Note sur les corps 2-rationnels

Jean-François Jaulent

Résumé. Nous déterminons le groupe de Galois de la pro-2-extension 2-ramifiée maximale d'un corps de nombres 2-rationnel.

Abstract. We compute the Galois group of the maximal 2-ramified pro-2-extension of a 2-rational number field.

Introduction

Les notions de corps ℓ-rationnel ou ℓ-régulier (pour un nombre premier ℓ) introduites idépendamment par A. Movahhedi et T. Nguyen Quang Do dans [11] d'une part, par G. Gras et l'auteur dans [3] d'autre part, se trouvent coïncider en présence des racines ℓ-ièmes de l'unité[1] donc, tout spécialement, pour $\ell = 2$.

- La ℓ-régularité se définit naturellement en termes de K-théorie et exprime simplement la trivialité du ℓ-noyau régulier du corps F considéré (*i.e.* du noyau dans la ℓ-partie du groupe universel $K_2(F)$ des symboles de Hilbert attachés aux places non complexes qui ne divisent pas ℓ).
- La ℓ-rationalité s'exprime en termes galoisiens et traduit la pro-ℓ-liberté du groupe de Galois $\mathcal{G}_F = \mathrm{Gal}(M_F/F)$ attaché à la pro-ℓ-extension (galoisienne) ℓ-ramifiée ∞-décomposée maximale M_F de F (*i.e.* au compositum des ℓ-extensions de F qui sont non ramifiées aux places finies[2] étrangères à ℓ et complètement décomposée aux places à l'infini).

Plus précisément, d'après [6] (Th.1.2), la ℓ-rationalité d'un corps de nombres K s'exprime comme suit :

Théorème & Définition 0. *Les conditions suivantes sont équivalentes :*

(i) Le groupe de Galois $\mathcal{G}_K = \mathrm{Gal}(M_K/K)$ de la pro-ℓ-extension ℓ-ramifiée ∞-décomposée maximale M_K de K est un pro-ℓ-groupe libre (sur $d_K = 1 + c_K$ générateurs, si c_K désigne le nombre de places complexes de K).

(ii) Le groupe de Galois $\mathcal{G}_K^{ab} = \mathrm{Gal}(M_K^{ab}/K)$ de la sous-extension abélienne maximale M_K^{ab}/K de M_K/K est un $\mathbb{Z}_\ell$-module libre de dimension $1 + c_K$.

(iii) Le corps K vérifie la conjecture de Leopoldt (pour le premier ℓ) et le sous-module de torsion $\mathcal{T}_K$ du groupe $\mathcal{G}_K^{ab} = \mathrm{Gal}(M_K^{ab}/K)$ est trivial.

(iv) Le groupe $V_K = \{x \in K^\times \mid x \in K_{\mathfrak{l}}^{\times\ell}\ \forall \mathfrak{l} \mid \ell \ \&\ v_{\mathfrak{p}}(x) \equiv 0 \mod \ell\ \ \forall \mathfrak{p} \nmid \ell\infty\}$ des éléments ℓ-hyperprimaires du corps K se réduit à $K^{\times\ell}$, et l'on a l'identité entre les ℓ-rangs des ℓ-groupes de racines de l'unité :

$$\mathrm{rg}_\ell\ \boldsymbol{\mu}_K = \textstyle\sum_{\mathfrak{l}\mid\ell} \mathrm{rg}_\ell\ \boldsymbol{\mu}_{K_{\mathfrak{l}}}.$$

[1] En fait dès que le corps F considéré contient le sous-corps réel $\mathbb{Q}[\zeta_\ell + \bar{\zeta}_\ell]$ du corps $\mathbb{Q}[\zeta_\ell]$.

[2] En accord avec les conventions de la Théorie ℓ-adique du Corps de Classes (*cf.* [2, 5]), nous ne parlons jamais de ramification à l'infini, mais de *complexification* des places réelles.

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

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

*(b) ou bien K ne contient pas ζ, auquel cas les places de K au-dessus de ℓ ne se décomposent pas complètement dans l'extension cyclotomique $K[\zeta]/K$ et la ω-composante du ℓ-groupe des ℓ-classes d'idéaux au sens restreint $\mathcal{C}\ell'_{K[\zeta]}$ du corps $K[\zeta]$ est triviale, si ω désigne le caractère cyclotomique (*i.e. *le caractère de l'action sur $\boldsymbol{\mu}_K$ de* $\mathrm{Gal}(K[\zeta]/K)$*).*

Lorsque ces conditions sont réunies, le corps K est dit ℓ-rationnel.

Remarque. Pour $\ell = 2$, il résulte clairement de la condition *(v,a)* ci-dessus qu'un corps 2-rationnel ne peut contenir qu'*une seule* place au-dessus de 2.

De fait les prémices de la notion de ℓ-régularité remontent aux travaux de G. Gras notamment à sa note sur le K_2 des corps de nombres [1], tandis que la notion de ℓ-rationalité apparait (sous une forme cachée) dans les travaux de H. Miki [10], à l'occasion de l'étude d'une condition suffisante de la conjecture de Leopoldt, ainsi que dans ceux de K. Wingberg [14, 15], où est étudiée la même condition.

Les articles [3, 11] cités plus haut en caractérisent complètement la propagation (dans une ℓ-extension) en termes de primitivité de la ramification, ce que les approches antérieures ne donnaient pas. Une synthèse de leurs résultats est présentée dans [6] et un exposé systématique en est donné dans le livre de G. Gras [2].

Diverses généralisations de ces notions ont été étudiées par O. Sauzet et l'auteur (*cf.* [7, 8]), notamment dans le cas $\ell = 2$ qui se révèle, comme à l'ordinaire, le plus compliqué ; elles donnent naissance, en particulier, à la notion de corps 2-birationnel.

Tout récemment, J. Jossey [9] a jugé bon d'introduire une notion de corps ℓ-rationnel qui diffère de celles déjà utilisée (en fait pour $\ell = 2$, dès lors que le corps de nombres considéré posssède des plongements réels), ce qui parait doublement malheureux, car s'écartant de l'usage établi et ne s'appliquant pas au corps *des* rationnels $\mathbb{Q}$.

Pour ces raisons, afin de prévenir toute confusion, il nous semble plus judicieux de parler dans son contexte de corps *2-surrationnel*. Précisons ce point :

Définition 1. *Soient K un corps de nombres ayant r_K places réelles et c_K places complexes, ℓ un nombre premier, M'_K la pro-ℓ-extension maximale de K qui est 2-ramifiée (*i.e. *non ramifiée aux places (finies) étrangères à ℓ) et M_K la sous-extension maximale de M'_K qui est complètement décomposée aux places à l'infini. Nous disons que le corps K est :*

(i) ℓ-surrationnel, lorsque le groupe $\mathcal{G}'_K = \mathrm{Gal}(M'_K/K)$ est pro-ℓ-libre ;

(ii) ℓ-rationnel, lorsque son quotient $\mathcal{G}_K = \mathrm{Gal}(M_K/K)$ est pro-ℓ-libre.

On voit alors que les deux notions coïncident, sauf précisément dans le cas où ℓ vaut 2 et où le corps K possède une ou plusieurs places réelles se complexifiant dans M'_K : ainsi tout corps ℓ-surrationnel est-il évidemment ℓ-rationnel, mais la réciproque n'est pas vraie en présence de complexification.

Le but de cette note est de déterminer la structure du groupe $\mathcal{G}'_K$ dans le cas exceptionnel où le corps considéré K est 2-rationnel mais non 2-surrationnel.

Théorème principal : description du groupe $\mathcal{G}'_K$

Notre résultat est extrèmement simple, qui s'énonce comme suit :

Théorème 2. *Soit K un corps de nombres 2-rationnel possédant $r_K \geq 1$ places réelles et c_K places complexes. Le groupe de Galois $\mathcal{G}'_K = \mathrm{Gal}(M'_K/K)$ de la pro-2-extension 2-ramifiée maximale M'_K de K est alors le pro-2-produit libre*

$$\mathcal{G}'_K \;\simeq\; \mathbb{Z}_2^{\circledast\, c_K} \circledast (\mathbb{Z}_2 \times C_2) \;\circledast\; C_2^{\circledast(r_K-1)}$$

de c_K exemplaires du groupe procyclique $\mathbb{Z}_2$, d'un exemplaire du produit direct $\mathbb{Z}_2 \times C_2$ et de $(r_K - 1)$ exemplaires du groupe cyclique C_2.

Corollaire 3. *Les corps de nombres 2-rationnels qui sont 2-surrationnels sont ceux totalement imaginaires.*

Preuve du Théorème. Si le corps 2-rationnel K considéré n'admet pas de plongement réel, *i.e.* dans le cas $r_K = 0$, il est alors 2-surrationnel ; et le groupe $\mathcal{G}'_K = \mathcal{G}_K$ est alors pro-2-libre sur $d_K = c_K + 1$ générateurs, comme annoncé.

Sinon, *i.e.* dans le cas $r_K > 0$, introduisons l'extension quadratique $L = K[i]$ engendrée par les racines 4^{es} de l'unité. Elle est évidemment 2-ramifiée sur K donc, en vertu des théorèmes de propagation de [3, 11] (*cf. e.g.* [6], Th. 3.5), 2-rationnelle ; et finalement 2-surrationnelle, puisque totalement imaginaire. En d'autres termes, le groupe de Galois $\mathcal{G}_L = \mathcal{G}'_L$ de la pro-2-extension 2-ramifiée maximale M_L de L est pro-2-libre :

$$\mathcal{G}_L \;\simeq\; \mathbb{Z}_2^{\circledast\, d_L}, \quad \text{avec} \quad d_L = c_L + 1 = r_K + 2c_K + 1.$$

Cela étant, comme l'extension quadratique L/K est 2-ramifiée, M_L est aussi la plus grande pro-2-extension M'_K de K qui est 2-ramifiée et le groupe de Galois $\mathcal{G}'_K$ est ainsi *potentiellement libre*, puisqu'il contient un sous-groupe ouvert qui est pro-2-libre, à savoir $\mathcal{G}_L$, lequel est d'indice 2 dans $\mathcal{G}'_K$.

Plus précisément, les résultats de structure de W. Herfort et P. Zalesskii (*cf.* [4], Th. 0.2) assurent qu'il existe alors une famille finie $(\mathcal{F}_i)_{i=0,\cdots,k}$ de pro-2-groupes libres sur respectivement $d_0, \cdots, d_k$ générateurs, où k dénombre les classes de conjugaisons de sous-groupes d'ordre 2 de $\mathcal{G}'_K$, tels qu'on ait :

$$\mathcal{G}'_K \;\simeq\; \mathcal{F}_0 \circledast \left(\mathop{\circledast}_{i=1}^{k} (C_2 \times \mathcal{F}_i) \right).$$

En particulier, l'abélianisé $\mathcal{G}'^{ab}_K$ de $\mathcal{G}'_K$ admet alors la décomposition directe :

$$\mathcal{G}'^{ab}_K \;\simeq\; \mathbb{Z}_2^{d_0} \oplus \left(\oplus_{i=1}^{k} (C_2 \oplus \mathbb{Z}_2^{d_i}) \right) \;\simeq\; \mathbb{Z}_2^{\sum d_i} \oplus C_2^k.$$

Et, puisque le corps 2-rationnel K vérifie la conjecture de Leopoldt, il vient :

$$\textstyle\sum_{i=0}^{k} d_i = d_K = c_K + 1\,; \text{ ainsi que l'isomorphisme : } \mathcal{T}'_K \simeq \mathcal{C}_2^k.$$

où $\mathcal{T}'_K$ désigne le sous-groupe de $\mathbb{Z}_2$-torsion du groupe $\mathcal{G}'^{ab}_K$.

Maintenant, il résulte clairement de la pro-2-décomposition de $\mathcal{G}'_K$ que les nombres minimaux de générateurs $d(\mathcal{G}'_K)$ et de relations $r(\mathcal{G}'_K)$ qui le définissent comme pro-2-groupe sont respectivement :

$$d(\mathcal{G}'_K) = k + \textstyle\sum_{i=0}^{k} d_i = k + c_K + 1 \;\text{ et }\; r(\mathcal{G}'_K) = \sum_{i=1}^{k}(1 + d_i) = d(\mathcal{G}'_K) - d_0.$$

Or les formules de Šafarevič (*cf.* [13], [2], § III.4, ou encore [12], Th. 8.7.3) :

$$\begin{aligned} d(\mathcal{G}'_K) &= \dim_{\mathbb{F}_\ell}(H^1(\mathcal{G}'_K,\mathbb{F}_\ell)) \\ &= c_K + 1 + \dim_{\mathbb{F}_\ell} V_K/K^{\times\ell} + (\sum_{\mathfrak{l}|\ell} \mathrm{rg}_\ell\, \boldsymbol{\mu}_{K_\mathfrak{l}} - \mathrm{rg}_\ell\, \boldsymbol{\mu}_K)\ ;\ \text{et} \end{aligned}$$

$$r(\mathcal{G}'_K) = \dim_{\mathbb{F}_\ell}(H^2(\mathcal{G}'_K,\mathbb{F}_\ell)) = \dim_{\mathbb{F}_\ell} V_K/K^{\times\ell} + (\sum_{\mathfrak{l}|\ell} \mathrm{rg}_\ell\, \boldsymbol{\mu}_{K_\mathfrak{l}} - \mathrm{rg}_\ell\, \boldsymbol{\mu}_K).$$

donnent ici, d'après la condition (v,a), pour $\ell = 2$ et K supposé 2-rationnel :

$$d(\mathcal{G}'_K) = \dim_{\mathbb{F}_2} {}^2\mathcal{G}'^{ab}_K = r_K + c_K + 1 \qquad \text{et} \qquad r(\mathcal{G}'_K) = \dim_{\mathbb{F}_2} {}^2\mathcal{T}'_K = r_K\ ;$$

d'où finalement : $k = r_K$ et $d_0 = c_K$; ce qui conduit bien au résultat attendu.

Références

[1] G. Gras, *Remaks on K_2 of number fields*, J. Numb. Th. **23** (1986), 64–80 .

[2] G. Gras, *Class Field Theory*, SMM (2003) ; second corrected printing (2005).

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

[4] W. Herfort & P. Zalesskii, *Finitely generated pro-2-groups with a free subgroup of index 2*, Manuscripta Math. **93** (1997), 457–464.

[5] J.-F. Jaulent, *Théorie ℓ-adique globale du corps de classes*, J. Théor. Nombres Bordeaux **10** (1998), 355–397.

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

[7] J.-F. Jaulent & O. Sauzet, *Pro-ℓ-extensions de corps de nombres $\mathfrak{l}$-rationnels*, J. Number Th. **65** (1997), 240–267 & **80** (2000), 318–319.

[8] J.-F. Jaulent & O. Sauzet, *Extensions quadratiques 2-birationnelles de corps totalelment réels*, Pub. Matemàtiques **44** (2000), 343–351.

[9] J. Jossey *Galois 2-extensions unramified outside 2,* J. Number Th. **124** (2007), 42–76.

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

[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] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of number fields,* Grund. der Math. Wissenschaften 323, Springer-Verlag, 2000.

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

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

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

Jean-François Jaulent
Institut de Mathématiques de Bordeaux
Université Bordeaux 1
351, cours de la libération
F-33405 Talence Cedex
courriel : Jean-Francois.Jaulent@math.u-bordeaux1.fr