Corps p-rationnels, corps p-réguliers et ramification restreinte*

Jean-François Jaulent & Thong Nguyen Quang Do

Résumé. Nous discutons les relations entre les résultats sur les corps p-réguliers obtenus par le premier auteur en collaboration avec G. Gras et ceux sur les corps p-rationnels obtenus par le second avec A. Movahheddi. Nous en déduisons en particulier une preuve plus simple du théorème de propagation de la p-rationalité dans les p-extensions, ainsi que quelques applications aux lois de réciprocité primitives.

Abstract. We discuss the relationship between the results on p-regular number fields obtained by the first author in collaboration with G. Gras and those on p-rational fields obtained by the second author in collaboration with A. Movaheddi. In particular we give a simpler proof of the main theorem on the propagation of p-rationality in p-extensions and some consequences on primitive reciprocity laws.

Table des matières

Introduction et notations

Fixons une fois pour toutes un nombre premier p. Pour chaque corps de nombres K (de degré fini sur $\mathbb{Q}$), désignons par Pl_K l'ensemble des places de K, et par $Pl_K(p)$ le sous-ensemble des places qui divisent p. Choisissons enfin un ensemble fini $S = S_K$ de places finies de K, disjoint de $Pl_K(p)$; notons M_S la pro-p-extension S-modérément ramifiée ∞-décomposée maximale de K (i.e. la composée des p-extensions galoisiennes de K qui sont non ramifiées en dehors des places de S et de celles qui divisent p, et complètement décomposées aux places à l'infini), puis $\mathcal{G}_S = \mathrm{Gal}\,(M_S/K)$ son groupe de Galois.

La théorie de la S-ramification (ou ramification restreinte) a pour objet essentiel l'étude du groupe de Galois $\mathcal{G}_S$ dont la structure reflète les propriétés arithmétiques du corps K par rapport au nombre premier p. Ainsi, la structure du groupe abélianisé $\mathcal{G}_S^{\mathrm{ab}} = \mathcal{G}_S/\mathcal{G}'_S$ est décrite par la théorie du corps de classes qui donne l'isomorphisme

$$\mathcal{G}_S^{\mathrm{ab}} \simeq \mathbb{Z}_p^{\rho} \oplus \mathcal{T}_S,$$

*J. Théor. Nombres Bordeaux **5** (1993), 343–363.

où ρ est égal à $1+c$ ($c = c_K$, nombre de places complexes de K) sous la conjecture de Leopoldt, et $\mathcal{T}_S$ est un p-groupe fini dont les propriétés sont intimement reliées à celles des fonctions L p-adiques (lorsqu'elles sont définies) ainsi qu'à celles des divers noyaux de la K-théorie (cf. e.g. [2, 7, 14]).

Dans cet article, nous nous proposons d'étudier des familles de corps de nombres, appelés p-réguliers dans [5], ou p-rationnels dans [11], pour lesquels on peut donner une description complète de $\mathcal{G}_S$ lorsque l'ensemble S est p-primitif au sens de Gras (cf. [4]). Une conséquence particulièrement intéressante de cette description est la propagation de la p-rationalité dans les p-extensions primitivement ramifiées, ce qui permet d'établir par des méthodes purement algébriques la validité des conjectures de Leopoldt et de Gross-Kuz'min pour une classe infinie de corps qui satisfont des conditions arithmétiques dures (mais de vérification facile) et sont essentiellement non-abéliens, donc inaccessibles (pour l'instant) aux méthodes transcendantes.

Avant d'énoncer ces conditions, fixons quelques notations. Étant donné un corps de nombres K, nous écrivons :

- M la pro-p-extension p-ramifiée ∞-décomposée maximale de K, et $\mathcal{G} = \mathrm{Gal}\,(M/K)$ son groupe de Galois ;
- M^{ab} la sous-extension maximale de M qui est abélienne sur K, et $\mathcal{G}^{\mathrm{ab}} = \mathrm{Gal}\,(M^{\mathrm{ab}}/K)$ son groupe Galois ;
- Z la composée des $\mathbb{Z}_p$-extensions de K, de sorte que le groupe fini $\mathcal{T} = \mathrm{Gal}\,(M^{\mathrm{ab}}/Z)$ est le sous-groupe de torsion de $\mathcal{G}$;
- $V = \{x \in K^\times \mid x \in K_{\mathfrak{p}}^{\times p} \ \forall \mathfrak{p}|p \ \ \& \ \ v_{\mathfrak{l}}(x) \equiv 0 \mod p \quad \forall \mathfrak{l} \nmid \infty\}$ le groupe des éléments hyperprimaires de K (relativement à p) ;
- Cl' le p-groupe des p-classes de diviseurs de K, i.e. le p-sous-groupe de Sylow du quotient du groupe des classes d'idéaux au sens restreint par le sous-groupe engendré par les classes des idéaux au-dessus de p.

Plus généralement, étant donné un ensemble fini S de places finies étrangères à p, nous notons :

- M_S la pro-p-extension S-modérément ramifiée ∞-décomposée maximale de K (i.e. la composée des p-extensions galoisiennes de K qui sont non ramifiées en dehors de S et de p et complètement décomposées aux places à l'infini), et $\mathcal{G}_S = \mathrm{Gal}\,(M_S/K)$ son groupe de Galois ;
- M_S^{ab} la sous-extension maximale de M_S qui est abélienne sur K, puis $\mathcal{G}_S^{\mathrm{ab}} = \mathrm{Gal}\,(M_S^{\mathrm{ab}}/K)$ son groupe de Galois, et $\mathcal{T}'_S = \mathrm{Gal}\,(M_S^{\mathrm{ab}}/Z)$ le sous-groupe de torsion de $\mathcal{G}_S^{\mathrm{ab}}$;
- $V = \{x \in K^\times \mid x \in K_{\mathfrak{p}}^{\times} \ \forall \mathfrak{p}|p \ \& \ v_{\mathfrak{l}}(x) \equiv 0 \mod p \ \forall \mathfrak{l} \nmid S\infty\}$ le groupe des éléments S-hyperprimaires de K (relativement à p) ;
- Cl'_S le p-groupe des Sp-classes de diviseurs de K, i.e. le quotient de Cl' par le sous-groupe engendré par les p-classes au sens restreint des idéaux construits sur les places de S.

1 Corps p-réguliers & corps p-rationnels

Définition & Proposition 1.1. *Nous disons qu'un corps de nombres K est :*

(i) p-régulier, lorsque le p-sous-groupe de Sylow $R_2(K)$ du noyau dans $K_2(K)$ des symboles réguliers est trivial ;

(ii) p-rationnel, lorsque le groupe de Galois $\mathcal{G}_K = Gal\,(M/K)$ de la pro-p-extension maximale M/K qui est p-ramifiée et ∞-décomposée est un pro-p-groupe libre.

Lorsque K contient le sous-corps réel maximal $Q[\zeta+\zeta^{-1}]$ du p-ième corps cyclotomique $Q[\zeta]$, il est équivalent d'affirmer que K est p-régulier ou qu'il est p-rationnel.

L'équivalence entre régularité et rationalité, sous la condition suffisante $(\zeta+\zeta^{-1}) \in K$, résulte de l'égalité entre p-rangs :

$$rg_p R_2(K) = rg_p \mathcal{T}_K + \delta_{\text{Leopoldt}} \qquad \text{(cf. [4], Th. 5)},$$

qui fait intervenir le défaut de la conjecture de Leopoldt dans K et de la caractérisation suivante :

Théorème 1.2. *Pour tout corps de nombres K, les conditions suivantes sont équivalentes :*

(i) Le groupe de Galois $\mathcal{G}_K = Gal\,(M/K)$ de la pro-p-extension maximale de K qui est p-ramifiée et ∞-décomposée est un pro-p-groupe libre (nécessairement sur $1+c_K$ générateurs, où c_K est le nombre de places complexes de K).

(ii) Le groupe de Galois $\mathcal{G}_K^{\mathrm{ab}} = Gal\,(M^{\mathrm{ab}}/K)$ de la pro-p-extension abélienne maximale de K qui est p-ramifiée et ∞-décomposée est un $\mathbb{Z}_p$-module libre de dimension $1+c_K$.

(iii) Le corps K vérifie la conjecture de Leopoldt (pour le nombre premier p) et le sous-module de torsion $\mathcal{T}_K$ de $Gal\,(M^{\mathrm{ab}}/K)$ est nul.

(iv) Le groupe V_K des éléments p-hyperprimaires du corps K se réduit à $K^{\times p}$ et l'on a l'identité entre les p-rangs des p-groupes de racines de l'unité :

$$rg_p\,\mu_K = \sum_{\mathfrak{p}|p} rg_p\,\mu_{K_p}.$$

(v) Le corps K vérifie l'une des deux conditions suivantes :

a) ou bien K contient une racine primitive p-ième de l'unité ζ_0, auquel cas K possède une unique place $\mathfrak{p}$ au dessus de p, et le p-groupe des p-classes d'idéaux au sens restreint Cl'_K est nul ;

b) ou bien K ne contient pas ζ, auquel cas les places de K au-dessus de p ne se décomposent pas complètement dans l'extension cyclotomique $K[\zeta]/K$ et la ω-composante du p-groupe des p-classes d'idéaux au sens restreint $Cl'_{K[\zeta]}$ du corps $K[\zeta]$ est nulle, si ω désigne le caractère cyclotomique de $Gal\,(V[\zeta]/K)$.

Preuve. Commençons par rappeler les formules de Šafarevič (cf. [16]) donnant les nombres minimaux de générateurs $d(\mathcal{G}_K)$ et de relations $r(\mathcal{G}_K)$ du pro-p-groupe de Galois $\mathcal{G}_K$:

$$\begin{aligned} d(\mathcal{G}_K) &= \dim_{\mathbb{F}_p}(H^1(\mathcal{G}_K,\mathbb{F}_p)) \\ &= c_K + 1 + \dim_{\mathbb{F}_p} V_K/K^{\times p} + (\sum_{\mathfrak{p}|p} rg_p\,\mu_{K_\mathfrak{p}} - rg_p\,\mu_K); \\ r(\mathcal{G}_K) &= \dim_{\mathbb{F}_p}(H^2(\mathcal{G}_K,\mathbb{F}_p)) = \dim_{\mathbb{F}_p} V_K/K^{\times p} + (\sum_{\mathfrak{p}|p} rg_p\,\mu_{K_\mathfrak{p}} - rg_p\,\mu_K). \end{aligned}$$

Cela étant, nous avons :

(i) $\Longrightarrow$ (ii), car $\mathcal{G}_K$ ne peut être libre que sur c_K+1 générateurs, auquel cas $\mathcal{G}_K^{\mathrm{ab}}$ est évidemment un $\mathbb{Z}_l$-module libre de dimension c_K+1.

(ii) $\Longrightarrow$ (iii), puisque la conjecture de Leopoldt affirme précisément que K possède exactement c_K+1 $\mathbb{Z}_p$-extensions indépendantes.

(iii) $\Longrightarrow$ (iv), en vertu précisément de l'identité sur les rangs, sous la conjecture de Leopoldt :

$$rg_p\mathcal{T}_K = \dim_{\mathbb{F}_p} V_K/K^{\times p} + (\sum_{\mathfrak{p}|p} rg_p\mu_{K_\mathfrak{p}} - rg_p\mu_K).$$

(iv) $\Longrightarrow$ (i), d'après les formules de Šafarevič énoncées plus haut.

Enfin, l'équivalence entre (iv) et (v) résulte de la théorie de Kummer : si K contient ζ, l'égalité $\sum_{\mathfrak{p}|p} rg_p\mu_{K_\mathfrak{p}} = rg_p\mu_K = 1$ signifie que K possède exactement une place au-dessus de p ; et le groupe $V_K/K^{\times p}$ s'identifie au radical de la p-extension abélienne élémentaire maximale de K qui est non ramifiée aux places (finies) étrangères à p et complètement décomposée à celles au-dessus de p, c'est à dire précisément au "dual" de Kummer du groupe Cl'_K :

$$V_K/K^{\times p} \simeq \ \mathrm{Hom}\ (Cl'_K\ ,\ {}_p\mu_K).$$

Si K ne contient pas ζ, la même description vaut pour le corps $K' = K[\zeta]$. Le groupe $V_K/K^{\times p}$ correspond à la composante unité du groupe $V_{K'}/K'^{\times p}$, donc, dans la dualité précédente, à la ω-composante du groupe $Cl'_{K'}$, puisque le caractère cyclotomique ω est le reflet du caractère unité dans l'involution du miroir. Enfin, l'identité $\sum_{\mathfrak{p}|p} rg_p\mu_{K_\mathfrak{p}} = rg_p\mu = 0$ signifie ici que les places de K au-dessus de p ne se décomposent pas complètement dans l'extension cyclotomique K'/K ; ce qui achève la démonstration.

Corollaire 1.3 (Exemples de corps p-réguliers ou p-rationnels)**.**

(i) Le corps $\mathbb{Q}$ des rationnels est p-régulier et p-rationnel pour tout nombre premier p.

(ii) Pour tout premier p, le corps cyclotomique $K = \mathbb{Q}[\zeta_{p^n}]$ engendré par une racine primitive p^n-ième de l'unité est p-régulier (et p-rationnel) si et seulement si le nombre premier p est régulier (au sens habituel).

(iii, a) Les corps quadratiques imaginaires $K = \mathbb{Q}[\sqrt{-d}]$ qui sont 2-réguliers (et 2-rationnels) sont $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{-2}]$, ainsi que les corps $\mathbb{Q}[\sqrt{-l}]$ et $\mathbb{Q}[\sqrt{-2l}]$ pour l premier impair, $l \equiv \pm 3 \pmod 8$.

(iii, b) Sont 3-réguliers (et 3-rationnels) le corps $\mathbb{Q}[\sqrt{3}]$ et les corps $\mathbb{Q}[\sqrt{-d}]$ pour lesquels $d \not\equiv 3 \pmod 9$ et 3 ne divise pas le nombre de 3-classes du corps quadratique réel $\mathbb{Q}[\sqrt{3d}]$.

(iii, c) Enfin, pour $p \geq 5$, les corps quadratiques imaginaires qui ont un p-groupe des classes trivial sont p-rationnels.

Preuve. Distinguons les divers cas :

(i) Le cas du corps des rationnels se traite en deux temps : D'un côté, un calcul direct (cf. [17]) montre que le noyau régulier $R_2(\mathbb{Q})$ est nul, de sorte que $\mathbb{Q}$ est p-rationnel pour tout p ; ce qui justifie la terminologie. D'un autre côté, la théorie élémentaire du corps de classes assure que la p-extension abélienne p-ramifiée ∞-décomposée maximale de $\mathbb{Q}$ est bien la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$; ce qui établit la régularité.

(ii) Pour les corps cyclotomiques $\mathbb{Q}[\zeta_{p^n}]$, la proposition 1 assure l'équivalence entre p-régularité et p-rationalité. Maintenant la condition (v, a) du théorème 2 montre que celle-ci se lit sur le nombre de classes (en l'occurrence au-sens ordinaire) du corps $\mathbb{Q}[\zeta_{p^n}]$.

(iii) Pour les corps quadratiques imaginaires $\mathbb{Q}[\sqrt{-d}]$, il convient de distinguer suivant les valeurs de p. Pour $p = 2$ ou 3 les notions de p-régularité et de p-rationalité coïncident, en vertu de la proposition 1 ; pour $p \geq 5$, en revanche, le théorème 2 ne permet d'atteindre que la p-rationalité.

- Si p vaut 2, la condition $(v.a)$ exige que le corps $\mathbb{Q}[\sqrt{-d}]$ n'admette qu'une place au-dessus de 2 (ce qui exclut $d \equiv -1 \pmod 8$), et que son nombre de 2-classes d'idéaux soit impair ce qui impose, d'après la formule des classes ambiges de Chevalley généralisée (cf. [7]), qu'il y ait au plus une place modérément ramifiée dans l'extension $K/\mathbb{Q}$, et plus précisément, qu'on ait soit $K = \mathbb{Q}[\sqrt{-1}]$ ou $\mathbb{Q}[\sqrt{-2}]$, soit $K = \mathbb{Q}[\sqrt{-l}]$ ou $\mathbb{Q}[\sqrt{-2l}]$, avec l premier impair tel que 2 ne soit pas norme dans l'extension $K/\mathbb{Q}$, ce qui s'écrit : $l \equiv \pm 3 \mod 8$.

- Si p vaut 3, une fois écarté le cas cyclotomique $K = \mathbb{Q}[\sqrt{-3}]$ déjà traité, la condition (v, b) exige $\mathbb{Q}_3[\sqrt{-d}] \neq \mathbb{Q}_3[\sqrt{-3}]$ (i.e. $d \not\equiv 3 \pmod 9$), et que 3 ne divise pas le nombre de 3-classes du corps quadratique réel $\mathbb{Q}[\sqrt{3d}]$ (qui est le reflet de $\mathbb{Q}[\sqrt{-d}]$ dans l'involution du miroir).

- Enfin, pour $p \geq 5$, la théorie du corps de classes montre directement que la p-extension abélienne p-ramifiée maximale de $K = \mathbb{Q}[\sqrt{-d}]$ est exactement la composée des $\mathbb{Z}_p$-extensions de K sous la condition suffisante que la p-partie du groupe des classes d'idéaux de K soit triviale.

Corollaire 1.4 (Généralisation d'un critère de Kummer)**.** *Soient p un nombre premier impair, K un corps p-rationnel, et u une unité de K. Si u vérifie la congruence*

$$u \equiv 1 \pmod{p^2},$$

c'est la puissance p-ième d'une unité v de K.

Preuve. Soient $v_\mathfrak{p}$ la valuation et $e_\mathfrak{p}$ l'indice de ramification absolu d'une place $\mathfrak{p}$ de K au-dessus de p. Par hypothèse nous avons :

$$v_\mathfrak{p}(u-1) \geq 2e_\mathfrak{p} > \frac{p}{p-1}\, e_\mathfrak{p} \ \text{ , indice d'hyperprimarité,}$$

donc $u \in K_\mathfrak{p}^{\times p}$, pour tout $\mathfrak{p}$ divisant p, i.e. $u \in V_K$. Le corps K étant supposé p-rationnel, ceci entraîne $u \in K^{\times p}$, par la condition (iv) du théorème ; d'où le résultat.

Ce critère sera sensiblement amélioré dans la section 4 (cf. Cor. 4.3).

Corollaire 1.5. *Toute p-extension p-ramifiée et ∞-décomposée d'un corps p-rationnel est encore un corps p-rationnel.*

Preuve. Rappelons qu'une p-extension L/K est, par définition, une extension galoisienne dont le groupe de Galois est un p-groupe (fini). Cela étant, si L/K est p-ramifiée et ∞-décomposée, alors L/K est une sous-extension de M/K, de sorte que M est encore la pro-p-extension p-ramifiée ∞-décomposée maximale de L. Ainsi $\mathcal{G}_L = \mathrm{Gal}\,(M/L)$ est un sous-groupe d'indice fini de $\mathcal{G}_K = \mathrm{Gal}\,(M/K)$. Si $\mathcal{G}_K$ est pro-p-libre, $\mathcal{G}_L$ l'est donc aussi ; autrement dit si K est p-rationnel, il en est de même de L.

Tout le problème de la section 3 consistera à étendre cette propriété de montée de la p-rationalité à certaines p-extensions L/K qui admettent de la ramification en dehors de p. Pour cela nous aurons besoin de quelques résultats sur l'arithmétique des p-extensions abéliennes des corps p-rationnels, que nous allons maintenant établir.

2 p-extensions abéliennes des corps p-rationnels.

Commençons par rappeler le formalisme p-adique de la théorie du corps de classes développé dans [7]. Le corps de base K étant supposé fixé, écrivons :

— $\mathcal{J} = \prod_{\mathfrak{l}}^{res} \mathcal{R}_{\mathfrak{l}}^{\times}$, le p-adifié du groupe des idèles, c'est-à-dire le produit restreint des complétés profinis $\mathcal{R}_{\mathfrak{l}}^{\times} = \varprojlim_n K_{\mathfrak{l}}^{\times}/K_{\mathfrak{l}}^{\times p^n}$ des groupes multiplicatifs des complétés non complexes de K, muni de sa topologie naturelle de limite inductive ;

— $\mathcal{U} = \prod_{\mathfrak{l}} \mathcal{U}_{\mathfrak{l}} = \prod_{\mathfrak{p}|p} \mathcal{U}_{\mathfrak{p}}\ \prod_{\mathfrak{l}\nmid p\infty} \mu_{\mathfrak{l}}$, le sous-groupe compact formé des idèles unités (le groupe $\mathcal{U}_{\mathfrak{l}}$ étant le groupe des unités principales de $K_{\mathfrak{l}}^{\times}$ lorsque $\mathfrak{l}$ divise p, son p-sous-groupe de torsion sinon, sauf lorsque $\mathfrak{l}$ est réelle, auquel cas $\mathcal{R}_{\mathfrak{l}} = \mu_{\mathfrak{l}}$ est le groupe $\mathbb{Z}_p/2\mathbb{Z}_p$ et $\mathcal{U}_{\mathfrak{l}}$ le sous-groupe trivial) ;

— $\mathcal{R} = \mathbb{Z}_p \otimes_{\mathbb{Z}} K^{\times}$, le groupe des idèles principaux, défini comme le tensorisé p-adique du groupe multiplicatif de K, et regardé comme plongé dans $\mathcal{J}$ (de sorte que le quotient $\mathcal{C} = \mathcal{J}/\mathcal{R}$ s'identifie, dans l'isomorphisme p-adique du corps de classes, au groupe de Galois de la pro-p-extension abélienne maximale de K) ;

— $\mathcal{D} = \mathcal{J}/\mathcal{U}$ le groupe des diviseurs de K, et $\mathcal{P} = \mathcal{R}\mathcal{U}/\mathcal{U}$ le sous-groupe des diviseurs principaux, image canonique de $\mathcal{R}$ dans $\mathcal{J}$; puis $Cl = \mathcal{D}/\mathcal{P}$ le groupe des classes de diviseurs, qui s'identifie canoniquement au p-sous-groupe de Sylow du groupe des classes d'idéaux de K prises au sens restreint ;

— $\mathcal{R}^{\infty}$, enfin, le sous-groupe infinitésimal de $\mathcal{R}$, i.e. le noyau de la surjection canonique s_p : $\mathcal{R} \to \mathcal{R}_p = \prod_{\mathfrak{p}|p} \mathcal{R}_{\mathfrak{p}}$ induite par le plongement diagonal de K dans le produit de ses complétés aux places divisant p.

Avec ces notations, la conjecture de Leopoldt affirme qu'un idèle principal $x \in \mathcal{R}$ qui est localement partout une racine de l'unité est une racine de l'unité dans $\mathcal{R}$, ce que nous écrivons :

$$\mathcal{R} \cap \prod_{\mathfrak{l}}\ \mu_{\mathfrak{l}} = \mu.$$

En particulier, puisque les groupes $\mathcal{R}_{\mathfrak{l}}$ pour $\mathfrak{l}$ réelle et $\mathcal{U}_{\mathfrak{l}}$ pour $\mathfrak{l}$ finie étrangère à p se réduisent à $\mu_{\mathfrak{l}}$, les unités (au sens ordinaire) de $\mathcal{R}^{\infty}$, i.e. les éléments du tensorisé $\mathbb{E} = \mathbb{Z}_p \otimes_{\mathbb{Z}} E$ qui sont infinitésimaux, sont les racines de l'unité dans $\mathcal{R}$ d'image triviale dans $\mathcal{R}_p$, donc égales à l ; ce qui s'écrit :

$$\mathcal{E}^{\infty} = \mathcal{E} \cap R^{\infty} = 1.$$

Cela posé, nous avons :

Proposition 2.1. *Soient K un corps p-rationnel et S un ensemble fini de places modérées de K (i.e. de places finies étrangères à p). Alors, dans la correspondance du corps de classes, le sous-groupe de torsion $\mathcal{T}_S = \mathrm{Gal}\,(M_S^{\mathrm{ab}}/Z)$ de la pro-p-extension abélienne S-modérément-ramifiée ∞-décomposée maximale M_S^{ab} de K (i.e. de la composée des p-extensions abéliennes de K qui* *sont non ramifiées en dehors de S et de p, et complètement décomposées aux places à l'infini) est donné par l'isomorphisme :*

$$\mathcal{T}_S = \ Gal\ (M_S^{\mathrm{ab}}/Z) \simeq \prod_{\mathfrak{l} \in S} \mu_{\mathfrak{l}}.$$

C'est donc le produit direct des sous-groupes d'inertie attachés aux places de S dans le groupe $\mathcal{G}_S^{\mathrm{ab}} = \mathrm{Gal}(M_S^{\mathrm{ab}}/K)$.

Preuve. Le corps K étant supposé p-rationnel, la composée Z des $\mathbb{Z}_p$-extensions de K est exactement la pro-p-extension abélienne p-ramifiée ∞-décomposée maximale M^{ab} de K. Il vient donc :

$$\mathrm{Gal}(Z/K) = \mathrm{Gal}(M^{\mathrm{ab}}/K) \simeq \mathcal{J} / \prod_{\mathfrak{l} \nmid p} \mu_{\mathfrak{l}} \quad R$$

et, par ailleurs :

$$\mathrm{Gal}(M_S^{\mathrm{ab}}/K) = \mathcal{J} / \prod_{\mathfrak{l} \nmid pS} \mu_L \ \mathcal{R}.$$

Par suite, le sous-module de torsion $\mathcal{T}_S$ de $\mathrm{Gal}(M_S^{\mathrm{ab}}/K)$ est bien :

$$\mathcal{T}^S = \ \mathrm{Gal}\ (M_S^{\mathrm{ab}}/Z) = \prod_{\mathfrak{l} \in S} \mu_{\mathfrak{l}} / \left(\prod_{\mathfrak{l} \in S} \mu_{\mathfrak{l}} \cap \mathcal{R} \prod_{\mathfrak{l} \nmid pS} \mu_L \right) = \prod_{\mathfrak{l} \in S} \mu_{\mathfrak{l}}.$$

puisque les idèles principaux qui interviennent au dénominateur sont des unités infinitésimales.

Pour obtenir maintenant une décomposition analogue du groupe $\mathcal{G}_S^{\mathrm{ab}}$ tout entier, faisant intervenir cette fois les groupes de décomposition attachés aux places de S, nous allons imposer aux éléments de S des conditions de primitivité :

Proposition & Définition 2.2. *Étant donné un corps de nombres K et un ensemble S de s places modérées de K (i.e. de s places finies étrangères à p), les conditions suivantes sont équivalentes :*

(i) Les symboles d'Artin $(\mathfrak{p}, Z/K)$ des places de S, pris dans la composée Z des $\mathbb{Z}_p$-extensions de K, engendrent un sous-module pur de Gal (Z/K), de dimension s.

(ii) Les mêmes symboles $(\mathfrak{p}, Z^{\acute{e}l}/K)$, pris dans la sous-extension élémentaire de Z, engendrent un sous-$\mathbb{F}_p$-espace vectoriel de Gal $(Z^{\acute{e}l}/K)$ de dimension s.

(iii) L'intersection $Z^{\acute{e}l}(S)$ des sous-corps de décomposition dans $Z^{\acute{e}l}$ des places de S est d'indice p^s dans $Z^{\acute{e}l}$.

Lorsqu'elles sont vérifiées, nous disons que S est primitif.

La notion d'ensemble primitif de places modérées a été introduite par G. Gras (cf. [3]), sous une forme différente, pour étudier la propagation de la p-régularité, sous la conjecture de Leopoldt. La condition (iii) a été utilisée tout à fait indépendamment par H. Miki pour produire précisément une condition suffisante de propagation de cette conjecture (cf. [9]). La forme (i) permet de construire directement des ensembles primitifs de places modérées en utilisant le logarithme divisoriel (cf. [5]) ; la forme (ii) permet de faire de même à l'aide des symboles modérés d'ordre p (cf. [11]). Bien entendu, l'équivalence de (i), (ii) et (iii) est immédiate.

Remarques.

(i) Le théorème de densité de Čebotarev garantit l'existence d'une infinité d'ensembles primitifs ne rencontrant pas un ensemble fini de places données.

(ii) Si l'ensemble S est primitif, son cardinal s est majoré par le nombre de $\mathbb{Z}_p$-extensions linéairement indépendantes sur K donc, sous la conjecture de Leopoldt, par la quantité $1 + c$, où c est le nombre de places complexes de K.

(iii) Sous la conjecture de Leopoldt, les ensembles primitifs maximaux (pour l'inclusion) sont exactement ceux de cardinal $1 + c$.

Exemples d'ensembles primitifs de places modérées.

(i) Soit K un corps totalement réel satisfaisant la conjecture de Leopoldt (pour le nombre premier p). Dans ce cas les ensembles primitifs de places modérées de K sont exactement les singletons $S = \{\mathfrak{l}\}$, où $\mathfrak{l}$ est une place de K totalement inerte dans la $\mathbb{Z}_p$-extension cyclotomique Z/K (autrement dit une place finie, étrangère à p, satisfaisant la condition $\mu_\mathfrak{l} = \mu$).

(ii) Soit K le corps cyclotomique $\mathbb{Q}[\zeta_p]$ engendré par une racine primitive p-ième de l'unité. Pour $p = 3$, l'ensemble $S = \{\mathfrak{l}_7, \mathfrak{l}_{19}\}$, où $\mathfrak{l}_7$ (resp.$\mathfrak{l}_{19}$) est une place de K au-dessus de 7 (resp. de 19), est 3-primitif. De même, pour $p = 5$, l'ensemble $S = \{\mathfrak{l}_{11}, \mathfrak{l}'_{11}, \mathfrak{l}''_{11}\}$, où $\mathfrak{l}_{11}, \mathfrak{l}'_{11}$ et $\mathfrak{l}''_{11}$ sont trois des quatre places au-dessus de 11, est 5-primitif.

Nous sommes désormais en mesure de préciser la proposition 1 :

Théorème 2.3. *Soient K un corps p-rationnel et S un ensemble p-primitif maximal de places modérées de K. Alors, dans la correspondance du corps de classes ℓ-adique, le groupe de Galois $\mathcal{G}_S^{\mathrm{ab}}$ de la pro-p-extension abélienne S-modérément ramifiée ∞-décomposée maximale M_S^{ab} de K (i.e. du compositum des p-extensions abéliennes de K qui sont non ramifiées en dehors de S et de p, et complètement décomposées aux places à l'infini) est donné par l'isomorphisme :*

$$\mathcal{G}_S^{\mathrm{ab}} = \mathrm{Gal}(M_S^{\mathrm{ab}}/K) \simeq \prod_{\mathfrak{l}\in S} \mathcal{R}_\mathfrak{l}.$$

C'est donc le produit direct des sous-groupes de décomposition des $c+1$ places de S.

Réciproquement, si pour un ensemble S de $c+1$ places modérées d'un corps de nombres K, le groupe $\mathcal{G}_S^{\mathrm{ab}} =$ Gal (M_S^{ab}/K) admet une décomposition du type précédent, le corps K est p-rationnel et l'ensemble S p-primitif maximal.

Preuve. Supposons le corps K p-rationnel et l'ensemble S p-primitif maximal. Dans ce cas, le groupe de Galois Gal $(Z/K) \simeq \mathcal{J}/\mathcal{R}\prod_{\mathfrak{q}\nmid pS}\mu_\mathfrak{q}$ du compositum des $\mathbb{Z}_p$-extensions de K est un $\mathbb{Z}_p$-module libre de dimension $c+1$ qui est produit direct des $c+1$ sous-groupes de décomposition $D_\mathfrak{l}(Z/K) = \mathcal{R}_\mathfrak{l}/\mathcal{R}_\mathfrak{l} \cap (\mathcal{R}\prod_{\mathfrak{q}\nmid pS}\mu_\mathfrak{q})$ attachés aux places de S. Cela étant, des isomorphismes $\mathcal{R}_\mathfrak{l} = \pi_\mathfrak{l}^{\mathbb{Z}_p}\mu_\mathfrak{l}$ (donnés par le choix d'une uniformisante $\pi_\mathfrak{l}$ dans $\mathcal{R}_\mathfrak{l}$), il suit donc :

$$\mathcal{R}_\mathfrak{l} \cap (\mathcal{R}\prod_{\mathfrak{q}\nmid pS}\mu_\mathfrak{q}) = \mu_\mathfrak{l} \;\text{ et }\; \mathrm{Gal}(Z/K) \simeq \prod_{\mathfrak{l}\in S}\mathcal{R}_\mathfrak{l}/\mu_\mathfrak{l}$$

ce qui, compte tenu du résultat $\mathrm{Gal}(M_S^{\mathrm{ab}}/Z) \simeq \prod_{\mathfrak{l}\in S}\mu_L\mathfrak{l}$ déjà obtenu, conduit à la décomposition annoncée. La réciproque est immédiate.

Corollaire 2.4. *Soient K p-rationnel et S p-primitif de cardinal $s \leq 1+c$. Alors, le groupe de Galois $\mathcal{G}_S^{\mathrm{ab}}$ s'écrit comme produit direct*

$$\mathcal{G}_S^{\mathrm{ab}} = (\prod_{\mathfrak{l}\in S}\mathcal{R}_\mathfrak{l}) \times \mathcal{H}^{\mathrm{ab}}$$

des groupes de décomposition des places de S et d'un $\mathbb{Z}_p$-module libre $\mathcal{H}^{\mathrm{ab}}$ de dimension $1+c-s$.

Corollaire 2.5. *Pour tout ensemble p-primitif S de places modérées d'un corps p-rationnel K, il existe une p-extension abélienne K_S^{ab}/K (généralement non unique) S-ramifiée et ∞-décomposée, maximalement ramifiée en toute place $\mathfrak{l}$ de S (en ce sens que le groupe d'inertie correspondant $I_\mathfrak{l}(K_S^{\mathrm{ab}}/K)$ a l'ordre de $\mu_\mathfrak{l}$), dont le groupe Galois est le produit direct des sous-groupes d'inertie attachés aux places de S, ce qui s'écrit ici :*

$$\mathrm{Gal}(K_S^{\mathrm{ab}}/K) \simeq \prod_{\mathfrak{l}\in S}\mu_\mathfrak{l}.$$

Preuve. Cela résulte immédiatement du corollaire précédent, le sous-groupe de torsion $\mu_S = \prod_{\mathfrak{l}\in S}\mu_\mathfrak{l}$ étant un facteur direct du produit $\mathcal{R}_S = \prod_{\mathfrak{l}\in S}\mathcal{R}_\mathfrak{l}$: il suffit de prendre pour K_S^{ab} le corps des points fixes dans M_S^{ab} d'un supplémentaire de μ_S.

Théorème 2.6. *Soient K un corps p-rationnel et S un ensemble p-primitif maximal de places modérées de K. L'injection diagonale $K^\times \to K_p^\times = \prod_{\mathfrak{p}|p} K_\mathfrak{p}^\times$ du groupe multiplicatif de K dans le produit de ceux de ses complétés aux places divisant p induit un isomorphisme du tensorisé p-adique $\mathcal{E}'_S = \mathbb{Z}_p \otimes E'_S$ du groupe de S_p-unités (au sens ordinaire) sur le produit $\mathcal{R}_p = \prod_{\mathfrak{p}|p} \mathcal{R}_\mathfrak{p}$.*

Réciproquement, si pour un ensemble S de $c+1$ places d'un corps de nombres, l'application de semi-localisation induit un isomorphisme de $\mathcal{E}'_S$ sur $\mathcal{R}_p$, alors le corps K est p-rationnel, et l'ensemble S p-primitif maximal, dès lors que le p-groupe Cl'_S des Sp-classes d'idéaux est trivial.

Preuve. D'après la théorie du corps de classes, le groupe de Galois $\mathcal{G}_S^{\mathrm{ab}}$ de la pro-p-extension abélienne S-modérément ramifiée ∞-décomposée maximale M_S^{ab} de K est donné par l'isomorphisme :

$$\mathcal{G}_S^{\mathrm{ab}} \simeq \mathcal{J}/\mathcal{R} \prod_{\mathfrak{l} \nmid pS} \mu_\mathfrak{l} \simeq \mathcal{R}_p\mathcal{R}_S/(\mathcal{R}_p\mathcal{R}_S \cap \mathcal{R} \prod_{\mathfrak{l} \nmid pS} \mu_\mathfrak{l}) = \mathcal{R}_p\mathcal{R}_S/s_{pS}(\mathcal{E}'_S),$$

sous réserve de trivialité du p-groupe $Cl'_S \simeq \mathcal{J}/\mathcal{R}\mathcal{R}_S\mathcal{R}_p \prod_{\mathfrak{l}\nmid pS} \mu_\mathfrak{l}$ des Sp-classes d'idéaux de K.

Si K est p-rationnel et S p-primitif maximal, cette condition est évidemment remplie (la p-extension abélienne non ramifiée $pS\infty$-décomposée de K étant alors triviale) ; et l'isomorphisme $\mathcal{G}_S^{\mathrm{ab}} \simeq \mathcal{R}_S$ donné par le théorème 3 affirme que le groupe $\mathcal{E}'_S$ s'envoie surjectivement sur le facteur $\mathcal{R}_p$, ce qui, compte tenu de l'égalité des rangs, signifie que l'application $s_p : \mathcal{E}'_S \to \mathcal{R}_p$ est un isomorphisme. La réciproque est immédiate.

En présence des racines p-ièmes de l'unité, nous donnerons plus loin un résultat dual de ce théorème, basé cette fois sur la théorie de Kummer.

3 p-extensions galoisiennes des corps p-rationnels

L'objet de cette section est de relever le théorème 2.3, qui décrit abélianisé $\mathcal{G}_S^{\mathrm{ab}}$ du groupe de Galois $\mathcal{G}_S = \mathrm{Gal}(M_S/K)$, en un théorème de structure pour le pro-p-groupe $\mathcal{G}_S$.

Introduisons pour cela quelques notations supplémentaires :

Désignons par $\circledast$ le produit libre dans la catégorie des pro-p-groupes, puis, pour chaque place $\mathfrak{l}$ de K, faisons choix de l'une $\mathfrak{L}$ des places de M_S au-dessus de $\mathfrak{l}$, et notons (par abus) $\mathcal{D}_\mathfrak{l}$ le groupe de décomposition de $\mathfrak{L}$ dans M_S/K (qui n'est donc défini qu'à conjugaison près). Notons maintenant $\mathcal{G}_\mathfrak{l}$ le groupe de Galois de la pro-p-extension maximale de $K_\mathfrak{l}$, et $\psi_\mathfrak{l}$ le morphisme de $\mathcal{G}_\mathfrak{l}$ dans $\mathcal{G}_S$ induit par la surjection canonique de $\mathcal{G}_\mathfrak{l}$ sur $\mathcal{D}_\mathfrak{l}$. Par la propriété universelle du produit libre, nous définissons ainsi un morphisme ψ_S du produit $\circledast_{\mathfrak{l}\in S}\mathcal{G}_\mathfrak{l}$ dans $\mathcal{G}_S$. Nous allons voir que, sous les hypothèses du théorème 2.3, l'application obtenue est un isomorphisme.

Nous aurons besoin pour cela du résultat technique suivant :

Lemme 3.1. *Soient $\varphi : \mathcal{H} \to \mathcal{G}$ un morphisme de pro-p-groupes, et $\varphi^{\mathrm{ab}} : \mathcal{H}^{\mathrm{ab}} \to \mathcal{G}^{\mathrm{ab}}$ l'abélianisé de φ. Sous la condition $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 1$, il est équivalent d'affirmer que φ ou φ^{ab} est un isomorphisme.*

Preuve. Il est bien clair que φ^{ab} est un isomorphisme dès que φ en est un. Réciproquement, supposons que φ^{ab} est un isomorphisme et notons pour abréger $H^i(\cdot)$ au lieu de $H^i(\cdot, \mathbb{Q}_p/\mathbb{Z}_p)$. La suite exacte d'inflation-restriction construite à partir de la suite exacte courte

$$1 \longrightarrow Im\,\varphi \longrightarrow \mathcal{G} \longrightarrow \text{ Coker } \varphi \longrightarrow 1,$$

s'écrit

$$1 \longrightarrow H^1(\text{Coker } \varphi) \longrightarrow H^1(\mathcal{G}) \longrightarrow H^1(Im\,\varphi) \longrightarrow ...$$

Maintenant φ^{ab} étant surjective, l'application induite $H^1(\mathcal{G}) \to H^1(\mathcal{H})$ est injective, ce qui entraîne $H^1(\text{Coker } \varphi) = 1$, i.e. Coker $\varphi = 1$, et φ est bien surjective.

Cela étant, la suite exacte d'inflation- restriction conduite à partir de la suite courte

$$1 \longrightarrow \text{Ker } \varphi \longrightarrow \mathcal{H} \longrightarrow \mathcal{G} \longrightarrow 1$$

s'écrit :

$$1 \longrightarrow H^1(\mathcal{G}) \xrightarrow{\sim} H^1(\mathcal{H}) \longrightarrow H^1(\mathrm{Ker}\ \varphi)^{\mathcal{G}} \longrightarrow H^2(\mathcal{G}) = 1$$

et le terme de droite est nul par hypothèse. Il vient donc $H^1(\mathrm{Ker}\ \varphi)^{\mathcal{G}} = 1$, i.e. $H^1(\mathrm{Ker}\ \varphi) = 1$ (puisque $\mathcal{G}$ est un pro-p-groupe opérant sur le p-groupe discret $H^1(\mathrm{Ker}\ \varphi)$), c'est-à-dire finalement $\mathrm{Ker}\ \varphi = 1$, comme attendu.

Théorème 3.2. *Soient K un corps p-rationnel, et S un ensemble p-primitif maximal de places modérées du corps K. L'application ψ_S définie sur le produit libre $\circledast_{\mathfrak{l}\in S}\mathcal{G}_{\mathfrak{l}}$ des groupes de Galois respectifs $\mathcal{G}_{\mathfrak{l}}$ des pro-p-extensions maximales des complétés $\mathfrak{l}$-adiques de K aux places de S (par le choix d'une place $\mathfrak{L}$ de M_S au-dessus de $\mathfrak{l}$ pour tout $\mathfrak{l}$ de S), à valeurs dans le groupe de Galois $\mathcal{G}_S$ de la pro-p-extension S-modérément ramifiée ∞-décomposée maximale M_S de K, est un isomorphisme :*

$$\mathcal{G}_S = \mathrm{Gal}(M_S/K) \simeq \circledast_{\mathfrak{l}\in S}\mathcal{G}_L = \circledast_{\mathfrak{l}\in S}\,\mathrm{Gal}(M_L/K_L)$$

Inversement, si pour un ensemble S de $c+1$ places modérées d'un corps de nombres K, le groupe $\mathcal{G}_S$ admet une décomposition du type précédent, le corps K est p-rationnel, et l'ensemble S p-primitif maximal.

Ce théorème résout complètement le problème de la description explicite de $\mathcal{G}_S$ (sous les hypothèses de p-rationalité et de p-primitivité), puisque la structure des groupes locaux $\mathcal{G}_{\mathfrak{l}}$ est parfaitement connue pour les places modérées (cf. [K]) :

Scolie 3.3. *Le groupe de Galois $\mathcal{G}_{\mathfrak{l}} = \mathrm{Gal}(M_{\mathfrak{L}}/K_{\mathfrak{l}})$ de la pro-p-extension maximale du complété d'un corps de nombres en une place finie étrangère à p est :*

- soit le pro-p-groupe libre $\tau_{\mathfrak{l}}^{\mathbb{Z}_p}$ engendré par le Frobenius, lorsque le p-sous-groupe de Sylow $\mu_{\mathfrak{l}}$ de $K_{\mathfrak{l}}^{\times}$ est trivial (i.e. lorsqu'on a $N\mathfrak{l} \not\equiv 1 \mod p$) ;

- soit le groupe de Demuškin $< \sigma_{\mathfrak{l}}, \tau_L \mid \tau_{\mathfrak{l}}^{N\mathfrak{l}-1}[\sigma_{\mathfrak{l}}, \tau_1\mathfrak{l}] = 1 >$ construit sur un relèvement quelconque $\sigma_{\mathfrak{l}}$ du Frobenius de la sous-extension non-ramifiée maximale de $M_{\mathfrak{L}}$, et un progénérateur quelconque $\tau_{\mathfrak{l}}$ du sous-groupe d'inertie de $M_{\mathfrak{L}}/K_{\mathfrak{l}}$, dans le cas contraire.

Preuve du Théorème. Le corps K étant p-rationnel par hypothèse, il satisfait en particulier la conjecture de Leopoldt et nous avons donc $H^2(\mathcal{G}_S, \mathbb{Q}_p/\mathbb{Z}_p) = 1$, ce qui est la traduction cohomologique de cette conjecture. Cela étant, le théorème 2.3 affirmant que l'abélianisée ψ_S^{ab} est un isomorphisme lorsque l'ensemble S est p-primitif maximal, le lemme 1 nous dit qu'il en est de même de ψ_S. La réciproque est immédiate.

Remarque. Le théorème de structure précédent peut être regardé comme un analogue en théorie des nombres du théorème d'existence de Riemann, les corps p-rationnels venant remplacer ceux de genre nul. On sait en effet, par la théorie des revêtements, que si k est un corps algébriquement clos de caractéristique nulle, et S un ensemble fini de places du corps des fractions rationnelles $K = k(x)$, autrement dit un ensemble fini $\{P_0, P_1, \cdots, P_S\}$ de points de $\mathbb{P}^1(k)$, le groupe de Galois $\mathcal{G}_S$ de l'extension algébrique S-ramifiée maximale de K, qui s'identifie au groupe fondamental algébrique $\pi^1(\mathbb{P}^1(k) \setminus S)$, est le produit libre profini

$$\mathcal{G}_S \simeq \circledast_{P\in\{P_1,\cdots,P_S\}} I_P$$

des groupes d'inertie (isomorphes à $\hat{\mathbb{Z}}$) des places de S, après l'élimination arbitraire de l'une d'elles.

Corollaire 3.4. *Soient K p-rationnel, et S p-primitif de cardinal $s \leq c+1$. Alors le groupe de Galois $\mathcal{G}_S$ de la pro-p-extension S-modérément-ramifiée ∞-décomposée maximale de K s'écrit comme produit libre*

$$\mathcal{G}_S \simeq (\circledast_{\mathfrak{l}\in S}\mathcal{G}_L)\circledast\mathcal{H}$$

des groupes de Galois locaux attachés aux places de S et d'un pro-p-groupe libre sur $1 + c - s$ générateurs.

Preuve. Il suffit de compléter S en un ensemble primitif maximal S', puis d'appliquer le théorème, en remarquant que $\mathcal{G}_S$ est le quotient de $\mathcal{G}_{S'}$ par le sous-groupe $\circledast_{\mathfrak{l}\in S'\setminus S}\ \mathcal{I}_{\mathfrak{l}}$ engendré par les sous-groupes d'inertie des places excédentaires.

Nous pouvons désormais procéder à la montée. Convenons de dire qu'une p-extension ∞-décomposée L/K est primitivement ramifiée lorsque l'ensemble $R_{L/K}$ des places modérément ramifiées dans L/K est p-primitif dans K. Cela posé, nous avons :

Théorème 3.5. *Étant donné une p-extension (finie) de corps de nombres, les deux conditions suivantes sont équivalentes :*
(i) Le corps L est p-rationnel.
(ii) Le corps K est p-rationnel, et l'extension L/K primitivement ramifiée.

Preuve. Nous allons procéder différemment pour la descente et la montée.

(i) $\Longrightarrow$ (ii) Pour la descente, remarquons simplement que si L est p-rationnel, il satisfait en particulier à la conjecture de Leopoldt ainsi que tous ses sous-corps, de sorte que tout revient à établir que le sous-groupe de torsion $\mathcal{T}_K$ est nul et que l'extension L/K est primitivement ramifiée, dés lors que $\mathcal{T}_L$ est nul. Or cela résulte immédiatement de la formule de points fixes de Gras (cf. [2]), où G désigne le groupe $\mathrm{Gal}(L/K)$, et $\mathcal{D}'$ le groupe des p-diviseurs :

$$|\mathcal{T}_L^G| = |\mathcal{T}_K| \frac{(\mathcal{D}_L'^G \ \ \mathcal{D}'_K)}{(\log \mathcal{D}_L'^G \ \ \log \mathcal{D}'_K)}$$

(ii) $\Longrightarrow$ (i) Pour la montée, la formule précédente n'est pas utilisable directement, puisque le corps L ne vérifie pas a priori la conjecture de Leopoldt. Complétons donc l'ensemble $R_{L/K}$ des places modérément ramifiées dans L/K en un ensemble p-primitif maximal S_K du corps p-rationnel K et introduisons la pro-p-extension S-modérément ramifiée ∞-décomposée maximale M_S de K. Le corps M_S contient L par construction ; c'est donc aussi la pro-p-extension S-modérément ramifiée ∞-décomposée maximale de L. En particulier, le pro-p-groupe $\mathcal{G}_S(L) = \mathrm{Gal}(M_S/L)$ est donc un sous-groupe ouvert du pro-p-groupe $\mathcal{G}_S(K) = \mathrm{Gal}(M_S/K)$. Maintenant, par le théorème 3.2, le groupe $\mathcal{G}_S(K)$ s'identifie au produit libre :

$$\mathcal{G}_S(K) \simeq \circledast_{\mathfrak{l}\in S_K} \mathcal{G}_{\mathfrak{l}}(K)$$

et le théorème de Binz-Neukirch-Wenzel (cf. [1]) nous assure que le sous-groupe $\mathcal{G}_S(L)$ s'identifie par conséquent au produit libre :

$$\mathcal{G}_S(L) \simeq (\circledast_{\mathfrak{L}\in S_L} \mathcal{G}_{\mathfrak{L}}(L)) \circledast \mathcal{H}\ ,$$

où $\mathfrak{L}$ parcourt les places de L au-dessus de S_K et $\mathcal{H}$ désigne un pro-p-groupe libre de rang $n = \sum_{\mathfrak{L}\in S_L}([L_{\mathfrak{L}} : K_{\mathfrak{l}}] - 1) - ([L : K] - 1)$. Prenant l'abélianisé $\mathcal{G}_S^{\mathrm{ab}}(L)$ et appliquant le corollaire 2.4, nous concluons que L est p-rationnel, comme attendu, et que l'ensemble S_L est p-primitif dans L. Ainsi :

Corollaire 3.6. *Dans une p-extension primitivement ramifiée L/K d'un corps p-rationnel, l'ensemble S des places modérément ramifiées est encore p-primitif dans L.*

Remarques.

(i) L'implication de montée a été obtenue par Miki à partir de la caractérisation (iv) du théorème 1.2. Sa démonstration très technique est malheureusement assez peu éclairante (cf. [9]).

(ii) Ultérieurement, Miki et Sato (cf. [12]) ont donné une autre démonstration du théorème de montée, en décrivant la structure du groupe de Galois Gal (Z_L/L) de la composée des $\mathbb{Z}_p$-extensions de L comme module sur l'algèbre $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$ dans le cas particulier où l'extension L/K est cyclique d'ordre p. Pour passer ensuite au cas général, il est nécessaire de vérifier que si L/K est primitivement ramifiée, l'ensemble des places modérément ramifiées dans L/K est encore primitif dans L (i.e. le corollaire 3.6 ci-dessus), ce que la méthode ne donne pas.

(iii) Dans [GJ], l'implication de montée pour la p-régularité est ramenée au cas abélien à l'aide de la théorie des genres ; elle est alors démontrée par la théorie p-adique du corps de classes, via la caractérisation (v) du théorème 1.2.

Corollaire 3.7. *Toute p-extension primitivement ramifiée L d'un corps p-rationnel est un corps p-rationnel qui vérifie la conjecture de Leopoldt (pour le nombre premier p). Si L contient les racines p-ièmes de l'unité, il vérifie en outre la conjecture de Gross-Kuz'min.*

En effet, tout corps p-rationnel vérifie la conjecture de Leopoldt ; tout corps p-régulier, celle de Gross-Kuz'min, dès lors qu'il contient ζ_p. En fait, comme expliqué dans [6], la nullité de le p-partie du noyau hilbertien $H_2(L)$ suffit alors à entraîner ces deux conjectures.

4 Lois de réciprocité primitives

Nous supposons désormais que K est un corps p-rationnel contenant les racines p-ièmes de l'unité, et S un ensemble p-primitif maximal de places modérées de K.

Comme expliqué au début de cet article (cf. Proposition 1.1) K est alors un corps p-régulier, ce qui signifie que tout symbole sur K à valeurs dans un p-groupe s'exprime comme produit (éventuellement infini) des symboles réguliers attachés aux places non complexes de K. Par exemple, puisque K possède une unique place $\mathfrak{p}$ au-dessus de p (cf. condition (v,a) du Théorème 1.2), le p-symbole de Hilbert attaché à $\mathfrak{p}$ (à valeurs dans le p-groupe μ_p des racines de l'unité dans $\mathcal{K}_p^\times$) est donné par la formule du produit

$$\left(\frac{\,.\,,\,.\,}{\mathfrak{p}}\right)^{-1} = \prod_{\mathfrak{l}\neq\mathfrak{p}} (\,.\,,\,.\,)_{\mathfrak{l}}^{p^{m_{\mathfrak{l}}-m}}$$

où $p^{m_{\mathfrak{l}}}$ désigne l'ordre du p-groupe local $\mu_{\mathfrak{l}}$, et p^m celui du p-groupe global, l'égalité $m = m_{\mathfrak{p}}$ résultant des hypothèses faites, puisque l'extension cyclotomique $K[\zeta_{p^{m+1}}]/K$ ne peut se décomposer en p (toujours d'après la condition (v,a) du théoréme 1.2).

Nous nous proposons ici de déterminer une loi de réciprocité explicite pour le symbole sauvage $\left(\frac{\,.\,,\,.\,}{\mathfrak{p}}\right)$ ne mettant en jeu qu'un nombre fini de symboles modérés. Le cas $p = 2$ faisant intervenir les symboles réguliers attachés aux places réelles, nous aurons besoin pour cela d'un résultat légèrement plus général que le théorème 2.3, que nous allons maintenant établir :

Théorème 4.1. *Soient K un corps p-rationnel et S un ensemble p-primitif maximal de places modérées de K. Alors, dans la correspondance du corps de classes, le groupe de galois $\mathcal{G}^{\mathrm{ab}}_{S\infty}$ de la pro-p-extension abélienne S-modérément ramifiée maximale $M^{\mathrm{ab}}_{S\infty}$ de K (i.e. de la composée des p-extensions abéliennes de K qui sont non ramifiées (aux places finies) en dehors de S et de p) est donné par l'isomorphisme :*

$$\mathcal{G}^{\mathrm{ab}}_{S\infty} = \mathrm{Gal}(M^{\mathrm{ab}}_{S\infty}/K) \simeq \prod_{\mathfrak{l}\in S\infty} \mathcal{R}_{\mathfrak{l}}.$$

C'est donc le produit direct des sous-groupes de décomposition des r places réelles et des $c+1$ places de S.

Preuve. La p-extension abélienne p-ramifiée $S\infty$-décomposée maximale de K étant triviale par hypothèse, un calcul direct donne :

$$\mathcal{G}^{\mathrm{ab}}_{S\infty} \simeq \mathcal{J}/\prod_{\mathfrak{l}\notin Sp} \mathcal{U}_p\,\mathcal{R} \simeq \prod_{\mathfrak{l}\in S\infty} \mathcal{R}_{\mathfrak{l}}/\left(\prod_{\mathfrak{l}\in S\infty} \mathcal{R}_{\mathfrak{l}} \cap \mathcal{R} \prod_{\mathfrak{l}\notin S\infty p} \mu_{\mathfrak{l}}\right)$$

et tout le problème consiste à vérifier que le dénominateur est nul. Or cela résulte par exemple du théorème 2.3, puisque les idèles principaux qui interviennent sont des S-unités infinitésimales (i.e. des éléments du tensorisé $\mathcal{E}_S = \mathbb{Z}_p \otimes_{\mathbb{Z}} E_S$ d'image 1 dans le facteur $\mathcal{R}_p = \prod_{\mathfrak{p}|p} \mathcal{R}_{\mathfrak{p}}$).

Corollaire 4.2 (Épimorphisme de dualité)**.** *Conservons les hypothèses du théorème et supposons en outre que le corps K contient les racines p-ièmes de l'unité. Alors l'application canonique*

$$\mathcal{E}'_S \to \mathcal{R}_{S\infty} = \prod_{\mathfrak{l}\in S\infty} \mathcal{R}_\mathfrak{l}$$

du tensorisé p-adique $\mathcal{E}'_S = \mathbb{Z}_p \otimes_\mathbb{Z} E'_S$ du groupe des Sp-unités (au sens ordinaire) de K dans le produit des complétés profinis $\mathcal{R}_\mathfrak{l}$, pour $\mathfrak{l} \in S\infty$, induite par le prolongement diagonal du groupe multiplicatif de K dans le produit de ceux de ses complétés aux places réelles ou contenues dans S est un épimorphisme.

Preuve. Comme le corps K contient les racines p-ièmes de l'unité, l'isomorphisme galoisien du théorème 1, transporté par la théorie de Kummer, montre que le radical $\mathrm{Rad}(M^{\text{él}}_{S\infty}/K)$ de la p-extension abélienne élémentaire S-modérément ramifiée maximale de K s'identifie au produit des radicaux locaux $\mathrm{Rad}(M^{\text{él}}_\mathfrak{l}/K_\mathfrak{l})$, pour $\mathfrak{l} \in S\infty$; ce qui s'écrit :

$$\mathcal{E}'_S/\mathcal{E}'^{\,p}_S \simeq \prod_{\mathfrak{l}\in S\infty} \mathcal{R}_\mathfrak{l}/\mathcal{R}^p_\mathfrak{l}.$$

D'après le lemme de Nakayama, cela suffit à établir que l'application naturelle

$$\mathcal{E}'_S \to \prod_{\mathfrak{l}\in S\infty} \mathcal{R}_\mathfrak{l}$$

est un épimorphisme. Bien entendu, ce n'est pas (en général) un isomorphisme, la source et l'arrivée n'étant pas des $\mathbb{Z}_p$-module de même rang.

Il est alors commode de réunir le théorème 2.3 et le corollaire 2 ci-dessus dans un même énoncé sous la forme :

Corollaire 4.3 (lemme d'approximation simultanée par les S-unités)**.** *Sous les hypothèses précédentes, les injections diagonales $E'_S \hookrightarrow K^\times_\mathfrak{p}$ et $E'_S \hookrightarrow \prod_{\mathfrak{l}\in S\infty} K^\times_\mathfrak{l}$ induisent les isomorphismes canoniques*

$$K^\times_p/K^{\times p^m}_p \quad \simeq \quad E'_S/E'^{p^m}_S \quad \simeq \quad K^\times_{S\infty}/K^{\times p^m}_{S\infty} \simeq \prod_{\mathfrak{l}\in S\infty} K^\times_\mathfrak{l}/K^{\times p^m}_\mathfrak{l},$$

où p^m est l'ordre du p-groupe μ_K des racines de l'unité dans K.

Cela étant, nous pouvons énoncer (en accord avec [15]) :

Théorème 4.4 (Loi de réciprocité primitive)**.** *Soient K un corps p-régulier contenant les racines p-ièmes de l'unité et $\mathfrak{p}$ l'unique place de K au-dessus de p. Alors, pour tout ensemble p-primitif maximal S de places modérées de K, les quotients*

$$K^\times_p/K^{\times p^m}_p \qquad \& \qquad K^\times_{S\infty}/K^{\times p^m}_{S\infty} \simeq \prod_{\mathfrak{l}\in S\infty} K^\times_\mathfrak{l}/K^{\times p^m}_\mathfrak{l}$$

où p^m est l'ordre du p-groupe μ des racines de l'unité dans K, sont naturellement anti-isométriques pour la structure (symplectique pour $p \neq 2$) donnée par les symboles de Hilbert.

Preuve. Il s'agit d'établir qu'il existe un isomorphisme canonique φ_S du quotient $K^\times_\mathfrak{p}/K^{\times p^m}_\mathfrak{p}$ sur le quotient $K^\times_{S\infty}/K^{\times p^m}_{S\infty}$, tel qu'on ait l'identité entre les symboles de Hilbert à valeurs dans μ :

$$\left(\frac{a, b}{\mathfrak{p}}\right) = \prod_{\mathfrak{l}\in S\infty} \left(\frac{\varphi_S(a), \varphi_S(b)}{\mathfrak{l}}\right) = \prod_{\mathfrak{l}\in S\infty} (\varphi_S(a), \varphi_S(b))_\mathfrak{l}$$

Or cela résulte immédiatement du lemme d'approximation simultanée par les S-unités ci-dessus et de la formule du produit rappelée plus haut, compte tenu de l'identité $m_\mathfrak{l} = m$, pour $\mathfrak{l} \in S$.

Remarques. Précisons quelques points en liaison avec la parité.

— Lorsque p^m est différent de 2, le corps K n'admet pas de plongement réel, et le quotient $E'_S/E'^{p^m}_S \simeq K^\times_S/K^{\times p^m}_S$ est alors un $\mathbb{Z}/p^m\mathbb{Z}$-module libre de dimension $2(c+1)$.

 — Si p est impair, les symboles de Hilbert à valeurs dans μ en font un module symplectique non dégénéré et il est facile de voir que le quotient E'/E'^{p^m}, construit sur les p-unités, est un sous-module totalement isotrope maximal (de dimension $c+1$). On obtient alors un supplémentaire totalement isotrope en faisant choix pour chaque $\mathfrak{l}$ dans S d'une uniformisante locale $\pi_\mathfrak{l}$ (que l'on regarde dans E'_S) et en formant le sous-module engendré par les $\pi_\mathfrak{l}$. Via la théorie de Kummer, cela revient à prendre le radical attaché à la sous-extension d'exposant p^m de l'extension abélienne K^{ab}_S/K donnée par le corollaire 2.5.

 — Si p vaut 2, le quotient $K^\times_S/K^{\times p^m}_S$ n'est plus un module symplectique : Le sous-groupe $\mu_S/\mu^{p^m}_S$ engendré par les racines locales de l'unité est toujours un sous-module totalement isotrope maximal ; mais il n'admet plus de supplémentaire isotrope puisque, pour toute uniformisante $\pi_\mathfrak{l}$, on a $(\pi_\mathfrak{l},\pi_\mathfrak{l})_\mathfrak{l} = -1$ par un calcul immédiat.

— Enfin, lorsque p^m vaut 2, le quotient E'_S/E'^2_S est un $\mathbb{F}_2$-espace quadratique de dimension $r+2(c+1)$, où r est le nombre de places réelles de K, qui admet comme sous-espace totalement isotrope maximal le quotient E'_+/E'^2_+ de dimension $c+1$, engendré par les p-unités totalement positives.

Références bibliographiques

[1] E. Binz, J. Neukirch & G.H. Wenzel, *A subgroup theorem for profinite groups*, J. of Algebra **19** (1971), 104–109.

[2] G. Gras, *Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres*, J. reine angew. Math. **333** (1982), 86–132.

[3] G. Gras, *Logarithme p-adique et groupes de Galois*, J. reine angew. Math. **343** (1982), 64–80.

[4] G. Gras, *Remarks on K_2 of numbers fields*, J. Numb. Th. **23** (1986), 322–335.

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

[6] J.-F. Jaulent, *Sur les conjectures de Leopoldt et de Gross*, Astérisque **147/148** (1987), 107–120.

[7] J.-F. Jaulent, *L'arithmétique des ℓ-extensions (Thèse d'État)*, Pub. Math. Fac. Sci. Besançon Théor. Nombres **1985/1986** (1986).

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

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

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

[11] 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.

[12] H. Miki & H. Sato, *Leopoldt's conjecture and Reiner's theorem*, J. Math. Soc. Japan. **36** (1984), 47–52.

[13] T. Nguyen Quang Do, *Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa*, Compositio Math. **46** (1982), 85–119.

[14] T. Nguyen Quang Do, *Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens*, Ann. Sci. Inst. Fourier **36** (1986), 27–46.

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

[16] I. R. Šafarevič, *Extensions with prescribed ramification points*, Pub. Math. I.H.E.S. **36** (1986), 71–95.

[17] J. Tate, *Sur la première démonstration par Gauss de la loi de réciprocité quadratique*, Colloque de Mathématiques Pures, Grenoble (1968).

Jean-François Jaulent
Université Bordeaux 1
Institut de Mathématiques
351, cours de la Libération
F-33405 TALENCE Cedex
jjaulent@u-bordeaux.fr

T. Nguyen Quang Do
UFR de Mathématiques
Université Paris VII
2, place Jussieu
F-75251 PARIS Cedex 05