{l} \cap \mathcal{R}\prod_{\mathfrak{p}\nmid\ell}\mu_\mathfrak{p} = \mathcal{R}_\mathfrak{l}$ (resp $D_{\mathfrak{l}'}(K_\ell^{ab}/K) \simeq \mathcal{R}_{\mathfrak{l}'}/\mathcal{R}_{\mathfrak{l}'} \cap \mathcal{R}\prod_{\mathfrak{p}\nmid\ell}\mu_\mathfrak{p} = \mathcal{R}_{\mathfrak{l}'}$) puisque les idèles principaux qui interviennent au dénominateur sont des éléments de $\mathcal{E}'$ d'image locale 1 dans $\mathcal{R}_{\mathfrak{l}'}$ (resp $\mathcal{R}_\mathfrak{l}$) ;

(iii)$\Rightarrow$(iv) car l'isomorphisme $Gal(K_\ell^{ab}/K) \simeq \mathcal{R}_\mathfrak{l} \simeq \mathcal{R}_{\mathfrak{l}'}$ montre que le rang essentiel de $G_\ell^{ab} = Gal(K_\ell^{ab}/K)$ est alors $d_\mathfrak{l} + 1 = d_{\mathfrak{l}'} + 1 = \frac{1}{2}(d_\mathfrak{l} + d_{\mathfrak{l}'}) + 1 \leq \frac{1}{2}(r+2c)+1 \leq c+1$ de sorte que K satisfait la conjecture de Leopoldt, ce qui entraine en particulier $H^2(G_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 1$; les conditions du lemme 1.10 se trouvent ainsi réunies, ce qui donne l'implication annoncée ;

(iv)$\Rightarrow$(i) puisque les égalités $G_S = Gal(K_\ell/K) = D_\mathfrak{l}(K_\ell/K) = D_{\mathfrak{l}'}(K_\ell/K)$ entre groupe de Galois global et groupes de décompositions (pour deux places $\mathfrak{L}$ et $\mathfrak{L}'$ de K_ℓ au dessus de $\mathfrak{l}$ et $\mathfrak{l}'$ respectivement) implique que les ℓ-extensions (abéliennes) maximales ℓ-ramifiées respectivement $\mathfrak{l}$ ou $\mathfrak{l}'$-décomposées soient triviales, ce qui caractérise la ℓ-birationalité de K.

Corollaire 1.12. *Soit K une extension galoisienne d'un corps de nombres F contenant les racines ℓ-ièmes de l'unité. Si K est $\mathfrak{l}$-rationnel en une place $\mathfrak{l}$ au dessus de ℓ, le groupe de décomposition associé $D_{\mathfrak{l}}(K/F)$ est un sous-groupe normal d'indice 1 ou 2 dans $Gal(K/F)$.*

Preuve. En effet, K est alors $\mathfrak{l}'$-rationnel pour toute place $\mathfrak{l}'$ conjuguée de $\mathfrak{l}$.

Corollaire 1.13. *Les corps quadratiques 2-birationnels sont les corps imaginaires $K = \mathbb{Q}[\sqrt{-p}]$ pour p premier, $p \equiv 7 \pmod{16}$ et $K = \mathbb{Q}[\sqrt{-pq}]$ pour p et q premiers, $p \equiv -q \equiv 3 \pmod 8$.*

Remarque. Ce résultat précise celui donné dans [Ts] dont la démonstration est incomplète.

Preuve. D'après ce qui précède, K est totalement imaginaire, admet exactement deux places au-dessus de 2, et son nombre de 2-classes est impair ; il est donc de la forme $\mathbb{Q}[\sqrt{-d}]$ avec $d \equiv$ -1 (mod 8), sans facteur carré, et la formule des 2-classes ambiges montre que d admet au plus deux diviseurs premiers (cf [J1],Th III.1.9). Plus précisément, nous avons ici

$$|{C\ell'_K}^G| \;=\; \frac{\prod_{p|d} e_p(K/\mathbb{Q})}{2\,\left(2^{\mathbb{Z}} : 2^{\mathbb{Z}} \cap N_{K/\mathbb{Q}}\right)}, \text{ donc}$$

- ou bien $d = p$ premier et le nombre de classes de K est impair en vertu de la formule des classes ambiges de Chevalley ;

- ou bien $d = pq$ avec p et q premiers et 2 non carré modulo p (comme modulo q) c'est à dire $p \equiv \pm 3 \pmod 8$, par exemple $p \equiv -q \equiv 3 \pmod 8$, et le nombre de classes de K est ici pair.

Examinons successivement les deux éventualités :

1^{er} cas : $K = \mathbb{Q}[\sqrt{-p}] \quad avec \;\; -p \equiv 1 \; (mod\ 8)$.

Notons h l'ordre (impair) de l'idéal premier $\mathfrak{l}$ et faisons choix d'une racine carrée δ de $-p$ dans $\mathbb{Z}_2$. Ecrivons $\pi = \frac{1}{2}(a + b\delta)$ l'image dans $\mathbb{Z}_2$ d'un générateur de $\mathfrak{l}^h$ (avec a et b dans $\mathbb{Z}$) ; son conjugué $\bar\pi = \frac{1}{2}(a - b\delta)$ est alors une unité de $\mathbb{Z}_2$ et K est 2-birationnel si et seulement si $\pm\bar\pi$ n'est pas un carré dans $\mathbb{Z}_2$, i.e. si et seulement si l'on a $\bar\pi \not\equiv \pm 1 \; (mod\ 8)$.

Maintenant, de l'identité normique $N(\mathfrak{l}^h) = 2^h = \pi\bar\pi = \frac{1}{4}(a^2 + pb^2)$ nous tirons $a^2 + pb^2 = 2^{h+2}$, ce qui nous prouve, puisque h est impair, que 2 est un carré modulo b, et nous donne $b \equiv \pm 1 \; (mod\ 8)$. D'un autre côté, puisque $\bar\pi$ est inversible dans $\mathbb{Z}_2$, nous avons $\bar\pi^{-1} \equiv \bar\pi \; (mod\ 8)$ donc, puisque 2^h vaut 2 ou 0 modulo 8 :

$$b\delta = \pi - \bar\pi = 2^h/\bar\pi - \bar\pi \equiv (2^h - 1)\bar\pi \equiv \pm\bar\pi \; (mod\ 8).$$

En résumé, il vient $\bar\pi \equiv \pm b\delta \equiv \pm\delta \; (mod\ 8)$ d'où comme attendu :

$$\bar\pi \not\equiv \pm 1 \; (mod\ 8) \Leftrightarrow \delta \not\equiv \pm 1 \; (mod\ 8) \Leftrightarrow -p \not\equiv 1 \; (mod\ 16).$$

2^{me} cas : $K = \mathbb{Q}[\sqrt{-pq}]$ avec $p \equiv -q \equiv 3 \pmod 8$.

L'extension abélienne 2-ramifiée 2-élémentaire M de K est ici encore de degré 8 sur K (Puisque son radical $Rad(M/K) = E'_K/{E'_K}^2$ sous la condition ${C\ell_K}' = 1$ est un $\mathbb{F}_2$-espace de dimension 3) ; c'est évidemment le corps $M = \mathbb{Q}[\sqrt{p}, \sqrt{q}, \sqrt{-1}, \sqrt{2}]$. Pour vérifier que K est birationnel, il suffit alors de constater que M ne possède que 2 places au-dessus de 2 ce qui résulte clairement du fait que la seule sous-extension de M quadratique sur $\mathbb{Q}$ qui est 2-décomposée est le corps $K = \mathbb{Q}[\sqrt{-pq}]$.

2. Ramification restreinte sur un corps S-rationnel

L'étude synoptique menée dans la section 1 conduit, en l'absence des racines ℓ-ièmes de l'unité à distinguer deux notions :

Définition 2.1. *Soit K un corps de nombres (contenant ou non les racines ℓ-ièmes de l'unité). Nous disons désormais que K est :*

- $\mathfrak{l}$-pseudo-rationnel lorsqu'il vérifie la condition (1) ou , de façon équivalente, les conditions (2) et (3) du théorème 1.3 ;

- $\mathfrak{l}$-rationnel lorsqu'il vérifie la condition (1') ou , de façon équivalente, les conditions (2') et (3') du théorème 1.7.

Plus généralement, les résultats de K. Wingberg (cf [W1] et [W2]) nous amènent à étendre comme suit la notion de corps $\mathfrak{l}$-rationnel :

Théorème & Définition 2.2. *Soit K un corps de nombres (contenant ou non les racines ℓ-ièmes de l'unité) et S un ensemble non vide de places ℓ-adiques de K. Nous disons que K est S-rationnel lorsqu'il vérifie les hypothèses équivalentes suivantes :*

(i) Le plongement naturel du sous-module principal $\mathcal{R} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$ dans le ℓ-adifié $\mathcal{J}$ du groupe des idèles induit une injection à conoyau $\mathbb{Z}_\ell$-libre de $\mathcal{R}$ dans la somme directe $\mathcal{R}_S \oplus \mathcal{I}d' = (\oplus_{\mathfrak{l}\in S}\mathcal{R}_\mathfrak{l}) \oplus (\oplus_{\mathfrak{p}\nmid\ell\infty}\mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p})$, ce que nous écrivons :

$$\mathcal{R} \rightarrowtail \mathcal{R}_S \oplus \mathcal{I}d' \ ;$$

(ii) les deux conditions suivantes sont réunies :

(ii,a) le pseudo-radical V'_S est trivial, qui est défini par :

$$V'_S = \{x\mathcal{R}^\ell \in \mathcal{R}/\mathcal{R}^\ell \mid x_\mathfrak{l} \in \mathcal{R}_\mathfrak{l}^\ell, \text{ pour } \mathfrak{l} \in S \ \&\ x_\mathfrak{p} \in \mu_\mathfrak{p}\mathcal{R}_\mathfrak{p}^\ell, \text{ pour } \mathfrak{p} \nmid \ell\}$$

(ii,b) et on a l'isomorphisme : $\oplus_{\mathfrak{l}\in S}\mu_\ell \simeq \mu$.

(iii) En particulier, le corps K est S-rationnel lorsque sont réunies les conditions suffisantes (qui sont également nécessaires en présence des racines ℓ-ièmes de l'unité) :

(iii,a) le ℓ-groupe des ℓ-classes Cl' est trivial ;

(iii,b) et l'application de semi-localisation s_S induit une injection à conoyau $\mathbb{Z}_\ell$-libre du tensorisé ℓ-adique $\mathcal{E}' = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E'$ du groupe des ℓ-unités dans le compactifié ℓ-adique $\mathcal{R}_S = \prod_{\mathfrak{l}\in S}\mathcal{R}_\mathfrak{l}$.

Remarques. (i) Lorsque $S = \{\mathfrak{l}\}$ est un singleton, la condition (i) ci-dessus n'est autre que la condition (1') déjà rencontrée. La notion de S-rationalité coïncide alors avec la notion de $\mathfrak{l}$-rationalité donnée plus haut.

(ii) Si K contient les racines ℓ-ièmes de l'unité, la condition (iii,b) implique que S soit un singleton. L'introduction de la notion de corps S-rationnel n'apporte donc rien de nouveau dans ce cas.

(iii) Les conditions (iii,a) et (iii,b) étant précisément celles proposées par K. Wingberg, le théorème 2.2 réunit ainsi les diverses notions de rationalité considérées jusqu'ici.

Preuve des équivalences. La démonstration de l'équivalence (i)$\Leftrightarrow$(ii) est identique à celle donnée lors de la preuve du théorème 1.7 ; il suffit pour cela de remplacer $\mathcal{R}_{\mathfrak{l}}$ par le produit $\mathcal{R}_S = \prod_{\mathfrak{l}\in S}\mathcal{R}_{\mathfrak{l}}$. Quant à l'équivalence (i)$\Leftrightarrow$(iii), elle s'obtient en observant que le pseudo-radical kummérien V'_S n'est autre que le noyau de l'application naturelle du quotient $\mathcal{R}/\mathcal{R}^\ell$ dans la somme directe $\mathcal{R}_S/\mathcal{R}_S^\ell \oplus \mathcal{I}d'/\mathcal{I}d'^{\ell}$; la condition (iii,a) signifie ainsi que $\mathcal{R}$ s'identifie à un sous-module pur de la somme $\mathcal{R}_S \oplus Id'$, et la condition (iii,b) que le quotient correspondant est sans $\mathbb{Z}_\ell$-torsion donc $\mathbb{Z}_\ell$-libre.

2.a Ensembles de places S-primitifs

Soit S un ensemble non vide de places ℓ-adiques d'un corps de nombres K, puis $S' = Pl_\ell \setminus S$ et $\mathcal{R}_{S'} = \prod_{\mathfrak{l}'\in S'}\mathcal{R}_{\mathfrak{l}'}$.

Proposition 2.3. *Pour qu'un corps K soit S-rationnel il faut et il suffit que le sous-groupe fermé $\mathcal{R}_{S'}\mathcal{R}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}}$ soit un facteur direct sans cotorsion (i.e. dont le quotient correspondant est sans torsion) du groupe des idèles $\mathcal{J}$, en d'autres termes que le groupe de Galois $\mathcal{F}_S$ de la pro-ℓ-extension abélienne maximale de K qui est ℓ-ramifiée et complètement décomposée aux places réelles et à celles $\mathfrak{l} \notin S$ divisant ℓ soit un $\mathbb{Z}_\ell$-module libre de dimension $x = d - r - c - l + s + 1$, où $d = \sum_{\mathfrak{l}\in S} d_{\mathfrak{l}}$ est la somme des degrés locaux des complétés de K aux places de S.*

Remarque. Sous les hypothèses de la proposition 2.3 on a $x = (c+1) - \sum_{\mathfrak{l}\in S'}(d_{\mathfrak{l}'}+1)$ et donc $d = c+1 \Leftrightarrow S = Pl_\ell$. En particulier si cette égalité a lieu, on retombe donc sur la notion de corps ℓ-rationnel.

Preuve. La condition (i) affirme que le ℓ-groupe $\mathcal{R}$ des idèles principaux s'identifie à un facteur direct sans cotorsion du quotient $\mathcal{J}/\mathcal{R}_{S'}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}}$ c'est à dire d'une part la trivialité de l'intersection $\mathcal{R}\cap\mathcal{R}_{S'}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}}$ (qui implique en particulier la conjecture de Leopoldt), d'autre part la liberté du quotient $\mathcal{F}_S = \mathcal{J}/\mathcal{R}\mathcal{R}_{S'}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}}$. La première condition s'écrit aussi bien $\mathcal{R}_{S'}\cap\mathcal{R}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}} = 1$. Quant à la dimension de $\mathcal{F}_S$ elle s'obtient comme suit : sous la conjecture de Leopoldt, le rang essentiel du quotient $\mathcal{J}/\mathcal{R}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}}$ est le nombre $c+1$ de $\mathbb{Z}_\ell$-extensions de K, tandis que celui du $\mathbb{Z}_\ell$-module $\mathcal{R}_{S'}$ vaut, lui, $(r+2c-d)+(l-s) = c+1-x$, ce qui donne comme annoncé $dim_{\mathbb{Z}_\ell}\mathcal{F}_S = x$. Réciproquement, si $\mathcal{F}_S$ est un $\mathbb{Z}_\ell$-module de dimension x, le même calcul montre que K vérifie la conjecture de Leopoldt et, plus précisément, que l'on a $\mathcal{R}_{S'}\cap\mathcal{R}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}} = 1$ donc $\mathcal{R}\cap\mathcal{R}_{S'}\prod_{\mathfrak{p}\nmid\ell}\mu_{\mathfrak{p}} = 1$, ce qui établit la condition (i).

Définition 2.4. *Soient K un corps S-rationnel, $S' = Pl_\ell \setminus S$ l'ensemble des places ℓ-adiques qui ne sont pas dans S et $\mathcal{F}_S$ le groupe de Galois de la ℓ-extension abélienne S-ramifiée $S'\infty$-décomposée maximale de K. Nous disons qu'un ensemble X*

de places modérées $\mathfrak{p} \nmid \ell\infty$ de K est S-primitif lorsque les images dans $\mathcal{F}_S$ des éléments de X forment une base d'un sous-module pur de $\mathcal{F}_S$, autrement dit lorsque les logarithmes de Gras des places de X forment une $\mathbb{Z}_\ell$-base d'un sous-module pur d'un supplémentaire de l'image de $\mathcal{R}_{S'}$ dans le groupe de Galois $Gal(K^z/K)$ de la composée K^z des $\mathbb{Z}_\ell$-extensions de K.

Remarque. La définition ci-dessus généralise la notion d'ensemble ℓ-primitif introduite par G. Gras et J.-F. Jaulent (cf [GJ]). Rappelons en effet que le logarithme de Gras d'une place finie $\mathfrak{p}$ étrangère à ℓ n'est autre que l'image de l'automorphisme de Frobenius associé à $\mathfrak{p}$ dans $Gal(K^z/K)$. En particulier :

Scolie 2.5. *Supposons $x > 0$. Dans ce cas le théorème de Čebotarev garantit l'existence d'ensembles S-primitifs autres que le vide, plus précisement que tout ensemble primitif de cardinal strictement inférieur à x peut être complété d'une infinité de façon en un ensemble primitif maximal (i.e. de cardinal maximal x).*

Nous sommes maintenant en mesure d'énoncer le résultat principal de cette section :

Théorème 2.6. *Soit K un corps S-rationnel et X un ensemble S-primitif maximal de places modérées de K. Alors :*

(i) Le groupe de Galois $G^{ab}_{\ell X} = Gal(K^{ab}_{\ell X}/K)$ de la pro-ℓ-extension abélienne ℓX-ramifiée maximale de K est donné par l'isomorphisme :

$$G^{ab}_{\ell X} \simeq \mathcal{J}/\mathcal{R} \prod_{\mathfrak{p}\nmid \ell X\infty} \mu_{\mathfrak{p}} \simeq \prod_{\mathfrak{l}'\in S'} \mathcal{R}_{\mathfrak{l}'} \oplus \prod_{\mathfrak{p}|\infty} \mathcal{R}_{\mathfrak{p}} \oplus \prod_{\mathfrak{p}|X} \mathcal{R}_{\mathfrak{p}}$$

comme somme directe des groupes de Galois locaux $\mathcal{R}_{\mathfrak{p}} \simeq Gal(\bar{K}^{ab}_{\mathfrak{p}}/K_{\mathfrak{p}})$ attachés aux places de $S'X\infty$ où S' est l'ensemble des places ℓ-adiques de K qui ne sont pas dans S.

(ii) Le groupe de Galois $G_{\ell X} = Gal(K_{\ell X}/K)$ de la pro-ℓ-extension ℓX-ramifiée maximale de K est donné par l'isomorphisme :

$$G_{\ell X} \simeq \ (\underset{\mathfrak{l}'\in S'}{\circledast} \mathcal{G}_{\mathfrak{l}'}) \ \circledast \ (\underset{\mathfrak{p}|\infty}{\circledast} \mathcal{G}_{\mathfrak{p}}) \ \circledast \ (\underset{\mathfrak{p}|X}{\circledast} \mathcal{G}_{\mathfrak{p}})$$

comme pro-ℓ-produit libre des groupes de Galois locaux $\mathcal{G}_{\mathfrak{p}} \simeq Gal(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ attachés aux places de $S'X\infty$.

Preuve. Le corps K étant supposé S-rationnel, il vérifie en particulier la conjecture de Leopoldt comme expliqué dans le corollaire 1.8, de sorte que nous avons $H^2(G_{\ell X}, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 1$ (ce qui est une traduction cohomologique de cette conjecture) et $\mathcal{R}\cap\prod_{\mathfrak{p}} \mu_{\mathfrak{p}} = \mu$ (ce qui en est la traduction idèlique). L'ensemble X étant supposé S-primitif, la condition de rationalité s'écrit ainsi (avec $\mathcal{R}_X = \oplus_{\mathfrak{p}|X}\mathcal{R}_{\mathfrak{p}}$) :

$$\mathcal{J} = (\mathcal{R} \prod_{\mathfrak{p}\nmid \ell X\infty} \mu_{\mathfrak{p}}) \oplus \mathcal{R}_{S'} \oplus \mathcal{R}_X,$$

ce qui nous donne la décomposition annoncée de $\mathcal{J}/\mathcal{R}\prod_{\mathfrak{p}\nmid\ell X} \mu_{\mathfrak{p}}$ comme produit direct des abélianisés locaux $\mathcal{G}^{ab}_{\mathfrak{p}} \simeq \mathcal{R}_{\mathfrak{p}}$ pour les places $\mathfrak{p} \notin S$ divisant $\ell X\infty$. Compte tenu de la condition $H^2(G_X, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 1$, cette condition se relève en une factorisation de G_X lui même comme pro-ℓ-produit libre des mêmes $\mathcal{G}_\mathfrak{p}$ (cf. lemme 1.10).

2.b Caractérisation de la $\mathfrak{l}$-rationalité

Le théorème 2.6 ci-dessus nous permet de retrouver très simplement le résultat principal de Wingberg (cf [W1], [W2]).

Théorème 2.7. *Soit K un corps de nombres, K_ℓ sa pro-ℓ-extension (galoisienne) ℓ-ramifiée maximale , et G_ℓ le groupe de Galois $Gal(K_\ell/K)$. Notons S un ensemble non vide de places ℓ-adiques, puis $d = \sum_{\mathfrak{l}\in S}[K_\mathfrak{l} : \mathbb{Q}_\ell]$ et x la quantité $d - r - c - l + s + 1$ où r, c et l sont respectivement les nombres de places réelles, complexes et ℓ-adiques de K et s le nombre de places dans S.*

Cela posé, les assertions suivantes sont équivalentes :

(i) Le corps K est S-rationnel ;

(ii) le groupe de Galois G_ℓ est isomorphe au pro-ℓ-produit libre

$$G_\ell \simeq (\underset{\mathfrak{p}|\ell\infty, \mathfrak{p}\notin S}{\circledast} \mathcal{G}_\mathfrak{p}) \circledast \mathcal{F}_x ,$$

où $\mathcal{F}_x$ est un pro-ℓ-groupe libre (nécessairement sur x générateurs) ;

(iii) le groupe abélien G_ℓ^{ab} s'identifie à la somme directe

$$G_\ell^{ab} \simeq \mathcal{J}/\mathcal{R}\prod_{\mathfrak{p}\nmid\ell} \mu_\mathfrak{p} \simeq \prod_{\mathfrak{p}|\ell\infty, \mathfrak{p}\notin S} \mathcal{R}_\mathfrak{p} \oplus \mathcal{F}_x^{ab},$$

où $\mathcal{F}_x^{ab}$ est un $\mathbb{Z}_\ell$-module libre (de dimension x).

Preuve. Rappelons que $\mathcal{G}_\mathfrak{p}$ désigne le groupe de Galois $Gal(\bar{K}_\mathfrak{p}/K_\mathfrak{p})$ de la ℓ-clôture galoisienne de $K_\mathfrak{p}$, que $\mathcal{G}_\mathfrak{p}^{ab} \simeq \mathcal{R}_\mathfrak{p}$ s'identifie par la théorie du corps de classes local au ℓ-adifié du groupe multiplicatif $K_\mathfrak{p}^\times$ et que, pour une place réelle $\mathfrak{p}$, le groupe $\mathcal{G}_\mathfrak{p} \simeq \mathcal{R}_\mathfrak{p}$ est cyclique d'ordre 2. Cela étant, nous avons :

$(i) \Rightarrow (ii)$ d'après le théorème 2.6 puisqu'en chaque place $\mathfrak{p}$ d'un ensemble S-primitif X, le quotient $\mathcal{G}_\mathfrak{p}/\mathcal{I}_\mathfrak{p}$ de $\mathcal{G}_\mathfrak{p}$ par son sous-groupe d'inertie est un pro-ℓ-groupe libre de dimension 1 ;

$(ii) \Rightarrow (iii)$ par passage à l'abélianisé ;

$(iii) \Rightarrow (i)$ d'après la caractérisation donnée par le théorème 2.2. La description de G_ℓ obtenue permet d'appliquer aux corps S-rationnels les résultats de [Ya] rappelés dans l'introduction. Il vient ainsi :

Corollaire 2.8. *Si K un corps S-rationnel, le rang du groupe de Galois d'une pro-ℓ-extension pro-ℓ-libre maximale de K est donné par :*

$$\rho = c + 1 - \sum_{\mu_\ell \subset K_{\mathfrak{l}'}} \left[\frac{([K_{\mathfrak{l}'} : \mathbb{Q}_\ell] - 1)}{2} \right]$$

où $[\ .\ ]$ est la partie entière et la somme à droite est étendue aux places $\mathfrak{l}' \notin S$ au-dessus de ℓ pour lesquelles le complété $K_{\mathfrak{l}'}$ contient les racines ℓ-ièmes de l'unité.

Preuve. Puisque une ℓ-extension pro-ℓ-libre est ℓ-ramifiée (cf [Ya]), tout revient à déterminer le rang maximal ρ d'un quotient pro-ℓ-libre du groupe de Galois $G_\ell = Gal(K_\ell/K)$ qui n'est autre , comme expliqué dans [Ya], que la somme des rangs des quotients correspondant de chacun de ses facteurs. Le théorème 2.7 nous donne alors :

$$\rho(G) = \sum_{\mathfrak{l}'\notin S} \rho(\mathcal{G}_{\mathfrak{l}'}) + \sum_{\mathfrak{p}|\infty} \rho(\mathcal{G}) + x = \sum_{\mathfrak{l}'\notin S} \rho(\mathcal{G}_{\mathfrak{l}'}) + x.$$

Distinguons maintenant deux cas :

- Si $K_{\mathfrak{l}'}$ ne contient pas μ_ℓ, le groupe $\mathcal{G}_{\mathfrak{l}'}$ est un pro-ℓ-groupe libre de rang $d_{\mathfrak{l}'}+1$, où $d_{\mathfrak{l}'} = [K_{\mathfrak{l}'} : \mathbb{Q}_\ell]$ désigne le degré local ;

- Dans le cas contraire , il est bien connu (cf [Se] Ch.II, Th.5.6) que $\mathcal{G}_{\mathfrak{l}'}$ est un groupe de Demuškin de rang $d_{\mathfrak{l}'}+2$, de sorte que par un résultat de J. Sonn (cf. [So] Th. 7) on a seulement $\rho(\mathcal{G}_{\mathfrak{l}'}) = \left[\frac{d_{\mathfrak{l}'}}{2}\right] + 1$.

Ainsi de l'égalité $x = d - r - c - l + s + 1 = (r + 2c - \sum d_{\mathfrak{l}'}) - r - c - l + s + 1 = c + 1 - \sum d_{\mathfrak{l}'} - (l - s - 1)$, nous concluons finalement :

$$\rho(G_S) = c + 1 - \sum_{\mu_\ell \subset K_{\mathfrak{l}'}} (d_{\mathfrak{l}'} - \left[\frac{d_{\mathfrak{l}'}}{2}\right]) = c + 1 - \sum_{\mu_\ell \subset K_{\mathfrak{l}'}} \left[\frac{d_{\mathfrak{l}'}-1}{2}\right].$$

On voit par là que les corps $\mathfrak{l}$-rationnels qui ne sont pas ℓ-rationnels, constituent une classe de corps de nombres pour lesquels on a généralement l'inégalité stricte : $\rho < c + 1$.

2.c Interprétation logarithmique de la S-rationalité

Le corps K étant supposé fixé, désignons par $\mathcal{F}_S = \mathcal{J}/\mathcal{R}_{S'}\mathcal{R}\prod_{\mathfrak{p}\nmid\ell\infty}^{res} \mu_{\mathfrak{p}}$ le quotient du ℓ-groupe des idèles $\mathcal{J}$ que la théorie ℓ-adique du corps de classes identifie au groupe de Galois de la pro-ℓ-extension abélienne maximale de K qui est non ramifiée en dehors de S et complètement décomposée aux places réelles ainsi qu'à celles $\mathfrak{l}' \notin S$ au-dessus de ℓ. Notons $\mathcal{T}_S = \mathcal{F}_S^{tor}$ le sous-module de $\mathbb{Z}_\ell$-torsion de $\mathcal{F}_S$. le quotient $\mathcal{X}_S = \mathcal{F}_S/\mathcal{T}_S$ est alors un $\mathbb{Z}_\ell$-module de dimension finie, disons x_S, et l'application :

$$\mathcal{L}_S \;\mid\; \mathcal{J} \to \mathcal{X}_S = \mathcal{F}_S/\mathcal{T}_S \simeq \mathbb{Z}_\ell^{x_S}$$

peut ainsi être regardée comme un analogue du logarithme de Gras (cf. [GJ]). L'intérêt de cette approche réside alors dans la caractérisation suivante de la S-rationalité

Proposition 2.9. *Avec les notations ci-dessus, on a : K S-rationnel $\Leftrightarrow \mathcal{T}_S = 1$*

Cela posé, nous avons :

Théorème 2.10. *Soit L/K une ℓ-extension finie de corps de nombres, de groupe de Galois G et S un ensemble non vide de places de K au-dessus de ℓ. Si le corps L vérifie la conjecture de Leopoldt en S (i.e. si le noyau $\mathcal{E}_S(L)$ de l'application* *de localisation s_S du ℓ-groupe des unités $\mathcal{E}(L) = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_{\mathfrak{l}}$ dans le groupe multiplicatif $\mathcal{R}_{S'}(L)$ est trivial), l'ordre du sous-groupe ambige de $\mathcal{T}_S(L)$ est donné comme produit de deux entiers par la formule :*

$$|\mathcal{T}_S(L)^G| = |\mathcal{T}_S(K)| \frac{(\mathcal{D}'(L)^G : \mathcal{D}'(K))}{(\mathcal{L}_S(\mathcal{D}'(L)^G) : \mathcal{L}_S(\mathcal{D}'(K)))}$$

où $\mathcal{D}'$ désigne le $\mathbb{Z}_\ell$-module libre construit sur les places finies étrangères à ℓ, et $\mathcal{L}_S$ est le logarithme de Gras à valeurs dans $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathcal{F}_S(L)$.

Preuve. Commençons par exprimer le groupe $\mathcal{T}_S$ en termes de classes de diviseurs : de l'égalité $\mathcal{J} = \prod^{res} \mathcal{R}_\mathfrak{p}\mathcal{R}$, nous tirons immédiatement :

$$\mathcal{F}_S = \prod_{\mathfrak{p}\nmid\ell\infty}^{res} \mathcal{R}_\mathfrak{p} / \prod_{\mathfrak{p}\nmid\ell\infty} \mathcal{R}_\mathfrak{p} \cap (\mathcal{R} \prod_{\mathfrak{p}|\ell\infty} \mu_\mathfrak{p} \mathcal{R}'_{\mathfrak{l}}) \simeq \mathcal{D}'/\mathcal{P}'_S$$

où $\mathcal{D}' = \prod_{\mathfrak{p}\nmid\ell\infty}^{res} \mathcal{R}_\mathfrak{p}/\mu_\mathfrak{p}$ est le ℓ-groupe des diviseurs étrangers à $\ell\infty$ et $\mathcal{P}'_S$ l'image canonique dans $\mathcal{D}'$ du sous-module $\mathcal{R}_S$ formé des élements de $\mathcal{R}$ d'image locale 1 dans $\mathcal{R}_{S'}$. En particulier, il suit :

$$\mathcal{T}_S = \mathcal{F}_S^{tor} \simeq \sqrt{\mathcal{P}'_S}/\mathcal{P}'_S,$$

si $\sqrt{\mathcal{P}'_S}$ désigne la racine dans $\mathcal{D}'$ du sous-module $\mathcal{P}'_S$. Cela étant, l'hypothèse $\mathcal{E}_{\mathfrak{l}} = 1$ dans l'énoncé du théorème équivaut à affirmer l'isomorphisme $\mathcal{P}'_S \simeq \mathcal{R}_S$. En particulier, de la suite exacte courte qui définit $\mathcal{R}_S$:

$$1 \to \mathcal{R}_S(L) \to \mathcal{R}(L) \to \mathcal{R}_{S'}(L) \to 1,$$

nous tirons la suite exacte de cohomologie : $\mathcal{R}_S(L)^G = \mathcal{R}_S(K) \hookrightarrow \mathcal{R}(L)^G = \mathcal{R}(K) \twoheadrightarrow \mathcal{R}_{S'}(K) \to H^1(G, \mathcal{R}_S(L)) \to H^1(G, \mathcal{R}(L)) \to ...$ et le théorème 90 de Hilbert nous donne alors

$$H^1(G, \mathcal{P}_S(L) = H^1(G, \mathcal{R}_S(L)) = H^1(G, \mathcal{R}(L)) = 1.$$

Par suite, du diagramme commutatif exact induit par les applications d'extension

$$\begin{array}{ccccccccc}
1 & \to & \mathcal{R}_S(K) = \mathcal{P}_S(K) & \to & \sqrt{\mathcal{P}_S(K)} & \to & \mathcal{T}_{\mathfrak{l}}(K) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathcal{R}_S(L)^G = \mathcal{P}_S(L)^G & \to & \sqrt{\mathcal{P}_S(L)}^G & \to & \mathcal{T}_{\mathfrak{l}}(L)^G & \to & H^1(G, \mathcal{P}_S(L)) = 1
\end{array}$$

nous concluons immédiatement :

$$|\mathcal{T}_S(L)^G| = |\mathcal{T}_S(K)|(\sqrt{\mathcal{P}_S(L)}^G : \sqrt{\mathcal{P}_S(K)}),$$

et $\sqrt{\mathcal{P}_S(L)}^G = \sqrt{\mathcal{P}_S(L)^G}$ n'est autre que la racine de $\mathcal{P}_S(L)$ dans le $\mathbb{Z}_\ell$-module $\mathcal{D}'(L)^G$ engendré par $\mathcal{D}'(K)$ et les $e_\mathfrak{p}^{-1}(L/K)\mathfrak{p}$ lorsque $\mathfrak{p}$ parcourt les idéaux premiers de K qui se ramifient modérément dans L/K. L'introduction du logarithme de Gras permet ainsi d'interpréter facilement le second facteur, et le diagramme commutatif

$$\begin{array}{ccccccccc} 1 & \to & \sqrt{\mathcal{P}_S(K)} & \to & \mathcal{D}'(K) & \to & \mathcal{L}_S(\mathcal{D}'(K)) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \sqrt{\mathcal{P}_S(L)}^G & \to & \mathcal{D}'(L)^G & \to & \mathcal{L}_S(\mathcal{D}'(L)^G) & \to & 1 \end{array}$$

nous donne le résultat attendu :

$$\big(\sqrt{\mathcal{P}_S(L)}^G : \sqrt{\mathcal{P}_S(K)}\big) \;=\; \frac{\big(\mathcal{D}'(L)^G : \mathcal{D}'(K)\big)}{\big(\mathcal{L}_S(\mathcal{D}'(L)^G) : \mathcal{L}_S(\mathcal{D}'(K))\big)}$$

Corollaire 2.11. *Sous les hypothèses du théorème 2.10, les assertions suivantes sont équivalentes :*
(i) L est S-rationnel ;
(ii) K est S-rationnel et l'extension L/K est S-primitivement ramifiée.

Preuve. Nous avons en effet :

$$\mathcal{T}_S(L) = 1 \Leftrightarrow \mathcal{T}_S(L)^G = 1 \Leftrightarrow \begin{cases} \mathcal{T}_S(L) = 1 \qquad \textit{et} \\ \big(\mathcal{L}_S(\mathcal{D}'(L)^G) : \mathcal{L}_S(\mathcal{D}'(K))\big) = \big(\mathcal{D}'(L)^G : \mathcal{D}'(K)\big), \end{cases}$$

avec $\big(\mathcal{D}'(L)^G : \mathcal{D}'(K)\big) \;=\; \prod_{\mathfrak{p}\nmid\ell} e_{\mathfrak{p}}(L/K)$.

Et l'égalité en bas a lieu si et seulement si les logarithmes de Gras des places $\mathfrak{p}$ de K qui se ramifient modérément dans L/K forment une $\mathbb{Z}_\ell$-base d'un sous module pur de $\mathcal{L}_S(\mathcal{D}'(K))$, autrement dit lorsque l'ensemble X des places modérément ramifiées dans L/K est S-primitif (au sens de la définition 2.4).

3. Propagation de la S-rationalité et lois primitives de réciprocité

3.a Propagation de la S-rationalité

Pour un nombre premier ℓ impair, il est possible de s'affranchir très simplement de l'hypothèse sur la comjecture de Leopoldt faite dans le théorème 2.10. Le théorème de propagation devient ainsi :

Théorème 3.1. *Soient un nombre premier ℓ impair et L une ℓ-extension d'un corps de nombre K. Les assertions suivantes sont équivalentes :*
(i) il existe un ensemble S de places au-dessus de ℓ pour lequel L est S-rationnel ;
(ii) il existe un ensemble S de places au-dessus de ℓ pour lequel K est S-rationnel et l'ensemble X des places moderement ramifiées dans L/K est S-primitif.

Preuve. (i)$\Rightarrow$(ii) Si L est S-rationnel, L vérifie alors trivialement la propriété de Leopoldt en S (D'après l'assertion (ii,b) du théorème 2.2) et les hypothèses du théorème 2.10 sont donc vérifiées. Il résulte donc du corollaire 2.11 que K est S-rationnel et L/K S-primitivement ramifiée.

(ii)$\Rightarrow$(i) Supposons maintenant que K est S-rationnel et que l'ensemble des places de K qui se ramifient modérément dans L/K peut être complété en un ensemble S-primitif maximal X. Notons $K_{\ell X}$ la pro-ℓ-extension X-modérément ramifiée maximale de K, et observons que c'est aussi la pro-ℓ-extension X-modérément ramifiée maximale de L. De l'isomorphisme donné par le théorème 2.6, il suit

$$Gal(L_{\ell X}/K) = Gal(K_{\ell X}/K) \simeq \underset{\mathfrak{p}|\ell X,\ \mathfrak{p}\notin S}{\circledast} Gal(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}}),$$

En particulier, le groupe de Galois de la pro-ℓ-extension ℓ-ramifiée maximale de L est alors

$$Gal(L_{\ell}/L) = \underset{\mathfrak{P}|\ell,\ \mathfrak{P}\notin S}{\circledast} Gal(\bar{L}_{\mathfrak{P}}/L_{\mathfrak{P}}) \circledast \mathcal{H},$$

où $\mathcal{H}$ est un pro-ℓ-groupe libre de rang : $rg\mathcal{H} = rg\mathcal{H}_X + x_L$ si x_L désigne le nombre places de L au-dessus de X. Il vient donc :

$$rg\mathcal{H} = \sum_{\mathfrak{P}|X}[L_{\mathfrak{P}} : K_{\mathfrak{p}}] + \sum_{\mathfrak{P}|\ell,\ \mathfrak{P}\notin S}([L_{\mathfrak{P}} : K_{\mathfrak{p}}] - 1) - ([L : K] - 1).$$

La contribution des places modérées est $\sum_{\mathfrak{p}|X}\sum_{\mathfrak{P}|\mathfrak{p}}[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = \sum_{\mathfrak{p}|X}[L : K] = x_K[L : K]$; celle des places sauvages vaut : $\sum_{\mathfrak{p}|\ell,\ \mathfrak{p}\notin S}\sum_{\mathfrak{P}|\mathfrak{p}}([L_{\mathfrak{P}} : K_{\mathfrak{p}}] - 1) = (l_K - s_K)[L : K] - (l_L - s_L)$, si l_K et l_L désignent respectivement le nombre de places sauvages de K et de L et s_K et s_L désignent respectivement le nombre de places de K dans S et au-dessus de S dans L ; et il suit comme attendu :

$$\begin{aligned} rg\mathcal{H} = [L : K](x_K + l_K - s_K - 1) - l_L + s_L + 1 &= [L : K](c_K - d_L) - l_L + s_L + 1 \\ &= c_L - d_L - l_L + +s_L + 1, \end{aligned}$$

ce qui est bien la caractérisation de la S-rationalité donnée par le théorème 2.7.

Remarque. Le théorème 3.1 ne vaut pas pour ℓ=2 puisqu'il peut arriver que le corps L soit 2-birationnel comme le montre l'étude effectuée dans la section 1.c pour les extensions quadratiques de $\mathbb{Q}$.

Corollaire 3.2. *Sous les hypothèses du théorème 3.1, si K est un corps de nombres S-rationnel et L/K une ℓ-extension S-primitivement ramifiée, alors pour tout ensemble S-primitif $X = X_K$ de places de K contenant les places modérément ramifiées dans L/K, l'ensemble X_L des places de L au-dessus de X est lui même S-primitif.*

Preuve. Les pro-ℓ-extensions X-modérément ramifiées maximales de K et L coïncident par hypothèse et il vient donc comme plus haut :

$$Gal(L_{\ell X}/L) = Gal(K_{\ell X}/L) \simeq \underset{\mathfrak{P}|\ell X,\ \mathfrak{P}\notin S}{\circledast} Gal(\bar{L}_{\mathfrak{P}}/L_{\mathfrak{P}}) \circledast \mathcal{H}_X,$$

pour un pro-ℓ-groupe convenable $\mathcal{H}_X$. On a aussi montré le résultat suivant :

Corollaire 3.3. *Soit K un corps de nombres $\mathfrak{l}$-rationnel contenant les racines ℓ-ièmes de l'unité ; alors la place $\mathfrak{l}$ ne se décompose dans aucune ℓ-extension de K primitivement ramifiée.*

Preuve. Si L/K est une ℓ-extension $\mathfrak{l}$-primitivement ramifiée, alors en vertu du théorème 3.1 L est S-rationnel pour l'ensemble S des places de L divisant $\mathfrak{l}$, lequel en présence des racines ℓ-ièmes de l'unité, est un singleton.

3.b Lois de réciprocité primitives

Nous revenons dans cette dernière section aux hypothèses de la première partie de ce travail : en particulier, sauf mention explicite du contraire, K désigne désormais un corps de nombres $\mathfrak{l}$-rationnel contenant les racines ℓ-ièmes de l'unité.

Théorème 3.4. *Soit K un corps $\mathfrak{l}$-rationnel (contenant ou non les racines ℓ-ièmes de l'unité) et X un ensemble $\mathfrak{l}$-primitif maximal de places (modérées) de K. Alors le morphisme de localisation $s_\mathfrak{l}$ de $\mathcal{R} = \mathbb{Z}_\ell \otimes_\mathbb{Z} K^\times$ dans $\mathcal{R}_\mathfrak{l}$ induit un ismorphisme*

$$\mathcal{E}'_X \simeq \mathcal{R}_\mathfrak{l}$$

du tensorisé $\mathcal{E}'_X = \mathbb{Z}_\ell \otimes_\mathbb{Z} E'_X$ du groupe des ℓX-unités (au sens ordinaire) sur le ℓ-adifié $\mathcal{R}_\mathfrak{l}$ du groupe multiplicatif du complété $K_\mathfrak{l}$ de K en la place $\mathfrak{l}$.

Preuve. Considérons le groupe de Galois $G^{ab}_{\ell X} = \mathcal{J}/\mathcal{R}\prod_{\mathfrak{p}\nmid\ell X\infty}\mu_\mathfrak{p}$ de la pro-ℓ-extension abélienne ℓX-ramifiée (i.e. non ramifiée aux places étrangères à ℓ et à X, mais éventuellement complexifiée aux places réelles) maximale de K. D'après le théorème 2.5, le groupe $G^{ab}_{\ell X}$ s'identifie au produit direct : $G^{ab}_{\ell X} \simeq \prod_{\mathfrak{p}|\ell X\infty,\mathfrak{p}\neq\mathfrak{l}}\mathcal{R}_\mathfrak{p}$

D'un autre côté puisque $G^{ab}_{\ell X}$ est engendré par les images des $\mathcal{R}_\mathfrak{p}$ pour $\mathfrak{p}|\ell X\infty, \mathfrak{p} \neq \mathfrak{l}$, l'isomorphisme du corps de classes nous donne :

$$G^{ab}_{\ell X} \simeq \prod_{\mathfrak{p}|\ell X\infty} \mathcal{R}_\mathfrak{p}/(\prod_{\mathfrak{p}|\ell X\infty} \mathcal{R}_\mathfrak{p} \cap (\mathcal{R} \prod_{\mathfrak{p}\nmid ellX\infty} \mu_\mathfrak{p}))$$

et les idèles principaux qui interviennent au dénominateur sont les éléments de $\mathcal{E}'_X$. En particulier le morphisme de localisation $s_\mathfrak{l}$ envoie donc $\mathcal{E}'_X$ sur $\mathcal{R}_\mathfrak{l}$. Des isomorphismes de $\mathbb{Z}_\ell$-modules

$$\mathcal{E}'_X \simeq \mu_\ell \mathbb{Z}_\ell^{r+c-1+s+x} = \mu_\ell \mathbb{Z}_\ell^{d+1} \quad et \quad \mathcal{R}_\mathfrak{p} \simeq \mu_\ell \mathbb{Z}_\ell^{d+1},$$

nous concluons alors à la bijectivité de $s_\mathfrak{l}$.

Corollaire 3.5. *(Loi de réciprocité primitive) Soit K un corps de nombres $\mathfrak{l}$-rationnel contenant les racines ℓ^k-ièmes de l'unité (avec $k \geq 1$). Alors, pour tout ensemble $\mathfrak{l}$-primitif maximal X de places (modérées) de K, les morphismes de localisation conduisent aux isomorphismes :*

$$\mathcal{R}_\mathfrak{l}/\mathcal{R}_\mathfrak{l}^{\ell^k} \xleftarrow{\sim} \mathcal{E}'_X/\mathcal{E}'^{\ell^k}_X \xrightarrow{\sim} \prod_{\mathfrak{p}|\ell X\infty,\ \mathfrak{p}\neq\mathfrak{l}} \mathcal{R}_\mathfrak{p}/\mathcal{R}_\mathfrak{p}^{\ell^k}$$

En particulier, les $\mathbb{Z}_\ell$-modules à droite et à gauche du diagramme sont anti-isométriques pour les structures bilinéaires antisymétriques définies par les symboles de Hilbert.

Preuve. L'isomorphisme de gauche résulte directement du théorème 3.4 par passage au quotient à partir de l'isomorphisme $\mathcal{E}'_X \simeq \mathcal{R}_\mathfrak{p}$. Remarquons au passage que le quotient $\mathcal{R}_\mathfrak{l}/\mathcal{R}_\mathfrak{l}{}^{\ell^k} \simeq K_\mathfrak{l}^\times/K_\mathfrak{l}^{\times\,\ell^k}$ s'identifie par la théorie du corps de classes local au groupe de Galois de la ℓ-extension abélienne maximale d'exposant ℓ^k du complété $K_\mathfrak{l}$, et par la théorie de Kummer, au radical de cette même extension.

Considérons maintenant la ℓ-extension abélienne ℓX-ramifiée maximale d'exposant ℓ^k de K. D'après le théorème 3.4, son groupe de Galois $G^{ab}_{\ell X}/G^{ab}_{\ell X}{}^{\ell^k}$ s'identifie à la somme directe $\prod_{\mathfrak{p}|\ell X\infty, \mathfrak{p}\neq\mathfrak{l}} \mathcal{R}_\mathfrak{p}/\mathcal{R}_\mathfrak{p}{}^{\ell^k}$ et il en est donc de même, par dualité, de son radical kummérien. Mais puisque le ℓ-groupe des ℓ-classes $\mathcal{C}l'$ de K est trivial (en vertu des théorèmes 1.3 (2) et 1.7 (2)') ce même radical est donné par le quotient $E'_X/E'_X{}^{\ell^k} \simeq \mathcal{E}'_X/\mathcal{E}'_X{}^{\ell^k}$. En résumé il vient donc comme annoncé :

$$\mathcal{R}_\mathfrak{l}/\mathcal{R}_\mathfrak{l}^{\ell^k} \simeq \mathcal{E}'_X/\mathcal{E}'_X{}^{\ell^k} \simeq \prod_{\mathfrak{p}|\ell X\infty,\ \mathfrak{p}\neq\mathfrak{l}} \mathcal{R}_\mathfrak{p}/\mathcal{R}_\mathfrak{p}^{\ell^k}.$$

Il reste enfin à démontrer que l'isomorphisme entre les modules extrêmes ainsi obtenu est une anti-isométrie. Or pour a et b dans $\mathcal{E}'_X$, la formule du produit pour les ℓ-symboles de Hilbert (i.e. les symboles de Hilbert à valeurs dans les ℓ-groupes locaux $\mu_\mathfrak{p}$) s'ecrit (avec $\ell^{m_\mathfrak{p}} = |\mu_\mathfrak{p}|$ et $\ell^m = |\mu|$) :

$$\prod_{\mathfrak{p}|\ell S\infty} \left(\frac{a,b}{\mathfrak{p}}\right)^{\ell^{m_\mathfrak{p}-m}} = 1$$

puisque les symboles $\left(\frac{a,b}{\mathfrak{p}}\right)$ sont alors triviaux pour $\mathfrak{p} \nmid \ell S\infty$. De l'églité $m_\mathfrak{l} = m$, nous concluons immédiatement à l'identité :

$$\left(\frac{a,b}{\mathfrak{l}}\right)^{-1} = \prod_{\mathfrak{p}|\ell S\infty,\ \mathfrak{p}\neq\mathfrak{l}} \left(\frac{a,b}{\mathfrak{p}}\right)^{\ell^{m_\mathfrak{p}-m}}$$

qui ramène le calcul des symboles dans $\mathcal{R}_\mathfrak{l}$ à des calculs locaux dans les complétés $K_\mathfrak{p}$ pour $\mathfrak{p}|\ell S\infty, \mathfrak{p}\neq\mathfrak{l}$. En particulier, notant $\left(\frac{\cdot,\cdot}{\mathfrak{p}}\right)_{\ell^k}$ le symbole de profondeur ℓ^k (i.e. la puissance $\ell^{m_\mathfrak{p}-m}$-ième du symbole $\left(\frac{\cdot,\cdot}{\mathfrak{p}}\right)$ sur $\mathcal{R}_\mathfrak{p}\times\mathcal{R}_\mathfrak{p}$, nous pouvons réécrire l'identité précédente sous la forme :

$$\left(\frac{\alpha,\beta}{\mathfrak{l}}\right)_{\ell^k} = \prod_{\mathfrak{p}|\ell S\infty,\ \mathfrak{p}\neq\mathfrak{l}} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_{\ell^k}$$

pour tout α et β dans $\mathcal{E}'_X/\mathcal{E}'_X{}^{\ell^k}$; ce qui nous montre que l'isomorphisme obtenu entre $\mathcal{R}_\mathfrak{l}/\mathcal{R}_\mathfrak{l}^{\ell^k}$ et $\prod_{\mathfrak{p}|\ell S\infty,\ \mathfrak{p}\neq\mathfrak{l}} \mathcal{R}_\mathfrak{p}/\mathcal{R}_\mathfrak{p}^{\ell^k}$ est anti-isométrique.

Remarque. Un calcul immédiat donne les identités dimensionnelles :

$$dim_{\mathbb{Z}/\ell^k\mathbb{Z}} \prod_{\mathfrak{l}'\neq\mathfrak{l}} \mathcal{R}_{\mathfrak{l}}/\mathcal{R}_{\mathfrak{l}}^{\ell^k} = (r+2c-d)+2(s-1),$$

$$dim_{\mathbb{Z}/\ell^k\mathbb{Z}} \prod_{\mathfrak{p}|\infty} \mathcal{R}_{\mathfrak{p}}/\mathcal{R}_{\mathfrak{p}}^{\ell^k} = r(=0 \ sauf \ \ pour \ \ell=2, k=1),$$

$$dim_{\mathbb{Z}/\ell^k\mathbb{Z}} \prod_{\mathfrak{p}|X} \mathcal{R}_{\mathfrak{p}}/\mathcal{R}_{\mathfrak{p}}^{\ell^k} = 2x,$$

soit au total $2(r+c+s+x)-(d+2) = d+2$, comme attendu.

La loi de réciprocité primitive permet de retrouver les résultats du corollaire 3.3.

Proposition 3.6. *Soient K un corps de nombres $\mathfrak{l}$-rationnel contenant les racines ℓ-ièmes de l'unité et X un ensemble $\mathfrak{l}$-primitif maximal de places de K. Alors la place $\mathfrak{l}$ ne se décompose dans aucune ℓ-extension (galoisienne) X-modérément ramifiée L de K (i.e. non ramifiée en dehors des places sauvages ou divisant X, éventuellement complexifiée aux places réelles)*

Preuve. Par un argument classique de la théorie de Galois (cf. [GJ], prop 2.4) il suffit évidemment de faire la démonstration lorsque la ℓ-extension considérée L/K est abélienne, c'est à dire finalement de vérifier que la projection $D_{\mathfrak{l}}(K_X^{ab}/K)$ du facteur $\mathcal{R}_{\mathfrak{l}}$ dans le quotient $\mathcal{J}/\prod_{\mathfrak{p}\nmid SX\infty}\mu_{\mathfrak{p}}\mathcal{R} \simeq Gal(K_X^{ab}/K)$ recouvre le groupe de Galois. Considérons le quotient $G = Gal(K_X^{ab}/K)/D_{\mathfrak{l}}(K_X^{ab}/K)$ qui s'identifie au groupe de Galois sur K du sous-corps de décomposition de $\mathfrak{l}$ dans K_X^{ab}. La description du groupe G_{SX}^{ab} donnée plus haut (cf. preuve du th.3.4) nous donne alors l'isomorphisme :

$$G \simeq \prod_{\mathfrak{p}|\ell X\infty} \mathcal{R}_{\mathfrak{p}}/\mathcal{R}_{\mathfrak{l}}(\prod_{\mathfrak{p}|\ell X\infty}\mathcal{R}_{\mathfrak{p}} \cap (\mathcal{R}\prod_{\mathfrak{p}\nmid\ell X\infty}\mu_{\mathfrak{p}})).$$

Et les idèles principaux qui interviennent au dénominateur sont des éléments de $\mathcal{E}'_X$. Si donc nous notons s'_X l'application de semi-localisation de $\mathcal{R}$ dans $\prod_{\mathfrak{l}|SX\infty,\mathfrak{p}\neq\mathfrak{l}}\mathcal{R}_{\mathfrak{p}}$, nous obtenons en fin de compte :

$$G \simeq \prod_{\mathfrak{p}|SX\infty} \mathcal{R}_{\mathfrak{p}}/s'_X(\mathcal{E}'_X),$$

c'est à dire $G=1$ en vertu de la surjectivité de s'_X donnée par le corollaire 3.5. D'où le résultat annoncé.

3.c Illustrations numériques

D'après la proposition 2.3, un corps de nombres K est $\mathfrak{l}$-rationnel (en une place $\mathfrak{l}$ au-dessus de ℓ) si et seulement si le groupe de Galois $\mathcal{F}_{\mathfrak{l}}$ de la pro-ℓ-extension abélienne ℓ-ramifiée complètement décomposée aux places réelles et en celles sauvages $\mathfrak{l}'\neq\mathfrak{l}$ est un pro-ℓ-groupe abélien libre de rang

$$x = (c+1) - \sum_{\mathfrak{l}'|\ell,\ \mathfrak{l}'\neq\mathfrak{l}} (d_{\mathfrak{l}'}+1).$$

Le cas où la somme à droite est nulle correspondant au cas ℓ-rationnel déjà étudié ailleurs (pour lequel x a sa valeur maximale $c+1$), nous avons choisi d'illustrer ici le cas opposé où, cette somme étant maximale, la quantité x est nulle. Bien entendu toutes les valeurs intermédiaires sont envisageables, mais le cas $x = 0$ présente l'avantage de s'interpréter simplement en termes de classes de rayons. Ainsi :

Proposition 3.7. *Soient K un corps de nombres de degré $n = r + 2c$ et $\mathfrak{l}$ une place de K au-dessus d'un nombre premier ℓ telle qu'on ait l'égalité :*

$$c + 1 = \sum_{\mathfrak{l}'|\ell,\ \mathfrak{l}'\neq\mathfrak{l}} (d_{\mathfrak{l}'} + 1)$$

Alors, pour que K soit $\mathfrak{l}$-rationnel, il faut et il suffit que le ℓ-groupe $\mathcal{C}l_{\mathfrak{l}^\kappa}$ des classes de rayon $\mathfrak{l}^\kappa$ du corps K (où $\kappa = \left[\frac{e_{\mathfrak{l}}\ell}{\ell-1}\right]+1$ designe l'indice de $\mathfrak{l}$-hyperprimarité de K et $e_{\mathfrak{l}}$ l'indice de ramification absolu de $\mathfrak{l}$) soit engendré par les images des diviseurs premiers $\mathfrak{l}' \neq \mathfrak{l}$ divisant ℓ.

Preuve. D'après la proposition 2.3 et sous les hypothèses de la proposition, le corps K est $\mathfrak{l}$-rationnel si et seulement si les sous-groupes de décomposition $D_{\mathfrak{l}'}(M/K)$ attachés aux places $\mathfrak{l}' \neq \mathfrak{l}$ au-dessus de ℓ engendrent conjointement le groupe de Galois $Gal(M/K)$ de la pro-ℓ-extension $\mathfrak{l}$-ramifiée maximale M de K. Par un argument classique de théorie des groupes, cette condition peut être testée en remplaçant M par sa sous-extension abélienne élémentaire $M^{él}$ ou encore par toute sous-extension contenant $M^{él}$ par exemple le ℓ-corps de classes de rayons $\mathfrak{l}^\kappa$ (puisque par construction les unités principales congrues à 1 modulo $\mathfrak{l}^\kappa$ sont des puissances ℓ-ièmes), ce qui conduit au critère annoncé.

Exemples en degré 6.

Nous donnons d'abord des exemples de corps de degré 6 sur $\mathbb{Q}$, totalement imaginaires, ayant 3 places au-dessus de ℓ notées $\mathfrak{l}, \mathfrak{l}', \mathfrak{l}''$, de degrés locaux respectifs 4, 1 et 1, ces hypothèses entrainant bien que x est nul. Nous donnons successivement un polynôme définissant le corps K, le discriminant factorisé, la structure du ℓ-groupe de classes de rayon $\mathfrak{l}^\kappa$ avec $\kappa = 3$ pour ℓ=2 et $\kappa = 2$ sinon (les extensions considérées étant non ramifiées en ℓ) ; ainsi que les images des places $\mathfrak{l}'$ et $\mathfrak{l}''$ en fonction des générateurs du groupe des classes de rayon obtenus par le système Pari.

$\ell = 2$

$P(x) = x^6 + x^5 - 17x^3 + 21x + 16$; Disc$(K) = -6863 * 65348117$

$< g_1 >$ d'ordre 8, $< g_2 >$ d'ordre 4

$< Cl_{\mathfrak{l}'} >=< g_1 >$; $< Cl_{\mathfrak{l}''} >=< g_2 >$

$P(x) = x^6 + x^5 - 17x^3 + 6x^2 + 11x + 16$; Disc$(K) = -870989556851$

$< g_1 >$ d'ordre 4, $< g_2 >$ d'ordre 2

$< Cl_{\mathfrak{l}'} >=< g_1 >$; $< Cl_{\mathfrak{l}''} >=< g_2 >$

$\ell = 3$

$P(x) = x^6 + x^5 - 26x^3 + 15x^2 + 17x + 24$; Disc$(K) = -2^2 * 89443 * 376801$

$< g_1 >$ d'ordre 3, $< g_2 >$ d'ordre 3
$< Cl_{\mathfrak{l}'} >=< g_1 >$; $< Cl_{\mathfrak{l}''} >=< g_2^2 >$
$P(x) = x^6 + x^5 - 26x^3 + 9x^2 + 32x + 30$; $\mathrm{Disc}(K) = -2^3 * 29 * 174317272123$
$< g_1 >$ d'ordre 3, $< g_2 >$ d'ordre 3
$< Cl_{\mathfrak{l}'} >=< g_2^2 >$; $< Cl_{\mathfrak{l}''} >=< g_1^2 >$

$\ell = 5$
$P(x) = x^6 + x^5 - 6x^3 - 7x^2 + 5x + 15$; $\mathrm{Disc}(K) = -5 * 155995831$
$< g_1 >$ d'ordre 5
$< Cl_{\mathfrak{l}'} >=< g_1 >$; $< Cl_{\mathfrak{l}''} >=< g_1^4 >$
$P(x) = x^6 + x^5 - 6x^3 - 7x^2 + 20x + 30$; $\mathrm{Disc}(K) = 2^3 * 3 * 5 * 19 * 28490857$
$< g_1 >$ d'ordre 5
$< Cl_{\mathfrak{l}'} >=< g_1 >$; $< Cl_{\mathfrak{l}''} >=< g_1 >$

$\ell = 7$
$P(x) = x^6 + x^5 - 26x^3 + 11x^2 + 28x + 30$; $\mathrm{Disc}(K) = -2^3 * 5587536383683$
$< g_1 >$ d'ordre 7
$< Cl_{\mathfrak{l}'} >=< g_1^6 >$; $< Cl_{\mathfrak{l}''} >=< g_1^2 >$
$P(x) = x^6 + x^5 - 26x^3 + 11x^2 + 31x + 30$; $\mathrm{Disc}(K) = -2^{11} * 271 * 1217 * 22229$
$< g_1 >$ d'ordre 7
$< Cl_{\mathfrak{l}'} >=< g_1^4 >$; $< Cl_{\mathfrak{l}''} >=< g_1 >$

Exemples en degré 7

Nous donnons ensuite des exemples de corps de degré 7, avec 3 places complexes et une réelle, ayant toujours trois places au dessus de ℓ, de degrés locaux respectifs 5, 1 et 1, de sorte que x est nul. Ces exemples sont obtenus pour ℓ=3.

$P(x) = x^7 + x^6 - x^3 - 2x^2 - x + 3$; $\mathrm{Disc}(K) = -127 * 2410721$
$< g_1 >$ d'ordre 3, $< g_2 >$ d'ordre 3
$< Cl_{\mathfrak{l}'} >=< g_2 >$; $< Cl_{\mathfrak{l}''} >=< g_1.g_2 >$
$P(x) = x^7 + x^6 - x^3 + x^2 - x + 6$; $\mathrm{Disc}(K) = -157 * 318568463$
$< g_1 >$ d'ordre 6, $< g_2 >$ d'ordre 3
$< Cl_{\mathfrak{l}'} >=< g_1 >$; $< Cl_{\mathfrak{l}''} >=< g_2^2 >$

On donne maintenant des exemples de corps $\mathfrak{l}$-rationnels qui ne sont pas ℓ-rationnels. Toujours en degré 7, et 3 places au dessus de 3, les degrés locaux respectifs sont maintenant 4,2 et 1 et on impose à $K_{\mathfrak{l}'}$ de contenir les racines 3-ièmes de l'unité.

$P(x) = x^7 + 2x^6 + 2x^5 + x^4 - x^3 - 4x^2 - x - 6$; $\mathrm{Disc}(K) = -3 * 5 * 7963 * 227251$
$< g_1 >$ d'ordre 3, $< g_2 >$ d'ordre 3
$< Cl_{\mathfrak{l}'} >=< g_2^2 >$; $< Cl_{\mathfrak{l}''} >=< g_1^2.g_2 >$
$P(x) = x^7 + 2x^6 + 2x^5 + x^4 - x^3 - 7x^2 - x - 3$; $\mathrm{Disc}(K) = -3 * 23 * 229 * 293 * 3911$
$< g_1 >$ d'ordre 3, $< g_2 >$ d'ordre 3
$< Cl_{\mathfrak{l}'} >=< g_1 >$; $< Cl_{\mathfrak{l}''} >=< g_1^2.g_2 >$

Exemple en degré 10

Pour finir nous donnons un exemple de corps contenant les racines 3-ièmes de l'unité. Pour cela nous avons composé une extension de degré 5 ayant 3 places au dessus de 3 de degrés locaux respectifs 3, 1 et 1, avec l'extension quadratique $\mathbb{Q}(\zeta_3)$. Ici encore x est nul, pour ℓ=3 qui donne κ=4. Cet exemple complète la classification de L.V. Kuz'min ([Ku]).

$P(x) = x^{10} + 19x^8 + 8x^7 + 130x^6 + 16x^5 + 166x^4 - 888x^3 - 15x^2 + 432x + 243$
$\mathrm{Disc}(K) = -2^4 * 3^5 * 7^2 * 18583^2$
$< g_1 >$ d'ordre 3, $< g_2 >$ d'ordre 3 ;
$< Cl_{\mathfrak{l}'} >=< g_1 >\ ; < Cl_{\mathfrak{l}''} >=< g_2^2 >$

Les auteurs remercient tout particulièrement H. Cohen, F. Diaz y Diaz et X. Roblot pour l'aide qu'ils leur ont apportée dans la recherche des premiers exemples numériques significatifs obtenus par PARI.

Bibliographie

[G] G. Gras, *Logarithme p-adique et groupes de Galois*, J. reine angew. Math. **202** (1984), 343–365.

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

[Ko] H. Koch, *Galoissche Theorie der p-Erweiterungen*, Deutscher Verlag des Wissenschaften, Berlin (1970).

[Ku] L. V. Kuz'min, *Local extensions associated with ℓ-extensions with given ramification*, Izvestija **9** (1975), 693–726.

[J0] J.-F. Jaulent, *Genre des corps surcirculaires*, Pub. Math. Fac. Sci. Besançon Théor. Nombres 1985/86 (1986).

[J1] J.-F. Jaulent, *L'Arithmétique des ℓ-extentions (thèse)*, Pub. Math. Fac. Sci. Besançon Théor. Nombres 1985/86 (1986).

[J2] J.-F. Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1995), 301–325.

[J3] J.-F. Jaulent, *Théorie ℓ-adique globale du corps de classes*, J. Théor. Nombres Bordeaux **10** (1999), 355–397.

[JN] J.-F. Jaulent & A. Michel, *Classes des corps surcirculaires et des corps de fonctions*, Sém. Théor. Nombres Paris 1989/1990, Prog. in Math. **102** (1992), 141–162.

[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.

[Mi] H. Miki, *On the Leopoldt conjecture on the p-adic regulators*, J. Numb. Th. **26** (1987), 117–128.

[Mo] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Math. Nachr. **149** (1990), 163–176.

[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.

[Ng] T. Nguyen Quang Do, *Lois de réciprocité primitives*, Manuscripta Math. **72** (1991), 307–324.

[Sa] I.R. Šafarevich, *Extensions with given points of ramification* , Inst. Hautes Etudes Sci. Publ. Math. **18** (1964), 295–319 ; Amer. math. Soc. Transl. **59** (1966), 128–149.

[Se] J. P. Serre, *Cohomologie Galoisienne*, Lect. Notes in Math. **5**, Springer-Verlag (1994).

[So] J Sonn, *Epimorphism of Demuškin groups*, Israel J. Math. **17** (1974), 176–190.

[Ts] V. M. Tsetkov, *Exemples of extensions with Demuškin group*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) **103** (1980), 146–149 ; J. Soviet Math. **24** (1984), 480–482.

[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.

[W3] K. Wingberg, *Galois groups of local and global type*, J. reine angew. Math. **517** (1999), 223–239.

[Ya] M. Yamagishi, *A note on free pro-p-extensions of algebraic number fields*, J. Théor. Nombres. Bordeaux **5** (1993), 165–178.

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