JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Landry SALLE

Sur les pro-p-extensions à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres

Tome 20, n° 2 (2008), p. 485-523.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_2_485_0>

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 485-523

Sur les pro-p-extensions à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres

par Landry SALLE

Résumé. On considère dans cet article les pro-p-extensions maximales à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres. Leur groupe de Galois est étudié, d'abord à travers le rang de la partie $\mathbb{Z}_p$-libre de leur abélianisé, puis par leurs nombres minimaux de générateurs et de relations. Pour cela, on utilise la théorie des corps de classes, et on reprend les éléments de l'étude par Koch des pro-p-extensions à ramification restreinte maximales, qui fonctionnent dans ce cadre au prix de quelques arguments techniques supplémentaires.

Abstract. We consider in this paper maximal pro-p-extensions with restricted ramification over the cyclotomic $\mathbb{Z}_p$-extension over a number field. We investigate their Galois groups, focusing first on the $\mathbb{Z}_p$-rank of their abelianization, and then on their minimal numbers of generators and relations. We make use of class field theory and we adapt Koch's arguments for the study of maximal pro-p-extensions with restricted ramification, under slight technical complications.

Introduction

Soient k un corps de nombres, p un nombre premier, k_∞ la $\mathbb{Z}_p$-extension cyclotomique de k, et S un ensemble fini de places finies de k. On s'intéresse dans cet article à la pro-p-extension S-ramifiée maximale de k_∞, notée $\tilde{L}_S(k_\infty)$, et à la sous-extension abélienne maximale de $\tilde{L}_S(k_\infty)/k$, notée $\tilde{L}_S(k_\infty)^{ab}$. Le cas $S = \emptyset$ sera d'un intérêt particulier, l'extension abélienne maximale correspondante, notée $\tilde{L}(k_\infty)^{ab}$, étant l'extension cyclotomiquement ramifiée, suivant l'article [5] de Jean-François Jaulent et Jonathan Sands. On remarque par ailleurs que dès que S contient toutes les places au-dessus de p, cette extension est précisément la pro-p-extension S-ramifiée maximale. Deux angles d'attaque sont envisagés.

Manuscrit reçu le 26 juin 2007.

On considère d'abord la partie $\mathbb{Z}_p$-libre du groupe $\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k)$, caractérisée donc en tant que $\mathbb{Z}_p$-module par son $\mathbb{Z}_p$-rang.

Définition 0.1. On note $\lambda^{ab} = \mathrm{rg}_{\mathbb{Z}_p}\ \mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty)$ le $\mathbb{Z}_p$-rang du groupe de Galois $\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty)$. Si $S \neq \emptyset$, on note $\lambda_S^{ab} = \mathrm{rg}_{\mathbb{Z}_p}\ \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty)$.

Plusieurs résultats dans ce sens sont disponibles dans l'article [5], concernant le cas $S = \emptyset$, donnant le $\mathbb{Z}_p$-rang, ou la structure de Δ-module, pour Δ un groupe de Galois d'une extension relative k/k_0, ainsi que dans l'annexe de l'article [3]. Cette approche est ici systématisée, conduisant aux théorèmes 1.4 et 2.4, qui se particularisent dans les situations étudiées par Jaulent et Sands, permettent de donner des résultats précis dans d'autres cas, et des estimations dans le cas général. L'outil essentiel est la théorie p-adique du corps de classes, telle que développée par Jaulent dans [2] ; les définitions des principaux objets de cette théorie sont brièvement rappelées dans la section *Notations*. Elle permet de faire apparaître notamment un groupe, noté $\phi_p(\tilde{\mathcal{E}}_{k,S})$, qui est l'image, par l'application de semi-localisation en p, des unités globales qui deviennent normes cyclotomiques locales aux places au-dessus de p, et ont une composante triviale en les places de S (voir définition 1.3). Notre méthode permet de déterminer le rang de ce groupe, sous la conjecture de Leopoldt, dans un certain nombre de situations.

On étudie ensuite, à la manière de Koch ([6]), le groupe $\mathrm{Gal}(\tilde{L}_S(k_\infty)/k)$ à travers son nombre de générateurs, qui est donc un majorant du $\mathbb{Z}_p$-rang précédent (théorème 3.3), et son nombre de relations (théorème 4.1). Ces deux calculs, menés indépendamment, font chacun apparaître un groupe de Kummer associé à la présente situation arithmétique (voir définition 3.1). Ce groupe intervient, comme dans les calculs de Koch, dans une majoration du noyau de Chafarevitch associé au H^2 des groupes de Galois considérés. Pour $S = \emptyset$, il a la particularité de se trivialiser pour des familles de corps de nombres au-delà des corps quadratiques imaginaires (proposition 3.5). Les outils de cette seconde partie sont la théorie des corps de classes, et la cohomologie galoisienne.

Enfin, on termine en raffinant le contrôle des relations par l'ajout de l'action du groupe de Galois d'une extension relative k/k_0 sur les groupes de cohomologie considérés, et par quelques remarques sur le comportement asymptotique des rangs calculés.

Remerciements

Ce travail est la première partie d'une thèse sous la direction de Christian Maire, que je ne saurais trop remercier. Je remercie aussi Jean-François

Jaulent et Thong Nguyen Quang Do pour l'intérêt qu'ils ont bien voulu porter à ce travail et pour les conseils qu'ils m'ont donné.

Notations

- p désigne un nombre premier.
- k un corps de nombres, E_k son groupe d'unités, $\delta(k)$ désigne une quantité valant 1 si le corps k contient les racines p-èmes de l'unité, 0 sinon. Cette notation est aussi utilisée pour les corps locaux. La lettre δ pourra aussi désigner le défaut de la conjecture de Leopoldt.
- $\mathrm{Pl}_p(k)$ est l'ensemble des places de k au-dessus de p.
- $\mathrm{Pl}_\infty(k)$ est l'ensemble des places à l'infini de k ; $r_1(k)$, et $r_2(k)$, les nombres de places respectivement réelles et complexes.
- S désigne un ensemble fini de places finies de k, qu'on sépare en $S_p = S \cap \mathrm{Pl}_p(k)$ et $S_0 = S - S_p$.
- k_∞ la $\mathbb{Z}_p$-extension cyclotomique de k, $\Gamma = \mathrm{Gal}(k_\infty/k)$ le groupe de Galois de cette extension.
- Pour un $\mathbb{Z}_p$-module A, nous notons $\mathrm{rg}_{\mathbb{Z}_p} A$ son $\mathbb{Z}_p$-rang. De même $\dim_{\mathbb{F}_p} E$ désigne la dimension du $\mathbb{F}_p$-espace vectoriel E.

Extensions de k.

- $H(k)$ est le p-corps de Hilbert, $H_S(k)$ la (pro-)p-extension abélienne maximale S-ramifiée de k.
- $\tilde{L}(k_\infty)^{ab}$ (l'extension abélienne cyclotomiquement ramifiée maximale) est la pro-p-extension abélienne, non ramifiée au-dessus de k_∞, maximale de k ; on note $\tilde{L}(k_\infty)$ la pro-p-extension non ramifiée maximale de k_∞, et ainsi, $\tilde{L}(k_\infty)^{ab}/k$ est la sous-extension abélienne maximale de $\tilde{L}(k_\infty)/k$.
- $\tilde{L}_S(k_\infty)^{ab}$(extension abélienne cyclotomiquement S-ramifiée maximale) est la pro-p-extension abélienne maximale de k, S-ramifiée au-dessus de k_∞. En particulier, si $S = \mathrm{Pl}_p(k)$, on retrouve la pro-p-extension p-ramifiée maximale de k, qu'on notera k_p.

Groupes multiplicatifs locaux. Les objets locaux ci-dessous sont introduits en vue d'utiliser la théorie p-adique locale du corps de classes, telle que développée par Jaulent dans [2]. Certaines notations diffèrent, notamment pour le groupe des normes cyclotomiques locales.

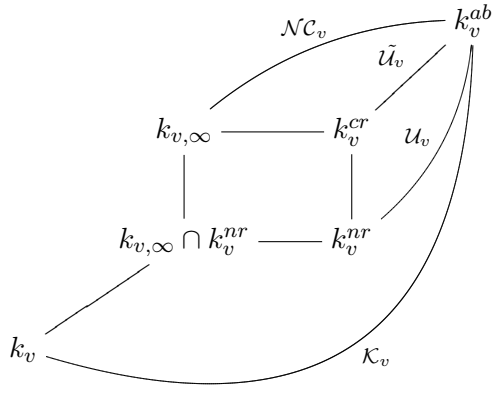
Pour une place non archimédienne v, on définit :

- $\mathcal{K}_v$ le compactifié p-adique du groupe multiplicatif $k_v^\times$ du localisé k_v de k en la place v, défini comme la limite projective $\varprojlim k_v^\times/(k_v^\times)^{p^n}$.
- $\mathcal{U}_v$ son sous-groupe unité. Si $v \mid p$, $\mathcal{U}_v$ s'identifie au produit direct du groupe fini $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v avec un $\mathbb{Z}_p$-module libre de rang $[k_v : \mathbb{Q}_p]$. Si, au contraire, $v \nmid p$, $\mathcal{U}_v$ est le groupe fini $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v.

– $\mathcal{NC}_v$ le groupe des normes cyclotomiques locales, défini comme le noyau d'une valuation logarithmique. Il coïncide avec $\mathcal{U}_v$, sauf dans le cas $v \mid p$, où c'est encore le produit direct du groupe fini $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v avec un $\mathbb{Z}_p$-module libre de rang $[k_v : \mathbb{Q}_p]$.
– $\tilde{\mathcal{U}}_v = \mathcal{U}_v \cap \mathcal{NC}_v$, groupe des unités qui sont normes cyclotomiques. Dans le cas où $v \mid p$, c'est le produit direct du groupe fini $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v avec un $\mathbb{Z}_p$-module libre de rang $[k_v : \mathbb{Q}_p] - 1$; chacun des deux quotients $\mathcal{U}_v/\tilde{\mathcal{U}}_v$ et $\mathcal{NC}_v/\tilde{\mathcal{U}}_v$ est un $\mathbb{Z}_p$-module libre de rang 1. Dans le cas où $v \nmid p$, ce groupe coïncide avec $\mathcal{U}_v$.

Dans le cas d'une place archimédienne v, on pose que $\mathcal{K}_v$ est trivial sauf si $p = 2$ et v est réelle, auquel cas on pose $\mathcal{K}_v = \mathcal{U}_v = \tilde{\mathcal{U}}_v \simeq \mathbb{Z}/2\mathbb{Z}$.

Par la théorie p-adique du corps de classes locale, ces groupes correspondent à des extensions abéliennes de k_v. Dans le cas où $v \mid p$, en posant k_v^{ab} la pro-p-extension abélienne maximale de k_v, k_v^{nr} sa pro-p-extension non ramifiée maximale (qui est une $\mathbb{Z}_p$-extension), $k_{v,\infty}$ sa $\mathbb{Z}_p$-extension cyclotomique, et k_v^{cr} le compositum de ces deux dernières, on obtient le diagramme d'extensions de corps suivant :



Groupes d'idèles.

– $\mathcal{J}_k$ est le p-adifié du groupe d'idèles ; c'est le produit des $\mathcal{K}_v$, restreint aux $\mathcal{U}_v$.
– $\tilde{\mathcal{J}}_k$ son sous-groupe qui est associé par la théorie p-adique du corps de classes globale à la $\mathbb{Z}_p$-extension cyclotomique de k. C'est le noyau de la formule du produit pour les valeurs absolues p-adiques.
– $\mathcal{U} = \mathcal{U}_k = \prod_v \mathcal{U}_v$ le sous-groupe des idèles unités ; $\tilde{\mathcal{U}} = \prod_v \tilde{\mathcal{U}}_v$, le sous-groupe des idèles unités qui sont normes cyclotomiques.
– $\mathcal{U}_p = \prod_{v|p} \mathcal{U}_v$; $\tilde{\mathcal{U}}_p = \prod_{v|p} \tilde{\mathcal{U}}_v$.
– $\mathcal{U}_{v\notin S} = \prod_{v\notin S} \mathcal{U}_v$; $\tilde{\mathcal{U}}_{v\notin S} = \prod_{v\notin S} \tilde{\mathcal{U}}_v$.
– $\mathcal{R}_k = \mathbb{Z}_p \otimes k^*$, le p-groupe des idèles principaux.
– $\mathcal{E}_k = \mathbb{Z}_p \otimes E_k$, le p-adifié du groupe des unités globales.

Lien entre unités globales et locales. Notons ϕ l'application de localisation :

$$\phi : \begin{array}{ccc} \mathcal{E}_k & \to & \prod_v \mathcal{U}_v \\ \epsilon & \mapsto & (\epsilon)_v \end{array}$$

On note ϕ_p la corestriction de ce morphisme au groupe $\mathcal{U}_p$, qu'on appelle application de semi-localisation en p. Son injectivité constitue la conjecture de Leopoldt. On note ϕ_v la corestriction à $\mathcal{U}_v$, pour v une place au-dessus de p, c'est l'application de localisation en v.

On désigne par $\tilde{\mathcal{E}_k}$ l'image réciproque par ϕ de $\tilde{U}$, c'est-à-dire les unités globales qui sont partout localement normes cyclotomiques. Rappelons que puisqu'on ne s'intéresse qu'aux p-parties, pour une unité la propriété d'être une norme cyclotomique est automatiquement vérifiée en dehors des places au-dessus de p.

Partie I : Partie $\mathbb{Z}_p$-libre

1. Sur le rang

Jaulent et Sands ont donné la valeur de l'invariant λ^{ab} dans un certain nombre de cas sur l'extension $k/\mathbb{Q}$: totalement décomposée en p, ou non décomposée en p, k corps CM (voir [5]). Rappelons par exemple le résultat suivant :

Théorème 1.1. *De manière générale, on a toujours la majoration, pour δ le défaut de la conjecture de Leopoldt en p pour k :*

$$\lambda^{ab} \leq r_2(k) + \delta.$$

Si de plus, p est totalement décomposé dans $k/\mathbb{Q}$, il y a égalité :

$$\lambda^{ab} = r_2(k) + \delta.$$

Enfin, si k admet un sous-corps k_0 tel que p est totalement décomposé dans $k_0/\mathbb{Q}$, et pour δ le défaut de la conjecture de Leopoldt en p pour le corps k_0 alors :

$$\lambda^{ab} \geq r_2(k_0) + \delta.$$

Démonstration. Pour la première assertion, il suffit de remarquer que $\tilde{L}(k_\infty)^{ab}$ est une sous-extension de k_p^{ab}, la pro-p-extension abélienne p-ramifiée maximale de k, et il est bien connu que $\mathrm{Gal}(k_p^{ab}/k)$ est de $\mathbb{Z}_p$-rang $r_2(k) + 1 + \delta$. En tant que quotient, $\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k)$ est de rang inférieur, et, par abélianité, on obtient le résultat sur le rang de $\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty)$.

Supposons maintenant que p est totalement décomposé dans $k/\mathbb{Q}$. Soit v une place de k au-dessus de p. Alors, par hypothèse de décomposition, $k_v = \mathbb{Q}_p$; ainsi, le localisé $(k_p^{ab})_v$ est contenu dans la pro-p-extension abélienne maximale $\mathbb{Q}_p^{ab}$, et contient sa $\mathbb{Z}_p$- extension cyclotomique $\mathbb{Q}_{p,\infty}$, qui est totalement ramifiée, et qui est la sous-extension p-ramifiée maximale de

$\mathbb{Q}_p^{ab}$ si p est impair, est d'indice fini dans cette extension si $p = 2$. Ainsi, le groupe d'inertie $I_v(k_p^{ab}/k) \simeq I_v((k_p^{ab})_v/\mathbb{Q}_p) = \mathrm{Gal}((k_p^{ab})_v/(k_p^{ab})_v \cap \mathbb{Q}_p^{nr})$ est isomorphe à un groupe de la forme $\mathbb{Z}_p \times$ (fini) (avec partie finie triviale si p est impair). Pour chaque place v, le corps fixé par $I_v(k_p^{ab}/k)$ est donc une extension de k, dont le groupe de Galois est de $\mathbb{Z}_p$-rang $r_2(k) + \delta$. Par compositum avec k_∞, on en déduit que k_p^{ab}/k_∞ est non ramifiée en v. Ceci étant vrai pour n'importe quelle place v au-dessus de p, et k_p^{ab}/k étant par définition non ramifiée aux autres places de k, on en déduit que $k_p^{ab} = \tilde{L}(k_\infty)^{ab}$, d'où la deuxième assertion.

La dernière assertion s'obtient tout simplement par compositum. □

Nous allons utiliser la théorie du corps de classes pour donner des estimations des invariants λ_S^{ab} valables pour tout corps de nombres.

Proposition 1.2. *Par la théorie p-adique du corps de classes, le groupe de Galois de la pro-p-extension cyclotomiquement ramifiée abélienne maximale $\tilde{L}(k_\infty)^{ab}/k$ s'interprète par l'isomorphisme suivant :*

$$\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k) \simeq \mathcal{J}_k/\mathcal{R}_k \prod_w \tilde{\mathcal{U}_w}.$$

Si S est un ensemble fini de places finies de k, on obtient :

$$\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k) \simeq \mathcal{J}_k/\mathcal{R}_k \prod_{w \notin S} \tilde{\mathcal{U}_w}.$$

Démonstration. Soit k^{ab} la pro-p-extension abélienne maximale de k. Alors, $\tilde{L}_S(k_\infty)^{ab}$ est la sous-extension de k^{ab}/k_∞ fixée par le sous-groupe engendré par les groupes d'inertie $I_v(k^{ab}/k_\infty)$, pour v parcourant l'ensemble des places de k_∞, en dehors de S. Par la théorie p-adique du corps de classes, on a l'isomorphisme :

$$\mathrm{Gal}(k^{ab}/k) \simeq \mathcal{J}_k/\mathcal{R}_k.$$

Par ailleurs, les sous-groupes d'inertie vérifient les isomorphismes :

$$I_v(k^{ab}/k) \simeq \mathcal{U}_v\mathcal{R}_k/\mathcal{R}_k.$$

Nous nous intéressons aux sous-groupes d'inertie pour la sous-extension k^{ab}/k_∞, et nous savons que le groupe de normes p-adique associé à l'extension abélienne k_∞/k est le groupe $\tilde{\mathcal{J}}$, noyau pour la formule du produit pour les valeurs absolues p-adiques principales. Ainsi, chaque groupe d'inertie dans l'extension k^{ab}/k_∞ vérifie :

$$I_v(k^{ab}/k_\infty) \simeq (\tilde{\mathcal{J}} \cap \mathcal{U}_v\mathcal{R}_k)/\mathcal{R}_k = \tilde{\mathcal{U}_v}\mathcal{R}_k/\mathcal{R}_k,$$

où $\tilde{\mathcal{U}_v} = \mathcal{U}_v \cap \mathcal{NC}_v$ est le groupe des unités locales en v qui sont normes cyclotomiques. On voit ainsi que le groupe des normes associé à l'extension abélienne $\tilde{L}_S(k_\infty)^{ab}/k$ est le produit des $\tilde{\mathcal{U}_v}$, pour v n'appartenant pas à S. Le cas $S = \emptyset$ en particulier s'en déduit. □

Cette proposition permet d'estimer l'invariant λ_S^{ab} en fonction de la signature du corps considéré (liée aux places à l'infini), de quantités analogues pour les places au-dessus de p, et d'un sous-groupe du groupe des unités qu'on introduit :

Définition 1.3. Pour k un corps de nombres, et S un ensemble fini de places finies de k, on note $\tilde{\mathcal{E}}_{k,S}$ le sous-groupe du p-adifié $\mathcal{E}_k$ du groupe des unités globales, image réciproque par l'application de localisation ϕ de $\prod_{v\notin S}\tilde{\mathcal{U}}_v$. On note $\tilde{\mathcal{E}}_{k,S_p}$ l'image réciproque par ϕ_p de $\prod_{v\in \mathrm{Pl}_p(k)-S_p}\tilde{\mathcal{U}}_v$. La finitude des groupes $\tilde{\mathcal{U}}_v$ pour v ne divisant pas p permet de voir que les groupes $\tilde{\mathcal{E}}_{k,S}$ et $\tilde{\mathcal{E}}_{k,S_p}$ ont même $\mathbb{Z}_p$-rang.

Théorème 1.4. *L'invariant λ_S^{ab} vaut :*

$$\lambda_S^{ab} = \sum_{v\in S_p}[k_v:\mathbb{Q}_p] + \#(\mathrm{Pl}_p(k) - S_p) - (r_1 + r_2 - \delta) + \mathrm{rg}_{\mathbb{Z}_p}\phi_p(\tilde{\mathcal{E}}_{k,S}),$$

où ϕ_p est l'application de semi-localisation en p et δ le défaut de la conjecture de Leopoldt en p pour k.

En particulier, on a donc les inégalités :

$$\lambda_S^{ab} \geq \sum_{v\in S_p}[k_v:\mathbb{Q}_p] + \#(\mathrm{Pl}_p(k) - S_p) - (r_1 + r_2 - \delta)$$

et

$$\lambda_S^{ab} \leq \min\left(r_2 + \delta, \#(\mathrm{Pl}_p(k) - S_p) - 1 + \sum_{v\in S_p}[k_v:\mathbb{Q}_p]\right).$$

Remarque 1.5.

(1) Pour un corps k totalement réel, vérifiant la conjecture de Leopoldt, $\lambda_S^{ab} = 0$, pour tout S.
De manière générale, si $S = \mathrm{Pl}_p(k)$, on trouve :

$$\lambda_S^{ab} = r_2(k) + \delta,$$

ce qui est bien connu, puisque toutes les $\mathbb{Z}_p$-extensions d'un corps de nombres sont non ramifiées en dehors de $\mathrm{Pl}_p(k)$.

(2) Si p est totalement décomposé dans $k/\mathbb{Q}$, le minorant dans l'inégalité ci-dessus est précisément $r_2 + \delta$, et donc, pour n'importe quelle partie S de $\mathrm{Pl}_p(k)$:

$$\lambda_S^{ab} = r_2 + \delta.$$

On retrouve le résultat pour ce cas du théorème 1.1. Remarquons que ceci provient *in fine*, de la finitude (et même de la trivialité pour p impair) de $\tilde{\mathcal{U}}_p$ sous ces hypothèses.

(3) Si p n'est pas décomposé dans $k/\mathbb{Q}$, et $S = \emptyset$, alors $\#\mathrm{Pl}_p(k) = 1$ et $\#S_p = 0$, et donc :
$$\lambda^{ab} = 0,$$
par la majoration dans le théorème précédent. On retrouve ainsi encore un résultat de Jaulent et Sands ([5]).

Remarque 1.6. Le résultat est indépendant de $S_0 = S - S_p$. En particulier, si S est un ensemble fini de places dont l'intersection avec $\mathrm{Pl}_p(k)$ est vide, on trouve $\lambda_S^{ab} = \lambda^{ab}$. Ceci est à comparer avec la relation sur les invariants d'Iwasawa $\lambda_S = \lambda + \#S$, démontrée dans le cas où k est un corps à multiplication complexe, contenant les racines $2p$èmes de l'unité (voir par exemple [4]).

Démonstration. Nous avons de façon évidente une suite exacte :
$$1 \to \mathcal{R}_k\mathcal{U}/\mathcal{R}_k\tilde{\mathcal{U}}_{v\notin S} \to \mathcal{J}_k/\mathcal{R}_k\tilde{\mathcal{U}}_{v\notin S} \to \mathcal{J}_k/\mathcal{R}_k\mathcal{U} \to 1,$$
qui se traduit, *via* la correspondance p-adique du corps de classes, par la suite exacte de groupes de Galois :
$$1 \to \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/H(k)) \to \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k) \to \mathrm{Gal}(H(k)/k) \to 1.$$
Le dernier terme de ces deux suites est un p-groupe fini, donc de $\mathbb{Z}_p$-rang nul. Le $\mathbb{Z}_p$-rang de $\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k)$ est donc égal à celui du premier terme, que nous simplifions :
$$N = \mathcal{R}_k\mathcal{U}/\mathcal{R}_k\tilde{\mathcal{U}}_{v\notin S} \simeq \mathcal{U}/\mathcal{R}_k\tilde{\mathcal{U}}_{v\notin S} \cap \mathcal{U}.$$
Or, tout idèle p-adique principal qui est partout une unité p-adique locale, est unité p-adique globale, et donc :
$$N \simeq \mathcal{U}/\mathcal{E}_k\tilde{\mathcal{U}}_{v\notin S} = \mathcal{U}_{S\cup\mathrm{Pl}_p(k)}/\phi_{S\cup\mathrm{Pl}_p(k)}(\mathcal{E}_k)\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}.$$
La décomposition en somme directe
$$\left(\mathcal{U}_{S\cup\mathrm{Pl}_p(k)}/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}\right) \simeq \mathcal{U}_{S_0} \oplus \left(\mathcal{U}_p/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}\right),$$
où $\mathcal{U}_{S_0}$ est fini, induit une injection à conoyau fini :
$$\mathcal{U}_p/\left(\phi_{S\cup\mathrm{Pl}_p(k)}(\mathcal{E}_k)\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \cap \mathcal{U}_p\right) \to \left(\mathcal{U}_{S\cup\mathrm{Pl}_p(k)}/\phi_{S\cup\mathrm{Pl}_p(k)}(\mathcal{E}_k)\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}\right).$$
Le premier terme s'identifie à $\mathcal{U}_p/\phi_p(\mathcal{E}_{k,S_0})\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}$, où $\mathcal{E}_{k,S_0}$ désigne le sous-groupe de $\mathcal{E}_k$ des éléments qui sont appliqués par $\phi_{\mathrm{Pl}_p(k)\cup S}$ dans $\mathcal{U}_p$, c'est-à-dire qui ont des composantes locales triviales en les places de S_0 (définition 1.3). On utilise ensuite la suite exacte :
$$1 \to \phi_p(\mathcal{E}_{k,S_0})\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \to \mathcal{U}_p/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \to \mathcal{U}_p/\phi_p(\mathcal{E}_{k,S_0})\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \to 1,$$

dont le premier terme est isomorphe à :

$$\phi_p(\mathcal{E}_{k,S_0})/\phi_p(\mathcal{E}_{k,S_0}) \cap \tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} = \phi_p(\mathcal{E}_{k,S_0})/\phi_p(\tilde{\mathcal{E}}_{k,S}),$$

où $\tilde{\mathcal{E}}_{k,S}$ est (voir définition 1.3) le sous-groupe des éléments de $\mathcal{E}_k$ qui ont, par le morphisme ϕ de localisation, des composantes locales triviales en les places de S, et, en les places au-dessus de p, des composantes locales appartenant aux groupes de normes cyclotomiques. Par additivité des $\mathbb{Z}_p$-rangs dans les suites exactes, puisque les groupes finis ont $\mathbb{Z}_p$-rang nul, enfin, puisque $\mathcal{E}_{k,S_0}$ et $\mathcal{E}_k$ ont même $\mathbb{Z}_p$-rang, on obtient :

$$\begin{aligned}\lambda_S^{ab} + 1 &= \mathrm{rg}_{\mathbb{Z}_p}\, \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k) \\ &= \mathrm{rg}_{\mathbb{Z}_p}\, \mathcal{U}_p - \mathrm{rg}_{\mathbb{Z}_p} \tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} - \mathrm{rg}_{\mathbb{Z}_p}\, \phi_p(\mathcal{E}_k) + \mathrm{rg}_{\mathbb{Z}_p}\, \phi_p(\tilde{\mathcal{E}}_{k,S}).\end{aligned}$$

Or, les rangs des groupes d'unités locales sont connus :

$$\mathrm{rg}_{\mathbb{Z}_p}\mathcal{U}_p = \sum_{v\in \mathrm{Pl}_p(k)} \mathrm{rg}_{\mathbb{Z}_p}\, \mathcal{U}_v = \sum_{v\in \mathrm{Pl}_p(k)} [k_v : \mathbb{Q}_p] = [k : \mathbb{Q}],$$

$$\mathrm{rg}_{\mathbb{Z}_p}\, \tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} = \sum_{v\in \mathrm{Pl}_p(k)-S_p} \mathrm{rg}_{\mathbb{Z}_p}\, \tilde{\mathcal{U}}_v = \sum_{v\in \mathrm{Pl}_p(k)-S_p} ([k_v : \mathbb{Q}_p] - 1).$$

Pour ce qui est des unités globales, il est bien connu que $\mathrm{rg}_{\mathbb{Z}_p}\phi_p(\mathcal{E}_k) = r_1 + r_2 - 1 - \delta$, où δ est un entier positif, nul sous la conjecture de Leopoldt, et où r_1 est le nombre de plongements réels du corps k, et r_2 le nombre de couples de plongements complexes conjugués. On obtient ainsi la première identité.

Enfin, les inégalités proviennent simplement de ce que le $\mathbb{Z}_p$-rang du groupe $\phi_p(\tilde{\mathcal{E}}_{k,S})$ vérifie :

$$\begin{aligned}0 \le \mathrm{rg}_{\mathbb{Z}_p}\, \phi_p(\tilde{\mathcal{E}}_{k,S}) &\le \min\, \left(\mathrm{rg}_{\mathbb{Z}_p}\mathcal{E}_k, \mathrm{rg}_{\mathbb{Z}_p}\, \tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}\right) \\ &\le \min\, \left(r_1 + r_2 - 1 - \delta, \sum_{v\in \mathrm{Pl}_p(k)-S_p} ([k_v : \mathbb{Q}_p] - 1)\right).\end{aligned}$$

□

2. Avec une action galoisienne

On considère maintenant k comme une extension galoisienne d'un sous-corps k_0. Notons Δ le groupe de Galois de k sur k_0, qui est fini. Nous souhaitons reprendre le travail précédent en munissant chaque p-groupe considéré d'une structure supplémentaire de Δ-module, et en adaptant les identités obtenues précédemment caractère par caractère.

2.1. Rappel sur les structures. Les objets sur lesquels on veut faire agir Δ sont essentiellement de deux types : groupes de Galois d'extensions de k, d'une part, et groupes d'unités p-adiques de k, globales ou locales, d'autre part. Il est facile de vérifier que Δ agit bien sur les groupes de Galois, puisqu'ils sont définis par des propriétés de maximalité. Il agit aussi naturellement sur les unités globales, et ses sous-groupes de décomposition agissent sur les objets locaux, induisant des actions de Δ sur des objets semi-locaux (plus précisément sur les produits d'objets locaux, indicés par les places de k au-dessus d'une place de k_0). La correspondance du corps de classes p-adique établit ainsi des isomorhismes de Δ-modules.

Pour traiter le cas où de la S-ramification est autorisée, on fera l'hypothèse supplémentaire que l'ensemble S de places de k considéré est Δ-invariant, c'est-à-dire qu'il est exactement constitué de toutes les places de k au-dessus d'un ensemble $S(k_0)$ de places de k_0.

Pour n'avoir à considérer que des caractères absolument irréductibles, nous allons effectuer les calculs sur des $\mathbb{C}_p[\Delta]$-modules, obtenus par tensorisation par $\mathbb{C}_p$; nous omettrons de noter cette tensorisation ; elle aura par ailleurs pour effet que seules sont prises en compte les parties $\mathbb{Z}_p$-libres, les parties de $\mathbb{Z}_p$-torsion étant annulées par tensorisation par $\mathbb{Q}_p$. Pour A un $\mathbb{C}_p[\Delta]$-module, nous notons $\chi(A)$ son caractère. Il peut s'écrire sous la forme :

$$\chi(A) = \sum_{\chi} r_\chi(A)\chi,$$

où les entiers $r_\chi(A)$ sont les χ-rangs de A, pour χ parcourant les caractères $\mathbb{C}_p$-irréductibles de Δ. En particulier, ces rangs sont soumis à la relation :

$$\mathrm{rg}_{\mathbb{Z}_p} A = \sum_{\chi} r_\chi(A)\deg(\chi).$$

On notera $\chi(A) \leq \chi(B)$, pour A et B deux $\mathbb{C}_p[\Delta]$-modules, si, pour tout caractère $\mathbb{C}_p$-irréductible χ, on a l'inégalité $r_\chi(A) \leq r_\chi(B)$. Enfin, on notera $\chi(A) \wedge \chi(B)$ le caractère :

$$\chi(A) \wedge \chi(B) = \sum_{\chi} \min(r_\chi(A), r_\chi(B))\chi,$$

la somme portant encore sur les caractères $\mathbb{C}_p$-irréductibles de Δ.

Si Δ_w est un sous-groupe de Δ, soit A un $\mathbb{C}_p[\Delta]$-module et A_w un $\mathbb{C}_p[\Delta_w]$-module. On dit que A est induit par A_w s'il existe un sous-espace Δ_w-stable de A, noté A_0, qui soit Δ_w-isomorphe à A_w, et tel que les $\sigma(A_0)$, pour σ parcourant un système de représentants des classes de Δ/Δ_w, forment une somme directe égale à A. On note :

$$A = \mathrm{Ind}_{\Delta_w}^{\Delta} A_w,$$

et en ce qui concerne les caractères :

$$\chi(A) = \mathrm{Ind}_{\Delta_w}^{\Delta} \chi_{\Delta_w}(A_w).$$

Si on définit par **1** la représentation triviale (ou son caractère !), la représentation régulière du groupe Δ apparaît comme l'induite :

$$\mathrm{Reg} = \mathrm{Ind}_{1}^{\Delta} \mathbf{1},$$

et on rappelle que son caractère est donné par :

$$\chi(\mathrm{Reg}) = \sum_{\chi} \deg(\chi)\chi,$$

la somme portant sur tous les caractères $\mathbb{C}_p$-irréductibles de Δ.

Les suites exactes obtenues dans la première partie, dont nous avons vu qu'elles sont des suites exactes aussi pour les structures de Δ-modules, montrent alors :

Proposition 2.1.

$$\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k)) = \chi(\mathcal{U}_p) - \chi(\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}) - \chi(\phi_p(\mathcal{E}_k)) + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S})).$$

Dans la section suivante, on calcule certains des caractères intervenant dans cette identité.

2.2. Calculs de caractères. Le caractère des unités globales est connu par le théorème de Herbrand :

$$\chi(\mathcal{E}_k) = \sum_{v \in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta} \mathbf{1} \; - \mathbf{1},$$

où on a noté **1** le caractère de la représentation triviale. Nous reportons à la section suivante le calcul de ces induits. En ce qui concerne les unités p-adiques, on trouve donc :

$$\chi(\phi_p(\mathcal{E}_k)) \leq \chi(\mathcal{E}_k),$$

avec égalité sous la conjecture de Leopoldt.

Nous donnons le calcul du caractère des unités semi-locales, qui est aussi bien connu. Soit v une place de k_0 au-dessus de p ; on commence par calculer la représentation de Δ_w sur les unités locales en une place w de k au-dessus de v. Le théorème de la base normale assure un isomorphisme :

$$k_w \simeq (k_0)_v[\Delta_w].$$

Ceci concerne les structures additives des corps considérés. Pour en déduire des propriétés sur les unités, on considère le logarithme p-adique, qui lie la structure additive à la structure multiplicative. En considérant de plus les p-adifiés, $\mathcal{U}_v$ devient $[(k_0)_v : \mathbb{Q}_p]$ fois le $\mathbb{Z}_p[\Delta_w]$-module trivial, puisque Δ_w agit trivialement sur $\mathcal{U}_v$, et que ce dernier est de dimension $[(k_0)_v : \mathbb{Q}_p]$ en

tant que $\mathbb{Z}_p$-module, *via* le logarithme p-adique. On en déduit que $\mathcal{U}_w$ est $[(k_0)_v : \mathbb{Q}_p]$ fois le $\mathbb{Z}_p[\Delta_w]$-module régulier.

On calcule maintenant le caractère de l'action de Δ sur $\mathcal{U}_p$, en remarquant que ce module s'écrit $\prod_{v\in \mathrm{Pl}_p(k_0)} \prod_{w\in \mathrm{Pl}_v(k)} \mathcal{U}_w$, et que chaque facteur $\prod_{w\in \mathrm{Pl}_v(k)} \mathcal{U}_w$ admet une structure de Δ-module, qui est l'induite de la structure de Δ_w-module de $\mathcal{U}_w$. On mène donc le calcul :

$$\begin{aligned}\chi(\mathcal{U}_p) &= \sum_{v\in \mathrm{Pl}_p(k_0)} \chi\Big(\prod_{w\in \mathrm{Pl}_v(k)} \mathcal{U}_w\Big)\\ &= \sum_{v\in \mathrm{Pl}_p(k_0)} \mathrm{Ind}_{\Delta_w}^{\Delta} \chi_{\Delta_w}(\mathcal{U}_w)\\ &= \sum_{v\in \mathrm{Pl}_p(k_0)} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg})\\ &= [k_0 : \mathbb{Q}]\chi(\mathrm{Reg}).\end{aligned}$$

Il faut maintenant calculer le caractère de $\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}$. En chaque place w dans $\mathrm{Pl}_p(k)$, au-dessus d'une place v dans $\mathrm{Pl}_p(k_0)$, on a une suite exacte :

$$1 \to \tilde{\mathcal{U}_w} \to \mathcal{U}_w \to \mathbb{Z}_p \to 1,$$

où la composante $\mathbb{Z}_p$ est isomorphe à un sous-groupe ouvert de $\mathcal{K}_w/\mathcal{NC}_w \simeq \mathbb{Z}_p$, ce dernier groupe correspondant par le corps de classes au groupe de Galois $\mathrm{Gal}(k_{w,\infty}/k_w)$. Comme la $\mathbb{Z}_p$-extension cyclotomique de k provient du compositum par k de celle de k_0, le groupe Δ agit trivialement sur $\mathrm{Gal}(k_\infty/k)$. Ainsi, par densité, pour chaque place v de k_0, et chaque place w de k au-dessus de v, l'action de Δ_w sur $\mathrm{Gal}(k_{w,\infty}/k_w)$ est triviale ; et l'action de Δ sur le produit $\prod_{w|v} \mathrm{Gal}(k_{w,\infty}/k_w)$ est donc l'action induite par l'action triviale de Δ_w. Cette action induite étant indépendante du choix de la place w au-dessus de v, on notera $\mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}$ son caractère. Ainsi :

$$\begin{aligned}\chi(\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}) &= \chi(\mathcal{U}_{\mathrm{Pl}_p(k)-S_p}) - \chi\left(\prod_{v\in \mathrm{Pl}_p(k_0)-S_p} \prod_{w\in \mathrm{Pl}_v(k)} \mathbb{Z}_p\right)\\ &= \sum_{v\in \mathrm{Pl}_p(k_0)-S_p} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg}) - \sum_{v\in \mathrm{Pl}_p(k_0)-S_p} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1},\end{aligned}$$

et donc :

$$\begin{aligned}\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k)) \geq \sum_{v\in S_p} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg}) + \sum_{v\in \mathrm{Pl}_p(k_0)-S_p} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}\\ - \sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} \ + \mathbf{1} + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S})),\end{aligned}$$

avec égalité sous la conjecture de Leopoldt. On considère enfin la suite exacte naturelle de pro-p-groupes abéliens :

$$1 \to \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty) \to \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k) \to \mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_p \to 1.$$

Puisque le groupe Δ agit trivialement sur $\mathrm{Gal}(k_\infty/k)$, on déduit de ce qui précède la proposition :

Proposition 2.2. *On a l'égalité :*

$$\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty)) = \sum_{v\in S_p} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg}) + \sum_{v\in \mathrm{Pl}_p(k_0)-S_p} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} - \sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} + \chi_R + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S})),$$

où χ_R désigne la différence $\chi(\mathcal{E}_k) - \chi(\phi_p(\mathcal{E}_k))$, dont l'annulation constitue la conjecture de Leopoldt en p pour le corps k.

Remarque 2.3. Si $k = k_0$, on retrouve le théorème 1.4.

Il est possible que certains caractères irréductibles viennent avec un coefficient négatif dans la somme des trois premiers termes du membre de droite de l'identité. Cela implique alors que le terme $\chi_R + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S}))$ est supérieur à chacun de ces caractères, ce qui fournit en retour une amélioration de la minoration de rang obtenue en 1.4. Le résultat général est le suivant :

Théorème 2.4. *Le caractère virtuel :*

$$\sum_{v\in S_p} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg}) + \sum_{v\in \mathrm{Pl}_p(k_0)-S_p} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} - \sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}$$

s'écrit de façon unique sous la forme $\chi_+ - \chi_-$, où χ_+ et χ_- sont deux caractères, tels qu'aucun caractère irréductible ne divise les deux simultanément. On a alors les inégalités suivantes de caractères :

$$\chi_R + \chi(\phi_p(\mathcal{E}_k)) \wedge \chi(\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}) \geq \chi_R + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S})) \geq \chi_-,$$

et

$$\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty)) \geq \chi_+.$$

En particulier, on a la minoration :

$$\lambda_S^{ab} \geq \deg \chi_+.$$

Si, de plus, la conjecture de Leopoldt en p pour le corps k est vraie, et que l'égalité $\chi(\tilde{\mathcal{E}}_{k,S}) = \chi_-$ est vérifiée, alors on a l'égalité

$$\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty)) = \chi_+.$$

Démonstration. L'écriture sous la forme $\chi_+ - \chi_-$ est un fait classique en théorie des représentations de groupes (voir [9]). Le caractère $\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty))$ est positif et vaut alors :

$$\chi_+ - \chi_- + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S})) + \chi_R$$

ce qui montre l'inégalité :

$$\chi(\phi_p(\tilde{\mathcal{E}}_{k,S})) + \chi_R \geq \chi_-.$$

Par ailleurs, la majoration de ce caractère provient des inclusions de $\phi_p(\tilde{\mathcal{E}}_{k,S})$ dans $\phi_p(\mathcal{E}_k)$ et $\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}$. On obtient ensuite la minoration :

$$\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty)) = \chi_+ - \chi_- + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S})) + \chi_R \geq \chi_+,$$

qui devient une égalité sous les hypothèses supplémentaires $\chi_- = \chi(\phi_p(\tilde{\mathcal{E}}_{k,S}))$ et $\chi_R = 0$, et qui fournit l'égalité de rang attendue. □

2.3. Illustrations. Tous les résultats suivants seront des conséquences du théorème ci-dessus. **On suppose désormais la conjecture de Leopoldt vérifiée pour tous les corps considérés**, c'est-à-dire que $\chi_R = 0$. On est en mesure sous ces conditions de calculer entièrement l'invariant λ_S^{ab} pour n'importe quel corps CM, et donc en particulier pour toute extension abélienne de $\mathbb{Q}$, le cas des corps totalement réels ayant déjà été traité. Ce cas, pour $S = \emptyset$, était déjà traité dans l'article [5].

Par ailleurs, sous l'hypothèse $S = \emptyset$, le cas d'une extension non décomposée en p d'une extension totalement décomposée en p, peut aussi être traité ; cela donne une nouvelle formulation pour les extensions abéliennes de $\mathbb{Q}$, peut-être plus agréable.

En vertu de la remarque 1.6, on suppose ici $S \subset \mathrm{Pl}_p(k)$.

Corollaire 2.5. *Soit k un corps CM, et k^+ sa sous-extension totalement réelle maximale. Soit S un ensemble de places dans $\mathrm{Pl}_p(k^+)$. Soit T_1 l'ensemble des places de $\mathrm{Pl}_p(k^+) - S$ qui se décomposent dans k/k^+, T_2 celles qui ne se décomposent pas. Alors :*

$$\chi(\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty)) = (\#T_1 + \sum_{v \in S}[k_v^+ : \mathbb{Q}_p])\chi_c,$$

où χ_c est le caractère non trivial du groupe $\mathrm{Gal}(k/k^+) \simeq \mathbb{Z}/2\mathbb{Z}$, et donc :

$$\lambda_S^{ab} = \#T_1 + \sum_{v \in S}[k_v^+ : \mathbb{Q}_p].$$

Démonstration. Dans ce cas, tous les groupes de décomposition associés aux places à l'infini sont totaux, et donc :

$$\sum_{v \in \mathrm{Pl}_\infty(k^+)} \mathrm{Ind}_{\Delta_v}^{\Delta} \mathbf{1} = r_1(k^+)\mathbf{1} = [k^+ : \mathbb{Q}]\mathbf{1}.$$

Par ailleurs, suivant les définitions de T_1 et T_2 dans l'énoncé, et puisque le groupe Δ_v est trivial si v se décompose dans k/k^+, total si v ne se décompose pas :

$$\sum_{v\in \mathrm{Pl}_p(k^+)-S} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} = \#T_1(\mathbf{1}+\chi_c) + \#T_2\mathbf{1}.$$

Le caractère virtuel auquel on souhaite appliquer le théorème 2.4 est donc :

$$(\sum_{v\in S}[k_v^+:\mathbb{Q}_p] + \#T_1 + \#T_2 - [k^+:\mathbb{Q}])\mathbf{1} + (\sum_{v\in S}[k_v^+:\mathbb{Q}_p] + \#T_1)\chi_c.$$

En appliquant le théorème 2.4, on trouve donc ici :

$$\begin{aligned}\chi_+ &= (\sum_{v\in S}[k_v^+:\mathbb{Q}_p] + \#T_1)\chi_c,\\ \chi_- &= ([k^+:\mathbb{Q}] - (\#T_1 + \#T_2 + \sum_{v\in S}[k_v^+:\mathbb{Q}_p]))\mathbf{1}\\ &= (\sum_{v\in \mathrm{Pl}_p(k^+)-S}[k_v^+:\mathbb{Q}_p] - (\#T_1+\#T_2))\mathbf{1}.\end{aligned}$$

On remarque en particulier que le caractère χ_- ci-dessus est bien positif. On considère ensuite la majoration de $\chi(\phi_p(\tilde{\mathcal{E}}_{k,S}))$ établie dans le théorème 2.4. Ici :

$$\chi(\phi_p(\mathcal{E}_k)) \leq ([k^+:\mathbb{Q}]-1)\mathbf{1},$$

avec égalité sous la conjecture de Leopoldt, ce qui montre que $\phi_p(\tilde{\mathcal{E}}_{k,S})$ a χ_c-rang nul. Et, d'autre part :

$$\chi(\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S}) = \sum_{v\in T_1}([k_v^+:\mathbb{Q}_p]-1)\chi(\mathrm{Reg}) + \sum_{v\in T_2}([k_v^+:\mathbb{Q}_p]\chi(\mathrm{Reg})-\mathbf{1}),$$

ce qui montre que le $\mathbf{1}$-rang de $\phi_p(\tilde{\mathcal{E}}_{k,S})$ est majoré par $\sum_{v\in \mathrm{Pl}_p(k^+)-S}[k_v^+:\mathbb{Q}_p] - (\#T_1+\#T_2)$. On a donc obtenu :

$$\chi(\phi_p(\tilde{\mathcal{E}}_{k,S})) \leq \chi_-,$$

et on conclut par le théorème 2.4. □

Corollaire 2.6. *On suppose ici $S=\emptyset$. Supposons que $k_0/\mathbb{Q}$ est une extension p-décomposée, et k/k_0 une extension galoisienne non décomposée en toutes les places au-dessus de p ; ces conditions sont en particulier vérifiées pour une extension $k/\mathbb{Q}$ abélienne, avec k_0 la sous-extension p-décomposée maximale. Alors :*

$$\begin{aligned}\chi(\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty)) &= r_2(k_0)\mathbf{1},\\ \lambda^{ab} &= r_2(k_0).\end{aligned}$$

Démonstration. En effet, dans ce contexte :

$$\chi(\mathcal{U}_p) - \chi(\tilde{\mathcal{U}}_p) = \sum_{v \in Pl_p(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta} \mathbf{1} = \#\mathrm{Pl}_p(k_0)\mathbf{1} = [k_0 : \mathbb{Q}]\mathbf{1},$$

puisque chacun des groupes de décomposition en les places v au-dessus de p de l'extension k/k_0 est total. Par ailleurs, pour chaque place à l'infini v, une utilisation du théorème de Frobenius, qu'on rappelle :

$$(\mathrm{Ind}_{\Delta_v}^{\Delta} \mathbf{1}, \mathbf{1})_{\Delta} = (\mathbf{1}, \mathrm{Res}_{\Delta_v}^{\Delta} \mathbf{1})_{\Delta_v} = 1,$$

permet de montrer que le $\mathbf{1}$-rang est 1. Les places à l'infini sont au nombre de $r_1(k_0) + r_2(k_0)$, et donc, le caractère χ_+ introduit au théorème 2.4 est :

$$\chi_+ = ([k_0 : \mathbb{Q}] - r_1(k_0) - r_2(k_0))\mathbf{1} = r_2(k_0)\mathbf{1}.$$

Quant au caractère χ_-, il vérifie l'identité suivante. On remarque en particulier que son $\mathbf{1}$-rang est trivial :

$$\chi_- = \sum_{v \in \mathrm{Pl}_\infty(k_0)} (\mathrm{Ind}_{\Delta_v}^{\Delta} \mathbf{1} - \mathbf{1}).$$

On utilise ensuite la majoration de $\chi(\phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}}_p)$ établie dans le théorème 2.4. On a d'une part :

$$\chi(\tilde{\mathcal{U}}_p) = [k_0 : \mathbb{Q}](\chi(\mathrm{Reg}) - \mathbf{1}),$$

et ce dernier caractère a un $\mathbf{1}$-rang trivial, ce qui montre que $\phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}}_p$ a lui-même un $\mathbf{1}$-rang trivial. Et d'autre part, on trouve :

$$\chi(\phi_p(\mathcal{E}_k)) = -\mathbf{1} + \sum_{v \in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta} \mathbf{1},$$

et ce dernier caractère a le même χ-rang que χ_-, pour chaque caractère $\mathbb{C}_p$-irréductible non trivial χ. On en déduit l'inégalité :

$$\chi(\phi_p(\tilde{\mathcal{E}}_k)) \leq \chi_-,$$

puis les résultats attendus par application du théorème 2.4. □

Remarque 2.7. Cette situation est celle d'un corps à conjugaison l-adique selon la terminologie de Jaulent ; le résultat est présent dans son article [3] (théorème 25). Dans le cas général sur S, notre méthode ne permet de fournir que des encadrements ; la raison étant qu'on ne dispose pas d'estimation satisfaisante pour les groupes $\mathcal{E}_{k,S}$, des unités globales ayant une composante triviale en S, dès que S n'est pas vide, et qui seraient voués à jouer le rôle que joue $\mathcal{E}_k$ ici pour l'estimation des χ-composantes, avec χ caractère $\mathbb{C}_p$-irréductible non trivial.

Enfin, on applique dans la proposition suivante la méthode à une situation non abélienne. On constate qu'on ne parvient pas à une évaluation précise du rang en général ; toutefois on pourra obtenir une identité pour certains χ-rangs :

Corollaire 2.8. *On suppose toujours $S = \emptyset$. Soit $k/\mathbb{Q}$ une extension galoisienne et soit k_0 l'intersection des sous-corps fixés par les groupes de décomposition D_v, pour v parcourant $S_p(k)$. On suppose qu'aucune place à l'infini ne se complexifie dans l'extension k/k_0, et que les sous-groupes de décomposition $\Delta_v(k/k_0)$, pour $v \in \mathrm{Pl}_p(k)$, sont conjugués dans $\Delta = \mathrm{Gal}(k/k_0)$. Pour chaque caractère $\mathbb{C}_p$-irréductible χ_i de Δ, notons, indépendamment de la place $v \in Pl_p(k)$, $\alpha_i = r_{\chi_i}\mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}$. Alors, pour chacun de ces caractères :*

$$\begin{aligned}[k_0 : \mathbb{Q}]\alpha_i - \#\mathrm{Pl}_\infty(k_0)\deg\,\chi_i &\leq r_{\chi_i}\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty) \\ &\leq \min\left(r_2(k_0)\deg\,\chi_i, [k_0 : \mathbb{Q}]\alpha_i\right)\end{aligned}$$

Démonstration. Les groupes de décomposition associés aux places à l'infini sont triviaux, et donc :

$$\sum_{v\in\mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} = (r_1(k_0) + r_2(k_0))\chi(\mathrm{Reg}) = \#\mathrm{Pl}_\infty(k_0)\chi(\mathrm{Reg}).$$

Les groupes de décomposition associés aux places au-dessus de p sont tous conjugués, et l'extension $k_0/\mathbb{Q}$ est totalement décomposée en p, donc :

$$\sum_{v\in Pl_p(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} = [k_0 : \mathbb{Q}]\mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}.$$

Pour chaque caractère $\mathbb{C}_p$-irréductible χ_i de Δ, on introduit alors α_i comme dans l'énoncé, et on peut écrire les χ_i-rangs des caractères χ_+ et χ_- du théorème 2.4 :

$$r_{\chi_i}\chi_+ = \max\left([k_0 : \mathbb{Q}]\alpha_i - \#\mathrm{Pl}_\infty(k_0)\deg\,\chi_i, 0\right).$$

La minoration annoncée de $\chi(\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty))$ se déduit de la première identité, et du théorème 2.4. Par ailleurs, grâce aux estimations :

$$\chi(\phi_p(\mathcal{E}_k)) \leq \#\mathrm{Pl}_\infty(k_0)\chi(\mathrm{Reg})$$

et

$$\chi(\tilde{\mathcal{U}_p}) = [k_0 : \mathbb{Q}](\chi(\mathrm{Reg}) - \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}),$$

on obtient, pour chaque caractère $\mathbb{C}_p$-irréductible χ_i de Δ, la majoration suivante :

$$r_{\chi_i}\phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}_p} \leq \min\left(\deg\,\chi_i\#\mathrm{Pl}_\infty(k_0), [k_0 : \mathbb{Q}](\deg\,\chi_i - \alpha_i)\right).$$

En réinjectant dans l'expression de $\chi(\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty))$, on obtient la majoration attendue. □

On va spécialiser la proposition précédente dans le cas où le groupe Δ est un groupe diédral D_n à $2n$ éléments. La minoration de λ^{ab} dans le cas n impair est à relever, puisqu'elle permet de voir que le slogan *pour un choix naturel de k_0, on a l'identité $\lambda^{ab} = r_2(k_0)$*, vrai pour une extension abélienne de $\mathbb{Q}$, tombe en défaut en général.

On rappelle les points suivants sur les caractères d'un groupe diédral (voir [9]) : si n est impair, il y a deux caractères irréductibles de degré 1, notés χ_1, χ_2, et tous les autres sont de degré 2, on les notera ψ_j, $j = 1 \dots \frac{n-1}{2}$ (respectivement, si n est pair, χ_1, χ_2, χ_3, χ_4 les quatre caractères de degré 1, et $j = 1 \dots \frac{n}{2} - 1$ pour ceux de degré 2). On suppose que les caractères de degré 1 sont numérotés de telle sorte que ceux d'indice pair sont ceux de trace nulle.

Exemple 2.9. On se place dans la situation précédente et on suppose que Δ est isomorphe à D_n, le groupe diédral à $2n$ éléments. On suppose de plus que les groupes de décomposition Δ_v sont isomorphes à des relevés du quotient $\mathbb{Z}/2\mathbb{Z}$ de D_n. Alors, pour chaque caractère ψ_j de degré 2 :

$$r_{\psi_j}\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty) \leq 2r_2(k_0),$$

pour chaque caractère χ_i de degré 1 d'indice impair :

$$r_2(k_0) \leq r_{\chi_i}\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty) \leq 2r_2(k_0),$$

pour chaque caractère χ_i de degré 1 d'indice pair :

$$r_{\chi_i}\mathrm{Gal}(\tilde{L}(k_\infty)^{ab}/k_\infty) = 0.$$

En particulier, on constate que, si n est impair :

$$\lambda^{ab} \geq 2r_2(k_0).$$

Démonstration. Il suffit d'appliquer la proposition précédente, en précisant les coefficients α_i grâce au calcul d'induite suivant :

$$\mathrm{Ind}_{\mathbb{Z}/2\mathbb{Z}}^{D_n}\mathbf{1} = \sum_{i \text{ pair}} \chi_i + \sum_j \psi_j.$$

□

Partie II : Nombres de générateurs et de relations

On commence par rappeler la situation. Soient k un corps de nombres, p un nombre premier, $\mathrm{Pl}_p(k)$ les places de k au-dessus de p, et S un ensemble fini de places finies de k. On considère k_∞ la $\mathbb{Z}_p$-extension cyclotomique de k, et, si p est impair, $\tilde{L}_S(k_\infty)$ la pro-p-extension non ramifiée en dehors de S maximale du corps k_∞ ; si p est pair, on impose de plus que toutes les places réelles restent réelles dans cette extension. Notons, pour $S_1 \subset S_2$, l'inclusion suivante : $\tilde{L}_{S_1}(k_\infty) \subset \tilde{L}_{S_2}(k_\infty)$. On s'intéresse au groupe de Galois $G_S = \mathrm{Gal}(\tilde{L}_S(k_\infty)/k)$.

Pour estimer les nombres minimaux de générateurs, $d(G_S)$, et de relations, $r(G_S)$, des groupes G_S, nous allons exploiter les identités :

$$d(G_S) = \dim_{\mathbb{F}_p} H^1(G_S, \mathbb{F}_p)$$

et

$$r(G_S) = \dim_{\mathbb{F}_p} H^2(G_S, \mathbb{F}_p),$$

que nous regroupons dans la caractéristique d'Euler-Poincaré tronquée à l'ordre 2 :

$$\chi_2(G_S, \mathbb{F}_p) = 1 - d(G_S) + r(G_S)$$

Dans ce qui suit, nous omettons de noter les coefficients des groupes de cohomologie considérés lorsqu'ils sont $\mathbb{F}_p$.

3. Générateurs

On donne une expression pour le nombre minimal de générateurs des groupes considérés, en s'inspirant de l'étude par Koch dans le cas d'une pro-p-extension S-ramifiée maximale (voir [6], section 11.3). On commence par introduire les groupes de Kummer adaptés à notre situation arithmétique :

Définition 3.1. Pour S un ensemble fini de places finies de k, on note $\tilde{V}_S$ le sous-groupe suivant des idèles principaux :

$$\tilde{V}_S = \tilde{\mathcal{U}}_{v\notin S}\mathcal{J}_k^p \cap \mathcal{R}_k,$$

où $\tilde{\mathcal{U}}_{v\notin S}$ est le produit direct $\prod_{v\notin S}\tilde{\mathcal{U}}_v = \prod_{v\in \mathrm{Pl}_p(k)-S_p}\tilde{\mathcal{U}}_v \prod_{v\notin \mathrm{Pl}_p(k)\cup S_0}\mathcal{U}_v$; on remarque que $\tilde{V}_S$ est décroissant (pour l'inclusion) par rapport à S. Pour le cas $S = \emptyset$, on notera simplement $\tilde{V} = \tilde{V}_\emptyset$.

Dès que S contient toutes les places de $\mathrm{Pl}_p(k)$, le groupe $\tilde{V}_S/\mathcal{R}_k^p$ est égal au groupe de Kummer habituel $V_S/\mathcal{R}_k^p$.

Lemme 3.2. *Pour $S \neq \emptyset$, les dimensions des $\mathbb{F}_p$-espaces vectoriels $\tilde{V}_S/\mathcal{R}_k^p$ et $\tilde{\mathcal{E}}_{k,S}/\tilde{\mathcal{E}}_{k,S}^p$ vérifient l'inégalité :*

$$\dim_{\mathbb{F}_p}\tilde{\mathcal{E}}_{k,S}/\tilde{\mathcal{E}}_{k,S}^p + \delta(k) \leq \sum_{v\in S}\delta(k_v) + \dim_{\mathbb{F}_p}\tilde{V}_S/\mathcal{R}_k^p,$$

et pour $S = \emptyset$, elles vérifient :

$$\dim_{\mathbb{F}_p}\tilde{\mathcal{E}}_k/\tilde{\mathcal{E}}_k^p \leq \dim_{\mathbb{F}_p}\tilde{V}/\mathcal{R}_k^p.$$

Démonstration. Pour tout S, on a une injection naturelle :

$$\tilde{\mathcal{E}}_{k,S}/\tilde{\mathcal{E}}_{k,S}\cap\mathcal{R}_k^p \hookrightarrow \tilde{V}_S/\mathcal{R}_k^p,$$

et une suite exacte :

$$1 \to \tilde{\mathcal{E}}_{k,S}\cap\mathcal{R}_k^p/\tilde{\mathcal{E}}_{k,S}^p \to \tilde{\mathcal{E}}_{k,S}/\tilde{\mathcal{E}}_{k,S}^p \to \tilde{\mathcal{E}}_{k,S}/\tilde{\mathcal{E}}_{k,S}\cap\mathcal{R}_k^p \to 1.$$

Le premier terme de la suite ci-dessus s'écrit encore $\tilde{\mathcal{E}}_{k,S} \cap \mathcal{E}_k^p / \tilde{\mathcal{E}}_{k,S}^p$. On forme une application partant de ce dernier ensemble, à valeurs dans $\prod_{v \in S} \mu_p(k_v)/\mu_p(k)$, en envoyant un élément représenté par $\epsilon = a^p \in \tilde{\mathcal{E}}_{k,S} \cap \mathcal{E}_k^p$ sur la classe de la famille $(\phi_v(a))_{v \in S}$ modulo $\mu_p(k)$. En remarquant, pour $v \notin S$, que les quotients $\mathcal{U}_v/\tilde{\mathcal{U}}_v$ sont libres (de rang 1 ou 0 suivant qu'on est en une place au-dessus de p ou non), on vérifie facilement que les éléments ayant image nulle sont exactement ceux de $\tilde{\mathcal{E}}_{k,S}^p$. On a donc une injection :

$$\tilde{\mathcal{E}}_{k,S} \cap \mathcal{R}_k^p / \tilde{\mathcal{E}}_{k,S}^p \to \prod_{v \in S} \mu_p(k_v)/\mu_p(k),$$

et on en déduit le lemme. □

Théorème 3.3. *Le nombre minimal de générateurs du groupe de Galois* $G_S = \mathrm{Gal}(\tilde{L}_S(k_\infty)/k)$ *est :*

$$\sum_{v \in S_0} \delta(k_v) + \#(\mathrm{Pl}_p(k) - S_p) + \sum_{v \in S_p} ([k_v : \mathbb{Q}_p] + \delta(k_v)) \\ - \delta(k) - r_1(k) - r_2(k) + 1 + \dim_{\mathbb{F}_p} \tilde{V}_S/\mathcal{R}_k^p,$$

où $\delta(k)$*et* $\delta(k_v)$ *valent 1 ou 0 suivant que les racines p-èmes de l'unité sont ou non dans* k *et* k_v*.*

Démonstration. On considère la suite exacte de groupes de Galois :

$$1 \to \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/H(k)) \to \mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k) \to \mathrm{Gal}(H(k)/k) \to 1,$$

qui correspond par la théorie du corps de classes à la suite exacte d'idèles :

$$1 \to \mathcal{U}/\mathcal{E}_{k,S}\tilde{\mathcal{U}}_{v \notin S} \to \mathcal{J}_k/\mathcal{R}_k\tilde{\mathcal{U}}_{v \notin S} \to \mathcal{J}_k/\mathcal{R}_k\mathcal{U} \to 1.$$

En remplaçant maintenant le premier terme par un groupe dont il est un quotient naturel, puis en passant au quotient par les puissances p-èmes, on obtient la suite exacte de $\mathbb{F}_p$-espaces vectoriels :

$$\mathcal{U}/\mathcal{U}^p\tilde{\mathcal{U}}_{v \notin S} \to \mathcal{J}_k/\mathcal{R}_k\mathcal{J}_k^p\tilde{\mathcal{U}}_{v \notin S} \to \mathcal{J}_k/\mathcal{R}_k\mathcal{J}_k^p\mathcal{U} \to 1.$$

Le groupe $\mathcal{J}_k/\mathcal{R}_k\mathcal{J}_k^p\tilde{\mathcal{U}}_{v \notin S}$ correspond alors *via* la théorie du corps de classes à la sous-extension p-élémentaire maximale de $\tilde{L}_S(k_\infty)^{ab}/k$, soit encore la sous-extension abélienne p-élémentaire maximale de $\tilde{L}_S(k_\infty)/k$. Il est donc isomorphe à $G_S/[G_S, G_S]G_S^p$, et c'est un résultat classique en théorie des pro-p-groupes que le nombre minimal de générateurs de G_S est égal à la dimension de ce groupe en tant que $\mathbb{F}_p$-espace vectoriel :

$$\dim_{\mathbb{F}_p} \mathcal{J}_k/\mathcal{R}_k\mathcal{J}_k^p\tilde{\mathcal{U}}_{v \notin S} = d(G_S).$$

On note aussi les identités suivantes :

$$\dim_{\mathbb{F}_p} \mathcal{J}_k/\mathcal{R}_k\mathcal{J}_k^p\mathcal{U} = \dim_{\mathbb{F}_p} A(k)/p,$$

$$\dim_{\mathbb{F}_p}\mathcal{U}/\mathcal{U}^p\tilde{\mathcal{U}}_{v\notin S} = \sum_{v\in S_0}\delta(k_v) + \#(\mathrm{Pl}_p(k) - S_p) + \sum_{v\in S_p}([k_v:\mathbb{Q}_p] + \delta(k_v)),$$

où $A(k)$, le p-Sylow du groupe des classes de k, a été identifié à un quotient du p-adifié du groupe d'idèles.

Pour évaluer $d(G_S)$, on souhaite compléter à gauche la suite précédente. On commence par introduire $\tilde{V}_S \subset V$, définis par :

$$V = \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k,$$
$$\tilde{V}_S = \tilde{\mathcal{U}}_{v\notin S}\mathcal{J}_k^p \cap \mathcal{R}_k.$$

On dispose des isomorphismes suivants, induits par les inclusions, grâce au principe de Hasse pour les puissances p-èmes (voir par exemple [1], partie II, théorème 6.3.3) :

$$V/\mathcal{R}_k^p \simeq \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k\mathcal{J}_k^p/\mathcal{J}_k^p,$$
$$\tilde{V}_S/\mathcal{R}_k^p \simeq \tilde{\mathcal{U}}_{v\notin S}\mathcal{J}_k^p \cap \mathcal{R}_k\mathcal{J}_k^p/\mathcal{J}_k^p.$$

On obtient alors une suite exacte, de $\mathbb{F}_p$-espaces vectoriels, à cinq termes :

$$1 \to \tilde{V}_S/\mathcal{R}_k^p \to V/\mathcal{R}_k^p \to \mathcal{U}/\mathcal{U}^p\tilde{\mathcal{U}}_{v\notin S} \to \mathcal{J}_k/\mathcal{R}_k\mathcal{J}_k^p\tilde{\mathcal{U}}_{v\notin S} \to \mathcal{J}_k/\mathcal{R}_k\mathcal{J}_k^p\mathcal{U} \to 1,$$

dont toutes les flèches sauf la deuxième ont déjà été définies, la deuxième associant $u \in \mathcal{U}$ à $ua \in \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k\mathcal{J}_k^p$, avec $u \in \mathcal{U}$, $a \in \mathcal{J}_k^p$. L'exactitude de la suite aux deuxième et troisième termes sont les seuls points à ne pas avoir déjà été vérifiés et ne soulèvent pas de difficulté.

Enfin, le calcul suivant de la dimension de $V/\mathcal{R}_k^p$ est classique (voir [6], partie 11.2). On le reproduit ici pour pouvoir s'y référer plus loin. On remarque que V admet l'écriture suivante :

$$V = \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k = \{\alpha \in \mathcal{R}_k/\exists\mathfrak{a}, (\alpha) = \mathfrak{a}^p\}.$$

En effet, si $\alpha = a^p u \in \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k$, avec $a \in \mathcal{J}_k$, $u \in \mathcal{U}$, l'idéal $\mathfrak{a} = \prod_v \mathfrak{p}_v^{v(a_v)}$ convient pour cette définition. On peut alors former une flèche Ψ qui associe à un élément $\alpha \in V$ la classe de l'idéal $\mathfrak{a}$; elle est à valeurs dans le sous-groupe des éléments de p-torsion du groupe des classes, noté $A(k)[p]$. On obtient alors la suite exacte courte :

$$1 \to \mathcal{E}_k/\mathcal{E}_k^p \to V/\mathcal{R}_k^p \to^{\Psi} A(k)[p] \to 1,$$

dont on déduit :

$$\dim_{\mathbb{F}_p} V/\mathcal{R}_k^p = \dim_{\mathbb{F}_p} A(k)[p] + \delta(k) + r_1(k) + r_2(k) - 1,$$

où $\delta(k)$ vaut 1 ou 0 suivant que les racines primitives p-èmes de l'unité sont ou non dans k, et en notant que la suite exacte suivante, obtenue en considérant la multiplication par p dans $A(k)$:

$$1 \to A(k)[p] \to A(k) \to A(k) \to A(k)/p \to 1,$$

et la finitude de $A(k)$ permettent de montrer que $A(k)/p$ et $A(k)[p]$ ont même cardinal, et donc même dimension si on les considère munis d'une structure de $\mathbb{F}_p$-espaces vectoriels.

En rassemblant toutes ces identités, on obtient le résultat annoncé. □

Le terme le plus difficile dans les formules obtenues est $\tilde{V}_S/\mathcal{R}_k^p$. On souhaiterait obtenir des conditions de trivialisation de ce groupe, notamment en lien avec le théorème 4.1 (ou, plus exactement, sa preuve), puisqu'un tel résultat fournirait la trivialisation d'un noyau de Chafarevitch. On commence par donner un corollaire bien connu du calcul habituel sur $V/\mathcal{R}_k^p$.

Corollaire 3.4. *Si k est un corps quadratique imaginaire dont le groupe des classes a un cardinal premier à p, alors $V/\mathcal{R}_k^p$ est trivial, et donc a fortiori tous les $V_S/\mathcal{R}_k^p$ et tous les $\tilde{V}_S/\mathcal{R}_k^p$.*

La proposition suivante donne des conditions pour mener un calcul analogue sur $\tilde{V}/\mathcal{R}_k^p$. Notamment la deuxième assertion de la proposition fait intervenir des propriétés que vérifient les corps dits p-rationnels (voir par exemple [1], partie III, lemme 4.2.4, théorème 4.2.5, et partie IV, théorème 3.5, et la preuve du corollaire 3.6), ce qui, conjugué avec les estimations des rangs des groupes $\phi_p(\tilde{\mathcal{E}}_k)$ qui découlent des preuves de la partie I, fournit des conditions suffisantes pour la trivialité de $\tilde{V}/\mathcal{R}_k^p$ (corollaire 3.6). On espère mener ces calculs plus loin dans un travail ultérieur.

Proposition 3.5. *Soit k un corps de nombres, on considère la restriction $\tilde{\Psi}$ à $\tilde{V}/\mathcal{R}_k^p$ de l'application Ψ de $V/\mathcal{R}_k^p$ dans $A(k)[p]$ rappelée dans la démonstration du théorème 3.3. Les propriétés suivantes sont vérifiées :*

1. *Si le groupe des classes de k a cardinal premier à p, alors l'application $\tilde{\Psi}$ est triviale sur $\tilde{V}/\mathcal{R}_k^p$.*
2. *Si l'application de semi-localisation des unités globales en les places au-dessus de p est injective (Leopoldt), et si le groupe semi-local $\mathcal{U}_p = \prod_{v\in \mathrm{Pl}_p(k)} \mathcal{U}_v$ se scinde en une $\mathbb{Z}_p$-somme directe $\phi_p(\mathcal{E}_k) \oplus \mathcal{U}_p/\phi_p(\mathcal{E}_k)$, alors le noyau de l'application $\tilde{\Psi}$ est $\tilde{\mathcal{E}}_k/\tilde{\mathcal{E}}_k^p$.*

Corollaire 3.6. *Soit k un corps p-rationnel, dont la p-partie du groupe des classes est triviale, et vérifiant l'une des deux conditions :*

1. *pour p impair, $k/\mathbb{Q}$ est totalement décomposée en p.*
2. *pour $p \geq 5$, k est un corps CM, dont le sous-corps totalement réel maximal est une extension p-décomposée de $\mathbb{Q}$.*

Alors, le groupe $\tilde{V}/\mathcal{R}_k^p$ est trivial, et donc a fortiori tous les $\tilde{V}_S/\mathcal{R}_k^p$.

Démonstration. Un corps p-rationnel vérifie la condition 2 de la proposition : cette condition est exactement le quatrième item de la caractérisation (ii) du théorème 3.5 de la partie IV du livre de Gras ([1]) ; la partie sur

les racines de l'unité de notre condition étant automatiquement vérifiée. On obtient ainsi d'après la proposition un isomorphisme entre $\tilde{V}/\mathcal{R}_k^p$ et $\tilde{\mathcal{E}}_k/\tilde{\mathcal{E}}_k^p$. Sous l'une des deux hypothèses de décomposition, le groupe $\tilde{\mathcal{E}}_k$ est un $\mathbb{Z}_p$-module libre (il ne contient pas de racine p-ème de l'unité), et on montre que son $\mathbb{Z}_p$-rang est trivial en utilisant les résultats de la partie I (voir remarque 1.5 et corollaire 2.5). □

Exemple 3.7. On choisit $p = 5$, et $q = 31$. La relation $5^3 \equiv 1 \bmod 31$ permet de montrer que le Frobenius de $\mathbb{F}_5(\zeta_{31})/\mathbb{F}_5$ est d'ordre 3 ; ainsi la sous-extension de degré 5 de $\mathbb{Q}(\zeta_{31})/\mathbb{Q}$ est 5-décomposée et c'est une extension 31-ramifiée : il s'agit de la 5-extension (abélienne) 31-ramifiée maximale de $\mathbb{Q}$. On en déduit en particulier que la 5-partie de son groupe des classes est triviale. De plus, d'après la caractérisation des p-extensions p-rationnelles abéliennes de $\mathbb{Q}$ (voir [1], partie IV, exemple 3.5.1), il s'agit d'un corps 5-rationnel. Toujours pour $p = 5$, on a des résultats analogues pour $q = 191$ (en utilisant la relation $5^{19} \equiv 1 \bmod 191$), $q = 271$ (grâce à $5^{27} \equiv 1 \bmod 271$).

Démonstration. On prouve maintenant la proposition 3.5. La première assertion de la proposition est triviale. On montre la deuxième. Le noyau considéré est l'intersection :

$$(\mathcal{E}_k/\mathcal{E}_k^p) \cap \left(\tilde{V}/\mathcal{R}_k^p\right) = \left(\mathcal{E}_k \cap \tilde{\mathcal{U}}\mathcal{J}_k^p\right)/\mathcal{E}_k^p = \left(\mathcal{E}_k \cap \tilde{\mathcal{U}}\mathcal{U}^p\right)/\mathcal{E}_k^p.$$

On considère $\mathcal{E}_k \cap \tilde{\mathcal{U}}\mathcal{U}^p$ qui s'injecte *via* l'application de semi-localisation ϕ_p dans $\phi_p(\mathcal{E}_k)$. Son image est alors dans $\phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}}_p\mathcal{U}^p$; soit $e = \tilde{u_1}u_2^p$ un élément de cette image.

On remarque que l'hypothèse sur la section de $\mathcal{U}_p$ implique que $\tilde{\mathcal{U}}_p$ se scinde aussi en une somme directe $\phi_p(\tilde{\mathcal{E}}_k) \oplus \tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k)$. Justifions ce point. Pour chaque $\mathbb{Z}_p$-module considéré, on utilise la lettre F pour désigner sa partie libre, et T sa partie de torsion. On obtient donc une suite exacte :

$$1 \to F\phi_p(\mathcal{E}_k) \oplus T\phi_p(\mathcal{E}_k) \to F\mathcal{U}_p \oplus T\mathcal{U}_p \to F(\mathcal{U}_p/\phi_p(\mathcal{E}_k)) \oplus T(\mathcal{U}_p/\phi_p(\mathcal{E}_k)) \to 1.$$

La section qui existe par hypothèse se restreint en une flèche partant de $T(\mathcal{U}_p/\phi_p(\mathcal{E}_k))$, qui est forcément injective, et à valeurs dans $T\mathcal{U}_p$, ce qui permet d'obtenir une suite exacte scindée :

$$1 \to T\phi_p(\mathcal{E}_k) \to T\mathcal{U}_p \to T(\mathcal{U}_p/\phi_p(\mathcal{E}_k)) \to 1.$$

On en vient maintenant à considérer $\tilde{\mathcal{U}}_p$ et $\phi_p(\tilde{\mathcal{E}}_k) = \phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}}_p$. Il existe une injection naturelle de $\tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k)$ dans $\mathcal{U}_p/\phi_p(\mathcal{E}_k)$. On en déduit en particulier une injection de la torsion dans la torsion. Or, un sous-module de torsion particulier de $\tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k)$ est $T\tilde{\mathcal{U}}_p/T\phi_p(\tilde{\mathcal{E}}_k)$. Il se trouve que la torsion de $\phi_p(\mathcal{E}_k)$, comme celle de $\mathcal{U}_p$, est donnée par les racines p-èmes de l'unité,

globales ou locales, et ce sont des normes cyclotomiques locales. On en déduit :

$$T\tilde{\mathcal{U}}_p/T\phi_p(\tilde{\mathcal{E}}_k) = T\mathcal{U}_p/T\phi_p(\mathcal{E}_k) = T(\mathcal{U}_p/\phi_p(\mathcal{E}_k)),$$

puis l'égalité avec $T(\tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k))$. On a déjà vu que ce sous-module de torsion est scindé dans $T\mathcal{U}_p = T\tilde{\mathcal{U}}_p$; la partie libre $F(\tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k))$ se scinde dans $F\tilde{\mathcal{U}}_p$. On en déduit que la propriété de section est vraie pour la suite exacte :

$$1 \to \phi_p(\tilde{\mathcal{E}}_k) \to \tilde{\mathcal{U}}_p \to \tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k) \to 1.$$

On écrit, suivant ces sommes directes : $\tilde{u_1} = \tilde{e_1}a_1$, pour $\tilde{e_1} \in \phi_p(\tilde{\mathcal{E}}_k)$, et $a_1 \in \tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k)$, ce dernier ensemble s'incluant dans $\mathcal{U}_p/\phi_p(\mathcal{E}_k)$; et $u_2 = e_2a_2$, pour $e_2 \in \phi_p(\tilde{\mathcal{E}}_k)$, et $a_2 \in \mathcal{U}_p/\phi_p(\mathcal{E}_k)$. On a alors l'identité : $\frac{e}{\tilde{e_1}e_2^p} = a_1a_2^p$, entre deux éléments dans des espaces supplémentaires, et on en déduit $e = \tilde{e_1}e_2^p$, ce qui montre bien, par injectivité de ϕ_p, que le noyau considéré est $\tilde{\mathcal{E}}_k/\mathcal{E}_k^p \cap \tilde{\mathcal{E}}_k = \tilde{\mathcal{E}}_k/\tilde{\mathcal{E}}_k^p$. □

On en déduit le résultat suivant sur la torsion de l'abélianisé du groupe G_S.

Corollaire 3.8. *Notons* $\mathrm{tor}(G_S^{ab})$ *le sous-*$\mathbb{Z}_p$*-module de torsion de* G_S^{ab}*. La dimension du* $\mathbb{F}_p$*-espace vectoriel* $\mathrm{tor}(G_S^{ab})/p$ *est :*

$$\dim_{\mathbb{F}_p}\mathrm{tor}(G_S^{ab})/p = -\delta(k) + \sum_{v\in S}\delta(k_v) + \dim_{\mathbb{F}_p}\tilde{V}_S/\mathcal{R}_k^p - \mathrm{rg}_{\mathbb{Z}_p}\phi_p(\tilde{\mathcal{E}}_{k,S}) - \delta,$$

où δ *désigne le défaut de la conjecture de Leopoldt en* p *pour le corps* k*, et où* $\delta(k)$ *et* $\delta(k_v)$ *testent l'appartenance des racines* p*-èmes de l'unités aux corps* k *et* k_v*.*
Pour $p \geq 5$*, et un corps quadratique imaginaire, cette torsion est triviale. De même, pour* $p \geq 3$ *et pour un corps* k *ne contenant pas les racines de l'unité et vérifiant les hypothèses* 1 *et* 2 *de la proposition 3.5, si* $S = \emptyset$*, et pour* S *quelconque si de plus* $k/\mathbb{Q}$ *est totalement décomposée en* p*.*

Démonstration. La première assertion résulte du théorème 3.3, et du théorème 1.4 (se rappeler que l'invariant λ_S^{ab} diffère du $\mathbb{Z}_p$-rang de G_S^{ab} de 1). La deuxième assertion s'en déduit, grâce aux conditions d'annulation de $\tilde{V}_S/\mathcal{R}_k^p$ données dans le corollaire 3.6. En particulier, on utilise le fait qu'un corps quadratique imaginaire, ni aucun de ses localisés en les places au-dessus de p, ne contiennent les racines p-èmes de l'unité dès que $p \geq 5$. □

4. Relations

On va montrer le théorème suivant :

Théorème 4.1. *Le nombre de relations du groupe de Galois de la pro-p-extension S-ramifiée au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres vérifie, si p est impair :*

$$r(G_S) \leq \sum_{v\in S}^{*} \delta(k_v) + \dim_{\mathbb{F}_p} \tilde{V}_S/\mathcal{R}_k^p + \#(\mathrm{Pl}_p(k) - S_p),$$

la notation $*$ soulignant que la somme peut être diminuée de 1 si S est non vide, et que k contient les racines p-èmes de l'unité ; et si $p = 2$:

$$r(G_S) \leq 2\#(\mathrm{Pl}_2(k) - S_2) + \#S - 1 + \dim_{\mathbb{F}_2} \tilde{V}_S/\mathcal{R}_k^2 - \sum_{v\in \mathrm{Pl}_2(k)-S_2} \epsilon_v,$$

où ϵ_v est une quantité valant toujours 0 si l'inflation de la proposition 4.8 est un isomorphisme et 1 sinon.

Remarque 4.2. La détermination générale des quantités ϵ_v reposerait sur une extension de la proposition 4.8 ci-dessous au cas général, ce qui est délicat.

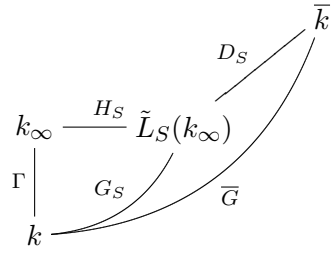
Corollaire 4.3. *La caractéristique d'Euler tronquée à l'ordre 2 du groupe G_S vérifie, si p est impair :*

$$\chi_2(G_S) \leq r_1(k) + r_2(k) + \delta(k) - \sum_{v\in S_p} [k_v : \mathbb{Q}_p],$$

le terme $\delta(k)$ pouvant être omis, si $S \neq \emptyset$; et, si $p = 2$:

$$\chi_2(G_S) \leq r_1(k) + r_2(k) + \#(\mathrm{Pl}_2(k) - S_2) - \sum_{v\in S_2} [k_v : \mathbb{Q}_2] - \sum_{v\in \mathrm{Pl}_2(k)-S_p} \epsilon_v.$$

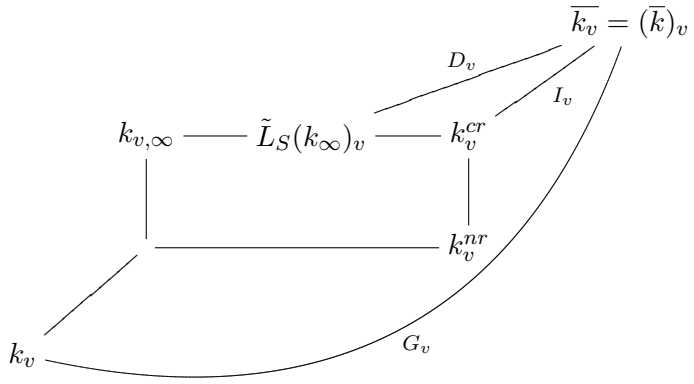
Démonstration. On introduit la pro-p-extension maximale de k, que nous notons $\overline{k}$, et on a la tour d'extensions globales suivante :



On introduit aussi la notation suivante, concernant les extensions de corps locaux :

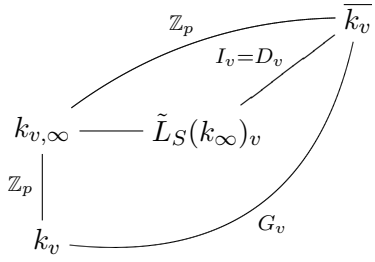
Définition 4.4. Si v est une place au-dessus de p, et k_v le localisé en cette place du corps de nombres k, alors k_v est une extension finie de $\mathbb{Q}_p$. On note k_v^{nr} la $\mathbb{Z}_p$-extension non ramifiée de k_v et k_v^{cr} le compositum de la $\mathbb{Z}_p$-extension cyclotomique de k_v et de k_v^{nr}. On note $\overline{k_v}$ la pro-p-extension maximale de k_v.

On commence par décrire les localisations en les places v de k en dehors de S (c'est-à-dire qu'on s'est fixé un prolongement de la place v à $\overline{k}$, et qu'on considère l'union des complétions des sous-extensions finies de $\overline{k}/k$, voir [10], paragraphe II.6) du diagramme d'extensions précédent. En une place $v \in \mathrm{Pl}_p(k) - S_p$, on obtient le diagramme d'extensions locales suivant :



Le groupe G_v est le pro-p-groupe de Galois absolu du corps local k_v, le groupe D_v introduit ici est le sous-groupe de décomposition en la place v du groupe de Galois global D_S, quant au groupe I_v, il est à la fois le sous-groupe d'inertie en la place v du groupe D_S, et du groupe $\mathrm{Gal}(\overline{k}/k_\infty)$ (l'extension $\tilde{L}_S(k_\infty)/k_\infty$ étant non ramifiée en v, qu'on a choisi en dehors de S).

En une place v en dehors de $\mathrm{Pl}_p(k)$, si le corps k_v ne contient pas les racines p-èmes de l'unité (c'est-à-dire si la norme Nv de l'idéal v n'est pas congrue à 1 modulo p), la pro-p-extension maximale de k_v est sa $\mathbb{Z}_p$-extension cyclotomique, qui est non ramifiée. En de telles places, on note I_v le groupe trivial. Dans le cas où Nv est congrue à 1 modulo p, on a en revanche le diagramme suivant :



Que v soit une place au-dessus de p ou non, on notera H_v le groupe quotient G_v/I_v. En particulier, dans le cas d'une place finie en dehors de $\mathrm{Pl}_p(k) \cup S$, le corps $\tilde{L}_S(k_\infty)_v$ est une extension non ramifiée de $k_{v,\infty}$ et est donc égal à $k_{v,\infty}$, ce qui implique que le groupe H_v est isomorphe à $\mathbb{Z}_p$ dans ce cas. Pour une place au-dessus de p, le groupe H_v est le groupe de Galois $\mathrm{Gal}(k_v^{cr}/k_v)$

et est isomorphe à $\mathbb{Z}_p^2$. De manière générale, on remarque que les extensions locales introduites en les places en dehors de S, correspondant aux groupes H_v, peuvent être définies de manière purement locale.

Enfin, on fait la convention de prendre $H_v = G_v$, le pro-p-groupe de Galois absolu, et $I_v = 1$ en les places de S.

Le point central de la preuve va être une comparaison des suites de Hochschild-Serre globale :

$$H^1(G_S) \xhookrightarrow{inf} H^1(\overline{G}) \xrightarrow{res} H^1(D_S)^{G_S} \xrightarrow{tra} H^2(G_S) \xrightarrow{inf} H^2(\overline{G}) \ ,$$

et locale, pour chaque place v de k (et principalement pour les places en dehors de S) :

$$H^1(H_v) \xhookrightarrow{inf} H^1(G_v) \xrightarrow{res} H^1(I_v)^{H_v} \xrightarrow{tra} H^2(H_v) \xrightarrow{inf} H^2(G_v) \ .$$

Il s'agit maintenant de lier ces deux suites par des applications de localisation. On dispose tout d'abord du lemme :

Lemme 4.5. *Il existe une injection :*

$$H^1(D_S)^{G_S} \hookrightarrow \prod_{v \notin S, Nv \equiv 0,1(p)} H^1(I_v)^{H_v} \times \delta_{p,2}(\mathbb{Z}/2\mathbb{Z})^{r_1(k)} \ ,$$

où $\delta_{p,2}$ vaut 1 si $p = 2$, et vaut 0 sinon.

Remarque 4.6. On peut se demander si cette flèche peut être naturellement incluse dans un sous-groupe du produit direct, à la manière de la proposition 21, du chapitre II du livre de Serre [10].

Démonstration. L'extension $\tilde{L}_S(k_\infty)/k_\infty$ étant la sous-extension S-ramifiée non complexifiée maximale de $\overline{k}/k_\infty$, le groupe de Galois $D_S = \mathrm{Gal}(\overline{k}/\tilde{L}_S(k_\infty))$ est topologiquement et normalement engendré par les sous-groupes d'inertie I_v de $\mathrm{Gal}(\overline{k}/k_\infty)$, pour v décrivant les places finies de k en dehors de S, et, dans le cas $p = 2$, les places archimédiennes de k. Ceci induit une flèche entre le pro-p-produit libre des I_v et D_S dont l'image est bien sûr fermée, et dont la clôture normale de l'image est D_S entier. On compose cette flèche avec le passage au quotient $D_S/D_S^p[D_S, G_S]$; la composée est alors surjective. La flèche ainsi obtenue, qui part du produit libre des I_v, se factorise alors dans le produit direct des $I_v/I_v^p[I_v, G_v]$ et fournit une application surjective :

$$\prod_{v \notin S} I_v/I_v^p[I_v, G_v] \twoheadrightarrow D_S/D_S^p[D_S, G_S].$$

Par ailleurs, si la norme de la place finie v n'est pas 0 ou 1 modulo p, le groupe I_v est trivial, et de même pour une place infinie complexe, et une place infinie réelle si p est impair ; en revanche, pour une place infinie réelle, et $p = 2$, on a $I_v = G_v = \mathbb{Z}/2\mathbb{Z}$, et donc $I_v/I_v^2[I_v, G_v] \simeq$

$\mathbb{Z}/2\mathbb{Z}$. Le dual de Pontryagin de cette flèche est la restriction $H^1(D_S)^{G_S} \to \prod_{v\notin S, Nv\equiv 0,1(p), v\in \mathrm{Pl}_r(k)} H^1(I_v)^{H_v} \times \delta_{p,2}\mathbb{Z}/2\mathbb{Z}^{r_1(k)}$, qui est donc bien une injection. □

On fait maintenant la remarque clef suivante sur la suite de Hochschild-Serre locale, d'abord dans le cas p impair.

Proposition 4.7. *Si p est un nombre premier impair, alors pour chaque place v en dehors de S, l'inflation $H^2(H_v) \to H^2(G_v)$ est triviale.*

Démonstration. Si v est une place en dehors de $S \cup \mathrm{Pl}_p(k)$, alors le groupe H_v est isomorphe à $\mathbb{Z}_p$, donc est un pro-p-groupe libre, et donc $H^2(H_v)$ est trivial.

Pour $v \in \mathrm{Pl}_p(k) - S_p$, on remarque que le groupe de Galois de la pro-p-extension maximale $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$ est un pro-p-groupe libre qu'on note F. Alors, pour toute extension finie k_v de $\mathbb{Q}_p$, le pro-p-groupe de Galois absolu G_v au-dessus de k_v admet pour quotient $\mathrm{Gal}(\overline{\mathbb{Q}_p}.k_v/k_v)$, qui s'identifie à un sous-groupe ouvert de F. Par ailleurs le corps k_v^{cr} est compositum de k_v et $\mathbb{Q}_p^{cr}$, il est donc inclus dans le compositum $\overline{\mathbb{Q}_p}.k_v$, et ainsi, le groupe H_v est un quotient de $\mathrm{Gal}(\overline{\mathbb{Q}_p}.k_v/k_v)$. On a donc les inflations suivantes qui commutent :

$$\begin{array}{ccc} H^2(H_v) & \longrightarrow & H^2(G_v) \\ & \searrow \quad \nearrow & \\ & H^2(\mathrm{Gal}(\overline{\mathbb{Q}_p}.k_v/k_v)) & \end{array}$$

et puisque le groupe $\mathrm{Gal}(\overline{\mathbb{Q}_p}.k_v/k_v)$ est libre en tant que sous-groupe d'un groupe libre, on en déduit que le terme central est nul, d'où la trivialité de l'inflation qui nous intéresse. □

Le cas $p = 2$ est plus difficile à traiter, et on ne donne pas une réponse complète, mais seulement la proposition suivante. Il sera utile ici, dans le cas des places au-dessus de 2, d'utiliser le fait que les groupes en jeu dans l'inflation $H^2(H_v) \to H^2(G_v)$ sont définis de manière purement locale.

Proposition 4.8. *Si $p = 2$, pour chaque place v en dehors de $\mathrm{Pl}_2(k) \cup S$, en particulier les places réelles à l'infini, l'inflation $H^2(H_v) \to H^2(G_v)$ est triviale.*

Pour les places v au-dessus de 2, on considère un instant l'inflation $H^2(\mathrm{Gal}(K^{cr}/K)) \to H^2(\mathrm{Gal}(\overline{K}/K))$ comme un objet purement local ; elle vérifie les propriétés suivantes dans une extension finie K/K_0 d'extensions finies de $\mathbb{Q}_2$:

(1) *la trivialité et la non trivialité se propagent dans les extensions K/K_0 de degré impair.*

(2) *la trivialité et la non trivialité se propagent dans les extensions* K/K_0 *contenues dans* K^{cr}*.*

(3) *la trivialité se propage dans toutes les extensions* K/K_0*.*

(4) *l'inflation est non triviale pour le corps* $\mathbb{Q}_2$*, et triviale pour les corps quadratiques* $\mathbb{Q}_2(i)$ *et* $\mathbb{Q}_2(\sqrt{-2})$*, et pour les autres corps quadratiques non inclus dans* $\mathbb{Q}_2^{cr}$*.*

En particulier, si K *est une extension abélienne de* $\mathbb{Q}_2$*, l'inflation est non triviale si et seulement si la sous-pro-2-extension maximale de* $K/\mathbb{Q}_2$ *est incluse dans* $\mathbb{Q}_2^{cr}$*.*

Démonstration. On revient à la proposition. Le cas des places finies en dehors de $\mathrm{Pl}_2(k) \cup S$ se traite comme dans le cas p impair, et le cas des places réelles à l'infini provient de la trivialité de H_v.

Soit donc v une place au-dessus de 2. On oublie ici la situation globale sous-jacente pour se concentrer sur la situation locale. On dispose donc d'une extension finie $K = k_v/\mathbb{Q}_2$, et on note $H = H_v$, et $G = G_v$ les groupes intervenant dans l'inflation. On a le diagramme commutatif suivant :

$$\begin{array}{ccccc} H^1(H) & \times & H^1(H) & \xrightarrow{\cup} & H^2(H) \\ \downarrow{\scriptstyle inf} & & \downarrow{\scriptstyle inf} & & \downarrow{\scriptstyle inf} \\ H^1(G) & \times & H^1(G) & \xrightarrow{\cup} & H^2(G) \end{array}$$

Les deux suites horizontales définissent des formes bilinéaires non dégénérées, les groupes G et H étant des groupes de Demuchkin. On note (u_1^*, u_2^*) un système de générateurs de $H^1(H)$, qui correspond dans la théorie de Kummer à un système (u_1, u_2) de générateurs kummériens de la sous-extension 2-élémentaire maximale de K^{cr}/K. Un résultat sur le groupe de Demuchkin $H \simeq \mathbb{Z}_p^2$ (voir [8], proposition 3.9.13) montre alors que $u_1^* \cup u_2^*$ est non trivial, et est donc un générateur de $H^2(H)$. Il reste à considérer $\inf(u_1^* \cup u_2^*) = \inf(u_1^*) \cup \inf(u_2^*)$, élément du groupe $H^2(G)$. Il existe un isomorphisme canonique de ce groupe dans le groupe des racines 2-èmes de l'unité ([6], théorème 8.12), et l'élément du H^2 qui nous intéresse correspond au symbole de Hilbert local $(u_1, u_2)_2$ (en fait sa 2-partie). La trivialité de l'inflation est donc équivalente à la nullité de ce symbole.

On démontre maintenant les propriétés de propagation. Pour une extension finie K/K_0, on notera encore H et G les groupes correspondant à K, et H_0 et G_0, ceux correspondant à K_0.

(1) si l'extension est de degré impair, alors $K_0^{cr} \cap K$ est trivial, et on a une égalité $H = H_0$ donnée par la flèche de restriction des éléments de H au corps K_0^{cr}. Par ailleurs, le compositum $\overline{K_0}.K$ est inclus dans $\overline{K}$, ce qui fournit une surjection de G dans G_0. On considère alors le

diagramme commutatif suivant d'inflations :

$$\begin{array}{ccc} & H^2(H_0) = H^2(H) & \\ \swarrow & & \searrow \\ H^2(G_0) & \longrightarrow & H^2(G) \end{array}$$

Il s'agit donc de démontrer que la flèche diagonale de gauche est un isomorphisme si et seulement si celle de droite en est un ; c'est-à-dire que la flèche horizontale est un isomorphisme. Les abélianisés des groupes G et G_0 s'écrivent $G^{ab} \simeq \mathbb{Z}/2^f\mathbb{Z} \oplus \mathbb{Z}_2^{d_0-1} \oplus \mathbb{Z}_2^{d-d_0}$ et $G_0^{ab} \simeq \mathbb{Z}/2^f\mathbb{Z} \oplus \mathbb{Z}_2^{d_0-1}$; en particulier, les $d - d_0$ dernières composantes de G^{ab} se trivialisent *via* la surjection sur G_0^{ab}, et les parties de torsion sont les mêmes puisqu'elles sont données par les 2-Sylow des groupes de racines de l'unité de K et K_0 respectivement, qui sont égaux puisque l'extension est supposée de degré impair. On considère $(\overline{y_i})_{i\leq d}$ un système de générateurs de G^{ab}, compatible avec l'isomorphisme précédent, qui s'envoie donc sur un système de générateurs $(\overline{x_i})$ de G_0^{ab}. En particulier, $\overline{x_i}$ est trivial pour $i > d_0$. On relève le premier en un système y_i de générateurs de G, dont on note l'image dans G_0 par x_i, et par commutativité, on en déduit que les x_i ont pour image les $\overline{x_i}$ dans G_0^{ab}. Ainsi, les systèmes $(x_i)_{i\leq d}$ puis $(x_i)_{i\leq d_0}$ (d'après, par exemple [10], proposition 25 de la partie I) sont générateurs de G_0. On considère les pro-p-groupes libres F et F_0 engendrés respectivement par $(y_i)_{i\leq d}$ et $(x_i)_{i\leq d_0}$; il existe une surjection entre eux compatible avec celle entre G et G_0, et on a donc obtenu des présentations de G et G_0 compatibles suivant le diagramme :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & R_0 & \longrightarrow & F_0 & \longrightarrow & G_0 & \longrightarrow & 1 \end{array}$$

et une flèche entre R et R_0 se déduit de ce diagramme. En passant à l'abélianisé pour les groupes F, F_0, G et G_0, et en se rappelant les propriétés entre les $\overline{y_i}$ et les $\overline{x_i}$, on obtient le diagramme :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R/R\cap[F,F] & \longrightarrow & \mathbb{Z}_2^d & \longrightarrow & \mathbb{Z}/2^f\mathbb{Z} \oplus \mathbb{Z}_2^{d-1} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & R_0/R_0\cap[F_0,F_0] & \longrightarrow & \mathbb{Z}_2^{d_0} & \longrightarrow & \mathbb{Z}/2^f\mathbb{Z} \oplus \mathbb{Z}_2^{d_0-1} & \longrightarrow & 1 \end{array}$$

Les noyaux des deux flèches verticales de droites sont égaux, et ce sont des surjections, on en déduit l'égalité :

$$R/(R \cap [F,F]) = R_0/(R_0 \cap [F_0,F_0]) \simeq 2^f\mathbb{Z}_2.$$

Par ailleurs, les groupes R et R_0 sont à un générateur en tant que sous-groupes normaux fermés de F et F_0 respectivement donc les quotients $R/[R,F]$ et $R_0/[R_0,F_0]$ sont cycliques, et admettent respectivement $R/(R\cap[F,F])$ et $R_0/(R_0\cap[F_0,F_0])$ comme quotients. On en déduit l'égalité entre $R/[R,F]$ et $R_0/[R_0,F_0]$, puis entre $H^1(R)^F$ et $H^1(R_0)^{F_0}$, puis entre les H^2.

(2) sous la condition que K est contenu dans K_0^{cr}, les groupes H et G sont des sous-groupes ouverts respectivement des groupes H_0 et G_0. Les corestrictions respectives entre les H^2 sont des isomorphismes, puisque tous ces groupes sont des groupes à dualité de Poincaré de dimension 2 (voir [10], chapitre 1, point (4) de la preuve de la proposition 30). La commutation entre corestriction et inflation permet de conclure.

(3) le point précédent permet de se ramener au cas où $K\cap K_0^{cr}$ est réduit à K_0, et on conclut comme dans le point (1) (sans avoir besoin de montrer un isomorphisme entre les H^2, la propagation n'étant ici que dans un sens).

On passe maintenant aux calculs explicites pour $\mathbb{Q}_2$, $\mathbb{Q}_2(i)$ et $\mathbb{Q}_2(\sqrt{-2})$. Une base de générateurs kummériens pour $\mathbb{Q}_2^{cr}/\mathbb{Q}_2$ est $(2,5)$. L'extension $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ est non ramifiée, et 2 est une uniformisante de $\mathbb{Q}_2$, donc le symbole d'Artin $\left(2,\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2\right)$ est un générateur de son groupe de Galois, il agit non trivialement sur $\sqrt{5}$, ce qui montre que le symbole de Hilbert $(2,5)_2$ est non trivial, et donc la non trivialité de l'inflation considérée.

Pour $\mathbb{Q}_2(i)$, on a à nouveau le même système de générateurs kummériens. On passe par le corps global $\mathbb{Q}(i)$, et la formule du produit (voir [1], partie II, théorème 7.3) pour calculer le symbole de Hilbert. Toutes les places infinies sont complexes et les symboles correspondant sont triviaux, et en les places différentes de la place au-dessus de 2 et des deux places $(1+2i)$ et $(1-2i)$ au-dessus de 5, tant 2 que 5 sont des unités, et ont donc un symbole trivial modulo 2. En les deux places au-dessus de 5, les entiers 2 et 5 vus comme entiers 5-adiques donnent les mêmes extensions kummériennes $\mathbb{Q}_5(\sqrt[4]{2})$ et $\mathbb{Q}_5(\sqrt[4]{5})$; les deux symboles correspondant à ces deux places sont égaux, d'abord à une racine quatrième de l'unité, puis, en passant au carré puisqu'on s'intéresse au symbole modulo 2, leur produit est trivial. Par la formule du produit, on en déduit la trivialité du symbole $(2,5)_2 = (2,5)^2_{(1+i)}$, calculé dans $\mathbb{Q}_2(i)$.

Pour conclure en ce qui concerne le corps $\mathbb{Q}_2(\sqrt{-2})$, on suit la même démarche. La place 5 est cette fois-ci inerte dans $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$, et le calcul modulo cette place est trivial puisque $\sqrt{2} \in \mathbb{Q}_5(\sqrt{-2})$.

On a ainsi traité cinq extensions quadratiques de $\mathbb{Q}_2$: les trois incluses dans $\mathbb{Q}_2^{cr}$, et les deux ci-dessus. Pour les deux extensions restantes, $\mathbb{Q}_2(\sqrt{-5})$ et $\mathbb{Q}_2(\sqrt{6})$, on conclut de la façon suivante : on considère le compositum de $\mathbb{Q}_2(\sqrt{-5})$ avec $\mathbb{Q}_2(i)$; la trivialité de l'inflation dans $\mathbb{Q}_2(i)$ s'y propage puis redescend à $\mathbb{Q}_2(\sqrt{-5})$ puisqu'il s'agit d'une extension inerte de ce dernier corps, donc incluse dans $\mathbb{Q}_2(\sqrt{-5})^{cr}$; de même pour l'autre corps en prenant le compositum avec $\mathbb{Q}_2(\sqrt{-2})$.

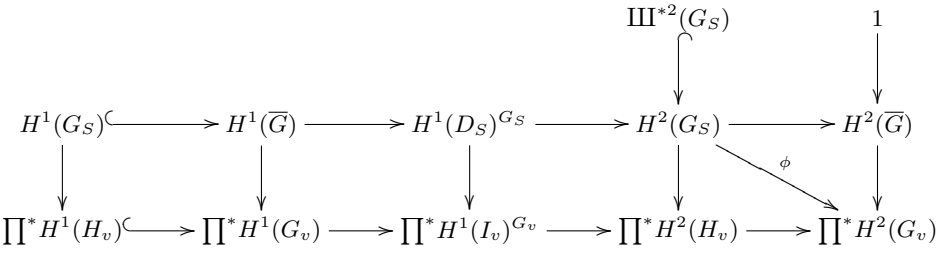
Plus généralement pour toute extension abélienne de $\mathbb{Q}_2$, la valeur de l'inflation se lit dans la sous-pro-2-extension maximale ; cette inflation est triviale dès que l'extension contient une extension quadratique de $\mathbb{Q}_2$ dans laquelle l'inflation est triviale, et donc, d'après ce qui précède, dès qu'elle contient une extension quadratique qui n'est pas dans $\mathbb{Q}_2^{cr}$, et donc dès qu'elle n'est pas incluse dans ce corps. □

Tous les éléments sont maintenant en place, et on commence la preuve du théorème proprement dite. On considère les applications suivantes, dont les lignes horizontales sont des suites de Hochschild-Serre, dont les lignes verticales n'ont aucune propriété d'exactitude, et dont les carrés sont commutatifs :

$$\begin{array}{ccccccccc}
H^1(G_S) & \xhookrightarrow{inf} & H^1(\overline{G}) & \xrightarrow{res} & H^1(D_S)^{G_S} & \xrightarrow{tra} & H^2(G_S) & \xrightarrow{inf} & H^2(\overline{G}) \\
\downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} \\
\prod H^1(G_{S,v}) & \xhookrightarrow{inf} & \prod H^1(G_v) & \xrightarrow{res} & \prod H^1(D_v)^{G_v} & \xrightarrow{tra} & \prod H^2(G_{S,v}) & \xrightarrow{inf} & \prod H^2(G_v) \\
\downarrow{\scriptstyle inf} & & \| & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle inf} & & \| \\
\prod H^1(H_v) & \xhookrightarrow{inf} & \prod H^1(G_v) & \xrightarrow{res} & \prod H^1(I_v)^{G_v} & \xrightarrow{tra} & \prod H^2(H_v) & \xrightarrow{inf} & \prod H^2(G_v)
\end{array}$$

En oubliant la suite exacte du milieu, on obtient alors le diagramme commutatif suivant, où on introduit le noyau de Chafarevitch $Ш^2(G_S)$ comme noyau de la quatrième flèche verticale. L'injectivité de la flèche verticale de droite est un résultat classique ([6], théorème 11.1), et, dans le cas où k contient les racines p-èmes de l'unité cette injectivité est assurée en corestreignant la flèche à la somme directe à laquelle on a ôté un terme (*ibid*, théorème 11.2), ce qu'on souligne par la notation $\prod^*$; le noyau $Ш^{*2}(G_S)$ apparaissant dans le diagramme est donc *a priori* plus grand que le noyau

de Chafarevitch introduit précédemment :



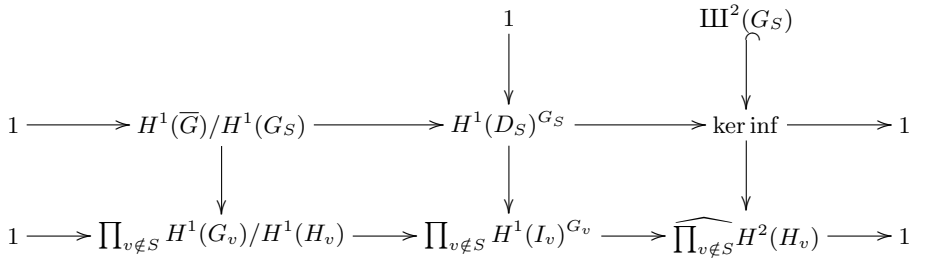
Cette injectivité permet d'obtenir la relation suivante, où on fait apparaître le noyau de l'inflation de $H^2(G_S)$ dans $H^2(\overline{G})$:

$$r(G_S) = \dim_{\mathbb{F}_p} H^2(G_S) = \dim_{\mathbb{F}_p} \ker\phi + \mathrm{rg}_{\mathbb{F}_p}\phi = \dim_{\mathbb{F}_p} \ker\inf + \mathrm{rg}_{\mathbb{F}_p}\phi,$$

et de s'assurer que le noyau $Ш^{*2}(G_S)$, et donc *a fortiori* le noyau de Chafarevitch $Ш^2(G_S)$, s'incluent dans le noyau de cette même inflation. La commutativité et la proposition 4.7 montrent que l'image de ϕ est incluse dans le produit direct fini $\prod^*_{v\in S} H^2(G_v) \times \left(\prod_{v\in \mathrm{Pl}_2(k)-S_2} H^2(G_v)\right)^{\delta_{2,p}}$. On a donc :

$$\mathrm{rg}_{\mathbb{F}_p}\phi \le \delta_{2,p} \sum_{v\in \mathrm{Pl}_2(k)-S_2} \delta(k_v) + \sum_{v\in S}^{*} \delta(k_v).$$

On déduit maintenant du diagramme précédent un nouveau diagramme dont les suites horizontales ont trois termes. Puisque les groupes G_v et H_v considérés sont égaux en les places au-dessus de S, et en utilisant le lemme 4.5, on vérifie facilement que le fait de considérer le terme $\ker\inf$ au lieu de $H^2(G_S)$ dans la suite horizontale supérieure permet de conserver l'exactitude du diagramme en ne considérant les suites locales qu'en des places en dehors de S. On utilise enfin les propositions 4.7 et 4.8 pour simplifier à droite les suites locales.



En particulier, la notation $\hat{\prod}$ souligne ici que dans le cas $p = 2$, il faut en fait considérer le produit :

$$\prod_{v\notin S\cup \mathrm{Pl}_2(k)} H^2(H_v) \prod_{v\in \mathrm{Pl}_2(k)-S_2} H^2(H_v)^{\alpha_v},$$

où chaque exposant α_v vaut 0 si l'inflation de la proposition 4.8 est un isomorphisme, et vaut 1 si elle est triviale. Le lemme du serpent permet alors d'obtenir une injection du groupe de Chafarevitch dans le conoyau de la flèche verticale de gauche, qu'on note abusivement res :

$$Ш^2(G_S) \hookrightarrow \mathrm{coker}(\mathrm{res}),$$

ce dont on déduit, en posant $\epsilon_v = 1 - \alpha_v$:

$$\begin{aligned}\dim_{\mathbb{F}_p} \ker\inf &\leq \dim_{\mathbb{F}_p}\mathrm{coker}(\mathrm{res}) + \widehat{\sum_{v\notin S}}\dim_{\mathbb{F}_p} H^2(H_v)\\ &= \dim_{\mathbb{F}_p}\mathrm{coker}(\mathrm{res}) + (1-\delta_{2,p})\#(\mathrm{Pl}_p(k) - S_p)\\ &\quad + \delta_{2,p}\sum_{v\in \mathrm{Pl}_2(k)-S_2}(1-\epsilon_v),\end{aligned}$$

la dernière égalité provenant de la description de H_v, suivant la nature de la place v, donnée au début de la preuve du théorème. Il reste donc à évaluer ce conoyau. Pour cela, on considère plutôt le diagramme dual :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & D_S/D_S^p[D_S,\overline{G}] & \xrightarrow{\psi} & \overline{G}/\overline{G}^p[\overline{G},\overline{G}] & & \\ & & \uparrow & & \uparrow{\scriptstyle \chi_1} & & \uparrow{\scriptstyle \chi_2} & & \\ 1 & \longrightarrow & \prod_{v\notin S} M_v & \longrightarrow & \prod_{v\notin S} I_v/I_v^p[I_v,G_v] & \longrightarrow & \prod_{v\notin S} I_v/I_v^p[G_v,G_v] & \longrightarrow & 1 \end{array}$$

Le dual de N est donc le terme $\ker\inf$. Donnons quelques précisions sur comment les suites horizontales du bas fournissent bien par dualité les suites horizontales inférieures dans le diagramme précédent. On part de la suite exacte :

$$1 \to I_v \to G_v \to H_v \to 1,$$

qui donne la suite exacte :

$$1 \to M_v \to I_v/I_v^p[G_v,I_v] \to G_v/G_v^p[G_v,G_v] \to H_v/H_v^p \to 1,$$

pour un certain $\mathbb{F}_p$-espace vectoriel M_v. On va voir que cette suite exacte à quatre termes se scinde en deux suites exactes à trois termes :

$$1 \to M_v \to I_v/I_v^p[G_v,I_v] \to I_v/I_v^p[G_v,G_v] \to 1,$$

qui est la suite qu'on veut dualiser, et,

$$1 \to I_v/I_v^p[G_v,G_v] \to G_v/G_v^p[G_v,G_v] \to H_v/H_v^p \to 1.$$

Justifions ceci : puisque le quotient $H_v = G_v/I_v$ est abélien, on a $I_v \supset [G_v,G_v]$, et puisqu'il est libre, on a $G_v^p \cap I_v = I_v^p$. On en déduit que le quotient $I_v/I_v^p[G_v,G_v]$ peut être vu comme un sous-groupe de $G_v/G_v^p[G_v,G_v]$, qui se trivialise dans H_v/H_v^p, et dont l'image dans $G_v/G_v^p[G_v,G_v]$ est la même que celle de $I_v/I_v^p[G_v,I_v]$, ce qui suffit pour écrire la seconde suite exacte. La première s'en déduit. La seconde suite exacte montre que le dual de $I_v/I_v^p[G_v,G_v]$ est bien $H^1(G_v)/H^1(H_v)$, et la suite duale de la première

est donc bien celle attendue. Les propositions 4.7 et 4.8 fournissent alors par dualité des estimations de l'espace M_v, dans certains cas.

Le conoyau cherché est alors dual du noyau de la flèche χ_2 dans le diagramme ci-dessus. On utilise maintenant les isomorphismes de corps de classes. Le groupe $\overline{G}/\overline{G}^p[\overline{G},\overline{G}]$ correspond par l'isomorphisme de corps de classes global à $\mathcal{J}_k/\mathcal{J}_k^p\mathcal{R}_k$, et chaque groupe $I_v/I_v^p[G_v,G_v]$ correspond à $\tilde{\mathcal{U}}_v/{\tilde{\mathcal{U}}_v}^p$. Le noyau de χ_2 est donc précisément $\tilde{\mathcal{U}}_{v\notin S}\cap\mathcal{J}_k^p\mathcal{R}_k/\tilde{\mathcal{U}}_{v\notin S}^p$, et fait l'objet du lemme :

Lemme 4.9. *On a un isomorphisme :*

$$\tilde{\mathcal{U}}_{v\notin S}\cap\mathcal{J}_k^p\mathcal{R}_k/\tilde{\mathcal{U}}_{v\notin S}^p\simeq\tilde{V}_S/\mathcal{R}_k^p.$$

Démonstration. Soit $(a_v)^p r$ un élément de $\tilde{\mathcal{U}}_{v\notin S}\cap\mathcal{J}_k^p\mathcal{R}_k$, avec $r\in\mathcal{R}_k$, et $(a_v)\in\mathcal{J}_k$. L'élément r est alors dans $\tilde{V}_S$. Si $(b_v)^p s$ est une autre écriture du même élément, on vérifie alors que r/s est un idèle principal qui est partout localement puissance p-ème, c'est donc une puissance p-ème d'un idèle principal : on a donc défini une flèche à valeur dans $\tilde{V}_S/\mathcal{R}_k^p$, qui est évidemment surjective.

Un élément dans le noyau est alors de la forme $r^p(a_v)^p$, sa composante en une place $v\notin S$ est donc dans $\tilde{\mathcal{U}}_v\cap\mathcal{K}_v^p$. Puisque le quotient $\mathcal{K}_v/\tilde{\mathcal{U}}_v$ est abélien libre (à 0, 1 ou 2 générateurs, suivant que v est réelle et $p=2$, que v est finie et en dehors de $\mathrm{Pl}_p(k)$, ou que v est dans $\mathrm{Pl}_p(k)$), on en déduit que cette intersection est ${\tilde{\mathcal{U}}_v}^p$, ce qui conclut la démonstration. □

On a donc montré :

$$\mathrm{coker}(\mathrm{res})\simeq(\tilde{V}_S/\mathcal{R}_k^p)^*,$$

le signe $*$ désignant ici l'espace dual, et cela conclut la démonstration du théorème. □

Enfin, on conclut cette partie en notant qu'il est possible de mener un calcul similaire en comparant, par la suite de Hoschschild-Serre, le groupe de Galois G_S au groupe de Galois de la pro-p-extension $\mathrm{Pl}_p(k)\cup S$-ramifiée maximale $\tilde{L}_{\mathrm{Pl}_p(k)\cup S}(k)$, qui est de type fini, et dont on connaît exactement les nombres minimaux de générateurs et de relations. Les résultats obtenus par ce calcul sont légèrement plus faibles que ceux exposés ici, le problème majeur étant que le localisé du corps $\tilde{L}_{\mathrm{Pl}_p(k)\cup S}(k)$ en une place v divisant p ne contient pas forcément le corps k_v^{cr}. Les théorèmes de Kuz'min (voir [8], théorème 10.6.4) et de Mukhamedov (voir [7]) donnent des conditions suffisantes pour qu'il en soit ainsi (corps global contenant les racines p-èmes de l'unité, ou corps CM, tel que toutes les places au-dessus de p sont décomposées depuis la sous-extension totalement réelle maximale). Ces théorèmes ont une portée plus générale, en cela qu'ils assurent que le localisé précédent contient toute la p-clôture algébrique du corps local k_v.

On pose donc la question de savoir si des conditions plus faibles peuvent assurer que le corps k_v^{cr} soit contenu dans le localisé précédent.

5. Remarques supplémentaires

5.1. Avec une action galoisienne. On considère à nouveau une action d'un groupe de Galois $\Delta = \mathrm{Gal}(k/k_0)$, cette fois sur les divers groupes de cohomologie qui sont intervenus dans les calculs de la section précédente. On suppose que ce groupe a cardinal premier à p. On suppose aussi que l'ensemble fini S de places de k considéré est invariant sous l'action de Δ, c'est-à-dire que si une place w de k au-dessus d'une place v de k_0 est dans S, alors toutes les autres places de k au-dessus de v sont aussi dans S.

Il vient, du fait que les extensions de k considérées sont maximales pour certaines propriétés, que les extensions $\tilde{L}_S(k_\infty)/k_0$ et $\overline{k}/k_0$ sont galoisiennes ; notons les groupes de Galois $\overline{\mathcal{G}} = \mathrm{Gal}(\overline{k}/k_0)$ et $\mathcal{G} = \mathrm{Gal}(\tilde{L}_S(k_\infty)/k_0)$. Les restrictions induisent des extensions de groupes :

$$1 \to \overline{G} \to \overline{\mathcal{G}} \to \Delta \to 1,$$
$$1 \to G \to \mathcal{G} \to \Delta \to 1,$$
$$1 \to D \to \overline{\mathcal{G}} \to \mathcal{G} \to 1,$$

et donc, Δ agit sur les groupes de cohomologie en $\overline{G}$ et G, et $\mathcal{G}$ agit sur les groupes de cohomologie en D ; et donc, par passage au quotient, Δ agit sur les sous-groupes fixés par G de ces derniers. De même, il y a des actions des groupes de décomposition de Δ sur les groupes de cohomologie locaux considérés, qui induisent des actions de Δ sur certaines sommes directes.

Les divers groupes de cohomologie étudiés dans la section précédente sont donc ainsi munis d'une structure de $\mathbb{F}_p[\Delta]$-modules. On considère leurs relevés en caractéristique zéro, pour obtenir une structure de $\mathbb{Z}_p[\Delta]$-module, qu'on tensorise ensuite par $\mathbb{C}_p$. Les caractères envisagés maintenant sont les caractères pour cette structure. L'hypothèse faite ici sur le cardinal du groupe Δ permet d'assurer que les Δ-modules considérés sont semi-simples (voir [9]).

Théorème 5.1. *Soit p un nombre premier impair, k/k_0 une extension galoisienne de corps de nombres de degré premier à p, de groupe de Galois Δ, et G_S le groupe de Galois de la pro-p-extension S-ramifiée maximale au-dessus de la $\mathbb{Z}_p$-extension cyclotomique de k, alors, les groupes de cohomologie de G_S voient leurs caractères pour la structure de Δ-module vérifier :*

$$\chi(H^1(G_S)) = \chi(\tilde{V}_S/\mathcal{R}_k^p) + \sum_{v\in S(k_0)} \chi(\mu_p(k_v))^* + \sum_{v\in S_p(k_0)} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg}) +$$
$$+ \sum_{v\in \mathrm{Pl}_p(k_0)-S_p(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} - \chi(\mu_p(k)) + \mathbf{1} - \sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1},$$

$$\chi(H^2(G_S)) \leq \chi(\tilde{V}_S/\mathcal{R}_k^p) + \sum_{v\in \mathrm{Pl}_p(k_0)-S_p(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} + \sum_{v\in S(k_0)} \chi(\mu_p(k_v))^*,$$

où le signe $*$ *désigne le dual, et donc :*

$$\chi(\chi_2(G_S)) \leq \chi(\mu_p(k)) + \sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} - \sum_{v\in S_p(k_0)} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg}),$$

où $\chi(\chi_2(G_S))$ *désigne la somme alternée des caractères* $\chi(H^i(G_S))$*, pour* i *allant de* 0 *à* 2*.*

Démonstration. Les deux premiers points sont des corollaires des démonstrations des théorèmes 3.3 et 4.1, et des calculs de caractères effectués dans la partie 1 ; le troisième point s'en déduit immédiatement. On souligne en particulier la trivialité de l'action de Δ_v sur le groupe H_v de la démonstration du théorème 4.1, et donc sur ses groupes de cohomologie, puisqu'il s'agit du groupe de Galois d'une extension qui provient par compositum d'une extension de $\mathbb{Q}_p$, et donc *a fortiori* de $(k_0)_v$. □

Exemple 5.2. Soit $p \neq 2$ et k un corps CM contenant les racines p-èmes de l'unité, de sous-corps totalement réel maximal k^+, et S un ensemble de places finies de k^+. Alors :

$$\chi(\chi_2(G_S)) \leq \left(\sum_{v\in \mathrm{Pl}_p(k^+)-S_p(k^+)} [k_v^+ : \mathbb{Q}_p]\right)\mathbf{1} - \left(1 - \sum_{v\in S_p(k^+)} [k_v^+ : \mathbb{Q}_p]\right)\chi_c,$$

où χ_c est la caractère irréductible non trivial du groupe $\mathrm{Gal}(k/k^+) \simeq \mathbb{Z}/2\mathbb{Z}$.

Démonstration. En effet, dans ce contexte, on trouve :

$$\chi(\mu_p(k)) = \chi_c,$$
$$\sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} = r_1(k^+)\mathbf{1},$$
$$\sum_{v\in S_p(k^+)} [k_v^+ : \mathbb{Q}_p]\chi(\mathrm{Reg})) = \sum_{v\in S_p(k^+)} [k_v^+ : \mathbb{Q}_p](\mathbf{1} + \chi_c).$$

En remarquant la relation :

$$r_1(k^+) = [k^+ : \mathbb{Q}] = \sum_{v\in S_p} [k_v^+ : \mathbb{Q}_p] + \sum_{v\in \mathrm{Pl}_p(k^+)-S_p} [k_v^+ : \mathbb{Q}_p],$$

on trouve le résultat annoncé. □

5.2. Comportements asymptotiques. L'extension $\tilde{L}_S(k_\infty)^{ab}$ est une sous-extension de $L_S(k_\infty)$, la pro-p-extension abélienne S-ramifiée maximale de k_∞. La théorie d'Iwasawa munit le groupe de Galois $\mathrm{Gal}(L_S(k_\infty)/k_\infty)$ d'une structure de $\mathbb{Z}_p[[\Gamma]]$-module, où Γ désigne le groupe de Galois k_∞/k, ou encore de $\Lambda = \mathbb{Z}_p[[T]]$-module, *via* un isomorphisme qui

fait correspondre à un progénérateur γ de Γ, le polynôme $T+1$; on notera alors $X_S(k_\infty) = \mathrm{Gal}(L_S(k_\infty)/k_\infty)$ ce groupe de Galois, pour faire ressortir sa structure de module d'Iwasawa. Il est pseudo-isomorphe à un module de la forme :

$$\Lambda^{\rho_S} \oplus \bigoplus_{i=1\ldots m_S} \Lambda/p^{a_i} \oplus \bigoplus_j \Lambda/(f_j^{b_j}),$$

où les f_j sont des polynômes distingués irréductibles, et les entiers ρ_S, $\mu_S = \sum_i a_i$, et $\lambda_S = \sum_j b_j \deg(f_j)$ sont appelés invariants d'Iwasawa de ce module. En particulier, pour $S = \emptyset$, il est connu que le module d'Iwasawa non ramifié $X(k_\infty)$ est de torsion, c'est-à-dire $\rho_S = 0$.

Le groupe de Galois $\mathrm{Gal}(\tilde{L}_S(k_\infty)^{ab}/k_\infty)$ est alors le quotient de $X_S(k_\infty)$ par le sous-module engendré par $\gamma - 1 = T$. Son $\mathbb{Z}_p$-rang λ_S^{ab} est la somme de l'invariant ρ_S et du nombre de composantes de la forme $\Lambda/(T^m)$ dans l'écriture sous forme canonique du Λ-module $X_S(k_\infty)$. Plus généralement, si on note k_n un étage de la $\mathbb{Z}_p$-extension cyclotomique de k, alors le groupe de la sous-extension maximale de $\tilde{L}_S(k_\infty)/k_\infty$ qui soit abélienne sur k_n est le quotient de $X_S(k_\infty)$ par le sous-module engendré par le polynôme $(1+T)^{p^n} - 1$, c'est-à-dire qu'il existe une suite exacte :

$$1 \to X_S(k_\infty)/\left((1+T)^{p^n} - 1\right) \to G_S(k_n)^{ab} \to p^n\mathbb{Z}_p \to 1.$$

L'invariant $\lambda_S^{ab}(k_n)$ vérifie donc une relation :

$$\lambda_S^{ab}(k_n) = p^n\rho_S + O(1),$$

où le terme $O(1)$ est majoré par l'invariant λ du module d'Iwasawa $X_S(k_\infty)$.

On peut aussi considérer le nombre de générateurs des groupes $G_S(k_\infty)^{ab}$, en prenant les quotients p-élémentaires dans la suite exacte ci-dessus. Par le théorème 3.3, en remarquant que les places finies sont finiment décomposées dans la $\mathbb{Z}_p$-extension cyclotomique, on obtient l'inégalité :

$$\dim_{\mathbb{F}_p} \tilde{V}_S(k_n)/\mathcal{R}_{k_n}^p + p^n\left(-r_1(k) - r_2(k) + \sum_{v\in S_p}[k_v : \mathbb{Q}_p]\right) \leq p^n(\rho_S + m_S) + O(1),$$

où on rappelle que m_S désigne le nombre de composantes de la forme $\Lambda/(p^a)$ dans la décomposition du Λ-module $X_S(k_\infty)$, et où le terme de gauche est borné inférieurement.

Puisque, si un corps k est CM, de sous-corps totalement réel k^+, les étages k_n de sa $\mathbb{Z}_p$-extension cyclotomique sont aussi des corps CM, de sous-corps totalement réel maximal k_n^+, on peut appliquer le corollaire 2.5 à tous ces étages, et on trouve :

Corollaire 5.3. *Si k est un corps CM de sous-corps totalement réel k^+, et S un ensemble de places au-dessus de p, alors :*

$$\rho_S = \sum_{v \in S} [k_v^+ : \mathbb{Q}_p].$$

Démonstration. Le corollaire 2.5 montre l'identité :

$$\lambda_S^{ab}(k_n) = \#T_{1,n} + \sum_{v \in S_n} [(k_n^+)_v : \mathbb{Q}_p],$$

où T_1 désigne une partie du complémentaire de S dans $\mathrm{Pl}_p(k^+)$. Le terme $\#T_{1,n}$ se stabilise, puisqu'aucune place au-dessus de p n'est infiniment décomposée dans la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres. Quant à l'autre terme, il vaut :

$$\begin{aligned}\sum_{w \in S_n} ([k_n^+)_w : \mathbb{Q}_p] &= \sum_{v \in S} \sum_{w|v} [(k_n^+)_w : k_v^+][k_v^+ : \mathbb{Q}_p] \\ &= \sum_{v \in S} [k_n^+ : k^+][k_v^+ : \mathbb{Q}_p] \\ &= p^n \sum_{v \in S} [k_v^+ : \mathbb{Q}_p],\end{aligned}$$

et on conclut par la remarque qui précède ce corollaire. □

Bibliographie

[1] Georges Gras. *Class field theory*. SMM. Springer, 2003.

[2] Jean-François Jaulent. Théorie l-adique globale du corps de classes. *Journal de Théorie des Nombres de Bordeaux*, 10 :355–397, 1998.

[3] Jean-François Jaulent. Plongements l-adiques et l-nombres de Weil. *preprint*, 2006.

[4] Jean-François Jaulent and Christian Maire. Sur les invariants d'Iwasawa des tours cyclotomiques. *Canadian Mathematical Bulletin*, 46 :178–190, 2003.

[5] Jean-François Jaulent and Jonathan Sands. Sur quelques modules d'Iwasawa semi-simples. *Compositio Mathematica*, 99 :325–341, 1995.

[6] Helmut Koch. *Galois theory of p-extensions*. SMM. Springer, 2002.

[7] V.G. Mukhamedov. Local extensions associated with the l-extensions of number fields with bounded ramification. *Mat. Zametki*, 35 :481–490, 1984.

[8] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. GmW. Springer, 2000.

[9] Jean-Pierre Serre. *Représentations linéaires des groupes finis*. Méthodes. Hermann, 1971.

[10] Jean-Pierre Serre. *Cohomologie galoisienne*. LNM. Springer, 1997 (1962).

Landry Salle
Université Paul Sabatier
Institut de Mathématiques de Toulouse
Équipe Émile Picard
118, route de Narbonne
31400 Toulouse
E-mail: salle@math.univ-toulouse.fr