Journal de Théorie des Nombres
de Bordeaux **17** (2005), 575–606

Sur la dimension cohomologique des pro-p-extensions des corps de nombres

par Christian MAIRE

À Georges Gras, pour son soixantième anniversaire
en témoignage de ma très grande reconnaissance

Résumé. Dans ce papier, nous étudions la dimension cohomologique des groupes $G_S := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$, où K_S est la pro-p-extension d'un corps de nombres K, non-ramifiée en dehors d'un ensemble fini de places S de K, et maximale pour ces propriétés. Si cette dimension est bien connue lorsque S contient toutes les places au-dessus de p, elle le semble moins bien dès lors que S ne contient pas toutes ces places. Néanmoins, il est possible d'obtenir des informations quand une $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$ se trouve dans K_S/K. En effet, dans ce cas, une étude du $\mathbb{Z}_p[[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]]$-module $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)^{ab}$ permet de donner des conditions suffisantes pour que le pro-p-groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ soit libre. Si tel est le cas, il s'en déduit que la dimension de G_S est au plus 2. Ici, nous développons une démarche explicite mettant en jeu ces conditions afin de trouver des exemples numériques pour lesquels il est effectivement possible de calculer cette dimension cohomologique.

Abstract. In this paper, we study the cohomological dimension of groups $G_S := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$, where K_S is the maximal pro-p-extension of a number field K, unramified outside a finite set S of places of K. This dimension is well-understood only when S contains all places above p; in the case where only some of the places above p are contained in S, one can still obtain some results if K_S/K contains at least one $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$. Indeed, in that case, the study of the $\mathbb{Z}_p[[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]]$-module $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)^{ab}$ allows one to give sufficient conditions for the pro-p-group $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ to be free. Under the latter condition, the dimension of G_S is at most 2. Here, we develop an explicit strategy for realizing these conditions so as to produce numerical examples for which we effectively compute this cohomological dimension.

Manuscrit reçu le 14 mai 2004.

Introduction

La nature des pro-p-extensions à ramification restreinte d'un corps de nombres K semble complètement différente suivant la quantité de ramification sauvage que l'on autorise. Par exemple, si S est un ensemble fini de places de K ne contenant aucune place au-dessus de p, la conjecture de Fontaine-Mazur (cf. [5], [3], [4], ...) indique que toute représentation continue $\rho : G_S \to \mathrm{Gl}_m(\mathbb{Z}_p)$ a une image finie, où $G_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$, K_S étant donc la pro-p-extension maximale de K non-ramifiée en dehors de S. Alors qu'au contraire, si S contient toutes les places au-dessus de p, l'extension cyclotomique montre que G_S a au moins un quotient p-analytique infini. Autre différence. Quand S contient toutes les places au-dessus de $p > 2$, il est bien connu que la dimension cohomologique de G_S est au plus 2 (cf. [11], [23], ... et pour $p = 2$ cf. [25]). Alors que finalement quand S ne contient aucune place au-dessus de p, peu de résultats ont été établis. Le plus remarquable est certainement celui de Labute [19]. Il donne les premiers exemples de groupes G_S à dimension cohomologique finie. Signalons une généralisation par Schmidt [26] du résultat de Labute ainsi qu'une étude numérique de Boston [2]. Enfin, notons que quand S contient quelques places au-dessus de p, le groupe G_S peut-être pro-p-libre. Ce cas a été étudié par Movahhedi [21], Movahhedi et Nguyen Quang Do [22], Jaulent et Nguyen Quang Do [16], Jaulent et Sauzet [17], ...

Plaçons nous dans la situation où il existe une représentation continue $\rho : G_S \twoheadrightarrow \mathbb{Z}_p$. Posons $\mathrm{K}_\infty := \mathrm{K}_S^{\ker\rho}$. L'extension $\mathrm{K}_\infty/\mathrm{K}$ est une $\mathbb{Z}_p$-extension. Il alors est possible de donner des conditions portant sur le $\mathbb{Z}_p[[X]]$-module $\mathcal{X}_S := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)^{ab}$ pour que le groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ soit pro-p-libre impliquant donc dans ce cas que la dimension du groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$ est au plus 2. C'est ainsi que Wingberg, dans [32], a montré que si $r_1+r_2 = \sum_{\mathfrak{p}\in S}[\mathrm{K}_p : \mathbb{Q}_p]$ et que si l'invariant μ_S du $\mathbb{Z}_p[[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]]$-module $\mathcal{X}_S$ est trivial, alors $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ est libre, (r_1, r_2) étant la signature du corps K. Notons que la première condition est extrêmement forte, elle appauvrit le groupe G_S puisque, dans cette situation, le $\mathbb{Z}_p[[X]]$-rang de $\mathcal{X}_S$ est trivial (ou encore, l'invariant ρ_S de $\mathcal{X}_S$ est trivial).

Le but de ce papier est la mise en place d'une stratégie permettant de trouver des exemples où le groupe G_S est assez gros et est de dimension cohomologique finie (en fait, au plus 2). En particulier, nous voulons que le $\mathbb{Z}_p[[X]]$-rang du module $\mathcal{X}_S$ soit non nul.

Nous aurons ainsi en permanence à l'esprit l'idée de rendre la démarche la plus explicite possible. Ceci nous permettra de détailler deux exemples pour lesquels

(i) G_S est de dimension cohomologique 2 (et $S \subsetneq S_p$) ;
(ii) il existe une suite exacte

$$1 \longrightarrow H_S \longrightarrow G_S \longrightarrow \mathbb{Z}_p \longrightarrow 1$$

où H_S^{ab} s'injecte avec un conoyau fini dans $\mathbb{Z}_p[[X]]^{\rho_S}$, avec $\rho_S \geq 1$.

Reprenons succintement les points clefs de notre méthode. Essentiellement tout tourne autour de l'invariant μ_S. Nous voulons obtenir des situations où le groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ est libre. Pour ce faire, il suffit de vérifier que d'une part une certaine condition arithmétique est satisfaite pour le corps K et que d'autre part l'invariant μ_S est trivial. Le premier point est aisé à tester numériquement. Quant au second, il peut être vérifié après quelques calculs dans la $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$. Mais pour ce faire, il est nécessaire de déterminer explicitement les étages de celle-ci. Ceci se fera à l'aide d'un logarithme p-adique construit sur les idéaux de K, utilisant ainsi des travaux de Gras [7], [8], [9]. Ensuite, pour vérifier la trivialité de μ_S, on est tenté d'utiliser le lemme de Nakayama. Malheureusement, une application brutale de ce lemme au module $\mathcal{X}_S$ tue les invariants d'Iwasawa ρ_S et μ_S simultanément, appauvrissant donc le groupe G_S. Pour remédier à ceci, et c'est le second point clef de notre méthode, nous appliquerons le lemme de Nakayama sur la partie de torsion du $\mathbb{Z}_p[[X]]$-module $\mathcal{X}_S$. Il faudra alors s'assurer qu'une certaine condition arithmétique est satisfaite le long de $\mathrm{K}_\infty/\mathrm{K}$. Ce sont des résultats de dualité dans $\mathrm{K}_\infty/\mathrm{K}$ qui permettront de vérifier cette condition et ce, après un nombre fini de calculs.

Dans la section 1, nous introduisons les principales notations. Dans la section 2, nous rappellerons les résultats standards de cohomologie des pro-p-groupes ainsi que ceux de théorie d'Iwasawa dont nous aurons besoin. Dans la section 3, nous développerons les notions de S-conditions de type "Leopoldt". Ces conditions de deux types, arithmétiques et cohomologiques, sont fondamentales dans la recherche d'exemples. La notion de S-condition cohomologique apporte des résultats sur la structure de G_S tandis que la notion de S-condition arithmétique se prête parfaitement aux calculs. Nous nous efforcerons ainsi de trouver le maximum de liens entre celles-ci. Dans la section 4, nous présenterons les résultats nécessaires pour effectuer les calculs dans une $\mathbb{Z}_p$-extension, en particulier le logarithme défini par Gras. Dans la section 5, nous présenterons des résultats de dualité le long d'une $\mathbb{Z}_p$-extension quelconque. Enfin, dans la section 6, nous présenterons deux exemples.

Pour finir, notons qu'un autre contrôle possible de la ramification sauvage est celui de la "profondeur". C'est une philosophie assez différente. Nous renvoyons à [12] pour plus détails.

L'ensemble des calculs ont été effectués avec GP-PARI [1].

Remerciements.

Ce travail a vu le jour lors de mon passage dans la chaire de Structures Algébriques et Géométriques de l'EPF Lausanne. Il a été terminé lors de ma visite à University of Massachussets, Amherst. Je remercie Éva Bayer et Farshid Hajir pour leur chaleureux accueil.

Enfin, je tiens également à remercier Thong Nguyen Quang Do pour ses remarques à propos de ces questions de dimension cohomologique.

1. Notations

Fixons un corps de nombres K ainsi qu'un nombre premier p. Les objets suivants interviendront tout au long de ce papier :

- $S_p = \{\mathfrak{p} \in Pl_{\mathrm{K}}, \mathfrak{p}|p\}$;
- S et T désignerons deux ensembles disjoints de places de K. On supposera S contenu dans S_p ;
- E_{K} désignera le groupe des unités de l'anneau des entiers $\mathcal{O}_{\mathrm{K}}$ de K ; plus généralement $E_{\mathrm{K}}^T := \{\varepsilon \in \mathcal{O}_{\mathrm{K}}, \mathrm{v}_{\mathfrak{p}}(\varepsilon) = 0, \forall \mathfrak{p} \notin T\}$ sera le groupe des T-unités de $\mathcal{O}_{\mathrm{K}}$;
- K_S désignera la pro-p-extension maximale de K, non-ramifiée en dehors de S (les places réelles restent réelles) ; $G_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$;
- $\widetilde{\mathrm{K}_S}$ désignera le compositum de toutes les $\mathbb{Z}_p$-extensions de K contenues dans K_S;
- K_∞ désignera une $\mathbb{Z}_p$-extension de K contenue dans K_S/K; $H_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$; $\chi_S = H_S^{ab} = H_S/[H_S; H_S]$.
- K_∞ étant fixé, K_n sera l'unique sous-corps de $\mathrm{K}_\infty/\mathrm{K}$ de degré p^n sur K;
- $\delta_S = \sum_{\mathfrak{p}\in S}[K_{\mathfrak{p}} : \mathbb{Q}_p]$ désignera le degré de S;
- $\widetilde{S}$ désignera l'ensemble des places de K qui sont totalement décomposées dans $\mathrm{K}_\infty/\mathrm{K}$; $\widetilde{s} = \#\widetilde{S}$;
- $S_n = \{\mathfrak{P} \in Pl_{\mathrm{K}_n}, \mathfrak{P}|\mathfrak{p}, \mathfrak{p} \in S\}$, $s_n = \#S_n$;
- $\mathrm{K}_{n,S}^T$ désignera la pro-p-extension maximale de K_n non-ramifiée en dehors de S et où toutes les places de T sont décomposées ; $G_{n,S}^T = \mathrm{Gal}(\mathrm{K}_{n,S}^T/\mathrm{K})$;

- $\mathrm{K}_{n,T}^{S}$ désignera la pro-p-extension maximale de K_n non-ramifiée en dehors de T et où toutes les places de S sont décomposées ; $G_{n,T}^{S} = \mathrm{Gal}(\mathrm{K}_{n,T}^{S}/\mathrm{K})$;
- $\mathrm{K}_{n,S}^{T,ab}$ désignera la pro-p-extension *abélienne* maximale de K_n contenue dans K_S^T ; $G_{n,S}^{T,ab} = \mathrm{Gal}(\mathrm{K}_{n,S}^{T,ab}/\mathrm{K})$;
- $\mathrm{K}_{n,T}^{S,ab}$ est la pro-p-extension *abélienne* maximale de K_n contenue dans $\mathrm{K}_{n,T}^{S}$; $G_{n,T}^{S,ab} = \mathrm{Gal}(\mathrm{K}_{n,T}^{S,ab}/\mathrm{K})$;
- $\mathrm{L}_S^T = \bigcup_n \mathrm{K}_{n,S}^{T,ab}$; $\mathcal{X}_S^T = \mathrm{Gal}(\mathrm{L}_S^T/\mathrm{K}_\infty)^{ab}$; $\mathrm{L}_T^S = \bigcup_n \mathrm{K}_{n,T}^{S,ab}$; $\mathcal{X}_T^S = \mathrm{Gal}(\mathrm{L}_T^S/\mathrm{K}_\infty)^{ab}$
- $(\rho_T^S, \mathrm{r}_T^S, \lambda_T^S)$ (respectivement $(\rho_S^T, \mathrm{r}_S^T, \lambda_S^T)$) désignerons les invariants d'Iwasawa du $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})$-module $\mathcal{X}_S^T$ (resp. $\mathcal{X}_T^S$) (cf. section 3);
- $U_S^1 = \prod_{\mathfrak{p}\in S} U_{\mathfrak{p}}^1$, où $U_{\mathfrak{p}}^1$ est le groupe des unités principales du complété $\mathrm{K}_{\mathfrak{p}}$ de K en $\mathfrak{p}$; le morphisme de $\mathbb{Z}_p$-modules $\varphi_S : \mathbb{Z}_p \otimes_{\mathbb{Z}} E_{\mathrm{K}} \to U_S^1$ est le morphisme naturel de plongements. Plus généralement, $U_{S_n}^1 = \prod_{\mathfrak{p}\in S_n} U_{\mathfrak{p}}^1$ et $\varphi_{n,S} : \mathbb{Z}_p \otimes_{\mathbb{Z}} E_{\mathrm{K}_n} \to U_{S_n}^1$. Rappelons que le $\mathbb{Z}_p$-rang de $G_S^{T,ab}$ est exactement le $\mathbb{Z}_p$-rang du conoyau de $\varphi_S^T : \mathbb{Z}_p \otimes_{\mathbb{Z}} E_{\mathrm{K}}^T :\to \prod_{\mathfrak{p}\in S} U_{\mathfrak{p}}^1$, (cf. [7],...)
- Si A est un pro-p-groupe, on dénotera par : $d_pA = \dim_{\mathbb{F}_p} A/A^p[A;A]$ le p-rang de $A/[A;A]$, par $\mathrm{rk}_{\mathbb{Z}_p}A$ le $\mathbb{Z}_p$-rang de $A/[A;A]$ et par $\mathrm{Tor}_{\mathbb{Z}_p}(A)$ la partie de torsion de $A/[A;A]$.
- Les polynômes ω_n et $\omega_{m,n}$ de l'algèbre d'Iwasawa $\Lambda := \mathbb{Z}_p[[X]]$ sont définis comme suit : $\omega_n = (1+X)^{p^n} - 1$, et pour $m > n$, $\omega_{m,n} = \omega_m/\omega_n$. Le polynôme $\omega_{n+1,n}$ est irréductible de degré $(p-1)p^n$.
- Enfin, si $\mathcal{X}$ est un Λ-module, et $f \in \Lambda$, $\mathcal{X}^f$ dénotera le sous-Λ-module de $\mathcal{X}$ constitué des éléments de $\mathcal{X}$ annulés par f.

2. Rappels

2.1. Dimension cohomologique et suite spectrale. L'ensemble des résultats de ce paragraphe sont issus de [18], [23], [29], ...

2.1.1. Rappelons, pour commencer, la notion de dimension cohomologique.

Soit G un pro-p-groupe. On dit que G est de dimension cohomologique $\mathrm{cd}(G) = m$, si le groupe $H^{m+1}(G, \mathbb{F}_p)$ est trivial et si $H^m(G, \mathbb{F}_p)$ ne l'est pas.

Pour déterminer un majorant de la dimension cohomologique d'un pro-p-groupe, trois critères sont bien connus.

Proposition 2.1. *1) Soit H un sous-groupe fermé d'un pro-p-groupe G. Alors* $\mathrm{cd}(H) \leq \mathrm{cd}(G)$. *Il y a égalité lorsque H est d'indice fini et* $\mathrm{cd}(G) < \infty$.

2) Soit H un sous-groupe fermé et distingué d'un pro-p-groupe G. Alors $\mathrm{cd}(G) \leq \mathrm{cd}(G/H) + \mathrm{cd}(H)$. *Il y a égalité lorsque cd(G/H),* $\mathrm{cd}(H)$ *et* $H^n(H, \mathbb{F}_p)$ *sont finis, où* $n = \mathrm{cd}(H)$.

3) Pour un pro-p-groupe G et lorsque celle-ci a un sens, notons par $\chi_n(G)$ *la caractéristique d'Euler-Poincaré tronquée à l'ordre n. Si cette caractéristique est multiplicative pour les sous-groupes ouverts de G, c'est-à-dire si pour tout sous-groupe ouvert U de G,* $\chi_n(U) = (G : U)\chi_n(G)$, *alors la dimension cohomologique de G est au plus n.*

À ce stade, il convient de citer un résultat de Schmidt [25] généralisant le point 3 de la proposition précédente.

Proposition 2.2. *S'il existe une constante c telle que pour tout sous-groupe ouvert U d'un pro-p-groupe infini G, il vient :* $(-1)^n\chi_n(U) + c \geq (-1)^n(G : U)\chi_n(G)$, *alors la dimension cohomologique de G est au plus n.*

2.1.2. Soit $\mathcal{C}$ la catégorie des groupes abéliens localement compacts. Pour un groupe $M \in \mathcal{C}$, notons par M^* le dual de Pontryagin de M : c'est le groupe $\mathrm{Hom}(M, \mathbb{R}/\mathbb{Z})$ des homomorphismes continus de M vers $\mathbb{R}/\mathbb{Z}$. On rappelle que cette dualité est un foncteur contravariant et que pour $M \in \mathcal{C}$, $M \simeq (M^*)^*$. Cette dualité transforme les groupes discrets en groupes compacts, les groupes divisibles en groupes sans torsion. Lorsque M est un pro-p-groupe, on a $\mathrm{Hom}(M, \mathbb{R}/\mathbb{Z}) \simeq \mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

Proposition 2.3. *Soit G un pro-p-groupe et A un G-module compact. Alors, pour tout $n \geq 0$,*

$$H^n(G, A^*) \simeq H_n(G, A)^*.$$

Pour $n = 0$, cette égalité s'écrit :

$$(A_G)^* \simeq (A^*)^G.$$

On arrive ainsi à une conséquence bien connue du lemme de Nakayama :

Proposition 2.4. *Pour $G \simeq \mathbb{Z}_p$ et tout G-module discret A, on a $A = 0$ si et seulement si $A^G = 0$.*

Rappelons une équivalence là aussi bien connue pour caractériser la liberté d'un pro-p-groupe.

Proposition 2.5. *Un pro-p-groupe non trivial G est libre (*$\mathrm{cd}(G) = 1$*) si et seulement si, $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ et G^{ab} est sans torsion.*

Preuve. Partons de la suite exacte :

$$1 \longrightarrow \mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p\mathbb{Z}_p \longrightarrow 1$$

qui après passage à l'homologie donne

$$\cdots H_2(G, \mathbb{Z}_p) \xrightarrow{p} H_2(G, \mathbb{Z}_p) \longrightarrow H_2(G, \mathbb{F}_p) \longrightarrow H_1(G, \mathbb{Z}_p) \xrightarrow{p} H_1(G, \mathbb{Z}_p) \cdots$$

ou encore

$$H_2(G,\mathbb{Z}_p)/p \hookrightarrow H_2(G,\mathbb{F}_p) \longrightarrow G^{ab}[p] \longrightarrow 1.$$

Il vient ainsi $d_pH^2(G,\mathbb{F}_p) = d_pH_2(G,\mathbb{Z}_p) + d_pG^{ab}[p]$. L'équivalence est alors immédiate. □

2.1.3. Partons de la suite exacte de pro-p-groupes

$$1 \longrightarrow H \longrightarrow G \longrightarrow \Gamma \longrightarrow 1,$$

avec $\Gamma \simeq \mathbb{Z}_p$.

Lorsque A est un Γ-module de p-torsion, on sait que $H^1(\Gamma,A) \simeq A_\Gamma$ (cf. par exemple [32], proposition 1.6.3, chapitre I).

Alors, la suite spectrale de Hochschild-Serre appliquée à la précédente suite exacte donne :

Proposition 2.6.

$$1 \longrightarrow H^1(\Gamma,H^1(H,\mathbb{Q}_p/\mathbb{Z}_p)) \longrightarrow H^2(G,\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^2(H,\mathbb{Q}_p/\mathbb{Z}_p)^\Gamma \longrightarrow 1,$$

où $H^1(\Gamma,H^1(H,\mathbb{Q}_p/\mathbb{Z}_p))$ *s'identifie à* $\left((H^{ab})^*\right)_\Gamma$.

Ce qui permet d'en déduire le corollaire suivant :

Corollaire 2.1. *La trivialité du groupe* $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p)$ *implique la trivialité de* $H^2(H,\mathbb{Q}_p/\mathbb{Z}_p)$.

Preuve. On utilise la proposition 2.6 puis la proposition 2.4 appliquée à $H^2(H,\mathbb{Q}_p/\mathbb{Z}_p)$. □

2.2. L'algèbre d'Iwasawa. Soit $\Lambda := \mathbb{Z}_p[[X]]$ l'algèbre d'Iwasawa topologiquement isomorphe à $\mathbb{Z}_p[[\Gamma]] := \varprojlim \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$, où $\Gamma =< \gamma >\simeq \mathbb{Z}_p$ et où $\gamma \to X+1$. Rappelons que si $\mathcal{X}$ est un Λ-module de type fini, il existe des polynômes distingués *irréductibles* $f_i \in \mathbb{Z}_p[X]$, des entiers a_i, b_i, et $\rho_\mathcal{X}$ tels que $\mathcal{X}$ est pseudo-isomorphe à

$$\mathcal{E} = \Lambda^{\rho_\mathcal{X}} \oplus \bigoplus_{i=1,\cdots,\mathrm{r}_\mathcal{X}} \Lambda/(p^{a_i}) \oplus \bigoplus_i \Lambda/(f_i^{b_i})$$

(c'est à dire, qu'il existe un morphisme de Λ-modules ϕ de $\mathcal{X}$ vers $\mathcal{E}$ à noyau et conoyau finis). Les entiers $\lambda_\mathcal{X} = \sum_i b_i \deg(f_i)$, $\mu_\mathcal{X} = \sum_{i=1}^{\mathrm{r}_\mathcal{X}} a_i$ et $\rho_\mathcal{X}$ sont appelés invariants d'Iwasawa de $\mathcal{X}$.

Le polynôme $P_\mathcal{X} = \prod_i f_i^{b_i}$ est appelé polynôme caractéristique de $\mathcal{X}$.

Ce théorème de structure permet de donner des informations sur le comportement du p-rang de certains quotients de $\mathcal{X}$ le long de $\mathrm{K}_\infty/\mathrm{K}$.

Lemme 2.1. *Soient* $\mathcal{X}$ *un* Λ*-module de type fini, pseudo-isomorphe à* $\mathcal{E}$*, et* $\mathcal{Y}$ *un sous-*Λ*-module de* $\mathcal{X}$ *tels que le* $\mathbb{Z}_p$*-module* $\mathcal{X}/\mathcal{Y}$ *soit de type fini. Fixons un entier* $m > 0$. *Alors*

(i) $d_p\mathcal{X}/\omega_{n,m}\mathcal{Y} = p^n(\rho_\mathcal{X} + \mathrm{r}_\mathcal{X}) + O(1)$;
(ii) $\mathrm{rk}_{\mathbb{Z}_p}\mathcal{X}/\omega_{n,m}\mathcal{Y} = p^n\rho_\mathcal{X} + O(1)$;
(iii) $\mathrm{rk}_{\mathbb{Z}_p}\mathcal{X}/\omega_n\mathcal{X} = p^n\rho_\mathcal{X} + \sum_i \mathrm{rk}_{\mathbb{Z}_p}\Lambda/(f_i, \omega_n)$

Preuve. Nous nous contenterons de montrer le point (i). Partons de la suite exacte

$$1 \longrightarrow A \longrightarrow \mathcal{X} \xrightarrow{\phi} \mathcal{E} \longrightarrow B \longrightarrow 1$$

où A et B sont deux Λ-modules finis. Cette suite exacte devient

$$\frac{B_0}{\omega_{n,m}\mathcal{Y} + p\mathcal{X}} \hookrightarrow \frac{\mathcal{X}}{\omega_{n,m}\mathcal{Y} + p\mathcal{X}} \longrightarrow \frac{\mathcal{E}}{\omega_{n,m}\mathcal{E} + p\mathcal{E}} \longrightarrow \longrightarrow \frac{\mathcal{E}}{\phi(\mathcal{X}) + \omega_{n,m}\mathcal{E} + p\mathcal{E}} \longrightarrow 1,$$

où $B_0 = \phi^{-1}(\omega_{n,m}\mathcal{E} + p\mathcal{E})$. Clairement, le dernier membre de cette suite est fini. Il reste à évaluer le premier membre. Pour cela, soit l'homomorphisme de Λ-modules

$$\begin{array}{rcl} F : B_0/(\omega_{n,m}\mathcal{Y} + p\mathcal{X}) & \to & \omega_{n,m}\mathcal{E} + p\mathcal{E}/(\phi(\omega_{n,m}\mathcal{Y}) + p\phi(\mathcal{X})) \\ \bar{x} & \mapsto & \overline{\phi(x)} \end{array}$$

Alors $\ker F$ est exactement $(\omega_{n,m}\mathcal{Y} + p\mathcal{X} + \ker\phi)/(\omega_{n,m}\mathcal{Y} + p\mathcal{X})$ et est donc fini.

Maintenant, la suite exacte

$$1 \longrightarrow \frac{\phi(\mathcal{X})}{\phi(\mathcal{Y})} \longrightarrow \frac{\mathcal{E}}{\phi(\mathcal{Y})} \longrightarrow \frac{\mathcal{E}}{\phi(\mathcal{X})} \longrightarrow 1$$

indique que $\mathcal{E}/\phi(\mathcal{Y})$ est de type fini sur $\mathbb{Z}_p$ (car $\mathcal{X}/\mathcal{Y}$ l'est). Il en est ainsi de même pour l'image de F (F est surjectif). En conclusion, $d_p\mathcal{X}/\omega_{n,m}\mathcal{Y} = d_p\mathcal{E}/\omega_{n,m}\mathcal{E} + O(1)$, d'où le résultat. □

Lemme 2.2. *Soient $\mathcal{X}$ un Λ-module de type fini, d'invariants $(\rho_\mathcal{X}, \mathrm{r}_\mathcal{X}, \lambda_\mathcal{X})$, et $\mathcal{Y}$ un sous-Λ-module de $\mathcal{X}$.*

1) Supposons qu'il existe deux entiers $m > n \geq 0$ tels que $\mathcal{X}/\mathcal{Y} = \mathcal{X}/\omega_{m,n}\mathcal{Y}$. Alors $\mathcal{X} = \mathcal{X}/\mathcal{Y}$. En particulier, si $\mathcal{X}/\mathcal{Y}$ est de type fini sur $\mathbb{Z}_p$, on a $\rho_\mathcal{X} = \mathrm{r}_\mathcal{X} = 0$ et $\lambda_\mathcal{X} = \dim_{\mathbb{Q}_p}\left(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{X}/\mathcal{Y}\right)$.

2) Supposons qu'il existe deux entiers $m > n \geq 0$ tel que $d_p\mathcal{X}/\omega_{m,n}\mathcal{Y} = d_p\mathcal{X}/\mathcal{Y}$. Alors $\mathcal{X}/p\mathcal{X} = \mathcal{X}/(p\mathcal{X} + \mathcal{Y})$. En particulier, si $\mathcal{X}/\mathcal{Y}$ est de type fini sur $\mathbb{Z}_p$, $\rho_\mathcal{X} = \mathrm{r}_\mathcal{X} = 0$.

Preuve. 1) Par hypothèse $\omega_{m,n}\mathcal{Y} = \mathcal{Y}$. Comme $\omega_{m,n}$ appartient à l'idéal maximal (p, T), par le lemme de Nakayama, $\mathcal{Y} = 0$. Ainsi $\mathcal{X}/\mathcal{Y} = \mathcal{X}$. Lorsque $\mathcal{X}/\mathcal{Y}$ est de type fini sur $\mathbb{Z}_p$, le p-rang de $\mathcal{X}$ est alors fini et par conséquent $\mu_\mathcal{X} = \rho_\mathcal{X} = 0$.

2) Par hypothèse, on a l'isomorphisme $\mathcal{X}/(\omega_{m,n}\mathcal{Y} + p\mathcal{X}) \simeq \mathcal{X}/(\mathcal{Y} + p\mathcal{X})$. Ainsi, $\omega_{m,n}\mathcal{Y} + p\mathcal{X} = \mathcal{Y} + p\mathcal{X}$. Par le lemme de Nakayama, le Λ-module

$(\mathcal{Y}+p\mathcal{X})/p\mathcal{X}$ est trivial et ainsi $\mathcal{Y}\subset p\mathcal{X}$. Par conséquent, $\mathcal{X}/(\mathcal{Y}+p\mathcal{X}) = \mathcal{X}/p\mathcal{X}$. Lorsque $\mathcal{X}/\mathcal{Y}$ est de type fini sur $\mathbb{Z}_p$, on trouve bien $\mu_{\mathcal{X}} = \rho_{\mathcal{X}} = 0$.□

2.2.1. *Modules d'Iwasawa et dimension cohomologique.* Soient G un pro-p-groupe et, H un sous-groupe fermé et distingué de G vérifiant $G/H = \Gamma \simeq \mathbb{Z}_p$. Rappelons que $\mathcal{X} = H^{ab}$ est un Λ-module (par rapport à Γ).

Lemme 2.3. *Lorsque $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p)$ est trivial, $\mathcal{X}$ n'a pas de sous-module fini.*

Preuve. Puisque $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p)$ est trivial, la proposition 2.6 indique que $(\mathcal{X})^\Gamma$ est trivial. Ainsi, le sous-module A^Γ des invariants par Γ d'un sous-module fini A de $\mathcal{X}$ est trivial, ce qui implique que A est trivial (d'après la proposition 2.4). □

Cette proposition permet alors de montrer la proposition suivante :

Proposition 2.7. *Sous les conditions $\mathrm{r}_{\mathcal{X}} = 0$ et $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p) = 0$, le pro-p-groupe H est libre. Ainsi, $\mathrm{cd}_p(G) \leq 2$.*

Preuve. Supposons $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p)$ trivial. D'après le corollaire 2.1, nous avons $H^2(H,\mathbb{Q}_p/\mathbb{Z}_p) = 0$. D'autre part, d'après le lemme précédent, $\mathcal{X} = H^{ab}$ n'a pas de sous-module fini. Ainsi

$$\mathcal{X} \hookrightarrow \Lambda^{\rho_{\mathcal{X}}} \oplus \bigoplus_{i=1,\cdots,\mathrm{r}_{\mathcal{X}}} \Lambda/(p^{a_i}) \oplus \bigoplus_i \Lambda/(f_i).$$

Si de plus $\mathrm{r}_{\mathcal{X}}$ est aussi trivial, alors

$$\mathcal{X} \hookrightarrow \Lambda^{\rho_{\mathcal{X}}} \oplus \bigoplus_i \Lambda/(f_i)$$

et ainsi $\mathcal{X}$ est sans $\mathbb{Z}_p$-torsion. D'après la proposition 2.5, le pro-p-groupe H est libre et par conséquent $\mathrm{cd}(G) \leq \mathrm{cd}(H) + \mathrm{cd}(\mathbb{Z}_p) \leq 2$. □

Remarque. (i) Lorsque H est de type fini et non trivial ou que G^{ab} a de la torsion, la dimension cohomologique $\mathrm{cd}_p(G)$ de G est exactement 2.

(ii) Lorsque $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p)$ est nul, il vient également : $\rho_{\mathcal{X}} = -\chi_2(G) := 1 - d_pG^{ab} + d_pH^2(G,\mathbb{F}_p)$.

2.2.2. *Modules d'Iwasawa et corps de nombres.* Reprenons les notations de la section 1. Soient K un corps de nombres, S un ensemble de places de K au-dessus de p, T un ensemble fini de places de K disjoint de S, et K_∞ une $\mathbb{Z}_p$-extension de K contenue dans K_S.

Lemme 2.4. *Soit K_n le sous corps de K_∞ de degré p^n sur* K. *Lorsque $\widetilde{T} = T$ (c'est-à-dire les places de T sont totalement décomposées dans $\mathrm{K}_\infty/\mathrm{K}$), il vient*

$$\mathrm{Gal}(\mathrm{K}_{n,S}^{T,ab}/\mathrm{K}_\infty) \simeq \mathcal{X}_S^T/\omega_n\mathcal{X}_S^T$$

Preuve. Contentons-nous de montrer le lemme pour $T = \emptyset$. Soit $\mathrm{K}_{n,S}^{ab}$ l'extension abélienne maximale de K_n contenue dans K_S. C'est aussi la pro-p-extension abélienne maximale de K_n non-ramifiée en dehors de S. Soit F_n le corps maximal fixé par $\omega_n\mathcal{X} = ((1+X)^{p^n}-1)\mathcal{X}$.

Le groupe de Galois $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}_n) =< \gamma^{p^n} >$ agit trivialement sur le quotient $\mathcal{X}/\omega_n\mathcal{X}$ (se rappeler : $\gamma \leftrightarrow X+1$). Ainsi, $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}_n)$ étant cyclique, l'extension F_n/K_n est abélienne. Par maximalité de $\mathrm{K}_{n,S}^{ab}$, on a $F_n \subset \mathrm{K}_{n,S}^{ab}$. L'inclusion inverse est évidente : $\mathrm{K}_{n,S}^{ab}/\mathrm{K}_n$ étant abélienne, $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}_n)$ agit trivialement sur $\mathrm{Gal}(\mathrm{K}_{n,S}^{ab}/\mathrm{K}_\infty)$. Ainsi $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}_n)$ est un quotient de $\mathcal{X}/\omega_n$ et $\mathrm{K}_{n,S}^{ab} \subset F_n$. □

Soit K_{n_0} un corps de nombres de $\mathrm{K}_\infty/\mathrm{K}$ où toutes les places ramifiées et inertes de S et T dans l'extension $\mathrm{K}_\infty/\mathrm{K}$ le sont totalement dans $\mathrm{K}_\infty/\mathrm{K}_{n_0}$.

Lemme 2.5. *(i) Il existe un sous-*Λ*-module* $\mathcal{Y}$ *de* $\mathcal{X}_T^S$ *tel que pour* $n \geq n_0$*,*

$$\mathrm{Gal}(\mathrm{K}_{n,T}^{S,ab}/\mathrm{K}_n) \simeq \mathcal{X}_T^S/\omega_{n,n_0}\mathcal{Y}$$

(ii) Lorsque T *est différent de* $\widetilde{T}$*, il existe un sous-*Λ*-module* $\mathcal{Y}$ *de* $\mathcal{X}_S^T$ *tel que pour* $n \geq n_0$*,*

$$\mathrm{Gal}(\mathrm{K}_{n,S}^{T,ab}/\mathrm{K}_n) \simeq \mathcal{X}_S^T/\omega_{n,n_0}\mathcal{Y}$$

Preuve. Il suffit de reprendre la preuve du lemme 13.18 de [31] tout en notant que : (i) toute extension K'/K de $\mathrm{L}_T^S/\mathrm{K}$, $S|\widetilde{S}$-décomposée, est S-décomposée ; (ii) toute extension K'/K de $\mathrm{L}_S^T/\mathrm{K}$, $T|\widetilde{T}$-décomposée, est T-décomposée. □

Remarque. Le lemme de Nakayama indique que les Λ-modules $\mathcal{X}_T^S$ et $\mathcal{X}_S^T$ sont de type fini.

Proposition 2.8. *Notons par* $G_{n,S}$ *(reps.* $G_{n,T}^S$*) le groupe de Galois* $\mathrm{Gal}(\mathrm{K}_{n,S}/\mathrm{K}_n)$ *(resp.* $\mathrm{Gal}(\mathrm{K}_{n,T}^S/\mathrm{K}_n)$*).*

(i) *S'il existe deux entiers* $m > n \geq 0$ *pour lesquels* $d_pG_{m,S} = d_pG_{n,S}$*, alors* $\rho_S = \mathrm{r}_S = 0$*;*

(ii) *S'il existe deux entiers* $m > n \geq n_0$ *pour lesquels* $d_pG_{n,T}^S = d_pG_{m,T}^S$*, alors* $\rho_T^S = \mathrm{r}_T^S = 0$*.*

Preuve. Ces deux points sont une conséquence immédiate des lemmes 2.2, 2.4 et 2.5. □

3. Les conditions de type "Leopoldt"

3.1. Quelques évidences.

Définition et Proposition. Les deux assertions suivantes sont équivalentes

(1) $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} G_S^{ab}$ est un $\mathbb{Q}_p$-espace vectoriel de dimension $\delta_S - (r_1 + r_2 - 1)$
(2) Le morphisme de $\mathbb{Z}_p$-modules $\varphi_S : \mathbb{Z}_p \otimes_{\mathbb{Z}_p} E_K \to \prod_{\mathfrak{p} \in S} U_{\mathfrak{p}}^1$ est injectif

où $\delta_S = \sum_{\mathfrak{p} \in S} [\mathrm{K}_{\mathfrak{p}} : \mathbb{Q}_p]$. Lorsque ces conditions sont remplies, nous disons que K vérifie la *S-condition arithmétique*.

Définition. Lorsque le groupe $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial (ou encore quand $H_2(G_S, \mathbb{Z}_p) = 0$), nous disons que K vérifie la *S-condition cohomologique*.

Lorsque S contient l'ensemble des places au-dessus de p, il y a équivalence entre la S-condition cohomologique et la S-condition arithmétique (cf. par exemple [24]). Pour le cas général, nous avons besoin du lemme suivant (par exemple, cf. [20], [7] appendice) :

Lemme 3.1.

$$d_p H_2(G_S, \mathbb{Z}_p) \leq \mathrm{rk}_{\mathbb{Z}_p} E_{\mathrm{K}} - \mathrm{rk}_{\mathbb{Z}_p} \mathrm{Im}(\varphi_S)$$

C'est plus ou moins une conséquence du lemme 3.2 à suivre.

Proposition 3.1. *La S-condition arithmétique implique la S-condition cohomologique.*

Preuve. Si la S-condition arithmétique est vérifiée, alors $d_p H_2(G_S, \mathbb{Z}_p) = 0$. Le lemme de Nakayama appliqué au $\mathbb{Z}_p$-module compact $H_2(G_S, \mathbb{Z}_p)$ permet de conclure. □

Notons que, comme pour la conjecture de Leopoldt, nous pouvons avancer deux S-conditions faibles.

Définition. Soient $\mathrm{K}_\infty/\mathrm{K}$ une $\mathbb{Z}_p$-extension de K contenue dans K_S et $H_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$. Nous disons que le couple (K, S) vérifie

- la *S-condition arithmétique faible* de Leopoldt pour $\mathrm{K}_\infty/\mathrm{K}$, si le p-rang du noyau de $\varphi_{n,S} : \mathbb{Z}_p \otimes_{\mathbb{Z}} E_{\mathrm{K}_n} \to U_{S_n}$ est borné ;
- la *S-condition cohomologique faible* de Leopoldt pour $\mathrm{K}_\infty/\mathrm{K}$, si le groupe $H_2(H_S, \mathbb{Z}_p)$ est trivial.

Proposition 3.2. *1) La S-condition cohomologique forte entraine la S-condition cohomologique faible (pour toutes les $\mathbb{Z}_p$-extensions $\mathrm{K}_\infty/\mathrm{K}$, contenue dans K_S/K).*

2) La S-condition arithmétique (resp. cohomologique) faible pour $\mathrm{K}_\infty/\mathrm{K}$ implique que le p-rang des groupes $H_2(G_{n,S}, \mathbb{Z}_p)$ est borné ($\bigcup \mathrm{K}_n = \mathrm{K}_\infty$).

3) Si $\mathrm{cd}_p(G_S) \leq 2$, la S-condition arithmétique faible entraine la S-condition cohomologique faible.

4) La S-condition arithmétique faible équivaut à $\rho_S = \delta_S - (r_1 + r_2)$.

Preuve. 1) La S-condition cohomologique se traduit par la trivialité du groupe $H^2(G_S/\mathbb{Q}_p/\mathbb{Z}_p)$. Maintenant la suite exacte de la proposition 2.6 montre que $H^2(H_S,\mathbb{Q}_p/\mathbb{Z}_p)^\Gamma$ est trivial. Il en est de même pour $H^2(H_S,\mathbb{Q}_p/\mathbb{Z}_p)$.

2) La condition $H_2(H_S,\mathbb{Z}_p)=0$ implique $H_2(G_{n,S},\mathbb{Z}_p)\simeq \mathcal{X}_S^{\omega_n}$. Ainsi, la suite des p-rang des groupes $H_2(G_{n,S},\mathbb{Z}_p)$ est bornée.

Enfin, le lemme 3.1 indique que si le S-défaut de Leopoldt est borné dans $\mathrm{K}_\infty/\mathrm{K}$ par m, alors le p-rang de $H_2(G_{n,S},\mathbb{Z}_p)$ est aussi borné par m.

3) On s'inspire de [23], chapitre V, lemme 5.6.13. Puisque G_S est de dimension cohomologique au plus 2, le groupe $H_2(H_S,\mathbb{Z}_p)$ est un Λ-module libre. Si la S-condition cohomologique faible est vérifiée, d'après le point 2) le p-rang des groupes $H_2(G_{n,S},\mathbb{Z}_p)$ est borné. De $\varprojlim_n H_2(G_{n,S},\mathbb{Z}_p)=H_2(H_S,\mathbb{Z}_p)$, on conclut alors aisément.

4) On rappelle que pour tout n,

$$\mathrm{rk}_{\mathbb{Z}_p}G_{n,S}^{ab}=p^n\delta_S-\mathrm{rk}_{\mathbb{Z}_p}\mathrm{Im}(\varphi_{S_n})=p^n(\delta_S-(r_1+r_2))+1+\mathrm{rk}_{\mathbb{Z}_p}\ker(\varphi_{S_n})$$

Mais, d'un autre coté, le théorème de structure nous indique que $\mathrm{rk}_{\mathbb{Z}_p}G_{n,S}^{ab}=p^n\rho_S+O(1)$. On conclut alors facilement. □

3.2. S-conditions et dimension cohomologique. Commencons par remarquer que la dimension cohomolgique de G_S est fortement liée à la S-condition arithmétique.

Proposition 3.3. *(i) Si la S-condition arithmétique faible est vérifiée le long de K_S/K, c'est à dire s'il existe une constante c telle que pour tout corps de nombres L contenu dans K_S/K, le $\mathbb{Z}_p$-rang du noyau de $\varphi_{\mathrm{L},S}:=E_\mathrm{L}\to U^1_{\mathrm{L},S}$ est borné par c, alors ou bien G_S est fini ou bien la dimension cohomologique de G_S est au plus 2.*

(ii) Si la S-dimension arithmétique forte est vérifiée le long de K_S/K, alors la dimension cohomologique de G_S est au plus 2.

Avant de passer à la preuve de ceci, nous rappellerons un lemme bien connu.

Lemme 3.2. *Soit G un pro-p-groupe pour lequel $H^1(G,\mathbb{F}_p)$ et $H^2(G,\mathbb{F}_p)$ sont finis. Alors*

$$d_pH_2(G,\mathbb{Z}_p)-\mathrm{rk}_{\mathbb{Z}_p}G^{ab}=\chi_2(G)-1,$$

où $\chi_2(G)$ est la caractéristique d'Euler-Poincaré de G tronquée à l'ordre 2.

Preuve. La preuve de la proposition 2.5 a fait apparaitre l'identité $d_pH^2(G,\mathbb{F}_p)=d_pH_2(G,\mathbb{Z}_p)+d_pG^{ab}[p]$.

On a donc bien : $d_pH^2(G,\mathbb{F}_p)=d_pH_2(G,\mathbb{F}_p)=d_pH_2(G,\mathbb{Z}_p)+d_pG^{ab}-\mathrm{rk}_{\mathbb{Z}_p}G^{ab}$. □

Remarque. C'est en partie ce lemme qui permet de montrer le lemme 3.1.

Preuve de la proposition 3.3. Avant toute chose, rappelons que pour un pro-p-groupe M, la caractéristique d'Euler-Poincaré $\chi_2(M)$ tronquée à l'ordre 2 est définie par : $\chi_2(M) := 1 - d_pH^1(M, \mathbb{F}_p) + d_pH^2(M, \mathbb{F}_p)$, lorsque tout ceci a un sens.

(i) Soit U un sous-groupe ouvert de G_S. Notons par L le corps de nombres associé par la théorie de Galois à U. D'après le lemme 3.2, $\chi_2(U) = 1 - \mathrm{rk}_{\mathbb{Z}_p}U^{ab} + d_pH_2(U, \mathbb{Z}_p) = 1 - (G : U)\delta_S + \mathrm{rk}_{\mathbb{Z}_p}\mathrm{Im}\varphi_{\mathrm{L},S} + d_pH_2(U, \mathbb{Z}_p)$ et également $\chi_2(G_S) = 1 - \delta_S + \mathrm{rk}_{\mathbb{Z}_p}\mathrm{Im}\varphi_S + d_pH_2(G, \mathbb{Z}_p)$.

Il vient ainsi, d'après le lemme 3.1, $\chi_2(G_S) \leq r_1 + r_2 - \delta_S$.

Si l'on suppose que dans l'extension K_S/K le défaut de la S-condition arithmétique est borné par c, alors $\mathrm{rk}_{\mathbb{Z}_p}U^{ab} \leq (\mathrm{L} : \mathrm{K})(\delta_S - (r_1+r_2)) + c + 1$. Il vient ainsi $\chi_2(U) \geq d_pH_2(U, \mathbb{Z}_p) - (\mathrm{L} : \mathrm{K})(\delta_S - (r_1+r_2)) - c$. Par conséquent, $c + \chi_2(U) \geq [G_S : U](r_1 + r_2 - \delta_S) \geq [G_S : U]\chi_2(G_S)$. On conclut avec le résultat de Schmidt (cf. proposition 2.2).

(ii) Supposons la S-condition arithmétique satisfaite le long de K_S/K. Pour tout ouvert U de G_S, le groupe $H_2(U, \mathbb{Z}_p)$ est trivial. Il vient ainsi : $\chi_2(U) = (G_S : U)(\delta_S - (r_1 + r_2))$. Par conséquent, χ_2 est multiplicatif pour les ouverts de G_S. Le point 3 de la proposition 2.1 permet de conclure. □

Nous venons de voir qu'une certaine condition arithmétique le long de G_S impliquait que la dimension de G_S est au plus 2. Citons un autre résultat dans ce sens.

Proposition 3.4. *Si* K *vérifie la S-condition arithmétique et s'il existe une $\mathbb{Z}_p$-extension* $\mathrm{K}_\infty/\mathrm{K}$ *pour laquelle* $\mathrm{r}_S = 0$*, alors* $\mathrm{cd}_p(G_S) \leq 2$.

Preuve. D'après la proposition 3.1, $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. La conclusion découle alors immédiatement de la proposition 2.7. □

C'est ce résultat que nous utiliserons. Ces conditions sont parfaitement adaptées aux calculs : la condition arithmétique se teste après réduction modulo une puissance p^i convenable ; la condition $\mathrm{r}_S = 0$ se teste avec le lemme de Nakayama (après quelques calculs dans les premiers étages de $\mathrm{K}_\infty/\mathrm{K}$: voir la proposition 2.8 pour une première version brute, et la section 5 pour une version plus fine).

Notons que le cas des corps quadratiques trouve une réponse immédiate grâce à un résultat de Gillard [6].

Proposition 3.5. *Soit* K/K_0 *une extension abélienne d'un corps quadratique imaginaire* K_0*. Soit $S \subset S_p$ un sous-ensemble non-vide de places de* K *au-dessus de p stable par* $\mathrm{Gal}(\mathrm{K}/\mathrm{K}_0)$*. Enfin, soit* $G_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$.

Alors la dimension cohomologique de G_S est au plus 2.

Preuve. Si S contient toutes les places au-dessus de p, c'est bien connu. Supposons que S ne contient qu'une place au-dessus de p. L'extension $\mathrm{K}_{0,S}/\mathrm{K}_0$ ne contient qu'une $\mathbb{Z}_p$-extension $\mathrm{K}_{0,\infty}$. Gillard dans [6] a montré que pour la $\mathbb{Z}_p$-extension $\mathrm{K}_{0,\infty}\mathrm{K}/\mathrm{K}$, l'invariant μ_S de $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_{0,\infty}\mathrm{K})^{ab}$ est trivial (cf. également [28]).

Ensuite φ_S est injective, c'est classique. Le théorème 3.4 s'applique. □

Remarque. (i) Plus généralement, Wingberg, dans [32], montre que si $\rho_S = 0$ et que si la S-condition arithmétique faible est vérifiée, alors $\mathcal{X}_S$ n'a pas de sous-module fini. Si l'on suppose de plus $\mathrm{r}_S = 0$, on obtient alors que le groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ est libre.

(ii) On peut noter que la conjecture de Schanuel (cf. [14], [20], ...) associée à la proposition 3.4 permet de remplacer dans la proposition 3.5 la condition "K/K_0 abélienne" par "K/K_0 galoisienne".

Enfin, nous avons vu que la condition arithmétique impliquait la condition cohomologique. Que peut-on dire de la réciproque ?

Proposition 3.6. *Soient* K *un corps de nombres et* $S \subset S_p$ *un sous-ensemble de places de* K *au-dessus de* p. *Soit* K_S *la pro-p-extension maximale de* K, *S-ramifiée ;* $G_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$. *Supposons* G_S *de dimension cohomologique au plus 2. Alors pour toute extension* L/K *de corps de nombres contenue dans* K_S/K, *il vient :*

$$d_p H_2(G_{\mathrm{L},S}, \mathbb{Z}_p) - d_p\ker(\varphi_{\mathrm{L},S}) = [\mathrm{L} : \mathrm{K}]\,(d_p H_2(G_{\mathrm{K},S}, \mathbb{Z}_p) - d_p\ker(\varphi_{\mathrm{K},S}))$$

Preuve. Soit $H = \mathrm{Gal}(\mathrm{K}_S/\mathrm{L})$. Comme G_S est de dimension cohomologique au plus 2, la caractéristique d'Euler-Poincaré s'arrête au plus au troisième terme et elle est multiplicative dans K_S/K. Il suffit alors de noter que $\mathrm{rk}_{\mathbb{Z}_p} G_{\mathrm{L},S} = rk_{\mathbb{Z}_p} H^{ab} = \delta_{\mathrm{L},S} - [\mathrm{L} : \mathrm{K}](r_1 + r_2) + 1 + \ker(\varphi_{\mathrm{L}}, S)$. □

On en déduit immédiatement le corollaire suivant :

Corollaire 3.1. *(i) Si* $\mathrm{cd}_p(G_S) = 1$, *la S-condition arithmétique est vérifiée pour* (K, S) *si et seulement si elle est conservée dans* K_S/K.

(ii) Supposons que la dimension cohomologique de G_S *est au plus* 2 *et que* K *vérifie la S-condition arithmétique. Alors, pour toute extension finie* L/K *contenue dans* K_S,

$$d_p\ker(\varphi_{\mathrm{L},S}) = d_p H_2(G_{\mathrm{L},S}, \mathbb{Z}_p)$$

En particulier, dans ce cas, il y a équivalence entre la S-condition cohomologique et la S-condition arithmétique.

3.3. *S*-conditions et polynôme caractéristique. Des informations sur les S-conditions cohomologiques peuvent se déduire à partir du Λ-module $\mathcal{X}_S$, le point de départ étant la proposition suivante :

Proposition 3.7. *Soit* $\mathrm{K}_\infty/\mathrm{K}$ *une* $\mathbb{Z}_p$*-extension contenue dans* K_S/K*. Alors la S-condition cohomologique est vérifiée pour* K *si et seulement si la S-condition cohomologique faible l'est et* ${\mathcal{X}_S}^X = (\mathcal{X}_S)^\Gamma = 0$*.*

Preuve. C'est la proposition 2.6. □

Proposition 3.8. *Supposons que* $\mathcal{X}_S$ *n'a pas de sous* Λ*-module fini. Alors, la S-condition cohomologique est vraie à l'étage* K_n *de* $\mathrm{K}_\infty/\mathrm{K}$ *si et seulement si, la S-condition cohomologique faible l'est et si le polynôme caractéristique* P_S *de* $\mathcal{X}_S$ *est premier avec* ω_n*.*

La preuve de cette proposition repose sur le lemme suivant :

Lemme 3.3. *Soit* $\mathcal{X}$ *un* Λ*-module de type fini n'ayant pas de sous-*Λ*-module fini. Alors, pour tout* n*,* $\mathcal{X}^{\omega_n} = 0$ *équivaut à* ω_n *et* $P_\mathcal{X}$ *premiers entre eux, où* $P_\mathcal{X} = \prod_i f_i^{b_i}$ *est le polynôme caractéristique de* $\mathcal{X}$*.*

Preuve. Par hypothèse, il existe un morphisme injectif de Λ-modules $\phi : \mathcal{X} \to \mathcal{E} = \Lambda^\rho \oplus \bigoplus_i \Lambda/(f_i^{b_i})$ à conoyau fini.

Soit $x \in \mathcal{X}$ tel que $\omega_n x = 0$. Alors $\omega_n \phi(x) = 0$. Si pour tout i, $(f_i, \omega_n) = 1$, alors $\phi(x) = 0$ et ainsi $x = 0$.

Réciproquement. Supposons ω_n et f_i non premiers entre eux, pour un certain indice i. Il existe $y \in \mathcal{E}$ avec $\mathbb{Z}_p y \simeq \mathbb{Z}_p$ et tel que $\omega_n y = 0$. D'autre part, il existe également $b \in B$ et $x \in \mathcal{X}$ tels que $y = \phi(x) + b$. En particulier, $\#B\omega_n \cdot y = \phi(\omega_n \#B \cdot x) = 0$, et ainsi $\omega_n \ \#B \cdot x = 0$. Par conséquent, $\#B \cdot x \in \mathcal{X}^{\omega_n}$. Comme $< y >_{\mathbb{Z}_p}$ est sans-torsion, on en déduit que $\mathcal{X}^{\omega_n}$ est non trivial. □

Preuve de la proposition 3.8. Supposons la S-condition cohomologique vérifiée pour K_n. Alors, d'une part, la S-condition cohomologique faible est satisfaite : $H_2(H_S, \mathbb{Z}_p)$ est trivial. Et d'autre part, d'après la proposition 2.6 et le lemme 3.3, P_S et ω_n sont premiers entre eux. La conclusion en découle.

La réciproque se montre de façon identique. □

Corollaire 3.2. *(i) Si la S-condition arithmétique forte est satisfaite pour un étage* K_n *de* $\mathrm{K}_\infty/\mathrm{K}$*, alors la S-condition arithmétique faible est satisfaite pour* $\mathrm{K}_\infty/\mathrm{K}$*.*

(ii) Supposons la S-condition arithmétique faible vérifiée pour $\mathrm{K}_\infty/\mathrm{K}$*. Alors pour tout étage* K_n *de* $\mathrm{K}_\infty/\mathrm{K}$*, la S-condition arithmétique forte et la S-condition cohomologique forte sont équivalentes.*

Preuve. (i) Supposons la S-condition arithmétique forte réalisée pour K_n. La S-condition cohomologique forte est donc aussi réalisée pour le corps K_n. Alors, $\mathcal{X}_S$ n'a pas de sous-$\mathbb{Z}_p[[\Gamma^{p^n}]]$-module fini et donc n'a pas de

sous Λ-module fini. D'autre part, d'après la proposition 3.8, le polynôme $P_S = \prod_i f_i^{b_i}$ est premier à ω_n. Maintenant, il est bien connu (cf. [31], par exemple), que pour un polynôme irréductible f, f et ω_n sont premiers entre eux si et seulement si, le quotient $\Lambda/(f, \omega_n)$ est fini. Ainsi, $\mathrm{rk}_{\mathbb{Z}_p}\mathcal{X}_S/\omega_n\mathcal{X}_S = p^n\rho_S + \sum_i \mathrm{rk}_{\mathbb{Z}_p}\Lambda/(f_i^{b_i}, \omega_n) = p^n\rho_S$. Il suffit ensuite de se rappeler que $\mathrm{rk}_{\mathbb{Z}_p}\mathcal{X}_S/\omega_n\mathcal{X}_S = \mathrm{rk}_{\mathbb{Z}_p}G_{n,S}^{ab} - 1 = p^n(\delta_S - (r_1+r_2)) + \mathrm{rk}_{\mathbb{Z}_p}\ker(\varphi_{S_n}) = p^n(\delta_S - (r_1 + r_2))$, ceci par hypothèse. Ainsi, $\rho_S = \delta_S - (r_1 + r_2)$, ce qui indique que la S-condition arithmétique faible est vérifiée dans $\mathrm{K}_\infty/\mathrm{K}$.

(ii) Il faut donc montrer, pour un étage K_n de $\mathrm{K}_\infty/\mathrm{K}$, que la S-condition cohomologique implique la S-condition arithmétique.

Supposons donc satisfaite la S-condition cohomologique à l'étage K_n. Alors $\mathcal{X}_S$ n'a pas de sous-Λ-module fini. La proposition 3.8 nous indique que P_S est premier à ω_n. Par conséquent, $\mathrm{rk}_{\mathbb{Z}_p}G_{n,S}^{ab} - 1 = \mathrm{rk}_{\mathbb{Z}_p}\mathcal{X}_S/\omega_n\mathcal{X}_S = p^n\rho_S$. Mais par hypothèse, $\rho_S = \delta_S - (r_1 + r_2)$. Et ainsi, $\varphi_{S_n} : \mathbb{Z}_p \otimes E_{\mathrm{K}_n} \to U_{S_n}^1$ est injectif. □

Pour terminer, notons qu'un nombre fini de calculs le long de $\mathrm{K}_\infty/\mathrm{K}$ permet de s'assurer dans certains cas si la S-condition arithmétique forte le long de $\mathrm{K}_\infty/\mathrm{K}$ est réalisée ou non. En effet :

Corollaire 3.3. *Supposons la quantité* $\mathrm{rk}_{\mathbb{Z}_p}G_{n,S}^{ab} - p^n\rho_S$ *bornée par une constante* $c+1$. *Alors la* S*-condition arithmétique est vérifiée pour tous les étages* K_n *de* $\mathrm{K}_\infty/\mathrm{K}$ *si et seulement si, elle est vérifiée pour le corps* K *ainsi que le corps* K_m *où* m *est le plus grand entier vérifiant* $(p-1)p^{m-1} \leq c$.

Preuve. Supposons assurée la S-condition arithmétique pour K. Ainsi : (i) la S-condition arithmétique faible est satisfaite dans $\mathrm{K}_\infty/\mathrm{K}$ (cf. corollaire 3.2); (ii) $H_2(G_S, \mathbb{Z}_p)$ est trivial.

Soit m le plus grand entier vérifiant $(p-1)p^m \leq c$.

D'après la proposition 3.8, pour $n \leq m$, P_S et ω_n sont premiers entre eux. Pour conclure, il suffit alors de noter que pour $j > 0$, nécessairement f_i et ω_{m+j} sont aussi premiers entre eux : en effet, sinon, $(\omega_{m+j,m}) = (f_i)$ pour un certain entier $j > 0$ (se rappeler que les polynômes f_i sont irréductibles) et alors, on aurait $\sum_i \Lambda/(f_i, \omega_{m+j}) > c$, et ainsi, $\mathrm{rk}_{\mathbb{Z}_p}G_{m+j,S} - p^{m+j}\rho_S = \mathrm{rk}_{\mathbb{Z}_p}\mathcal{X}_S/\omega_{m+j} + 1 - p^{m+j}\rho_S = d_p\ker(\varphi_{S_{m+j}}) + \sum_i \Lambda/(f_i, \omega_{m+j}) + 1 > c+1$, d'où la contradiction. La proposition 3.8 s'applique : la S-condition cohomologique est vérifiée le long de $\mathrm{K}_\infty/\mathrm{K}$. D'après le corollaire 3.2, il en est de même pour la S-condition arithmétique. □

3.4. S-conditions et Λ-torsion de $\mathcal{X}_S$. Notons par $\mathcal{T}_S$ le sous-Λ-module de torsion de $\mathcal{X}_S$.

Le quotient $\mathcal{X}_S/\mathcal{T}_S$ est un Λ-module de type fini sans torsion. En particulier, $\mathcal{X}_S/\mathcal{T}_S$ n'a pas de sous-module fini. Le théorème de structure nous

indique alors l'existence d'un Λ-module fini B tel que l'on ait la suite exacte de Λ-modules :

$$1 \longrightarrow \mathcal{X}_S/\mathcal{T}_S \longrightarrow \Lambda^{\rho_S} \longrightarrow B \longrightarrow 1$$

Appliquant ω_n à cette suite puis utilisant le lemme du serpent, on obtient :

$$1 \longrightarrow B^{\omega_n} \longrightarrow \mathcal{X}_S/(\mathcal{T}_S+\omega_n\mathcal{X}_S) \longrightarrow \Lambda^{\rho_S}/\omega_n\Lambda^{\rho_S} = \mathbb{Z}_p^{p^n\rho_S} \longrightarrow B/\omega_n B \longrightarrow 1$$

Ainsi, B^{ω_n} est exactement la partie de torsion du $\mathbb{Z}_p$-module de type fini $\mathcal{X}_S/(\mathcal{T}_S + \omega_n\mathcal{X}_S)$.

Ce dernier Λ-module apparait dans la suite exacte :

$$1 \longrightarrow (\mathcal{T}_S + \omega_n\mathcal{X}_S)/\omega_n\mathcal{X}_S \longrightarrow \mathcal{X}_S/\omega_n\mathcal{X}_S \longrightarrow \mathcal{X}_S/(\mathcal{T}_S + \omega_n\mathcal{X}_S) \longrightarrow 1$$

où $(\mathcal{T}_S + \omega_n)\mathcal{X}_S/\omega_n\mathcal{X}_S$ est naturellement isomorphe au module $\mathcal{T}_S/\omega_n\mathcal{T}_S$.

Lemme 3.4. *Si la S-condition cohomologique est vérifiée pour tout étage K_n de $\mathrm{K}_\infty/\mathrm{K}$, alors $\mathcal{T}_S/\omega_n\mathcal{T}_S$ est fini.*

Preuve. En effet, le Λ-module $\mathcal{T}_S/\omega_n\mathcal{T}_S$ est annulé à la fois par ω_n et à la fois par $p^\alpha P_S$, où $\alpha = \max_i a_i$ (cf. section 2.2). Par hypothèse, ces polynômes sont premiers entre eux, et ainsi $\mathcal{T}_S/\omega_n\mathcal{T}_S$ est fini. □

À présent, supposons vérifiée la S-condition cohomologique forte à chaque étage K_n de $\mathrm{K}_\infty/\mathrm{K}$. La suite exacte précédente de $\mathbb{Z}_p$-modules devient dans ce cas :

$$1 \longrightarrow \mathcal{T}_S/\omega_n\mathcal{T}_S \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{X}_S/\omega_n\mathcal{X}_S) \longrightarrow B^{\omega_n} \longrightarrow 1$$

Ainsi,

Corollaire 3.4. *Lorsque la S-condition cohomologique forte est vérifiée le long de $\mathrm{K}_\infty/\mathrm{K}$, le quotient $\mathcal{T}_S/\omega_n\mathcal{T}_S$ s'injecte dans la torsion de $G_{n,S}^{ab}$.*

Ceci va nous permettre de montrer que si le rang de $\mathrm{Tor}_{\mathbb{Z}_p}(G_{n,S}^{ab})$ ne croit pas suffisament vite, alors r_S est trivial.

Proposition 3.9. *Supposons la S-condition cohomologique vérifiée à chaque étage K_n de $\mathrm{K}_\infty/\mathrm{K}$.*

(a) S'il existe $n \geq 0$ pour lequel

$$d_p\mathrm{Tor}_{\mathbb{Z}_p}(G_{n,S}^{ab}) \leq n,$$

alors : (i) $\mathcal{T}_S/p\mathcal{T}_S$ est fini ; (ii) $\mathrm{r}_S = 0$.

(b) S'il existe $n \geq 0$ pour lequel

$$\#\mathrm{Tor}_{\mathbb{Z}_p}(G_{n,S}^{ab}) \leq p^n,$$

alors : (i) $\mathcal{T}_S$ est trivial; (ii) $\lambda_S = \mathrm{r}_S = 0$.

Preuve. (a). Si $n = 0$, alors $\mathcal{T}_S/X\mathcal{T}_S = 0$. Par le lemme de Nakayama, on en déduit que $\mathcal{T}_S$ est trivial.

Pour $n > 0$, on a la suite de quotients :

$$\mathcal{T}_S/(\mathcal{T}_S + \omega_n\mathcal{T}_S) \twoheadrightarrow \mathcal{T}_S/(p\mathcal{T}_S + \omega_{n-1}\mathcal{T}_S) \twoheadrightarrow \cdots \twoheadrightarrow \mathcal{T}_S/(p\mathcal{T}_S + X\mathcal{T}_S)$$

Comme $d_p\mathcal{T}_S/\omega_n\mathcal{T}_S \leq n$, on est assuré que : ou bien $\mathcal{T}_S/X\mathcal{T}_S$ est trivial ; ou bien que pour un certain entier m, $\mathcal{T}_S/(p\mathcal{T}_S+\omega_m\mathcal{T}_S) \simeq \mathcal{T}_S/(p\mathcal{T}_S+\omega_{m+1}\mathcal{T}_S)$. Dans le premier cas, on a $\mathcal{T}_S = 0$. Dans le second, il vient $p\mathcal{T}_S + \omega_m\mathcal{T}_S = p\mathcal{T}_S + \omega_{m+1,m}\omega_m\mathcal{T}_S$, et ainsi $\omega_m\mathcal{T}_S + p\mathcal{T}_S/p\mathcal{T}_S$ est trivial, et ce par le lemme de Nakayama. Par conséquent, $\omega_m\mathcal{T}_S \subset p\mathcal{T}_S$. Ainsi, le quotient $\mathcal{T}_S/p\mathcal{T}_S$, qui est isomorphe à $\mathcal{T}_S/(\omega_m\mathcal{T}_S + p\mathcal{T}_S)$, est fini, car $\mathcal{T}_S/\omega_m\mathcal{T}_S \hookrightarrow \mathrm{Tor}_{\mathbb{Z}_p}(G^{ab}_{m,S})$ l'est, ce qui prouve (i). D'après le lemme de Nakayama, le $\mathbb{Z}_p$-module compact $\mathcal{T}_S$ (car $\mathcal{X}_S$ l'est) est donc de type fini, et ainsi $\mathrm{r}_S = 0$.

(b) Le point (i) implique clairement (ii).

Montrons donc (i).

Si $n = 0$, alors $\mathcal{T}_S/X\mathcal{T}_S = 0$. Par le lemme de Nakayama, on en déduit que $\mathcal{T}_S$ est trivial.

Pour $n > 0$, on a la suite de quotients :

$$\mathcal{T}_S/\omega_n\mathcal{T}_S \twoheadrightarrow \mathcal{T}_S/\omega_{n-1} \twoheadrightarrow \cdots \twoheadrightarrow \mathcal{T}_S/X\mathcal{T}_S$$

Comme $\#\mathcal{T}_S/\omega_n\mathcal{T}_S \leq p^n$, on est assuré que : ou bien $\mathcal{T}_S/X\mathcal{T}_S$ est trivial; ou bien que pour un certain entier m, $\mathcal{T}_S/\omega_m\mathcal{T}_S \simeq \mathcal{T}/\omega_{m+1}\mathcal{T}_S$. Dans le premier cas, on a $\mathcal{T}_S = 0$. Dans le second, il vient $\omega_{m+1,m}\omega_m\mathcal{T}_S = \omega_m\mathcal{T}_S$, et ainsi $\omega_m\mathcal{T}_S = 0$. Or,

$$\mathcal{T}_S \simeq \mathcal{T}_S/\omega_m\mathcal{T}_S \hookrightarrow \mathrm{Tor}_{\mathbb{Z}_p}(G^{ab}_{m,S})$$

Par conséquent, $\mathcal{T}_S$ est fini. La S-condition cohomologique étant vérifiée, $\mathcal{X}_S$ n'a donc pas de sous-Λ-module fini. En conclusion, $\mathcal{T}_S = 0$. □

Remarque. Restons dans la situation où la S-condition cohomologique le long de $\mathrm{K}_\infty/\mathrm{K}$ est vérifiée.

Supposons que la norme de $\mathrm{Tor}_{\mathbb{Z}_p}(G^{ab}_{n,S})$ vers $\mathrm{Tor}_{\mathbb{Z}_p}(G^{ab}_{n+1,S})$ est un isomorphisme pour un entier n. Alors, le diagramme commutatif

$$\begin{array}{ccccccc}
\mathcal{T}_S/\omega_n\mathcal{T}_S & \hookrightarrow & \mathrm{Tor}(\mathcal{X}_S/\omega_n\mathcal{X}_S) & \longrightarrow & B^{\omega_n} & \longrightarrow & 1 \\
\uparrow & & \uparrow & & \uparrow{\scriptstyle \omega_{n+1,n}} & & \\
\mathcal{T}_S/\omega_{n+1}\mathcal{T}_S & \hookrightarrow & \mathrm{Tor}(\mathcal{X}_S/\omega_{n+1}\mathcal{X}_S) & \longrightarrow & B^{\omega_{n+1}} & \longrightarrow & 1
\end{array}$$

nous indique que $B^{\omega_{n+1}} \overset{\omega_{n+1,n}}{\longrightarrow} B^{\omega_n}$ est aussi un isomorphisme.

Le lemme du serpent appliqué à

$$\begin{array}{ccccc}
B^{\omega_n} & \hookrightarrow & B & \twoheadrightarrow & \omega_n B \\
\uparrow{\scriptstyle \omega_{n+1,n}} & & \uparrow{\scriptstyle \omega_{n+1,n}} & & \uparrow{\scriptstyle incl} \\
B^{\omega_{n+1}} & \hookrightarrow & B & \twoheadrightarrow & \omega_{n+1} B
\end{array}$$

montre que $B^{\omega_{n+1},n}$ est trivial. Par conséquent, d'après le lemme de Nakayama, B l'est aussi. On obtient, dans ce cas, et pour tout n, que $G_{n,S}^{ab}$ est sans-torsion.

On peut alors faire la remarque suivante. Supposons les conditions de la proposition 3.9 satisfaites (cf. section 6). Pour $n >> 0$, les groupes de torsion de $G_{n,S}^{ab}$ sont isomorphes, mais cet isomorphisme ne provient pas de la norme (lorsque ceux-ci ne sont pas triviaux). Ce qui indique que, pour $n >> 0$, une partie de torsion à l'étage n est absorbée par les $\mathbb{Z}_p$-extensions du $(n+1)$-ème étage.

Pour plus de détails sur ce module de torsion, on renvoit par exemple à [14].

4. $\mathbb{Z}_p$-extensions et logarithme de Gras.

Certains renseignements sur l'extension $\mathrm{K}_S^{ab}/\mathrm{K}$ s'obtiennent après calcul dans un corps de rayon $\mathrm{K}_{\mathfrak{m}}$ adapté. Par exemple, rappelons comment on peut calculer de cette façon le p-rang de G_S.

4.1. Calcul de $d_p(G_S)$. Le rayon à prendre est facile à déterminer lorsque K contient les racines p-èmes de l'unité. Il découle de la proposition suivante :

Proposition 4.1. *Soit $K_{\mathfrak{p}}/\mathbb{Q}_p$ un corps local contenant les racines p-èmes de l'unité. Soit π une uniformisante de $K_{\mathfrak{p}}$. Posons $\mathfrak{a} = pe(\mathrm{K}_{\mathfrak{p}}/\mathbb{Q}_p)/(p-1)$. Le plus petit entier n pour lequel U^n est contenu dans $K_{\mathfrak{p}}^p$ est l'entier $\mathfrak{a}+1$. Ce dernier est appelé module d'hyperprimalité de $K_{\mathfrak{p}}/\mathbb{Q}_p$.*

Corollaire 4.1. *Supposons que les racines p-èmes de l'unité sont dans* K. *Le compositum* L *des p-extensions élémentaires de* K *contenues dans* K_S *est contenu dans l'extension* $\mathrm{K}_{\mathfrak{f}}$ *de* K *de conducteur* $\mathfrak{f} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{\mathfrak{a}_{\mathfrak{p}}+1}$, *où* $a_{\mathfrak{p}} = pe(\mathrm{K}_{\mathfrak{p}}/\mathbb{Q}_p)/(p-1)$.

Corollaire 4.2. *Soit le module* $\mathfrak{m} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{\mathfrak{a}_{\mathfrak{p}}+1}$. *Alors, lorsque* K *contient les racines p-èmes de l'unité,* $d_p G_S = d_p \mathrm{Cl}_{\mathrm{K},\mathfrak{m}}$.

4.2. Le logarithme de Gras. Fixons S un ensemble fini de premiers de K au-dessus de p. Pour un idéal $\mathfrak{A}$ de $I_{\mathrm{K},S}$ (idéaux fractionnaires de K premiers à S), le logarithme $\mathrm{Log}(\mathfrak{A})$ de $\mathfrak{A}$ relativement à S est défini comme suit : Soient $n \in \mathbb{N}$ et $x \in \mathcal{O}_{\mathrm{K}}$ tels que $\mathfrak{A}^n = (x)$. On pose $\mathrm{Log}'(\mathfrak{A}) = 1/n \prod_{\mathfrak{p}\in S} \log_{\mathfrak{p}}(x) \in \prod_p \mathrm{K}_{\mathfrak{p}}$ puis $\mathrm{Log}(\mathfrak{A}) = \mathrm{Log}'(\mathfrak{A}) + \mathbb{Q}_p\mathrm{Log}'(E_{\mathrm{K}}) \bmod \mathbb{Q}_p\mathrm{Log}'(E_{\mathrm{K}})$.

On peut noter que le logarithme sur les idéaux de $I_{\mathrm{K},S}$ est défini à partir d'un système de générateurs du groupes des classes de K et du logarithme

$\mathrm{Log}(P_\mathrm{K})$ des idéaux principaux P_K. Le théorème d'approximation indique alors que $\mathrm{Log}(P_\mathrm{K}) = \prod_{\mathfrak{p}\in S} \log_\mathfrak{p}(U^1_\mathfrak{p}) + \mathbb{Q}_p\mathrm{Log}'(E_\mathrm{K}) \bmod \mathbb{Q}_p\mathrm{Log}'(E_\mathrm{K})$.

Le théorème suivant est au coeur des calculs à venir. Il permet, entre autre, de décrire la loi de décomposition des idéaux premiers dans une $\mathbb{Z}_p$-extension.

Théorème 4.1 (Gras, cf. [7], chapitre III, théorème 2.5)**.** *1) Notons par* $\widetilde{\mathrm{K}_S}$ *le compositum des* $\mathbb{Z}_p$*-extensions de* K *contenues dans* S*. Il vient alors la suite exacte :*

$$1 \longrightarrow \mathrm{Tor}(G_S^{ab}) \longrightarrow I_{\mathrm{K},S} \xrightarrow{\mathrm{Log}} < \mathrm{Log}(I_{\mathrm{K},S}) >_{\mathbb{Z}_p} \longrightarrow 1,$$

où $< \mathrm{Log}(I_{\mathrm{K},S}) >_{\mathbb{Z}_p} \overset{Artin}{\simeq} \mathrm{Gal}(\widetilde{\mathrm{K}_S}/\mathrm{K})$.

2) Pour $\mathfrak{p} \notin S$*, le groupe de décomposition de* $\mathfrak{p}$ *dans* $\widetilde{K_S}/K$ *est donné par* $\mathbb{Z}_p\ \mathrm{Log}(\mathfrak{p})$.

3) L'ordre de la torsion $\mathrm{Tor}(G_S^{ab})$ *de* G_S^{ab} *est donné par la formule :*

$$|\mathrm{Tor}(G_S^{ab})| = |\mathrm{Tor}_{\mathbb{Z}_p}(U_S^1/\varphi_{\mathrm{K},S}(E_\mathrm{K}))| \times \frac{|\mathbb{Z}_p \otimes \mathrm{Cl}_\mathrm{K}|}{(\mathbb{Z}_p\mathrm{Log}(\mathrm{Cl}_\mathrm{K}) + \mathrm{Log}(U_S^1) : \mathrm{Log}(U_S^1))}$$

4) Enfin, $[\mathrm{K}^H \cap \widetilde{\mathrm{K}}_S : \mathrm{K}] = (\mathbb{Z}_p\mathrm{Log}(\mathrm{Cl}_\mathrm{K}) + \mathrm{Log}(U_S^1) : \mathrm{Log}(U_S^1))$*, où* K^H *est le corps de Hilbert de* K*.*

À noter que dans [10], on trouve une généralisation du logarithme de Gras.

4.3. Recherche des $\mathbb{Z}_p$-extensions de K. Commençons par une simple question. Soit L une sous-extension finie de K_S/K. A quelle condition, le corps de nombres L est-il un étage d'une $\mathbb{Z}_p$-extension de K ? C'est le "logarithme de Gras" qui va nous permettre de répondre explicitement à cette question. Précisons notre situation.

Soit un corps de nombres K contenant les racines p-èmes de l'unité. Soit $S \subset S_p$ un sous-ensemble de places de K tel que le $\mathbb{Z}_p$-rang de G_S^{ab} est au moins 1. Soit K_i le i-ème étage d'une $\mathbb{Z}_p$-extension de K contenue dans K_S/K. On veut déterminer toutes les p-extensions élémentaires $\mathrm{L} = \mathrm{K}_i(\sqrt[p]{\alpha})$ de K_i qui correspondent au $i+1$-ème étage d'une $\mathbb{Z}_p$-extension de K_S/K.

Il y a deux volets. D'une part, il faut déterminer si $\mathrm{L} = \mathrm{K}_i(\sqrt[p]{\alpha})$ est dans le compositum $\widetilde{\mathrm{K}_S}$ des $\mathbb{Z}_p$-extensions de K contenues dans K_S : c'est le logarithme de Gras qui va permettre de répondre. D'autre part, il faut voir si L est l'étage d'une $\mathbb{Z}_p$-extension. Pour ce second point, on peut s'appuyer

sur le lemme suivant, conséquence d'un résultat élémentaire à propos des modules sur les anneaux principaux.

Lemme 4.1. *Soient* $\mathrm{K} \subset \mathrm{L} \subset \widetilde{\mathrm{K}}_S$. *Alors* L *est l'étage d'une* $\mathbb{Z}_p$*-extension de* K *si et seulement si,* L/K *est cyclique.*

Preuve. Un sens est évident. Réciproquement. Supposons L/K cyclique. Soit H le sous-groupe de $G = \mathrm{Gal}(\widetilde{\mathrm{K}}_S/\mathrm{K})$ vérifiant $G/H \simeq \mathrm{Gal}(\mathrm{L}/\mathrm{K}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Le $\mathbb{Z}_p$-module H est de même rang r que G. D'après la théorie des diviseurs élémentaires, il existe une $\mathbb{Z}_p$-base $\{e_1, \cdots, e_r\}$ de G telle que $\{e_1, \cdots, e_{r-1}, p^n e_r\}$ soit aussi une base de H. Soit $H' = \mathbb{Z}_p e_1 + \cdots + \mathbb{Z}_p e_{r-1}$. Alors $H' \subset H$. Le sous-corps de $\widetilde{\mathrm{K}}_S$ fixé par H' contient L et c'est aussi une $\mathbb{Z}_p$-extension de K. □

La recherche va alors se faire en trois étapes.

(i) Déterminer, à l'aide de la théorie de Kummer, toutes les extensions p-élémentaires de K_i contenues dans K_S. Parmi celles-ci, trouver celles qui sont abéliennes puis cycliques sur K ;

(ii) Déterminer un conducteur $\mathfrak{f}$ de K tel que $\mathrm{K}_\mathfrak{f}$ contient toutes les p-extensions élémentaires de K_i abéliennes sur K.

Trouver ensuite un système de Frobenius $\mathrm{frob}(\mathfrak{p}^{(1)}), \cdots, \mathrm{frob}(\mathfrak{p}^{(r)})$ engendrant le groupe $\mathrm{Gal}(\mathrm{K}_\mathfrak{f}/\mathrm{K}_i) \subset \mathrm{Gal}(\mathrm{K}_\mathfrak{f}/\mathrm{K})$ (il faut s'assurer que pour $i = 1, \cdots, r$, $\mathfrak{p}^{(i)}$ est premier à p) . Notons par Ω une telle famille.

Le lemme suivant est une application immédiate du théorème 4.1.

Lemme 4.2. *Soit* $\Omega(i+1) =$

$$\{\mathfrak{b} = \prod_i^r \mathrm{frob}(\mathfrak{p}^{(i)})^{a_i}, \mathfrak{p}^{(i)} \in \Omega, a_i = 0, \cdots, p-1 \mid \mathrm{Log}(\mathfrak{b}) \in p^{i+1}\mathrm{Log}I_{\mathrm{K},S}\}$$

Alors le sous-corps maximal de $\mathrm{K}_\mathfrak{f}$ *fixé par tous les éléments de* $\Omega(i+1)$ *est le compositum de tous les* $i+1$*-étages de* $\widetilde{\mathrm{K}_S}/\mathrm{K}$.

(iii) Enfin, la proposition suivante permet de conclure.

Proposition 4.2. *Soit* $\mathrm{L} = \mathrm{K}_i(\sqrt[p]{\alpha})/\mathrm{K}$ *une sous-extension cyclique de* K_S/K. *Le corps* $\mathrm{K}_i(\sqrt[p]{\alpha})$ *est le* $i+1$*-étage d'une* $\mathbb{Z}_p$*-extension de* $\widetilde{\mathrm{K}}_S/\mathrm{K}$ *si et seulement si, pour tout* $\mathfrak{b} = \prod_i^r \mathrm{frob}(\mathfrak{p}^{(i)})^{a_i} \in \Omega(i+1)$,

$$\prod_{j=1}^{r} \left(\frac{\alpha}{\mathfrak{P}^{(j)}}\right)^{a_j} = 1,$$

où $\mathfrak{P}^{(j)}$, $j = 1, \cdots, r$ *est un premier (quelconque) de* K_i *au-dessus de* $\mathfrak{p}^{(j)}$.

Preuve. Notons tout d'abord que par le choix de $\mathfrak{f}$, L est un sous-corps de $\mathrm{K}_{\mathfrak{f}}$. Pour $j = 1, \cdots, r$, l'idéal $\mathfrak{p}^{(j)}$ est décomposé dans K_i/K. Ainsi, on a la propriété suivante du symbole d'Artin :

$$\mathrm{frob}(\mathfrak{p}^{(j)}) = \left(\frac{\mathfrak{p}^{(j)}}{\mathrm{K}_{\mathfrak{f}}/\mathrm{K}}\right) = \left(\frac{\mathfrak{P}^{(j)}}{\mathrm{K}_{\mathfrak{f}}/\mathrm{K}_i}\right)$$

pour n'importe quel idéal premier $\mathfrak{P}^{(j)}$ de K_i au-dessus de $\mathfrak{p}^{(j)}$. Ensuite, $\sigma_{\mathfrak{p}^{(j)}|\mathrm{L}} = \left(\dfrac{\mathfrak{P}^{(j)}}{\mathrm{L}/\mathrm{K}_i}\right)$. Ainsi, il vient :

$$\left(\frac{\mathfrak{b}}{\mathrm{K}_i(\sqrt[p]{\alpha})/\mathrm{K}_i}\right)\sqrt[p]{\alpha} = \prod_{j=1}^{r}\left(\frac{\mathfrak{P}^{(j)}}{\mathrm{K}_i(\sqrt[p]{\alpha})/\mathrm{K}_i}\right)^{a_j}\sqrt[p]{\alpha} = \prod_{j=1}^{r}\left(\frac{\alpha}{\mathfrak{P}^{(j)}}\right)^{a_j}\sqrt[p]{\alpha}.$$

Le lemme 4.2 permet finalement de conclure . □

5. À propos du théorème du miroir

Choisissons maintenant T et S vérifiant $S \cup T = S_p$. Supposons toujours également que K_S/K contient une $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$.

Nous désirons appliquer un résultat de dualité le long de $\mathrm{K}_\infty/\mathrm{K}$. Pour ce faire, nous allons supposer que K contient les racines p-èmes de l'unité. Il va alors être possible de donner des informations sur les invariants r_S et ρ_S de $\mathcal{X}_S$ à partir du Λ-module $\mathcal{X}_T^S$. À noter que contrairement à la $\mathbb{Z}_p$-extension cyclotomique, $\mathrm{K}_\infty/\mathrm{K}$ ne va contenir qu'un nombre fini de racines de l'unités, nous empêchant d'obtenir théoriquement des renseignements sur l'invariant λ_S.

Ceci nous permettra de donner un critère de nullité de l'invariant r_S. Celui-ci est adapté à la situation "déséquilibrée", c'est à dire lorsque δ_S est bien plus grand que δ_T.

Pour l'étude d'une telle dualité dans le cas cyclotomique, nous renvoyons à [15].

Proposition 5.1. *Soit* K *un corps totalement imaginaire contenant les racines p-èmes de l'unité. Soit* $\mathrm{K}_\infty/\mathrm{K}$ *une* $\mathbb{Z}_p$*-extension contenue dans* K_S/K. *Notons par* $(\rho_S^T, \mathrm{r}_S^T, \lambda_T^S)$ *(respectivement* $(\rho_T^S, \mathrm{r}_T^S, \lambda_S^T)$*) les invariants du* Λ*-module* $\mathcal{X}_S^T$ *(respectivement* $\mathcal{X}_T^S$*) relativement à* $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})$. *Notons par* $\tilde{s}$ *(respectivement* $\tilde{t}$*) le nombre de places de S (respectivement de T) totalement décomposées dans* $\mathrm{K}_\infty/\mathrm{K}$. *Il vient alors la formule suivante :*

$$\frac{\delta_T}{2} + \tilde{t} + \rho_S^T + \mathrm{r}_S^T = \frac{\delta_S}{2} + \tilde{s} + \rho_T^S + \mathrm{r}_T^S.$$

Preuve. Nous allons utiliser une identité due à Gras que l'on peut trouver dans [7] (théorème 4.6, chapitre I).

Proposition 5.2. *Sous la condition $T \cup S = S_p$, nous avons pour chaque étage K_n la formule*

$$d_p G_{n,T}^S - d_p G_{n,S}^T = t_n - s_n + \delta_{T_n} - r_2(\mathrm{K}_n)$$

D'après les lemmes 2.1, 2.4 et 2.5, asymptotiquement cette formule devient

$$p^n(\rho_T^S + \mathrm{r}_T^S) - p^n(\rho_S^T + \mathrm{r}_S^T) = p^n(\tilde{t} - \tilde{s}) + p^n\delta_T - p^n r_2 + O(1)$$

On conclut en notant que $2r_2 = \delta_T + \delta_S$. □

Nous sommes en mesure de pouvoir donner un critère de nullité de l'invariant r_S.

Corollaire 5.1. *Sous les hypothèses de la proposition 5.1, il vient*

$$\mathrm{r}_S^T \leq \tilde{s} + \rho_T^S + \mathrm{r}_T^S$$

Ainsi dès lors que $\tilde{t} = \tilde{s} = \rho_T^S = \mathrm{r}_T^S = 0$, on a $\mathrm{r}_S = 0$ et $\rho_S = 1/2(\delta_S - \delta_T) = \delta_S - r_2$.

Preuve. À l'étage K_n, le $\mathbb{Z}_p$-rang du groupe $\mathrm{Gal}(\mathrm{K}_{n,S}^T/\mathrm{K}_n)$ est exactement égal à $\delta_{S_n} - rk_{\mathbb{Z}_p}\varphi_{S_n}(E_{\mathrm{K}_n}^T)$ et est donc minoré par $\delta_{S(\mathrm{K}_n)} - (r_2(\mathrm{K}_n) + t_n - 1)$. Pour n assez grand le $\mathbb{Z}_p$-rang de $\mathrm{Gal}(\mathrm{K}_{n,S}^T/\mathrm{K}_n)$ est donc minoré par :

$$p^n(\delta_S) - p^n(r_2 + \tilde{t}) + O(1)$$

On a donc l'inégalité (avec le lemme 2.1)

$$p^n\rho_S^T \geq p^n\delta_S - p^n(r_2 + \tilde{t}) + O(1)$$

qui permet d'obtenir

$$\rho_S^T \geq \delta_S - r_2 - \tilde{t}$$

Reportant cette inégalité dans celle de la proposition 5.1 et en notant que $r_2 = \delta^S + \delta^T$, on obtient bien :

$$\mathrm{r}_S^T \leq \tilde{s} + \rho_T^S + \mathrm{r}_T^S.$$

Lorsque $\tilde{s} = \rho_T^S = \mathrm{r}_T^S = 0$, il vient $\mathrm{r}_S^T = 0$. Maintenant si $\tilde{t} = 0$, cela signifie qu'il n'y a qu'un nombre fini de places dans $\mathrm{K}_\infty/\mathrm{K}$ au-dessus des places de T. Or on passe de $\mathcal{X}_S$ à $\mathcal{X}_S^T$ en quotientant par les groupes de décomposition des places de T, chacun étant cyclique ou pro-cyclique. Ces groupes étant en nombre fini, le quotient ne change pas l'invariant r et par conséquent $\mathrm{r}_S = \mathrm{r}_S^T = 0$.

La formule de la proposition 5.1 montre alors que $\rho_S^T = 1/2(\delta_S - \delta_T)$. La aussi, comme $\tilde{t} = 0$, on conclut en notant que $\rho_S^T = \rho_S$. □

Remarque. Soit K_{n_0} un étage de $\mathrm{K}_\infty/\mathrm{K}$ où toutes les places inertes et ramifiées de S_p dans $\mathrm{K}_\infty/\mathrm{K}$ le sont totalement dans $\mathrm{K}_\infty/\mathrm{K}_{n_0}$. Supposons qu'il existe $n \geq n_0$ tel que $d_p G^S_{n,T} = d_p G^S_{n+1,T}$. Alors, pour tout $m \geq n$, on a $d_p G^S_{n,T} = d_p G^S_{m,T}$. Utilisant ensuite le proposition 5.2, on obtient, pour tout $m \geq n$, $d_p G^T_{m,S} = -t_m + s_m - p^m \delta^T + p^m r_2 + d_p G^S_{n,T}$.

Nous allons montrer que dans un certain sens, le corollaire 5.1 est optimal.

Mais avant d'énoncer le résultat, remarquons que la section 4, peut être développée dans un contexte un peu plus général, en considérant des pro-p-extensions S-ramifiées et T-décomposées (avec T non nécessairement contenu dans S_p). D'après le lemme 2.4, la lecture à chaque étage K_n du groupe $G^{T,ab}_{n,S}$ est alors relativement simple. Comme pour le cas $T = \emptyset$, il alors est naturel d'introduire les notions de $S-T$-conditions arithmétiques faibles et fortes, cohomologiques faibles et fortes. Les résultats de la section 4 restent alors parfaitement valables dans ce cadre.

Revenons au contexte de cette section. On suppose donc $S \cup T = S_p$, mais également que pour une $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$ contenue dans K_S, il vient $T = \widetilde{T}$.

Cela signifie en particulier que la quantité $\delta_S - \mathrm{rk}_{\mathbb{Z}_p}\varphi(E^T_{\mathrm{K}})$ n'est pas nulle.

Alors sous ces conditions, on a la proposition suivante :

Proposition 5.3. *Supposons le morphisme $\varphi_S : \mathbb{Z}_p \otimes E^T_{\mathrm{K}} \to U^1_S$ injectif (c'est ce que l'on peut appeler la $S-T$ condition arithmétique forte). Alors,*

$$\mathrm{r}_S = \mathrm{r}^T_S = \mathrm{r}^S_T + \rho^S_T + \widetilde{s}$$

Preuve. La $S-T$-condition arithmétique est satisfaite pour le corps K. Cela signifie que pour toute $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$ contenue dans $\mathrm{K}^T_S/\mathrm{K}$, la $S-T$ condition arithmétique faible est vérifiée, à savoir : $\rho^T_S = \delta_S - (r_1 + r_2 + t)$, ceci d'après les propositions 3.1, 3.2 et le lemme 3.2. Il en est de même pour la S-condition arithmétique faible le long de toute $\mathbb{Z}_p$-extension contenue dans K_S/K : $\rho_S = \delta_S - (r_1 + r_2)$.

Ainsi, pour une $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$ contenue dans $\mathrm{K}^T_S/\mathrm{K}$, la proposition 5.1 nous donne exactement : $\mathrm{r}^T_S = \rho^S_T + \mathrm{r}^S_T + \widetilde{s}$.

De plus,

$$\mathrm{rk}_{\mathbb{Z}_p}\mathrm{Gal}(\mathrm{K}^T_{n,S}/\mathrm{K}_n)^{ab} = p^n(\rho_S - t) + O(1)$$
$$\mathrm{rk}_{\mathbb{Z}_p}\mathrm{Gal}(\mathrm{K}_{n,S}/\mathrm{K}_n)^{ab} = p^n\rho_S + O(1).$$

Il vient ainsi :

$$\mathrm{rk}_{\mathbb{Z}_p} < D_{n,\mathfrak{P}}, \mathfrak{P} \in T_n >= p^n t + O(1),$$

où $D_{n,\mathfrak{P}}$ est le groupe de décomposition de $\mathfrak{P}$ dans l'extension $\mathrm{K}_{n,S}^{ab}/\mathrm{K}_n$. Les groupes $D_{n,\mathfrak{P}}$ étant procyclique, il vient $d_p < D_{n,\mathfrak{P}}, \mathfrak{P} \in T_n >= p^n t + O(1)$.

Pour finir, l'égalité $(\rho_S^T + \mathrm{r}_S^T)p^n = (\rho_S + \mathrm{r}_S)p^n - d_p < D_{n,\mathfrak{P}}, \mathfrak{P} \in T_n > +O(1)$, devient après simplification :

$$\mathrm{r}_S^T = \mathrm{r}_S - t + 1/p^n d_p < D_{n,\mathfrak{P}}, \mathfrak{P} \in T_n > +1/p^n O(1)$$

d'où $\mathrm{r}_S^T = \mathrm{r}_S$. □

Cette proposition indique donc que pour montrer que l'invariant r_S est trivial, il est nécessaire d'effectuer un choix judicieux de la $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$. L'exemple 6.2 illustrera ceci.

6. Deux exemples

Dans cette section, nous allons détailler deux exemples. Tout d'abord, présentons notre démarche.

On se donne un corps de nombres K, un nombre premier p et un ensemble fini S de places de K contenu dans S_p.

• Dans un premier temps, le logarithme de Gras nous permet de privilégier une $\mathbb{Z}_p$-extension K_∞ de K.

• Ensuite, on vérifie que K satisfait la S-condition arithmétique forte. Si c'est le cas, le corollaire 3.2 et la proposition 3.2 montrent que l'invariant ρ_S du $\mathbb{Z}_p[[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]]$-module $\mathcal{X}_S$ est exactement $\delta_S - (r_1 + r_2)$.

• Dans un contexte favorable, le corollaire de dualité 5.1 permet de montrer que $\mu_S = 0$. La proposition 3.4 indique alors que la dimension cohomologique de G_S est au plus 2.

• Maintenant, si le corollaire 5.1 ne s'applique pas, on peut essayer la proposition plus fine 3.9. Dans ce cas, il faut s'assurer que la S-condition arithmétique est satisfaite le long de $\mathrm{K}_\infty/\mathrm{K}$. A noter que ce corollaire peut également servir à montrer que l'invariant λ_S est trivial.

• Le résultat de dualité de la remarque 5 peut permettre de donner une majoration de la quantité $\mathrm{rk}_{\mathbb{Z}_p} G_{n,S} - p^n \rho_S$ le long de $\mathrm{K}_\infty/\mathrm{K}$. Si la situation est bien choisie, cette majoration ne dépendra pas de n.

• Grâce au corollaire 3.3, on s'assure, après un nombre fini de calculs, que la S-condition arithmétique (ou cohomologique) est vérifiée le long de $\mathrm{K}_\infty/\mathrm{K}$. Si tel est le cas, une partie des hypothèses de la proposition 3.9 est réunie.

• Enfin, si la partie de torsion de $G_{n,S}^{ab}$ ne grandit pas trop vite, la proposition 3.9 s'applique et μ_S est trivial.

6.1. Prenons $\mathrm{K} = \mathbb{Q}(\theta)$, où θ vérifie $\theta^4 + \theta^3 + 8\theta^2 - 4\theta + 2 = 0$.

La signature de K est $(0, 2)$. L'anneau des entiers $\mathcal{O}_\mathrm{K}$ de K est monogène : $\mathcal{O}_K = \mathbb{Z}[\theta]$; $E_\mathrm{K} =< \pm 1, \varepsilon := 207\theta^3 - 383\theta^2 + 190\theta - 65 >$. Le discriminant de $\mathcal{O}_\mathrm{K}$ vaut $132692 = 2^2 \cdot 7^2 \cdot 677$.

Enfin, le groupe des classes de K est d'ordre 2, il est engendré par un idéal $\mathfrak{p}_5$ au-dessus de 5.

Il y a exactement deux places de K au-dessus de 2 : $\mathfrak{p}_2^{(1)} = (\theta)$ et $\mathfrak{p}_2^{(2)} = (2, 1+\theta) = (17+3\theta+2\theta^2)$. L'indice de ramification de $\mathfrak{p}_2^{(1)}$ est 3.

Prenons $p = 2$.

Exemple. Soit $\mathrm{K} = \mathbb{Q}(\theta)$ avec θ vérifiant $\theta^4+\theta^3+8\theta^2-4\theta+2 = 0$. Posons $S = \{(\theta)\}$. Il existe une $\mathbb{Z}_2$-extension K_∞ de K contenue dans K_S/K telle que

(i) $\mathrm{K}_S/\mathrm{K}_\infty$ est libre ;
(ii) le Λ-module $H_S^{ab} = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)^{ab}$ est un sous-Λ-module de $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]]$ d'indice fini ($\rho_S = 1$ et $\mu_S = \lambda_S = 0$).

De plus, la dimension cohomologique de G_S est exactement 2.

L'ensemble des calculs vont être effectués dans $\mathrm{K}_{\mathfrak{p}_2^{(1)}}$: $\pi = \theta$ est une uniformisante de $\mathrm{K}_{\mathfrak{p}_2^{(1)}}$; on notera par $\mathrm{v} = \mathrm{v}_\pi$ la valuation.

On sait tout d'abord que $U^1_{\mathfrak{p}_2^{(1)}} \simeq \pm 1 \oplus (1+\pi)^{\mathbb{Z}_2} \oplus (1+\pi^5)^{\mathbb{Z}_2} \oplus (1+\pi^6)^{\mathbb{Z}_2}$, voir par exemple [13].

On obtient ainsi la décomposition suivante de l'unité fondamentale :

$$\varepsilon = (1+\pi)^{2+\cdots}(1+\pi^5)^{1+\cdots}(1+\pi^6)^{2+\cdots}$$

Rappelons ensuite que le logarithme défini par Gras donne l'isomorphisme suivant

$$\mathrm{Gal}(\widetilde{\mathrm{K}_S}/\mathrm{K}) \simeq \log U^1_{\mathfrak{p}_2^{(1)}} + \mathbb{Q}_2 \log(\varepsilon) \bmod \mathbb{Q}_2 \log(\varepsilon),$$

où log désigne le logarithme 2-adique dans $\mathrm{K}_{\mathfrak{p}_2^{(1)}}$. (on identifiera log et Log).

Le groupe des classes de K est engendré par un premier $\mathfrak{p}_5$ au-dessus de 5 : $\mathfrak{p}_5 = (5, 3+\theta)$. Il vient $\mathfrak{p}_5^2 = (x_5)$ avec $x_5 = 3-8\theta-\theta^2-\theta^3$ et finalement

$$x_5 = (1+\pi)^{2+\cdots}(1+\pi^5)^{4(\cdots)}(1+\pi^6)^{4(\cdots)}$$

Ainsi clairement $\log(\mathfrak{p}_5) = 1/2 \log(x_5) \in \log U^1_{\mathfrak{p}_2^{(1)}}$.

Par conséquent,

$$\left(1/2\log(x_5) + \log U^1_{\mathfrak{p}_2^{(1)}} + \mathbb{Q}_2\log(\varepsilon) : \log U^1_{\mathfrak{p}_2^{(1)}} + \mathbb{Q}_2\log(\varepsilon)\right) = 1$$

Il y a donc disjonction linéaire entre K^H et $\widetilde{\mathrm{K}}_S$ (cf. théorème 4.1).

Notons ensuite que $x_5 = (1+\theta+\theta^2)^2 - 4(2-2\theta+9\theta^2+5\theta^3)$. Ainsi l'extension quadratique $\mathrm{K}(\sqrt{x_5})/\mathrm{K}$ est non-ramifiée.

Un calcul élémentaire montre que l'ordre de la torsion de G_S^{ab} est 2 (celui-ci vaut $2 \cdot \#\mathrm{Tor}_{\mathbb{Z}_p}(\log U_S^1/\log(E_{\mathrm{K}}))$).

Notons enfin que le morphisme φ_S est (trivialement) injectif et ainsi l'extension K_S/K contient deux $\mathbb{Z}_2$-extensions linéairement indépendantes. On peut résumer tout ceci dans le

Lemme 6.1. *(i)* $G_S^{ab} \simeq \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

(ii) $\mathrm{K}(\sqrt{x_5})$ *est le corps de Hilbert* K^H *de* K. *Il est linéairement disjoint de* $\widetilde{\mathrm{K}_S}$.

6.1.1. *Les* $\mathbb{Z}_2$*-extensions de* K_S/K. Comme $\mathfrak{p}_2^{(2)} = (17 + 3\theta + 2\theta^2)$, le groupe de décomposition $D_{\mathfrak{p}_2^{(2)}}$ de $\mathfrak{p}_2^{(2)}$ dans $\mathrm{Gal}(\widetilde{\mathrm{K}}_S/\mathrm{K})$ correspond, via le logarithme de Gras, à $\mathbb{Z}_2 \log(17 + 3\theta + 2\theta^2)$ dans $\mathbb{Q}_2 \log U^1_{\mathfrak{p}_2^{(1)}} + \mathbb{Q}_2 \log \varepsilon$ mod $\mathbb{Q}_2 \log \varepsilon$.

De l'égalité $17 + 3\theta + 2\theta^2 = (1+\pi)^{1+\cdots}(1+\pi^5)^{2+\cdots}(1+\pi^6)^{1+\cdots}$, on en déduit que le groupe $D_{\mathfrak{p}_2^{(2)}}$ est engendré par $a_1 \log(1+\pi) + 2a_2 \log(1+\pi^5) + a_3 \log(1+\pi^6)$ dans $\mathbb{Z}_2 \log U^1_{\mathfrak{p}_2^{(1)}} + \mathbb{Q}_2 \log \varepsilon$ mod $\mathbb{Q}_2 \log \varepsilon$, avec $a_i \in \mathbb{Z}_2^\times$. Posons $x_2 = 17 + 3\theta + 2\theta^2$.

Remarquons ensuite que le premier 43 se décompose dans K en produit de trois idéaux premiers principaux (non-ramifiés) dont l'un, noté $\mathfrak{p}_{43}$, est de degré résiduel 1 : $\mathfrak{p}_{43} = (-1 + 17\theta + 3\theta^2 + 2\theta^3)$. Posons $x_{43} = -1 + 17\theta + 3\theta^2 + 2\theta^3$.

On note ensuite que $x_{43} = (1+\pi)^{1+4+\cdots}(1+\pi^5)^{1+\cdots}(1+\pi^6)^{2+\cdots}$. Ainsi

$$\log(x_{43}) = b_1 \log(1+\pi) + b_2 \log(1+\pi^5) + 2b_3 \log(1+\pi^6)$$

avec $b_i \in \mathbb{Z}_2^\times$.

La famille $\{\log x_2, \log x_{43}, \log(1+\pi)\}$ constitue une base de $\log U^1_{\mathfrak{p}_2{}^{(1)}}$ (il suffit de noter que le déterminant de la matrice de passage est dans $\mathbb{Z}_2^\times$). Ensuite, il est facile de voir que le $\mathbb{Z}_2$-rang de $< \log x_{43}, \log x_2 > + \mathbb{Q}_2 \log \varepsilon$ mod $\mathbb{Q}_2 \log \varepsilon$ vaut 2.

Montrons pour finir que $\log(1+\pi) \in < \log x_{43}, \log x_2 > + \mathbb{Q}_2 \log \varepsilon$. Supposons qu'il existe une puissance de 2 non triviale et minimale, 2^m, telle que $2^m \log(1+\pi) = \alpha \log x_{43} + \beta \log x_2 + \gamma \log \varepsilon$, avec $\alpha, \beta, \gamma \in \mathbb{Z}_2$. En regardant la composante en $\log(1+\pi^6)$, on trouve $\beta \equiv 0 \bmod 2$. Reportant dans l'équation issue de la composante en $\log(1+\pi)$, on en déduit $\alpha \equiv 0 \bmod 2$, puis finalement $\gamma \equiv 0 \bmod 2$, ce qui contredit la minimalité de m. Ainsi $\log(1+\pi) \in < \log x_{43}, \log x_2 > + \mathbb{Q}_2 \log \varepsilon$.

On vient donc de montrer que $\mathrm{Gal}(\widetilde{\mathrm{K}_S}/\mathrm{K}) = D_{\mathfrak{p}_2^{(2)}} \times < \mathrm{frob}(\mathfrak{p}_{43}) >$. Posons

$$\mathrm{K}_\infty = \widetilde{\mathrm{K}_S}^{<\mathrm{frob}(\mathfrak{p}_{43})>}$$

Le sous-corps K_∞ de K_S est une $\mathbb{Z}_2$-extension de K dans laquelle $\mathfrak{p}_2^{(2)}$ est totalement inerte. La place $\mathfrak{p}_2^{(1)}$ est totalement ramifiée dans $\mathrm{K}_\infty/\mathrm{K}$. Ainsi, pour $\mathrm{K}_\infty/\mathrm{K}$, $\tilde{t} = \tilde{s} = 0$.

6.1.2. *Le premier étage de* $\mathrm{K}_\infty/\mathrm{K}$.

Lemme 6.2. *Les extensions quadratiques de* K *contenues dans* K_S/K *sont les extensions* $\mathrm{K}(\sqrt{\theta})$, $\mathrm{K}(\sqrt{\varepsilon})$, $\mathrm{K}(\sqrt{x_5})$ *ainsi que leurs compositums. Les extensions quadratiques de* K *contenues dans* $\widetilde{\mathrm{K}}_S/\mathrm{K}$ *sont :* $\mathrm{K}(\sqrt{\varepsilon \cdot x_5})$, $\mathrm{K}(\sqrt{\theta})$, $\mathrm{K}(\sqrt{\theta \cdot \varepsilon \cdot x_5})$. *Le premier étage de la* $\mathbb{Z}_2$*-extension* $\mathrm{K}_\infty/\mathrm{K}$ *est le corps* $\mathrm{K}(\sqrt{\theta \cdot \varepsilon \cdot x_5})$.

Preuve. On peut noter que $x, \varepsilon \equiv 1 \bmod (\mathfrak{p}_2^{(2)})^2$. Les extensions $\mathrm{K}(\sqrt{\theta})$, $\mathrm{K}(\sqrt{\varepsilon})$ sont donc S-ramifiées.

On veut ensuite déterminer le p-radical de $\widetilde{\mathrm{K}_S}/\mathrm{K}$. Tout va se passer dans le corps de rayon $\mathrm{K}_\mathfrak{m}$ de K pour $\mathfrak{m} = (\theta^7)$.

Un calcul montre : $\mathrm{Cl}_{\mathrm{K},\mathfrak{m}} = \mathbb{Z}/4 \times (\mathbb{Z}/2)^2 =< \mathrm{Cl}(\mathfrak{p}_5), \mathrm{Cl}(\mathfrak{p}_5'), \mathrm{Cl}(\mathfrak{p}_7) >$, où $\mathfrak{p}_5$, $\mathfrak{p}_5'$, $\mathfrak{p}_7$ sont des idéaux premiers au-dessus de 5 et 7.

Il faut alors déterminer le développement de ces générateurs dans $U_{\mathfrak{p}_2^{(1)}}$:

- $\mathfrak{p}_5^2 = (x_5 := 3 - 8\theta - \theta^2 - \theta^3)$; $x_5 = (1+\pi)^{2+\cdots}(1+\pi^5)^{4(\cdots)}(1+\pi^6)^{4(\cdots)}$;
- ${\mathfrak{p}_5'}^2 = (x_5' := -5 + 8\theta + \theta^2 + \theta^3)$; $\varepsilon x_5' = (1+\pi)^{16+\cdots}(1+\pi^5)^{8+\cdots}(1+\pi^6)^{2+\cdots}$;
- $\mathfrak{p}_7^2 = (x_7 := -1 + 2\theta - 3\theta^2 - \theta^3)$; $\varepsilon x_7 = (1+\pi)^{4+\cdots}(1+\pi^5)^{2+\cdots}(1+\pi^6)^{4+\cdots}$

De l'algèbre linéaire élémentaire dans $\mathbb{F}_2$ montre que seul $\mathrm{Log}(\mathfrak{p}_7) \in 2\mathrm{Log}I_{\mathrm{K},S}$ (ici, $\Omega(1) = \{\mathfrak{p}_7\}$). Ainsi le radical des 2-extensions élémentaires de $\widetilde{\mathrm{K}}_S/\mathrm{K}$ est fixé par le frobenius de $\mathfrak{p}_7$.

Comme $\left(\frac{\varepsilon}{\mathfrak{p}_7}\right) = \left(\frac{x_5}{\mathfrak{p}_7}\right) = \left(\frac{3}{7}\right) - 1$, $\left(\frac{\theta}{\mathfrak{p}_7}\right) = \left(\frac{4}{7}\right) = 1$, concernant le radical, on conclut facilement.

Pour finir, rappelons que la place $\mathfrak{p}_{43} = (-1 + 17\theta + 3\theta^2 + 2\theta^3)$ doit être décomposée dans K_1/K. Comme $\theta \equiv 35 \bmod \mathfrak{p}_{43}$, $\varepsilon \equiv 32 \bmod \mathfrak{p}_{43}$ et $x_5 \equiv 26 \bmod \mathfrak{p}_{43}$, il vient, $\left(\frac{\theta}{\mathfrak{p}_{43}}\right) = -1$, $\left(\frac{\varepsilon}{\mathfrak{p}_{43}}\right) = +1$, et $\left(\frac{x_5}{\mathfrak{p}_{43}}\right) = -1$, d'où $\mathrm{K}_1 = \mathrm{K}(\sqrt{\theta \cdot \varepsilon \cdot x_5})$. □

6.1.3. *Les Λ-modules $\mathcal{X}_T^S$ et $\mathcal{X}_S^T$.* On peut calculer directement la torsion de $G_{1,S}^{ab}$ et noter que celle-ci est d'ordre 2. Si l'on montre que la S-condition cohomologique est satisfaite le long de $\mathrm{K}_\infty/\mathrm{K}$, alors la proposition 3.9 peut s'appliquer, pour obtenir $\mathrm{r}_S = \lambda_S = 0$, c'est à dire $H_S^{ab} \hookrightarrow \Lambda$.

D'autre part, d'après le corollaire 3.4, on a $\mathrm{cd}(G_S) \leq 2$. Comme le groupe G_S^{ab} a de la torsion, G_S n'est pas libre est ainsi $\mathrm{cd}(G_S) = 2$.

Il reste donc à s'assurer que l'on peut appliquer la proposition 3.9.

La stratégie va être la suivante. Nous allons d'abord contrôler le rang du défaut de la S-condition arithmétique le long de $\mathrm{K}_\infty/\mathrm{K}$. Pour ce faire, nous allons utiliser la dualité le long de $\mathrm{K}_\infty/\mathrm{K}$. Puis, nous appliquerons le corollaire 3.3.

Lemme 6.3. *On a l'égalité suivante :*

$$d_2 G_T^S = d_2 G_{1,T}^S = 1$$

Preuve. D'après la proposition 5.2, nous avons

$$d_p G_T^S = d_p G_S^T - 1$$

D'autre part, $G_S^{ab} \simeq \mathbb{Z}_2^2 \times \mathrm{Cl}_\mathrm{K}$. Comme $\mathfrak{p}_2^{(2)}$ est inerte dans $\mathrm{K}_\infty/\mathrm{K}$, on a $d_2 G_S^T = 2$, d'où $d_2 G_T^S = 1$.

Au niveau du second étage, la proposition 4.1 indique

$$d_p G_{1,T}^S = d_p G_{1,S}^T - 2$$

Après calcul, on a : $d_2 G_{1,S} = 4$. Comme la place de T est inerte dans $\mathrm{K}_\infty/\mathrm{K}$, il vient : $d_2 G_{1,S}^T = 4 - 1 = 3$. Par conséquent, $d_2 G_{1,T}^S = 1$. □

A noter que l'on obtient dès ici $\mathrm{r}_T^S = \rho_T^S = 0$, ceci par la proposition 2.8. En fait, le module $\mathcal{X}_T^S$ est de 2-rang égal à 1 et ainsi pour tout n, $d_2 G_{n,T}^S = 1$.

Utilisant la formule de la remarque 5, on en déduit $d_2 G_{n,S}^T = 2^n + 1$, et ce pour tout entier n. L'extension $\mathrm{K}_\infty/\mathrm{K}$ étant S-ramifiée mais pas T-décomposée, on obtient que pour tout n, $d_2 G_{n,S} = 2^n + 2$ (car $t_n = 1$).

On va appliquer le corollaire 3.3. Pour cela, on note que $\mathrm{rk}_{\mathbb{Z}_2} G_{n,S}^{ab} - {\rho_S}^n \leq 2$. Ainsi le polynôme caractéristique P_S de $\mathcal{X}_S$ ne peut-être divisible que par X ou bien par $X + 2$. Il faut donc vérifier que la S-condition arithmétique est satisfaite pour K et K_1. Pour K, c'est déja fait. Pour $\mathrm{K}_1 = \mathrm{K}(\alpha)$, avec $\alpha^8 + 7\alpha^6 + 26\alpha^4 + 56\alpha^2 + \alpha = 0$, on note que $E_{\mathrm{K}_1} =< \pm 1 > \times < \varepsilon_1, \varepsilon_2, \varepsilon_2 >$, tel que : $\varepsilon_1 \equiv 1 + \pi^{11} + \pi^{13} \bmod(\pi^{15})$, $\varepsilon_2 \equiv 1 + \pi^{11} \bmod(\pi^{15})$ $\varepsilon_5 \equiv 1 + \pi^2 + \pi^5 + \pi^{10} + \pi^{12} \bmod(\pi^1 5)$, où π est une uniformisante du complété de K_1 en l'unique place $\mathfrak{P}$ de K_1 au-dessus de $\mathfrak{p}_2^{(1)}$.

Si $\prod_i \varepsilon_i^{a_i} = 1$ est une relation linéaire entre les unités fondamentales ε_i de K_1, avec $a_i \in \mathbb{Z}_2$, il suffit de la regarder modulo π^{13}, pour obtenir $a_i = 0$, quelque soit $i = 1, 2, 3$. La condition arithmétique est donc vérifiée pour K_1. Le corollaire 3.3 s'applique. La S-condition cohomologique est vérifiée le long de $\mathrm{K}_\infty/\mathrm{K}$. □

Pour finir, notons que le corps $\mathrm{K}_1\mathrm{K}^H$ est absorbé dans une $\mathbb{Z}_2$-extension de K_1.

6.2. L'exemple qui vient illustre la proposition 5.3.

Soit le corps $\mathrm{K} = \mathbb{Q}(\theta)$, où θ vérifie $\theta^{10} + 2\theta^9 + 2\theta^8 + \theta^7 + 2 = 0$.

Le corps K est totalement imaginaire. L'anneau des entiers est $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\theta]$, $E_\mathrm{K} = \pm 1 < \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 >$, avec $\varepsilon_1 = \theta^7 + \theta^6 + \theta^5 + \theta^4 - 1$, $\varepsilon_2 = \theta^7 + 2\theta^6 + 2\theta^5 + \theta^4 + \theta^3 + \theta^2 - 1$, $\varepsilon_3 = \theta^9 + \theta^8 + 1$ et $\varepsilon_4 = \theta^9 + \theta^7 - \theta^6 + \theta^5 - \theta^4 + \theta^3 + 1$.

L'ideal $2\mathcal{O}_\mathrm{K}$ se factorise comme suit : $2\mathcal{O}_\mathrm{K} = {\mathfrak{p}_2^{(1)}}^7 \mathfrak{p}_2^{(2)} \mathfrak{p}_4$, où $\mathfrak{p}_4$ est un idéal premier de degré résiduel 2.

Posons $S = \{\mathfrak{p}_2^{(1)}, \mathfrak{p}_2^{(2)}\}$ et $T = \{\mathfrak{p}_4\}$.

On peut alors vérifier que $G_S^{ab} \simeq \mathbb{Z}_2^4 \times \mathbb{Z}/2\mathbb{Z}$. En particulier, K vérifie la S-condition arithmétique.

Exemple. Soit $\mathrm{K}(\theta)$ avec θ vérifiant $\theta^{10} + 2\theta^9 + 2\theta^8 + \theta^7 + 2 = 0$. Posons $S = \{(\theta), (1+\theta)\}$.

(i) Il existe une $\mathbb{Z}_2$-extension $\mathrm{K}_\infty/\mathrm{K}$ contenue dans K_S/K où le $\mathbb{Z}_2[[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]]$-module $H_S^{ab} := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)^{ab}$ a pour invariant $\rho_S = 3$ et $\mu_S = \lambda_S = 0$.

(ii) Le groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ est libre et la dimension cohomologique de G_S est exactement 2.

(iii) Il existe une $\mathbb{Z}_2$-extension $\mathrm{K}'_\infty/\mathrm{K}$ contenue dans K_S/K où le $\mathbb{Z}_2[[\mathrm{Gal}(\mathrm{K}'_\infty/\mathrm{K})]]$-module ${H'_S}^{ab}$ a pour invariant $\rho'_S = 3$ et $\mu'_S = 1$. Le groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}'_\infty)$ est de dimension cohomologique 2.

Détaillons succintement cet exemple.

6.2.1. *Une première $\mathbb{Z}_2$-extension.* Le logarithme de Gras permet ensuite de montrer que le corps $\mathrm{K}_1 = \mathrm{K}(\sqrt{\theta^2 + \theta})$, de degré 20 sur $\mathbb{Q}$, est le premier étage d'une $\mathbb{Z}_2$-extension de K contenue dans K_S/K. Soit K_∞ une telle $\mathbb{Z}_2$-extension. Pour cette $\mathbb{Z}_2$-extension, l'invariant ρ_S de $\mathcal{X}_S := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)^{ab}$ est donc égal à $\delta_S - (r_1 + r_2)$ c'est à dire à 3.

On vérifie dans un premier temps que $d_2 G_T = d_2 G_{1,T} = 0$.

D'après la proposition 2.8, $\mathcal{X}_T = 0$. Il en est donc de même pour $\mathcal{X}_T^S$.

D'après la remarque 5, pour tout n, $d_2 G_{n,S}^T = -t_n + s_n - 2 \cdot 2^n + 5 \cdot 2^n$.

Ainsi, $d_2 G_{n,S} - 2^n \rho_S \leq d_2 G_{n,S}^T + t_n \leq 2$.

D'après la proposition 3.1, la condition arithmétique est satisfaite le long de $\mathrm{K}_\infty/\mathrm{K}$ si et seulement si, elle l'est pour les corps K et K_1, ce que l'on peut vérifier.

Pour K_1, on note ensuite que le 2-rang de $\mathrm{Tor}_{\mathbb{Z}_2}(G_{1,S}^{ab})$ est égal à 1.

La proposition 3.9 s'applique et ainsi $\mathrm{r}_S = 0$.

Par conséquent, le groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}_\infty)$ est libre et donc $\mathrm{cd}(G_S) = 2$.

6.2.2. *Une seconde $\mathbb{Z}_2$-extension.* Posons ensuite $S' = \{\mathfrak{p}_2^{(1)}\}$ et $T' = \{\mathfrak{p}_2^{(2)}, \mathfrak{p}_4\}$. Un calcul montre que le morphisme de $\mathbb{Z}_2$-modules $\varphi_{S'} := \mathbb{Z}_2 \otimes E_{\mathrm{K}}^{T'} \to U^1_{\mathfrak{p}_2^{(1)}}$ est injectif. Par conséquent, $\mathrm{rk}_{\mathbb{Z}_2} G_{S'}^{T',ab} = 7 - (4+2) = 1$. Il existe une unique $\mathbb{Z}_2$-extension K'_∞ de K contenue dans K_S et dans laquelle, les places $\mathfrak{p}_2^{(2)}$ et $\mathfrak{p}_4$ sont totalement décomposées. En fait, on a : $\mathrm{Gal}(G_{S'}^{T'}/\mathrm{K}) \simeq \mathbb{Z}_2$.

La proposition 5.3 indique que pour cette $\mathbb{Z}_2$-extension $\mathrm{K}'_\infty/\mathrm{K}$, l'invariant r'_S du $\mathbb{Z}_2[[\mathrm{Gal}(\mathrm{K}'_\infty/\mathrm{K})]]$-module $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}'_\infty)^{ab}$ est au moins 1. Calculons sa valeur exacte : Le corps $\mathrm{K}'_1 = \mathrm{K}(\sqrt{-\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 \cdot \theta})$ est le premier étage de $\mathrm{K}'_\infty/\mathrm{K}$. On vérifie ensuite que ${\rho'}_T^S = {\mathrm{r}'}_T^S = 0$. Ainsi, la proposition 5.3 indique que l'invariant r'_S est égal à 1.

En résumé, le pro-2-groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K}'_\infty)$ n'est pas libre. Il est de dimension cohomologique 2.

Bibliographie

[1] C. Batut, K. Belabas, H. Cohen, M. Olivier, *User's guide to PARI-GP*. A2X, Université Bordeaux I, 1999.

[2] N. Boston, *Explicit Galois groups of infinite p-extensions unramified outside p*, preprint 2003.

[3] N. Boston, *Some cases of the Fontaine-Mazur conjecture*. Journal of Number Theory **42** (1992), 285–291.

[4] N. Boston, *Some cases of the Fontaine-Mazur conjecture II*. Journal of Number Theory **75** (1999), 161–169.

[5] J.-M. Fontaine, B. Mazur, *Geometric Galois representations*. Elliptic curves, modular forms and Fermat's last theorem, Internat. Press, Cambridge, MA, 1995.

[6] R. Gillard, *Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes*. Crelle **358** (1985), 76–91.

[7] G. Gras, *Class Field Theory*. SMM, Springer 2003.

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

[9] G. GRAS, *Plongements kummériens dans les $\mathbb{Z}_p$-extensions*. Compositio Math. **55** (1985), 383–396.
[10] G. GRAS, J.-F. JAULENT, *Sur les corps de nombres réguliers*. Math. Z. **202** (1989), 343–365.
[11] K. HABERLAND, *Galois cohomology of algebraic number fields, With two appendices by Helmut Koch and Thomas Zink*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.
[12] F. HAJIR, C. MAIRE, *Extensions of number fields with ramification of bounded depth*. International Math. Research Notices **13** (2002), 667–696.
[13] H. HASSE, *Number Theory*. Classics in Mathematics, Springer, 1980.
[14] J.-F. JAULENT, *L'arithmétique des l-extensions*. Publications Math. de Besançon, 1986.
[15] J.-F. JAULENT, C. MAIRE, *Sur les invariants d'Iwasawa des tours cyclotomiques*. Canadian Math. Bulletin **46** (2003), 178–190.
[16] J.-F. JAULENT, T. NGUYEN QUANG DO, *Corps p-rationnels, corps réguliers et ramification restreinte*. J. Théorie des Nombres de Bordeaux **5** (1993), 343–363.
[17] J.-F. JAULENT, O. SAUZET, *Pro-l-extensions de corps de nombres l-rationnels*. Jour. Number Theory **65** (1997), 240–267.
[18] H. KOCH, *Galoissche Theorie der p-Erweiterungen*. VEB, Berlin, 1970.
[19] J. LABUTE, *Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$*. J. Reine Angew. Math., à paraître.
[20] C. MAIRE, *On the $\mathbb{Z}_l$-rank of abelian extensions with restricted ramification*. Journal of Number Theory **92** (2002), 376–404.
[21] A. MOVAHHEDI, *Sur les p-extensions des corps p-rationnels*. Math. Nach. **149** (1990), 163–176.
[22] A. MOVAHHEDI, T. NGUYEN QUANG DO, *Sur l'arithmétique des corps de nombres p-rationnels*. Sém. Théorie des Nombres, Paris (1987/89), Prog. Math **81**, 155–200.
[23] J. NEUKIRCH, A. SCHMIDT, K. WINGBERG, *Cohomology of Number Fields*. Grundlehren **323**, Springer-Verlag 2002.
[24] T. NGUYEN QUANG DO, *Formations de classes et modules d'Iwasawa*. Number Theory, Noordwijkerhout 1983, Lecture Notes in Math. **1068**, 167–185.
[25] A. SCHMIDT, *On the relation between 2 and ∞ in Galois Cohomology of Number Fields*. Compositio Math. **133** (2002), 267–288.
[26] A. SCHMIDT, *Circular sets of prime numbers and p-extensions of the rationals*, preprint, 2005.
[27] A. SCHMIDT, *Bounded defect in partial Euler characteristics*. Bull. London Math. Soc. **28** (1996), 463–464.
[28] L. SCHNEPS, *On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication*. Journal of Number Theory **25** (1987), 20–33.
[29] J.-P. SERRE, *Galois Cohomology*. Lecture Notes in Math., Springer-Verlag, Berlin, 1994.
[30] J.-P. SERRE, *Corps locaux*. Publications de l'Université de Nancago, Hermann, Paris, 1968.
[31] L.C. WASHINGTON, *Introduction to cyclotomic fields*. GTM **83**, Springer 1997.
[32] K. WINGBERG, *Galois groups of number fields generated by torsion points of elliptic curves*. Nagoya Math. J **104** (1986), 43–53 .

Christian MAIRE
GRIMM
Université Toulouse le Mirail
5, allées A. Machado
31058 Toulouse cédex
E-mail : maire@univ-tlse2.fr
URL: http://www.univ-tlse2.fr/grimm/maire