

Publications mathématiques de Besançon

ALGÈBRE ET THÉORIE DES NOMBRES

Georges Gras

Sur le module de Bertrandias–Payan dans une p -extension – Noyau de capitulation

2016, p. 25-44.

http://pmb.cedram.org/item?id=PMB_2016____25_0

© Presses universitaires de Franche-Comté, 2016, tous droits réservés.

L'accès aux articles de la revue « Publications mathématiques de Besançon » (<http://pmb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://pmb.cedram.org/legal/>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

*Publication éditée par le laboratoire de mathématiques
de Besançon, UMR 6623 CNRS/UFC*

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>*

SUR LE MODULE DE BERTRANDIAS–PAYAN DANS UNE p -EXTENSION – NOYAU DE CAPITULATION

par

Georges Gras

Résumé. — Pour un corps de nombres K et un nombre premier p on désigne par BP_K le composé des p -extensions cycliques de K plongeables dans une p -extension cyclique de degré arbitrairement grand. L'extension BP_K/K est p -ramifiée et extension finie du composé K des Z_p -extensions de K . Le groupe $BP_K := \text{Gal}(BP_K/K)$ est appelé le *module de Bertrandias–Payan*. Nous étudions l'application transfert $j_{L/K} : BP_K \rightarrow BP_L$ (comme morphisme de capitulation de classes d'idéaux) dans une p -extension L/K . Dans le cas cyclique de degré p , nous prouvons que $j_{L/K}$ est injectif sauf si L/K est kummerienne, p -ramifiée, non globalement cyclotomique mais localement cyclotomique en p (théorème 3.1). Nous donnons une formule explicite (théorème 5.2) pour $|BP_L^G| \cdot |BP_K|^{-1}$ et montrons de quelle façon son intégralité dépend du groupe de torsion T_L du groupe de Galois de la pro- p -extension abélienne p -ramifiée maximale de L , en utilisant un logarithme p -adique convenable.

Abstract. — (On the Bertrandias–Payan module in a p -extension – Capitulation kernel) For a number field K and a prime number p we denote by BP_K the compositum of the cyclic p -extensions of K which are embeddable into a cyclic p -extension of arbitrary large degree. The extension BP_K/K is p -ramified and is a finite extension of the compositum K of the Z_p -extensions of K . The group $BP_K := \text{Gal}(BP_K/K)$ is called the *Bertrandias–Payan module*. We study the transfer map $j_{L/K} : BP_K \rightarrow BP_L$ (as a capitulation morphism of ideal classes) in a p -extension L/K . In the cyclic case of degree p , we prove that $j_{L/K}$ is injective except if L/K is kummerian, p -ramified, non globally cyclotomic but locally cyclotomic at p (Theorem 3.1). We give an explicit formula (Theorem 5.2) for $|BP_L^G| \cdot |BP_K|^{-1}$ and we show how its entirety depends on the torsion group T_L of the Galois group of the maximal abelian p -ramified pro- p -extension of L , by using a suitable p -adic logarithm.

Ce texte, bien que personnel, résulte d'un travail en lien étroit avec Jean–François Jaulent (Bordeaux) et Thong Nguyen Quang Do (Besançon). L'originalité de la démarche étant que trois techniques sont proposées (une par auteur) pour aborder le même sujet tout en développant des conséquences et applications différentes. Ceci nous a semblé nécessaire dans la mesure où toutes ces techniques sont issues de la théorie du corps de classes, mais ont été

Classification mathématique par sujets (2010). — 11R04, 11R11, 11R16.

Mots clefs. — Class field theory, p -ramification, Bertrandias–Payan module, capitulation of ideal classes, transfer map, Kummer theory.

formalisées di éremment (tant au plan des notions que des notations) selon les grands axes naturels du corps de classes (classes d'idéaux et d'idèles, corps de classes global p -adique et logarithmique, cohomologie galoisienne et théorie d'Iwasawa).

Ainsi le lecteur est-il invité à comparer ces méthodologies qui ont a priori le même potentiel de résultats, mais avec des avantages et inconvénients di érents selon le but recherché (allant du plus concret et numérique au plus abstrait et conceptuel), cette multiplicité étant souvent à l'origine de di cultés éditoriales d'antériorité (voir un historique au § 1.2).

Remerciements : je remercie mes deux partenaires pour les nombreux échanges constructifs que nous avons eus.

1. Généralités sur le module de Bertrandias–Payan

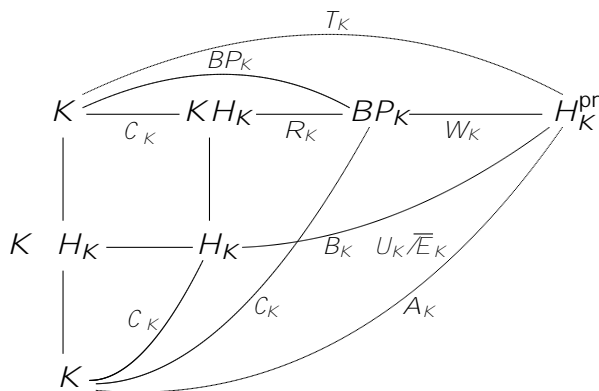
1.1. Le schéma de la p -ramification abélienne. — En raison de la commodité que confère un livre, on se référera le plus souvent à [Gr1] (2003) et notamment à l'édition Springer 2005, corrigée et augmentée, bien que de nombreuses références soient chaque fois concernées et seraient à citer (elles le sont dans le livre).

Soit K un corps de nombres et soit p un nombre premier. On considère le schéma ci-après ([Gr1], § III.2, (c), Fig. 2.2), au sens ordinaire de la notion de classes d'idéaux, dans lequel K est le composé des Z_p -extensions de K , H_K le p -corps de classes de Hilbert de K , H_K^{pr} la pro- p -extension abélienne p -ramifiée (i.e., non ramifiée en dehors de p) maximale de K .

Pour un corps k quelconque de caractéristique $= p$, on désigne par μ_k le groupe des racines p -ièmes de l'unité de k .

On désigne par $U_K := \prod_{v|p} U_v$ le Z_p -module des unités locales p -principales¹ pour K , où chaque U_v est le groupe des unités v -principales du complété K_v de K en v/p , par $W_K = \text{tor}_{Z_p} U_K = \prod_{v|p} \mu_{K_v}$, et par \bar{E}_K l'adhérence dans U_K de l'image diagonale du groupe des unités globales (p -principales) E_K de K . On suppose $p > 2$.

On pose $W_K = W_K / i_K(\mu_K) \quad \text{tor}_{Z_p} U_K / \bar{E}_K \quad T_K := \text{tor}_{Z_p}(\text{Gal}(H_K^{pr}/K))$ (inclusions valables sous la conjecture de Leopoldt pour p dans K), où i_K est l'injection diagonale :



¹D'une manière générale, dans un groupe de nombres algébriques, les éléments p -principaux sont ceux dont l'image résiduelle est égale à 1 en toute place v/p .

1.2. Historique de la p -ramification Abélienne. — Le p -groupe de torsion T_K joue un rôle capital dans toutes les questions de type *théorie du corps de classes* et plus précisément de type *théorie de la p -ramification abélienne* dans la mesure où il met en jeu de façon subtile le p -groupe des classes C_K et le régulateur p -adique des unités R_K , sous la conjecture de Leopoldt ; il est lié au groupe de Galois G_K de la pro- p -extension p -ramifiée (non complexifiée si $p = 2$) maximale de K via une relation de dualité de la forme $T_K \cong H^2(G_K, Z_p)$.

Il a été longuement étudié selon la chronologie approximative suivante :

[Kub] (1957), [Mi] (1978), [Gr2] (1982), [Gr3] (1983), [Ja1] (1983), [Ja2] (1984), [Gr4] (1985), [Gr5] (1986), [Ng1] (1986), [MoNg1] (1987), [He] (1988), [Ja3] (1990), [Th] (1993), [Ja4] (1998), [Seo1] (2011), [Seo2] (2013), [Seo3] (2013), [Gr6] (2014), [MoNg2] (2015), [Gr7] (2015), [Seo4] (2015), [Seo5] (2015), [Seo6] (2015), [Gre] (2015), [HM2] (2016).

Les sujets essentiels développés dans ce cadre sont les suivants, soit au niveau « fini » d'un corps de nombres, soit dans le cadre « infini » de la théorie d'Iwasawa :

(i) détermination du radical initial dans les Z_p -extensions lorsque $\mu_K = 1$, à savoir, trouver les nombres $K^\times / K^{\times p}$ tels que $K(\sqrt[p]{}) = K$, sachant que $\sqrt[p]{} \in K$ est tel que $\sqrt[p]{} = \alpha_0^p \cdot \alpha_p$, où α_0 est un idéal étranger à p et α_p un produit d'idéaux premiers au-dessus de p ([CK], [Gr4], [He], [MoNg2], [Th], [JaM1], [Seo1], [Seo2]) ;

(ii) étude des notions de p -rationalité et p -régularité, la p -rationalité de K étant la nullité de T_K sous la conjecture de Leopoldt, et la p -régularité celle du p -Sylow $R_2(K)$ du noyau (dans $K_2(K)$) des symboles réguliers ([Gr1], [Gr5], [GrJ],[Ja4], [JaNg], [Mo], [MoNg1]), ainsi que des cas particuliers de ces notions, notamment pour $p = 2$ (travaux de J.-F. Jaulent, F. Soriano–Gafiuk, O. Sauzet) ; également la notion de groupe des classes logarithmiques introduite et étudiée par J.-F. Jaulent et dont la finitude est équivalente à la conjecture de B. H. Gross ([Ja1], [Ja2], [Ja3], [Ja4], [Ja5], et une synthèse partielle dans [Gr1], § III.7) ;

(iii) généralisations de la notion de p -tours de corps de classes et structure du groupe de Galois de la pro- p -extension maximale d'un corps de nombres (e.g. [JaS], [JaM1], [JaM2], [Ha], [HM1], [Mai1], [Mai2], [Ng2], [Seo6], [HM2] et de nombreuses références depuis le livre de H. Koch [Ko], sans parler des nombreux travaux ultérieurs de N. Boston et de bien d'autres mathématiciens) ;

(iv) obtention de résultats numériques sur le radical initial, sur le groupe T_K , et sur la structure de $\text{Gal}(K^{\text{ab}}/K)$ où K^{ab} est la pro- p -extension abélienne maximale de K ([Cha], [He], [PV], [Th], [AS], [Gr6]) ;

(v) analyse d'aspects conjecturaux lorsque p (e.g. [Gr7] conjecturant la p -rationalité de tout corps de nombres pour p assez grand). Récemment, la notion de p -rationalité et ses propriétés ont été « redécouvertes » par certains auteurs et ont acquis une importance nouvelle en vue d'autres conjectures, dans le cadre des représentations Galoisienne (cf. [Gre]), ou de la notion d'invariant μ d'Iwasawa des pro- p groupes uniformes (cf. [HM2]).

Les techniques utilisées dans ces travaux sont de nature « classes d'idéaux » ou bien de nature « diviseurs », aux sens généralisés des infinitésimaux développés au début par G. Gras et J.-F. Jaulent et leurs élèves, ou encore de nature « cohomologie galoisienne et théorie d'Iwasawa » développée par T. Nguyen Quang Do et ses élèves, puis reprises plus récemment au moyen d'autres points de vue de type cohomologique, comme par exemple par S. Seo, souvent indépendamment des travaux précédents.

Dans [JaPMB], [NgPMB] et l'article présent, réunis dans ce volume des PMB, on trouvera des compléments et mises au point à ce sujet au moyen de l'étude du module de Bertrandias–Payan dans une p -extension de corps de nombres, étude qui se prête bien à l'utilisation systématique de ces techniques, les trois auteurs ayant conscience que ces trois approches similaires ont pâti jusqu'ici de l'absence de « table de concordance » détaillée, ce qui est sans doute à l'origine des difficultés d'analyse et de comparaison des publications.

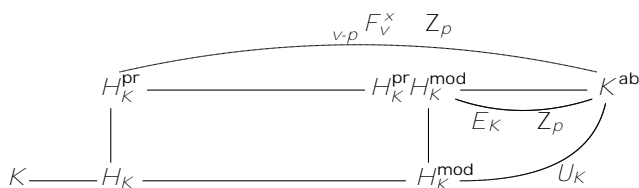
1.3. Le module de Bertrandias–Payan. — On sait que sous la conjecture de Leopoldt dans K (pour $p = 2$ en raison du « cas spécial », cf. [AT], Ch. X, Theorem 1, ou [Gr1], § II.6.3), $W_K = \text{tor}_{Z_p}(U_K/\bar{E}_K)$ fixe l'extension BP_K qui est la pro- p -extension maximale de K composée des p -extensions cycliques plongeables dans une p -extension cyclique de K de degré arbitrairement grand (cf. e.g. [Gr1], Corollary III.4.15.8) ; le groupe :

$$BP_K := \text{Gal}(BP_K/K) = T_K/W_K,$$

qui est le groupe de torsion du groupe $C_K = \text{Gal}(BP_K/K)$, est appelé depuis [Ng1] le module de Bertrandias–Payan à la suite de l'article [BP].

On a $BP_K = T_K$ pour tout p assez grand car $W_K = 1$ pour $p > 2$ suppose que $[K_v : \mathbb{Q}_p]$ est multiple de $p - 1$ pour au moins une place v/p , ce qui suppose $[K : \mathbb{Q}]$ assez grand.

Le corps BP_K est aussi le composé des p -extensions cycliques de K localement plongeables, en toute place finie v , dans une p -extension cyclique de K_v de degré arbitrairement grand (première preuve dans [AT], Ch. X, § 3, cf. [Gr1], remarque III.4.15.7 (ii)). Ceci est encore équivalent à la plongeabilité locale dans une Z_p -extension de K_v , pour toute place finie v ; pour cela on remarque que le p -groupe de torsion du groupe de Galois de la pro- p -extension Abélienne maximale de K_v est isomorphe à μ_{K_v} ; on peut aussi se reporter au schéma fondamental suivant (cf. [Gr1], § III.4.4.1) dans lequel toutes les extensions sont des pro- p -extensions, H_K^{mod} étant celle qui est modérée maximale et où F_v est le corps résiduel en v ; les projections dans $\text{Gal}(H_K^{\text{pr}}/K)$ de $\text{tor}_{Z_p}(E_K/Z_p) = \mu_K$ et de $\text{tor}_{Z_p}(U_K) = {}_{v/p}\mu_{K_v}$ conduisent au corollaire III.4.15.3 de [Gr1] sur le relèvement de W_K dans $\text{Gal}(K^{\text{ab}}/K)$:



De nombreux travaux, comme ceux mentionnés dans l'historique précédent, évoquent le rôle de BP dans la théorie du corps de classes, aussi nous souhaitons montrer ici que l'on dispose depuis longtemps des techniques permettant d'étudier les propriétés de ce module.

Soit S un ensemble fini de places de K contenant l'ensemble $S_p := \{v, v/p\}$ des p -places ; S sera choisi en fonction de l'extension L/K considérée et en particulier contiendra les places ramifiées dans L/K . Les résultats ne dépendront finalement que de S_p . Notre ensemble S jouera un rôle différent de celui utilisé dans [JaPMB] et [NgPMB].

On pose $K_1^x = K_1^x/Z_p$, où K_1^x est le groupe des éléments p -principaux de K^x étrangers à S , $I_K = I_K/Z_p$, où I_K est le groupe des idéaux de K étrangers à S , et $P_K = \{(x), x \in K_1^x\} = P_K/Z_p$, où $P_K = \{(x), x \in K_1^x\}$. On pose $E_K = E_K/Z_p$ (groupe des unités).

Soit i_K le plongement (surjectif) de K_1^\times dans $U_K = \prod_{v|p} U_v$ et soit K^\times le noyau de i_K (groupe des infinitésimaux étrangers à S de Jaulent, [Ja1], [Ja2], [Ja4]) ; on a facilement $i_K(E_K) = \overline{E}_K$. On désigne par P_K le groupe des idéaux principaux (x) , $x \in K^\times$.

On a alors ([Gr1], théorème III.2.4) :

$$A_K := \text{Gal}(H_K^{\text{pr}}/K) \quad I_K/P_K, \quad B_K := \text{Gal}(H_K^{\text{pr}}/H_K) \quad P_K/P_K, \quad T_K := \text{tor}_{Z_p} A_K.$$

Tous ces groupes de Galois sont des Z_p -modules de type fini.

Remarque 1.1. — De fait, la théorie du corps de classes définit $A_K = \text{Gal}(H_K^{\text{pr}}/K)$ de la façon suivante : on a $A_K = \varinjlim_n \text{Gal}(K^{(p^n)}/K) \varinjlim_n (I_K/P_{K,(p^n)}) \cong \varinjlim_n (I_K/P_{K,(p^n)})$, où $K^{(p^n)}$ est le p -corps de rayon modulo (p^n) , $P_{K,(p^n)} := \{(x), x \in K_1^\times, x \equiv 1 \pmod{p^n}\}$ et $P_{K,(p^n)} = P_{K,(p^n)} \cdot Z_p$; or on a $\varinjlim_n P_{K,(p^n)} = P_K$, ([Gr1], Proposition III.2.4.1).

Le fait de pouvoir travailler avec des groupes d'idéaux étrangers à S provient du théorème d'approximation idélique ou simplement du fait que toute classe d'idéaux contient un représentant étranger à S (e.g. [Gr1], théorème I.4.3.3 et remarque I.5.1.2). On a alors, avec des notations évidentes au niveau fini des corps de rayons :

$$\text{Gal}(K^{(p^n)}/K) \cong I_{K,S_p}/P_{K,S_p,(p^n)} \cong I_{K,S}/P_{K,S,(p^n)},$$

où les isomorphismes avec le groupe de Galois sont obtenus via le symbole d'Artin qui est par nature défini pour les idéaux de K étrangers à S_p , donc a fortiori étrangers à S .

On définit les mêmes objets relatifs à toute p -extension L de K en utilisant l'ensemble, noté encore S , des places de L au-dessus de S (de même pour S_p). Les objets ainsi obtenus par tensorisation avec Z_p se comportent comme les objets d'origine en raison de la platitude de Z_p . Nous commencerons par le cas L/K cyclique de degré p qui est en un sens universel et qui permet une plus grande efficacité quant au plan numérique.

On utilisera à plusieurs reprises les lemmes suivants pour un corps de nombres k (où l'on rappelle que i_k est à valeurs dans $U_k = \prod_{v|p} U_v$ et que les structures galoisiennes de U_k sont déduites du fait que l'image diagonale de k_1^\times y est dense) ; le lemme 1.4, particulièrement important, traduit de façon très arithmétique la conjecture de Leopoldt pour le corps k :

Lemme 1.2. — Soit k un corps de nombres vérifiant la conjecture de Leopoldt pour p . Soit $E_k := E_k \cdot Z_p$ telle que $i_k(\cdot)^{p^e} = 1$, $e \geq 0$ (i.e., $i_k(\cdot) \in W_k$). Alors μ_k et $p^e = 1$.

Démonstration. — Caractérisation très classique utilisant l'injectivité de i_k sur E_k sous la conjecture de Leopoldt ([Gr1], théorème III.3.6.2 (vi) et [Ja3], théorème 12).

Lemme 1.3. — Soit L/K cyclique de degré p et soit s un générateur de $G := \text{Gal}(L/K)$.

- (i) Si $\mu_K = 1$, alors $\mu_L = 1$ et $H^1(G, \mu_L) = 0$.
- (ii) Si $\mu_K = \mu_L^p = 1$ (i.e., L/K est extension cyclotomique globale de degré p), alors $N_{L/K}(\mu_L) = \mu_K$ et $\mu_L^{1-s} = 1$, où $1 - \mu_K$ est d'ordre p , d'où $H^1(G, \mu_L) = 0$.

Si $\mu_K = \mu_L = 1$, $N_{L/K}(\mu_L) = \mu_K^p$, $\mu_L^{1-s} = 1$, et $H^1(G, \mu_L) \cong Z/pZ$.

- (iii) Si $W_L \subset W_K$ vérifie $\mu_L^{1-s} = i_L(\cdot)$, où $i_L = i_L$, alors W_L est d'ordre 1 ou p .

On a $W_L^G = W_K$ et $W_L^p \subset W_K$.

Démonstration. — (i) Si $\mu_K = 1$ et si L contenait ζ_p d'ordre p , on aurait $K(\zeta_p) = L$ où $K(\zeta_p)/K$ serait de degré égal à un diviseur de $p - 1$ différent de 1 (absurde).

(ii) Ce point sur les racines de l'unité est classique (e.g. [Wa]).

(iii) Soit $L = W_L$. On a $\mathbb{Z}_p \subset W_K$ car si $w \in \mu_{L_w}$ est une composante de L telle que $w \in \mu_{K_v}$, alors, comme pour le cas global, $\mu_{K_v} = 1$, $[L_w : K_v] = p$, $\mathbb{Z}_p \subset \mu_{K_v}(\mathbb{O}_p(\mu_p))/\mathbb{O}_p$ a « même structure galoisienne » que $\mathbb{O}_p(\mu_p)/\mathbb{O}_p$ car p y est totalement ramifié.

Comme $W_L = \text{tor}_{\mathbb{Z}_p} U_L$ et que $U_L^G = U_K$, il en résulte que $W_L^G = \text{tor}_{\mathbb{Z}_p} U_K = W_K$.

Lemme 1.4. — *On a, sous la conjecture de Leopoldt pour p dans le corps de nombres k , la suite exacte $1 \rightarrow W_k/i_k(\mu_k) \rightarrow \text{tor}_{\mathbb{Z}_p} U_k/\overline{E}_k \xrightarrow{\log_k} R_k := \text{tor}_{\mathbb{Z}_p} \log_k(U_k)/\mathbb{Z}_p \log_k(E_k) \rightarrow 0$, où \log_k est le logarithme p -adique usuel ([Gr1], lemme III.4.2.4); R_k est appelé, par abus, le régulateur p -adique normalisé de k (l'écriture $\log_k(E_k)$ signifie $\log_k(i_k(E_k))$).*

Lemme 1.5. — *Soit L/K une p -extension cyclique et soit $y \in L^\times$ tel que $N_{L/K}(y) = 1$. Alors il existe $y \in L^\times$ tel que $y = y^{1-s}$ (Théorème de Hilbert–Speiser–Nøther dans L^\times).*

La preuve est donnée par exemple dans [Gr1] (preuve du lemme IV.3.1), et dans [Ja1].

2. Étude du « transfert » $j_{L/K} : C_K \rightarrow A_K/W_K \rightarrow C_L \rightarrow A_L/W_L$

2.1. Généralités. — Faisons un rappel sur le morphisme de transfert $A_K \rightarrow A_L$ en p -ramification Abélienne ([Gr1], Théorème IV.2.1) :

Lemme 2.1. — *Dans une extension L/K quelconque de corps de nombres, le morphisme de transfert $A_K \rightarrow A_L$ est injectif sous la conjecture de Leopoldt pour p dans la clôture galoisienne de L sur K . Il en résulte l'injectivité de $T_K = \text{tor}_{\mathbb{Z}_p} A_K \rightarrow T_L = \text{tor}_{\mathbb{Z}_p} A_L$.*

De fait, la première preuve de ce résultat a été donnée en 1982 dans [Gr2], théorème I.1, développée dans [Gr3], puis redonnée dans d'autres cadres techniques, comme dans [Ja1], [Ja2], [Ng1], et constitue une propriété classique, caractéristique de la conjecture de Leopoldt, qui pourrait simplifier considérablement l'approche de [Seo3], [Seo4], [Seo6].

On suppose désormais $p = 2$. On s'intéresse au noyau de l'application qui s'en déduit :

$$j_{L/K} : BP_K = \text{tor}_{\mathbb{Z}_p} C_K \longrightarrow BP_L = \text{tor}_{\mathbb{Z}_p} C_L$$

(définitions du § 1.1), dans une p -extension L/K , ultérieurement cyclique de degré p .

D'après le lemme 2.1 et la finitude de W_L , l'application $C_K \rightarrow C_L$ a même noyau (A_K étant de type fini, ce noyau est sous-groupe fini de C_K , donc de torsion). On peut alors travailler sur cette application plus simple notée encore $j_{L/K}$.

Son noyau est aussi un noyau de capitulation de classes d'idéaux puisque (relativement au choix de S défini au § 1.3) $A_K = I_K/P_K$, et $A_L = I_L/P_L$, sont des groupes de classes d'idéaux; aussi en raison de la méthode utilisée, nous parlerons pour $j_{L/K}$ de *morphisme de capitulation* et pour $\text{Ker}(j_{L/K})$ de *noyau de capitulation*, comme dans [JaPMB], [NgPMB].

2.2. Identification de W_K comme groupe de classes d'idéaux. — On a la suite exacte

$$1 \rightarrow K^\times/E_K/E_K \rightarrow K_1^\times/E_K \xrightarrow{i_K} U_K/\overline{E}_K \rightarrow 1$$

et les isomorphismes :

$$U_K/\overline{E}_K \cong K_1^\times/K^\times E_K \cong P_K/P_K, \quad \text{Gal}(H_K^{pr}/H_K).$$

L'isomorphisme $U_K/\overline{E}_K \cong P_K/P_K$, est donc ainsi défini : à partir de $u \in U_K$ on prend $x \in K_1^\times$ d'image u par i_K (x est défini modulo K^\times) et on considère la classe de l'idéal principal (x) modulo P_K , qui ne dépend pas du choix de x .

La surjectivité est évidente, et si u conduit à $(x) = (x') P_K$, on a $x = x' \kappa$, $\kappa \in E_K$, d'où $i_K(x) = u = i_K(\kappa) \overline{E}_K$. Inversement, à $(x) \in P_K$ on associe $i_K(x) \pmod{\overline{E}_K}$.

On suppose que la conjecture de Leopoldt est vérifiée dans toute extension L de K considérée :

Lemme 2.2. — (i) L'image de $W_K = W_K/i_K(\mu_K)$, dans P_K/P_K , est formée des classes modulo P_K des idéaux de P_K de la forme (x) , où $i_K(x) = \kappa \in W_K$, ce que l'on peut résumer par l'isomorphisme $W_K \cong \{(x), x \in K_1^\times, i_K(x) \in W_K\}/P_K$.

(ii) Le morphisme de capitulation $j_{L/K}$ est l'extension des « classes d'idéaux » :

$$I_K \{(x), x \in K_1^\times, i_K(x) \in W_K\} \rightarrow I_L \{(y), y \in L_1^\times, i_L(y) \in W_L\}.$$

Démonstration. — Le point (i) résulte de la définition de $U_K/\overline{E}_K \cong P_K/P_K$, appliquée au sous-groupe de torsion $W_K = \text{tor}_{Z_p} U_K/\overline{E}_K$ (sous la conjecture de Leopoldt, en utilisant les Lemmes 1.2, 1.4). Il en résulte que $C_K = A_K/W_K \cong I_K \{(x), x \in K_1^\times, i_K(x) \in W_K\}$, d'où le point (ii) du lemme.

2.3. Caractérisation du noyau de capitulation (cas cyclique de degré p). — Soit

$\mathfrak{a} \in I_K$ tel que par extension, $(\mathfrak{a})_L = (y)$ où $y \in L_1^\times$, avec $i_L(y) = \kappa \in W_L$ (Lemme 2.2 (ii)).

À partir de $(\mathfrak{a})_L = (y)$, la norme arithmétique $N_{L/K}$ conduit en idéaux à la relation $\mathfrak{a}^p = (N_{L/K}(y))$, ce qui donne la relation $y^p = N_{L/K}(y) \cdot \kappa$, $\kappa \in E_L$, ou encore la relation $i_L(y)^p = N_{L/K}(i_L(y)) \cdot i_L(\kappa)$ qui s'écrit par hypothèse $i_L(\kappa) = N_{L/K}(\kappa) \cdot i_L(\kappa)$; donc d'après le lemme 1.2 on a $i_L(\kappa) = \mu_L$; d'après le lemme 1.3, on a $i_L(\kappa) \in W_K$, par conséquent $i_L(\kappa) \in W_L^G = W_K$ et $i_L(\kappa) = \mu_K$.

Posons $a := N_{L/K}(y) \cdot \kappa \in K_1^\times$. On a donc la relation $a = y^p \cdot \kappa$ que l'on interprète de la façon suivante :

(i) Cas $y = x \in K_1^\times$. On a $i_L(y) = i_L(x) = \kappa \in W_L^G$, donc $i_L(x) = \mu_K$; comme $\mathfrak{a} = (x)$ dans K , ceci caractérise la trivialité de la classe de \mathfrak{a} dans C_K (Lemme 2.2).

(ii) Cas $y \notin K_1^\times$. Soit s un générateur de $G := \text{Gal}(L/K)$. Puisque $y^p = a \cdot \kappa$, on est nécessairement dans un cas kummerien où $y^s = \zeta y$, $\zeta \in \mu_K$ d'ordre p , et $L = K(\zeta)$, $\zeta \in K_1^\times$ (de fait on doit prendre pour ζ un représentant, dans K_1^\times , de a modulo $K_1^{\times p}$, ce qui donne l'extension kummerienne L par unicité du radical). Comme a , donc ζ , est par définition étranger à S , et que la ramification modérée se lit sur l'idéal (ζ) , il en résulte que l'extension L/K est nécessairement p -ramifiée.

On déduit de ce qui précède qu'en dehors du cas kummerien p -ramifié, il ne peut y avoir capitulation non triviale et on a donc obtenu le résultat suivant remarqué dans [Seo6].

Théorème 2.3. — Soit L/K une p -extension, $p > 2$. Sous la conjecture de Leopoldt pour p dans L , si $\mu_K = 1$, le morphisme de capitulation $j_{L/K} : BP_K \rightarrow BP_L$ est injectif.²

Démonstration. — Comme L/K est une p -extension, on est ramené au cas cyclique ci-dessus en remarquant que les hypothèses se transmettent à tout corps F utilisé par induction et compris entre K et L ($\mu_F = 1$ et conjecture de Leopoldt).

Une condition nécessaire (mais non suffisante) pour que $\text{Ker}(j_{L/K})$ soit non trivial est donc que L/K soit kummerienne et p -ramifiée (si L/K est abélienne on a $L = H_K^{pr}$).

Poursuivons l'étude du noyau de capitulation avec la seule hypothèse L/K cyclique p -ramifiée de degré p et par conséquent $S = S_p$ (l'hypothèse kummerienne n'est pas nécessaire pour l'instant car on la retrouvera dans le calcul du noyau).

On revient à $\mathfrak{a} \subset K$ tel que par extension, $(\mathfrak{a})_L = (y)$ où $y \in L^\times$, avec $i_L(y) = \mu_L \in W_L$, et $y^p \in K_1^\times$. Il vient $y^{1-s} = \mu_L$ où $\mu_L \in \mu_K$ est d'ordre 1 ou p . Alors $\mu_L^{1-s} = i_L(\mu_L)$.

Réciproquement, si $\mu_L \in W_L$ est tel que $\mu_L^{1-s} = i_L(\mu_L)$, en prenant $y \in L^\times$ tel que $i_L(y) = \mu_L$, il vient $i_L(\mu_L) = i_L(y)^{1-s}$, d'où $\mu_L = y^{1-s}y^s$, $y \in L^\times$; on a $N_{L/K}(y) = N_{L/K}(\mu_L) = 1$ d'après ce qui précède; d'où (lemme 1.5) $y = y^{1-s}y^s$, $y \in L^\times$, et on obtient une relation de la forme $\mu_L = y^{1-s}$, ce qui conduit à $(y) \subset L^\times = (K)_L$ car il n'y a pas de ramification en dehors de p et (y) est étranger à p . L'idéal (y) de L est l'étendu d'un idéal \mathfrak{a} de K étranger à p dont la classe est dans le noyau de $j_{L/K}$. On a donc démontré à ce stade :

$$\text{Ker}(j_{L/K}) = \{ \mathfrak{a} \subset K, (\mathfrak{a})_L = (y), i_L(y) = \mu_L \text{ et } \mu_L^{1-s} = i_L(\mu_L) \} / \{ (x), x \in K_1^\times, i_K(x) \in W_K \},$$

qu'il reste à simplifier.

Soit $\mathfrak{a} \subset K$ tel que $(\mathfrak{a})_L = (y)$, $i_L(y) = \mu_L \in W_L$, $\mu_L^{1-s} = i_L(\mu_L)$; si $\mathfrak{a} = (x)$ avec $i_K(x) \in W_K$, il vient $i_L(y) = i_L(x) i_L(\mu_L)$, $\mu_L \in E_L$, soit $\mu_L = \mu_K i_L(\mu_L)$; donc $i_L(\mu_L)$ est de la forme $i_L(\mu_L)$, $\mu_L \in \mu_L$, d'où $\mu_L \in W_K i_L(\mu_L)$.

Réciproquement, si $\mu_L = \mu_K i_L(\mu_L) \in W_K i_L(\mu_L)$ (qui implique $\mu_L^{1-s} = i_L(\mu_L)$), on a $i_L(y) = i_L(x) i_L(\mu_L)$ pour $x \in K_1^\times$ tel que $i_K(x) = \mu_K$, d'où, en idéaux, $(y) = (x)_L (y)$ et $(\mathfrak{a})_L = (x)_L (y)$, où $(y) \subset P_L^G = P_K$, (lemme 1.2), d'où $\mathfrak{a} = (x)$ avec $i_K(x) \in W_K$.

La classe de \mathfrak{a} dans le noyau de $j_{L/K}$ est nulle si et seulement si dans l'écriture $(\mathfrak{a})_L = (y)$, on a $i_L(y) \in W_K i_L(\mu_L)$.

On a donc obtenu une première description du noyau de capitulation dans le cas L/K cyclique p -ramifiée de degré p :

Lemme 2.4. — On a $\text{Ker}(j_{L/K}) = \{ \mu_L \in W_L, \mu_L^{1-s} = i_L(\mu_L) \} / W_K \cdot i_L(\mu_L)$. Si de plus $\mu_K = 1$, on a $i_L(\mu_L) = 1$, $\{ \mu_L \in W_L, \mu_L^{1-s} = 1 \} = W_K$, et le noyau de capitulation est nul (ce qui redonne le théorème 2.3).

Démonstration. — Il suffit de considérer l'application qui à \mathfrak{a} , dont la classe est dans le noyau de capitulation, associe μ_L (qui est définie modulo l'image de μ_L).

²Dès les lemmes 1.2, 1.3 et 1.4, le résultat est évident car on a $W = W_K \otimes_{\mathbb{Z}} \text{tor}_{\mathbb{Z}}(U/\overline{E}) \subset T$ et $BP = T/W$ (pour K et L) : donc si pour $\mu_K \in T_K$, on a $j_{L/K}(\mu_K) = \mu_L \in W_L$, on a $\mu_L \in W_L^G = W_K$.

2.4. Étude de $\text{Ker}(j_{L/K})$ dans le cas kummerien p -ramifié cyclique de degré p . —

On suppose désormais que μ_1 d'ordre p est dans K . On a (lemme 2.4), la suite exacte :

$$1 \rightarrow \text{Ker}(j_{L/K}) \rightarrow W_L/W_K \cdot i_L(\mu_L)^{1-s} \rightarrow W_L^{1-s}/W_L^{1-s} \cdot i_L(\mu_K) \rightarrow 1,$$

qui conduit, puisque $W_L^{1-s} = W_L/W_K$ et $W_K \cdot i_L(\mu_L)/W_K = \mu_L/\mu_K$, à l'énoncé :

Lemme 2.5. — *Dans le cas kummerien p -ramifié cyclique de degré p , et sous la conjecture de Leopoldt pour p dans L , on a $|\text{Ker}(j_{L/K})| = |W_L^{1-s} \cdot i_L(\mu_K)| \times \frac{|\mu_K|}{|\mu_L|}$, où $W_L^{1-s} \cdot i_L(\mu_K) \cdot i_L(\mu_1)$ est d'ordre 1 ou p .*

Si $\mu_K = \mu_L = 1$, on a $|\text{Ker}(j_{L/K})| = |W_L^{1-s} \cdot i_L(\mu_K)|$.

Si $\mu_K = \mu_L^p = 1$ (i.e. L/K est cyclotomique globale), $j_{L/K}$ est injectif.

Démonstration. — En effet, d'après le Lemme 1.3 (iii), on a $W_L^{1-s} \cdot i_L(\mu_K) \cdot i_L(\mu_1) \cdot \mu_1$ est d'ordre p . Ainsi il y a injectivité de $j_{L/K}$ si et seulement si L/K est cyclotomique globale ou bien si $\mu_K = \mu_L = 1$ et $i_L(\mu_1) \notin W_L^{1-s}$.

Ceci peut se caractériser de la première façon concrète suivante (analogue du théorème 2.1 de [NgPMB], Proposition 8 et Exemple 12 de [JaPMB]) :

Théorème 2.6. — *Soit L/K une extension cyclique, p -ramifiée, de degré $p > 2$, vérifiant la conjecture de Leopoldt pour p . On suppose que $\mu_K = \mu_L = 1$ (i.e., L/K est kummerienne non globalement cyclotomique). Le morphisme de capitulation $j_{L/K} : BP_K \rightarrow BP_L$ est injectif si et seulement si il existe $v_0 \mid p$ dans K , non décomposée dans L , telle que $\mu_{L_{w_0}} = \mu_{K_{v_0}}$ pour l'unique $w_0 \mid v_0$.*

Démonstration. — Écrivons $W_L = \prod_{v \mid p} W_{L,v}$ en un sens évident. On a alors trois cas pour $W_{L,v}^{1-s}$ selon que v est décomposée dans L/K ou non, puis que L_w/K_v est une extension cyclotomique ou non, sachant que $\mu_{K_v} = 1$ par hypothèse puisque $\mu_1 \in K$. On calcule alors $H^1(G, W_{L,v})$ pour obtenir $W_{L,v}^{1-s}$:

(i) Cas décomposé, i.e., $W_{L,v} = \mu_{K_v}$: on a $H^1(G, W_{L,v}) = 0$ (lemme de Shapiro) et $W_{L,v}^{1-s} = W_{L,v}$ qui contient l'image de μ_1 .

(ii) Cas non décomposé et $\mu_{L_w}^p = \mu_{K_v}$: on a $H^1(G, W_{L,v}) = 0$ et $W_{L,v}^{1-s} = i_v(\mu_1)$.

(iii) Cas non décomposé et $\mu_{L_w} = \mu_{K_v}$: on a $H^1(G, W_{L,v}) = \mathbb{Z}/p\mathbb{Z}$ et $W_{L,v}^{1-s} = 1$.

Le théorème en résulte puisque la condition diagonale contraire $i_L(\mu_1) \in W_L^{1-s}$ ($j_{L/K}$ non injectif) équivaut à $W_{L,v}^{1-s} = 1$ pour tout $v \mid p$; or seul (iii) conduit à une impossibilité.

Remarque 2.7. — Il résulte de ceci que lorsque $\mu_K = 1$ (i.e., $\mu_1 \in K$), la notion usuelle de p -extension cyclotomique globale, locale, résiduelle en caractéristique $\neq p$ (i.e., de K, K_v, F_v), est équivalente à celle de p -extension contenue dans la Z_p -extension cyclotomique correspondante.

Ainsi, « L/K p -ramifiée et localement cyclotomique en p » (i.e., toute place $v \mid p$ est non ramifiée et en toute place $v \mid p$ non décomposée, $\mu_{L_w}^p = \mu_{K_v}$) équivaut à « L/K partout localement cyclotomique » ou « logarithmiquement non ramifiée » au sens plus général défini

par Jaulent ([JaPMB], §3). En effet, si $v - p$ est non ramifiée, c'est le corps de classes local par relèvement des extensions résiduelles qui sont cyclotomiques, si v / p c'est par hypothèse. Noter que pour toute place finie v décomposée, l'algèbre $_{w/v} L_w$ peut aussi être qualifiée de cyclotomique de façon galoisienne car il existe $_{L,v} W_{L,v}$ tel que $_{L,v}^{1-s} = 1$ et $_{L,v}^p = \mu_{K_v}$: pour cela, prendre $_{L,v} = (v, v \cdot \zeta_1^{-1}, \dots, v \cdot \zeta_1^{-(p-1)})$ pour un générateur v de $\mu_{K_v} = \mu_{L_w}$. Tout corps de nombres k admet une pro- p -extension Abélienne localement cyclotomique maximale H_k^c , sous-corps de H_k^{pr} fixe par les groupes de décomposition relatifs des places v / p dans H_k^{pr}/k (où k est la Z_p -extension cyclotomique de k) et alors $\text{Gal}(H_k^c/k)$ est isomorphe au groupe des classes logarithmiques introduit par Jaulent ([Ja4], [Ja5] [JaM1], [JaM2], [JaS]); voir aussi [Gr1], § III.7.

Dans [JaPMB] et [NgPMB] c'est aussi le vocabulaire adopté systématiquement.

3. Interprétation de $\text{Ker}(j_{L/K}) = 1$ via un radical kummerien global

On suppose $\mu_K = 1$ et on pose $L = K(\zeta^{\frac{1}{p}})$, K^x ; on suppose que L/K est p -ramifiée non globalement cyclotomique (i.e., $\mu_L = \mu_K$). On a donc $(\zeta) = \mathfrak{a}_0^p \alpha_p$, où \mathfrak{a}_0 est un idéal de K étranger à p et où l'on peut supposer que α_p est un produit d'idéaux premiers au-dessus de p à une puissance $< p$. On pose $(\zeta^{\frac{1}{p}})^{1-s} = \zeta_1$ d'ordre p .

D'après le Théorème 2.6, $j_{L/K}$ est *non injectif* si et seulement si pour toute place v / p , non décomposée dans L/K , $\mu_{K_v} = \mu_{L_w}^p$ pour l'unique place w / v de L . Dans ce cas, il existe $\alpha \in I_K$ dont la classe (d'ordre p dans BP_K , donc dans $I_K / \{(x), x \in K_1^x, i_K(x) \in W_K\}$, et d'ordre une puissance de p dans I_K / P_K) est dans le noyau de $j_{L/K}$; on a (cf. §2.3) $(\alpha)_L = (y)$, avec $i_L(y) = \zeta_1 W_L$ et $y^p = a \in K_1^x$.

Soit v / p fixée non décomposée ; on a, avec des notations évidentes, $i_w(y) = \zeta_1$ et $i_w(y)^{1-s} = \zeta_1^{1-s} = i_w(\zeta_1)$ et par conséquent on peut prendre ζ_1 comme radical local, autrement dit $L_w = K_v(\zeta_1^{\frac{1}{p}})$ où $\zeta_1^{\frac{1}{p}} =: \zeta_1 W_L$ et il en résulte, par "unicité" d'un radical modulo K_v^x/p , que $\alpha_p = 1$ et que $i_v(a) = \zeta_1^p$ (bien que certaines places v/p puissent se ramifier dans L/K ; cf. [Gr1], Proposition II.1.6.3 pour le calcul du v -conducteur).

On a $i_L(y)^{1-s} = i_L(\zeta_1^{\frac{1}{p}})^{1-s} = i_L(\zeta_1) = i_L(\zeta^{\frac{1}{p}})^{1-s}$, d'où, $y = \zeta^{\frac{1}{p}} \bar{a} = \zeta^{\frac{1}{p}} \cdot x^{-1}$, $x \in K_1^x$, ce qui relie α et \mathfrak{a}_0 via l'égalité :

$$\alpha = \mathfrak{a}_0 \cdot (x)^{-1}.$$

En résumé vérifie les conditions nécessaires et suffisantes suivantes :

$$(1) \quad (\zeta) = \mathfrak{a}_0^p \text{ et } \zeta = a \cdot x^p, a, x \in K_1^x \text{ et } i_K(a) \in W_K, \zeta \in W_L^p.$$

Noter que $i_L(\zeta^{\frac{1}{p}} \cdot x^{-1}) = \zeta_1$ et que par conséquent, il existe une puissance p^e de p telle que $(\zeta^{\frac{1}{p}} \cdot x^{-1})^{p^e} \in K^x$ ou encore que $\alpha = \mathfrak{a}_0 \cdot (x)^{-1}$ est tel que :

$$(2) \quad \alpha^{p^e} = (\mathfrak{a}_0 \cdot (x)^{-1})^{p^e} \in P_K.$$

On peut donc, à partir de la relation (1), énoncer le résultat suivant, où l'on rappelle que pour un corps de nombres k , μ_k est le p -groupe des racines de l'unité, k le composé des Z_p -extensions, U_k le Z_p -module d'unités locales principales en p et $W_k = \text{tor}_{Z_p} U_k$. On désigne par BP_k la pro- p -extension abélienne maximale de k composée des p -extensions cycliques

plongeables dans une p -extension cyclique de k de degré arbitrairement grand ; on pose $BP_k := \text{Gal}(BP_k/k)$:

Théorème 3.1. — Soit L/K une extension cyclique de corps de nombres, de degré premier $p > 2$. On suppose que L vérifie la conjecture de Leopoldt pour p . Alors le morphisme de capitulation $j_{L/K} : BP_K \rightarrow BP_L$ est non injectif si et seulement si les deux conditions suivantes sont satisfaites :

(i) $\mu_L = \mu_K = 1$, $L = K(\sqrt[p]{})$, $K^\times \cap () = \mathfrak{a}_0^p$, où \mathfrak{a}_0 est un idéal de K étranger à p (i.e., L/K est kummerienne, non globalement cyclotomique (i.e., $\not\subset \mu_K \cdot K^{\times p}$), et p -ramifiée (i.e., non ramifiée en dehors de p)) ;

(ii) l'image diagonale de () dans U_K est égale à ${}_K U_K^p \cdot {}_K W_K \cdot u_K \cdot U_K$, avec ${}_K W_K \subset W_L^p$ (i.e., L/K est localement cyclotomique en toute place $v \mid p$).

On pourrait alors obtenir le résultat plus général suivant (cf. [JaPMB], corollaire 11 pour le cas cyclique et [NgPMB], théorème 2.5 pour le cas abélien) :

Théorème 3.2. — Dans une p -extension abélienne L/K de corps de nombres, contenant les racines p -ièmes de l'unité, et satisfaisant à la conjecture de Leopoldt pour le nombre premier $p > 2$, le sous-groupe $\text{Ker}(j_{L/K})$ des éléments de BP_K qui capitulent dans BP_L est d'ordre $\min |\mu_K|, [L : K^{lc} : K(\mu_L)]$, où K^{lc} est la pro- p -extension localement cyclotomique maximale de K .

4. Le p -groupe des classes et le régulateur p -adique

4.1. Existence de L/K cyclique de degré p telle que $\text{Ker}(j_{L/K}) = 1$. — On considère une extension de Kummer $L = K(\sqrt[p]{})$ vérifiant les conditions (i) et (ii) du théorème 3.1, donc telle que $j_{L/K}$ est non injectif. On a alors $() = \mathfrak{a}_0^p$, \mathfrak{a}_0 idéal de K étranger à p , et tel que $i_K() \in W_L^p \cdot U_K^p$. Il y a alors deux cas qui s'excluent : ou bien \mathfrak{a}_0 n'est pas principal et la classe (au sens usuel) de cet idéal capitule dans L puisque $(\mathfrak{a}_0)_L = (\sqrt[p]{})$, ou bien \mathfrak{a}_0 est principal et, modulo $K^{\times p}$, () est une unité E_K et $L = K(\sqrt[p]{})$ (() non racine de l'unité).

(a) Dans le premier cas (cf. § 3, relation (2)), il existe $\mathfrak{a} = \mathfrak{a}_0 \cdot (x)^{-1}$, $x \in K_1^\times$, dont la classe dans I_K/P_K est d'ordre fini et engendre $\text{Ker}(j_{L/K})$ dans BP_K ; soit ${}_K T_K$ correspondant à cette classe dans I_K/P_K , alors la restriction ${}_K$ de ${}_K$ à H_K est dans $\text{Gal}(H_K/H_K \cdot K)$ et correspond à la classe de \mathfrak{a} dans I_K/P_K (d'ordre p puisque $\mathfrak{a} = \mathfrak{a}_0 \cdot (x)^{-1}$), et par conséquent c'est une classe du sous-groupe $C_K = \text{Gal}(H_K/H_K \cdot K)$ de C_K qui capitule (cf. Schéma du § 1.1).³

(b) Dans le cas d'une unité () , écrivons $i_K() = {}_K U_K^p \cdot W_L^p \cdot U_K^p$. Il vient $\log_K(i_K()) = p \log_K(u_K)$; montrons que $\log_K(u_K)$ définit un élément d'ordre p du régulateur R_K : si au contraire $\log_K(u_K) = \log_K(i_K())$, pour une unité E_K , on obtient $\log_K(i_K()) = p \log_K(i_K())$ qui implique $i_K() = {}_K i_K(^p)$, ${}_K W_K$, ce qui conduit (lemme 1.2) à ${}_K = i_K() \cdot i_K(\mu_K)$ ou encore à $() = {}_K ^p$. On aurait donc $L = K(\sqrt[p]{})$ (absurde).

³D'après [Gr1], corollaire III.2.6.1 (i), on a $[H_K : H_K \cdot K] = |C_K| / |(\text{Log}_K(I_K) : \text{Log}_K(P_K))|$, où $\text{Log}_K : I_K \rightarrow K_v \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \log_K(E_K)$, est la fonction logarithme définie dans [Gr1], § III.2.2 et reprise au § 5.3.2.

Par contre dans L , il est clair que $\log_L(\overline{{}^p i_K(\)}) = \frac{1}{p} \log_L(i_K(\)) = \log_L(u_K)$ montre que $\log_K(u_K)$ devient d'ordre 1 dans R_L , et on parlera par analogie de capitulation dans L d'un élément d'ordre p du régulateur de K .

Remarques 4.1. — (i) Dans les deux cas, la capitulation ne concerne qu'une classe ou unité particulière en raison de la condition supplémentaire L/K localement cyclotomique en p . On est donc amené à considérer le sous-ensemble des *pseudo-unités localement cyclotomiques* :

$$F_K := \{ K_1^{\times}, (\) = \alpha_0^p, \alpha_0 \in I_K \text{ et } i_K(\) = \frac{p}{L} \cdot u_K^p, L = W_L, u_K \in U_K \} K_1^{\times p},$$

dont le F_p -rang est majoré par $r_1 + r_2 + c$ où c est le F_p -rang du groupe des classes de K .

(ii) La condition $i_K(\) = \frac{p}{L} \cdot u_K^p$ est équivalente à $i_K(\) = \frac{p}{K} \cdot u_K^p, K = W_L^p$ ou encore à $\frac{p}{L} \cdot W_L \cdot u_K$, puisque $W_L^p = W_K$ (Lemme 1.3 (iii)). Une condition *nécessaire mais non su sante* est $\log_K(i_K(\)) = p \cdot \log_K(u_K)$; elle devient su sante si $W_K = W_L^p$.

(iii) La relation $|BP_K| = |C_K| \times |R_K|$ montre que si $j_{L/K}$ est non injectif, nécessairement l'un des deux facteurs au moins est non trivial et contribue à la capitulation (points (a) et (b)). À comparer au § 7 de [JaPMB], définition, et proposition 20 et au complément 2.6 de [NgPMB].

4.2. Exemples numériques. — On prend pour K le corps biquadratique $K = \mathbb{Q}(\sqrt{-9}, j)$ contenant le corps $\mathbb{Q}(j)$ des racines cubiques de l'unité et le corps $\mathbb{Q}(\sqrt{-237})$; on considère $p = 3$. Comme 3 est décomposé dans K en deux idéaux premiers, les deux complétés de K sont égaux à $\mathbb{Q}_3(j)$ (voir des exemples analogues dans [JaPMB], § 4).

Le nombre de classes de $\mathbb{Q}(\sqrt{-9})$ est 3, celui de $\mathbb{Q}(\sqrt{-237})$ est 12 :

(i) Prenons l'unité $\epsilon_1 = j$ où $\epsilon_1 = 80 + 9\sqrt{-9}$ (l'unité fondamentale de $\mathbb{Q}(\sqrt{-9})$ qui est 3-primaire et localement un cube en 3). Soit $L_1 = K(\sqrt[3]{\epsilon_1})$; on a bien $\mu_{L_1} = \mu_K = 1$. On a $\epsilon_1 \cdot j^{-1} = 80 + 9\sqrt{-9} = u_K^3$, ce qui montre que les deux complétés de L_1 sont égaux à $\mathbb{Q}_3(\epsilon_1)$, où ϵ_1 est une racine de l'unité d'ordre 9; on est dans le cas $\mu_{K_v} = \mu_{L_{1,w}}^3$ pour toute place $v/3$, et les deux conditions du théorème 3.1 sont donc satisfaites puisque $i_K(\epsilon_1) = \frac{p}{K} \cdot u_K^3$, avec $\frac{p}{K} = (j, j) = (\epsilon_1, \epsilon_1)^3$; donc $j_{L_1/K}$ est non injectif.

(ii) On considère l'unité $\epsilon_2 = \epsilon_1 = 80 + 9\sqrt{-9}$ et $L_2 = K(\sqrt[3]{\epsilon_2})$. Comme ϵ_2 est localement un cube, L_2/K est décomposée en toutes les places $v/3$. Donc $j_{L_2/K}$ est encore non injectif.

Noter que par la dualité de Kummer, L_2 est ici le composé du 3-corps de Hilbert $L_2^- := H_{K^-}$ et de $\mathbb{Q}(j)$, où $K^- := \mathbb{Q}(\sqrt{-237})$, et que comme $j \notin K^-$, $j_{L_2^-/K^-}$ est injectif et le noyau de $j_{L_2/K}$ est un sous-groupe non trivial de $T_{K^-}^{\frac{1-t}{2}}$, où t engendre $\text{Gal}(K/K^-)$.

(iii) Si l'on prend $\epsilon_3 = 8 + 3\sqrt{-237}$ (qui est 3-primaire) et $L_3 = K(\sqrt[3]{\epsilon_3})$, on a $(\epsilon_3) = \mathfrak{p}_{13}^3$ dans K^- pour un idéal premier non principal $\mathfrak{p}_{13}/13$ car la condition (ii) n'est pas vérifiée; les extensions $K(\sqrt[3]{j}), K(\sqrt[3]{j-3}), K(\sqrt[3]{j^2-3})$ sont ramifiées en 3 et, dans $K(\sqrt[3]{-3})$ (contenue dans le 3-corps de classes de Hilbert $K(\sqrt[3]{-}, \sqrt[3]{-3})$ de K), 3 est inerte; or il faudrait une décomposition de 3 dans l'une d'elles.

On voit aussi que la condition $\log(\epsilon_3) = 3 \cdot \log(u_K)$ n'est pas vérifiée car ϵ_3 est 3-primaire sans être localement un cube. Dans ce cas, $j_{L_3/K}$ est injectif bien qu'il y ait capitulation d'une classe d'idéaux dans L_3 . Ici aussi on peut écrire L_3 comme composé du 3-corps de Hilbert H_{K^+} et de $\mathbb{Q}(j)$, où $K^+ := \mathbb{Q}(\sqrt{-9})$, et les deux composantes de $j_{L_3/K}$ sont injectives.

Prenons pour K le corps biquadratique $K = \mathbb{Q}(\sqrt{-107}, j)$. Le nombre de classes de $K^- := \mathbb{Q}(\sqrt{-107})$ est 3 et celui de $K^+ := \mathbb{Q}(\sqrt{321})$ est aussi 3; l'unité fondamentale de K^+ est $\epsilon = 215 + 12\sqrt{321}$ qui est 3-primaire sans être localement un cube; on a $(59 + 2\sqrt{321}) = \mathfrak{p}_{13}^3$ dans le sous-corps réel ($\epsilon := 59 + 2\sqrt{321}$ est non 3-primaire). Dans le sous-corps quadratique imaginaire K^- , on a $(270 + 17\sqrt{-107}) = \mathfrak{p}_{47}^3$, pour \mathfrak{p}_{47} non principal, où $\epsilon := 270 + 17\sqrt{-107}$ est 3-primaire et localement un cube car $\epsilon^2 \equiv 1 \pmod{9}$. L'extension $L = K(\sqrt[3]{\epsilon})$ conduit au même raisonnement qu'en (ii) avec ici échange des sous-corps K^- et K^+ . On a $H_{K^+}(\mathbb{Q}(j)) = K(\sqrt[3]{\epsilon})$ et $H_{K^-}(\mathbb{Q}(j)) = K(\sqrt[3]{\epsilon})$; l'extension $K(\sqrt[3]{\epsilon})$ est ramifiée en 3 mais n'est pas localement cyclotomique.

5. Points fixes du module de Bertrandias–Payan

Dans cette section, L/K est une p -extension quelconque de corps de nombres ($p > 2$), de groupe de Galois G , que l'on supposera cyclique de degré p à partir du §5.2. On suppose seulement que L vérifie la conjecture de Leopoldt pour p , ce qui implique que T_L^G contient un sous-groupe isomorphe à T_K (injectivité du morphisme $T_K \rightarrow T_L$, lemme 2.1).

On omet le plus souvent les plongements diagonaux i_K et i_L .

Ici il n'y a aucune hypothèse sur la ramification dans L/K ni sur les groupes μ_K, μ_L .

On a la suite exacte qui définit BP_L à partir de $T_L = \text{Gal}(H_L^{\text{pr}}/L)$:

$$1 \rightarrow W_L/\mu_L \rightarrow T_L \rightarrow BP_L \rightarrow 1,$$

où $W_L = \prod_{v|p} W_{L,v}$, avec $W_{L,v} = \prod_{w|v} \mu_{L_w}$ pour toute place $v|p$ de K .

On a de même la suite exacte :

$$1 \rightarrow W_K/\mu_K \rightarrow T_K \rightarrow BP_K \rightarrow 1.$$

5.1. Suites exactes fondamentales. — On a la suite exacte :

$$1 \rightarrow (W_L/\mu_L)^G \rightarrow T_L^G \rightarrow BP_L^G \rightarrow H^1(G, W_L/\mu_L), \tag{1}$$

et à partir de $1 \rightarrow \mu_L \rightarrow W_L \rightarrow W_L/\mu_L \rightarrow 1$, on a la suite exacte :

$$1 \rightarrow W_K/\mu_K \rightarrow (W_L/\mu_L)^G \rightarrow H^1(G, \mu_L) \rightarrow H^1(G, W_L), \tag{2}$$

avec $H^1(G, W_L) = \prod_{v|p} H^1(G, W_{L,v})$.

Dans le cas G cyclique d'ordre p (engendré par s) on aura les suites exactes :

$$1 \rightarrow (W_L/\mu_L)^G \rightarrow T_L^G \rightarrow BP_L^G \rightarrow N(W_L/\mu_L) (W_L/\mu_L)^{1-s}, \tag{1}$$

$$1 \rightarrow W_K/\mu_K \rightarrow (W_L/\mu_L)^G \rightarrow N\mu_L \mu_L^{1-s} \rightarrow \prod_{v|p} N W_{L,v} / W_{L,v}^{1-s}. \tag{2}$$

Remarque 5.1. — Dans le cas G cyclique d'ordre p , les noyaux de la « norme » $N = N_G$ sont ceux de la norme algébrique (ici $N_G = 1 + s + \dots + s^{p-1}$). Or on peut utiliser, par commodité des calculs, la norme arithmétique $N_{L/K}$ à condition que pour les objets X_L et X_K , l'application naturelle $i_{L/K} : X_K \rightarrow X_L$ soit injective puisque $i_{L/K} N_{L/K} = N_G$.

C'est le cas ici pour les objets du type $U_k, \bar{E}_k, \mu_k, W_k, W_k = W_k/\mu_k, A_k, B_k = U_k/\bar{E}_k, T_k$, mais non nécessairement pour C_k, C_k, R_k, BP_k .

On souhaite voir, comme dans [Seo3], [Seo4], [Seo6], à quelles conditions $|BP_K|$ divise $|BP_L|$ au moyen, par exemple, de la condition suffisante $|BP_K|$ divise $|BP_L^G|$. D’après (1) et (2) il vient :

$$|BP_L^G| = \frac{|T_L^G| \cdot |\text{Im}(\)|}{|(W_L/\mu_L)^G|} = \frac{|T_L^G| \cdot |\text{Im}(\)|}{|W_K/\mu_K| \cdot |\text{Im}(\)|} = \frac{|T_L^G|}{|T_K|} \cdot |BP_K| \cdot \frac{|\text{Im}(\)|}{|\text{Im}(\)|}. \tag{3}$$

En utilisant la formule des points fixes pour T_L ([Gr1], théorème IV.3.3), il vient :

Théorème 5.2. — Soit L/K une p -extension de corps de nombres ($p > 2$) vérifiant la conjecture de Leopoldt pour p . On a la formule suivante (où le premier facteur est entier) :

$$|BP_L^G| = \frac{q^{-p} e_q}{q^{-p} \frac{1}{e_q} Z_p \text{Log}_K(\mathfrak{q}) + \text{Log}_K(I_K) : \text{Log}_K(I_K)} \cdot |BP_K| \cdot \frac{|\text{Im}(\)|}{|\text{Im}(\)|},$$

où e_q est l’indice de ramification de \mathfrak{q} dans L/K , et $\text{Log}_K : I_K \rightarrow \prod_{v|p} K_v \otimes_{\mathbb{Q}_p} \log_K(E_K)$, la fonction logarithme définie dans [Gr1], § III.2.2 (voir aussi le § 5.3.2).

Corollaire 5.3. — On peut trouver une infinité de p -extensions L/K telles que $|BP_L^G| = 1$ et même telles que $|BP_L^G| = q^{-p} e_q \cdot |BP_K| \cdot \frac{|\text{Im}(\)|}{|\text{Im}(\)|} = q^{-p} e_q \cdot |BP_K| \cdot \frac{1}{|H^1(G, \mu_L)|}$.

Corollaire 5.4. — Lorsque l’extension L/K est p -primitivement ramifiée, ce qui est équivalent à $q^{-p} \frac{1}{e_q} Z_p \text{Log}_K(\mathfrak{q}) + \text{Log}_K(I_K) : \text{Log}_K(I_K) = q^{-p} e_q$ ([Gr1], définition IV.3.4), on a $|BP_L^G| = |BP_K|$ si et seulement si $|\text{Im}(\)| = |\text{Im}(\)|$.

5.2. Caractérisation de $|\text{Im}(\)| = p$ pour L/K p -ramifiée cyclique de degré p . — Pour un cadre plus général voir [NgPMB] et [JaPMB].

On a $|\text{Im}(\)| = |{}_N \mu_L \mu_L^{1-s}| = p$. On écarte donc le cas trivial $|{}_N \mu_L \mu_L^{1-s}| = 1$, et on suppose (cf. Lemme 1.3) que $\mu_K = \mu_L = 1$ (i.e., L/K kummerienne non globalement cyclotomique). On a $|\text{Im}(\)| = p$ si et seulement si $i_v = 0$ dans (2) ; or l’image de i_1 par $\text{Im}(\)$ est la classe de l’image diagonale dans W_L de $i_1 \pmod{W_L^{1-s}}$. Cette classe est nulle si et seulement si $i_v(1) \in W_{L,v}^{1-s}$ pour tout $v|p$. Autrement dit (cf. lemme 2.5, théorème 2.6 ou Théorème 3.1) :

Proposition 5.5. — Soit L/K p -ramifiée cyclique de degré $p > 2$. On a $|\text{Im}(\)| = p$ si et seulement si $|\text{Ker}(j_{L/K})| = p$, ou encore si et seulement si $|W_L^G| = p \cdot |W_K|$.

Si $|\text{Im}(\)| = p$, il suffit d’avoir $|\text{Im}(\)| = p$ pour que l’inégalité $|BP_L^G| = |BP_K|$ soit vérifiée ; or $\text{Im}(\)$ dépend du noyau de l’application $\text{Im}(\) : H^1(G, W_L/\mu_L) \rightarrow H^1(G, T_L)$, qui fait l’objet du paragraphe suivant.

5.3. Calcul de $\text{Ker}(\)$. — On reprend la suite exacte (1) en la prolongeant comme suit :

$$1 \rightarrow (W_L/\mu_L)^G \xrightarrow{T_L^G} T_K \xrightarrow{BP_L^G} {}_N(W_L/\mu_L) \xrightarrow{(W_L/\mu_L)^{1-s}} {}_N T_L \xrightarrow{T_L^{1-s}} 1.$$

On est donc dans le cadre de non injectivité de $j_{L/K}$, L/K étant cyclique de degré p , p -ramifiée, kummerienne non globalement cyclotomique (i.e., $\mu_K = \mu_L = 1$), et localement cyclotomique en p (cf. remarque 2.7).

Lemme 5.6. — Sous les hypothèses précédentes, on a $H^1(G, W_L/\mu_L) \cong \mathbb{Z}/p\mathbb{Z}$. Un générateur de ce groupe est donné par l'image d'un $\bar{z} \in W_L$ tel que $N_{L/K}(\bar{z}) = i_K(\bar{z})$, où \bar{z} est un générateur de μ_K .

Démonstration. — La suite exacte $1 \rightarrow \mu_L \rightarrow W_L \rightarrow W_L/\mu_L \rightarrow 1$ conduit à :

$$H^1(G, W_L) \rightarrow H^1(G, W_L/\mu_L) \rightarrow H^2(G, \mu_L) \rightarrow H^2(G, W_L).$$

Or $H^1(G, W_L) = \varinjlim_p H^1(G, W_{L,p}) = 0$ sous les hypothèses précédentes (théorème 2.6) ; donc $H^2(G, W_L) = 0$. D'où :

$$H^1(G, W_L/\mu_L) \cong H^2(G, \mu_L) \cong \mathbb{Z}/p\mathbb{Z}.$$

Comme $H^2(G, W_L) = W_K \wedge N_{L/K}(W_L) = 0$, $i_K(\bar{z}) \in N_{L/K}(W_L)$ et l'existence de \bar{z} (unique modulo $W_L^{1-s}\mu_L$) est immédiate ; son image dans le groupe $H^1(G, W_L/\mu_L)$ est d'ordre p car $\bar{z} \notin W_L^{1-s}\mu_L$.

5.3.1. *Caractérisation de $\text{Ker}(\cdot)$ en termes d'idéaux.* — À $\bar{z} \in W_L$ tel que $N_{L/K}(\bar{z}) = i_K(\bar{z})$, où \bar{z} engendre μ_K , l'application \cdot associe l'élément $\bar{z} \in N_{L/K}T_L$ défini par l'image de \bar{z} dans W_L/T_L . Puisque $\bar{z} \notin W_L^{1-s}\mu_L$, on a $\bar{z} \notin W_L^{1-s}$: la nullité éventuelle de \cdot (i.e., $\bar{z} \in T_L^{1-s}$) n'est donc pas triviale et concerne T_L en entier.

Soit $z \in L_1^\times$ tel que $i_L(z) = \bar{z}$; alors on a $N_{L/K}(z) = \bar{z} \in K^\times$, $x \in K^\times$, et l'image de \bar{z} dans L_1/P_L est celle de l'idéal (z) .

Comme (x) est norme d'idéal et x norme locale en p , on a (principe des normes globales de Hasse) $x = N_{L/K}(y)$, $y \in L^\times := L^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p$. Par le théorème d'approximation, on peut supposer que $y \in L_1^\times$ (le problème venant des idéaux premiers \mathfrak{p}/p décomposés divisant y) : pour cela écrire $x = x_1 \cdot x_1^p$, $x_1 \in K_1^\times$, $x_1 \in K_1^\times$; comme $x_1 = x \cdot x_1^{-p}$ est partout norme locale, il existe $t \in L^\times$ tel que $x_1 = N_{L/K}(t) = N_{L/K}(t \cdot t^{1-s}) \in N_{L/K}(L_1^\times)$, pour un $t \in L^\times$ convenable ; finalement $x = N_{L/K}(t \cdot t^{1-s} \cdot x_1) \in N_{L/K}(L_1^\times)$.

On doit ensuite étendre l'application i_L à L^\times ; elle est alors à valeurs dans le complété profini $\varprojlim_{w/p} L_w^\times := \varprojlim_{w/p} \varprojlim_w^{\mathbb{Z}_p} U_w$ de $\varprojlim_{w/p} L_w^\times$, où w est une uniformisante en w . L'application i_L est surjective (de noyau L^\times) car $i_L(L^\times)$ est dense dans $\varprojlim_{w/p} L_w^\times$ et le \mathbb{Z}_p -module engendré par $i_L(L^\times)$ (qui est égal à $i_L(L^\times)$) est fermé dans le complété profini qui est un \mathbb{Z}_p -module de type fini.

Puisque $x = N_{L/K}(y)$, avec $i_L(y) \in U_L$ et $N_{L/K}(i_L(y)) = 1$, il existe $\bar{z} \in \varprojlim_{w/p} L_w^\times$ tel que $i_L(y) = \bar{z}^{1-s}$; si $Y \in L^\times$ est tel que $\bar{z} = i_L(Y)$, on a $y = Y^{1-s}$, d'où $x = N_{L/K}(y)$ et $N_{L/K}(z) = \bar{z} \in N_{L/K}(Y)$; comme $z \in L_1^\times$ est défini modulo L^\times , on peut supposer que $N_{L/K}(z) = \bar{z}$ et que, en idéaux, $N_{L/K}((z)) = 1$, soit :

$$(z) = \mathfrak{B}^{1-s}, \quad \mathfrak{B} \in I_L.$$

Si on a une autre écriture $(z) = \mathfrak{B}^{1-s}, \mathfrak{B} \in I_L$, il vient $\mathfrak{B} = \mathfrak{B}' \cdot (\mathfrak{a})_L$, $\mathfrak{a} \in I_K$.

On aura $\text{Ker}(\cdot) = \bar{z}^{1-s}$ (i.e., $\cdot = 0$) si et seulement si il existe $\bar{z} \in N_{L/K}T_L$ tel que $\bar{z} = \bar{z}^{1-s}$, donc si et seulement si il existe un idéal $\mathfrak{b} \in I_L$, de la forme $\mathfrak{B}' \cdot (\mathfrak{a})_L^{-1}$, tel que $\text{Log}_L(\mathfrak{b}) = 0$ (voir ci-dessous les rappels sur la fonction Log).

5.3.2. *Rappels sur la fonction Log.* — Il faut pouvoir étudier (pour un corps de nombres k) les groupes de torsion T_k de façon effective, ce qui est possible en utilisant le logarithme Log_k introduit dans [Gr1], § III.2.2, et qui conduit à la suite exacte (dans laquelle $A_k = \text{Gal}(k/k)$) :

$$1 \rightarrow T_k \rightarrow A_k \rightarrow I_k/P_k \xrightarrow{\text{Log}_k} A_k \rightarrow \text{Log}_k(I_k) = Z_p \text{Log}_k(I_k) \rightarrow 0,$$

où l'on rappelle que (\log_k étant le logarithme p -adique usuel) :

$$\text{Log}_k : I_k/P_k \rightarrow \prod_{v|p} k_v \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \log_k(E_k),$$

est défini pour tout idéal \mathfrak{a} de k étranger à p par :

$$\text{Log}_k(\mathfrak{a}) := \frac{1}{m} \log_k(a) \pmod{\mathbb{Q}_p \log_k(E_k)},$$

où m est n'importe quel entier tel que \mathfrak{a}^m est un idéal principal (a).

En pratique $\text{Log}_k(P_k) = Z_p \text{Log}_k(P_k)$ est l'image de $\log_k(U_k) = Z_p \log_k(k_1^\times)$ dans le \mathbb{Q}_p -espace $\prod_{v|p} k_v \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \log_k(E_k)$, et le Z_p -module $\text{Log}_k(I_k)$ est connu numériquement dès que le groupe des classes l'est (au moyen d'idéaux générateurs $\mathfrak{b}_1, \dots, \mathfrak{b}_r$ modulo P_k) :

$$\text{Log}_k(I_k) = \frac{1}{h} \log_k(b_1), \dots, \frac{1}{h} \log_k(b_r) \Big|_{Z_p} + \log_k(U_k) + \mathbb{Q}_p \log_k(E_k),$$

avec $\mathfrak{b}_i^h = (b_i)$, $i = 1, \dots, r$, où h est par exemple l'ordre du groupe des classes de k . Comme $H := \frac{1}{h} \log_k(b_1), \dots, \frac{1}{h} \log_k(b_r) \Big|_{Z_p} + \log_k(U_k) \Big|_{Z_p}^{[k:\mathbb{Q}]}$ et $V := \mathbb{Q}_p \log_k(E_k) \Big|_{\mathbb{Q}_p}^{\mathbb{Q}_p^{r_1+r_2-1}}$ sous la conjecture de Leopoldt (où $r_1 + 2r_2 = [k:\mathbb{Q}]$), $\text{Log}_k(I_k) = (H + V)/V$ s'identifie à un sous- Z_p -module H de H tel que $H = H^- \oplus (H^+ - V)$ (où $H^- = H$ et $H^+ = (H - V) \Big|_{Z_p}$, avec les notations habituelles lorsque k est un corps CM).

5.3.3. *Calcul effectif de $(\bar{})_L$.* — On a vu au § 5.3.1 que $\bar{}_L$ est nulle si et seulement si il existe $\mathfrak{b} \in I_L$ tel que $(z) = \mathfrak{b}^{1-s}$ avec $\text{Log}_L(\mathfrak{b}) = 0$; comme on a obtenu $(z) = \mathfrak{B}^{1-s}$, pour un $\mathfrak{B} \in I_L$ particulier, on a $\bar{}_L = 0$ si et seulement si il existe $\mathfrak{a} \in I_K$ tel que $\mathfrak{B} \cdot (\mathfrak{a})_L^{-1} = \mathfrak{b}$, ce qui est équivalent à $\text{Log}_L(\mathfrak{B}) = \text{Log}_L((I_K)_L)$.

Soit $\bar{}_L \in A_L$ correspondant à l'image de \mathfrak{B} dans I_L/P_L , et $\bar{}_L \in T_L$ correspondant à celle de (z) ; on a seulement à ce stade $\bar{}_L = \bar{}_L^{-1-s} \in A_L^{1-s}$ ou encore l'existence de $e = 0$ tel que :

$$\bar{}_L^{-p^e} \in A_L^G = j_{L/K}(A_K) \tag{1}$$

(d'après la formule de points fixes de [Gr1], théorème IV.3.2 dans le cas L/K p -ramifiée).

Par contre, si $\mathfrak{b} = \mathfrak{B} \cdot (\mathfrak{a})_L^{-1}$ existe tel que $\text{Log}_L(\mathfrak{b}) = 0$ et si $\bar{}_K \in A_K$ est l'image de \mathfrak{a} , on a $\text{Log}_L(\bar{}_L \cdot j_{L/K}(\bar{}_K^{-1})) = 0$, ce qui est équivalent à $\bar{}_L \cdot j_{L/K}(\bar{}_K)^{-1} \in T_L$, ou encore à $\bar{}_L = \bar{}_L^{-1-s} \in T_L^{1-s}$ comme attendu (puisque $N_{L/K}(\bar{}_L) = 1$, la projection de $\bar{}_L$ dans A_K est triviale, donc $\bar{}_L \in \text{Gal}(H_L^{\text{pr}}/L H_K^{\text{pr}})$).

Il reste à calculer $\mathfrak{B} \in I_L$. Sur un plan effectif, on a besoin d'un renseignement global calculable; or $\bar{}_K$ est aussi partout norme locale et $\bar{}_K = N_{L/K}(t)$ où l'on peut, par le théorème d'approximation, supposer $t \in L_1^\times$ et l'idéal (t) de la forme \mathfrak{A}^{1-s} , \mathfrak{A} (idéal « ordinaire ») étranger à p . De $N_{L/K}(i_L(z) \cdot i_L(t)^{-1}) = 1$ on déduit l'existence de $\bar{}_L \in \prod_{w|p} L_w^\times$ tel que $i_L(z) \cdot i_L(t)^{-1} = \bar{}_L^{1-s}$. Soit $Z \in L^\times$ tel que $i_L(Z) = \bar{}_L$; on a $z \cdot t^{-1} = Z^{1-s} \cdot Z$, soit $(\mathfrak{B} \cdot \mathfrak{A}^{-1})^{1-s} = (Z)^{1-s} \cdot (Z)$; donc $N_{L/K}(Z) = E_K \in K^\times$, d'où $N_{L/K}(Z) = 1$ et $Z \in L^{\times(1-s)}$ (lemme 1.5), et quitte à modifier Z modulo L^\times il vient :

$$\mathfrak{B} \cdot \mathfrak{A}^{-1} = (Z) \cdot (\mathfrak{c})_L^{-1}, \quad \mathfrak{c} \in I_K \Big|_{Z_p}. \tag{2}$$

Comme $(Z) \cdot (\mathfrak{c})_L^{-1} \in I_L$, on vérifie que \bar{L} , donc Z et \mathfrak{c} , peuvent être choisis étrangers à p . Puisque $(z) = \mathfrak{B}^{1-s}$ et $\text{Log}_L(z) = 0$, il vient $(1-s)\text{Log}_L(\mathfrak{B}) = 0$, d'où :

$$\text{Log}_L(\mathfrak{B}) \stackrel{w/p}{=} \frac{L_w}{\mathbb{Q}_p} \log_L(E_L) \stackrel{G}{=} \frac{K_v}{v/p} \mathbb{Q}_p \log_K(E_K).$$

Numériquement on aura $\text{Log}_L(\mathfrak{B}) = \frac{1}{p^e} \cdot \text{Log}_L(I_K)$, $e \in \mathbb{Z}$, avec a priori $e \geq 0$ (relation (1)) ; comme \mathfrak{A} et t sont connus, il suffit de connaître Z modulo une puissance de p assez grande pour savoir (cf. (2)) si $\text{Log}_L(\mathfrak{B}) = \text{Log}_L(\mathfrak{A}) + \text{Log}_L(Z) = \text{Log}_K(I_K)$ ou non dans la mesure où $\text{Log}_K(I_K)$ se calcule facilement (cf. §5.3.2).

Or $i_L(Z) \in U_L$ est donné par une résolvante de Hilbert ; par exemple pour $p = 3$, on a (au produit près par un élément de $\frac{K_v^\times}{v/p}$) : $i_L(Z) = 1 + \bar{L} \cdot i_L(t)^{-1} + (\bar{L} \cdot i_L(t)^{-1})^{1+s}$; il suffit de prendre $Z = 1 + z t^{-1} + (z t^{-1})^{1+s} \in I_L$, où $z \in L$ est tel que $i_L(z)$ approche \bar{L} .

5.3.4. Autre formulation du critère de nullité de \bar{L} . — On sait que l'on peut interpréter l'image de A_L (ou de I_L/P_L) par Log_L comme étant $A_L := \text{Gal}(L/L)$ et que le transfert $A_K \rightarrow A_L$ est injectif (lemme 2.1). Comme la condition nécessaire et suffisante de nullité de \bar{L} est $\text{Log}_L(\bar{L}) \in \text{Log}_L(A_K)$, où \bar{L} correspond à l'image de \mathfrak{B} dans $A_L = I_L/P_L$ (avec $(z) = \mathfrak{B}^{1-s}$), il vient :

Une condition nécessaire et suffisante pour que \bar{L} soit nulle est que la projection de \bar{L} dans $\text{Gal}(L/L)$ (où $(\bar{L}) = \bar{L} = \bar{L}^{-1-s}$) soit dans le transfert de $\text{Gal}(K/K)$.

Il paraît clair, en raison des valeurs aléatoires des logarithmes d'idéaux, de $t \in L^\times$ tel que $N_{L/K}(t) = \bar{K}$ et \mathfrak{A} tel que $(t) = \mathfrak{A}^{1-s}$, que numériquement tout type d'exemple est possible.

5.3.5. Une condition suffisante de nullité de \bar{L} . — Comme le quotient de Herbrand de T_L est nul on a $|N T_L / T_L^{1-s}| = \frac{|T_K|}{|N_{L/K}(T_L)|}$. Or la norme arithmétique de T_L dans L/K correspond, par la loi de réciprocité d'Artin, à la restriction $T_L \rightarrow T_K$ des automorphismes, et une condition suffisante pour que \bar{L} soit nulle est que cette norme soit surjective. D'où le résultat suivant (sous la conjecture de Leopoldt) :

Théorème 5.7. — *Soit L/K une extension cyclique de degré $p > 2$, kummerienne, p -ramifiée, non globalement cyclotomique et localement cyclotomique en p (cf. théorème 3.1). Alors une condition suffisante pour que $|BP_L^G| = |BP_K|$ est que $L = K$ et que H_K^p/K et L/K soient linéairement disjointes sur K .*

On fera le lien avec le point de vue développé dans [NgPMB], lemme 3.1, proposition 3.2.

6. Conclusion

Le cas trivial où $\mu_K = 1$ (théorème 2.3) permet de construire les p -tours p -ramifiées définies par S. Seo dans [Seo6], lesquelles sont infinies dans le cas où $BP_K = 1$ (sous la conjecture de Leopoldt pour p dans toute p -extension de K), mais dans les autres cas se pose le problème de la propagation des hypothèses faites au premier étage. Une définition plus canonique de ces p -tours est proposée dans [JaS] et repris dans [JaPMB] où est aussi posée la question de leur infinitude (cf. [JaPMB], §8).

Si le p -groupe des classes de K est trivial (ou si $H_K = K$, i.e., $C_K = 1$) on a (cf. lemme 1.4) :

$$BP_K = R_K = \text{tor}_{\mathbb{Z}_p} \log_K(U_K) / \mathbb{Z}_p \log_K(E_K),$$

qui dépend simplement des propriétés congruentielles du groupe des unités de K et grosso modo du régulateur p -adique normalisé usuel de K .

Dans [Gr7] (cf. conjectures 8.9, 8.11), nous avons conjecturé, pour tout p assez grand, la p -rationalité de tout corps de nombres K (cf. § 1.2 (ii)) ; ceci entraînerait la nullité de BP_K pour tout p assez grand indépendamment de toute hypothèse (conjecture de Leopoldt comprise).

Il serait utile d'étudier la « p -rationalité faible », que nous avons introduite dans [Gr6], et qui stipule que BP_K est trivial ; pour K fixé, elle n'est distincte de la p -rationalité que pour un nombre fini de p .

Mais on peut dire, pour conclure cette étude, que c'est bien l'ensemble des invariants T_K qui fait la synthèse des propriétés classiques des classes et unités des corps de nombres K .

Références

- [AS] Angelakis, A. and Stevenhagen, P., *Absolute abelian Galois groups of imaginary quadratic fields*, In : proceedings volume of ANTS-X, UC San Diego 2012, E. Howe and K. Kedlaya (eds), OBS 1 (2013).
- [AT] Artin, E. and Tate, J., *Class field theory*, Benjamin, New York, Amsterdam 1968 ; second edition : Advanced Book Classics, Addison-Wesley Publ. Comp., Redwood City 1990 ; Reprint of the 1990 second edition (2009).
- [BP] Bertrandias, F. et Payan, J.-J., *p -extensions et invariants cyclotomiques*, Ann. Sci. Ec. Norm. Sup. 4, **5**, (1972), 517–548.
- [CK] Carroll, J.E. and Kisilevsky, H., *Initial layers of \mathbb{Z} -extensions of complex quadratic fields*, Compositio Math., **32**, (1976), 157–168.
- [Cha] Charifi, A., *Groupes de torsion attachés aux extensions Abéliennes p -ramifiées maximales (cas des corps totalement réels et des corps quadratiques imaginaires)*, Thèse de 3^e cycle, Mathématiques, Université de Franche-Comté (1982), 50 pp.
- [Gr1] Gras, G., *Class Field Theory. From theory to practice*, SMM, Springer-Verlag 2003 ; second corrected printing 2005.
- [Gr2] Gras, G., *Groupe de Galois de la p -extension abélienne p -ramifiée maximale d'un corps de nombres*, J. reine angew. Math., **333**, (1982), 86–132.
- [Gr3] Gras, G., *Logarithme p -adique et groupes de Galois*, J. reine angew. Math., **343**, (1983), 63–80.
- [Gr4] Gras, G., *Plongements kummeriens dans les \mathbb{Z}_p -extensions*, Compos. Math., **55**, (1985), 383–396.
- [Gr5] Gras, G., *Remarks on K_2 of number fields*, Jour. Number Theory, **23**, (1986), 322–335.
- [Gr6] Gras, G., *On the structure of the Galois group of the Abelian closure of a number field*, Journal de théorie des nombres de Bordeaux, **26**, no. 3 (2014), 635–654.
- [Gr7] Gras, G., *Les p -régulateurs locaux d'un nombre algébrique – Conjectures p -adiques*, Canadian Journal of Mathematics, **68**, (2016), 571–624.
- [Gre] Greenberg, R., *Galois representations with open image*, Annales de Mathématiques du Québec, special volume in honor of Glenn Stevens, **40**, 1, (2016), 83–119.

- [GrJ] Gras, G. et Jaulent, J.-F., *Sur les corps de nombres réguliers*, Math. Z., **202**, (1989), 343–365.
- [Ha] Hajir, F., *Tame pro- p Galois groups : a survey of recent work*, Proceedings of the 9th conference on Algebraic Geometry and Coding Theory, Luminy (2004).
- [HM1] Hajir, F. and Maire, Ch., *On the invariant factors of class groups in towers of number fields*, preprint (2015). Disponible à <http://arxiv.org/pdf/1511.09026v1.pdf>
- [HM2] Hajir, F. and Maire, Ch., *Prime decomposition and the Iwasawa μ -invariant*, preprint (2016). Disponible à <http://front.math.ucdavis.edu/1601.04195>
- [He] Hemard, D., *Modules galoisiens de torsion et plongements dans les Z_p -extensions*, Journal of Number Theory, **30**, 3 (1988), 357–374.
- [Ja1] Jaulent, J.-F., *L'arithmétique des p -extensions* (Thèse d'Etat, Université de Franche-Comté, Besançon), Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 1984/86.
- [Ja2] Jaulent, J.-F., *S -classes infinitésimales d'un corps de nombres algébriques*, Ann. Sci. Inst. Fourier, **34**, (1984), 1–27.
- [Ja3] Jaulent, J.-F., *La Théorie de Kummer et le K_2 des corps de nombres*, J. Théorie des Nombres de Bordeaux, **2**, (1990), 377–411.
- [Ja4] Jaulent, J.-F., *Théorie p -adique globale du corps de classes*, J. Théorie des Nombres de Bordeaux **10**, 2 (1998), 355–397.
- [Ja5] Jaulent, J.-F., *Sur les normes cyclotomiques et les conjectures de Leopoldt et de Gross-Kuz'min*, preprint 2015. Disponible à <http://arxiv.org/pdf/1509.02743.pdf>
- [JaPMB] Jaulent, J.-F., *Sur la capitulation pour le module de Bertrandias-Payan*, dans ce volume.
- [JaM1] Jaulent, J.-F. et Maire, C., *A propos de la tour localement cyclotomique d'un corps de nombres*, Abh. Math. Semin. Univ. Hamburg, **70**, (2000), 239–250 ;
- [JaM2] Jaulent, J.-F. et Maire, C., *Radical hilbertien et tour localement cyclotomique*, Jap. J. Math., New Ser., **28**, 2 (2002), 203–213.
- [JaNg] Jaulent, J.-F. et Nguyen Quang Do, T., *Corps p -rationnels, corps p -réguliers et ramification restreinte*, J. Théorie des Nombres de Bordeaux, **5**, (1993), 343–363.
- [JaS] Jaulent, J.-F. et Soriano, F., *Sur les tours localement cyclotomiques*, Archiv. Math. (1999), 132–140.
- [Ko] Koch, H., *Galois Theory of p -extensions*, Springer Monographs in Mathematics, Springer 2002.
- [Kub] Kubota, T., *Galois group of the maximal abelian extension of an algebraic number field*, Nagoya Math. J., **12**, (1957), 177–189.
- [Mai1] Maire, Ch., *Sur la dimension cohomologique des pro- p -extensions des corps de nombres*, J. Th. des Nombres de Bordeaux, **17**, 2, (2005), 575–606.
- [Mai2] Maire, Ch., *Sur la structure Galoisienne de certaines pro- p -extensions de corps de nombres*, Mathematische Zeitschrift, **267**, (2011), 887–913.
- [Mi] Miki, H., *On the maximal Abelian p -extension of a finite algebraic number field with given ramification*, Nagoya Math. J., **70**, (1978), 183–202.
- [Mo] Movahhedi, A., *Sur les p -extensions des corps p -rationnels*, Math. Nachr., **149**, (1990), 163–176.
- [MoNg1] Movahhedi, A. et Nguyen Quang Do, T., *Sur l'arithmétique des corps de nombres p -rationnels*, Sém. Théorie des Nombres, Paris (1987/89), Progress in Math., **81**, Birkhäuser (1990), 155–200.

- [MoNg2] Movahhedi, A., and Nguyen Quang Do, T., *On universal norms and the first layers of Z_p -extensions of a number field*, Math. Annalen, **362**, (2015), 817–838.
- [Ng1] Nguyen Quang Do, T., *Sur la Z_p -torsion de certains modules galoisiens*, Ann. Inst. Fourier, **36**, (1986), 27–46.
- [Ng2] Nguyen Quang Do, T., *Formations de classes et modules d'Iwasawa*, Noordwijkerhout 1983, Lecture Notes in Math., **1068**, Springer 1984, 167–185.
- [NgPMB] Nguyen Quang Do, T., *Descente galoisienne et capitulation entre modules de Bertrandias–Payan*, dans ce volume.
- [PV] Pitoun, F. and Varescon, F., *Computing the torsion of the p -ramified module of a number field*, Math. Comp., published electronically, **84**, (2015), 371–383.
- [Seo1] Seo, S., *On first layers of Z_p -extensions II*, Acta Arith., **150**, (2011), no. 4, 385–397.
- [Seo2] Seo, S., *On first layers of Z_p -extensions*, Journal of Number Theory, **133**, (2013), 4010–4023.
- [Seo3] Seo, S., *On the Tate module of a number field* (ASARC). Preprint 13-06 (2013). Disponible à http://asarc.kaist.ac.kr/bbs/view.php?board_id=preprint&no=108.
- [Seo4] Seo, S., *On the universal norm group of the global units and the p -units* (preprint, 2014). Disponible à <http://web.yonsei.ac.kr/sgseo/N3.pdf>
- [Seo5] Seo, S., *On the conjectures of Gross and Leopoldt* (ASARC). Disponible à http://asarc.kaist.ac.kr/bbs/view.php?board_id=preprint&no=107
- [Seo6] Seo, S., *On torsion towers of the maximal finitely-ramified Abelian p -extensions* (preprint, private communication, 2015).
- [Th] Thomas H., *Étage initial d'une Z_p -extension*, Manuscripta Mathematica, **81**, 1 (1993), 413–435.
- [Wa] Washington, L.C., *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer enlarged second edition 1997.

18 décembre 2015

Georges Gras, Villa la Gardette, chemin Château Gagnière, F-38520 Le Bourg d'Oisans
E-mail : g.mn.gras@wanadoo.fr