





École doctorale Carnot-Pasteur

Thèse de doctorat

présentée par

Marine Rougnant

Pour obtenir le grade de
Docteur en Mathématiques de l'Université
de Bourgogne Franche-Comté

SUR QUELQUES ASPECTS DES EXTENSIONS À RAMIFICATION RESTREINTE

Thèse soutenue le 16 Avril 2018, devant le jury composé de :

Bruno Anglès	Rapporteur
Cécile Armana	Examinatrice
Bruno Deschamps	Examinateur et Président du jury
Florent Jouve	Rapporteur
Philippe Lebacque	Examinateur
Christian Maire	Directeur de thèse

Marine Rougnant
Université de Franche Comté, Laboratoire de Mathématiques, UMR CNRS 6623,
UFR Sciences et Techniques, 16 route de Gray, 25030 Besançon Cedex, France.
E-mail : marine.rougnant@univ-fcomte.fr

***Classification mathématique par sujets* (2010).** — 11R37, 11R29, 11R34, 12G10, 11R11.

Mots clefs. — Extensions de corps de nombres à ramification restreinte, pro-p groupes G_S, pro-p groupes *mild*, algèbre d'Iwasawa, corps p-rationnels.

SUR QUELQUES ASPECTS DES EXTENSIONS À RAMIFICATION RESTREINTE

Marine Rougnant

REMERCIEMENTS

Mes premiers remerciements vont naturellement à mon directeur de thèse, Christian Maire, qui m'a initiée à la recherche. Merci de m'avoir fait confiance, de m'avoir laissé tant d'autonomie et de m'avoir si bien conseillée et guidée. Merci d'avoir tant partagé avec moi et merci pour Halloween et tout le reste.

Je remercie également Bruno Anglès, Cécile Armana, Bruno Deschamps, Florent Jouve et Philippe Lebacque pour avoir accepté de faire partie de mon jury. C'est un grand plaisir et un honneur pour moi d'avoir pu partager mon travail avec eux. Merci plus particulièrement à Bruno Anglès et Florent Jouve pour leur travail de rapporteur.

Merci au Laboratoire de Mathématiques de Besançon pour son accueil et à tous ses membres pour leur extrême bienveillance. Je pense en particulier à Catherine, Pascaline, Lydie et Claudia qui ont toujours su garder le sourire face à mon incompétence administrative, à Odile et Emilie qui ferment les yeux sur deux mois de retard, à Christian, Christophe et Louis pour leurs soutiens aux différents projets des doctorants et à Romain, Richard, Christopher, Jean-Pierre et Julien pour leurs réponses efficaces à mes "Pourquoi ça marche pas ? !". Je pense aussi à Agnès et Cécile pour leur disponibilité, leurs conseils et leur gentillesse. Je n'oublie pas Martine, de l'Ecole Doctorale Carnot Pasteur qui m'a tant de fois "sauvée".

J'ai eu l'occasion de beaucoup voyager pendant ces trois années et demi. Cela a été très enrichissant et motivant. Je remercie Farshid Hajir, Emmanuel Giroux, Jàn et Leslie Minac et Hugo Chapdelaine de m'avoir si bien accueillie à Amherst, Montréal, London et Québec.

Merci à la salle café et à ses occupants plus ou moins réguliers. Vous avez su supporter mes humeurs et mes râleries, ça vaut presque une médaille. Merci surtout aux copains, doctorants ou pas, co-bureau ou pas, pour l'ambiance de rêve qui règne dans les couloirs des 3ème et 4ème étages du bâtiment B : Quentin et ses jeux de mots, Othman, Olivier, Johann qui se plaignait si bien, Firmin –chut !–, Charlotte et Aude mes deux mamans, Cyril mon phare dans la brume d'i-prof, roi incontesté du sarcasme, Isabelle, Lucie (:-*), Antonio, Guillaume, Alessandro, Michou best co-bureau ever, Pammella qui m'a fait le plus beau des cadeaux, Olga, Colin –Tu es toléré ici, toléré.–, Youssef, Benjamin, Thao et tous les autres. Clément, ton cas est à traiter à part : tu as fait tant de choses pour moi et avec moi. Comment notre bonne entente a pu survivre à l'organisation des JED ? Ça reste un mystère...

Je pense aussi à vous, rencontrés ici et là (et surtout ailleurs) : Coline, Victoria, Kamilia, Gautier, Aurel, Bill et toute la famille PARI/GP, Marina, Lara, ...

Bien sûr, je n'aurais probablement jamais envisagé de faire une thèse si je n'avais pas eu au cours de ma scolarité des professeurs aussi impliqués ; eux aussi ont une place de choix sur cette page. Merci pour le dynamisme et la passion avec lesquels vous donniez vos cours, c'est la plus belle vitrine de ce métier !

Les filles, c'est aussi un peu grâce à vous tout ça. Amélie, Chloé, Chloé, Elodie, Laura et Pauline, vous m'avez tant dit "mais si, t'es capable" et "au pire ce sera pas si pire" que j'ai fini par y croire !

Je remercie bien évidemment ma famille, ma belle-famille et mes amis pour leur soutien et leurs encouragements. Merci surtout à toi Maman d'être si sécurisante, à vous Titi et Théo pour les moments précieux qu'on passe ensemble et à toi Papa, pour la fierté que j'ai lue dans tes yeux.

Je finirai évidemment par celui qui partage ma vie, mes peines et mes éclats de rire. Merci Thomas de m'avoir soutenue, sur tous les plans, tout le temps. ♡

Et si je devais dédier ce tapuscrit à quelqu'un, ce serait à Plastique, parce que c'était pas gagné !

TABLE DES MATIÈRES

1. Introduction 1
1.1. Premier axe : groupes mild 1
1.2. Deuxième axe : structure galoisienne, corps p-rationnels 4

2. Outils 9
2.1. Théorie p-adique du corps de classes 9
2.2. Cohomologie 11

3. Propagation de la propriété *mild* au-dessus d'une extension quadratique imaginaire de $\mathbb{Q}$ 17
3.1. Généralités 17
3.2. Calculs de cup-produits 20
3.3. Critère de Labute-Minac-Schmidt par rapport à S ; calculs 22
3.4. Un critère de propagation du caractère *mild* de $G_{\mathbb{Q},S}$ à $G_{\mathrm{L},S}$ 25
3.5. Exemple complémentaire 30

4. Sur les φ-composantes de la structure galoisienne de certaines pro-p-extensions de corps de nombres 35
4.1. Quelques précisions algébriques 36
4.2. Extensions à ramification restreinte : rappels 43
4.3. Quelques contextes arithmétiques 45
4.4. Études statistiques 53

A. Calcul local des cup-produits et critère (LMS_f) : philosophie du code Pari-GP 63
A.1. Premiers auxiliaires 63
A.2. Calcul local des cup-produits 63
A.3. Critère (LMS_f) 64

B. Statistiques sur la liberté des φ-composantes 65
B.1. Extensions cubiques cycliques 65
B.2. Extensions diédrales 67
B.3. Extensions cycliques de degré 4 68

Index des notations 71

Bibliographie 73

CHAPITRE 1

INTRODUCTION

La clôture algébrique $\overline{\mathrm{k}}$ d'un corps de nombres k est une extension galoisienne, elle admet donc un groupe de Galois $G_{\overline{\mathrm{k}}}$ appelé groupe de Galois absolu de k. Ce groupe profini est un objet mystérieux, même dans le cas $\mathrm{k} = \mathbb{Q}$. L'idée pour le comprendre un peu mieux est de le décomposer en parties que l'on peut étudier indépendamment les unes des autres, comme on le ferait pour un groupe fini via la décomposition en p-parties. Donnons-nous donc un nombre premier p et considérons l'analogue profini de la p-partie : le pro-p quotient maximal $G_{\overline{\mathrm{k}}}(p)$ de $G_{\overline{\mathrm{k}}}$. Par construction, ce pro-p groupe correspond à la pro-p extension maximale de k. Pour avoir encore plus de contrôle sur les extensions, et donc une meilleure compréhension de leurs groupes de Galois, on peut également restreindre la ramification. En effet, on sait quel premier se ramifie ou non dans une extension finie. Si on se donne un ensemble fini S de premiers de k, on peut donc considérer le compositum de toutes les p-extensions finies de k dans lesquelles seuls les éléments de S peuvent se ramifier. On obtient une extension non ramifiée en dehors de S, galoisienne par maximalité et dont le groupe de Galois est limite projective de p-groupes finis : c'est un pro-p-groupe. Ce quotient de $G_{\overline{\mathrm{k}}}(p)$ est noté $G_{\mathrm{k},S}$; il correspond à la pro-p extension maximale de k non-ramifiée en dehors de S, qui sera notée k_S dans toute la suite.

L'étude d'un tel groupe était également motivée par des questions géométriques, notamment sur les recouvrements finis de surfaces de Riemann ramifiées en un nombre fini de premiers, par la théorie du corps de classes et par la connaissance profonde des groupes de Galois de corps locaux. On retrouve ce type de questionnement dans les articles de Shafarevich, puis dans l'article de Golod et Shafarevich dans lequel est démontré le théorème du même nom. On s'intéressera dans ce manuscrit aux deux cas extrêmes : le cas sauvage, où l'on suppose que S contient tous les premiers au dessus de p, et le cas modéré, où l'on suppose au contraire que S ne contient aucun diviseur de p.

Les extensions à ramification restreinte ont fait l'objet de nombreux travaux. Citons trois références majeures, qui sont le fil conducteur de tout ce qui suit : le livre de Koch ([**29**]), le livre de Neukirch, Schmidt et Wingberg ([**42**]) et plus particulièrement les chapitres I, V et X, et le livre de Gras ([**17**]).

Remarquons dès maintenant que seuls les premiers dont la norme est congrue à 0 ou 1 modulo p sont susceptibles d'être ramifiés dans une p-extension. *On supposera sans perte de généralité pour la suite l'ensemble S minimal, c'est-à-dire contenant uniquement de tels premiers. Pour plus de confort, nous supposerons également le nombre premier p impair.*

1.1. Premier axe : groupes mild

Si l'on suppose que S contient tous les premiers de k divisant p, alors les travaux de Kuz'min ont montré que le groupe $G_S := G_{\mathrm{k},S}$ est de dimension cohomologique inférieure ou égale à 2 lorsque $p > 2$. Schmidt a plus tard totalement décrit le cas $p = 2$. On renvoie à [**42**, chap. X] pour un état de l'art sur cette question.

Si maintenant on se place dans le cas modéré, c'est-à-dire si S ne contient aucun premier au dessus de p, la question est encore ouverte. Artin pensait (et c'était une conjecture, [**13**, chap. 15]) que la pro-p extension non-ramifiée maximale d'un corps de nombres était nécessairement finie. Le résultat de Golod et Shafarevich en 1964 implique qu'un groupe G_S peut être infini, par exemple si l'on suppose $S = \varnothing$, ce qui invalide la conjecture faite par Artin. Mais si ce groupe est infini, quelle est sa dimension cohomologique ?

En 1981, puis 1985, Anick publie deux articles sur les algèbres non commutatives et notamment sur l'algèbre de Lie associée à un groupe dans lesquels il introduit les notions de suite strictement libre, suite combinatoirement libre, suite fortement libre et groupe *mild*. Labute s'intéresse aux propriétés des pro-p groupes *mild* et notamment au lien entre le caractère *mild* et la dimension cohomologique : un tel groupe est de dimension cohomologique inférieure ou égale à 2. En 2005, lors d'une visite à London (Ontario) il cherche à redémontrer les résultats de Kuz'min en appliquant le travail de Anick à l'algèbre de Lie graduée obtenue à partir de la suite centrale descendante de G_S. Contrairement à son intuition, ces outils se révèlent inadaptés au cas sauvage. Cependant, ils lui permettent d'exhiber dans [**30**] les premiers exemples de pro-p groupe G_S de dimension cohomologique 2 dans le cas modéré pour $\mathrm{k} = \mathbb{Q}$ et $p > 3$. Il utilise le résultat suivant de Koch [**29**], qui donne une description explicite du début des relations de G_S :

Théorème 1.1.1. — *On considère une présentation minimale $G_S = F/R$ du pro-p groupe G_S, où F est le pro-p groupe libre sur m générateurs $x_1, \dots, x_m$. Si on note F^p le sous-groupe de F engendré par les puissances p-èmes, alors le sous-groupe normal fermé R est engendré par d éléments $r_1, \dots r_d \in F^p[F,F]$ vérifiant*

$$r_i \equiv x_i^{pa_i} \prod_{i \neq j} [x_i, x_j]^{\ell_{ij}} \bmod F^{(3)},\ a_i, \ell_{ij} \in \mathbb{Z}/p\mathbb{Z},$$

où $F^{(3)} = (F^{(2)})^p[F, F^{(2)}]$ avec $F^{(2)} = F^p[F,F]$.

Les puissances ℓ_{ij} sont appelées *linking numbers*. Labute associe alors au groupe G_S un diagramme, appelé *linking diagram*, dont les sommets sont les éléments de S et dont les arcs sont pondérés par les *linking numbers* et introduit la notion de circuit non-singulier :

Définition 1.1.2. — Un *linking diagram* Γ est appelé circuit non-singulier lorsque :

(i) les sommets de Γ peuvent être ordonnés de sorte que $v_1 v_2 \dots v_m$ soit un circuit ;
(ii) aucun arc ne relie deux sommets d'indices impairs et

$$\ell_{12}\ell_{23}\dots\ell_{m1} - \ell_{1m}\ell_{21}\dots\ell_{m,m-1} \neq 0.$$

On rappelle qu'un circuit est chemin de longueur strictement plus grande que 1 qui relie un sommet à lui-même. La notion de circuit non-singulier est reliée au travail d'Anick de la manière suivante :

Théorème 1.1.3 **(Labute, [30]).** — *Soit G un pro-p groupe admettant une présentation de Koch. Alors la suite de ses relations est fortement libre si $p \neq 2$ et si les sommets du linking diagram associé forment un circuit non-singulier.*

On peut énoncer ce résultat en terme de groupe *mild* :

Théorème 1.1.4 **(Labute, [30]).** — *Le pro-p groupe G_S est mild si les sommets du linking diagram associé forment un circuit non-singulier.*

A. Schmidt reformule ensuite ce résultat puis l'étend dans [**49**] et [**50**]. Partant du fait que les *linking numbers* sont en fait des valeurs prises par le cup-produit sur le premier groupe de cohomologie de G_S, il déduit qu'un pro-p groupe G est *mild* si le cup-produit sur son premier groupe de cohomologie (sur $\mathbb{F}_p$) vérifie certaines propriétés. Il faudra attendre seulement quelques mois pour que Vogel publie [**55**] dans lequel il utilise les méthodes de Labute et les adapte au cas de certains corps quadratiques imaginaires. Deux ans plus tard, en 2009, Labute et Minac dans [**31**] prouvent que le résultat reste vrai pour $p = 2$, et donnent de nouveaux exemples de pro-p groupes G_S, toujours au dessus du corps des rationnels.

Finalement, Forré publie en 2011 [**12**] dans lequel il propose une preuve plus immédiate (dans le sens où elle ne nécessite pas de traiter à part le cas $p = 2$) du critère du cup-produit : il utilise lui aussi la présentation de Koch et les travaux de Anick, mais les applique à une algèbre de séries formelles plutôt qu'à l'algèbre de Lie associée à G_S. C'est cette approche que nous avons choisi de suivre ici (dans le chapitre 3).

Nous appellerons dans toute la suite "critère de Labute, Minac et Schmidt" le critère issu des travaux successifs de ces trois mathématiciens :

***Théorème 1.1.5* (Critère (LMS)).** — *Soit G un pro-p groupe de p-rang fini. Si les groupes de cohomologie (sur $\mathbb{F}_p$) de G satisfont les conditions suivantes :*

(i) *il existe deux $\mathbb{F}_p$-espaces vectoriels U et V tels que $H^1(G, \mathbb{F}_p) \simeq U \oplus V$,*
(i) *le cup-produit $V \otimes V \to H^2(G, \mathbb{F}_p)$ est trivial,*
(ii) *le cup-produit $U \otimes V \to H^2(G, \mathbb{F}_p)$ est surjectif.*

Alors le pro-p groupe G est mild.

La plupart des exemples de pro-p groupes G_S *mild* présents dans la littérature sont issus de cette série de papiers et concernent donc des pro-p extensions de $\mathbb{Q}$ ou de corps quadratiques imaginaires.

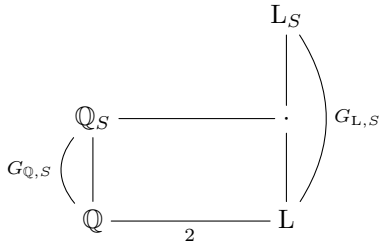
La question de la propagation du caractère *mild* d'un groupe $G_{\mathrm{K},S}$ est vaste. Considérons une extension L de K et $G_{\mathrm{L},S}$ le groupe de Galois correspondant, où on note par abus S l'ensemble des places de L divisant les éléments de S. Le caractère *mild* se conserve-t-il lorsque $G_{\mathrm{K},S}$ est un quotient de $\mathrm{Gal}(\mathrm{L}_S/\mathrm{K})$? Lorsque L/K est une extension de degré p ? Lorsque L/K est une extension linéairement disjointe de K_S/K de degré premier à p ?

Le théorème montré par Gras dans [**18**] permet de répondre en partie à cette dernière question, dans le cas d'une extension quadratique du corps des rationnels dont on suppose le p-groupe de classes (c'est-à-dire le p-sous-groupe de Sylow du groupe des classes) trivial : en s'appuyant sur un résultat de théorie des groupes de Tate ([**53**]), le résultat de Gras montre que si les premiers de S sont inertes dans l'extension L/K, alors le groupe $G_{\mathrm{L},S}$ est isomorphe à $G_{\mathrm{K},S}$. Les groupes $G_{\mathrm{K},S}$ et $G_{\mathrm{L},S}$ sont donc dans ce cas simultanément *mild*.

Dans le chapitre 3 de ce manuscrit, on se place dans la situation extrême opposée : on suppose que tous les éléments de S sont totalement décomposés dans l'extension L/K. Pour simplifier les calculs, on se concentre sur les extensions quadratiques imaginaires du corps des rationnels $\mathbb{Q}$ mais un raisonnement similaire est envisageable dans un cas plus général. La problématique est donc la suivante :

Question 1.1.6. — *En supposant que le groupe $G_{\mathbb{Q},S}$ est mild, sous quelles conditions le groupe $G_{\mathrm{L},S}$ conserve-t-il cette propriété ?*

On se place dans la situation galoisienne :



où L est un corps quadratique imaginaire (différent de $\mathbb{Q}(j)$ si $p = 3$). On suppose que toutes les places de S se décomposent totalement dans l'extension L/$\mathbb{Q}$ et que L est de p-groupe de classes trivial.

Sous cette dernière hypothèse, les éléments du deuxième groupe de cohomologie peuvent être vus comme des objets locaux. Ceci vaut en particulier pour les cup-produits qui pourront alors être calculés grâce à des outils de théorie du corps de classes.

Ce contexte permet de considérer une version faible (LMS_f) du critère de Labute-Minac-Schmidt, où la décomposition $H^1(G_S, \mathbb{F}_p) \simeq U \oplus V$ correspond à une partition $S_1 \cup S_2$ de l'ensemble S (on dit alors que le critère (LMS) est vérifié en respectant S). En l'implémentant dans PARI/GP, nous tentons dans un premier temps d'apporter une réponse statistique à la question 1.1.6 : si (LMS_f) est vérifié par le groupe $G_{\mathbb{Q},S}$, à quelle proportion de groupes $G_{\mathrm{L},S}$ le critère (LMS_f) s'applique-t-il ?

A S fixé tel que $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S, on note $\mathbb{E}_S(X)$ l'ensemble des corps quadratiques imaginaires de discriminants inférieurs à X, de p-groupe de classes triviaux et dans lesquels éléments de S sont décomposés. On calcule grâce à la méthode des premiers auxiliaires (section 3.3.1) la quantité

$$P_{S,p}(X) = \frac{\#\{\mathrm{L} \in \mathbb{E}_S(X), \text{le critère } (LMS_f) \text{ s'applique à L})\}}{\#\{\mathrm{L} \in \mathbb{E}_S\}}$$

et on obtient par exemple les valeurs suivantes :

S	$P_{S,3}(10^5)$
$\{13, 127, 193, 349\}$	$\frac{1879}{2151} \simeq 0.8735$
$\{337, 349, 379, 463\}$	$\frac{2004}{2341} \simeq 0.8560$

Parmi les corps quadratiques de l'ensemble $\mathbb{E}_S$, certains ne vérifient pas le critère (LMS_f), mais vérifient le critère de Labute-Minac-Schmidt 3.1.5.

La seconde partie du chapitre 3 est consacrée à une étude théorique de ce phénomène de propagation. Nous associons à chaque couple (S, p) et chaque corps quadratique imaginaire L deux graphes orientés $\mathcal{G}_S$ et $\mathcal{G}_S*$. Bien que leurs sommets soient les premiers de S, ces graphes diffèrent des *linking diagram* de Labute et Vogel : les arcs sont cette fois déterminés par des conditions de ramification dans des extensions p-élémentaires de L. Afin d'étudier le caractère *mild* du pro-p groupe $G_{\mathrm{L},S}$, nous introduisons la notion de graphe quasi-circulaire :

Définition 1.1.7. — Un graphe est dit quasi-circulaire s'il admet un sous-graphe couvrant dont les sommets sont de degré entrant égal à 1.

En exploitant les propriétés du cup-produits et la correspondance donnée par la théorie du corps de classes locale, nous montrons alors :

Théorème 1.1.8. — *Soit* L *une extension quadratique imaginaire de* $\mathbb{Q}$ *de p-groupe de classes trivial (différente de* $\mathbb{Q}(j)$ *si* $p = 3$*) telle que tout premier de* S *est décomposé dans* $\mathrm{L}/\mathbb{Q}$.

Si $\mathbb{Q}$ *vérifie le critère de Labute-Minac-Schmidt en respectant* S *(le pro-p groupe* $G_{\mathbb{Q},S}$ *est donc mild) et si l'un des graphes* $\mathcal{G}_S$ *ou* $\mathcal{G}_S^*$ *est quasi-circulaire, alors le groupe* $G_{\mathrm{L},S}$ *est mild et* $\dim_{\mathbb{F}_p} H^1(G_{\mathrm{L},S}, \mathbb{F}_p) = \dim_{\mathbb{F}_p} H^2(G_{\mathrm{L},S}, \mathbb{F}_p) = 2|S|$.

Ce résultat nous permet en particulier d'exhiber de nouveaux exemples de pro-p groupes G_S *mild* au dessus d'extensions quadratiques imaginaires qui ne peuvent être détectés par le résultat de Vogel ([**55**]).

Ces travaux, présentés dans le chapitre 3 de ce manuscrit, font l'objet de l'article [**48**].

1.2. Deuxième axe : structure galoisienne, corps p-rationnels

Les pro-p groupes G_S peuvent également être étudiés via leur structure de module. Commençons par rappeler dans les grandes lignes le cadre de la théorie d'Iwasawa qui nous intéresse. On renvoie pour plus de précisions à [**42**, chap. V].

Considérons une $\mathbb{Z}_p$-extension $\mathrm{k}_\infty/\mathrm{k}$, c'est-à-dire une extension galoisienne de k dont le groupe de Galois Γ est isomorphe au pro-p groupe libre $\mathbb{Z}_p$; on note γ un générateur de Γ. On appelle de manière standard algèbre d'Iwasawa l'algèbre $\mathbb{Z}_p[\![\Gamma]\!]$ et module d'Iwasawa tout $\mathbb{Z}_p[\![\Gamma]\!]$-module compact (voir [**42**, chap. V, §3]). L'isomorphisme de $\mathbb{Z}_p$-algèbres topologiques

$$\begin{array}{ccc} \mathbb{Z}_p[\![T]\!] & \to & \mathbb{Z}_p[\![\Gamma]\!] \\ T & \mapsto & \gamma - 1 \end{array}$$

permet d'obtenir pour tout module d'Iwasawa le théorème de structure suivant :

Théorème 1.2.1. — *Si M est un module d'Iwasawa de type fini, alors il existe des polynômes de Weierstrass irréductibles F_j, des entiers r, m_i et n_j et un homomorphisme*

$$M \to \mathbb{Z}_p[\![\Gamma]\!]^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_p[\![\Gamma]\!]/p^{m_i} \oplus \bigoplus \mathbb{Z}_p[\![\Gamma]\!]/F_j^{n_j}$$

de noyau et conoyau finis.

Les entiers r, $\mu = \sum m_i$ et $\lambda = \sum n_j \deg(F_j)$ sont entièrement déterminés par le module M, on parle alors d'invariants d'Iwasawa.

Revenons aux pro-p extensions à ramification restreinte : on considère S un ensemble de premiers de k contenant les diviseurs de p et notons k_∞ une $\mathbb{Z}_p$-extension de k contenue dans k_S. On note Γ le groupe de Galois de l'extension $\mathrm{k}_\infty/\mathrm{k}$ et $\mathcal{H}$ le sous-groupe de G_S défini par la suite exacte suivante :

$$1 \longrightarrow \mathcal{H} \longrightarrow G_S \longrightarrow \Gamma \longrightarrow 1 \ .$$

Les propriétés des groupes G_S associées au lemme de Nakayama topologique permettent de montrer que l'abélianisé $\mathcal{X} := \mathcal{H}^{ab}$ est un module d'Iwasawa. Le théorème de structure permet alors de lier les propriétés des groupes G_S et $\mathcal{H}$ – et notamment leurs premiers groupes de cohomologie – aux propriétés du $\mathbb{Z}_p[\![\Gamma]\!]$-module $\mathcal{X}$ et de ses sous-modules. On renvoie par exemple à [**42**, chap. V, §3, chap. V, §6].

Dans le chapitre 4 de ce manuscrit, on suppose que Γ est un pro-p groupe quelconque. Considérons par exemple $\mathcal{H}$ un sous-groupe fermé normal de G_S quelconque et notons G le quotient $G := G_S/\mathcal{H}$. On note toujours $\mathcal{X} := \mathcal{H}^{ab}$. Alors $\mathcal{X}$ est encore naturellement muni d'une structure de $\mathbb{Z}_p[\![G]\!]$-module !

De plus, l'algèbre $\mathbb{Z}_p[\![G]\!]$ conserve de bonnes propriétés : c'est un anneau local d'idéal maximal engendré par son idéal d'augmentation et par p ([**5**], [**42**]). Le théorème de structure 1.2.1 ne s'applique pas ici mais Maire, dans [**38**], définit néanmoins un invariant pour le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}$:

Définition 1.2.2. — Lorsque $\mathcal{X}$ est $\mathbb{Z}_p[\![G]\!]$-libre et de type fini, le rang $\rho_{\mathcal{X}}$ est l'unique entier vérifiant $\mathcal{X} \simeq \mathbb{Z}_p[\![G]\!]^{\rho_{\mathcal{X}}}$.

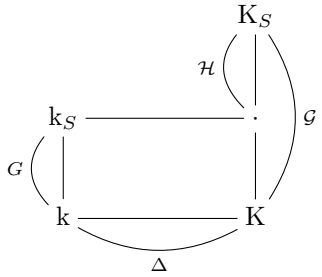
Il montre alors que la liberté du module $\mathcal{X}$ est liée, sous de bonnes hypothèses à la $\mathbb{Z}_p$-torsion du groupe $\mathcal{G}^{ab}$.

Théorème 1.2.3 **(Maire, [38]).** — *On suppose que G_S est de présentation finie et que G_S et G sont de dimension cohomologique au plus 2. Si les multiplicateurs de Schur $H^2(\mathcal{G}_\mathcal{S}, \mathbb{Q}_p/\mathbb{Z}_p)$, $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$ et $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p)$ sont triviaux et si $\mathcal{X}$ est de type fini, alors le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}$ est libre si et seulement si le morphisme $\mathrm{Tor}_{\mathbb{Z}_p} G_S^{ab} \to G^{ab}$ est injectif.*

On a dans ce cas $\mathrm{rg}_{\mathbb{Z}_p} \mathcal{X}_G = \mathrm{rg}_{\mathbb{Z}_p} G_S^{ab} - \mathrm{rg}_{\mathbb{Z}_p} G^{ab}$.

Ce théorème s'applique bien à certaines situations arithmétiques parmi lesquelles les extensions de corps locaux, les corps CM et l'étude des groupes G_S.

Reprenons le contexte galoisien déjà évoqué, en supposant cette fois que l'ensemble S contient les places p-adiques et que le groupe Δ est d'ordre premier à p :



On peut dans ce cas être plus précis que Maire dans [**38**]. En effet, le groupe de Galois de l'extension K/k agit sur le $\mathbb{Z}_p[\![\Delta \times G]\!]$-module $\mathcal{X} := \mathcal{H}^{ab}$. La décomposition en idempotents de $\mathbb{Z}_p[\Delta]$ permet de parler de φ-composantes de $\mathcal{X}$ où ici φ désigne un caractère $\mathbb{Q}_p$-irréductible de Δ. En supposant que Δ est d'ordre premier à p, on s'assure que les groupes Δ et G commutent ; la composante $\mathcal{X}^{\varphi}$ est alors également munie d'une structure de $\mathbb{Z}_p[\![G]\!]$-module. On renvoie au chapitre 4 pour plus de précisions sur ces modules. La décomposition en somme directe de φ-composantes permet de pousser plus loin le travail fait dans [**38**] : imaginons que le théorème ne permette pas de prouver que le module $\mathcal{X}$ est libre, on peut quand même espérer déterminer de quelle φ-composante vient l'obstruction. On arrive à montrer le théorème suivant :

Théorème 1.2.4. — *Soit* K/k *une extension galoisienne de groupe de Galois* Δ *d'ordre premier à* p*. Soit* φ *un caractère* $\mathbb{Q}_p$*-irréductible non-trivial de* Δ*. Sous les notations précédentes et sous la conjecture de Leopoldt, le module* $\mathcal{X}^{\varphi}$ *est* $\mathbb{Z}_p[\![G]\!]$*-libre si et seulement si* $\mathrm{Tor}_{\mathbb{Z}_p}\left(\mathcal{G}^{ab}\right)^{\varphi}$ *est trivial.*

Ici, $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}^{ab}$ désigne la torsion du $\mathbb{Z}_p$-module $G^{ab}_{\mathrm{K},S} := G_{\mathrm{K},S}/[G_{\mathrm{K},S}, G_{\mathrm{K},S}]$. Le cas du caractère trivial est traité à part et on retrouve évidemment le théorème 1.2.3.

L'objet arithmétique essentiel est donc le $\mathbb{Z}_p$-module de torsion $\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}_{\mathrm{K},S}$. Il ne dépend pas du groupe $\mathcal{H}$ choisi et par un théorème de déploiement (voir [**17**, chap. III, §4, th. 4.1.5]), son étude se ramène au cas où $S = S_p$. Sous la conjecture de Léopoldt, le groupe fini $\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}_{\mathrm{K},S_p}$ est également central dans l'étude de la p-rationalité du corps K : on dit que K est p-rationnel lorsque ce groupe est trivial.

Le livre de Gras [**17**] donne une présentation détaillée des corps p-rationnels qui ont par ailleurs été l'objet de nombreux travaux : Movaheddi-Nguyen [**41**], Gras-Jaulent [**20**], Jaulent-Nguyen [**26**], Greenberg [**21**], etc... Récemment, Gras a émis la conjecture suivante ([**19**, conj. 8.11]) :

***Conjecture 1.2.5* (Gras).** — *Soit* K *un corps de nombres. Pour* p *assez grand, le corps* K *est* p*-rationnel.*

Sous cette conjecture, le théorème 1.2.4 implique alors que pour p assez grand, le module $\mathcal{X}^{\varphi}$ est libre (pour tout caractère $\varphi \neq \mathbb{1}$ et quand $S = S_p$).

La théorie du corps de classes permet d'exprimer $\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}_{\mathrm{K},S_p}$ comme un produit de deux quantités dont l'une devient triviale lorsque le p-Sylow du groupe des classes Cl(K) de K est trivial. Sous cette hypothèse, le calcul du module $\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}_{\mathrm{K},S_p}$ se ramène à l'étude du quotient des unités des complétés p-adiques par les unités globales. Encore mieux, en s'assurant qu'aucun complété p-adique de K ne contient de racines p-ème de l'unité, l'étude de $\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}_{\mathrm{K},S_p}$ "se résume" à celle du régulateur normalisé défini par Gras [**15**, def. 5.1]. Cette observation que l'on trouve déjà dans [**17**, chap. III, §4.14] est propice à une étude statistique : si on se place au dessus de $\mathbb{Q}$ dans des extensions bien choisies, la condition à vérifier est en fait une condition de congruences modulo p ! Le chapitre 4 s'achèvera ainsi sur des applications numériques dans plusieurs familles d'extensions données par des polynômes dont les racines engendrent le groupe des unités du corps de décomposition. Ces polynômes sont issus de familles données par Balady [**2**], Lecacheux [**33**] et Balady-Washington [**3**]. Les résultats obtenus confortent la conjecture de Gras sur les corps p-rationnels. À noter que Pitoun-Varescon [**47**] et plus récemment Gras [**14**] ont donné des

algorithmes pour tester la p-rationalité d'un corps de nombres en toute généralité. Nous nous efforcerons de comparer les différentes vitesses de calculs.

Cette approche, développée dans le chapitre 4, a donné lieu à un article rédigé en collaboration avec Christian Maire (actuellement soumis).

CHAPITRE 2

OUTILS

Comme nous l'avons expliqué dans l'introduction, nous suivrons deux approches différentes dans les chapitres 3 et 4 ; en revanche, nous utiliserons majoritairement les deux mêmes "outils" pour démontrer les théorèmes 1.1.8 et 1.2.4 : la théorie p-adique du corps de classes et la cohomologie. Nous rappelons dans cette section les principaux résultats que nous utiliserons par la suite.

2.1. Théorie p-adique du corps de classes

La théorie p-adique du corps de classes, développée par Jaulent dans [**27**], est un outil efficace pour l'étude de pro-p extensions de corps de nombres : elle relie des (pro-p) objets globaux à certains groupes de normes locaux via la correspondance d'Artin. Nous rappelons ici les notations et les principaux résultats que l'on peut retrouver dans [**27**].

Soit K un corps de nombres de degré n sur $\mathbb{Q}$. La théorie p-adique du corps de classes lui fait correspondre deux $\mathbb{Z}_p$-modules : le premier, global, est le p-adifié $\mathcal{R}_{\mathrm{K}} = \mathbb{Z}_p \otimes \mathrm{K}^{\times}$ du groupe multiplicatif $\mathrm{K}^{\times}$, et le second, semi-local, est appelé p-groupe d'idèles de K et noté $\mathcal{J}_{\mathrm{K}}$; il est défini comme suit. Si v est une place de K, on note $\mathcal{R}_v$ et $\mathcal{U}_v$ les complétions p-adiques respectives du corps complété K_v de K en v, et du groupe des unités de l'anneau local associé à K_v. Le groupe des idèles $\mathcal{J}_{\mathrm{K}}$ de K est défini comme le produit restreint sur les places de K des $\mathcal{R}_v$ suivant $\mathcal{U}_v$:

$$\mathcal{J}_{\mathrm{K}} = \prod_{v \in Pl_{\mathrm{K}}}^{res} \mathcal{R}_v.$$

Autrement dit, si $x = (x_v)_v$ est un élément de $\mathcal{J}_{\mathrm{K}}$, alors il existe un ensemble fini S de places de K tel que $x_v \in \mathcal{R}_v$ si v est un élément de S et $x_v \in \mathcal{U}_v$ sinon. L'injection diagonale de K dans ses complétés induit une injection continue de $\mathcal{R}_{\mathrm{K}}$ dans le p-groupe des idèles $\mathcal{J}_{\mathrm{K}}$, qu'on note ι (c'est le plongement diagonal). Pour S un ensemble fini de places de K, on note encore ι ($= \iota_S$) le plongement diagonal $\iota : \mathcal{R}_{\mathrm{K}} \to \prod_{v \in S} \mathcal{R}_v$. On identifiera pour la suite $\mathcal{R}_{\mathrm{K}}$ à un sous-$\mathbb{Z}_p$-module de $\mathcal{J}_{\mathrm{K}}$.

Pour T, S deux ensembles fini disjoints de places de K, notons par K_S^T la pro-p-extension maximale de K, non-ramifiée en dehors de S et dans laquelle les places de T sont totalement décomposées ; posons $G_{\mathrm{K},S}^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$. La correspondance de la théorie du corps de classes apporte l'isomorphisme suivant (induit par l'application d'Artin) :

$$(G_{\mathrm{K},S}^T)^{ab} \simeq \frac{\mathcal{J}_{\mathrm{K}}}{\mathcal{R}_{\mathrm{K}} \prod_{v \notin S} \mathcal{U}_v \prod_{v \in T} \mathcal{R}_v}. \tag{1}$$

Enfin, les unités jouent un rôle important dans ce qui suit. On note $\mathcal{E}_{\mathrm{K}} = \mathbb{Z}_p \otimes E_{\mathrm{K}}$ le p-adifié du groupe des unités globales de K. Plus généralement, soit $E_{\mathrm{K},S}^T$ (ou encore E_S^T) le groupe des T-unités de K congrues à 1 modulo S. Posons $\mathcal{E}_{\mathrm{K},S}^T = \mathcal{E}_S^T = \mathbb{Z}_p \otimes E_S^T$.

L'étude de $(G_{\mathrm{K},S}^T)^{ab}$ peut se faire de façon relative, par exemple à travers le p-groupe des classes de K. Présentons un résultat bien connu.

Proposition 2.1.1. — *Soient les ensembles finis de places de* K, $S \subset \Sigma$ *et* $T' \subset T$, *avec* $T \cap S = T' \cap \Sigma = \varnothing$. *Alors le noyau du morphisme naturel de restriction* $G_{\mathrm{K},\Sigma}^{T',ab} \to G_{\mathrm{K},S}^{T,ab}$ *est isomorphe, via l'application d'Artin, au quotient*

$$\frac{\prod_{v\in\Sigma\setminus S}\mathcal{U}_v \prod_{v\in T\setminus T'}\mathcal{R}_v}{\iota(\mathcal{E}_S^T)},$$

où ι *est le plongement diagonal sous-jacent.*

Démonstration. — C'est immédiat. Considérons la suite exacte courte

$$1 \longrightarrow W \longrightarrow G_{\mathrm{K},\Sigma}^{T',ab} \longrightarrow G_{\mathrm{K},S}^{T,ab} \longrightarrow 1\ .$$

D'après la théorie p-adique du corps de classes rappelée précédemment, le groupe $G_{\mathrm{K},S}^{T,ab}$ est isomorphe, via l'application d'Artin, au quotient $\mathcal{J}_\mathrm{K}/\mathcal{R}_\mathrm{K}\prod_{v\notin S}\mathcal{U}_v\prod_{v\in T}\mathcal{R}_v$ du groupe d'idèles de K. On a donc :

$$\begin{aligned} W &\simeq \mathrm{Ker}\left(\mathcal{J}_\mathrm{K}/\mathcal{R}_\mathrm{K}\prod_{v\notin\Sigma}\mathcal{U}_v\prod_{v\in T'}\mathcal{R}_v \to \mathcal{J}_\mathrm{K}/\mathcal{R}_\mathrm{K}\prod_{v\notin S}\mathcal{U}_v\prod_{v\in T}\mathcal{R}_v\right)\\ &\simeq \frac{\prod_{v\in\Sigma\setminus S}\mathcal{U}_v\prod_{v\in T\setminus T'}\mathcal{R}_v}{(\prod_{v\notin\Sigma}\mathcal{U}_v\prod_{v\in T'}\mathcal{R}_v)\cap(\mathcal{R}_\mathrm{K}\prod_{v\in\Sigma\setminus S}\mathcal{U}_v\prod_{v\in T\setminus T'}\mathcal{R}_v)}, \end{aligned}$$

d'où le résultat. □

Lorsque $S = T = \varnothing$, la théorie du corps de classes globale permet d'identifier le groupe de Galois de la pro-p extension abélienne non-ramifiée maximale de K au p-Sylow du groupe des classes de K (voir par exemple [**17**]) Ainsi, il vient :

Corollaire 2.1.2. — *Soit* p *tel que le* p*-Sylow du groupe des classes* Cl(K) *de* K *est trivial. Alors*

$$G_{\mathrm{K},S}^{ab} \simeq \frac{\prod_{v\in S}\mathcal{U}_v}{\iota(\mathcal{E}_\mathrm{K})}.$$

Nous utiliserons dans la suite beaucoup de résultats de cohomologie. Les groupes de cohomologie sur $\mathbb{F}_p$ de $G_{\mathrm{K},S}^T$, de son abélianisé et de son quotient par les puissances p-èmes étant identiques, nous pourrons dans certains cas ramener notre étude à celle du groupe $G_{\mathrm{K},S}^{T,p,el} := G_{\mathrm{K},S}^{T,ab}/(G_{\mathrm{K},S}^{T,ab})^p$. On note $\mathrm{K}_S^{T,p,el}$ le sous-corps de K_S^T correspondant : c'est la p-extension élémentaire maximale de K non-ramifiée en dehors de S et T-décomposée.

Corollaire 2.1.3. — *Soit* p *tel que le* p*-groupe des* T*-classes de* K *est trivial. Alors*

$$G_{\mathrm{K},S}^{T,p,el} \simeq \frac{\prod_{v\in S}\mathcal{U}_v}{\iota(\mathcal{E}_S^T)\mathcal{J}_\mathrm{K}^p\cap\prod_{v\in S}\mathcal{U}_v}.$$

Démonstration. — La démonstration est là encore immédiate. Le groupe $G_{\mathrm{K},S}^T$ se surjecte sur le groupe $G_{\mathrm{K},\varnothing}^T$, groupe de Galois de la pro-p extension maximale de K, T-décomposée et non-ramifiée. En prenant leurs abélianisés et en quotientant par p, on a donc une suite exacte

$$1 \longrightarrow W \longrightarrow (G_S^T)^{ab}/p \longrightarrow (G_\varnothing^T)^{ab}/p \longrightarrow 1\ .$$

D'une part l'hypothèse sur le p-groupe des T-classes de K équivaut à la trivialité de $(G_\varnothing^T)^{ab}/p$, donc W et $(G_S^T)^{ab}/p$ sont isomorphes. D'autre part, l'isomorphisme (1) appliqué aux groupes $(G_S^T)^{ab}/p$ et $(G_\varnothing^T)^{ab}/p$ permet de déterminer W :

$$W \simeq \frac{\mathcal{R}_\mathrm{K}\mathcal{J}_\mathrm{K}^p\prod_{v\in Pl_\mathrm{K}}\mathcal{U}_v\prod_{v\in T}\mathcal{R}_v}{\mathcal{R}_\mathrm{K}\mathcal{J}_\mathrm{K}^p\prod_{v\notin S}\mathcal{U}_v\prod_{v\in T}\mathcal{R}_v} \simeq \frac{\prod_{v\in S}\mathcal{U}_v}{(\mathcal{R}_\mathrm{K}\mathcal{J}_\mathrm{K}^p\prod_{v\notin S}\mathcal{U}_v\prod_{v\in T}\mathcal{R}_v)\cap\prod_{v\in S}\mathcal{U}_v},$$

d'où le résultat. □

Lorsque l'on n'impose pas de condition de décomposition, c'est-à-dire dans le cas où $T = \varnothing$, et sous de bonnes hypothèses, on peut même en déduire un résultat sur la structure de $G_S^{p,el}$.

Théorème 2.1.4. — *Soit* K *un corps de nombres de p-groupe des classes trivial. Si on suppose que les unités sont des puissances p-èmes en les places v de S, alors on a la décomposition :*

$$G_S^{p,el} \simeq \prod_{v\in S} G_{\{v\}}^{p,el}.$$

Démonstration. — Par le corollaire précédent, on a déjà les isomorphismes

$$G_S^{p,el} \simeq \frac{\prod_{v\in S}\mathcal{U}_v}{\iota(\mathcal{E}_S)\mathcal{J}_{\mathrm{K}}^p \cap \prod_{v\in S}\mathcal{U}_v} \simeq \prod_{v\in S} \mathcal{U}_v \Big/ \mathcal{U}_v^p,$$

car les unités sont supposées être des puissances p-èmes en les places v de S.

En appliquant cela dans le cas où S ne contient qu'une seule place v, on a également $G_{\{v\}}^{p,el} \simeq \mathcal{U}_v \Big/ \mathcal{U}_v^p$, ce qui permet de conclure. □

2.2. Cohomologie

On renvoie à [**42**, chap. I] pour la définition des groupes de cohomologie et les preuves de leurs propriétés utilisées ci-après.

L'étude des premiers groupes de cohomologie sur $\mathbb{F}_p$ vient naturellement lorsqu'on décrit un pro-p groupe G par générateurs et relations. Si l'on considère une présentation minimale

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1\ ,$$

le nombre (minimal) de générateurs du pro-p groupe libre F est donné par la $\mathbb{F}_p$-dimension $d_p(G)$ du premier groupe de cohomologie $H^1(G) := H^1(G,\mathbb{F}_p)$. On dit alors que G est de p-rang $d_p(G)$. D'autre part, si la présentation de G est minimale, le nombre $r(G)$ de relations entre les générateurs de G est égal à la $\mathbb{F}_p$-dimension du deuxième groupe de cohomologie $H^2(G) := H^2(G,\mathbb{F}_p)$ (voir par exemple [**52**]). En particulier, G est de présentation finie lorsque $\dim_{\mathbb{F}_p} H^i(G,\mathbb{F}_p)$ est fini pour $i = 1, 2$.

2.2.1. Relations : correspondance locale-globale. — Lorsque deux pro-p groupes sont reliés par une application naturelle de conjugaison, injection ou surjection, leurs k-èmes groupes de cohomologie le sont également via, respectivement, la conjugaison, la restriction et l'inflation. On peut alors construire, sous certaines hypothèses, une correspondance locale-globale entre les deuxièmes groupes de cohomologie du pro-p groupe $G_{\mathrm{K},S}^T$ et de certains groupes d'extensions locales.

Définissons ici les objets locaux en jeu. Fixons S, T deux ensembles disjoints de places d'un corps de nombres K. On suppose comme avant que les éléments de S sont congrus en norme à 0 ou 1 modulo p.

Pour $v \in S$, on note K_v le complété de K pour $|\cdot|_v$ et $\overline{\mathrm{K}_v}$ la pro-p extension maximale de K_v ; on pose $\overline{G_v} := \mathrm{Gal}(\overline{\mathrm{K}_v}/\mathrm{K}_v)$. Si $\mathcal{M}/\mathrm{K}$ est une extension infinie, on définit $\mathcal{M}_v$ comme la réunion des complétés des sous-extensions finies de $\mathcal{M}/\mathrm{K}$. On note en particulier $G_v = \mathrm{Gal}((\mathrm{K}_S^T)_v/\mathrm{K}_v)$.

L'injection $i_v : G_v \hookrightarrow G_{\mathrm{K},S}^T$ et la surjection $\pi_v : \overline{G_v} \twoheadrightarrow G_v$ permettent de définir les applications :

$$\mathrm{res}_{G_v}^{G_{\mathrm{K},S}^T} : \begin{array}{rcl} H^2(G_{\mathrm{K},S}^T) & \longrightarrow & H^2(G_v) \\ f & \longmapsto & f\circ i_v \end{array} \quad \text{et} \quad \mathrm{inf}_{\overline{G_v}}^{G_v} : \begin{array}{rcl} H^2(G_v) & \longrightarrow & H^2(\overline{G_v}) \\ f & \longmapsto & f\circ \pi_v \end{array},$$

puis les applications induites :

$$\begin{array}{ccc} H^2(G_{\mathrm{K},S}^T) & \longrightarrow & \bigoplus_v H^2(\overline{G_v}) \\ & {\scriptstyle\mathrm{res}}\searrow \quad \nearrow{\scriptstyle\mathrm{inf}} & \\ & \bigoplus_v H^2(G_v) & \end{array},$$

où les sommes directes peuvent être restreintes aux premiers de K qui se ramifient dans $\mathrm{K}_S^T/\mathrm{K}$. En effet, si v est non-ramifié dans $\mathrm{K}_S^T/\mathrm{K}$, alors l'extension $(\mathrm{K}_S^T)_v/\mathrm{K}_v$ est non-ramifiée et on a les surjections

$\overline{G_v} \twoheadrightarrow \mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v)$ et $\mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v) \twoheadrightarrow G_v$, où K_v^{nr} désigne la pro-p extension non-ramifiée maximale de K_v. Par transitivité de l'inflation on a alors :

$$\inf_{\overline{G_v}}^{G_v} = \inf_{\overline{G_v}}^{\mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v)} \circ \inf_{\mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v)}^{G_v}.$$

Mais $\mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v)$ est un pro-p groupe libre, donc $H^2(\mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v)) = 0$ et $\inf_{\mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v)}^{G_v} : H^2(G_v) \to H^2(\mathrm{Gal}(\mathrm{K}_v^{nr}/\mathrm{K}_v))$ est identiquement nulle. L'application $\inf_{\overline{G_v}}^{G_v}$ est donc identiquement nulle pour tout v non-ramifié dans $\mathrm{K}_S^T/\mathrm{K}$ et on a :

$$\begin{array}{ccc} H^2(G_{\mathrm{K},S}^T) & \longrightarrow & \bigoplus_{v\in S} H^2(\overline{G_v}) \ . \\ & \searrow^{\mathrm{res}} \quad \nearrow_{\inf} & \\ & \bigoplus_{v\in S} H^2(G_v) & \end{array}$$

Définition 2.2.1. — On note $Ш(G_{\mathrm{K},S}^T)$ (ou $Ш_S^T$) le noyau de l'application $\inf \circ \mathrm{res} : H^2(G_{\mathrm{K},S}^T) \longrightarrow \bigoplus_v H^2(\overline{G_v})$. C'est le noyau de Shafarevich du groupe $G_{\mathrm{K},S}^T$.

Remarque 2.2.2. — Lorsque le corps K contient les racines p-èmes de l'unité et que S est non vide, on peut encore enlever une des places de S (n'importe laquelle !) de la somme directe. Une preuve est donnée dans [**29**, th. 11.4].

D'après le diagramme commutatif ci-dessus, lorsque le groupe $Ш_S^T$ est trivial, les relations du groupe $G_{\mathrm{K},S}^T$ sont en fait des relations « locales », c'est-à-dire des éléments des groupes $H^2(\overline{G_v}), v \in S$. Ces groupes étant totalement décrits lorsque v est premier à p (voir par exemple [**29**, th. 10.2]), il y a un réel intérêt à se placer dans une telle situation. Bien que le groupe $Ш_S^T$ n'est en général pas connu, Koch montre dans [**29**] qu'on peut le plonger dans le dual d'un autre objet.

On considère l'ensemble

$$V_S^T = \{\alpha \in \mathrm{K}_S^{\times p}, (\alpha) = \mathfrak{a}^p \mathfrak{a}_T, \mathfrak{a} \in I_S, \mathfrak{a}_T \in \langle T \rangle, i_v(\alpha) \in \mathrm{K}_v^{\times p} \ \forall v \in S\}.$$

Théorème 2.2.3 **([34]).** — *Le noyau $Ш_S^T$ s'injecte dans le dual de $V_S^T/\mathrm{K}_S^{\times,p}$.*

La formule de Shafarevich (voir [**17**, chap. I, §4.6]) relie le p-rang du quotient à celui du p-groupe des T-classes de K. En particulier, la finitude du p-groupe de classes de K implique celle du p-rang de $V_S^T/\mathrm{K}_S^{\times p}$ et on a :

Corollaire 2.2.4. — *Soit* K *un corps de nombres et soient S et T deux ensembles finis de premiers de* K *disjoints. Le groupe de Galois $G_{\mathrm{K},S}^T$ possède un nombre fini de relations.*

Démonstration. — Par définition du noyau de Shafarevich on a la suite exacte :

$$1 \longrightarrow Ш_S^T \longrightarrow H^2(G_{\mathrm{K},S}^T) \longrightarrow \bigoplus_v H^2(\overline{G_v}),$$

ce qui donne en terme de dimensions, par ce qui précède :

$$\begin{aligned} r(G_{\mathrm{K},S}^T) = \dim_{\mathbb{F}_p} H^2(G_{\mathrm{K},S}^T) &\leqslant \dim_{\mathbb{F}_p} Ш_S^T + \dim_{\mathbb{F}_p} \bigoplus_v H^2(\overline{G_v}) \\ &\leqslant \dim_{\mathbb{F}_p} V_S^T/\mathrm{K}_S^{\times p} + \dim_{\mathbb{F}_p} \bigoplus_v H^2(\overline{G_v}) \\ &< +\infty. \end{aligned}$$

□

Supposons maintenant $T = \varnothing$. Le théorème 2.2.3 permet également de se placer sous un ensemble d'hypothèses annulant $Ш_S$:

Théorème 2.2.5. — *Si* $\mathrm{K}=\mathbb{Q}$ *ou si* K *est un corps quadratique imaginaire dont le p-groupe des classes est trivial (on choisira* K *différent de* $\mathbb{Q}(j)$ *si* $p=3$*), et si S est un ensemble fini de places de* K *congrues à* 0 *ou* 1 *en norme, alors le groupe* $Ш_S$ *est trivial.*

Démonstration. — Par définition, pour tout $x \in V_\varnothing(\mathrm{K})$ il existe un idéal $\mathfrak{a}$ de K tel que l'idéal (x) engendré par x soit égal à $\mathfrak{a}^p$. L'application φ ainsi définie induit, par passage au quotient, une application $\overline{\varphi} : V_\varnothing(\mathrm{K})/\mathrm{K}^{\times p} \to \mathrm{Cl}(\mathrm{K})$ de noyau $E_\mathrm{K}/E_\mathrm{K}^p$, où $\mathrm{Cl}(\mathrm{K})$ est le p-groupe des classes de K et E_K est le groupe des unités de $\mathcal{O}_\mathrm{K}$. D'après le théorème des unités de Dirichlet, $E_\mathrm{K}/E_\mathrm{K}^p$ est isomorphe au produit du groupe libre $\mathbb{F}_p^{r_1+r_2-1}$ et du p-groupe $\mu_p(\mathrm{K})$ des racines de l'unité contenues dans K. On a donc :

$$\dim_{\mathbb{F}_p} V_\varnothing(\mathrm{K})/\mathrm{K}^{\times p} = \dim_{\mathbb{F}_p} \mathrm{Cl}(\mathrm{K}) + \dim_{\mathbb{F}_p} \mu_p(\mathrm{K}) + r_1 + r_2 - 1.$$

Par hypothèse, $\mathrm{Cl}(\mathrm{K})$ est de p-dimension nulle, K ne contient pas de racine p-ème de l'unité et $r_1+r_2-1 = 0$, donc finalement $\dim_{\mathbb{F}_p} V_\varnothing(\mathrm{K})/\mathrm{K}^{\times p} = 0$.

On conclut avec le théorème 2.2.3 en remarquant que $V_S(\mathrm{K})/\mathrm{K}^{\times p}$ est un sous-groupe de $V_\varnothing(\mathrm{K})/\mathrm{K}^{\times p}$. □

Le théorème 2.2.5 pose le cadre du chapitre 3. En effet, l'injection

$$H^2(G_{\mathrm{K},S}^T) \hookrightarrow \bigoplus_v H^2(\overline{G_v})$$

permet de voir les relations de $G_{\mathrm{K},S}^T$ comme des éléments de $\bigoplus_v H^2(\overline{G_v})$. On pourra ainsi calculer "localement" les cup-produits d'éléments de $H^1(G_{\mathrm{K},S}^T)$.

2.2.2. Générateurs. — Remarquons ici que pour tout pro-p groupe G on a :

$$H^i(G,\mathbb{F}_p) = H^i(G^{ab}/p,\mathbb{F}_p) = H^i(G^{p,el},\mathbb{F}_p).$$

On peut alors tout de suite montrer par la théorie du corps de classes que le groupe $G_{\mathrm{K},S}^T$ est de p-rang fini. Citons par exemple la formule de p-rang donnée par Koch dans [**29**] dans le cas où $T=\varnothing$:

Théorème 2.2.6 **([29]).** — *Soit* K *un corps de caractéristique différente de p et soit S un ensemble fini de places de* K*. Alors :*

$$\dim_{\mathbb{F}_p} H^1(G_{\mathrm{K},S}) = \sum_{\substack{v\in S\\ \chi(v)=p}} [\mathrm{K}_v:\mathbb{Q}_p] - \delta - r + 1 + \sum_{v\in S} \delta(\mathrm{K}_v) + \dim_{\mathbb{F}_p}\left(V_S/\mathrm{K}^{\times p}\right),$$

où $\chi(v)$ *désigne la caractéristique du complété* K_v*,* δ *vaut* 1 *ou* 0 *suivant si le corps* K *contient les racines p-èmes de l'unité ou non et* $r = r_1 + r_2$*.*

Sous des hypothèses un peu plus fortes, le théorème 2.1.4 permet d'avoir plus : la structure du groupe de cohomologie $H^1(G_{\mathrm{K},S})$.

Corollaire 2.2.7. — *Soient* K *un corps de nombres de p-groupe de classes trivial et S un ensemble fini de places de K qui ne divisent pas p. On suppose que les unités de K sont des puissances p-èmes localement en les places de S. On a alors la décomposition :*

$$H^1(G_S) \simeq \bigoplus_{v\in S} H^1(G_{\mathrm{K},\{v\}}^{p,el}).$$

Démonstration. — Sous ces hypothèses, le théorème 2.1.4 s'applique. On conclut en dualisant. □

2.2.3. Suite spectrale de Hochschild-Serre. — Le contexte du chapitre 4 nous amène à considérer un pro-p groupe $\mathcal{G}$ et son quotient par un sous-groupe normal fermé $\mathcal{H}$. La suite spectrale de Hochschild-Serre permet de relier leurs groupes de cohomologie ; elle apporte l'argument principal de la preuve du théorème 1.2.4.

Commençons par rappeler quelques généralités sur les suites spectrales : l'établissement des suites exactes à 5, 6 et 7 termes. On suit ici ce qui est fait par exemple dans [**40**, Appendix B] avec les notations usuelles.

Suite exacte à 4 termes. — Soit $E_2^{p,q} \Rightarrow E^n$ une suite spectrale. La filtration $E^1 \supset E_1^1 \supset 0$ sur E^1 donne la suite exacte

$$0 \longrightarrow E_1^1 \longrightarrow E^1 \longrightarrow E^1/E_1^1 \longrightarrow 0$$

où, par définition, $E^1/E_1^1 = E_\infty^{0,1}$. Le morphisme $d_3^{0,1}$ est trivial donc $E_\infty^{0,1} = E_3^{0,1} = \text{Ker } d_2^{0,1}$ et on a en fait :

$$0 \longrightarrow E_1^1 \longrightarrow E^1 \longrightarrow E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0}.$$

De plus, $E_1^1 = E_1^1/0 = E_1^1/E_2^1 = E_\infty^{1,0}$. Comme le morphisme $d_2^{1,0}$ est trivial, $E_\infty^{1,0}$ est égal à $E_2^{1,0}$, donc $E_1^1 = E_2^{1,0}$ et on a finalement la suite exacte :

$$0 \longrightarrow E_2^{1,0} \longrightarrow E^1 \longrightarrow E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0}.$$

Suite exacte à 5 termes. — Le morphisme $d_2^{2,0}$ est trivial, donc $\text{Ker } d_2^{2,0} = E_2^{2,0}$ et $E_3^{2,0} = E_2^{2,0}/\text{Im } d_2^{0,1}$. On a donc $\text{Im } d_2^{0,1} = \text{Ker}(E_2^{2,0} \to E_3^{2,0})$ et la suite est exacte :

$$0 \longrightarrow E_2^{1,0} \longrightarrow E^1 \longrightarrow E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0} \twoheadrightarrow E_3^{2,0}.$$

D'autre part, comme le morphisme $d_3^{2,0}$ est trivial, on a $E_4^{2,0} = E_3^{2,0}$ d'où $E_3^{2,0} = E_\infty^{2,0} = E_2^2$ et :

$$0 \longrightarrow E_2^{1,0} \longrightarrow E^1 \longrightarrow E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0} \twoheadrightarrow E_2^2.$$

Suite exacte à 6 termes. — Par définition, on a $E_1^2/E_2^2 = E_\infty^{1,1}$. Comme le morphisme $d_3^{1,1}$ est trivial, on a $E_\infty^{1,1} = E_3^{1,1}$ et on déduit $E_2^2 = \text{Ker}(E_1^2 \twoheadrightarrow E_3^{1,1})$, d'où :

$$0 \longrightarrow E_2^{1,0} \longrightarrow E^1 \longrightarrow E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0} \longrightarrow E_1^2 \twoheadrightarrow E_3^{1,1}.$$

Suite exacte à 7 termes. — On a $E_3^{1,1} = \text{Ker } d_2^{1,1}$ d'où :

$$0 \longrightarrow E_2^{1,0} \longrightarrow E^1 \longrightarrow E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0} \longrightarrow E_1^2 \longrightarrow E_2^{1,1} \xrightarrow{d_2^{1,1}} E_2^{3,0}.$$

Dans le cadre de ce travail, on exploitera une suite spectrale en particulier : la suite de Hochschild-Serre.

Théorème 2.2.8. — *Soit $\mathcal{G}$ un groupe profini, soit $\mathcal{H}$ un sous-groupe normal fermé de $\mathcal{G}$ et soit A un $\mathcal{G}$-module. Alors on a une suite spectrale cohomologique*

$$E_2^{p,q} = H^p(\mathcal{G}/\mathcal{H}, H^q(\mathcal{H}, A)) \Rightarrow H^n(\mathcal{G}, A)$$

appelée suite spectrale de Hochschild-Serre.

Démonstration. — [**42**, th. 2.1.5] □

Les groupes de cohomologie sur $\mathbb{Q}_p/\mathbb{Z}_p$ présentent un intérêt structurel : la dualité de Pontryagin relie l'abélianisé du pro-p groupe G à son premier groupe de cohomologie sur $\mathbb{Q}_p/\mathbb{Z}_p$:

$$G^{ab} \simeq H_1(G, \mathbb{Z}_p) \simeq (H^1(G, \mathbb{Q}_p/\mathbb{Z}_p))^*.$$

En choisissant $A = \mathbb{Z}_p$, on obtient :

Lemme 2.2.9. — *Soit $\mathcal{G}$ un pro-p groupe et $\mathcal{H}$ un sous-groupe normal fermé de $\mathcal{G}$. On note G le quotient de $\mathcal{G}$ par $\mathcal{H}$. Alors on a la suite exacte d'homologie à 5 termes :*

$$H_2(\mathcal{G}, \mathbb{Z}_p) \longrightarrow H_2(G, \mathbb{Z}_p) \longrightarrow \mathcal{H}_G^{ab} \longrightarrow \mathcal{G}^{ab} \twoheadrightarrow G^{ab}.$$

Si on suppose de plus $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$ trivial, alors on a la suite exacte d'homologie à 7 termes :

$$H_3(G, \mathbb{Z}_p) \longrightarrow H_1(G, \mathcal{H}^{ab}) \longrightarrow H_2(\mathcal{G}, \mathbb{Z}_p) \longrightarrow H_2(G, \mathbb{Z}_p) \longrightarrow \mathcal{H}_G^{ab} \longrightarrow \mathcal{G}^{ab} \twoheadrightarrow G^{ab}.$$

Démonstration. — On utilise la suite spectrale de Hochschild-Serre :

$$H^i(G, H^j(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)) \Rightarrow H^{i+j}(\mathcal{G}, \mathbb{Q}_p/Z_p).$$

D'après la discussion qui précède, on a la suite exacte à cinq termes :

$$0 \longrightarrow H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)^G \longrightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow E_2^2,$$

et par définition de E_2^2, on a $E_2^2 \subset E^2 = H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p)$. En dualisant on obtient alors la suite exacte d'homologie

$$0 \longleftarrow \underbrace{H_1(G, \mathbb{Z}_p)}_{G^{ab}} \longleftarrow \underbrace{H_1(\mathcal{G}, \mathbb{Z}_p)}_{\mathcal{G}^{ab}} \longleftarrow \underbrace{H_1(\mathcal{H}, \mathbb{Z}_p)_G}_{\mathcal{H}_G^{ab}} \longleftarrow H_2(G, \mathbb{Z}_p) \longleftarrow H_2(\mathcal{G}, \mathbb{Z}_p).$$

On a également vu plus haut que la suite à sept termes suivante est exacte :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) & \longrightarrow & H^1(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) & \longrightarrow & H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)^G & \longrightarrow & H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \\ & & & & & & & & \downarrow \\ & & & & & & & & E_1^2 \\ & & & & & & & \swarrow & \\ & & & & H^3(G, \mathbb{Q}_p/\mathbb{Z}_p) & \longleftarrow & H^1(G, H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)) & & \end{array}$$

Comme $E_\infty^{0,2}$ est par définition un sous-module de $E_2^{0,2} = H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$, en supposant $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$ trivial on annule le quotient $E^2/E_1^2 (= E_\infty^{0,2})$. Cela implique : $E_1^2 = E^2 = H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p)$. Il reste alors à dualiser :

$$\begin{array}{ccccccccc} 0 & \longleftarrow & \underbrace{H_1(G, \mathbb{Z}_p)}_{G^{ab}} & \longleftarrow & \underbrace{H_1(\mathcal{G}, \mathbb{Z}_p)}_{\mathcal{G}^{ab}} & \longleftarrow & \underbrace{H_1(\mathcal{H}, \mathbb{Z}_p)_G}_{\mathcal{H}_G^{ab}} & \longleftarrow & H_2(G, \mathbb{Z}_p) \longleftarrow H_2(\mathcal{G}, \mathbb{Z}_p) \\ & & & & & & & & \uparrow \\ & & & & & & & & \underbrace{H_1(G, H_1(\mathcal{H}, \mathbb{Z}_p))}_{H_1(G, \mathcal{H}^{ab})} \\ & & & & & & & \nwarrow & \\ & & & & & & H_3(G, \mathbb{Z}_p) & & \end{array}$$

et on a bien :

$$H_3(G, \mathbb{Z}_p) \longrightarrow H_1(G, \mathcal{H}^{ab}) \longrightarrow H_2(\mathcal{G}, \mathbb{Z}_p) \longrightarrow H_2(G, \mathbb{Z}_p) \longrightarrow \mathcal{H}_G^{ab} \longrightarrow \mathcal{G}^{ab} \twoheadrightarrow G^{ab}.$$

□

Corollaire 2.2.10. — *Soit $\mathcal{G}$ un pro-p groupe et $\mathcal{H}$ un sous-groupe distingué fermé. On note G le quotient de $\mathcal{G}$ par $\mathcal{H}$ et on suppose $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$ trivial. Si la dimension cohomologique $cd(G)$ de G est inférieure ou égale à 2, alors on a la suite exacte d'homologie :*

$$H_1(G, \mathcal{H}^{ab}) \hookrightarrow H_2(\mathcal{G}, \mathbb{Z}_p) \longrightarrow H_2(G, \mathbb{Z}_p) \longrightarrow \mathcal{H}_G^{ab} \longrightarrow \mathcal{G}^{ab} \twoheadrightarrow G^{ab}.$$

Remarque 2.2.11. — La suite exacte à cinq termes peut être montrée sans avoir recours à la notion de suite spectrale (voir par exemple [**42**, prop. 1.6.6]). Cette seconde preuve permet de rendre explicite les applications entre les groupes de cohomologie : si $\mathcal{G}$ est un pro-p groupe, $\mathcal{H}$ un sous-groupe normal fermé et G le quotient de $\mathcal{G}$ par $\mathcal{H}$, alors on a la suite exacte de cohomologie :

$$H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \overset{inf}{\hookrightarrow} H^1(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) \overset{res}{\longrightarrow} H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)^G \overset{tg}{\longrightarrow} H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \overset{inf}{\longrightarrow} H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p).$$

CHAPITRE 3

PROPAGATION DE LA PROPRIÉTÉ *MILD* AU-DESSUS D'UNE EXTENSION QUADRATIQUE IMAGINAIRE DE $\mathbb{Q}$

On s'intéresse dans ce chapitre aux extensions à ramification restreinte **modérée**. On se donne donc un corps de nombres K, un nombre premier p impair et un ensemble fini S de premiers de K, de normes congrues à 1 modulo p pour que l'ensemble S soit minimal et la ramification modérée dans l'extension K_S/K ; on note toujours $G_{\mathrm{K},S} := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$.

Labute, Minac et Schmidt se sont intéressés à une propriété assurant à un pro-p groupe $G_{\mathrm{K},S}$ d'être de dimension cohomologique 2 : le caractère *mild*. Le critère (LMS) (critère 3.1.5), issu de la combinaison de leurs travaux, est le point de départ de ce chapitre.

En nous plaçant dans un contexte favorable, nous exploiterons la correspondance locale-globale de la section 2.2.1 pour calculer "localement" les cup-produits d'éléments de $H^1(G_S)$. Cela nous permettra d'implémenter un corollaire du critère (LMS), le critère (LMS_f) (critère 3.1.7), et d'observer un phénomène de propagation du caractère *mild* dans les extensions quadratiques imaginaires L de $\mathbb{Q}$. Nous déterminerons alors dans la cinquième section des conditions sur la ramification des premiers de S assurant au groupe $G_{\mathrm{L},S}$ d'être *mild*, grâce auxquelles nous définirons deux graphes $\mathcal{G}_S$ et $\mathcal{G}_S^*$ pour enfin montrer le théorème 1.1.8 : le pro-p groupe $G_{\mathrm{L},S}$ est *mild* si le groupe $G_{\mathrm{K},S}$ vérifie le critère (LMS_f) et si l'un des graphes $\mathcal{G}_S$ et $\mathcal{G}_S^*$ est quasi-circulaire (voir définition 3.4.11). La dernière section est dédiée à l'étude détaillée d'un exemple. On y remarque notamment que les exemples de groupes *mild* ainsi obtenus ne vérifient pas tous le critère de Vogel ([**55**]).

Tous les calculs ont été effectués avec Pari/GP ([**54**])

À l'exception de la section 3.1.1, on se place dans la situation suivante : on considère un nombre premier p impair, un corps quadratique imaginaire L *(qu'on choisira différent de $\mathbb{Q}(j)$ si $p = 3$) de p-groupe des classes trivial et un ensemble fini $S = \{v_1, \ldots, v_s\}$ de nombres premiers congrus à 1 modulo p. On suppose de plus que tout élément de S est décomposé dans l'extension* $\mathrm{L}/\mathbb{Q}$*. L'ensemble des premiers de* L *divisant les éléments de S sera noté S', ou S lorsque cela ne présentera aucune ambiguïté.*

En particulier, les énoncés des différents résultats se placeront implicitement sous ces hypothèses.

3.1. Généralités

3.1.1. Groupes de Galois de pro-p extensions maximales à ramification restreinte. — Soit K un corps de nombres, p un nombre premier et S un ensemble fini de premiers de K de norme congrue à 1 modulo p. On s'intéresse ici à la pro-p extension maximale de K non-ramifiée en dehors de S, c'est-à-dire seulement (et éventuellement) ramifiée en les premiers de S. L'extension K_S est donc le compositum de toute les p-extensions finies de K non-ramifiées en dehors de S. En supposant que les premiers de S sont tous de norme congrue à 1 modulo p, la ramification en les premiers de S est modérée. Nous avons montré dans le chapitre 2 un certain nombre de résultats autour de la structure et de la p-dimension des premiers groupes de cohomologie de $G_{\mathrm{K},S}$ sur $\mathbb{F}_p$. Rappelons ceux dont nous nous servirons par la suite.

Pour $v \in S$, on note K_v le complété de K pour $|\cdot|_v$ et $\overline{\mathrm{K}_v}$ la pro-p extension maximale de K_v ; on pose $\overline{G_v} := \mathrm{Gal}(\overline{\mathrm{K}_v}/\mathrm{K}_v)$. Si $\mathcal{M}/\mathrm{K}$ est une extension infinie, on définit $\mathcal{M}_v$ comme la réunion des complétés des sous-extensions finies de $\mathcal{M}/\mathrm{K}$. On note en particulier $G_v = \mathrm{Gal}((\mathrm{K}_S)_v/\mathrm{K}_v)$. Les deux applications naturelles $i_v : G_v \hookrightarrow G_{\mathrm{K},S}$ et $\pi_v : \overline{G_v} \twoheadrightarrow G_v$ induisent l'application suivante, dont la construction est décrite dans la partie 2.2.1 :

$$\begin{array}{ccc} \inf \cdot \mathrm{res} : \ H^2(G_{\mathrm{K},S}) & \longrightarrow & \bigoplus_{v\in S} H^2(\overline{G_v}) \ . \\ & \searrow^{\mathrm{res}} \quad \nearrow_{\inf} & \\ & \bigoplus_{v\in S} H^2(G_v) & \end{array}$$

Son noyau, noté $Ш_S(G_{\mathrm{K},S})$ (ou $Ш_S$) est le noyau de Shafarevich du groupe $G_{\mathrm{K},S}$. Notons ici qu'une conséquence directe de cette construction est la finitude de la $\mathbb{F}_p$-dimension de $H^2(G_{\mathrm{K},S}) := H^2(G_{\mathrm{K},S}, \mathbb{F}_p)$.

D'après le diagramme commutatif ci-dessus, lorsque le groupe $Ш_S$ est trivial, les relations du groupe $G_{\mathrm{K},S}$ sont en fait des relations « locales », dans le sens où on peut les voir comme des éléments des groupes $H^2(\overline{G_v}), v \in S$. Ces groupes étant totalement décrits lorsque v est premier à p (voir par exemple [**29**, th. 10.2]), il y a un réel intérêt à se placer dans une telle situation. Nous avons montré dans le théorème 2.2.5 que c'est le cas si l'on suppose que $\mathrm{K} = \mathbb{Q}$ ou que K est un corps quadratique imaginaire bien choisi :

Théorème. — *Si* $\mathrm{K} = \mathbb{Q}$ *ou si* K *est un corps quadratique imaginaire dont le p-groupe des classes est trivial (on choisira* K *différent de* $\mathbb{Q}(j)$ *si* $p = 3$*), et si* S *est un ensemble fini de places de* K*, alors le groupe* $Ш_S$ *est trivial.*

On peut de plus montrer que sous de bonnes hypothèses arithmétiques, le groupe de cohomologie $H^1(G_{\mathrm{K},S})$ est somme directe de p-groupes. On note $\mathrm{K}_S^{p,el}/\mathrm{K}$ la p-extension élémentaire maximale de K non-ramifiée en dehors de S et $G_S^{p,el}$ son groupe de Galois. Pour $v \in S$, on note $\mathrm{K}_v^{p,el}$ le corps $\mathrm{K}_{\{v\}}^{p,el}$ et Γ_v le groupe $\mathrm{Gal}(\mathrm{K}_{\{v\}}^{p,el}/\mathrm{K})$. Rappelons le théorème 2.1.4 :

Théorème. — *On suppose le p-groupe de classes de* K *trivial. Si on suppose de plus que les unités sont des puissances p-èmes en les places* v *de* S*, alors on a la décomposition :*

$$G_{\mathrm{K},S}^{p,el} \simeq \prod_{v\in S} G_v^{p,el}.$$

En particulier, si on choisit K vérifiant les hypothèses du théorème 2.2.5 rappelé plus haut, alors $\mathcal{E}_\mathrm{K} = (1)$ et le théorème 2.1.4 s'applique. En remarquant que

$$H^1(G_{\mathrm{K},S}) \simeq H^1(G_{\mathrm{K},S}^{p,el})$$

puis en dualisant, on obtient également une décomposition en somme directe de $H^1(G_{\mathrm{K},S})$ donnée dans le corollaire 2.2.7 :

Corollaire. — *Si* $\mathrm{K} = \mathbb{Q}$ *ou si* K *est une extension quadratique imaginaire de* $\mathbb{Q}$ *vérifiant les conditions du théorème 2.2.5, on a la décomposition*

$$H^1(G_{\mathrm{K},S}) \simeq \bigoplus_{v\in S} H^1(\Gamma_v).$$

Remarque 3.1.1. — Sous les hypothèses du théorème 2.1.4, l'espace vectoriel $H^1(\Gamma_v)$ est de dimension 1 pour tout v dans S. On a donc en particulier $\dim_{\mathbb{F}_p} H^1(G_{\mathrm{K},S}) = |S|$.

3.1.2. Pro-p groupes *mild* et critère de Labute-Minac-Schmidt. — Soit G un pro-p groupe de type fini et F/R une présentation minimale de G ; F est un pro-p groupe libre sur les générateurs de G, engendré par $d(G) = \dim_{\mathbb{F}_p} H^1(G)$ éléments $x_1, \ldots, x_d$.

L'application

$$\begin{array}{rcl} \{x_1, \ldots, x_d\} & \longrightarrow & \mathbb{F}_p^{nc}[\![X_1, \ldots, X_d]\!] \\ x_i & \longmapsto & 1 + X_i \end{array}$$

induit un isomorphisme entre l'algèbre $\mathbb{F}_p[\![F]\!]$ et l'algèbre non-commutative $\mathbb{F}_p^{nc}[\![X_1, \ldots, X_d]\!]$ des séries formelles sur $\mathbb{F}_p$ à d variables, appelée algèbre de Magnus (voir par exemple **[12]**, ou **[29**, chap. 7**]** pour une preuve). On peut alors plonger F dans l'algèbre de Magnus et voir les relations de G comme des séries formelles appartenant à son idéal d'augmentation I.

La notion de famille strictement libre de séries formelles est introduite par Forré dans **[12]**.

Définition 3.1.2 **(Forré, [12]).** — Soit $\{\rho_1, \ldots, \rho_r\}$ une famille d'éléments de I. On note R l'idéal bilatère de $\mathbb{F}_p^{nc}[\![X_1, \ldots, X_d]\!]$ engendré par les ρ_i et B l'algèbre quotient $\mathbb{F}_p^{nc}[\![X_1, \ldots, X_d]\!]\Big/_R$. La famille $\{\rho_1, \ldots, \rho_r\}$ est dite strictement libre si ${}^R\!/_{RI}$ est un B-module libre à gauche sur les classes des ρ_i.

On peut alors donner une définition de pro-p groupe *mild* équivalente à celle qu'utilise par exemple Labute dans **[30]**, sans avoir recours à l'étude d'algèbres de Lie.

Définition 3.1.3. — Le pro-p groupe G est dit *mild* s'il existe une présentation minimale de G telle que les images des relations de G forment une famille strictement libre dans $\mathbb{F}_p^{nc}[\![X_1, \ldots, X_d]\!]$.

Labute, dans **[30]**, et Forré, dans **[12]**, ont démontré qu'un groupe *mild* possède des propriétés intéressantes, notamment :

Théorème 3.1.4 **(Labute, [30]).** — *Soit G un groupe mild et $G = F/(\rho_1, \ldots, \rho_r)$ une présentation minimale strictement libre de G. On suppose $r \neq 0$. Alors :*

(a) *Le groupe G est de dimension cohomologique 2.*

(b) *On note $\mathrm{gr}(\mathbb{F}_p[\![G]\!])$ l'algèbre graduée associée à la filtration de $\mathbb{F}_p[\![G]\!]$ par les puissances de son idéal d'augmentation.*
La série de Poincaré de $\mathrm{gr}(\mathbb{F}_p[\![G]\!])$ est $\dfrac{1}{1 - dt + \sum_{i=1}^{r} t^{\deg(\rho_i)}}$.

Montrer qu'un pro-p groupe est *mild* en appliquant la définition 3.1.3 nécessite d'avoir une description explicite du début des relations de G. Le résultat suivant, issu des travaux de Labute, Minac et Schmidt (**[49]**, **[30]**, **[31]**) et basé sur un critère d'Anick (**[1]**) permet d'établir le caractère *mild* d'un pro-p groupe en étudiant le cup-produit sur son premier groupe de cohomologie.

Théorème 3.1.5 **(Critère de Labute-Minac-Schmidt, [49], [50], [31])**
Soit G un pro-p groupe de p-rang fini. Si les groupes de cohomologie (sur $\mathbb{F}_p$) de G satisfont les conditions suivantes :

(i) *il existe deux $\mathbb{F}_p$-espaces vectoriels U et V tels que $H^1(G) \simeq U \oplus V$,*
(ii) *la restriction du cup-produit $\cup : H^1(G) \times H^1(G) \to H^2(G)$ à $V \otimes V$ est identiquement nulle,*
(iii) *la restriction du cup-produit $\cup : H^1(G) \times H^1(G) \to H^2(G)$ à $U \otimes V$ est surjective,*

alors le pro-p groupe G est mild.

Dans le cadre dans lequel se place ce chapitre, c'est-à-dire pour K un corps de nombres et S un ensemble fini de premiers de K tels que le groupe de Galois $G_{\mathrm{K},S}$ soit de p-rang fini et de noyau de Shafarevich $Ш_S$ trivial, les cup-produits sont plus faciles à calculer localement (voir section suivante). On regardera donc plutôt la composée du cup-produit avec l'application $\inf \cdot \mathrm{res}$ (qu'on notera encore $\cup$) :

Corollaire 3.1.6. — *Si il existe deux $\mathbb{F}_p$-espaces vectoriels U et V tels que :*

(i) $H^1(G_{\mathrm{K},S}) \simeq U \oplus V$,
(ii) $\cup : V \otimes V \to \bigoplus_{v \in S} H^2(\overline{G_v})$ *est identiquement nulle,*

(iii) $\cup : U \otimes V \to \bigoplus_{v\in S} H^2(\overline{G_v})$ *est surjective,*

alors le pro-p groupe $G_{\mathrm{K},S}$ *est mild et* $r(G_{\mathrm{K},S}) = \dim_{\mathbb{F}_p} H^2(G_{\mathrm{K},S}) = |S|$.

De plus, d'après le corollaire 2.2.7, on a la décomposition :

$$H^1(G_{\mathrm{K},S}) = \bigoplus_{v\in S} H^1(\Gamma_v).$$

On supposera donc naturellement que la décomposition de $H^1(G_{\mathrm{K},S})$ vérifiant le critère de Labute-Minac-Schmidt est « compatible » avec cette écriture, c'est-à-dire qu'il existe $\mathcal{U}, \mathcal{V}$ deux sous-ensembles de S tels que les $\mathbb{F}_p$-espaces vectoriels U et V soient de la forme :

$$U = \bigoplus_{v\in\mathcal{U}} H^1(\Gamma_v), \qquad V = \bigoplus_{v\in\mathcal{V}} H^1(\Gamma_v),$$

et on utilisera en pratique le corollaire suivant :

Corollaire 3.1.7. — *S'il existe deux* $\mathbb{F}_p$*-espaces vectoriels* $U = \bigoplus_{v\in\mathcal{U}} H^1(\Gamma_v)$ *et* $V = \bigoplus_{v\in\mathcal{V}} H^1(\Gamma_v)$ *tels que :*

(i) $H^1(G_{\mathrm{K},S}) \simeq U \oplus V$,

(ii) $\cup : V \otimes V \to \bigoplus_{v\in S} H^2(\overline{G_v})$ *est identiquement nulle,*

(iii) $\cup : U \otimes V \to \bigoplus_{v\in S} H^2(\overline{G_v})$ *est surjective,*

alors le pro-p groupe $G_{\mathrm{K},S}$ *est mild et* $r(G_{\mathrm{K},S}) = \dim_{\mathbb{F}_p} H^2(G_{\mathrm{K},S}) = |S|$.

Définition 3.1.8. — On dira dans ce cas que le corps K vérifie le critère de Labute-Minac-Schmidt en respectant S. On fera référence au corollaire 3.1.7 par la notation (LMS_f).

Remarque 3.1.9. — Pour que le corps K vérifie le critère de Labute-Minac-Schmidt en respectant S, il faut $|\mathcal{U}||\mathcal{V}| \geqslant |S|$, et en particulier $|S| \geqslant 4$, $|\mathcal{U}| \geqslant 2$ et $|\mathcal{V}| \geqslant 2$.

Remarque 3.1.10. — Le critère de Labute-Minac-Schmidt et sa version faible (LMS_f) ne sont pas équivalents (l'exemple 3.5.1 à venir est un contre-exemple).

3.2. Calculs de cup-produits

3.2.1. Calculs de cup-produits dans le cas d'un corps local. — Dans cette section, k désignera un localisé $\mathbb{Q}_v$ ou L_w pour $v \in S$ ou $w \in S'$. Par définition de L (voir préambule du chapitre), k est une extension finie de $\mathbb{Q}_v$ pour un certain $v \in S$. On note $\hat{\mathrm{k}}$ sa pro-p- extension séparable maximale, k^{nr} sa pro-p-extension non-ramifiée maximale et $\overline{G}$, G^{nr} les groupes de Galois correspondants. Par définition de S, le corps k contient les racines p-èmes de l'unité, et on notera ζ_p une racine primitive p-ème de l'unité.

Les cup-produits d'éléments de $H^1(\overline{G})$ peuvent être calculés grâce au symbole d'Artin, via l'isomorphisme entre $H^2(\overline{G})$ et le groupe de racines p-èmes de l'unité μ_p. On suit ici ce qui est fait, par exemple, dans [**29**, chap. 10] et [**42**, chap.7].

La suite exacte de Kummer

$$0 \longrightarrow \mathbb{F}_p \xrightarrow{\lambda} \hat{\mathrm{k}}^\times \xrightarrow{p} \hat{\mathrm{k}}^\times \longrightarrow 1\ ,$$

où $\lambda : a \mapsto \zeta_p^a$ et $p : x \mapsto x^p$, induit les suites exactes de cohomologie suivantes :

$$H^0(\overline{G}, \hat{\mathrm{k}}^\times) \xrightarrow{p} H^0(\overline{G}, \hat{\mathrm{k}}^\times) \longrightarrow H^1(\overline{G}) \longrightarrow H^1(\overline{G}, \hat{\mathrm{k}}^\times)\ ,$$

$$H^1(\overline{G}, \hat{\mathrm{k}}^\times) \longrightarrow H^2(\overline{G}) \xrightarrow{\lambda^*} H^2(\overline{G}, \hat{\mathrm{k}}^\times) \xrightarrow{p} H^2(\overline{G}, \hat{\mathrm{k}}^\times)\ .$$

Par définition de $\overline{G}$, on a $H^0(\overline{G}, \hat{\mathrm{k}}^\times) = (\hat{\mathrm{k}}^\times)^{\overline{G}} = \mathrm{k}^\times$, et d'après le théorème de Hilbert 90, $H^1(\overline{G}, \hat{\mathrm{k}}^\times) = 0$. La première suite exacte donne donc l'isomorphisme $H^1(\overline{G}) \simeq \mathrm{k}^\times/\mathrm{k}^{\times p}$.

Toujours d'après le théorème d'Hilbert 90, λ^* est injective. On obtient donc de la deuxième suite exacte de cohomologie l'égalité

$$\dim_{\mathbb{F}_p} H^2(\overline{G}, \hat{\mathrm{k}}^\times)[p] = \dim_{\mathbb{F}_p} H^2(\overline{G}).$$

Comme k est un corps local contenant les racines de l'unité, on a de plus $\dim_{\mathbb{F}_p} H^2(\overline{G}) = 1$ (voir par exemple [**29**, th. 10.2]). Le groupe $H^2(\overline{G}, \hat{\mathrm{k}}^\times)[p]$ est donc un groupe cyclique d'ordre p, isomorphe à $\mathbb{Z}_p/p\mathbb{Z}_p$, donc à μ_p car ici l'action de $\overline{G}$ sur μ_p est triviale (on rappelle que $\mu_p \subset \mathrm{k}$). On peut expliciter un tel isomorphisme. En notant

$$\begin{array}{rcl} \iota : H^2(\overline{G}, \hat{\mathrm{k}}^\times) & \longrightarrow & \mu_p \\ \varepsilon & \longmapsto & \zeta_p^{p \cdot \mathrm{inv}_{\mathrm{k}} \varepsilon} \end{array},$$

où $\mathrm{inv}_{\mathrm{k}} : H^2(\overline{G}, \hat{\mathrm{k}}^\times) \to \mathbb{Q}/\mathbb{Z}$, la composition $\psi = \iota \circ \lambda^*$ est un isomorphisme de $H^2(\overline{G})$ sur μ_p ([**29**, sec. 8.9]).

D'autre part, si $\alpha \in \mathrm{k}^\times$ et si g est un élément de $\overline{G}$, alors l'image $g(\sqrt[p]{\alpha})$ est de la forme $g(\sqrt[p]{\alpha}) = \zeta_p^{\chi_\alpha(g)} \sqrt[p]{\alpha}$, où, par définition, χ_α est un caractère de $\overline{G}$. On définit ainsi un isomorphisme

$$\begin{array}{rcl} \varphi : \mathrm{k}^\times/\mathrm{k}^{\times p} & \longrightarrow & H^1(\overline{G}) \\ \alpha & \longmapsto & \chi_\alpha \end{array}.$$

On peut alors montrer :

Proposition 3.2.1. — *L'application φ fait commuter le diagramme :*

$$\begin{array}{ccccc} H^1(\overline{G}) & \times & H^1(\overline{G}) & \xrightarrow{\cup} & H^2(\overline{G}) \\ \| & & \downarrow{\scriptstyle \varphi^{-1}} & & \uparrow{\scriptstyle \psi^{-1}} \\ H^1(\overline{G}) & \times & \mathrm{k}^\times/\mathrm{k}^{\times p} & \xrightarrow{\cup} & \mu_p \end{array},$$

où la flèche du bas est définie par $\chi \cup \alpha = \chi(\sigma_\alpha)$, avec σ_α l'élément de $\overline{G}$ associé à α par la théorie du corps de classes.

Démonstration. — Ce résultat est montré dans [**42**, prop. 7.2.13]. □

Corollaire 3.2.2. — *L'espace vectoriel $H^1(G^{nr})$ est égal à son orthogonal (pour le cup-produit).*

Démonstration. — Soit ψ un caractère de $\overline{G}$ et χ un générateur de $H^1(G^{nr})$. Soit $\alpha \in \mathrm{k}^\times/\mathrm{k}^{\times p}$ tel que $\chi = \varphi\alpha$. Comme χ est un caractère non ramifié, α est une unité et d'après la proposition 3.2.1, on a alors $\psi \cup \chi = \psi(\sigma_\alpha)$, où σ_α est l'élément du groupe d'inertie $\overline{I}$ de $\overline{G}$ associé à α par la théorie du corps de classes. Le cup-produit $\psi \cup \chi$ est donc nul si ψ est trivial sur $\overline{I}$, c'est-à-dire $H^1(G^{nr}) \subset H^1(G^{nr})^\perp$.

Comme k est un corps local contenant les racines p-èmes de l'unité, le cup-produit est une forme bilinéaire non dégénérée et on peut conclure avec un argument de dimensions : l'espace vectoriel $H^1(G^{nr})$ est de dimension 1, et $H^1(\overline{G})$ est de dimension 2, donc $\dim_{\mathrm{k}} H^1(G^{nr})^\perp = 1$ et on a bien égalité. □

3.2.2. Calcul local des cup-produits. — Replaçons-nous dans le contexte initial. On considère un corps K égal à $\mathbb{Q}$ ou à une extension quadratique imaginaire de $\mathbb{Q}$, vérifiant les conditions décrites dans le préambule du chapitre.

D'après le théorème 2.2.5, le groupe de cohomologie $H^2(G_{\mathrm{K},S})$ s'injecte dans la somme $\bigoplus_{v \in S} H^2(\overline{G_v})$. On appellera « calcul local » des cup-produits de caractères de $G_{\mathrm{K},S}$ le calcul de l'image de ces cup-produits dans $\bigoplus_{v \in S} H^2(\overline{G_v})$. La commutativité du diagramme

$$\begin{array}{ccccc} & & \bigoplus_{v \in S} H^1(\overline{G_v}) \times \bigoplus_{v \in S} H^1(\overline{G_v}) & & \\ & \overset{\mathrm{inf}\cdot\mathrm{res}}{\nearrow} & & \overset{\cup}{\searrow} & \\ H^1(G_{\mathrm{K},S}) \times H^1(G_{\mathrm{K},S}) & \xrightarrow{\cup} & H^2(G_{\mathrm{K},S}) & \xrightarrow{\mathrm{inf}\cdot\mathrm{res}} & \bigoplus_{v \in S} H^2(\overline{G_v}) \end{array}$$

permet dans ce cas de ramener, via l'application $\inf \cdot \mathrm{res}$, les calculs dans le contexte local étudié dans la section précédente.

On a montré dans le corollaire 2.2.7 que le groupe $H^1(G_{\mathrm{K},S})$ admet une décomposition $\bigoplus_{v\in S} H^1(\Gamma_v)$ en somme directe de groupes de cohomologie de $\mathbb{F}_p$-dimension 1. On note χ_v un générateur de $H^1(\Gamma_v)$ pour $v \in S$. Le cup-produit étant bilinéaire, on s'intéressera uniquement aux cup-produits $\chi_v \cup \chi_w$, $v, w \in S$.

Théorème 3.2.3. — *Soient v_1, v_2, w trois premiers de S. En notant $(\chi_{v_1} \cup \chi_{v_2})_w$ l'image du cup-produit $\chi_{v_1} \cup \chi_{v_2}$ sur la composante $H^2(\overline{G_w})$ de $\bigoplus_{v\in S} H^2(\overline{G_v})$, on a :*

$$(\chi_{v_1} \cup \chi_{v_2})_w = \begin{cases} 0 \text{ si } w \neq v_1, v_2, \text{ ou } v_1 = v_2, \\ 0 \text{ si } w = v_i \text{ et } v_j \text{ est décomposé dans l'extension } \mathrm{K}_{v_i}^{p,el}/\mathrm{K}, \\ \neq 0 \text{ sinon.} \end{cases}$$

Démonstration. — Soient $v_1, v_2, w \in S$. On s'intéresse à l'image du cup-produit $\chi_{v_1} \cup \chi_{v_2}$ sur la composante $H^2(\overline{G_w})$ de $\bigoplus_{v\in S} H^2(\overline{G_v})$. Comme le cup-produit sur le premier groupe de cohomologie est antisymétrique, on a $(\chi_v \cup \chi_v)_w = 0$ pour tous $v, w \in S$. On suppose pour la suite $v_1 \neq v_2$. On suppose en particulier sans perte de généralité que le caractère $\inf \cdot \mathrm{res}_w(\chi_{v_2})$, s'il est non trivial, est non ramifié. Le corollaire 3.2.2 permet alors de conclure : le cup-produit $(\chi_{v_1} \cup \chi_{v_2})_w$ est non-nul si et seulement si les caractères $\inf \cdot \mathrm{res}_w(\chi_{v_1})$ et $\inf \cdot \mathrm{res}_w(\chi_{v_2})$ sont respectivement ramifié et non trivial, donc si et seulement si $v_1 = w$ et v_2 est inerte dans l'extension $\mathrm{K}_w^{p,el}/\mathrm{K}$.

□

3.3. Critère de Labute-Minac-Schmidt par rapport à S ; calculs

3.3.1. Frobenius auxiliaires. — Si l'on souhaite comparer les cup-produits d'éléments de $\bigoplus_{v\in S} H^1(\Gamma_v)$ dans l'espace vectoriel $\bigoplus_{v\in S} H^2(\overline{G_v})$, pour vérifier les hypothèses du critère (LMS_f) par exemple, savoir si chacune des composante est, ou non, nulle peut ne pas suffire. Dans ce cas, on calcule les cup-produits par la méthode des Frobenius auxiliaires (voir [**39**, sec. 2.7]).

Pour chaque $v \in S$, on choisit un premier p_v de K tel que :

- p_v est inerte dans l'extension $\mathrm{K}_v^{p,el}/\mathrm{K}$,
- p_v est totalement décomposé dans l'extension $\mathrm{K}_w^{p,el}/\mathrm{K}$ pour $w \in S, w \neq v$.

Le Frobenius en p_v, noté F_{p_v}, engendre le groupe de décomposition $D_{p_v}(\mathrm{L}_S^{p,el}/\mathrm{L})$. Or, par hypothèses, $D_{p_v}(\mathrm{K}_S^{p,el}/\mathrm{K}) = I_v(\mathrm{K}_v^{p,el}/\mathrm{K})$, donc F_{p_v} engendre le groupe d'inertie $I_v(\mathrm{K}_v^{p,el}/\mathrm{K})$ et la famille $\{F_{p_v}, v \in S\}$ est une base de $\mathrm{Gal}(\mathrm{K}_S^{p,el}/\mathrm{K})$. On note $\{\widetilde{\chi}_v, v \in S\}$ sa base duale. Le caractère $\widetilde{\chi_v}$ est donc, par construction, un générateur du groupe de cohomologie $H^1(\Gamma_v)$.

On note a_v le générateur de $\mathcal{U}_v/\mathcal{U}_v^p$ associé à F_{p_v} par la théorie du corps de classes.

Proposition 3.3.1. — *Avec les notations précédentes, si v, w sont deux éléments de S avec v inerte dans $\mathrm{K}_w^{p,el}/\mathrm{K}$, la composante locale en w du cup-produit $\widetilde{\chi}_w \cup \widetilde{\chi}_v$ est donnée par l'entier l_{vw} tel que $F_v = F_{p_w}^{l_{vw}}$ dans Γ_w.*

Démonstration. — Soient v, w deux éléments de S. Supposons v inerte dans $\mathrm{K}_w^{p,el}/\mathrm{K}$. D'après la proposition 3.2.1, $(\widetilde{\chi}_w \cup \widetilde{\chi}_v)_w = \inf \cdot \mathrm{res}_w(\widetilde{\chi}_w)(\sigma_v)$, où σ_v est l'élément de $\overline{I_w}$ associé à $\alpha_v = \varphi^{-1}(\inf \cdot \mathrm{res}_w(\widetilde{\chi}_v))$ par la théorie du corps de classes. Comme $\inf \cdot \mathrm{res}_w(\widetilde{\chi}_v)$ est un caractère non-ramifié, α_v est une unité et il existe un entier k tel que $\alpha_v = a_w^k$ dans $\mathcal{U}_w/\mathcal{U}_w^p$. Ceci implique $\sigma_v = F_{p_w}^k$ et

$$(\widetilde{\chi}_w \cup \widetilde{\chi}_v)_w = \inf \cdot \mathrm{res}_w(\widetilde{\chi}_w)(F_{p_w}^k) = k.$$

Pour obtenir la composante en w du cup-produit $\widetilde{\chi}_w \cup \widetilde{\chi}_v$, il suffit donc de déterminer l'image de σ_v dans $\mathrm{K}_w^{p,el}/\mathrm{K}$. □

Remarque 3.3.2. — Ce calcul dépend du choix du premier p_w de la manière suivante :

Soit q_w un premier auxiliaire pour w différent de p_w. On note $\widehat{\chi}_w$ le caractère dual de son Frobenius et b_w l'élément qui lui est associé par la théorie du corps de classe. On a alors $b_w = a_w^k$, où k est premier à p, et $(\widehat{\chi}_w \cup \widetilde{\chi}_v)_w = k l_{vw}$.

Remarque 3.3.3. — Les entiers l_{vw} ainsi définis sont appelés *linking numbers* par Labute dans [**30**] et Vogel dans [**55**] (voir sec. 3.5.2).

Le critère (LMS_f) peut se reformuler de la manière suivante :

Proposition 3.3.4. — *Sous les hypothèses décrites dans le préambule du chapitre, s'il existe un entier $t \in \{1, \dots, |S|\}$ et si on peut ordonner les premiers de S de sorte que la matrice $C = (c_{i,j})$ définie pour $1 \leqslant i \leqslant t|S|$, $0 \leqslant j \leqslant |S|$, par :*

$$c_{i,j} = \begin{cases} \delta_{j,m} l_{v_n, v_m} + \delta_{j,n} l_{v_m, v_n} & si \quad 1 \leqslant i \leqslant t^2, i-1 = (n-1)t + (m-1) \\ \delta_{j,m} l_{v_{n+t}, v_m} + \delta_{j,n+t} l_{v_m, v_{n+t}} & si \quad t^2+1 \leqslant i \leqslant t|S|, \\ & \qquad i-1 = (n-1)(|S|-t) + (m-1) + t^2 \end{cases}$$

vérifie :

- *les t premières lignes de la matrices C sont nulles ;*
- *la matrice C est de rang $|S|$;*

alors le pro-p groupe $G_{\mathrm{K},S}$ est mild et $r(G_{\mathrm{K},S}) = \dim_{\mathbb{F}_p} H^2(G_{\mathrm{K},S}) = |S|$.

3.3.2. Exemples. — La méthode des Frobenius auxiliaires ramène le calcul local de cup-produits à la comparaison de Frobenius dans des extensions relatives de degré p. Une fois implémenté dans PARI/GP ([**54**]), ce procédé permet d'obtenir des exemples variés de pro-p groupes *mild*. La philosophie du code utilisé est présentée en annexe A.

Exemple 3.3.5. — Soit $p = 3$, $\mathrm{K} = \mathbb{Q}$ et $S = \{\ell_1 = 7, \ell_2 = 13, \ell_3 = 79, \ell_4 = 97\}$.

On calcule les premiers auxiliaires suivants : $p_1 = 131$, $p_2 = 433$, $p_3 = 239$ et $p_4 = 811$.
Les *linking numbers* l_{21}, l_{31} et l_{41} s'obtiennent en comparant les Frobenius F_{ℓ_2}, F_{ℓ_3} et F_{ℓ_4} à F_{p_1} dans le groupe Γ_{ℓ_1}. L'extension $\mathbb{Q}_{\ell_1}^{3,el} = \mathbb{Q}(\theta_1)$ est définie par une racine θ_1 du polynôme $x^3 - 21x + 7$. Les premiers ℓ_2 et ℓ_4 sont décomposés dans cette extension, et $F_{\ell_3} = F_{p_1}$, donc $l_{21} = l_{41} = 0$ et $l_{31} = 1$.

Dans l'extension $\mathbb{Q}_{\ell_2}^{3,el}$, engendrée par une racine θ_2 de $x^3 - 39x - 65$, le premier ℓ_3 est décomposé et $F_{\ell_1} = F_{\ell_4} = F_{p_2}$. On a donc $l_{12} = l_{42} = 1$ et $l_{32} = 0$. On calcule de la même manière $l_{13} = l_{14} = l_{24} = -1$, $l_{23} = 1$ et $l_{43} = l_{34} = 0$.

En posant $\mathcal{L}_1 = \ell_3, \mathcal{L}_2 = \ell_4, \mathcal{L}_3 = \ell_1, \mathcal{L}_4 = \ell_2$, la matrice définie dans la proposition 3.3.4 est la transposée de la matrice suivante :

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

Elle vérifie bien les deux conditions de la proposition 3.3.4, donc le groupe $G_{\mathrm{K},S}$ est *mild*.

Le groupe $G_{\mathrm{K},S}$ dépend de trois données : le corps de base K, le premier p et l'ensemble S de places de K. Soit $\mathrm{L}/\mathbb{Q}$ une extension quadratique et S un ensemble fini de nombres premiers tels que les corps $\mathbb{Q}$ et L vérifient le critère de Labute-Minac-Schmidt en respectant S pour un premier p donné. Peut-on faire varier le corps L ou le premier p tout en conservant le caractère *mild* au dessus de L ?

Sous les hypothèses décrites dans le préambule du chapitre, un corps quadratique ne peut vérifier le critère de Labute-Minac-Schmidt en respectant un ensemble S donné que pour un nombre fini de premiers p, chaque élément de S devant être de norme congrue à 1 modulo p.

Exemple 3.3.6. — Soit $S = \{31, 61, 151, 211\}$. Le corps $\mathrm{L} = \mathbb{Q}(\sqrt{-15})$ vérifie le critère de Labute-Minac-Schmidt en respectant S pour $p = 3$ et $p = 5$.

On fixe maintenant un ensemble S de nombres premiers et p un nombre premier impair tels que $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S. Les exemples suivants montrent qu'il peut exister plusieurs corps quadratiques vérifiant le critère de Labute-Minac-Schmidt en respectant S.

Exemple 3.3.7. — Soit $p = 3$ et $S = \{7, 13, 79, 97\}$. La proposition 3.3.4 s'applique aux corps $\mathbb{Q}(\sqrt{-d})$ pour $d \in \{66, 94, 185, 285, 290, 355, 391, 454, 458, 521, 607, 614, 647, 703, 829, 881, 906\}$.

Exemple 3.3.8. — Soit $S = \{37, 103, 127, 139\}$ et $\mathrm{L} = \mathbb{Q}(\sqrt{-d})$ un corps quadratique de p-groupe de classes trivial dans lequel tous les éléments de S se décomposent. Si $p = 3$ et $d < 10^3$, le corps L vérifie le critère de Labute-Minac-Schmidt en respectant S.

3.3.3. Quelques données statistiques. — Les exemples 3.3.7 et 3.3.8 montrent qu'à p fixé, un ensemble S donné permet de construire plusieurs pro-p groupes *mild*. Cette section apporte une réponse statistique à la question de leur nombre, en proposant de calculer pour plusieurs ensembles S la proportion de corps quadratiques vérifiant les hypothèses données dans le préambule du chapitre, de discriminant borné, auquel la proposition 3.3.4 s'applique.
On note $\mathbb{E}_S(X)$ l'ensemble des corps quadratiques imaginaires de discriminants inférieurs à X, de p-groupes de classes triviaux et dans lesquels les éléments de S sont décomposés.

On calcule

$$P_{S,p}(X) = \frac{\#\{\mathrm{L} \in \mathbb{E}_S(X), \text{la proposition 3.3.4 s'applique à L}\}}{\#\{\mathrm{L} \in \mathbb{E}_S(X)\}}.$$

Les tableaux suivants présentent les valeurs de $P_{S,3}(10^5)$ et $P_{S,5}(10^5)$ pour différents exemples d'ensembles S tels que $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S.

S	$P_{S,3}(10^5)$
$\{13, 127, 193, 349\}$	$\frac{1879}{2151} \simeq 0.8735$
$\{223, 271, 307, 499\}$	$\frac{1997}{2258} \simeq 0.8844$
$\{67, 157, 337, 421\}$	$\frac{1929}{2238} \simeq 0.8619$
$\{31, 79, 199, 409\}$	$\frac{1778}{2103} \simeq 0.8455$

S	$P_{S,3}(10^5)$
$\{337, 349, 379, 463\}$	$\frac{2004}{2341} \simeq 0.8560$
$\{37, 103, 127, 139\}$	$\frac{1900}{2140} \simeq 0.8879$
$\{79, 103, 157, 331\}$	$\frac{1833}{2204} \simeq 0.8317$
$\{97, 151, 313, 457\}$	$\frac{1933}{2236} \simeq 0.8645$

S	$P_{S,5}(10^5)$
$\{101, 131, 211, 251\}$	$\frac{1931}{2888} \simeq 0.6686$
$\{11, 31, 41, 211\}$	$\frac{1820}{2561} \simeq 0.7107$
$\{31, 181, 191, 271\}$	$\frac{1970}{2865} \simeq 0.6876$
$\{211, 251, 401, 421\}$	$\frac{1897}{2916} \simeq 0.6505$

3.4. Un critère de propagation du caractère *mild* de $G_{\mathbb{Q},S}$ à $G_{\mathrm{L},S}$

Soit p un nombre premier, L un corps quadratique imaginaire et S un ensemble fini de nombres premiers vérifiant les conditions énoncées dans le préambule du chapitre. Afin d'alléger les notations, les groupes $G_{\mathbb{Q},S}$ et $G_{\mathrm{L},S}$ seront respectivement notés G_S et H_S dans toute cette section et les autres notations seront adaptées en conséquence.

3.4.1. Cup-produits d'éléments de $H^1(H_S)$. — On a vu dans la section 3.2.2 que les cup-produits de caractères de H_S peuvent être calculés localement, mais sous les hypothèses fixées ici, on peut également les déduire en partie des cup-produits sur $H^1(G_S)$. En effet, les extensions $\mathrm{L}/\mathbb{Q}$ et $\mathbb{Q}_S/\mathbb{Q}$ étant linéairement disjointes, on a une surjection $H_S \twoheadrightarrow G_S$, et comme chaque $v \in S$ est décomposé dans $\mathrm{L}/\mathbb{Q}$, les groupes $\overline{H_w}$ et $\overline{G_v}$ sont isomorphes pour $w|v$. Les applications $\inf_{H_S}^{G_S}$ et $\inf_{\overline{H_w}}^{\overline{G_v}}$ pour $w|v$ sont donc bien définies. On notera pour la suite $\inf = \sum_{\substack{w|v \\ v\in S}} \inf_{\overline{H_w}}^{\overline{G_v}}$.

Proposition 3.4.1. — *Le diagramme suivant est commutatif :*

$$\begin{array}{ccccc}
H^1(H_S)\times H^1(H_S) & \xrightarrow{\cup} & H^2(H_S) & \xrightarrow{\inf\cdot\mathrm{res}} & \bigoplus_{w\in S'} H^2(\overline{H_w}) \\
\uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} \\
H^1(G_S)\times H^1(G_S) & \xrightarrow{\cup} & H^2(G_S) & \xrightarrow{\inf\cdot\mathrm{res}} & \bigoplus_{v\in S} H^2(\overline{G_v}),
\end{array}$$

où les applications $\inf\cdot\mathrm{res}$ *sont définies comme dans la section 2.1.*

Démonstration. — Ce résultat se montre directement avec les cocycles, en utilisant [**42**, prop. 1.5.3] pour le carré de gauche et [**42**, prop. 1.5.5] pour le carré de droite. □

On suppose pour la suite que le corps K vérifie le critère de Labute-Minac-Schmidt en respectant S et on notera U et V les sous-espaces vectoriels de $H^1(G_S)$ vérifiant les hypothèses du critère (LMS_f). D'après le théorème 2.1.4, on a les décompositions :

$$H^1(G_S) = \bigoplus_{v\in S} H^1(\Gamma_v) \quad \text{et} \quad H^1(H_S) = \bigoplus_{w\in S'} H^1(\gamma_w),$$

où les groupes $\Gamma_v = \mathrm{Gal}(\mathrm{K}_v^{p,el}/\mathrm{K})$ et $\gamma_w = \mathrm{Gal}(\mathrm{L}_w^{p,el}/\mathrm{L})$ sont tous de p-rang 1. Pour $v \in S$, on note χ_v un générateur de $H^1(\Gamma_v)$ et pour $w \in S'$, on note Ψ_w un générateur de $H^1(\gamma_w)$.

3.4.1.1. *Plongements diagonaux.* — Si $E = \bigoplus_{v\in\mathcal{E}} H^1(\Gamma_v)$ est un sous-$\mathbb{F}_p$-espace vectoriel de $H^1(G_S)$, on note $\underline{E}$ son plongement diagonal dans $H^1(H_S)$ via l'inflation.

• Soit $v \in S$. On note F le compositum $\mathrm{L}\mathbb{Q}_v^{p,el}$. Comme v est totalement ramifié dans $\mathbb{Q}_v^{p,el}/\mathbb{Q}$ et totalement décomposé dans $\mathrm{L}/\mathbb{Q}$, $v^{(1)}$ et $v^{(2)}$ sont ramifiés dans F/L. L'extension F/L est donc une sous-extension de $\mathrm{L}_v^{p,el}/\mathrm{L}$ de degré p, distincte de $\mathrm{L}_{v^1}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v^2}^{p,el}/\mathrm{L}$.

On en déduit que $\underline{H^1(\Gamma_v)} = \inf(H^1(\Gamma_v)) = \langle a_v\Psi_{v^{(1)}} + b_v\Psi_{v^{(2)}}\rangle$ dans $H^1(H_S)$, où $a_v, b_v \in \mathbb{F}_p$ avec $a_v b_v \neq 0$. Pour la suite, on choisit les générateurs $\Psi_{v^{(1)}}$ et $\Psi_{v^{(2)}}$ de telle sorte que $a_v = b_v = 1$.
En particulier, si $\mathcal{E}$ est une partie de S et E le $\mathbb{F}_p$-espace vectoriel $E = \bigoplus_{v\in\mathcal{E}} H^1(\Gamma_v)$, on a :

$$\underline{E} = \bigoplus_{v\in\mathcal{E}} \langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}}\rangle.$$

De plus, pour tout $v \in S$, l'inflation induit un isomorphisme entre les espaces vectoriels (de $\mathbb{F}_p$-dimension 1) $H^1(\Gamma_v)$ et $\langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}} \rangle$. En particulier :

$$H^1(G_S) = \bigoplus_{v\in S} H^1(\Gamma_v) \overset{\inf}{\simeq} \bigoplus_{v\in S} \langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}} \rangle,$$
$$U \simeq \underline{U} = \bigoplus_{u\in \mathcal{U}} \langle \Psi_{u^{(1)}} + \Psi_{u^{(2)}} \rangle,$$
$$V \simeq \underline{V} = \bigoplus_{v\in \mathcal{V}} \langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}} \rangle.$$

• Soit $v \in S$, $w \in S', w|v$. Comme v est décomposé dans l'extension $\mathrm{L}/\mathbb{Q}$, les groupes $\overline{G_v}$ et $\overline{H_w}$ sont identiques. L'application $\inf_{\overline{H_w}}^{\overline{G_v}}$ est alors un isomorphisme et

$$\inf(H^2(\overline{G_v})) = \inf_{\overline{H_{v^{(1)}}}}^{\overline{G_v}}(H^2(\overline{G_v})) + \inf_{\overline{H_{v^{(2)}}}}^{\overline{G_v}}(H^2(\overline{G_v})) = \langle E_{v^{(1)}} + E_{v^{(2)}} \rangle$$

dans $\prod_{w\in S'} H^2(\overline{H_w})$, où $E_{v^{(1)}}$ et $E_{v^{(2)}}$ sont des générateurs respectivement de $H^2(\overline{H_{v^{(1)}}})$ et $H^2(\overline{H_{v^{(2)}}})$ images d'un même générateur de $H^2(\overline{G_v})$.

On a finalement :

Lemme 3.4.2. — *Le diagramme suivant est commutatif :*

$$\begin{array}{ccccc}
\bigoplus_{v\in S}\langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}} \rangle \times \bigoplus_{v\in S}\langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}} \rangle & \longrightarrow & H^2(H_S) & \longrightarrow & \bigoplus_{v\in S}\langle E_{v^{(1)}} + E_{v^{(2)}} \rangle \\
\uparrow \inf & & \uparrow \inf & & \uparrow \inf \\
\bigoplus_{v\in S} H^1(\Gamma_v) \times \bigoplus_{v\in S} H^1(\Gamma_v) & \xrightarrow{\cup} & H^2(G_S) & \xrightarrow{\inf\cdot\mathrm{res}} & \bigoplus_{v\in S} H^2(\overline{G_v}),
\end{array}$$

et les flèches verticales de droite et de gauche sont des isomorphismes.

3.4.1.2. *Critère de Labute-Minac-Schmidt sur H_S.* — On utilise le paragraphe précédent pour déterminer des espaces vectoriels $\overline{U}$ et $\overline{V}$ et des hypothèses sur la ramification des premiers de S' tels que le corollaire 3.1.6 s'applique à $H^1(H_S) = \overline{U} \oplus \overline{V}$.

On pose $\overline{V} := \underline{V}$.

Lemme 3.4.3. — *L'application de $\overline{V}\otimes\overline{V}$ dans $\bigoplus_{w\in S'} H^2(\overline{H_w})$ induite par $\inf\cdot\mathrm{res}\cdot\cup$ est identiquement nulle.*

Démonstration. — Le groupe G_S vérifie le critère de Labute-Minac-Schmidt en respectant S ; en particulier l'application $V \otimes V \longrightarrow \bigoplus_{v\in S} H^2(\overline{G_v})$ induite par $\inf\cdot\mathrm{res}\cdot\cup$ est identiquement nulle. On conclut grâce au lemme 3.4.2. □

Lemme 3.4.4. — *L'application de $\underline{U}\otimes\overline{V}$ dans $\bigoplus_{v\in S}\langle E_{v^{(1)}} + E_{v^{(2)}} \rangle$ induite par $\inf\cdot\mathrm{res}\cdot\cup$ est surjective.*

Démonstration. — Considérons le diagramme :

$$\begin{array}{ccc}
\underline{U}\otimes\overline{V} & \xrightarrow{\inf\cdot\mathrm{res}\cdot\cup} & \bigoplus_{v\in S}\langle E_{v^{(1)}} + E_{v^{(2)}} \rangle \\
\uparrow \inf & & \uparrow \inf \\
U \otimes V & \xrightarrow{\inf\cdot\mathrm{res}\cdot\cup} & \bigoplus_{v\in S} H^2(\overline{G_v}),
\end{array}$$

où $U = \bigoplus_{v\in\mathcal{U}} H^1(\Gamma_v)$, $V = \bigoplus_{v\in\mathcal{V}} H^1(\Gamma_v)$, $\underline{U} = \inf(U) = \bigoplus_{u\in\mathcal{U}}\langle \Psi_{u^{(1)}} + \Psi_{u^{(2)}} \rangle$ et $\overline{V} = \underline{V} = \bigoplus_{v\in\mathcal{V}}\langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}} \rangle$. Ce diagramme est commutatif d'après le lemme 3.4.2. D'après le théorème 2.2.5, l'application $\inf\cdot\mathrm{res} : H^2(G_S) \to \bigoplus_{v\in S} H^2(\overline{G_v})$ est injective. Comme G_S vérifie les hypothèses du corollaire 3.1.7, on a de plus la surjection $U \otimes V \twoheadrightarrow \bigoplus_{v\in S} H^2(\overline{G_v})$. D'après le lemme 3.4.2, la flèche du bas est donc une

surjection. Les observations du paragraphe 3.4.1.1 montrent que la flèche de droite est un isomorphisme. La flèche diagonale est donc surjective, ce qui implique la surjectivité de la flèche du haut. □

On fait pour la suite l'une des deux hypothèses suivantes :

($H1$) (a) Pour tout $v \in \mathcal{V}$, il existe $v^1|v$, $u_v \in \mathcal{U}$, et $u_v^1|u_v$ tels que u_v^1 est inerte dans $\mathrm{L}_{v^1}^{p,el}/\mathrm{L}$ et décomposé dans $\mathrm{L}_{v^2}^{p,el}/\mathrm{L}$, et v^1 et v^2 sont décomposés dans $\mathrm{L}_{u_v^1}^{p,el}/\mathrm{L}$.

(b) Pour tout $u \in \mathcal{U}$, il existe $v_u \in \mathcal{V}$ et $i,j \in \{1,2\}$ tels que v_u^i est inerte et v_u^j décomposé dans $\mathrm{L}_{u^1}^{p,el}/\mathrm{L}$, et u^1 est inerte dans $\mathrm{L}_{v_u^i}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v_u^j}^{p,el}/\mathrm{L}$.

ou

($H2$) (a) Pour tout $u \in \mathcal{U}$, il existe $u^1|u$, $v_u \in \mathcal{V}$ et $v_u^1|v_u$ tels que u^1 est inerte dans $\mathrm{L}_{v_u^1}^{p,el}/\mathrm{L}$ et décomposé dans $\mathrm{L}_{v_u^2}^{p,el}/\mathrm{L}$, et v_u^1 et v_u^2 sont décomposés dans $\mathrm{L}_{u^1}^{p,el}/\mathrm{L}$.

(b) Pour tout $v \in \mathcal{V}$, il existe $u_v \in \mathcal{U}$ et $i,j \in \{1,2\}$ tels que v^i est inerte et v^j décomposé dans $\mathrm{L}_{u_v^1}^{p,el}/\mathrm{L}$, et u_v^1 est inerte dans $\mathrm{L}_{v^i}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v^j}^{p,el}/\mathrm{L}$.

Par symétrie, on peut se placer sans perte de généralité sous l'hypothèse ($H1$).
Pour chaque $u \in \mathcal{U}$ (resp. $v \in \mathcal{V}$), on choisit $v_u \in \mathcal{V}$ (resp. $u_v \in \mathcal{U}$) qui vérifie l'hypothèse ($H1$). On construit ainsi un ensemble $\mathcal{E} = \{(u,v_u),(v,v_u)\}$ de $|S|$ couples de $\mathcal{U} \times \mathcal{V}$.

On note respectivement F_u et F_v les images de $(\Psi_{v_u^1} + \Psi_{v_u^2}, \Psi_{u^1}) \in \overline{V} \times H^1(\gamma_{u^1})$ et $(\Psi_{v^1} + \Psi_{v^2}, \Psi_{u_v^1}) \in \overline{V} \times H^1(\gamma_{u_v^1})$ dans $\bigoplus_{w \in S'} H^2(\overline{H_w})$ pour $(u,v_u),(u_v,v) \in \mathcal{E}$.

Lemme 3.4.5. — *La famille $\{F_w, w \in S\}$ ainsi construite complète la famille $\{E_{w^{(1)}} + E_{w^{(2)}}, w \in S\}$ en une base de $\bigoplus_{\nu \in S'} H^2(\overline{H_\nu})$.*

Démonstration. — Soit $u \in \mathcal{U}$. On a alors d'après le théorème 3.2.3 :

$$(\Psi_{v_u^1} \cup \Psi_{u^1})_{u^1} \neq 0 \text{ et } (\Psi_{v_u^2} \cup \Psi_{u^1})_{u^1} = 0,$$
$$(\Psi_{v_u^1} \cup \Psi_{u^1})_{u^2} = (\Psi_{v_u^2} \cup \Psi_{u^1})_{u^2} = 0,$$
$$(\Psi_{v_u^1} \cup \Psi_{u^1})_{v_u^1} \neq 0 \text{ et } (\Psi_{v_u^2} \cup \Psi_{u^1})_{v_u^2} \neq 0$$

d'où, par bilinéarité du cup-produit :

$$((\Psi_{v_u^1} + \Psi_{v_u^2}) \cup \Psi_{u^1})_{u^1} \neq 0,$$
$$((\Psi_{v_u^1} + \Psi_{v_u^2}) \cup \Psi_{u^1})_{u^2} = 0,$$
$$((\Psi_{v_u^1} + \Psi_{v_u^2}) \cup \Psi_{u^1})_{v_u^1} \neq 0,$$
$$((\Psi_{v_u^1} + \Psi_{v_u^2}) \cup \Psi_{u^1})_{v_u^2} \neq 0.$$

On a alors d'après ce qui précède $F_u = (\Psi_{v_u^1} + \Psi_{v_u^2}) \cup \Psi_{u^1} = (*,0,*,*)$ dans $H^2(\overline{H_{u^1}}) \oplus H^2(\overline{H_{u^2}}) \oplus H^2(\overline{H_{v_u^1}}) \oplus H^2(\overline{H_{v_u^2}})$, où les $*$ sont non nuls. D'après le théorème 3.2.3, F_u est nul sur $\bigoplus_{\substack{w \in S \\ w \neq u, v_u}} H^2(\overline{H_{w^1}}) \oplus H^2(\overline{H_{w^2}})$.

Toujours d'après le théorème 3.2.3 on a pour $v \in \mathcal{V}$:

$$((\Psi_{v^1} + \Psi_{v^2}) \cup \Psi_{u_v^1})_{u_v^1} = 0,$$
$$((\Psi_{v^1} + \Psi_{v^2}) \cup \Psi_{u_v^1})_{u_v^2} = 0,$$
$$((\Psi_{v^1} + \Psi_{v^2}) \cup \Psi_{u_v^1})_{v^1} \neq 0,$$
$$((\Psi_{v^1} + \Psi_{v^2}) \cup \Psi_{u_v^1})_{v^2} = 0,$$

donc $F_v = (\Psi_{v^1} + \Psi_{v^2}) \cup \Psi_{u_v^1}$ est nul sur $\bigoplus_{\substack{w \in S \\ w \neq u_v, v}} H^2(\overline{H_{w^1}}) \oplus H^2(\overline{H_{w^2}})$ et de la forme $(0,0,*,0)$ avec $*$ non nul dans $H^2(\overline{H_{u_v^1}}) \oplus H^2(\overline{H_{u_v^2}}) \oplus H^2(\overline{H_{v^1}}) \oplus H^2(\overline{H_{v^2}})$.

On peut maintenant montrer le lemme. Considérons une combinaison linéaire $\sum_{w \in S} \alpha_w (E_{w^1} + E_{w^2}) + \sum_{w \in S} \beta_w F_w$, $(\alpha_w)_{w \in S}, (\beta_w)_{w \in S} \subset \mathbb{F}_p$. Elle est nulle si et seulement si chacune de ses composantes est nulle.

Soit $u \in \mathcal{U}$. D'après ce qui précède, le seul élément de cette combinaison linéaire dont la composante sur $H^2(\overline{H_{u^2}})$ est non nulle est $(E_{u^1} + E_{u^2})$, ce qui implique $\alpha_u = 0$, et ceci est valable pour tout $u \in \mathcal{U}$. En raisonnant composante par composante, on peut de même montrer que les $\beta_u, u \in \mathcal{U}$, les $\alpha_v, v \in \mathcal{V}$, et enfin les $\beta_v, v \in \mathcal{V}$ sont également nuls. La famille $\{E_{w^{(1)}} + E_{w^{(2)}}, F_w, w \in S\}$ est bien une base de $\bigoplus_{\nu \in S'} H^2(\overline{H_\nu})$.

□

Remarque 3.4.6. — Si on se place sous l'hypothèse $(H2)$, on a :

- pour $u \in \mathcal{U}$, $F_u = (0, 0, *, 0)$ dans $H^2(\overline{H_{u_v^1}}) \oplus H^2(\overline{H_{u_v^2}}) \oplus H^2(\overline{H_{v^1}}) \oplus H^2(\overline{H_{v^2}})$, où $*$ est non nul,
- pour $v \in \mathcal{V}$, $F_v = (*, 0, *, *)$ dans $H^2(\overline{H_{u^1}}) \oplus H^2(\overline{H_{u^2}}) \oplus H^2(\overline{H_{v_u^1}}) \oplus H^2(\overline{H_{v_u^2}})$, où les $*$ sont non nuls.

Finalement, considérons les sous-$\mathbb{F}_p$-espaces vectoriels de $\bigoplus_{v \in S'} H^1(\gamma_v)$

$$\overline{V} = \bigoplus_{v \in \mathcal{V}} \langle \Psi_{v^{(1)}} + \Psi_{v^{(2)}} \rangle,$$

$$\mathring{U} = \bigoplus_{u \in \mathcal{U}} \langle \Psi_{u^{(1)}} + \Psi_{u^{(2)}} \rangle + \bigoplus_{\substack{u \in \mathcal{U} \\ (u, v_u) \in \mathcal{E}}} H^1(\gamma_{u^1}) + \sum_{\substack{v \in \mathcal{V} \\ (u_v, v) \in \mathcal{E}}} H^1(\gamma_{u_v^1}).$$

Soit $\overset{\bullet}{U}$ un supplémentaire de $\overline{V} + \mathring{U}$ (qui existe puisque $\bigoplus_{v \in S'} H^1(\gamma_v)$ est un espace vectoriel de dimension finie $2|\mathcal{U}| + 2|\mathcal{V}|$). Par définition, $\overline{V}$ et $\mathring{U}$ sont en somme directe, donc $\mathring{U} \oplus \overset{\bullet}{U}$ est en fait un supplémentaire de $\overline{V}$ dans $\bigoplus_{v \in S'} H^1(\gamma_v)$, que l'on notera $\overline{U}$.

On peut montrer le lemme suivant :

Lemme 3.4.7. — *L'application de $\overline{U} \otimes \overline{V}$ dans $\bigoplus_{w \in S'} H^2(\overline{H_w})$ induite par $\inf \cdot \mathrm{res} \cdot \cup$ est surjective.*

Démonstration. — Considérons la base $\mathcal{B} = \{E_{w^{(1)}} + E_{w^{(2)}}, F_w, w \in S\}$ de $\bigoplus_{\nu \in S'} H^2(\overline{H_\nu})$ précédemment construite. Pour tout $w \in S$, l'élément $E_{w^{(1)}} + E_{w^{(2)}}$ a un antécédent dans $\underline{U} \otimes \overline{V}$ d'après le lemme 3.4.4. D'autre part, pour $u \in \mathcal{U}$, F_u est l'image de $(\Psi_{u^1}, \Psi_{v_u^{(1)}} + \Psi_{v_u^{(2)}}) \in H^1(\gamma_{u^1}) \times \overline{V}$ et, pour $v \in \mathcal{V}$, F_v est l'image d'un élément de $\overline{V} \times H^1(\gamma_{u_v^1})$.

Par définition, les espaces vectoriels $\bigoplus_{\substack{u \in \mathcal{U} \\ (u, v_u) \in \mathcal{E}}} H^1(\gamma_{u^1})$, $\sum_{\substack{v \in \mathcal{V} \\ (u_v, v) \in \mathcal{E}}} H^1(\gamma_{u_v^1})$ et $\underline{U}$ sont inclus dans $\overline{U}$, donc tout élément de $\mathcal{B}$ a un antécédent dans $\overline{U} \otimes \overline{V}$ par l'application $\inf \cdot \mathrm{res} \cdot \cup$ et le lemme est prouvé.

□

Finalement, si on suppose que $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S et que les hypothèses sur la ramification des premiers de S considérées ci-dessus sont vérifiées, alors les lemmes 3.4.3 et 3.4.7 s'appliquent et les hypothèses du critère (LMS_f) sont vérifiées.

Proposition 3.4.8. — *Si $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S et si l'une des hypothèses $(H1)$ ou $(H2)$ est vérifiée, alors le groupe H_S est mild et $d(H_S) = r(H_S) = 2|S|$.*

3.4.2. Utilisation de l'action galoisienne. — Le groupe de Galois $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$, engendré par un élément σ d'ordre 2, agit transitivement sur les premiers de L divisant un même nombre premier.

Soit u un élément de S. Le conjugué par σ d'un premier ramifié (resp. décomposé, inerte) dans $\mathrm{L}_{u^1}^{p,el}/\mathrm{L}$ est ramifié (resp. décomposé, inerte) dans l'extension $\sigma(\mathrm{L}_{u^1}^{p,el})/\mathrm{L}$. En particulier, $\sigma(\mathrm{L}_{u^1}^{p,el})/\mathrm{L}$ est une extension de degré p non-ramifiée en dehors de $u^2 = \sigma(u^1)$. Par maximalité de $\mathrm{L}_{u^2}^{p,el}$, on déduit $\sigma(\mathrm{L}_{u^1}^{p,el}) = \mathrm{L}_{u^2}^{p,el}$.

Ces observations permettent de réécrire les hypothèses de la proposition 3.4.8. On considère l'hypothèse $(H1)$, le résultat s'étendra à $(H2)$ par symétrie. Les deux points de $(H1)$ sont stables sous l'action de $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$. En effet, sous l'action de $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$, l'hypothèse devient :

$(\sigma(H1))$ (a') Pour tout $v \in \mathcal{V}$, il existe $v^2|v$, $u_v \in \mathcal{U}$ et $u_v^2|u_v$ tels que u_v^2 est inerte dans $\mathrm{L}_{v^2}^{p,el}/\mathrm{L}$ et décomposé dans $\mathrm{L}_{v^1}^{p,el}/\mathrm{L}$, et v^2 et v^1 sont décomposés dans $\mathrm{L}_{u_v^2}^{p,el}/\mathrm{L}$.

(b') Pour tout $u \in \mathcal{U}$, il existe $v_u \in \mathcal{V}$ et $i, j \in \{1, 2\}$ tels que v_u^j est inerte et v_u^i est décomposé dans $\mathrm{L}_{u^2}^{p,el}/\mathrm{L}$, et u^2 est inerte dans $\mathrm{L}_{v_u^j}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v_u^i}^{p,el}/\mathrm{L}$.

Les hypothèses $(H1)$ et $(H2)$ sont donc respectivement équivalentes à

$(H1')$ (a) pour tout $v \in \mathcal{V}$, il existe $u_v \in \mathcal{U}$ tel que u_v^1 est inerte et u_v^2 est décomposé dans $\mathrm{L}_{v^1}^{p,el}/\mathrm{L}$, et v^1 est décomposé dans $\mathrm{L}_{u_v^1}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{u_v^2}^{p,el}/\mathrm{L}$, où v^1 et u_v^1 sont des premiers de L divisant respectivement v et u_v, et u_v^2 le conjugué de u_v^1,

(b) pour tout $u \in \mathcal{U}$, il existe $v_u \in \mathcal{V}$ tel que v_u^1 est inerte et v_u^2 est décomposé dans $\mathrm{L}_{u^1}^{p,el}/\mathrm{L}$, et u^1 est inerte dans $\mathrm{L}_{v_u^1}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v_u^2}^{p,el}/\mathrm{L}$, où u^1 et v_u^1 sont des premiers de L divisant respectivement u et v_u, et v_u^2 le conjugué de v_u^1,

et

$(H2')$ (a) pour tout $u \in \mathcal{U}$, il existe $v_u \in \mathcal{V}$ tel que u^1 est inerte et u^2 est décomposé dans $\mathrm{L}_{v_u^1}^{p,el}/\mathrm{L}$, et v_u^1 est décomposé dans $\mathrm{L}_{u^1}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{u^2}^{p,el}/\mathrm{L}$, où v_u^1 et u^1 sont des premiers de L divisant respectivement v_u et u, et u^2 le conjugué de u^1,

(b) pour tout $v \in \mathcal{V}$, il existe $u_v \in \mathcal{U}$ tel que v^1 est inerte et v^2 est décomposé dans $\mathrm{L}_{u_v^1}^{p,el}/\mathrm{L}$, et u_v^1 est inerte dans $\mathrm{L}_{v^1}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v^2}^{p,el}/\mathrm{L}$, où u_v^1 et v^1 sont des premiers de L divisant respectivement u_v et v, et v^2 le conjugué de v^1.

La proposition 3.4.8 devient alors :

Proposition 3.4.9. — *Si $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S et si l'une des hypothèses $(H1')$ ou $(H2')$ est vérifiée, alors le groupe H_S est mild et $d(H_S) = r(H_S) = 2|S|$.*

3.4.3. Graphes quasi-circulaires. — On conserve les mêmes notations. On suppose que $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S pour la décomposition $S = \mathcal{U} \cup \mathcal{V}$, et on construit les graphes orientés $\mathcal{G}_S$ et $\mathcal{G}_S^*$ dont les sommets sont les premiers de S de la manière suivante :

- Un arc (v_i, v_j) relie le premier v_i au premier v_j dans le graphe $\mathcal{G}_S$ lorsque :
  - le premier v_i^1 est inerte et le premier v_i^2 est décomposé dans l'extension $\mathrm{L}_{v_j^1}^{p,el}/\mathrm{L}$, et le premier v_j^1 est inerte dans les extensions $\mathrm{L}_{v_i^1}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v_i^2}^{p,el}/\mathrm{L}$, si $v_i \in \mathcal{V}$ et $v_j \in \mathcal{U}$
  - le premier v_i^1 est inerte et le premier v_i^2 est décomposé dans $\mathrm{L}_{v_j^1}^{p,el}/\mathrm{L}$, et le premier v_j^1 est décomposé dans les extensions $\mathrm{L}_{v_i^1}^{p,el}/\mathrm{L}$ et $\mathrm{L}_{v_i^2}^{p,el}/\mathrm{L}$, si $v_i \in \mathcal{U}$ et $v_j \in \mathcal{V}$.

- Un arc (v_i, v_j) relie le premier v_i au premier v_j dans le graphe $\mathcal{G}_S^*$ lorsque (v_j, v_i) est un arc du graphe $\mathcal{G}_S$.

Comme $S = \mathcal{U} \cup \mathcal{V}$, on obtient deux graphes bipartis.

Remarque 3.4.10. — Pour une décomposition $S = \mathcal{U} \cup \mathcal{V}$ donnée, les graphes $\mathcal{G}_S$ et $\mathcal{G}_S^*$ sont distincts par définition, mais leurs graphes non-orientés sous-jacents sont égaux.

On définit la notion de graphe quasi-circulaire :

Définition 3.4.11. — Un graphe est dit quasi-circulaire s'il admet un sous-graphe couvrant dont les sommets sont de degré entrant égal à 1.

On peut désormais montrer le théorème :

Théorème 3.4.12. — *Si $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S et si l'un des graphes $\mathcal{G}_S$ ou $\mathcal{G}_S^*$ est quasi-circulaire, alors le groupe H_S est mild et $d(H_S) = r(H_S) = 2|S|$.*

Démonstration. — Les premiers de S vérifient la condition $(H1')$ de la proposition 3.4.9 si et seulement si chaque élément $u \in \mathcal{U}$ (resp. $v \in \mathcal{V}$) peut être relié à un élément $v_u \in \mathcal{V}$ (resp. $u_v \in \mathcal{U}$) par un arc (v_u, u) (resp. (u_v, v)) dans le graphe $\mathcal{G}_S$. On note $\mathcal{A}$ l'ensemble de ces $|S|$ arcs. On note $\mathcal{H}_S$ le sous-graphe de $\mathcal{G}_S$ défini par $\mathcal{A}$. Par définition de $\mathcal{A}$, $\mathcal{H}_S$ est un sous-graphe couvrant de $\mathcal{G}_S$ dont chaque sommet est

de degré entrant 1. Finalement, la condition $(H1')$ est vérifiée par les premiers de S si et seulement si le graphe $\mathcal{G}_S$ est quasi-circulaire.

On montre de même l'équivalence entre la condition $(H2')$ et le caractère quasi-circulaire du graphe $\mathcal{G}_S^*$. Finalement, le théorème 3.4.12 est équivalent à la proposition 3.4.9, d'où le résultat.

□

Remarque 3.4.13. — On peut montrer (voir par exemple [**23**, th. 16.5]) qu'un graphe orienté faiblement connexe a tous ses sommets de degré entrant 1 si et seulement si il contient exactement un circuit élémentaire $\mathcal{Z}$ et si les composantes faiblement connexes du sous-graphe obtenu en lui enlevant les arcs de $\mathcal{Z}$ sont des arbres enracinés (dont les racines sont des sommets appartement initialement à $\mathcal{Z}$). Le sous-graphe couvrant $\mathcal{H}_S$ est donc une union disjointe de tels graphes, et le nombre de circuits élémentaires contenus dans $\mathcal{H}_S$ est borné par $\frac{1}{2}\min\{|\mathcal{U}|, |\mathcal{V}|\}$.

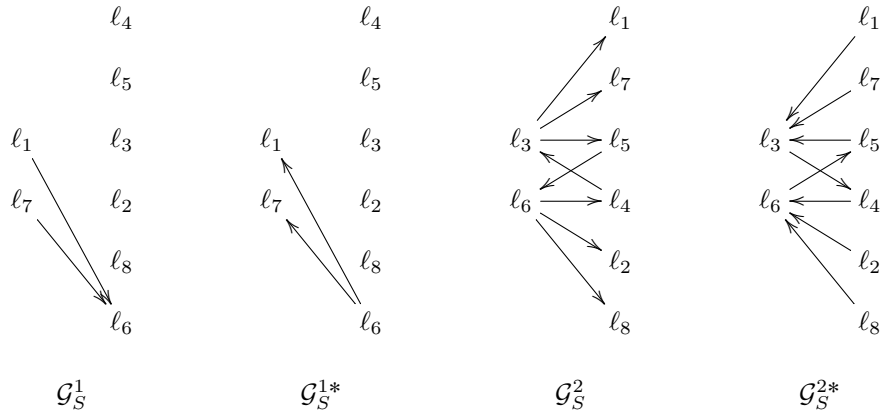
Corollaire 3.4.14. — *Si $|S| = 4$, alors les premiers de S vérifient la condition $(H1')$ (resp. $(H2')$) si et seulement si le graphe $\mathcal{G}_S$ (resp. $\mathcal{G}_S^*$) admet comme sous-graphe un circuit élémentaire (de longueur 4). En particulier, les graphes $\mathcal{G}_S$ et $\mathcal{G}_S^*$ sont dans ce cas simultanément quasi-circulaires.*

Remarque 3.4.15. — Les graphes $\mathcal{G}_S$ et $\mathcal{G}_S^*$ dépendent de la décomposition $S = \mathcal{U} \cup \mathcal{V}$ pour laquelle $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt en respectant S. Il arrive que cette décomposition ne soit pas unique et dans ce cas plusieurs situations peuvent se produire :

- Si deux décompositions $\mathcal{U}_1 \cup \mathcal{V}_1$ et $\mathcal{U}_2 \cup \mathcal{V}_2$ sont symétriques (c'est-à-dire si $\mathcal{U}_1 = \mathcal{V}_2$), alors pour $i \neq j$, les graphes $\mathcal{G}_S^i$ et $\mathcal{G}_S^{j*}$ sont identiques.

  Exemple : $p = 3, d = 418, S = \{7, 181, 307, 313\}$.
- Sinon, le théorème 3.4.12 peut être vérifié pour l'une des deux décomposition sans l'être pour l'autre.

  Exemple : Soit $S = \{\ell_1 = 7, \ell_2 = 43, \ell_3 = 61, \ell_4 = 103, \ell_5 = 109, \ell_6 = 163, \ell_7 = 223, \ell_8 = 241\}$, $\mathrm{L} = \mathbb{Q}(\sqrt{-5})$ et $p = 3$. Le corps $\mathbb{Q}$ vérifie le critère de Labute-Minac-Schmidt pour les décompositions $\mathcal{U}_1 \cup \mathcal{V}_1 = \{\ell_2, \ell_3, \ell_4, \ell_5, \ell_6, \ell_8\} \cup \{\ell_1, \ell_7\}$ et $\mathcal{U}_2 \cup \mathcal{V}_2 = \{\ell_1, \ell_2, \ell_4, \ell_5, \ell_7, \ell_8\} \cup \{\ell_3, \ell_6\}$. On obtient quatre graphes distincts, et seul $\mathcal{G}_S^2$ est quasi-circulaire :



3.5. Exemple complémentaire

Cette section est dédiée à l'étude détaillée d'un exemple. Nous montrerons dans un premier temps, via l'étude du groupe $G_{\mathrm{L},S}$ dans le cas où $p = 3$, $\mathrm{L} = \mathbb{Q}(\sqrt{-5})$ et $S = \{61, 223, 229, 487\}$, qu'il existe des groupes de Galois vérifiant le théorème 3.4.12 auxquels on ne peut pas appliquer le critère (LMS_f). Le paragraphe 3.5.2 prouve que les exemples de groupes *mild* obtenus par le théorème 3.4.12 ne vérifient pas tous le critère de Vogel ([**55**]).

Comme dans la section précédente, si $\mathrm{L}/\mathbb{Q}$ est une extension quadratique, on notera $G_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ et $H_S = \mathrm{Gal}(\mathrm{L}_S/\mathrm{L})$. De plus, pour $i = 1, \ldots, 4$, $j = 1, 2$, on note χ_i un générateur de $H^1(G_{v_i}^{p,el})$ et Ψ_i^j

un générateur de $H^1(H^{p,el}_{v_i^{(j)}})$. Les cup-produits sont calculés localement grâce à la méthode des Frobenius auxiliaires (section 3.3.1) et exprimés sous forme de 4-uplets (resp. 8-uplets) dans $\bigoplus_{v\in S} H^2(\overline{G_v})$ (resp. $\bigoplus_{v\in S'} H^2(\overline{H_v})$).

3.5.1. Un exemple de pro-p groupe *mild* ne vérifiant pas le critère 3.1.7. —

Exemple 3.5.1. — Prenons $p = 3, S = \{61, 223, 229, 487\}, d = 5$.

On note $p_1 = 61, p_2 = 223, p_3 = 229, p_4 = 487$.

• Le groupe G_S :

On a :

$$\chi_1 \cup \chi_2 = (1,2,0,0) \quad \chi_1 \cup \chi_3 = (1,0,0,0) \quad \chi_1 \cup \chi_4 = (0,0,0,0)$$
$$\chi_2 \cup \chi_3 = (0,2,2,0) \quad \chi_2 \cup \chi_4 = (0,0,0,1) \quad \chi_3 \cup \chi_4 = (0,0,2,1)$$

En posant $U = H^1(G^{p,el}_{p_2}) \oplus H^1(G^{p,el}_{p_3})$ et $V = H^1(G^{p,el}_{p_1}) \oplus H^1(G^{p,el}_{p_4})$, le groupe G_S vérifie les hypothèses du critère (LS_f). Le groupe G_S est donc *mild*.

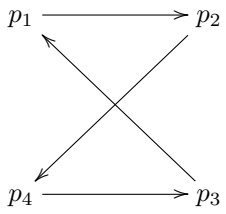
• Le groupe H_S :

L'extension $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ est une extension quadratique imaginaire de $\mathbb{Q}$ de 3-groupe des classes trivial. De plus, $\left(\frac{-5}{61}\right) = \left(\frac{-5}{223}\right) = \left(\frac{-5}{229}\right) = \left(\frac{-5}{487}\right) = 1$, donc L/$\mathbb{Q}$ est bien S-décomposée.

Le tableau suivant donne la ramification des premiers $p_j^{(k)}$ dans les extensions $\mathrm{L}^{p,el}_{p_i^{(l)}}/\mathrm{L}$. Le coefficient à la i-ème ligne et j-ème colonne est -1,0 ou 1 suivant si le premier $p_j^{(k)}$ et ramifié, décomposé ou inerte dans $\mathrm{L}^{p,el}_{p_i^{(l)}}/\mathrm{L}$.

	p_1^1	p_1^2	p_2^1	p_2^2	p_3^1	p_3^2	p_4^1	p_4^2
p_1^1	-1	0	1	1	0	1	1	1
p_1^2	0	-1	1	1	1	0	1	1
p_2^1	1	0	-1	1	1	0	0	0
p_2^2	0	1	1	-1	0	1	0	0
p_3^1	0	0	0	1	-1	1	1	0
p_3^2	0	0	1	0	1	-1	0	1
p_4^1	1	1	1	0	1	1	-1	1
p_4^2	1	1	0	1	1	1	1	-1

On obtient le graphe $\mathcal{G}_S$ suivant :



Le circuit $(p_1p_2p_4p_3p_1)$ est un circuit élémentaire de longueur 4 passant par tous les sommets de $\mathcal{G}_S$. Le groupe H_S est donc un groupe *mild*, à 8 générateurs et 8 relations.

On peut également, en reprenant ce qui est fait dans la section 3.4.1.2, expliciter des ensembles $\overline{U}$ et $\overline{V}$ pour lesquels le groupe H_S vérifie le critère 3.1.6 :
Ici, $V = H^1(G^{p,el}_{p_1}) \oplus H^1(G^{p,el}_{p_4})$, donc $\overline{V}$ est de la forme $\overline{V} = \langle \Psi_1^1 + \Psi_1^2 \rangle \oplus \langle \Psi_4^1 + \Psi_4^2 \rangle$. On sait de plus que $\overline{U}$ contient $\langle \Psi_2^1 + \Psi_2^2 \rangle \oplus \langle \Psi_3^1 + \Psi_3^2 \rangle$, ainsi que $\langle \Psi_2^1 \rangle$ et $\langle \Psi_3^1 \rangle$ d'après le tableau ci-dessus. Comme les cup-produits de

$$\overline{V} \times \langle \Psi_2^1 + \Psi_2^2 \rangle \oplus \langle \Psi_3^1 + \Psi_3^2 \rangle \oplus \langle \Psi_2^1 \rangle \oplus \langle \Psi_3^1 \rangle$$

engendrent $\bigoplus_{v\in S'} H^2(\overline{H_v})$, il suffit de considérer un supplémentaire de $\overline{V}$ dans $H^1(H_S)$ contenant $\langle \Psi_2^1 + \Psi_2^2 \rangle \oplus \langle \Psi_3^1 + \Psi_3^2 \rangle \oplus \langle \Psi_2^1 \rangle \oplus \langle \Psi_3^1 \rangle$.

Remarque 3.5.2. — Le corps $\mathbb{Q}(\sqrt{-5})$ ne vérifie pas le critère de Labute-Minac-Schmidt en respectant S dans l'exemple précédant. En effet, il n'existe pas d'ensembles de places $\mathcal{U}$ et $\mathcal{V}$ tels que $H^1(H_S) = \overline{U} \oplus \overline{V}$ avec $\overline{U} = \bigoplus_{u\in\mathcal{U}} H^1(H^{p,el}_u)$, $\overline{V} = \bigoplus_{v\in\mathcal{V}} H^1(H^{p,el}_v)$ tels que le cup-produits soit trivial sur $\overline{V} \times \overline{V}$ et surjectif de $\overline{U} \times \overline{V}$ dans $\bigoplus_{v\in S'} H^2(\overline{H_v})$.

Le calcul local des cup-produits donne les candidats suivants pour $\mathcal{V}$: $\{p_2^1, p_4^2\}$, $\{p_2^2, p_4^1\}$, $\{p_1^2, p_3^2\}$, $\{p_1^1, p_3^1\}$ et $\{p_1^1, p_1^2\}$. Pour déterminer si le cup-produit est, ou non, surjectif pour chacun de ces ensembles, on applique la proposition 3.3.4 en utilisant la méthode des Frobenius auxiliaires (section 3.3.1).

Par exemple, si on suppose $\mathcal{V} = \{p_2^1, p_4^2\}$, on calcule le rang de la matrice ci-dessous, dont les lignes sont données par les composantes des cup-produits $\Psi_{p_2^1} \cup \Psi_{p_1^1}$, $\Psi_{p_2^1} \cup \Psi_{p_1^2}$,$\Psi_{p_2^1} \cup \Psi_{p_2^2}$, $\Psi_{p_2^1} \cup \Psi_{p_3^1}$, $\Psi_{p_2^1} \cup \Psi_{p_3^2}$, $\Psi_{p_2^1} \cup \Psi_{p_4^1}$, $\Psi_{p_4^2} \cup \Psi_{p_1^1}$, $\Psi_{p_4^2} \cup \Psi_{p_1^2}$, $\Psi_{p_4^2} \cup \Psi_{p_2^2}$, $\Psi_{p_4^2} \cup \Psi_{p_3^1}$ $\Psi_{p_4^2} \cup \Psi_{p_3^2}$, et $\Psi_{p_4^2} \cup \Psi_{p_4^1}$ dans $\bigoplus_{v \in S'} H^2(\overline{H_v})$.

$$\begin{pmatrix}
2&0&1&0&0&0&0&0\\
0&2&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0\\
0&0&1&0&0&0&0&0\\
0&0&0&0&0&2&0&0\\
0&0&0&0&0&0&2&0\\
1&0&0&0&0&0&0&2\\
0&2&0&0&0&0&0&1\\
0&0&0&0&0&0&0&2\\
0&0&0&0&0&0&0&2\\
0&0&0&0&0&2&0&1\\
0&0&0&0&0&0&2&2
\end{pmatrix}$$

Cette matrice est de rang $7 < \#S'$, donc le groupe de cohomologie $H^1(H_S)$ ne vérifie pas les hypothèses du critère (LMS_f) pour cette décomposition.

De même, l'étude des autres cas revient au calcul du rang des matrices ci-dessous, qui sont elles aussi de rang strictement inférieur à 8. Finalement, aucune décomposition de $H^1(H_S)$ ne permet d'appliquer le critère (LMS_f), et L ne vérifie pas le critère de Labute-Minac-Schmidt en respectant S.

$$\begin{pmatrix}
2&0&0&0&0&0&0&0\\
0&2&0&1&0&0&0&0\\
0&0&1&1&0&0&0&0\\
0&0&0&0&1&0&0&0\\
0&0&0&2&0&0&0&0\\
0&0&0&0&0&0&0&2\\
2&0&0&0&0&0&1&0\\
0&2&0&0&0&0&1&0\\
0&0&0&0&0&0&2&0\\
0&0&0&0&2&0&1&0\\
0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&2&2
\end{pmatrix}
\quad
\begin{pmatrix}
0&0&0&0&0&0&0&0\\
0&2&0&0&0&0&0&0\\
0&2&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0\\
0&2&0&0&0&0&1&0\\
0&2&0&0&0&0&0&1\\
1&0&0&0&0&0&0&0\\
0&0&0&0&0&2&0&0\\
0&0&0&1&0&0&0&0\\
0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&0\\
0&0&0&0&0&2&0&1
\end{pmatrix}
\quad
\begin{pmatrix}
0&0&0&0&0&0&0&0\\
2&0&1&0&0&0&0&0\\
2&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0\\
2&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&2\\
0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0\\
0&0&0&0&2&0&0&0\\
0&0&0&0&1&1&0&0\\
0&0&0&0&2&0&1&0\\
0&0&0&0&0&0&0&1
\end{pmatrix}
\quad
\begin{pmatrix}
2&0&1&0&0&0&0&0\\
2&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0\\
2&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&2\\
0&2&0&0&0&0&0&0\\
0&2&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0\\
0&2&0&0&0&0&1&0\\
0&2&0&0&0&0&0&1
\end{pmatrix}$$

3.5.2. Comparaison avec les ensembles strictement circulaires de Labute. — Dans [**30**], Labute utilise une représentation sous forme de graphes pour démontrer une condition nécessaire pour qu'un pro-p groupe $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ soit *mild*. Les notions qu'il définit sont ensuite reprises par Vogel dans [**55**], où il étudie de manière analogue le cas d'un corps quadratique imaginaire. Cependant, les graphes utilisés ici et dans [**55**] sont définis différemment. On renvoie à [**55**] pour les notations dans ce qui suit.

Vogel construit à partir des *linking numbers* associés aux premiers de S' (cf def. 3.3.3) le graphe orienté $\Gamma(S)$ ayant pour sommets les premiers de S' dans lequel un arc $\mathfrak{q}_i\mathfrak{q}_j$ relie le premier $\mathfrak{q}_i$ au premier $\mathfrak{q}_j$ si $\ell_{ij} \neq 0$. Il définit alors la notion d'ensemble strictement circulaire de premiers.

Définition 3.5.3. — Un ensemble fini de premiers de L de normes congrues à 1 modulo p est dit strictement circulaire (par rapport à p) s'il existe un ordre $S' = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ sur les premiers de S' tel que les conditions suivantes soient vérifiées :

(1) Les sommets $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ de $\Gamma(S')$ forment un circuit $\mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_n\mathfrak{q}_1$.
(2) Si i et j sont deux indices impairs, alors $\mathfrak{q}_i\mathfrak{q}_j$ n'est pas une arête de $\Gamma(S')$.
(3) $\ell_{12}\ell_{23} \ldots \ell_{n-1,n}\ell_{n1} \neq \ell_{1n}\ell_{n,n-1} \ldots \ell_{32}\ell_{21}$.

Vogel montre alors le théorème suivant :

Théorème 3.5.4 **([55]).** — *Soit p un premier impair et* K *un corps de nombres quadratique imaginaire de p-groupe de classes trivial, différent de $\mathbb{Q}(\sqrt{-3})$ si $p = 3$. Soit $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ un ensemble de premiers de* K *de norme congrue à 1 modulo p. Si S est strictement circulaire (par rapport à p), alors* $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$ *est un pro-p groupe mild.*

Reprenons l'exemple 3.5.1 et montrons que l'ensemble S' considéré n'est pas strictement circulaire.

On note $S = \{61, 223, 229, 487\}$ et $S' = \{p_i^{(k)}, i = 1, \ldots, 4, k = 1, 2\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_8\}$ l'ensemble des premiers de $\mathrm{L} = \mathbb{Q}(\sqrt{-5})$ au dessus de S. On considère le cas $p = 3$, et on note $M = (m_{ij})$ la matrice associée au tableau suivant :

	p_1^1	p_1^2	p_2^1	p_2^2	p_3^1	p_3^2	p_4^1	p_4^2
$\mathfrak{q}_1 = p_1^1$	-1	0	1	1	0	1	1	1
$\mathfrak{q}_2 = p_1^2$	0	-1	1	1	1	0	1	1
$\mathfrak{q}_3 = p_2^1$	1	0	-1	1	1	0	0	0
$\mathfrak{q}_4 = p_2^2$	0	1	1	-1	0	1	0	0
$\mathfrak{q}_5 = p_3^1$	0	0	0	1	-1	1	1	0
$\mathfrak{q}_6 = p_3^2$	0	0	1	0	1	-1	0	1
$\mathfrak{q}_7 = p_4^1$	1	1	1	0	1	1	-1	1
$\mathfrak{q}_8 = p_4^2$	1	1	0	1	1	1	1	-1

où le coefficient à la i-ème ligne et j-ème colonne est -1,0 ou 1 suivant si le premier $p_j^{(k)}$ et ramifié, décomposé ou inerte dans $\mathrm{L}_{p_i^{(l)}}^{p,el}/\mathrm{L}$.

Remarquons que, par définition, le *linking number* ℓ_{ij} est non nul si et seulement si le premier $\mathfrak{q}_i$ est inerte dans l'extension $\mathrm{L}_{\mathfrak{q}_j}^{p,el}$. On en déduit que $\mathfrak{q}_i\mathfrak{q}_j$ est une arête du graphe $\Gamma(S')$ si et seulement si le coefficient m_{ji} est non nul.

Pour que l'ensemble S' soit strictement circulaire, il faut en particulier qu'il vérifie la deuxième condition de la définition 3.5.3, c'est-à-dire qu'aucune arête du graphe $\Gamma(S')$ ne doit relier deux premiers d'indices impairs (pour un certain réordonnement des $\mathfrak{q}_i$). Ici, cette condition implique que les quatre colonnes de M associées aux premiers d'indices impairs doivent contenir au moins trois 0. Les premiers d'indices impairs sont donc nécessairement p_1^1, p_1^2, p_4^1 et p_4^2. Or le coefficient m_{78} est non nul, donc une arête relie p_4^2 à p_4^1 et l'un de ces premiers ne peut pas être d'indice impair.

Finalement, quelque soit l'ordre des premiers de S', la deuxième condition de la définition 3.5.3 n'est pas vérifiée. L'ensemble S' n'est donc pas strictement circulaire.

CHAPITRE 4

SUR LES φ-COMPOSANTES DE LA STRUCTURE GALOISIENNE DE CERTAINES PRO-p-EXTENSIONS DE CORPS DE NOMBRES

La motivation de ce chapitre est encore l'étude de pro-p extensions à ramification restreinte, mais nous ne supposons plus que la ramification est modérée. On considère p un nombre premier impair, K/k une extension galoisienne finie de corps de nombres de groupe de Galois Δ d'ordre premier à p et S un ensemble fini de places de k contenant l'ensemble des places p-adiques S_p. Soit ensuite F/K une sous-extension de K_S/K obtenue par compositum avec le corps K d'une sous-extension L/k de k_S/k. Posons $\mathcal{H} = \mathrm{Gal}(\mathrm{K}_S/\mathrm{F})$ puis $\mathcal{G} = G_{K,S}$ et $G := \mathcal{G}/\mathcal{H}$. Alors le groupe Δ agit semi-simplement sur $\mathcal{X} = \mathcal{H}/[\mathcal{H},\mathcal{H}]$.

On se place dans un premier temps dans un cadre plus général où $\mathcal{G}$ est un pro-p groupe, $\mathcal{H}$ un sous-groupe normal fermé de $\mathcal{G}$ et Δ un sous-groupe fini du groupe des automorphismes (continus) de $\mathcal{G}$. Maire, dans [**38**], étudie la liberté du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}$. L'action de Δ nous permet de généraliser ici son travail en étudiant la liberté non plus du module $\mathcal{X}$ mais de chacune de ses φ-composantes $\mathcal{X}^{\varphi}$, où φ est un caractère $\mathbb{Q}_p$-irréductible de Δ. Sous la conjecture de Leopoldt et pour un caractère φ non trivial, on montre que la liberté du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^{\varphi}$ équivaut à la trivialité du module de torsion $\mathrm{Tor}_{\mathbb{Z}_p}\big(\mathcal{G}^{ab}\big)^{\varphi}$.

Nous appliquerons ce théorème à plusieurs situations arithmétiques, et en particulier au contexte galoisien exposé plus haut. Le groupe fini $\mathrm{Tor}_{\mathbb{Z}_p}\big(G_{K,S_p}^{ab}\big)$ se ramène, via la théorie du corps de classes et sous de bonnes hypothèses, à un quotient des unités p-adiques par les unités globales. Dans un cadre adapté, la trivialité de $\mathrm{Tor}_{\mathbb{Z}_p}\big(G_{K,S_p}^{ab}\big)^{\varphi}$ équivaut à une condition de congruence modulo p, idéale pour les expérimentations numériques : nous finirons par une étude statistique dans des extensions cubiques cycliques, diédrales et cycliques totalement réelles de degré 4. Les situations pour lesquelles le module $\mathcal{X}^{\varphi}$ n'est pas libre sont très rares et confortent la conjecture de Gras selon laquelle le corps de nombres K est p-rationnel pour p suffisamment grand.

L'ensemble des calculs ont été effectués à l'aide du logiciel PARI/GP [**54**].

Notations

• Si M désigne un $\mathbb{Z}_p$-module de type fini, nous notons par

– $\mathrm{rg}_{\mathbb{Z}_p}M$ le $\mathbb{Z}_p$-rang de M, *i.e* la dimension sur $\mathbb{Q}_p$ de $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$;
– $\mathrm{Tor}_{\mathbb{Z}_p}M := \{x \in M,\ \exists p^k,\ p^k x = 0\}$, le sous-module de torsion de M ;
– $M[p] = \{x \in M,\ px = 0\}$, les éléments de p-torsion de M ;
– $d_p M$ le nombre minimal de générateurs de M, *i.e.* la dimension sur $\mathbb{F}_p$ de $\mathbb{F}_p \otimes_{\mathbb{Z}_p} M$.

Si de plus M est muni d'une action d'un groupe fini Δ, nous notons par

– $M^{\Delta} := \{x \in M,\ \sigma \cdot x = x,\ \forall \sigma \in \Delta\}$ le sous-groupe des invariants de M sous l'action de Δ ;
– $M_{\Delta} := M/I_{\Delta}M$ les coinvariants de M sous l'action de Δ, ici $I_{\Delta} = \langle \sigma - 1, \sigma \in \Delta \rangle$ est l'idéal d'augmentation de l'algèbre $\mathbb{Z}_p[\Delta]$. Ainsi, M_{Δ} est le plus grand quotient de M sur lequel Δ agit trivialement.

On étend ces deux dernières notations au cas où Δ est profini avec action continue de Δ.

• Si Δ est d'ordre premier à p, nous sommes dans le cas "semi-simple" : l'algèbre $\mathbb{Z}_p[\Delta]$ est munie d'un système fondamental d'idempotents orthogonaux $(e_\varphi)_\varphi$, φ parcourant l'ensemble des caractères $\mathbb{Q}_p$-irréductibles $\mathrm{Irr}(\Delta, \mathbb{Q}_p)$ de Δ. On rappelle que $e_\varphi = \frac{\psi(1)}{|\Delta|} \sum_{s\in\Delta} \varphi(s)s^{-1}$, où ψ désigne un caractère $\mathbb{C}_p$-irréductible divisant φ. Ainsi, si φ désigne un caractère $\mathbb{Q}_p$-irréductible de Δ, nous notons par $M^\varphi := e_\varphi M$ la φ-composante de M.

Grâce au système d'idempotents orthogonaux, on a donc $M = \bigoplus_{\varphi\in\mathrm{Irr}(\Delta,\mathbb{Q}_p)} M^\varphi$, et ainsi la projection sur les φ-composantes conserve les suites exactes.

Lorsque M est de plus $\mathbb{Z}_p$-libre, on identifie le caractère de $\mathbb{Q}_p \otimes M$, à valeurs dans $\mathbb{Q}_p$, avec celui de $M/M^p := \mathbb{F}_p \otimes M$, à valeurs dans $\mathbb{F}_p$. On rappelle que dans ce cas le $\mathbb{Z}_p[\Delta]$-module M est projectif.

On note par $\mathbb{1}$ le caractère trivial, *i.e.* le caractère de la représentation triviale (c'est-à-dire le caractère du module $M = \mathbb{Z}_p$) et par Rg le caractère de la représentation régulière (c'est-à-dire le caractère du module $M = \mathbb{Z}_p[\Delta]$). Posons alors $\mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p) = \mathrm{Irr}(\Delta, \mathbb{Q}_p)\backslash\{\mathbb{1}\}$, l'ensemble des caractères $\mathbb{Q}_p$-irréductibles et non-triviaux de Δ.

Notons enfin que $M^\Delta = M^{\mathbb{1}}$, et la décomposition de M suivant les caractères irréductibles nous indique que $M^\Delta = \{0\}$ si et seulement si $M_\Delta = \{0\}$.

Pour plus de détails, voir par exemple [**51**], [**7**], etc.

• Si $\mathcal{G}$ désigne un pro-p-groupe de type fini et Δ un sous-groupe du groupe des automorphismes (continus) de $\mathcal{G}$, on note par $\mathcal{G}_\Delta$ le plus grand quotient de $\mathcal{G}$ sur lequel Δ agit trivialement et par $\mathcal{H}(\Delta)$ le sous-groupe normal fermé associé : $\mathcal{G}/\mathcal{H}(\Delta) = \mathcal{G}_\Delta$.

• Si G désigne un pro-p-groupe, on note par $[G, G]$ le sous-groupe fermé normal de G engendré par ses commutateurs, par G^{ab} le quotient $G/[G, G]$, puis par $G^{ab,p}$ le quotient $G/G^p[G, G]$, où ici G^p désigne le sous-groupe de G engendré par les puissances p-èmes.

• Si K/$\mathbb{Q}$ désigne un corps de nombres, on note par

- $\mathcal{O}_\mathrm{K}$ son anneau des entiers,
- $E_\mathrm{K} := \mathcal{O}_\mathrm{K}^\times$ le groupe des unités de K,
- Cl(K) le groupe des classes de K,
- S_p l'ensemble des places de K au-dessus de p (auxquelles on ajoute les places infinies quand $p = 2$).

• Si K/k désigne une extension de corps de nombres et S $(= S_\mathrm{k})$ un ensemble de places de k, nous notons également par S $(= S_\mathrm{K})$ l'ensemble des places de K au-dessus de celles de S_k.

• Si K désigne un corps (de nombres ou local) et si p désigne un nombre premier, on note par

- $\mu_{p^\infty}(\mathrm{K})$ le groupe des racines de l'unité d'ordre une puissance de p contenues dans K (éventuellement trivial),
- $\mu_p(\mathrm{K})$ les racines de l'unité d'ordre divisant p contenues dans K,
- $\mu_{p^\infty} := \mu_{p^\infty}(\overline{\mathrm{K}})$ et $\mu_p := \mu_p(\overline{\mathrm{K}})$, où ici $\overline{\mathrm{K}}$ est une clôture algébrique de K fixée dès le début.

4.1. Quelques précisions algébriques

Une bonne référence pour une partie des résultats présentés dans cette section est le livre de Neukirch, Schmidt et Wingberg [**42**, Part "Algebraic Theory"].

4.1.1. Le contexte algébrique. — Soit p un nombre premier ; posons suivant le contexte $\Omega = \mathbb{F}_p$ ou $\mathbb{Z}_p$.

4.1.1.1. — Soit G un pro-p-groupe de type fini. On considère l'algèbre d'Iwasawa complète

$$\Omega[\![G]\!] = \varprojlim_U \Omega[G/U],$$

où la limite projective est prise sur les sous-groupes ouverts normaux U de G. Notons I_G l'idéal d'augmentation de $\Omega[\![G]\!]$, c'est le noyau du morphisme naturel de réduction :

$$I_G = \ker\left(\Omega[\![G]\!] \twoheadrightarrow \Omega\right).$$

L'algèbre $\Omega[\![G]\!]$ est un anneau local d'idéal maximal $\mathfrak{M}_G := p\Omega[\![G]\!] + I_G$ pour laquelle il vient $\Omega[\![G]\!]/\mathfrak{M}_G \simeq \mathbb{F}_p$.

4.1.1.2. — Soient $\mathcal{G}$ un pro-p-groupe de type fini, $\mathcal{H}$ un sous-groupe fermé normal de $\mathcal{G}$ et le quotient $G := \mathcal{G}/\mathcal{H}$. Posons

$$\mathcal{X} := \mathcal{H}^{ab} = \mathcal{H}/[\mathcal{H},\mathcal{H}] \quad \text{et} \quad \mathcal{Y} = \mathcal{X}/\mathcal{X}^p.$$

Proposition 4.1.1. — *Le pro-p-groupe abélien $\mathcal{X}$ (resp. $\mathcal{Y}$) est naturellement muni d'une structure de $\mathbb{Z}_p[\![G]\!]$-module (resp. de $\mathbb{F}_p[\![G]\!]$-module) d'action continue pour les topologies naturelles sous-jacentes (issues des limites projectives).*

Pour la suite quand on parlera des $\Omega[\![G]\!]$-modules $\mathcal{X}$ et $\mathcal{Y}$, il faudra comprendre $\Omega = \mathbb{Z}_p$ pour $\mathcal{X}$ et $\Omega = \mathbb{F}_p$ pour $\mathcal{Y}$.

Par le lemme de Nakayama topologique (voir par exemple [**42**, chap. V, §2]), les $\Omega[\![G]\!]$-modules $\mathcal{X}$ et $\mathcal{Y}$ sont de type fini si et seulement si le $\mathbb{F}_p$-module $\mathcal{Y}/\mathfrak{M}_G$ l'est.

L'étude de la suite exacte

$$1 \longrightarrow \mathcal{H} \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1$$

apporte le lemme suivant :

Lemme 4.1.2. — *Si l'on suppose finis les groupes de cohomologie $H^2(\mathcal{G},\mathbb{F}_p)$ et $H^1(\mathcal{G},\mathbb{F}_p)$, alors les $\Omega[\![G]\!]$-modules $\mathcal{X}$ et $\mathcal{Y}$ sont de type fini.*

Dans nos contextes arithmétiques, les groupes $\mathcal{G}$ en jeu sont bien de présentation finie. Nous reviendrons rapidement sur ce fait par la suite.

4.1.2. Action semi-simple. — À présent, on se donne un sous-groupe fini Δ du groupe des automorphismes (continus) de $\mathcal{G}$, d'ordre premier à p. À ce niveau, nous suivons [**56**]. Soit le produit semi-direct $\Gamma := \Delta \ltimes \mathcal{G}$ induit par l'action de Δ sur $\mathcal{G}$. Notons par $\mathcal{G}_\Delta$ le plus grand quotient de $\mathcal{G}$ sur lequel Δ agit trivialement. Ce quotient est bien défini. Avant d'énoncer un résultat de Wingberg, rappelons que si M désigne un Δ-module, nous notons par M^Δ le sous-module de M constitué des points fixes sous l'action de Δ. Si M est un $\mathbb{F}_p[\Delta]$-module de type fini, alors $M^\Delta = M^{\mathbb{1}}$ est la composante isotypique de M associée au caractère trivial $\mathbb{1}$.

Proposition 4.1.3 **(Wingberg, [56]).** — *On a $\mathcal{G}_\Delta \simeq \Gamma(p)$, où $\Gamma(p)$ est le pro-p-quotient maximal de Γ. De plus, $H^1(\mathcal{G}_\Delta,\mathbb{F}_p) \simeq H^1(\mathcal{G})^\Delta$ et $H^2(\mathcal{G}_\Delta,\mathbb{F}_p) \hookrightarrow H^2(\mathcal{G},\mathbb{F}_p)^\Delta$.*

Ce résultat permet de donner des situations où $\mathcal{G}_\Delta$ est pro-p-libre, nous y reviendrons plus tard. Wingberg obtient même un peu plus lorsque le pro-p-groupe $\mathcal{G}$ est de Demushkin (pour un rappel sur les groupes de Demushkin voir par exemple [**42**, chap. III, §9].

Proposition 4.1.4 **(Wingberg, [56]).** — *Supposons $\mathcal{G}$ de Demushkin de rang $n+2$, $n \geqslant 0$. Alors $H^2(\mathcal{G}_\Delta,\mathbb{F}_p) \simeq H^2(\mathcal{G},\mathbb{F}_p)^\Delta$. En particulier si $H^2(\mathcal{G},\mathbb{F}_p)^\Delta = 0$ alors $\mathcal{G}_\Delta$ est pro-p-libre (de rang $\frac{n}{2}+1$ lorsque Δ est d'ordre 2). Par contre, dans le cas contraire, c'est-à-dire si $H^2(\mathcal{G},\mathbb{F}_p)^\Delta$ n'est pas trivial, le quotient $\mathcal{G}_\Delta$ est également de Demushkin.*

Posons $\mathcal{H}(\Delta)$ le sous-groupe normal de $\mathcal{G}$ tel que $\mathcal{G}/\mathcal{H}(\Delta) = \mathcal{G}_\Delta$ et revenons au contexte du début de cette section.

Pour toute la suite, on choisit $\mathcal{H}$ contenant $\mathcal{H}(\Delta)$ pour la raison suivante : le groupe Δ agit trivialement sur le quotient $\mathcal{G}_\Delta \twoheadrightarrow \mathcal{G}/\mathcal{H} := G$.

Ainsi comme G et Δ commutent, il vient $\Omega[\![G\times\Delta]\!]\simeq\Omega[\![G]\!][\Delta]$. Les actions de $\Omega[\Delta]$ et $\Omega[\![G]\!]$ sur $\mathcal{X}$ (resp. sur $\mathcal{Y}$) commutent et $\mathcal{X}$ (resp. $\mathcal{Y}$) a de fait une structure de $(\Omega[\![G]\!],\Omega[\Delta])$-bimodule, ce qui peut être assemblé dans la proposition suivante :

Proposition 4.1.5. — *Supposons $\mathcal{X}$ de type fini sur $\mathbb{Z}_p[\![G]\!]$. L'anneau $\mathbb{Z}_p[\Delta]$ agit sur $\mathcal{X}$ et les φ-composantes $\mathcal{X}^\varphi$ du $\mathbb{Z}_p[\Delta]$-module $\mathcal{X}$ sont des $\mathbb{Z}_p[\![G]\!]$-modules. En particulier $\mathcal{X}^\varphi$ est de type fini sur $\mathbb{Z}_p[\![G]\!]$. Il en est de même pour $\mathcal{Y}$.*

Démonstration. — Comme les actions de G et Δ commutent, on a pour tout $g\in G$: $ge_\varphi=e_\varphi g$. Par conséquent,

$$g\cdot(\mathcal{X}^\varphi)=g\cdot(e_\varphi\mathcal{X})=e_\varphi(g\cdot\mathcal{X})\subset\mathcal{X}^\varphi,$$

c'est-à-dire que G agit bien sur la φ-composante $\mathcal{X}^\varphi$ de $\mathcal{X}$.

De plus, comme on est dans le cas semi-simple, il vient la décomposition $\mathcal{X}=\bigoplus_\varphi\mathcal{X}^\varphi$, et donc $\mathcal{X}^\varphi\simeq\mathcal{X}/(\bigoplus_{\chi\neq\varphi}\mathcal{X}^\chi)$, le tout étant un isomorphisme de $\mathbb{Z}_p[\![G]\!][\Delta]$-modules. Si l'on suppose que $\mathcal{X}$ est de type fini comme $\mathbb{Z}_p[\![G]\!]$-module, tous ses quotients le sont et en particulier les $\mathcal{X}^\varphi$. L'assertion sur $\mathcal{Y}^\varphi$ se montre de la même façon. □

Traitons le caractère trivial.

Proposition 4.1.6. — *Pour $\mathcal{H}=\mathcal{H}(\Delta)$, il vient $\mathcal{X}^{\mathbb{1}}=\{1\}$.*

Démonstration. — En effet, supposons que $\mathcal{X}^{\mathbb{1}}$ n'est pas trivial. Alors il existe un sous-groupe normal $\mathcal{H}_0$ de $\mathcal{G}$, sous-groupe strict de $\mathcal{H}(\Delta)$, tel que Δ agisse trivialement sur le quotient $G':=\mathcal{H}(\Delta)/\mathcal{H}_0$ (on peut par exemple s'assurer que $|G'|=p$) : cela repose sur le fait que le pro-p-groupe $\mathcal{G}_\Delta$ agit sur le pro-p-groupe $\mathcal{X}^{\mathbb{1}}$. Posons $G=\mathcal{G}/\mathcal{H}_0$. Regardons l'action de Δ sur G. Soit $\sigma\in\Delta$ d'ordre $n\neq1$ premier à p, et soit $g\in G$. Alors $\sigma(g)=gh$ avec $h\in G'$. Or $\sigma(h)=h$. Ainsi $g=\sigma^n(g)=gh^n$ et par conséquent $h^n=1$. Comme G' est un p-groupe, il vient que $h=1$ et donc $\sigma(g)=g$. On vient ainsi de montrer que le groupe Δ agit trivialement sur un quotient de $\mathcal{G}$ contenant strictement $\mathcal{G}_\Delta$, ce qui contredit la maximalité de $\mathcal{G}_\Delta$. □

Terminons ce paragraphe par une première réduction possible quand $\varphi\in\mathrm{Irr}^\bullet(\Delta,\mathbb{Q}_p)$. En effet, quand φ est différent du caractère trivial $\mathbb{1}$, le résultat suivant nous montre que l'étude de la φ-composante $\mathcal{X}^\varphi$ est réduite à la situation où $G=\mathcal{G}_\Delta$. Cela ne sera pas du tout le cas pour le caractère trivial $\varphi=\mathbb{1}$. Conservons le contexte de la section 4.1.2

Proposition 4.1.7. — *Soient $\mathcal{H}_1\subset\mathcal{H}_2$ deux sous-groupes normaux fermés de $\mathcal{G}$ contenant $\mathcal{H}(\Delta)$. Pour $i=1,2$, soient les quotients $G_i=\mathcal{G}/\mathcal{H}_i$. Posons $\mathcal{X}_i=\mathcal{H}_i^{ab}$ puis $H:=\mathcal{H}_2/\mathcal{H}_1$. Alors pour tout caractère $\varphi\in\mathrm{Irr}^\bullet(\Delta,\mathbb{Q}_p)$, il vient l'isomorphisme de $\mathbb{Z}_p[\![G_2]\!]$-module : $\mathcal{X}_{1,H}^\varphi\simeq\mathcal{X}_2^\varphi$. En particulier, si $\mathcal{X}_1^\varphi$ est $\mathbb{Z}_p[\![G_1]\!]$-libre, il en est de même pour $\mathcal{X}_2^\varphi$ en tant que $\mathbb{Z}_p[\![G_2]\!]$-module.*

Démonstration. — On part de la suite exacte $1\longrightarrow\mathcal{H}_1\longrightarrow\mathcal{H}_2\longrightarrow H\longrightarrow1$ qui devient

$$\cdots\longrightarrow H_1(H,\mathbb{Z}_p)\longrightarrow\mathcal{X}_{1,H}\longrightarrow\mathcal{X}_2\longrightarrow H^{ab}\longrightarrow1.$$

Il suffit ensuite de prendre les φ-composantes et d'utiliser le fait que Δ agit trivialement sur le quotient H et donc aussi sur $H_1(H,\mathbb{Z}_p)$ et sur H^{ab}. □

4.1.3. Suite spectrale à sept termes. — Le point de départ algébrique est la suite exacte à sept termes du lemme 2.2.9, également point de départ de **[38]**, dont une preuve est donnée dans le chapitre 2.

Lemme. — *Soit $\mathcal{G}$ un pro-p groupe et soit $\mathcal{H}$ un sous-groupe de $\mathcal{G}$, distingué et fermé. On note G le quotient de $\mathcal{G}$ par $\mathcal{H}$ et on suppose que le groupe de cohomologie $H^2(\mathcal{H},\mathbb{Q}_p/\mathbb{Z}_p)$ est trivial. Alors on a la suite exacte d'homologie :*

$$(2)\qquad H_3(G,\mathbb{Z}_p)\longrightarrow H_1(G,\mathcal{H}^{ab})\longrightarrow H_2(\mathcal{G},\mathbb{Z}_p)\longrightarrow H_2(G,\mathbb{Z}_p)\longrightarrow\mathcal{H}_G^{ab}\longrightarrow\mathcal{G}^{ab}\twoheadrightarrow G^{ab}.$$

La nouveauté ici consiste à regarder cette suite exacte dans le contexte d'une action semi-simple Δ, en supposant que $\mathcal{H}(\Delta)\subset\mathcal{H}$. Rappelons que l'on note le quotient $G:=\mathcal{G}/\mathcal{H}$.

Proposition 4.1.8. — *Conservons le contexte de la section 4.1.2 et supposons $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p)$ et $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$ triviaux. Alors la suite exacte à sept termes (2) est également une suite exacte de $\mathbb{Z}_p[\Delta]$-modules.*

Démonstration. — La preuve est inspirée de [**42**, chap 1, §6, exercice 3].

La suite spectrale de Hochschild-Serre donne la suite exacte à sept termes (2) qui, sous l'hypothèse $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, se scinde en deux suites exactes (après passage au dual) :

$$H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \hookrightarrow H^1(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)^G \twoheadrightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p), \tag{3}$$

$$H^1(G, H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)) \hookrightarrow H^3(G, \mathbb{Q}_p/\mathbb{Z}_p). \tag{4}$$

Rappelons maintenant le fait cohomologique suivant. Si Γ désigne un groupe profini et H un sous-groupe fermé de Γ, alors pour tout H-sous-module B d'un Γ-module A et pour $\sigma \in \Gamma$, il vient, pour chaque $n \geqslant 1$, l'isomorphisme $\sigma_* : H^n(H, B) \to H^n(\sigma \cdot H, \sigma B)$, qu'on appellera encore conjugaison (voir [**42**, chap. I, §5]). On renvoie également à [**42**, chap. I, §5 et §6] pour les définitions des morphismes d'inflation, de restriction et de transgression.

Utilisant ce rappel dans notre contexte, on note alors que le groupe Δ agit sur chacun des termes des suites exactes (3) et (4).

D'après [**42**, prop. 1.5.4], la conjugaison σ_* commute avec les applications inflation et restriction, donc avec les deux premiers morphismes de la suite exacte (3). Pour montrer que la suite exacte (3) est une suite exacte de $\mathbb{Z}_p[\Delta]$-modules, il reste à prouver que σ_* commute également avec la transgression

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

Ceci qui prouvera également que Δ commute avec le morphisme de la suite exacte (4).

Soit A un $\mathcal{G}$-module (discret). On définit le $\mathcal{G}$-module A_1 par la suite exacte

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}_{\mathcal{G}}(A) \longrightarrow A_1 \longrightarrow 0\ ,$$

où $\mathrm{Ind}_{\mathcal{G}}(A)$ est le module induit de A : c'est l'ensemble des fonctions continues de $\mathcal{G}$ vers A muni d'une action naturelle de $\mathcal{G}$. On a alors la suite exacte longue de cohomologie

$$0 \longrightarrow A^{\mathcal{H}} \longrightarrow \mathrm{Ind}_G(A)^{\mathcal{H}} \longrightarrow A_1^{\mathcal{H}} \longrightarrow H^1(\mathcal{H}, A) \longrightarrow H^1(\mathcal{H}, \mathrm{Ind}_{\mathcal{G}}(A)) \longrightarrow \dots$$

Mais $\mathrm{Ind}_{\mathcal{G}}(A)$ est également un $\mathcal{H}$-module induit donc le groupe de cohomologie $H^1(\mathcal{H}, \mathrm{Ind}_{\mathcal{G}}(A))$ est trivial ([**42**, 1.3.6 et 1.3.7]). On a donc en fait une suite exacte à quatre termes qu'on coupe en deux en notant B l'image de $\mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}}$ dans $A_1^{\mathcal{H}}$:

$$0 \longrightarrow A^{\mathcal{H}} \longrightarrow \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}} \longrightarrow B \longrightarrow 0\ , \tag{5}$$

$$0 \longrightarrow B \longrightarrow A_1^{\mathcal{H}} \longrightarrow H^1(\mathcal{H}, A) \longrightarrow 0\ . \tag{6}$$

Soit maintenant un rang $n \geqslant 1$. La suite exacte (5) donne

$$H^n(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}}) \longrightarrow H^n(\mathcal{G}, B) \longrightarrow H^{n+1}(\mathcal{G}, A^{\mathcal{H}}) \longrightarrow H^{n+1}(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}})$$

où les termes $H^n(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}})$ et $H^{n+1}(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}})$ sont triviaux puisque $\mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}}$ est un $\mathcal{G}$-module induit. Finalement le δ-morphisme de connexion

$$\delta' :\ H^n(\mathcal{G}, B) \longrightarrow H^{n+1}(\mathcal{G}, A^{\mathcal{H}})$$

est un isomorphisme. Sa composée avec le δ-morphisme

$$\delta'' :\ H^{n-1}(\mathcal{G}, H^1(\mathcal{H}, A)) \longrightarrow H^n(\mathcal{G}, B)$$

obtenu à partir de la suite exacte (6) est, d'après [**42**, chap. II, §4, exercice 3], le morphisme $d_2^{n-1,1}$ associé à la suite spectrale de Hochschild-Serre. Comme la conjugaison σ_* commute avec les δ-morphismes de

connexion, elle commute avec les morphismes $d_2^{n-1,1}$ pour tout $n \geqslant 1$ et donc en particulier avec la transgression. □

Comme Δ est d'ordre premier à p, on peut projeter les termes de la suite exacte du lemme 2.2.9 sur leurs φ-composantes : si φ est un caractère $\mathbb{Q}_p$-irréductible de Δ, on a la suite exacte suivante (sous la condition $H_2(\mathcal{G}, \mathbb{Z}_p) = H_2(\mathcal{H}, \mathbb{Z}_p) = 0$) :

$$H_3(G,\mathbb{Z}_p)^\varphi \longrightarrow H_1(G,\mathcal{X})^\varphi \longrightarrow 0 \longrightarrow H_2(G,\mathbb{Z}_p)^\varphi \longrightarrow (\mathcal{X}_G)^\varphi \longrightarrow (\mathcal{G}^{ab})^\varphi \twoheadrightarrow (G^{ab})^\varphi. \tag{7}$$

4.1.4. Liberté des φ-composantes. —

4.1.4.1. *Résultats préparatoires.* — Fixons $\mathcal{X}$ un $\mathbb{Z}_p[\![G]\!][\Delta]$-module de type fini.

La proposition suivante va être d'une grande importance.

Proposition 4.1.9. — *Pour tout caractère irréductible φ de Δ, on a l'isomorphisme de Δ-modules : $H_1(G, \mathcal{X}^\varphi) \simeq H_1(G, \mathcal{X})^\varphi$.*

Démonstration. — Commençons par le lemme suivant :

Lemme 4.1.10. — *Sous les conditions précédentes, on a l'isomorphisme de Δ-modules : $(\mathcal{X}_G)^\varphi \simeq (\mathcal{X}^\varphi)_G$. On notera par $\mathcal{X}_G^\varphi$ ce Δ-module.*

Démonstration. — La preuve est immédiate, elle repose sur le fait que les actions de G et de Δ commutent. □

Soit une présentation minimale du $\mathbb{Z}_p[\![G \times \Delta]\!]$-module $\mathcal{X}$:

$$1 \longrightarrow R \longrightarrow F \longrightarrow \mathcal{X} \longrightarrow 1, \tag{8}$$

où $F \simeq \mathbb{Z}_p[\![G \times \Delta]\!]^r$.

Pour φ un caractère irréductible de Δ, on peut alors projeter la présentation de $\mathcal{X}$ sur les φ-composantes et on obtient une présentation du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^\varphi$:

$$1 \longrightarrow R^\varphi \longrightarrow F^\varphi \longrightarrow \mathcal{X}^\varphi \longrightarrow 1\ , \tag{9}$$

où ici F^φ est $\mathbb{Z}_p[\![G]\!]$-libre car en effet :

Lemme 4.1.11. — *Le $\mathbb{Z}_p[\![G]\!]$-module F^φ est libre. En particulier, $H_i(G, F^\varphi) = 0$ pour tout $i \geqslant 1$.*

Démonstration. — Comme $\mathbb{Z}_p[\![G \times \Delta]\!] \simeq \mathbb{Z}_p[\![G]\!][\Delta]$, il vient que $\mathbb{Z}_p[\![G \times \Delta]\!]$ est $\mathbb{Z}_p[\![G]\!]$-libre, et donc que F est $\mathbb{Z}_p[\![G]\!]$-libre. De plus, on a la somme directe de $\mathbb{Z}_p[\Delta]$-modules : $F = \oplus_{\varphi \in \mathrm{Irr}(\Delta, \mathbb{Q}_p)} F^\varphi$, où la somme directe est prise sur les caractères $\mathbb{Q}_p$-irréductibles de Δ. Les φ-composantes étant des bimodules, ce sont en particulier des $\mathbb{Z}_p[\![G]\!]$-modules et la somme directe reste valable pour la structure de $\mathbb{Z}_p[\![G]\!]$-module. Finalement, F^φ est un facteur direct du $\mathbb{Z}_p[\![G]\!]$-module libre F, c'est donc un $\mathbb{Z}_p[\![G]\!]$-module projectif, c'est-à-dire libre car $\mathbb{Z}_p[\![G]\!]$ est un anneau local. □

La suite exacte (9) donne la suite exacte longue d'homologie :

$$1 \longrightarrow H_1(G,\mathcal{X}^\varphi) \longrightarrow \underbrace{H_0(G,R^\varphi)}_{(R^\varphi)_G} \longrightarrow \underbrace{H_0(G,F^\varphi)}_{(F^\varphi)_G} \longrightarrow \underbrace{H_0(G,\mathcal{X}^\varphi)}_{(\mathcal{X}^\varphi)_G} \longrightarrow 1. \tag{10}$$

D'autre part, la présentation minimale (8) de $\mathcal{X}$ donne la suite exacte d'homologie :

$$1 \longrightarrow H_1(G,\mathcal{X}) \longrightarrow H_0(G,R) \longrightarrow H_0(G,F) \longrightarrow H_0(G,\mathcal{X}) \longrightarrow 1.$$

Comme Δ agit sur les groupes G, $\mathcal{X}$, R et F, Δ agit sur tous les termes de cette suite exacte. On projette sur les φ-composantes pour obtenir :

$$1 \longrightarrow H_1(G,\mathcal{X})^\varphi \longrightarrow \underbrace{H_0(G,R)^\varphi}_{(R_G)^\varphi} \longrightarrow \underbrace{H_0(G,F)^\varphi}_{(F_G)^\varphi} \longrightarrow \underbrace{H_0(G,\mathcal{X})^\varphi}_{(\mathcal{X}_G)^\varphi} \longrightarrow 1. \tag{11}$$

Mais d'après le lemme 4.1.10, on a $(R_G)^\varphi = (R^\varphi)_G = R_G^\varphi$, $(F_G)^\varphi = (F^\varphi)_G = F_G^\varphi$ et $(\mathcal{X}_G)^\varphi = (\mathcal{X}^\varphi)_G = \mathcal{X}_G^\varphi$. Le résultat se déduit des suites exactes (10) et (11). □

Corollaire 4.1.12. — *La φ-composante $\mathcal{X}^\varphi$ de $\mathcal{X}$ est $\mathbb{Z}_p[\![G]\!]$-libre si et seulement si les deux conditions suivantes sont satisfaites :*

(i) *$H_1(G,\mathcal{X})^\varphi$ est trivial ;*
(ii) *$\mathcal{X}_G^\varphi$ est $\mathbb{Z}_p$-libre.*

Démonstration. — Soit une présentation minimale du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^\varphi$:

$$1 \longrightarrow \tilde{R} \longrightarrow \tilde{F} \longrightarrow \mathcal{X}^\varphi \longrightarrow 1,$$

où $\tilde{F} = \mathbb{Z}_p[\![G]\!]^t$ avec $t = d_p\mathcal{X}_G^\varphi$.

Le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^\varphi$ est libre si et seulement si le $\mathbb{Z}_p[\![G]\!]$-module $\tilde{R}$ est trivial. Par le lemme de Nakayama c'est équivalent à la trivialité du $\mathbb{F}_p$-module $\tilde{R}_G/p$. La présentation minimale de $\mathcal{X}^\varphi$ donne la suite exacte longue d'homologie :

$$1 \longrightarrow H_1(G,\mathcal{X}^\varphi) \longrightarrow \underbrace{H_0(G,\tilde{R})}_{\tilde{R}_G} \longrightarrow \underbrace{H_0(G,\tilde{F})}_{\tilde{F}_G} \longrightarrow \underbrace{H_0(G,\mathcal{X}^\varphi)}_{\mathcal{X}_G^\varphi} \longrightarrow 1.$$

Le module $\tilde{R}_G/p$ est donc trivial si et seulement si le module $H_1(G,\mathcal{X}^\varphi)$ est trivial et $\mathcal{X}_G^\varphi$ est $\mathbb{Z}_p$-libre. □

4.1.4.2. *Un premier résultat et quelques conséquences.* — Nous sommes en mesure d'énoncer une extension du résultat de [**38**] (voir aussi [**42**, chap. V, §6]) :

Théorème 4.1.13. — *Soit φ un caractère $\mathbb{Q}_p$-irréductible de Δ et soit $\mathcal{H}$ un sous-groupe normal de $\mathcal{G}$ contenant $\mathcal{H}(\Delta)$. Supposons :*

(i) *$H_2(\mathcal{H},\mathbb{Z}_p) = 0$,*
(ii) *$H_2(\mathcal{G},\mathbb{Z}_p) = 0$.*

Si le caractère φ n'est pas trivial, alors le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^\varphi$ est libre si et seulement si le groupe $(\mathcal{G}^{ab})^\varphi$ est sans $\mathbb{Z}_p$-torsion. Si tel est le cas, le rang de $\mathcal{X}^\varphi$ est égal à

$$d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^\varphi.$$

Si $\varphi = \mathbb{1}$ et si G est de dimension cohomologique $cd(G)$ inférieure à 2, alors $\mathcal{X}^{\mathbb{1}}$ est $\mathbb{Z}_p[\![G]\!]$-libre lorsque le morphisme $\mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}} \to G^{ab}$ est injectif. Si tel est le cas, le rang de $\mathcal{X}^{\mathbb{1}}$ est égal à

$$d_{\mathbb{1}} = d_pH_2(G,\mathbb{F}_p) - d_pG + \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}}.$$

Démonstration. — Soit φ un caractère irréductible de Δ. Reprenons la suite exacte (7) :

$$H_3(G,\mathbb{Z}_p)^\varphi \longrightarrow H_1(G,\mathcal{X})^\varphi \longrightarrow 0 \longrightarrow H_2(G,\mathbb{Z}_p)^\varphi \longrightarrow (\mathcal{X}_G)^\varphi \tag{12}$$
$$\downarrow$$
$$(G^{ab})^\varphi \twoheadleftarrow (\mathcal{G}^{ab})^\varphi$$

Supposons que le caractère φ ne soit pas trivial. Par hypothèse (c'est-à-dire par le choix de $\mathcal{H}$), le groupe Δ agit trivialement sur G. En particulier, les modules $H_3(G,\mathbb{Z}_p)^\varphi$, $H_2(G,\mathbb{Z}_p)^\varphi$ et $(G^{ab})^\varphi$ sont triviaux. La suite exacte (12) implique donc

$$H_1(G,\mathcal{X})^\varphi = 0 \quad \text{et} \quad \mathcal{X}_G^\varphi \simeq (\mathcal{G}^{ab})^\varphi.$$

Ainsi le $\mathbb{Z}_p$-module $\mathcal{X}_G^\varphi$ est sans torsion si et seulement si $(\mathcal{G}^{ab})^\varphi$ est sans $\mathbb{Z}_p$-torsion. On peut alors conclure grâce au corollaire 4.1.12.

Supposons maintenant que φ est égal au caractère trivial $\mathbb{1}$. Sous l'hypothèse $cd(G) \leqslant 2$, le groupe $H_3(G,\mathbb{Z}_p)$ est trivial et il en est de même du groupe $H_1(G,\mathcal{X})^{\mathbb{1}}$. La suite exacte (12) devient :

$$0 \longrightarrow H_2(G,\mathbb{Z}_p) \longrightarrow \mathcal{X}_G^{\mathbb{1}} \longrightarrow (\mathcal{G}^{ab})^{\mathbb{1}} \longrightarrow (G^{ab})^{\mathbb{1}} \longrightarrow 0$$

dont on déduit que le $\mathbb{Z}_p$-module $\mathcal{X}_G^{\mathbb{1}}$ est sans torsion si et seulement si le morphisme $\mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}} \to (G^{ab})^{\mathbb{1}}$ est injectif (car $H_2(G,\mathbb{Z}_p)$ est sans torsion), et on peut conclure grâce à la proposition 4.1.12. Les calculs sont ensuite immédiats. □

Remarque 4.1.14. — Notre résultat principal peut être vu comme une réciproque à la proposition 4.1.7. En effet, pour $\varphi \neq \mathbb{1}$, nous montrons que $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G]\!]$-libre pour tout quotient G de $\mathcal{G}_\Delta$ si et seulement si $\mathcal{X}_0^{\varphi}$ est $\mathbb{Z}_p$-libre où $\mathcal{X}_0 := \mathcal{G}^{ab}$, en d'autres termes pour le plus petit quotient de $\mathcal{G}_\Delta$.

Remarque 4.1.15. — Sous les conditions du théorème 4.1.13 et pour $\mathcal{H} = \mathcal{H}(\Delta)$, on obtient que $H^2(\mathcal{G}_\Delta, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial : en effet, dans ce cas, $\mathcal{X}^{\mathbb{1}} = \{1\}$.

Donnons à présent quelques situations immédiates.

Corollaire 4.1.16. — *Soit $\mathcal{G}$ un pro-p-groupe de dimension cohomologique stricte 2. Soit $\mathcal{H}$ un sous-groupe fermé et distingué de $\mathcal{G}$ contenant $\mathcal{H}(\Delta)$ et soit $\mathcal{G}_0$ un sous-groupe ouvert et distingué de $\mathcal{G}$ contenant $\mathcal{H}$. Posons $G = \mathcal{G}/\mathcal{H}$ et $G_0 = \mathcal{G}_0/\mathcal{H}$. Alors pour $\varphi \in \mathrm{Irr}^{\bullet}(\Delta, \mathbb{Q}_p)$, le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^{\varphi}$ est libre si et seulement si il l'est en tant que $\mathbb{Z}_p[\![G_0]\!]$-module.*

Démonstration. — Un sens est immédiat, mais nous allons montrer ce résultat par équivalence directe. Comme $\mathcal{G}$ est de dimension cohomologique stricte 2, les hypothèses du théorème 4.1.13 sont satisfaites et ainsi $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G]\!]$-libre si et seulement si $\mathrm{Tor}_{\mathbb{Z}_p}\left(\mathcal{G}^{ab}\right)^{\varphi}$ est trivial. Il en est de même de $\mathcal{X}^{\varphi}$ en tant que $\mathbb{Z}_p[\![G_0]\!]$-module. Mais la dimension cohomologie stricte de $\mathcal{G}$ apporte également que le morphisme de transfert induit un isomorphisme entre $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}^{ab}$ et $\left(\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}_0^{ab}\right)^{\mathcal{G}/\mathcal{G}_0}$ (voir par exemple [**42**, th. 3.6.4]). Ainsi, les φ-composantes de $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}^{ab}$ et de $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}_0^{ab}$ sont simultanément nulles ou non. Le résultat s'en déduit. □

Corollaire 4.1.17. — *Soit $\mathcal{G}$ un pro-p-groupe libre à d générateurs. Soit $\mathcal{H}$ un sous-groupe fermé de $\mathcal{G}$ contenant $\mathcal{H}(\Delta)$. Alors pour $\varphi \in \mathrm{Irr}^{\bullet}(\Delta, \mathbb{Q}_p)$, on a $\mathcal{X}^{\varphi} \simeq \mathbb{Z}_p[\![G]\!]^{d_\varphi}$, où $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\varphi}$.*

Démonstration. — Le groupe $\mathcal{G}$ est un pro-p-groupe libre donc pour tout sous-groupe fermé $\mathcal{H}$ de $\mathcal{G}$, il vient $H_2(\mathcal{H}, \mathbb{Z}_p) = 0$. D'autre part, l'abélianisé $\mathcal{G}^{ab}$ est isomorphe à $\mathbb{Z}_p^d$ donc pour tout caractère $\mathbb{Q}_p$-irréductible φ de Δ, la φ-composante $(\mathcal{G}^{ab})^{\varphi}$ est sans $\mathbb{Z}_p$-torsion. Le théorème 4.1.13 s'applique et ainsi $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G]\!]$-libre de rang d_φ. □

À ce niveau, on peut avancer un résultat un peu plus général quand $\mathcal{H} = \mathcal{H}(\Delta)$. Si F_d est le pro-p-groupe libre à d générateurs $x_1, \cdots, x_d$, on rappelle l'isomorphisme ψ entre $\mathbb{Z}_p[\![\mathbb{F}_d]\!]$ et l'algèbre de Magnus des séries formelles non commutatives $\mathbb{Z}_p[\![X_1, \cdots, X_d]\!]^{nc}$ donné par $\psi(x_i) = X_i + 1$ (voir par exemple [**29**, chap. 7, §7.6]).

Corollaire 4.1.18. — *Sous les conditions du théorème 4.1.13, prenons $\mathcal{H} = \mathcal{H}(\Delta)$. Supposons $(\mathcal{G}^{ab})^{\varphi}$ et $(\mathcal{G}^{ab})^{\mathbb{1}}$ sans $\mathbb{Z}_p$-torsion, où $\varphi \in \mathrm{Irr}^{\bullet}(\Delta, \mathbb{Q}_p)$. Alors*

$$\mathcal{X}^{\varphi} \simeq \left(\mathbb{Z}_p[\![X_1, \cdots, X_{d_{\mathbb{1}}}]\!]^{nc}\right)^{d_\varphi},$$

où $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\varphi}$.

Remarque 4.1.19. — On rappelle que nous avons vu dans la proposition 4.1.6 que pour $\mathcal{H} = \mathcal{H}(\Delta)$, on a $\mathcal{X}^{\mathbb{1}} = \{1\}$.

Démonstration. — Par hypothèses et comme on suppose $(\mathcal{G}^{ab})^{\varphi}$ sans $\mathbb{Z}_p$-torsion, le théorème 4.1.13 s'applique et $\mathcal{X}^{\varphi}$ est libre de rang d_φ, *i.e.* $\mathcal{X}^{\varphi} \simeq \mathbb{Z}_p[\![\mathcal{G}_\Delta]\!]^{d_\varphi}$. De plus, la suite exacte $1 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{F}_p \longrightarrow 1$ apporte la suite exacte de Δ-modules

$$\cdots \longrightarrow H_2(\mathcal{G}, \mathbb{Z}_p) \longrightarrow H_2(\mathcal{G}, \mathbb{F}_p) \twoheadrightarrow \mathcal{G}^{ab}[p].$$

Par hypothèses $H_2(\mathcal{G}, \mathbb{Z}_p) = 0$ et $\left(\mathcal{G}^{ab}[p]\right)^{\mathbb{1}} = 0$. Ainsi, $H_2(\mathcal{G}, \mathbb{F}_p)^{\mathbb{1}} = 0$ et la proposition 4.1.3 indique que $\mathcal{G}_\Delta$ est pro-p-libre de rang égal au p-rang de $(\mathcal{G}^{ab})^{\mathbb{1}}$ c'est-à-dire à $\mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}}$. On conclut en appliquant l'isomorphisme de Magnus à $\mathbb{Z}_p[\![\mathcal{G}_\Delta]\!]$. □

Pour le dernier corollaire de cette section, faisons le rappel suivant : un groupe de Demushkin $\mathcal{G}$ est de dimension cohomologique stricte 2 si et seulement si pour tout sous-groupe ouvert $\mathcal{U}$ de $\mathcal{G}$, $H^2(\mathcal{U}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, ou encore si et seulement si $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{U}^{ab} \neq \{0\}$; la dernière équivalence provient de la suite exacte

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

associée au fait que $H_2(\mathcal{U}, \mathbb{F}_p) \simeq \mathbb{Z}/p\mathbb{Z}$ (pour la première équivalence voir par exemple [**52**, chap I §3 prop. 19]). Cette suite exacte indique également que si $\mathcal{G}$ est de dimension cohomologique stricte 2, on a l'isomorphisme de Δ-modules :

$$H_2(\mathcal{G}, \mathbb{F}_p) \simeq_\Delta \mathcal{G}^{ab}[p].$$

Corollaire 4.1.20. — *Soit $\mathcal{G}$ un groupe de Demushkin de dimension cohomologique stricte 2. Soit ω le caractère de Δ résultant de l'action sur $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}^{ab}$.*

(i) *Si $\mathcal{G}_\Delta$ est pro-p-libre, alors $\mathcal{X}^\omega$ est non libre en tant que $\mathbb{Z}_p[\![\mathcal{G}_\Delta]\!]$-module, et pour $\varphi \neq \omega$, $\mathcal{X}^\varphi$ est $\mathbb{Z}_p[\![\mathcal{G}_\Delta]\!]$-libre.*

(ii) *Si $\mathcal{G}_\Delta$ est de Demushkin, pour tout $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$, on a $\mathcal{X}^\varphi = \mathbb{Z}_p[\![\mathcal{G}_\Delta]\!]^{d_\varphi}$, avec $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})_\varphi$.*

Démonstration. — Comme $\mathcal{G}$ est de Demushkin de dimension cohomologique stricte 2, les conditions sur les multiplicateurs de Schur $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ et $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ sont satisfaites pour tout sous-groupe fermé $\mathcal{H}$ de $\mathcal{G}$.

Suivant la proposition 4.1.4, $\mathcal{G}_\Delta$ est pro-p-libre si et seulement si $H^2(\mathcal{G}, \mathbb{F}_p)^{\mathbb{1}} = 0$. Dans ce cas ω n'est pas le caractère trivial et $\mathcal{X}^\omega$ n'est pas libre. Par contre les autres φ-composantes sont libres. Dans l'autre cas, $H^2(\mathcal{G}, \mathbb{F}_p)^{\mathbb{1}}$ n'est pas trivial, ainsi $\omega = \mathbb{1}$ et $\mathcal{X}^\varphi$ est libre pour tout $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$. □

4.2. Extensions à ramification restreinte : rappels

Le contexte que l'on va considérer par la suite est celui des extensions à ramification restreinte. On se donne un nombre premier impair p, un corps de nombres K et deux ensembles finis disjoints de places de K, qu'on note T et S. On suppose que les premiers qui composent S sont, en norme, congrus à 0 ou 1 modulo p. On renvoie à la section 2.1 pour les notations dans ce qui suit.

Pour notre étude, il convient de noter à ce niveau que les groupes de cohomologie $H^i(G^T_{\mathrm{K},S}, \mathbb{F}_p)$, $i = 1, 2$, sont finis. Voir section 2.2.

4.2.1. Torsion relative. — On a vu dans le chapitre 2 que la théorie p-adique du corps de classes est un outil particulièrement adapté à l'étude de pro-p extensions de corps de nombres. Rappelons en particulier que le noyau du morphisme naturel de restriction $G^{T',ab}_{\mathrm{K},\Sigma} \to G^{T,ab}_{\mathrm{K},S}$ est isomorphe, via l'application d'Artin, au quotient

$$\frac{\prod_{v\in\Sigma\setminus S}\mathcal{U}_v \prod_{v\in T\setminus T'}\mathcal{R}_v}{\iota(\mathcal{E}^T_S)},$$

où ι est le plongement diagonal sous-jacent (prop. 2.1.1). Cet isomorphisme est compatible avec la structure de Δ-module :

Remarque 4.2.1. — Lorsque les objets en jeu dans la proposition 2.1.1 sont munis d'une action d'un groupe Δ, l'isomorphisme est un isomorphisme de Δ-modules.

L'étude de $(G^T_{\mathrm{K},S})^{ab}$ peut alors se faire de façon relative : la théorie (globale) du corps de classes identifie le groupe $G^{\varnothing,p}_{\mathrm{K},\varnothing}$ au p-Sylow du groupe des classes de K. Il vient alors :

Corollaire. — *Soit p tel que le p-Sylow du groupe des classes* Cl(K) *de* K *est trivial. Alors*

$$G^{ab}_{\mathrm{K},S} \simeq \frac{\prod_{v\in S}\mathcal{U}_v}{\iota(\mathcal{E}_\mathrm{K})}.$$

Ce corollaire, démontré dans le chapitre 2, montre que les nombres premiers qui divisent l'ordre du groupe des classes jouent un rôle bien particulier pour notre étude. Nous les appelons *nombres premiers exceptionnels*.

Pour terminer cette section, rappelons que le théorème de Brauer-Siegel (cf [**32**, chap. XVI, §1]) apporte l'inégalité $|\mathrm{Cl}(\mathrm{K})| \leqslant |\mathrm{Disc}_{\mathrm{K}}|^{C}$, où $\mathrm{Disc}_{\mathrm{K}}$ est le discriminant du corps K et où C est une constante universelle. Rappelons également qu'il est conjecturé que pour tout $\varepsilon > 0$: $|\mathrm{Cl}(\mathrm{K})[p]| \ll_{\varepsilon,[\mathrm{K}:\mathbb{Q}]} |\mathrm{Disc}_{\mathrm{K}}|^{\varepsilon}$. Voir par exemple Ellenberg-Venkatesh [**10**] pour une présentation de cette conjecture. Voir également [**4**], [**6**], [**9**], [**24**], [**25**], [**45**], [**46**], etc.

4.2.2. Le module $\prod_{w|v} \mathcal{U}_w$. — Partons d'une extension galoisienne K/k de groupe de Galois Δ d'ordre premier à p. Soit v une place de k et soit $w|v$ une place de K au-dessus de v. Par abus, posons $D_v = D_w$ le groupe décomposition de w dans K/k. On rappelle que $D_w \simeq \mathrm{Gal}(\mathrm{K}_w/\mathrm{k}_v)$. Posons $N = |\mu_{p^\infty}(\mathrm{K}_w)|$.

Définition 4.2.2. — La représentation induite $\mathrm{Ind}_{D_v}^{\Delta} \mu_{p^\infty}(\mathrm{K}_w)$ de D_v à Δ du module $\mu_{p^\infty}(\mathrm{K}_w)$ est notée $\chi_{D_v}^{\Delta}$:

$$\chi_{D_v}^{\Delta} = \mathbb{Z}_p[\Delta] \otimes_{D_v} \mu_{p^\infty}(\mathrm{K}_w).$$

Bien entendu, la représentation $\chi_{D_v}^{\Delta}$ ne dépend pas du choix de la place w au-dessus de v.

Remarquons que par semi-simplicité, la suite exacte

$$1 \longrightarrow \mu_p(\mathrm{K}_w) \longrightarrow \mu_{p^\infty}(\mathrm{K}_w) \xrightarrow{p} \mu_{p^\infty}(\mathrm{K}_w) \longrightarrow \mu_{p^\infty}(\mathrm{K}_w)/\big(\mu_{p^\infty}(\mathrm{K}_w)\big)^p \longrightarrow 1,$$

indique que les deux $\mathbb{F}_p[\Delta]$-modules $\mu_p(\mathrm{K}_w)$ et $\mu_{p^\infty}(\mathrm{K}_w)/\big(\mu_{p^\infty}(\mathrm{K}_w)\big)^p$ ont même caractère.

Si l'on regarde plus en détail $\chi_{D_v}^{\Delta}$, il vient deux cas.

• Si v ne divise pas p, le groupe $\mu_{p^\infty}(\mathrm{K}_w)$ est isomorphe à $\mathcal{U}_w$. Dans ce cas, $\chi_{D_v}^{\Delta} = \prod_{w|v} \mathcal{U}_w$.

À noter que si k_v contient une racine primitive p-ème de l'unité, alors D_v agit trivialement sur $\mu_{p^\infty}(\mathrm{K}_w)$ et ainsi $\chi_{D_v}^{\Delta} = \mathrm{Ind}_{D_v}^{\Delta}\big(\mathbb{Z}/N\mathbb{Z}\big) \simeq \mathbb{Z}_p[\Delta] \otimes_{D_v} \mathbb{Z}/N\mathbb{Z}$. Si $|\mu_{p^\infty}(\mathrm{k}_v)| = p$, on a $\chi_{D_v}^{\Delta} = \mathrm{Ind}_{D_v}^{\Delta} \mathbb{1}$.

• Si v divise p, alors $\mathcal{U}_w$ est isomorphe au groupe des unités principales de K_w, dont la partie de torsion est égale à $\mu_{p^\infty}(\mathrm{K}_w)$. Par semi-simplicité (ici $p \nmid |D_w|$), le $\mathbb{Z}_p[D_w]$-module $\mathcal{U}_w/\mu_{p^\infty}(\mathrm{K}_w)$ étant $\mathbb{Z}_p$-libre, il est projectif, et ainsi

$$\mathcal{U}_w \simeq \mu_{p^\infty(\mathrm{K}_w)} \oplus \mathcal{U}_w/\mu_{p^\infty}(\mathrm{K}_w).$$

On a même mieux : le logarithme p-adique permet de montrer que le quotient $\mathcal{U}_w/\mu_{p^\infty}(\mathrm{K}_w)$ est isomorphe, en tant que $\mathbb{Z}_p[\Delta]$-module, au module libre $(\mathbb{Z}_p[\Delta])^{[\mathrm{k}_v:\mathbb{Q}_p]}$. Ainsi,

$$\mathcal{U}_w \simeq \mu_{p^\infty}(\mathrm{K}_w) \oplus (\mathbb{Z}_p[D_w])^{[\mathrm{k}_v:\mathbb{Q}_p]}.$$

Ensuite, il suffit de noter que Δ agit transitivement sur $(\mathcal{U}_w)_{w|v}$ pour obtenir

$$\prod_{w|v} \mathcal{U}_w \simeq \mathrm{Ind}_{D_v}^{\Delta} \mu_{p^\infty}(\mathrm{K}_w) \oplus (\mathbb{Z}_p[\Delta])^{[\mathrm{k}_v:\mathbb{Q}_p]}.$$

Ou encore : le $\mathbb{F}_p[\Delta]$-module $\prod_{w|v} \mathcal{U}_w/\mathcal{U}_w^p$ a pour caractère $\omega + [\mathrm{k}_v : \mathbb{Q}_p]\mathrm{Rg}$, où ici $\omega := \mathbb{F}_p \otimes \chi_{D_v}^{\Delta}$.

4.2.3. La conjecture de Leopoldt (rappels). — On rappelle que la conjecture de Leopoldt pour le corps de nombres K et le nombre premier p stipule que l'application de semi-localisation induit un $\mathbb{Z}_p$-morphisme injectif du p-adifié $\mathcal{E}_{\mathrm{K}}$ du groupe des unités globales dans le produit $\mathcal{U}_p = \prod_{v|p} \mathcal{U}_v$ des p-groupes d'unités locales pour les places divisant p. Rappelons une équivalence de cette formulation.

Proposition 4.2.3 **([43]).** — *La conjecture de Leopoldt est vérifiée par le corps de nombres* K *et le nombre premier p si et seulement si le multiplicateur de Schur $H_2(G_{\mathrm{K},S}, \mathbb{Z}_p)$ du pro-p-groupe $G_{\mathrm{K},S}$ est trivial dès que S contient l'ensemble S_p.*

Soit S un ensemble fini de places de K contenant S_p. Supposons la conjecture de Leopoldt vérifiée pour toute extension finie du corps K contenue dans K_S/K. Alors (et c'est même équivalent) on a $H_2(\mathcal{U}, \mathbb{Z}_p) = 0$ pour tout sous-groupe ouvert normal $\mathcal{U}$ de $G_{\mathrm{K},S}$. Comme on sait que le pro-p-groupe $G_{\mathrm{K},S}$ est de dimension cohomologique au plus 2, il vient que la conjecture de Leopoldt le long de K_S/K

équivaut au fait que le pro-p-groupe $G_{\mathrm{K},S}$ est de dimension cohomologique stricte au plus 2 (il peut être libre), et ce pour tout ensemble fini S contenant S_p. (Pour plus d'informations voir [**16**, chap. 3, §3] ou [**42**, chap. X, §3].)

On supposera pour toute la suite que la conjecture de Leopoldt est vérifiée pour toutes les extensions finies de K. Ainsi pour tout sous-groupe fermé $\mathcal{H}$ de $G_{\mathrm{K},S}$ le groupe $H_2(\mathcal{H},\mathbb{Z}_p)$ est trivial : les hypothèses du théorème 4.1.13 dans les contextes globaux à venir seront vérifiées.

Notons ici qu'en se plaçant sous la conjecture de Leopoldt et pour $S = S_p$ avec p ne divisant pas le nombre de classes de K, déterminer les composantes $\mathcal{X}^\varphi$ non libres revient en fait à déterminer le défaut de p-rationalité du corps K. Gras, dans [**15**], définit sous la conjecture de Leopoldt le régulateur p-adique normalisé de K comme la $\mathbb{Z}_p$-torsion du quotient $\log(\prod_{v|p}\mathcal{U}_v)/\log(\iota(\mathcal{E}_\mathrm{K}))$.

Terminons cette section en rappelant un théorème de déploiement de la ramification ([**17**, chap. III, §4, th. 4.1.5]) :

Théorème 4.2.4. — *Supposons la conjecture de Leopoldt vérifiée pour le corps de nombres* K *et le premier p. Alors il vient la suite exacte*

$$1 \longrightarrow \prod_{v\in S\setminus S_p} \mathcal{U}_v \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p} G_{\mathrm{K},S}^{ab} \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p} G_{S_p}^{ab} \longrightarrow 1.$$

Bien entendu, lorsque les objets en jeu sont munis d'une action d'un groupe Δ, la suite exacte du théorème 4.2.4 est une suite exacte de Δ-modules.

4.3. Quelques contextes arithmétiques

4.3.1. La situation locale. — Donnons le contexte naturel. Partons d'une tour d'extensions locales $\mathrm{K}/\mathrm{k}/\mathbb{Q}_p$ de degrés relatifs finis. On suppose que l'extension K/k est galoisienne de groupe de Galois Δ, d'ordre premier à p. Notons par $\overline{\mathrm{K}}$ la pro-p-extension maximale de K et posons $\mathcal{G} = \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$. Soit $\Gamma = \Delta \ltimes \mathcal{G}$. Posons $\mathcal{H} = \mathcal{H}(\Delta)$, $\mathcal{X} = \mathcal{H}^{ab}$, $G = \mathcal{G}/\mathcal{G}_\Delta$ et soit l'algèbre d'Iwasawa $\Lambda := \mathbb{Z}_p[\![G]\!]$. Le pro-$p$-groupe $G \simeq \mathcal{G}(p)$ est isomorphe au groupe de Galois $\mathrm{Gal}(\overline{\mathrm{k}}/\mathrm{k})$: c'est un pro-p-groupe à $[\mathrm{k}:\mathbb{Q}_p]+1+\delta_p(\mathrm{k})$ générateurs. Suivant que k contient les racines p-èmes de l'unité ou non, le pro-p-groupe G est un groupe de Demushkin ou un pro-p-groupe libre. La situation correspond à celle des corollaires 4.1.17 ou 4.1.20.

Corollaire 4.3.1. — *Si* K *ne contient pas les racines p-èmes de l'unité, le pro-p-groupe $\mathcal{G}$ est pro-p-libre et pour tout caractère $\mathbb{Q}_p$-irréductible $\varphi \in \mathrm{Irr}^\bullet(\Delta,\mathbb{Q}_p)$, il vient $\mathcal{X}^\varphi \simeq \Lambda^{d_\varphi}$, avec $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^\varphi = \deg(\varphi)[\mathrm{k}:\mathbb{Q}_p]$.*

Démonstration. — C'est une application immédiate du corollaire 4.1.17. □

Supposons maintenant que K contient les racines p-èmes de l'unité. Alors $\mathcal{G}$ est un groupe de Demushkin et l'on se retrouve dans la situation du corollaire 4.1.20. Soit ω le caractère cyclotomique.

Corollaire 4.3.2. — *Supposons que* K *contient les racines p-èmes de l'unité.*

(i) *Pour $\varphi \neq \omega$ et $\varphi \neq \mathbb{1}$, il vient $\mathcal{X}^\varphi \simeq \Lambda^{d_\varphi}$, où $d_\varphi = \deg(\varphi)[\mathrm{k}:\mathbb{Q}_p]$.*
(ii) *Quand $\omega \neq \mathbb{1}$, $\mathcal{X}^\omega$ n'est pas Λ-libre.*
(iii) *Quand $\omega = \mathbb{1}$, $\mathcal{X}^{\mathbb{1}} = \{1\}$.*

Démonstration. — C'est donc une application du corollaire 4.1.20 associé à la théorie du corps de classes locale. Seuls les caractères $\mathbb{1}$ et ω sont à discuter. Si ω n'est pas le caractère trivial, cela signifie que k ne contient pas les racines p-èmes de l'unité et donc que G est pro-p-libre, c'est le point (i) du corollaire en question qui s'applique. Si $\omega = \mathbb{1}$, cela signifie que G est de Demushkin de dimension cohomologique stricte 2 et cette fois-ci, c'est le point (ii) qui s'applique. □

4.3.2. Extensions de corps de nombres. — Soit K/k une extension galoisienne de corps de nombres de groupe de Galois Δ d'ordre premier à p. Soit S un ensemble de places de k. Par abus, nous notons encore par S l'ensemble des places de K au-dessus de celles de $S_{\mathrm{k}} = S$. Notons par K_S la pro-p-extension maximale de K non-ramifiée en dehors de S ; $G_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$. On va appliquer les résultats de la section 4.1 au groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{k}) =: \Gamma = \Delta \ltimes \mathcal{G}$, où l'on a posé $\mathcal{G} := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$.

Pour qu'une place $w \in S$ puisse jouer un rôle, nous nous assurons que,

- ou bien w est une place p-adique ;
- ou bien, si $w \nmid p$, le corps local K_w contient une racine primitive d'ordre p.

Faisons la remarque que pour $v|w$, avec $v \nmid p$, le corps k_v peut ne pas contenir de racine primitive d'ordre p (*i*.e. que $|\mu_{p^\infty}(\mathrm{k}_v)| = 1$).

Soit $G := \mathcal{G}_\Delta$ le plus grand quotient de $\mathcal{G}$ sur lequel Δ agit trivialement. On a alors immédiatement :

Lemme 4.3.3. — *Le groupe de Galois G est isomorphe au groupe de Galois* $\mathrm{Gal}(\mathrm{k}_S/\mathrm{k})$.

Démonstration. — En effet, on sait d'après la proposition 4.1.3 que G est isomorphe à $\Gamma(p)$, le plus grand pro-p-quotient de Γ. Par conséquent le résultat se déduit facilement en se rappelant que k_S/k est la pro-p-extension *maximale* de k non ramifiée en dehors de S. □

En d'autres termes, le sous-corps fixé par $\mathcal{H}(\Delta)$ correspond, par la théorie de Galois, au compositum Kk_S/K.

4.3.2.1. *Premiers corollaires.* — Supposons maintenant que S contient S_p (on rappelle que par confort, on suppose $p > 2$). Alors la conjecture de Leopoldt nous assure la trivialité des multiplicateurs de Schur $H_2(\mathcal{H}, \mathbb{Z}_p)$ pour tout sous-groupe fermé $\mathcal{H}$ de G_S.

Ainsi, pour toute la suite, *on suppose la conjecture de Leopoldt vraie pour le nombre premier p considéré et les extensions en jeu.*

Notre étude a montré que les résultats attendus reposent sur des conditions différentes suivant que $\varphi = \mathbb{1}$ ou non.

Pour $\varphi \neq \mathbb{1}$, d'après le théorème 4.1.13, l'étude de la liberté du module $\mathcal{X}^\varphi$ revient à l'étude de la torsion de $(G_{\mathrm{K},S}^{ab})^\varphi$. Dans ce contexte, le corollaire 2.1.2 nous permet d'obtenir :

Corollaire 4.3.4. — *Soit p tel que $p \nmid |\mathrm{Cl}(\mathrm{K})|$ et soit $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$. Alors le module $\mathcal{X}^\varphi$ est $\mathbb{Z}_p[\![G]\!]$-libre si et seulement si,*

(*i*) $\big(\prod_{w \in S \setminus S_p} \mathcal{U}_w\big)^\varphi = \{1\}$, *et*

(*ii*) $\mathrm{Tor}_{\mathbb{Z}_p} \dfrac{\big(\prod_{w \in S_p} \mathcal{U}_w\big)^\varphi}{\iota(\mathcal{E}_{\mathrm{K}}^\varphi)} = \{1\}$, *où ι est le plongement diagonal sous-jacent.*

Démonstration. — C'est une simple application du théorème 4.1.13 associé au corollaire 2.1.2 et au théorème de déploiement 4.2.4. □

Prenons p *générique*, c'est-à-dire tel que :

- le p-Sylow du groupe des classes $\mathrm{Cl}(\mathrm{K})$ de K est trivial (le premier p n'est pas exceptionnel), et
- pour toute place $v|p$, $\mathrm{K}_v^\times$ ne contient pas de racine primitive p-ème de l'unité.

Dans ce contexte, le corollaire 2.1.2 nous permet d'obtenir :

Corollaire 4.3.5. — *Soit p générique et soit un caractère $\mathbb{Q}_p$-irréductible $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$ de Δ tels que les deux φ-composantes suivantes soient nulles :*

(i) $\mathcal{E}_{\mathrm{K}}^\varphi$ *et,*

(ii) $\big(\prod_{w \in S \setminus S_p} \mathcal{U}_w\big)^\varphi$.

Alors le module $\mathcal{X}^\varphi$ est $\mathbb{Z}_p[\![G]\!]$-libre.

Démonstration. — C'est une conséquence directe du corollaire 4.3.4. □

Dans la section 4.4, nous ferons un certain nombre d'expérimentations sur la liberté de $\mathcal{X}^{\varphi}$. Pour ce faire, nous utiliserons PARI/GP [**54**], sans "travailler" dans le corps de nombres mais seulement à partir du polynôme P définissant le corps de nombres. Il nous faudra partir d'un polynôme P dont les racines permettent de donner une base des unités du corps K, nous utiliserons des familles de polynômes bien particuliers.

Remarquons qu'il nous faut des générateurs de $\mathcal{E}_{\mathrm{K}}$, ce qui est moins "fin" que des générateurs de E_{K}. Ainsi, il nous aurait été possible d'utiliser le principe suivant. Soit un polynôme unitaire $P \in \mathbb{Z}[X]$, irréductible, et de coefficient constant ± 1, dont les racines engendrent le corps K. Posons $r = r_1 + r_2$, où (r_1, r_2) est la signature de K, *i.e.* r_1 est le nombre de plongements réels de K et r_2 le nombre de couples de plongements complexes conjugués. On note σ_i, $i \in [\![1, r]\!]$, les plongements de K. Le coefficient constant de P est une unité de $\mathbb{Z}$ donc les racines de P sont des unités de l'anneau des entiers de K. Si de ces unités on peut extraire une famille $\mathcal{F} := (\varepsilon_i)_{i=1,\cdots,r-1}$ pour laquelle le régulateur est non nul :

$$\mathrm{Reg}(\mathcal{F}) := |\det\left(\log|\sigma_i(\varepsilon_j)|\right)_{i,j}| \neq 0$$

alors la famille $\mathcal{F}$ est d'indice fini dans $\mathcal{O}_{\mathrm{K}}^{\times}$. Si ensuite on utilise des estimations sur les régulateurs pour obtenir une majoration de l'indice $[\mathcal{O}_{\mathrm{K}}^{\times} : \langle\mathcal{F}\rangle_{\mathbb{Z}}]$ (par exemple pour les corps cubiques, il y a les estimations de Cusick [**8**]), il vient alors que pour p assez grand, *i.e.*, pour p strictement supérieur au plus grand nombre premier divisant $[\mathcal{O}_{\mathrm{K}}^{\times} : \langle\mathcal{F}\rangle_{\mathbb{Z}}]$:

$$\mathcal{E}_{\mathrm{K}} := \mathbb{Z}_p \otimes E_{\mathrm{K}} = \langle 1 \otimes \varepsilon_1, \cdots, 1 \otimes \varepsilon_{r-1} \rangle.$$

Une fois obtenue une base de $\mathcal{E}_{\mathrm{K}}$, on peut travailler φ-composante par φ-composante. Voici maintenant le principe de nos calculs à venir. Plaçons-nous dans le contexte du corollaire 4.3.5 avec p générique ($p \nmid |\mathrm{Cl}(\mathrm{K})|$, et pour toute place $w \in S_p$, $\mu_{p^\infty}(\mathrm{K}_w) = \{1\}$). Partons d'une φ-composante $\mathcal{E}_{\mathrm{K}}^{\varphi} = \langle x_1, \cdots, x_d \rangle$ de $\mathbb{Z}_p$-rang $d > 0$. Alors

$$\mathrm{Tor}_{\mathbb{Z}_p} \frac{\left(\prod_{w \in S_p} \mathcal{U}_w\right)^{\varphi}}{\iota(\mathcal{E}_{\mathrm{K}}^{\varphi})} \neq \{1\},$$

si et seulement si il existe $a_1, \cdots, a_d \in [0, \cdots, p-1]$, *non tous nuls*, tels que

$$\forall w \in S_p,\ \iota_w(x_1^{a_1} \ldots x_d^{a_d}) \in \mathcal{U}_w^p,$$

ici ι_w est le plongement de K dans $\mathcal{U}_w$. Si l'on suppose par exemple $a_1 \neq 0$, par la relation de Bezout entre a_1 et p, on se ramène à tester la condition $\iota_w(x_1 x_2^{a_2} \ldots x_d^{a_d}) \in \mathcal{U}_w^p$, pour tout $w \in S_p$, quand les puissances a_i varient dans $[0, p-1]$. Notons également que l'on peut être plus précis sur les coefficients a_i dès lors que l'on a explicitement la représentation irréductible (voir la section 4.4.1.1). La dernière condition obtenue est alors très simple à tester, en effet, c'est une simple condition de congruence !

Typiquement, il y a le cadre bien agréable suivant : lorsque $\mathcal{E}^{\varphi} = \langle\varepsilon\rangle$ est engendré par une unité ε de K qui de plus s'exprime facilement à partir des racines de P. Alors dans ce cas, et pour p générique, $\mathrm{Tor}_{\mathbb{Z}_p}(G_{\mathrm{K},S}^{ab})^{\varphi} \neq \{0\}$ si et seulement si $\iota_w(\varepsilon) \in \mathcal{U}_w^p$ pour toute place $w \in S_p$. Nous reviendrons sur cette observation plus tard.

Remarque 4.3.6. — À ce stade, il convient de rappeler la conjecture de Gras donnée en introduction : étant donné un corps de nombres K, pour p assez grand, il vient $\mathrm{Tor}_{\mathbb{Z}_p} \frac{\left(\prod_{w \in S_p} \mathcal{U}_w\right)}{\iota(\mathcal{E}_{\mathrm{K}})} = \{1\}$. Ceci implique, sous les conditions du corollaire 4.3.4, que le module $\mathcal{X}^{\varphi}$ est conjecturalement $\mathbb{Z}_p[\![G]\!]$-libre.

4.3.2.2. *Extensions à multiplication complexe.* — Soit K/k une extension quadratique à multiplication complexe : le corps k est totalement réel et le corps K est totalement imaginaire. Posons $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = \Delta = \langle\sigma\rangle$.

Reprenons le cadre de la section 4.3.2. Soit S un ensemble de places de k contenant l'ensemble des places au-dessus de p (que l'on suppose toujours impair). Soit $\mathcal{G} = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$, $G = \mathcal{G}_{\Delta}$, et $\mathcal{X} = \mathcal{H}(\Delta)$. On note par $\mathcal{X}^-$ la composante de $\mathcal{X}$ sur laquelle σ agit par -1. Les résultats précédents nous permettent d'obtenir (sous la conjecture de Leopoldt) :

Corollaire 4.3.7. — *Soit* K/k *une extension quadratique à multiplication complexe. Soit $p > 2$ générique.*

(i) *Si une place $v \in S\backslash S_p$ se décompose dans* K/k *ou si elle est telle que $\mu_{p^\infty}(\mathrm{k}_v) = \{1\}$, alors $\mathcal{X}^-$ n'est pas $\mathbb{Z}_p[\![G]\!]$-libre.*

(ii) *Supposons le contraire,* i.e. *que pour toute place $v \in S\backslash S_p$, on a $\mu_{p^\infty}(\mathrm{k}_v) \neq \{1\}$ et que v est soit inerte, soit ramifiée dans* K/k. *Alors $\mathcal{X}^-$ est $\mathbb{Z}_p[\![G]\!]$-libre de rang $|S_\mathrm{k}|$.*

Faisons la remarque suivante : en prenant p générique, on a $\mu_p(\mathrm{K}) = \{1\}$.

Démonstration. — Remarquons tout d'abord que comme K/k est à multiplication complexe et que $\mu_p(\mathrm{K}) = \{1\}$, alors $(\mathcal{E}_\mathrm{K})^- = \{1\}$.

Ensuite, d'après le théorème 4.1.13, la liberté du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^-$ équivaut à la trivialité de $\mathrm{Tor}_{\mathbb{Z}_p}(G_S^{ab})^-$; on utilise alors l'isomorphisme du corollaire 2.1.2 pour arriver à

$$\mathrm{Tor}_{\mathbb{Z}_p}(G_S^{ab})^- \simeq \mathrm{Tor}_{\mathbb{Z}_p}\left(\frac{\prod_{w\in S}\mathcal{U}_w}{\iota(\mathcal{E}_\mathrm{K})}\right)^- \simeq \mathrm{Tor}_{\mathbb{Z}_p}(\prod_{w\in S}\mathcal{U}_w)^-.$$

Si une place $v \in S\backslash S_p$ est décomposée dans K/k, alors le module $\prod_{w|p}\mathcal{U}_w$ est de torsion, a une partie − non triviale, et ainsi $\mathrm{Tor}_{\mathbb{Z}_p}(G_S^{ab})^-$ n'est pas triviale. Par contre, dans le cas contraire, il vient

$$\mathrm{Tor}_{\mathbb{Z}_p}(G_S^{ab})^- \simeq \mathrm{Tor}_{\mathbb{Z}_p}(\prod_{w|p}\mathcal{U}_w)^- = \{1\},$$

car par hypothèse sur p, le $\mathbb{Z}_p$-module $\mathcal{U}_w$ est sans torsion. □

Les groupes $G_{\mathrm{K},S}$ peuvent être de Demushkin et on peut alors leur appliquer le corollaire 4.1.20. Wingberg dans **[57]** donne une description assez précise de la situation. Nous nous contentons de donner le résultat que l'on peut obtenir dans le cas à multiplication complexe. Pour ce faire, on commence par rappeler le résultat suivant :

Théorème 4.3.8 **(Wingberg, [57]).** — *Soit* K/k *une extension à multiplication complexe. Supposons qu'il existe une place $w \in S$ telle que $\mu_p(\mathrm{K}_w) \neq \{1\}$. Soit $v|w$. Alors $G_{\mathrm{K},S}$ est un groupe de Demushkin si et seulement si les conditions suivantes sont vérifiées :*

(i) $S = S_p = \{v\}$ *et* $|S_\mathrm{K}| = 1 + \delta_\mathrm{K}$, *où* $\delta_\mathrm{K} = 1$ *si* $\mu_p(\mathrm{K}) \neq \{1\}$, 0 *sinon ;*

(ii) $G_{\mathrm{k},S}$ *est un groupe de Demushkin et* $\mu_p(\mathrm{k}_v) \neq \{1\}$ *;*

(iii) $G_\mathrm{K}^{S,ab} = \{1\}$.

On en déduit alors le corollaire suivant :

Corollaire 4.3.9. — *Sous les conditions de cette section, supposons que $G_{\mathrm{K},S}$ est un groupe de Demushkin. Alors le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^-$ est libre.*

Démonstration. — D'après le théorème 4.3.8, le groupe $G_{\mathrm{k},S}$ est de Demushkin, c'est alors une simple application du corollaire 4.1.20. □

Pour être complet, donnons un critère de **[57]** qui donne des corps totalement réels k pour lesquels $G_{\mathrm{k},S}$ est de Demushkin (en fait Wingberg donne une équivalence pour les corps totalement réels). Avant d'énoncer ce critère, soit

$$\mathrm{V}_S = \{x \in \mathrm{k}^\times,\ x \in (\mathrm{k}_v)^p \quad \forall v \in S, \quad x \in \mathcal{U}_{v'}(\mathrm{k}_{v'})^p \quad \forall v' \notin S\}$$

et soit

$$V^S = \{x \in \mathrm{k}^\times,\ x \in \mathcal{U}_{v'}(\mathrm{k}_{v'})^p \quad \forall v' \notin S\}.$$

Théorème 4.3.10 **(Wingberg, [57]).** — *Soit* k *un corps totalement réel avec $S = S_p = \{v\}$. Supposons $\mu_p(\mathrm{K}) \neq \{1\}$. Alors $G_{\mathrm{k},S}$ est de Demushkin si et seulement si $d_p\mathrm{V}_S^S/(\mathrm{k}^\times)^p = 0$ et $d_p\mathrm{V}^S/(\mathrm{k}^\times)^p = [\mathrm{k}_v : \mathbb{Q}_p]$.*

À noter que quand $\mu_p(\mathrm{k}_v) \neq \{1\}$, alors l'égalité $d_p\mathrm{V}^S/\mathrm{K}^p - d_p\mathrm{V}_S^S/\mathrm{K}^p = [\mathrm{k}_v : \mathbb{Q}_p]$ équivaut à $d_pG_{\mathrm{k},S} - d_pG_{\mathrm{k}}^S = 2$: en effet, cela provient de la suite exacte

$$1 \longrightarrow \mathrm{V}_S^S/(\mathrm{k}^\times)^p \longrightarrow \mathrm{V}^S/(\mathrm{k}^\times)^p \longrightarrow \mathrm{k}_v^\times/(\mathrm{k}_v^\times)^p \longrightarrow G_{\mathrm{k},S}^{ab,p} \longrightarrow \left(G_{\mathrm{k}}^S\right)^{ab,p} \longrightarrow 1.$$

4.3.2.3. *Caractères fidèles.* — Lorsque l'on étudie des objets arithmétiques dans un contexte semi-simple, cette étude se ramène pour certaines φ-composantes à l'étude dans un sous-corps strict. Rappelons ce principe (en suivant [**16**, chap. 3, §3]).

Partons d'un groupe fini Δ d'ordre premier à p. Considérons un caractère $\mathbb{Q}_p$-irréductible φ de Δ. On appelle noyau de φ, noté $\mathrm{Ker}(\varphi)$, le noyau de toute représentation de caractère φ.

Définition 4.3.11. — Soit φ un caractère $\mathbb{Q}_p$-irréductible de Δ. Par restriction de φ, on peut définir un unique caractère $\mathbb{Q}_p$-irréductible fidèle φ' sur $\Delta/\mathrm{Ker}(\varphi)$, qu'on appelle caractère fidèle associé à φ.

Si l'on part d'une extension galoisienne de corps de nombres K/k et de groupe de Galois Δ, on note $\mathrm{K}(\varphi)$ le sous-corps de K correspondant par la théorie de Galois à $\mathrm{Ker}(\varphi)$.

On note k^{gal} l'extension galoisienne maximale d'ordre premier à p de k. Considérons une famille $(M_F)_F$ de $\mathbb{Z}_p[\mathrm{Gal}(\mathrm{k}^{alg}/\mathrm{k})]$-modules de type fini indexée par les sous-extensions galoisiennes finies de $\mathrm{k}^{alg}/\mathrm{k}$ pour laquelle on dispose d'applications

$$N_{\mathrm{L}'/\mathrm{L}} : M_{\mathrm{L}'} \to M_{\mathrm{L}}, \quad j_{\mathrm{L}'/\mathrm{L}} : M_{\mathrm{L}} \to M_{\mathrm{L}'} \quad (\mathrm{L} \subset \mathrm{L}') \tag{13}$$

vérifiant

$$N_{\mathrm{L}'/\mathrm{L}} \cdot j_{\mathrm{L}'/\mathrm{L}} = [\mathrm{L}' : \mathrm{L}], \qquad j_{\mathrm{L}'/\mathrm{L}} \cdot N_{\mathrm{L}'/\mathrm{L}} = Tr_{\mathrm{L}'/\mathrm{L}}. \tag{14}$$

Ici *traditionnellement* $N_{\mathrm{L}'/\mathrm{L}}$ (resp. $Tr_{\mathrm{L}'/\mathrm{L}}$) correspond à la norme (resp. à la trace).

On a alors (voir donc par exemple [**16**]) :

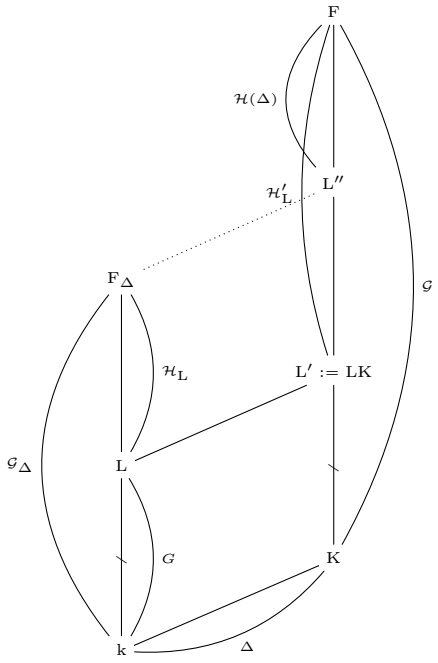
Proposition 4.3.12. — *Soit* K/k *une sous-extension galoisienne finie de* k^{gal}/k *de groupe de Galois* Δ*. Sous les hypothèses précédentes, on a la décomposition*

$$M_{\mathrm{K}} \simeq \bigoplus_{\varphi \in \mathrm{Irr}(\Delta, \mathbb{Q}_p)} M_{\mathrm{K}(\varphi)}^{\varphi'},$$

où la somme porte sur les caractères $\mathbb{Q}_p$*-irréductibles de* Δ*.*

Notons que lorsque $\varphi = \mathbb{1}$ est le caractère trivial, il vient $M_{\mathrm{K}}^{\mathbb{1}} = M_{\mathrm{k}}$.

Nous allons montrer que ce principe s'applique à l'étude du Δ-module $\mathcal{X}$ (on conserve le contexte de cette section). Partons des extensions suivantes :



Typiquement, dans notre cadre arithmétique on a : $\mathrm{F} = \mathrm{K}_S$ et $\mathrm{F}_\Delta = \mathrm{k}_S$.

Montrons que les groupes $\mathcal{X}_{\mathrm{L}} := \mathcal{H}_{\mathrm{L}}^{ab}$ et $\mathcal{X}_{\mathrm{L}'} := \mathcal{H}_{\mathrm{L}'}^{ab}$ peuvent être munis de deux morphismes N et j satisfaisant les identités (13) et (14). Détaillons-les. Tout d'abord, la surjection $\mathcal{H}_{\mathrm{L}'} \twoheadrightarrow \mathcal{H}_{\mathrm{L}}$ induit le morphisme de restriction $N : \mathcal{H}_{\mathrm{L}'}^{ab} \twoheadrightarrow \mathcal{H}_{\mathrm{L}}^{ab}$. Le morphisme j correspond au transfert que nous rappelons rapidement. Appliquons à la suite exacte de groupes finis

$$1 \longrightarrow \mathrm{Gal}(\mathrm{F}/\mathrm{L}') \longrightarrow \mathrm{Gal}(\mathrm{F}/\mathrm{L}) \longrightarrow \Delta \longrightarrow 1 \tag{15}$$

le principe du transfert (ce qui est possible car Δ est fini) pour obtenir

$$j : \mathrm{Gal}(\mathrm{F}/\mathrm{L})^{ab} \to \mathcal{X}_{\mathrm{L}'}.$$

Il reste alors à décrire correctement $\mathrm{Gal}(\mathrm{F}/\mathrm{L})^{ab}$, ce qui fait l'objet de la proposition suivante :

Proposition 4.3.13. — *On a un isomorphisme naturel entre* $\mathrm{Gal}(\mathrm{F}/\mathrm{L})^{ab}$ *et* $\mathcal{X}_{\mathrm{L}} \times \Delta^{ab}$.

Démonstration. — Posons $M = \mathrm{Gal}(\mathrm{F}/\mathrm{L})$ et $N = \mathrm{Gal}(\mathrm{F}/\mathrm{L}')$. Partons de la suite exacte (15) pour obtenir

$$1 \longrightarrow \left(N^{ab}\right)_\Delta \longrightarrow M^{ab} \longrightarrow \Delta^{ab},$$

car $H_2(\Delta, \mathbb{Z}_p) = 0$. Pour conclure, il suffit alors de noter le lemme suivant (car Δ^{ab} est d'ordre premier à p) :

Lemme 4.3.14. — *Sous les conditions précédentes, on a :*

$$\left(\mathcal{X}_{\mathrm{L}'}\right)_\Delta \simeq \mathcal{X}_{\mathrm{L}}.$$

Démonstration. — Cette fois-ci partons de la suite exacte

$$1 \longrightarrow \mathcal{H}(\Delta) \longrightarrow \mathcal{H}_{\mathrm{L}'} \longrightarrow \mathcal{H}_{\mathrm{L}} \longrightarrow 1,$$

qui devient

$$\cdots \longrightarrow \left(\mathcal{H}(\Delta)^{ab}\right)_{\mathcal{H}_{\mathrm{L}}} \longrightarrow N^{ab} \longrightarrow \mathcal{X}_{\mathrm{L}} \longrightarrow 1.$$

Or, par maximalité de L'', Δ agit sans point fixe sur $\mathcal{H}(\Delta)^{ab}$ (voir proposition 4.1.6), ce qui implique $\left(\left(\mathcal{H}(\Delta)^{ab}\right)_{\mathcal{H}_{\mathrm{L}}}\right)^\Delta = \{0\}$. Par conséquent, si l'on note par R le noyau $R = \ker(N^{ab} \to \mathcal{X}_{\mathrm{L}})$ qui est sous-Δ-module de $\left(\mathcal{H}(\Delta)^{ab}\right)_{\mathcal{H}_{\mathrm{L}}}$, il vient la suite exacte longue d'homologie suivante :

$$\cdots \longrightarrow R_\Delta \longrightarrow (N^{ab})_\Delta \longrightarrow (\mathcal{X}_{\mathrm{L}})_\Delta \longrightarrow 1.$$

Or $R^{\Delta} = \{0\}$, par conséquent $R_{\Delta} = \{0\}$. Au final on obtient donc : $(N^{ab})_{\Delta} \simeq \left(\mathcal{X}_{\mathrm{L}}\right)_{\Delta} \simeq \mathcal{X}_{\mathrm{L}}$. □

Ce qui termine la preuve de la proposition 4.3.13. □

Notons que dans notre contexte, le morphisme de transfert de $\mathcal{H}_{\mathrm{L}}^{ab}$ vers $\mathcal{H}_{\mathrm{L}'}^{ab}$ correspond, via le symbole d'Artin, aux extensions des classes d'idèles et le morphisme de $\mathcal{H}_{\mathrm{L}'}^{ab}$ vers $\mathcal{H}_{\mathrm{L}}^{ab}$ à la norme arithmétique.

Définition 4.3.15. — Soit K/k une extension galoisienne de groupe de Galois Δ d'ordre premier à p. Soit S un ensemble de places de k contenant S_p. Soit $\mathcal{H}$ un sous-groupe fermé et normal de $G_{\mathrm{K},S}$ contenant $\mathcal{H}(\Delta)$. Notons par :

- $\mathrm{k}(\mathcal{H})$ la sous-extension de k_S/k fixée par $\langle \mathcal{H}, \Delta \rangle$;
- $\mathrm{E}(\mathcal{H})$ le compositum $\mathrm{Ek}(\mathcal{H})$ pour toute sous-extension galoisienne E/k de K/k.

Suivant les notations précédentes, $\mathrm{k}(\mathcal{H})$ est le corps L et $\mathrm{K}(\mathcal{H})$ le corps L′.

Définition 4.3.16. — Si S est un ensemble de places et L une sous-extension de K_S/K, notons par $\mathcal{X}_{\mathrm{L}/\mathrm{K},S}$ le pro-p-groupe abélien $\mathrm{Gal}(\mathrm{K}_S/\mathrm{L})^{ab}$.

Les résultats précédents nous permettent d'obtenir la proposition suivante :

Proposition 4.3.17. — *Soit* K/k *une extension galoisienne de groupe de Galois* Δ *d'ordre premier à* p*. Soit* S *un ensemble de places de* k *contenant* S_p*. Soit* φ *un caractère* $\mathbb{Q}_p$*-irréductible de* Δ*. Alors pour tout sous-groupe fermé distingué* $\mathcal{H}$ *de* $G_{\mathrm{K},S}$ *contenant* $\mathcal{H}(\Delta)$*, il vient :*

$$\mathcal{X}^{\varphi}_{\mathrm{K}(\mathcal{H})/\mathrm{K},S} \simeq \mathcal{X}^{\varphi'}_{\mathrm{K}(\varphi)(\mathcal{H})/\mathrm{K}(\varphi),S},$$

où φ' *est un caractère fidèle de* φ*.*

4.3.3. Sous-module libre de rang maximal. — Que peut-on faire quand les multiplicateurs de Schur ne sont pas triviaux ? Tentons de donner quelques éléments de réponse.

4.3.3.1. *Quelques situations arithmétiques.* — Fixons toujours un nombre premier $p > 2$.

Dans cette partie, nous présentons quelques pistes pour produire des situations où les extensions galoisiennes en jeu ont un sous-module libre non trivial. Plus précisément, soit L/K une extension galoisienne *finie* de corps de nombres, de groupe de Galois G. Lorsque $\mathrm{L} \subset \mathrm{K}_S$, pour S contenant l'ensemble des places au-dessus de p, nous avons donc vu comment nous assurer que $\mathcal{X}$ ait des sous-modules $\mathbb{Z}_p[G]$-libres. Mais notre méthode exclut de fait le cas du caractère trivial (dans le contexte d'une action semi-simple) et également de fait le cas où $S \cap S_p = \varnothing$ (dans ce dernier cas le pro-p-groupe $\mathcal{X}$ est fini).

Pour la suite, on note $\mathcal{X}_S^T := \mathrm{Gal}(\mathrm{L}_S^T/\mathrm{L})^{ab}$, $\mathcal{Y}_S^T := \mathbb{F}_p \otimes \mathcal{X}_S^T \simeq \mathcal{X}_S^T/\mathcal{X}_S^{T,p}$. Lorsque $T = \varnothing$, on pose $\mathcal{Y}_S^{\varnothing} = \mathcal{Y}_S$.

Dans le cas semi-simple, *i.e.* quand $p \nmid |G|$, les caractères des modules en jeu permettent de faire ressortir assez facilement des situations pour lesquelles le $\mathbb{F}[G]$-module $\mathcal{Y}_S$ contient un sous-module libre de grand rang. Nous souhaitons donc mettre de côté cette situation particulière et considérer la situation la plus générale possible (*i.e* quand les p-Sylow de G ne sont pas triviaux). Commençons par la proposition suivante.

Proposition 4.3.18. — *Soit* L/K *une extension galoisienne finie de corps de nombres. Il existe un ensemble* Θ_1 *de places de* K *de densité positive, toutes étrangères à* p*, tel que pour tout* $t \in \mathbb{N}$ *et tout sous-ensemble* $S = \{v_1, \cdots, v_t\}$*, de places de* Θ_1*, avec* $|S| = t$*, il vient le morphisme de* G*-modules :*

$$\bigoplus_{i=1}^{t} \mathbb{F}_p[G] \hookrightarrow \mathcal{Y}_S.$$

Démonstration. — Prenons tout d'abord un ensemble T de places de K tel que $G_{\mathrm{L}}^{T,ab} = \{1\}$. Alors par la proposition 2.1.1, il vient

$$G_{\mathrm{L},S}^{T,ab} \simeq \frac{\prod_{w \in S} \mathcal{U}_w}{\iota(\mathcal{E}_{\mathrm{L}}^T)}.$$

Soit ensuite l'extension galoisienne $\mathrm{L}' = \mathrm{L}(\mu_p, \sqrt[p]{E_{\mathrm{L}}^T})/\mathrm{K}$. Soit Θ_1 l'ensemble des places de K totalement décomposées dans L'/K. Par le théorème de densité de Chebotarev, l'ensemble Θ_1 est de densité positive. Pour $v \in \Theta_1$, faisons le choix d'une place $w|v$ de L'. Par abus, continuons à noter v cette place le long de l'extension L'/K. Comme $\mathrm{L}'_v = \mathrm{L}_v(\mu_p, \sqrt[p]{E_{\mathrm{L}}^T})$, il vient que toute T-unité E_{L}^T de L est une puissance p-ème localement en v dans $\mathrm{K}_v = \mathrm{L}_v$, ou encore que $\iota_v(\mathcal{E}_{\mathrm{L}}^T) \subset \mathcal{U}_v^p$. Notons au passage que pour $v \in \Theta_1$, $\mu_p(\mathrm{K}_v) \neq \{1\}$. Soit alors un ensemble $S = \{v_1, \cdots, v_t\}$ contenant t places de Θ_1. On a :

$$\mathcal{Y}_S^T \simeq \frac{\prod_{w|v\in S} \mathcal{U}_w}{\iota(\mathcal{E}_{\mathrm{L}}^T) \prod_{w|v\in S} \mathcal{U}_w^p} \simeq \prod_{w|v\in S} \mathcal{U}_w/\mathcal{U}_w^p.$$

Maintenant comme les places v de S sont totalement décomposées dans L/K, alors (se rappeler que $\mu_v(\mathrm{K}_v) \neq \{1\}$) :

$$\prod_{w|v} \mathcal{U}_w/\mathcal{U}_w^p \simeq \mathbb{F}_p[G],$$

et par conséquent,

$$\mathcal{Y}_S^T \simeq \bigoplus_{i=1}^{t} \mathbb{F}_p[G].$$

On conclut en notant que $\mathcal{Y}_S \twoheadrightarrow \mathcal{Y}_S^T$, par projectivité cela signifie que le $\mathbb{F}_p[G]$-module $\mathcal{Y}_S$ contient un sous-$\mathbb{F}_p[G]$-module libre de rang t. □

On peut retrouver la proposition 4.3.18 par une variante qui s'appuie sur le résultat suivant (voir [**16**, chap. III, 4.2.8]) :

Proposition 4.3.19. — *Soit* L/K *une extension de corps de nombres pour laquelle on suppose la conjecture de Leopoldt en p. Alors pour tout ensemble fini S de places de* K *contenant les places p-adiques, il vient :*

$$\frac{\prod_{w|v\in S} \mu_p(\mathrm{L}_w)}{\mu_p(\mathrm{L})} \hookrightarrow G_{\mathrm{L},S}^{ab}[p].$$

Ainsi, si l'on s'autorise la présence des places au-dessus de p, la conjecture de Leopoldt au niveau du corps L et la non présence de μ_p dans L, alors en utilisant un argument semblable à celui de la preuve de la proposition 4.3.18, on retrouve le résultat de la proposition en question. À noter que dans ce cas, l'ensemble de places Θ peut être pris avec une densité plus grande.

Pour être complet, citons la proposition suivante, conséquence d'un résultat de structure sur les unités dans [**22**], qui permet finalement de se passer de la conjecture de Leopoldt mais à condition de considérer une extension L/K modérément ramifiée.

Proposition 4.3.20. — *Soit* L/K *une extension de corps de nombres modérément ramifiée de groupe de Galois G. Soit* Θ_2 *l'ensemble des places de* K *totalement décomposées dans* L/K. *Supposons que* K *contient* μ_p. *Il existe une constante* $\alpha(\mathrm{L/K})$ *dépendant de* L/K *telle que pour tout ensemble fini S de places de* Θ_2, *il vient*

$$\bigoplus_{i=1}^{t} \mathbb{F}_p[G] \hookrightarrow \mathcal{Y}_\Sigma,$$

avec $t \geqslant |S| - \alpha(\mathrm{L/K})$, *où* $\Sigma = S \cup S_p$.

Démonstration. — En effet, sous les conditions de la proposition en question, Hajir et Maire montrent dans [**22**] que $\mathbb{F}_p[G]^t \hookrightarrow E_{\mathrm{L}}^S/(E_{\mathrm{L}}^S)^p$. Il suffit ensuite de considérer l'extension de Kummer $\mathrm{L}(\sqrt[p]{E_{\mathrm{L}}^S})/\mathrm{L}$: c'est une extension abélienne p-élémentaire non-ramifiée en dehors de Σ et donc un quotient de $\mathcal{Y}_\Sigma$ de structure galoisienne voulue. Comme précédemment, on conclut par un argument de projectivité. □

Remarque 4.3.21. — À noter que l'ensemble Θ_2 de la proposition 4.3.20 est de plus grande densité que l'ensemble Θ_1 de la proposition 4.3.18.

4.3.3.2. *Une approche algébrique.* — Le résultat de structure sur les unités de [**22**] repose sur une approche algébrique. Rappelons celle-ci. Soit donc G un groupe fini. L'algèbre $\mathbb{F}_p[G]$ est une algèbre de Frobenius ; c'est de plus un anneau local si G est un p-groupe. Ainsi tout sous-module libre M_0 d'un $\mathbb{F}_p[G]$-module de type fini M est en somme directe dans M et par conséquent tout $\mathbb{F}_p[G]$-module M de type fini admet en facteur direct un sous-module libre (de rang maximal) : il existe un entier t tel que

$$M = \mathbb{F}_p[G]^t \oplus N,$$

où N est de torsion (pour tout $x \in N$, il existe $\lambda \in \mathbb{F}_p[G]$, $\lambda \neq 0$, tel que $\lambda \cdot x = 0$). Par le théorème de Krull-Schmidt, l'entier t est unique.

Remarque 4.3.22. — Si M est $\mathbb{F}_p[G]$-libre, c'est-à-dire si $N = 0$, alors $M^G \simeq \mathbb{F}_p^t$ et l'entier t vérifie la relation : $t = d_pM - (|G| - 1) \cdot d_pM^G$.

On trouve dans un travail de Ozaki [**44**] :

Proposition 4.3.23. — *Soit M un $\mathbb{F}_p[G]$-module de type fini. Ecrivons $M = \mathbb{F}_p[G]^t \oplus N$, avec N de torsion. Alors*

$$t \geqslant d_pM - \big(|G| - 1\big) \cdot d_pM^G.$$

Revenons au contexte de la section 4.1 en tentant d'appliquer le principe ci-dessus.

Plus précisément, soit G un quotient $\mathcal{G}_\Delta = \mathcal{G}/\mathcal{H}(\Delta)$; soit $\mathcal{H}$ le sous-groupe normal de $\mathcal{G}$ tel que $G = \mathcal{G}/\mathcal{H}$. Soit φ un caractère $\mathbb{Q}_p$-irréductible de Δ. On note $\mathcal{Z}$ la φ-composante de $\mathcal{Y} = \mathcal{H}^{ab} \otimes \mathbb{F}_p$.

Soit $(H_n)_n$ une suite décroissante de sous-groupes ouverts de G que l'on suppose être une base de voisinage ; posons $G_n = G/H_n$ et soit $\mathcal{G}_n$ le sous-groupe ouvert de $\mathcal{G}$ correspond au quotient G_n, *i.*e. $\mathcal{G}/\mathcal{G}_n \simeq G_n$. Soit $\mathcal{Z}_n$ la φ-composante de $\mathcal{Y}_n = \mathcal{X}_n \otimes \mathbb{F}_p$, où $\mathcal{X}_n = \mathcal{G}_n^{ab}$. Ecrivons $\mathcal{Z}_n = \mathbb{F}[G_n]^{t_n} \oplus N_n$.

Lemme 4.3.24. — *Supposons $\varphi \neq \mathbb{1}$. Alors la suite $(t_n)_n$ est décroissante.*

Démonstration. — D'après la proposition 4.1.7, on a $(\mathcal{Z}_{n+1})_{H_n/H_{n+1}} \simeq \mathcal{Z}_n$. Comme $\mathbb{F}_p[G_{n+1}]_{H_n/H_{n+1}} \simeq \mathbb{F}_p[G_n]$ (voir par exemple [**29**, th. 7.2]), on a

$$(\mathcal{Z}_{n+1})_{H_n/H_{n+1}} \simeq \big(\mathbb{F}_p[G_{n+1}]^{t_{n+1}}\big)_{H_n/H_{n+1}} \oplus (N_{n+1})_{H_n/H_{n+1}} \simeq \mathbb{F}_p[G_n]^{t_{n+1}} \oplus (N_{n+1})_{H_n/H_{n+1}},$$

et par conséquent $t_{n+1} \leqslant t_n$. □

Il existe ainsi n_0 tel que pour tout $n \geqslant n_0$, $t_n = t_{n_0} := t$. Remarquons ensuite que pour tout caractère non trivial φ, il vient $\mathcal{Z}_n = \mathcal{Z}_{H_n}$. D'autre part pour $n \geqslant n_0$, $\mathcal{Z}_{H_n}$ contient un sous-module libre $\mathbb{F}_p[G_n]^t$ de rang constant t. Par conséquent, on obtient deux systèmes projectifs dont les applications sont les morphismes de restriction vérifiant $\mathbb{F}_p[\![G]\!] = \varprojlim_n \mathbb{F}_p[G_n]$ et $\mathcal{Z} = \varprojlim_n \mathcal{Z}_{H_n}$, par le choix de la suite $(H_n)_n$. Cela montre que $\mathcal{Z}$ contient, en somme directe, un sous-module libre $\mathbb{F}_p[\![G]\!]^t$ de rang t.

Il serait alors intéressant de trouver des situations arithmétiques *infinies* faisant apparaître des extensions galoisiennes avec des sous-modules libres non triviaux à tout étage fini afin de produire des $\mathbb{F}_p[\![G]\!]$-modules libres de rang $t \geqslant 1$.

4.4. Études statistiques

On se propose de faire quelques simulations statistiques dans des familles de corps cubiques cycliques de $\mathbb{Q}$, dans des familles d'extensions diédrales d'ordre 6 et dans des familles d'extensions cycliques de degré 4. On prend toujours $p > 2$ par confort, et même $p > 3$ pour les extensions de degré 3 et de degré 6 pour une raison de semi-simplicité. On suppose la conjecture de Leopoldt vraie dans les extensions en jeu. Notre étude est concentrée sur les nombres premiers p non exceptionnels, c'est-à-dire ceux qui ne divisent pas $|\mathrm{Cl}(\mathrm{K})|$, et l'objet arithmétique à calculer est la φ-partie du régulateur normalisé, *i.e.* la φ-partie de la $\mathbb{Z}_p$-torsion du quotient $\prod_{v|p} \mathcal{U}_v/\iota(\mathcal{E}_\mathrm{K})$ (ici, dans les cas étudiés, on a pour tout $v|p$, $\mu_p(\mathrm{K}_v) = \{1\}$).

4.4.1. Extensions cubiques cycliques. — Considérons un polynôme P de degré 3 irréductible sur $\mathbb{Q}$. On suppose que P définit un corps cubique cyclique totalement réel que l'on note K. Le groupe $\Delta = \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ étant d'ordre 3, il admet trois caractères $\mathbb{C}_p$-irréductibles : le caractère trivial $\mathbb{1}$ et deux caractères conjugués φ et φ^2. La représentation de degré 2 de Δ de caractère $\varphi + \varphi^2$ est donnée par

$$\rho(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

où σ est un générateur de Δ fixé. On fait le choix pour la suite d'ordonner les racines de P par ordre croissant : $\varepsilon_1 < \varepsilon_2 < \varepsilon_3$, et de prendre pour générateur du groupe Δ le morphisme σ défini par $\sigma(\varepsilon_1) = \varepsilon_2$ et $\sigma(\varepsilon_2) = \varepsilon_3$.

On va utiliser les corollaires 4.3.4 et 4.3.5, redonnons le contexte. On prend S un ensemble fini de nombres premiers de $\mathbb{Z}$, tous congrus à 1 modulo p, et tous inertes dans $\mathrm{K}/\mathbb{Q}$, auquel on ajoute le nombre premier p : ainsi $S_p \subset S$. Puis on pose $\mathcal{G} = G_{\mathrm{K},S}$. On rappelle alors que $\mathcal{G}_\Delta \simeq G_{\mathbb{Q},S}$ et qu'ici $G_{\mathbb{Q},S} \simeq \mathbb{Z}_p$ si et seulement si $S = S_p$. Rappelons que la conjecture de Leopoldt est vérifiée au niveau du corps K (et aussi, pour $S = S_p$, le long du compositum abélien $\mathbb{Q}_S\mathrm{K}$). Remarquons que le groupe $G_{\mathbb{Q},S}$ n'est pas p-adique analytique pour S assez grand. On prend $\mathcal{H} = \mathcal{H}(\Delta) = \mathrm{Gal}(\mathrm{K}/\mathbb{Q}_S\mathrm{K})$, puis $\mathcal{X} = \mathcal{H}^{ab}$.

La proposition 4.1.6 règle le cas du caractère trivial puisque $\mathcal{X}^{\mathbb{1}} = 0$. Occupons nous des composantes $\mathcal{X}^{\varphi}$ et $\mathcal{X}^{\varphi^2}$.

Soit un nombre premier p non exceptionnel (ou encore tel que $p \nmid |\mathrm{Cl}(\mathrm{K})|$), il vient d'après le corollaire 2.1.2

$$G_{\mathrm{K},S}^{ab} \simeq \frac{\prod_{v|p} \mathcal{U}_v \prod_{v|\ell,\ell\in S-S_p} \mathcal{U}_v}{\iota(\mathcal{E}_\mathrm{K})},$$

où ι est le plongement diagonal sous-jacent. Par le choix des nombres premiers ℓ, l'action de σ sur $\prod_{v|\ell,\ell\in S-S_p} \mathcal{U}_v$ est triviale et il vient ainsi

$$\mathrm{Tor}_{\mathbb{Z}_p}(G_{S,\mathrm{K}}^{ab})^{\varphi} \simeq \mathrm{Tor}_{\mathbb{Z}_p}\Big(\frac{\big(\prod_{v|p}\mathcal{U}_v\big)^{\varphi}}{\iota(\mathcal{E}_\mathrm{K}^{\varphi})}\Big);$$

il en est de même pour φ^2.

On a vu au début de la section 4.3.2 que si les racines de P engendrent le groupe des unités de l'anneau des entiers de K (ou si l'on peut s'assurer qu'elles engendrent un sous-module d'indice fini de E_K), on peut déterminer si la φ-composante $\mathcal{X}^{\varphi}$ est libre ou non en testant une condition de congruence (que l'on détaillera). Nous avons donc besoin, pour effectuer des calculs dans un contexte favorable, que les racines du polynôme P engendrent E_K. C'est à ce niveau que l'on va utiliser des familles de polynômes bien particuliers.

Balady, dans [**2**], donne plusieurs familles de polynômes qui généralisent celles de Kishi [**28**] et qui vérifient la condition cherchée. Ils sont construits de la manière suivante : on se donne f et g deux polynômes à coefficients entiers et on pose

$$\lambda = \big(f^3 + g^3 + 1\big)/fg,$$

et

$$a = 3\big(f^2 + g^2 - fg\big) - \lambda\big(f + g\big).$$

Soit alors la famille de polynômes $P_n = X^3 + a(n)X^2 + \lambda(n)X - 1, n \in \mathbb{Z}$. Balady montre que sous les hypothèses :

(i) λ est un polynôme à coefficients entiers,
(ii) $n \neq -1$,
(iii) $3a(n) + \lambda(n)^2$ est sans facteurs carrés,

les polynômes P_n déterminent des corps cubiques totalement réels K_n (noté également K) dont le p-tensorisé $\mathcal{E}_{\mathrm{K}_n} := \mathbb{Z}_p \otimes E_{\mathrm{K}_n}^{\times}$ du groupe des unités est engendré par les p-tensorisés des racines de P_n (et ce pour tout nombre premier p).

Remarque 4.4.1. — Les familles obtenues à partir de deux couples (f,g) et (f',g') distincts ne sont pas nécessairement disjointes l'une de l'autre.

Rappelons comment on peut exprimer les racines de P entre elles. Le changement de variable classique $Y = X - \frac{a}{3}$ permet de ramener l'étude au polynôme $\tilde{P} = Y^3 + pY + q$, où les constantes p et q sont données par

$$p = \lambda - \frac{a^2}{3}, \qquad q = \frac{2a^3}{27} - \frac{a\lambda}{3} - 1.$$

Notons α, β et γ les trois racines de $\tilde{P}$. On a alors les relations

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta\gamma = -q, \quad p + a^2 = \frac{-q}{a}.$$

En notant $\delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$ (de sorte que $\delta^2 = \mathrm{disc}(\tilde{P}) = 4p^3 + 27q^2$), on a

$$2\beta + \alpha = \beta - \gamma = \frac{\delta}{(\alpha-\beta)(\gamma-\alpha)}.$$

D'autre part,

$$-(\alpha-\beta)(\gamma-\alpha) = \alpha^2 - \alpha(\beta+\gamma) + \beta\gamma = 2\alpha^2 - \frac{q}{\alpha} = 3\alpha^2 + p.$$

Finalement,

$$\beta = \frac{1}{2}\left(\frac{-\delta}{3\alpha^2+p} - \alpha\right) = \frac{1}{2}\left(-\delta\left(\frac{6p}{\delta^2}\alpha^2 - \frac{9q}{\delta^2}\alpha + \frac{4p^2}{\delta^2}\right) - \alpha\right),$$

et on obtient de même une expression de la troisième racine γ de $\tilde{P}$ en une fonction polynomiale en α. En notant x une racine quelconque de P, l'ensemble des racines de P est donc donné par

$$\left\{x, \pm\frac{1}{2}\left(\frac{6p}{\delta}(x+\frac{a}{3})^2 - \frac{9q}{\delta}(x+\frac{a}{3}) + \frac{4p^2}{\delta}\right) - \frac{1}{2}(x+\frac{a}{3}) - \frac{a}{3}\right\}. \tag{16}$$

Notons que dans ces expressions, les dénominateurs des coefficients sont divisibles par 2, 3 et par les diviseurs du discriminant $\mathrm{disc}(P)$ de P : ceci aura son importance pour nos calculs.

4.4.1.1. *Quand* 3 *divise* $p-1$. — Supposons que $p \equiv 1 \pmod 3$. Les caractères φ et φ^2 sont alors définis sur $\mathbb{Q}_p$. Soit $a \in \mathbb{F}_p^\times$ une racine primitive cubique de l'unité, $1 < a < p-1$. Par le lemme de Hensel, a se relève dans $\mathbb{Z}_p$ en une unique racine primitive cubique ζ de 1 caractérisée par la relation $\zeta \equiv a \pmod p$. On fixe pour la suite φ le caractère associé à ζ : $\varphi(\sigma) = \zeta$. Un rapide calcul donne les vecteurs propres u_φ et u_{φ^2} de $\rho(\sigma)$ pour les valeurs propres ζ et ζ^2 :

$$u_\varphi = \varepsilon_1 \varepsilon_2^{-\zeta} \quad \text{et} \quad u_{\varphi^2} = \varepsilon_1 \varepsilon_2^{-\zeta^2}.$$

Il vient ainsi $\mathcal{E}_\mathrm{K}^\varphi = \langle u_\varphi \rangle$ et $\mathcal{E}_\mathrm{K}^{\varphi^2} = \langle u_{\varphi^2} \rangle$. On retrouve le résultat annoncé par le théorème de Dirichlet galoisien, à savoir que $\mathcal{E}_\mathrm{K}$ a pour caractère $\varphi + \varphi^2$. En conclusion :

$$\mathrm{Tor}_{\mathbb{Z}_p}(G_{S,\mathrm{K}}^{ab})^\varphi \simeq \mathrm{Tor}_{\mathbb{Z}_p}\Big(\frac{(\prod_{w\in S_p}\mathcal{U}_w)^\varphi}{\langle \iota(u_\varphi)\rangle}\Big).$$

Supposons maintenant le nombre premier p inerte ou décomposé dans $\mathrm{K}/\mathbb{Q}$. Soit $w|p$ une place de K. Alors le logarithme p-adique apporte un isomorphisme topologique entre le groupe des unités principales $\mathcal{U}_w^1$ et $\pi_w\mathcal{O}_w$, où ici $\mathcal{O}_w$ désigne l'anneau des entiers p-adique de K_w. En particulier, $x \in \mathcal{U}_w^p$ si et seulement si $x - 1 \equiv 0 \pmod{\pi_v^2}$, où π_w est une uniformisante de K_w. Posons

$$a_p = \begin{cases} p-1 & \text{si } p \text{ est décomposé,} \\ p^3-1 & \text{si } p \text{ est inerte.} \end{cases}$$

Alors $\mathrm{Tor}_{\mathbb{Z}_p}(G_{S,\mathrm{K}}^{ab})^\varphi \neq \{1\}$ si et seulement si $u_\varphi^{a_p} \in \mathcal{U}_w^p$ pour toute place $w \in S_p$, ou encore si et seulement si $u_\varphi^{a_p} - 1 \equiv 0 \pmod{\pi_w^2}$ pour toute place $w \in S_p$, ce qui se traduit par :

$$u_\varphi^{a_p} \equiv 1 \pmod{p^2}.$$

En conclusion, d'après le théorème 4.1.13, la φ-composante $\mathcal{X}^{\varphi}$ est libre, en fait triviale ici, si et seulement si

$$\left(\varepsilon_1\varepsilon_2^{-a}\right)^{a_p} - 1 \not\equiv 0 \pmod{p^2}.$$

En utilisant (16), on voit que l'on peut donc facilement vérifier si les φ-composantes $\mathcal{X}^{\varphi}$ et $\mathcal{X}^{\varphi^2}$ sont libres (*i*.e. triviales) ou non, par de simples calculs de congruences dans $\mathbb{Z}$.

Pour terminer, faisons la remarque suivante qui sera de grande utilité pour le cas où 3 ne divise pas $p-1$: les modules $\mathcal{X}^{\varphi}$ et $\mathcal{X}^{\varphi^2}$ sont simultanément non triviaux si et seulement si $\left(\varepsilon_1^2\varepsilon_2\right)^{a_p} \in \mathcal{U}_w^p$, pour toute place $w|p$. En effet, si les composantes ne sont pas triviales, cela signifie que la torsion sur φ et φ^2 n'est pas triviale, et donc que $u_{\varphi}^{a_p}$ et $u_{\varphi^2}^{a_p}$ sont des puissances p-èmes dans tous les complétés $\mathcal{U}_w$, $w|p$, ce qui implique facilement que $\left(\varepsilon_1^2\varepsilon_2\right)^{a_p}$ est lui-même une puissance p-ème localement pour tout $w|p$. Réciproquement, si $\left(\varepsilon_1^2\varepsilon_2\right)^{a_p} \in \mathcal{U}_w^p$ pour tout $w|p$ alors la torsion de $G_{\mathrm{K},S}^{ab}$ n'est pas triviale, ce qui signifie qu'au moins une de ses composantes en φ et φ^2 ne l'est pas non plus, par exemple φ, et la relation sur $\varepsilon_1^2\varepsilon_2$ implique que l'autre composante ne l'est pas non plus !

• Prenons la famille de polynômes P_n donnée par Balady et rappelée au début de cette section, avec $f(n) = -n^2$ et $g(n) = n^3 - 1$ pour $n \in \mathbb{Z}$. On se propose ici de tester, grâce à PARI/GP, la liberté des φ-composantes de $\mathcal{X}$. Comme expliqué plus haut, la condition testée est en fait une congruence ; le programme est donc plutôt simple.

À n fixé, les formules données en début de section donnent l'expression de la racine ε_2 en fonction de ε_1 (on suppose ici qu'on les a ordonnées par ordre croissant). On note R le couple $[\varepsilon_1, \varepsilon_2]$. Pour un premier p donné, il suffit alors de considérer un relèvement a d'une racine primitive cubique mod p puis de calculer les congruences. Rappelons ici une remarque faite plus haut : les dénominateurs des coefficients intervenant dans les expressions des racines ε_1 et ε_2 sont divisibles par 2, 3 et par les diviseurs du discriminant du polynôme P_n. Il faut donc écarter ces nombres premiers, pour lesquels ε_2 ne sera pas inversible.

Le code `torsionZ3` détaillé en appendice B.1 renvoie alors un couple $[T1, T2]$, où chacune des composante est 0 ou 1 suivant si la φ-composante associée est libre ou non. Attention cependant : pour tirer cette conclusion, il faut que le théorème 4.1.13 s'applique, et donc que le premier p ne soit pas exceptionnel (ou encore qu'il ne divise pas le nombre de classes du corps K_n).

Afin de réduire au maximum les temps de calcul, la liste des relèvements des racines cubique modulo p pour tous les premiers inférieurs à une certaine borne (15×10^7 pour nous) est calculée à part. Lorsque, à n fixé, nous faisons varier p de 1 à 10^6, cette stratégie nous permet de diviser le temps de calcul par plus de 60 ; ou encore de faire varier à la fois p de 1 à 10^6 et n de 1 à 100 dans le temps nécessaire au même calcul pour une seule valeur de n.

On désigne respectivement par $\mathcal{D}_{\mathrm{disc}}$ et $\mathcal{D}_{Cl}$ l'ensemble des diviseurs du discriminant du polynôme P et du nombre de classes du corps K. On note pour la suite $\mathbb{P}$ ($= \mathbb{P}_{\mathrm{K}}$) l'ensemble des nombres premiers p vérifiant

(i) $p \equiv 1 (\mathrm{mod}\ 3)$,
(ii) $p \notin \mathcal{D}_{\mathrm{disc}} \cup \mathcal{D}_{Cl}$.

Posons alors pour la borne $X \geqslant 0$ l'ensemble

$$\mathcal{A}_{nl} := \mathcal{A}_{nl}(X) = \{p \leqslant X,\ p \in \mathbb{P},\ \mathcal{X}^{\varphi} \text{ ou } \mathcal{X}^{\varphi^2} \text{ non libre}\}.$$

On a vu que tout caractère irréductible φ de Δ peut être représenté par un entier a : $\varphi(\sigma) = \zeta$ avec $\zeta \equiv a (\mathrm{mod}\ p)$, en respectant le choix de σ et en ordonnant les unités ε_i par ordre croissant. Pour un nombre premier $p \in \mathcal{A}_{nl}$, on renseignera en indice l'entier a associé à la composante non-libre.

Pour $X = 8 \times 10^7$, on obtient par exemple :

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{A}_{nl}(15\times10^7)$
1	$\{19\}$	$\varnothing$	$\{67_{29^2}, 193_{84}, 337_{128^2}, 7321_{308^2}\}$
2	$\{11, 13, 79\}$	$\{3\}$	$\{19_{7^2}, 439_{171}, 2887_{698^2}, 59060857_{26994113}\}$

Le tableau en annexe B.1.1 donne les résultats obtenus pour $X = 15\times10^7$ et $n \leqslant 100$. On observe très peu de couples (n,p) pour lesquels une des φ-composantes est non-libre. Notons que parmi ces rares cas, on n'a aucun exemple où les deux composantes ne sont pas libres (simultanément).

Dans ces calculs, à n fixé, deux ensembles de premiers sont exclus : pour une raison purement calculatoire, l'ensemble $\mathcal{D}_{disc}$ constitué des premiers divisant le discriminant du polynôme P (en particulier les premiers ramifiés dans $\mathrm{K}/\mathbb{Q}$) et dans l'esprit du corollaire 2.1.2, l'ensemble des premiers exceptionnels $\mathcal{D}_{Cl}$, *i.e.* l'ensemble des premiers qui divisent le nombre de classes du corps K. Il est néanmoins possible de faire le calcul différemment et de conclure pour ces deux ensembles grâce aux algorithmes de Gras [**14**] et Pitoun-Varescon [**47**]. En effet, notre hypothèse sur l'ensemble S fait que tout se passe au niveau des complétés p-adiques et ainsi, finalement, tester la liberté des composantes de $\mathcal{X}$ équivaut à tester la p-rationalité du corps K (ce que testent ces algorithmes) : le défaut de non rationalité de K est localisé en φ ou/et φ^2 (car $\mathbb{Q}$ est p-rationnel).

Commençons par les premiers $p \in \mathcal{D}_{disc}\backslash\mathcal{D}_{Cl}$. Le résultat est alors immédiat : dans les intervalles étudiés ($X \leqslant 15\times10^7$ et $n \leqslant 100$), les corps sont p-rationnels.

Pour les premiers $p \in \mathcal{D}_{Cl}$, on ne trouve aucun corps p-rationnel. Concentrons-nous sur la trivialité du régulateur normalisé (on rappelle que l'on suppose $p \neq 3$ par semi-simplicité) :

- (i) Quand p n'est pas ramifié dans $\mathrm{K}/\mathbb{Q}$, le régulateur normalisé est non-trivial uniquement lorsque : $(n,p) \in \{(11,7)_4, (16,7)_4, (17,7)_{4^2}, (49,7)_4, (67,7)_4\}$. À noter que $d_p\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}_{\mathrm{K},S_p} = 1$ pour $(11,7)$ et $(67,7)$, et que $d_p\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}_{\mathrm{K},S_p} = 2$ pour les couples $(16,7)$, $(17,7)$ et $(49,7)$. Ainsi en dehors de ces cas, le défaut de non-liberté de $\mathcal{X}^{\varphi}$ est donné par le groupe des classes de K.
- (ii) Quand p est ramifié : la congruence à tester est de la forme $(\varepsilon_1\varepsilon_2^a)^{p-1} \equiv 1 (\mathrm{mod}\ \pi_v^4)$. Le régulateur normalisé est trivial dans tous les cas.

• Prenons maintenant la famille de Lecacheux [**33**], que l'on retrouve à partir des polynômes de Balady pour $f = -1$ et $g = -n$. Avec les mêmes notations que précédemment, toujours pour $X = 15\times10^7$, on obtient par exemple :

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{A}_{nl}(15\times10^7)$
14	$\{13, 157, 199\}$	$\{3, 13\}$	$\{43_{6^2}, 397849_{136077^2}\}$
16	$\{3, 5, 7, 37, 211\}$	$\{3, 43\}$	$\{62347_{4200^2}\}$

Les tableaux en annexe B.1.2 donnent les résultats obtenus pour $X = 15\times10^7$ avec tous les polynômes de Lecacheux de paramètre $n \leqslant 100$.

Là encore, on traite à part en utilisant l'algorithme de Pitoun-Varescon les premiers de $\mathcal{D}_{disc}$ et de $\mathcal{D}_{Cl}$. Dans les intervalles étudiés, pour chaque premier $p \in \mathcal{D}_{disc}\backslash\mathcal{D}_{Cl}$, le corps est p-rationnel, à l'exception des trois situations suivantes : $n = 50$, $n = 62$ et $n = 76$ pour le nombre premier $p = 7$. On peut alors faire le calcul directement dans le corps de nombres pour déterminer quelle φ-composante est non-libre. On voit ainsi que pour $n = 62$ et $n = 76$, la composante $\mathcal{X}^{\varphi}$ est non-libre pour φ donné par la racine cubique 4 mod 7. Détaillons le cas $n = 50$: on se place donc dans le corps engendré par le polynôme P_{50} pour $f = -1$ et $g = -50$. D'après l'algorithme de Pitoun-Varescon, ce corps n'est pas 7-rationnel ; pour la suite de cet exemple, on prend $p = 7$. On rappelle que pour φ un caractère irréductible non trivial de Δ, la φ-composante du module $\mathcal{X}$ est non-libre si et seulement si la $\mathbb{Z}_p$-torsion du quotient $\big(\prod_{w|p}\mathcal{U}_w\big)^{\varphi}/\langle\iota(u_\varphi)\rangle$ est non-triviale, c'est-à-dire si la valuation $v_{\mathfrak{p}_i}(u_\varphi^{a_p} - 1)$ est supérieure ou égale à 2

pour tout premier $\mathfrak{p}_i$ de K divisant p. Ici, p est décomposé dans le corps K et 4 est une racine cubique modulo 7. On a donc

$$u_{\varphi}^{a_p} = (\varepsilon_1 \varepsilon_2^{-4})^6 \quad \text{et} \quad u_{\varphi^2}^{a_p} = (\varepsilon_1 \varepsilon_2^{-16})^6.$$

Un rapide calcul avec PARI/GP donne de plus $\varepsilon_2 = -2451\varepsilon_1^2/49 + 6009802\varepsilon_1 + 6007352/49$ puis, grâce à la fonction `idealval`, on voit qu'aucune des composantes $\mathcal{X}^{\varphi}$ et $\mathcal{X}^{\varphi^2}$ n'est libre. Sur tous les exemples étudiés jusqu'à présent, c'est le seul cas où les deux composantes non triviales sont simultanément non-libres.

Pour $p \in \mathcal{D}_{Cl}$, aucun corps n'est p-rationnel dans les intervalles étudiés. En revanche, les seules situations où le régulateur normalisé est non-trivial sont les suivantes : $(n,p) \in \{(34,7)_4, (68,13)_{3^2}, (98,7)_4\}$, où le couple $(34,7)$ correspond à un premier ramifié.

Faisons ici quelques remarques sur les algorithmes de Pitoun-Varescon et de Gras. Comme on l'a expliqué plus tôt, ces algorithmes déterminent le module de torsion $\mathrm{Tor}_{\mathbb{Z}_p} G_{S_p}^{ab}$, testant ainsi si un corps donné est, ou non, p-rationnel pour un premier p fixé. Nous avons choisi pour nos calculs d'utiliser d'abord notre code, puis de traiter les cas particulier avec l'algorithme de Pitoun-Varescon. L'inverse aurait été possible : nous aurions déterminé pour chaque corps non p-rationnel la ou les composantes apportant de la torsion grâce à notre code. Une des différences majeures entre les deux algorithmes est l'utilisation de fonctions "lourdes" associées à la théorie du corps de classes. Nous calculons ici le corps de classes de K_n pour obtenir son nombre de classes mais, à n fixé, on peut faire varier p et ne plus calculer que des congruences alors que l'algorithme de Pitoun-Varescon nécessite le calcul d'un corps de classes de rayon pour chaque premier p, ce qui prend plus de temps. À titre de comparaison, voici les temps mis par les deux programmes pour le polynôme $P = X^3 + 309X^2 - 10X - 1$ (polynôme de Balady, $n = 2$) lorsque l'on fait varier le premier p de 1 à 10^6 : on obtient la liste des corps non p-rationnels en plus d'une heure, alors que notre algorithme renvoie la liste des composantes non-libres en 4.808ms (en calculant les racines cubiques au préalable). Pour être complet, notons que sur cet exemple l'algorithme de Gras est plus rapide que celui de Pitoun-Varescon (un peu moins d'une heure).

4.4.1.2. *Quand* 3 *ne divise pas* $p-1$. — On note toujours φ le caractère associé à ζ. Cette fois-ci les caractères φ et φ^2 sont définis sur $\mathbb{Q}_p(\zeta)$ et Δ a deux caractères $\mathbb{Q}_p$-irréductibles : le caractère trivial, et le caractère $\varphi + \varphi^2$ de degré 2. Un raisonnement identique à celui effectué dans le cas précédent montre qu'il suffit de regarder si $\left(\varepsilon_1^2 \varepsilon_2\right)^{a_p}$ est une puissance p-ème dans tous les complétés $\mathcal{U}_v$, $v|p$, ou encore tester la condition

$$\left(\varepsilon_1^2 \varepsilon_2\right)^{a_p} - 1 \equiv 0 \pmod{p^2}.$$

• Pour $f = -x^2$, $g = x^3 - 1$, pour n allant de 1 à 100, on trouve 51 polynômes vérifiant les conditions de Balady. Pour $p < 10^9$, les seuls cas non-libres trouvés sont :

- $n = 1, p = 3$ (inerte) ;
- $n = 62, p = 23$ (décomposé).

• Pour $f = -1$, $g = -x$, pour n allant de 1 à 100, on trouve 25 polynômes vérifiant les conditions de Balady. Pour $p < 10^9$, les seuls cas non-libres trouvés sont :

- $n = 38, p = 5$ (inerte) ;
- $n = 88, p = 5$ (inerte).

Ici encore l'algorithme de Pitoun-Varescon permet d'étudier la liberté des φ-composantes pour chaque valeur de $p \in \mathcal{D}_{disc} \cup \mathcal{D}_{Cl}$. Dans le cas des polynômes de Balady, tous les corps sont p-rationnels (pour $p > 3$), donc toutes les composantes restantes sont en fait libres. Parmi les corps engendrés par les polynômes de Lecacheux, aucun n'est 3-rationnel, mais pour des raisons de semi-simplicité, nous passons sur ces cas. On trouve seulement deux autres cas où le corps n'est pas p-rationnel pour lesquels un calcul dans le corps de nombres permet de conclure : pour $(n,p) \in \{(26,5),(76,5)\}$, la $(\varphi + \varphi^2)$-composante de $\mathcal{X}$ n'est pas libre. Pour ces deux cas, $p \in \mathcal{D}_{disc} \backslash \mathcal{D}_{\mathrm{Cl}}$.

4.4.2. Extensions diédrales. — Focalisons-nous sur la famille $P_n = X^3 + nX + 1$, $n \in \mathbb{N}^*$, abordée dans [**37**]. Notons par $d_n = -4n^3 - 27 < 0$ le discriminant du polynôme P_n que l'on suppose sans facteurs carrés ; par [**11**], on sait que les entiers n vérifiant cette condition sont de densité positive. Soit le corps quadratique imaginaire $\mathrm{F}_n = \mathbb{Q}(\sqrt{d_n})$. On note ε une racine réelle de P_n et on note K_n le corps $\mathbb{Q}(\sqrt{d_n}, \varepsilon)$; K_n est le corps de décomposition de P_n.

Remarque 4.4.2. — Si l'on fait le choix d'un polynôme cubique de discriminant positif, la situation ressemble fortement à celle de la section précédente.

Cette fois-ci le corps de décomposition $\mathrm{K} = \mathrm{K}_n$ de P_n est de groupe de Galois isomorphe à S_3. Posons $\Delta = \mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \langle s, t, s^2 = 1, t^3 = 1, sts = t^{-1} \rangle$. Le groupe Δ a deux représentations $\mathbb{Q}_p$-irréductibles de degré 1 (la représentation triviale $\mathbb{1}$ et la représentation ψ définie par $\psi(s) = -1$ et $\psi(t) = 1$), et une représentation $\mathbb{Q}_p$-irréductible φ de degré 2.

Prenons p générique : p ne divise pas $|\mathrm{Cl}_\mathrm{K}|$, et pour $v|p$, $\mu_p(\mathrm{K}_v) = \{1\}$. Le $\mathbb{Z}_p[\Delta]$-module $\prod_{w|p} \mathcal{U}_w$ a pour caractère $\mathrm{Rg} = \mathbb{1} + \psi + 2\varphi$. Quant au p-tensorisé des unités $\mathcal{E}_\mathrm{K}$ de K, il a pour caractère φ.

Prenons ensuite un ensemble fini S constitué de nombres premiers ℓ tous congrus à 1 modulo p et tels que P_n est irréductible modulo ℓ, auquel on ajoute p. Rappelons que pour S assez grand, le groupe $G_{\mathbb{Q},S}$ n'est pas p-adique analytique. Comme dans la section précédente, on pose $\mathcal{H} = \mathcal{H}(\Delta) = \mathrm{Gal}(\mathrm{K}_S/\mathbb{Q}_S\mathrm{K})$, puis $\mathcal{X} = \mathcal{H}^{ab}$. On cherche donc à déterminer la liberté du $\mathbb{Z}_p[\![G_{\mathbb{Q},S}]\!]$-module $\mathcal{X}$. Comme précédemment, $\mathcal{X}^{\mathbb{1}} = \{1\}$.

Pour $\ell \in S \backslash S_p$, l'action de Δ sur $\prod_{w|\ell} \mathcal{U}_w$ a pour caractère $\mathbb{1} + \psi$ (ici $\chi_{D_v}^{\Delta} = \mathrm{Ind}_{\langle t \rangle}^{\Delta} \mu_{p^\infty}(\mathrm{K}_w)$). Par conséquent la composante $(G_{S,\mathrm{K}}^{ab})^\psi$ est $\mathbb{Z}_p$-libre si et seulement si $S = S_p$ et dans ce cas, $\mathcal{X}^\psi = \{1\}$.

La situation intéressante se trouve donc dans l'étude de $\mathcal{X}^\varphi$. Pour $\ell \in S \backslash S_p$, $(\prod_{w|\ell} \mathcal{U}_w)^\varphi = \{1\}$, on est donc dans le cadre du corollaire 4.3.4. Ainsi, si $\mathcal{X}^\varphi$ est $\mathbb{Z}_p[\![G_{\mathbb{Q},S}]\!]$-libre, alors il est libre de rang 2 (ou de φ-rang 1).

Notons par $\Delta_0 = \langle t \rangle$ le sous-groupe cyclique de Δ d'ordre 3. Alors $\varphi_{|\Delta_0} = \varphi' + (\varphi')^2$, où φ' est un des deux caractères non triviaux de Δ_0. On va alors s'appuyer sur les calculs de la situation précédente pour déterminer si $\mathcal{X}^\varphi$ est libre ou non. Notons qu'ici, $\mathcal{X}^{\varphi'}$ est $\mathbb{Z}_p[\![G_{\mathrm{F},S}]\!]$-libre si et seulement si $\mathcal{X}^{(\varphi')^2}$ est $\mathbb{Z}_p[\![G_{\mathrm{F},S}]\!]$-libre.

Notons ε_2 une seconde racine de P_n (distincte de ε). L'étude de l'extension cubique $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ permet de montrer que $\{\varepsilon, \varepsilon_2\}$ forme une $\mathbb{Z}_p$-base des unités de K_n. En effet, dans [**37**], Maire utilise les estimations données par Cusick dans [**8**] pour minorer le régulateur du corps $\mathbb{Q}(\varepsilon)$. Il montre ainsi que le sous groupe $< \pm\varepsilon >$ est d'indice 1 dans $E_{\mathbb{Q}(\varepsilon)}$, en d'autres termes que ε est une unité fondamentale de $\mathbb{Q}(\varepsilon)$. Un raisonnement sur les normes lui permet ensuite de montrer que $\{\varepsilon, \varepsilon_2\}$ forme une $\mathbb{Z}_p$-base des unités de K_n. Ainsi, suivant les calculs de la situation précédente, il nous faut simplement tester la condition

$$\left(\varepsilon\varepsilon_2^2\right)^{a_p} \equiv 1 \pmod{p^2},$$

où comme précédemment, $a_p = p^{f_p} - 1$, f_p étant le degré résiduel de p dans $\mathrm{K}_n/\mathbb{Q}$: $f_p = 1$ si P_n est scindé modulo p, $f_p = 3$ si P_n est irréductible modulo p, et $f_p = 2$ dans le dernier cas.

Comme dans le cas cubique cyclique, il n'est pas nécessaire d'effectuer les calculs dans le corps de nombres K. La forme particulière du polynôme considéré nous donne les relations suivantes entre les racines :

$$\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 0, \quad \varepsilon_1\varepsilon_2\varepsilon_3 = -1,$$

et en posant $\delta = (\varepsilon_1 - \varepsilon_2)(\varepsilon_2 - \varepsilon_3)(\varepsilon_3 - \varepsilon_1)$ (on a alors $\delta^2 = d_n$) on a également :

$$2\varepsilon_2 - \varepsilon_1 = \varepsilon_2 - \varepsilon_3 = \frac{\delta}{(\varepsilon_1 - \varepsilon_2)(\varepsilon_3 - \varepsilon_1)}.$$

D'autre part,

$$(\varepsilon_1 - \varepsilon_2)(\varepsilon_3 - \varepsilon_1) = 2\varepsilon_1^2 + \varepsilon_2\varepsilon_3 = 2\varepsilon_1^2 - \frac{1}{\varepsilon_1} = 3\varepsilon_1^2 + n,$$

donc finalement :

$$\varepsilon_2 = \frac{\delta}{2(20n^2 - d_n)}(12n\varepsilon_1^2 - 9\varepsilon_1 + 16n^2) - \frac{\varepsilon_1}{2}.$$

On prenant $\varepsilon_1 = \varepsilon$, on a donc

$$\varepsilon\varepsilon_2^2 = \varepsilon\left(\frac{\delta}{2(20n^2 - d_n)}(12n\varepsilon^2 - 9\varepsilon + 16n^2) - \frac{\varepsilon}{2}\right)^2.$$

Le programme `torsionS3` permettant de tester la condition de congruence $\left(\varepsilon\varepsilon_2^2\right)^{a_p} \equiv 1 \pmod{p^2}$ est alors simple à mettre en oeuvre. Il est détaillé en appendice B.2.

Le polynôme P_n est irréductible et de discriminant sans facteurs carrés pour 61 valeurs de n comprises entre 2 et 100. En faisant varier p de 5 à 10^8 dans chacune de ces situations, les seuls cas où la φ-composante de $\mathcal{X}$ n'est pas libre sont :

- $n = 25$, $p = 5$ (degré résiduel $a_p = 2$) ;
- $n = 49$, $p = 7$ (degré résiduel $a_p = 1$) ;
- $n = 50$, $p = 5$ (degré résiduel $a_p = 2$) ;
- $n = 98$, $p = 7$ (degré résiduel $a_p = 1$).

Ici encore nous avons écarté des nombres premiers pour des raisons calculatoires : ceux qui divisent la quantité $20n^2 - d_n$. À nouveau nous étudions chacun de ces cas particuliers par l'algorithme de Pitoun-Varescon. On trouve alors, pour n variant de 2 à 100 et p inférieur à 10^8 une douzaine de corps non 3-rationnels et deux corps non-7-rationnels : pour $n = 52$ et $n = 80$. Pour une raison de semi-simplicité, on passe sur les corps 3-rationnels. Pour les deux corps non 7-rationnels en revanche on peut conclure de la façon suivante. Dans les deux cas, le 7-rang du groupe des classes du corps K vaut 1, on vérifie ensuite qu'il provient du sous-corps quadratique imaginaire F_n et que F_n n'est pas 7-rationnel. D'un autre côté, un calcul montre que $d_p\mathrm{Tor}_{\mathbb{Z}_p}G_{\mathrm{K},S_7}^{ab} = 1$, et ainsi, $\left(\mathrm{Tor}_{\mathbb{Z}_p}G_{\mathrm{K},S_7}^{ab}\right)^{\varphi} = \{1\}$.

Pour les premiers p de $\mathcal{D}_{Cl}\backslash\mathcal{D}$, on trouve seulement cinq situations non p-rationnelles : $(n,p) \in \{(19,7),(31,5),(32,7),(97,5),(100,5)\}$. Ici, seul le couple $(100,5)$ a un régulateur normalisé non trivial (en la composante φ).

La très faible proportion de couples (n,p) pour lesquels on détecte une composante non-libre subsiste pour d'autres valeurs de n : lorsque l'on fait varier à la fois l'entier n et le premier p de 1 à 10^5, on balaye 62486 corps, et on teste plus de 56×10^8 composantes associées à ces corps de nombres pour finalement ne trouver que 4041 couples (n,p) pour lesquels une des composantes est non-libre, ce qui revient à moins de $7.2 \times 10^{-5}\%$ des cas seulement ! Notons enfin que pour $313 < p < 10^5$, les composantes étudiées sont toutes libres.

Remarque 4.4.3. — Il serait possible de considérer le cas des extensions à ramification restreinte avec S ne contenant pas nécessairement toutes les places au-dessus de p. Typiquement, en partant d'une extension quadratique imaginaire $\mathrm{k}/\mathbb{Q}$ dans laquelle p est totalement décomposé. Si $S \cap S_p = \{v_0\}$, la conjecture de Schanuel nous assure quand même ici que $G_{\mathrm{k},S}$ est de dimension cohomologique stricte au plus 2 (voir par exemple **[36]** et **[35]**).

4.4.3. Extensions cycliques totalement réelles de degré 4. — On suit la même idée que celle du cas cubique cyclique. On se donne p un nombre premier tel que $p \equiv 1 (\mathrm{mod}\ 4)$, de sorte que $\mathbb{Q}_p$ contienne une racine quatrième de l'unité, notée ζ : si a est une racine primitive quatrième de l'unité dans $\mathbb{F}_p$, le lemme de Hensel nous assure l'existence et l'unicité d'un relèvement ζ de a dans $\mathbb{Z}_p$ vérifiant la relation $\zeta \equiv a \pmod{p}$.

Soit P un polynôme irréductible de degré 4 et K son corps de décomposition, qu'on suppose quartique cyclique et totalement réel. On note Δ le groupe de Galois de l'extension $\mathrm{K}/\mathbb{Q}$ et on fixe σ un générateur. On ordonne alors les racines (réelles) de P de sorte que σ soit donné par le cycle $(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4)$ de longueur 4

Comme $p \equiv 1 (\mathrm{mod}\ 4)$, le groupe Δ a quatre caractères $\mathbb{Q}_p$-irréductibles de degré 1 : $\mathbb{1}$, φ, φ^2 et φ^3, où φ est défini par $\varphi(\sigma) = \zeta$.

Considérons la représentation de degré trois $\rho = \varphi + \varphi^2 + \varphi^3$. Elle est représentée par la matrice

$$\rho(\sigma) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix};$$

c'est la matrice de l'action de σ sur le module $\mathbb{Z}_p\varepsilon_1 \oplus \mathbb{Z}_p\varepsilon_2 \oplus \mathbb{Z}_p\varepsilon_3$.

Soit S un ensemble fini de nombres premiers de $\mathbb{Z}$, tous congrus à 1 modulo p et tous inertes dans $\mathrm{K}/\mathbb{Q}$, auquel on ajoute le nombre premier p : ainsi $S_p \subset S$. On pose $\mathcal{G} = G_{\mathrm{K},S}$, puis $\mathcal{H} = \mathrm{Gal}(\mathrm{K}_S/\mathbb{Q}_S\mathrm{K})$ et $\mathcal{X} = \mathcal{H}^{ab}$. On sait déjà que $\mathcal{X}^{\mathbb{1}} = \{1\}$, et que d'après la proposition 4.3.17, $\mathcal{X}^{\varphi^2} \simeq (\mathcal{X}_{\mathrm{F}})^{\mathbb{1}}$, où F est le sous-corps quadratique réel de $\mathrm{K}/\mathbb{Q}$.

Pour p générique et par choix des éléments de $S\backslash S_p$, le corollaire 2.1.2 donne

$$\mathrm{Tor}_{\mathbb{Z}_p}(G_{S,\mathrm{K}}^{ab})^{\varphi} \simeq \mathrm{Tor}_{\mathbb{Z}_p}\Big(\frac{\big(\prod_{v|p}\mathcal{U}_v\big)^{\varphi}}{\iota(\mathcal{E}_{\mathrm{K}}^{\varphi})}\Big);$$

il en est de même pour φ^2 et φ^3.

Supposons alors que les p-tensorisés des racines de P engendrent le groupe $\mathcal{E}_K$. La matrice $\rho(\sigma)$ admet trois valeurs propres distinctes : ζ, -1 et $-\zeta$. On obtient après calcul les vecteurs propres :

$$u_{\varphi} = \varepsilon_1\varepsilon_2^{1-\zeta}\varepsilon_3^{-\zeta}, \quad u_{\varphi^2} = \varepsilon_1\varepsilon_3 \quad \text{et} \quad u_{\varphi^3} = \varepsilon_1\varepsilon_2^{1+\zeta}\varepsilon_3^{\zeta},$$

et il vient $\mathcal{E}_{\mathrm{K}}^{\varphi} = \langle u_{\varphi}\rangle$, $\mathcal{E}_{\mathrm{K}}^{\varphi^2} = \langle u_{\varphi^2}\rangle$ et $\mathcal{E}_{\mathrm{K}}^{\varphi^2} = \langle u_{\varphi^3}\rangle$.

Pour $i = 1, 2, 3$, on peut alors, via le théorème 4.1.13, étudier la liberté du module $\mathcal{X}^{\varphi^i}$ en déterminant si l'image du vecteur u_{φ^i} est une racine p-ième dans tous les groupes d'unités locaux $\big(\prod_{w|p}\mathcal{U}_w\big)^{\varphi^i}$, c'est-à-dire en vérifiant la condition de congruence :

$$u_{\varphi^i}^{a_p} \equiv 1 (\mathrm{mod}\ p^2),$$

où $a_p = p^{f_p} - 1$, avec f_p le degré résiduel de p dans l'extension $\mathrm{K}/\mathbb{Q}$.

Cette stratégie repose sur l'hypothèse faite sur les racines du polynôme P. Dans **[3]**, Balady et Washington adaptent le travail de Balady dans **[2]** au cas quartique. Ils exhibent une famille de polynômes

$$P_s = X^4 + 4(s^3 - s^2 + 2s - 1)X^3 + 6(-s^2 - 1)X^2 + 4X + 1,$$

dont le corps de décomposition K_s est un corps totalement réel cyclique de degré 4 et dont les racines engendrent soit les unités de K_s soit un sous-groupe d'ordre 5 si l'on s'assure que :

(i) $s \in \mathbb{Z}^*$,
(ii) $3s^2 - 4s + 4$ est un carré,
(iii) $s^2 + 2$ sans facteurs carrés.

Notons que ces conditions sur le paramètre s sont très restrictives : pour $|s| < 10^6$, il n'y a que les entiers -34272, -2460, -12, 48, 660, 127908 qui vérifient ces deux propriétés à la fois.

Lors de la construction de cette famille de polynômes, Balady et Washington choisissent pour générateur σ de Δ la matrice d'ordre 4 de $PGL_2(\mathbb{Z})$

$$\begin{pmatrix} f & -1 \\ \dfrac{f^2+g^2}{2} & -g \end{pmatrix},$$

où $f = \dfrac{2 + \sqrt{3s^2 - 4s + 4}}{2}$ et $g = \dfrac{2 - \sqrt{3s^2 - 4s + 4}}{2}$. Son action sur les racines de P donne alors immédiatement

$$\varepsilon_2 = \frac{f\varepsilon_1 - 1}{\dfrac{f^2+g^2}{2}\varepsilon_1 - g}, \quad \varepsilon_3 = \frac{(f+g)\varepsilon_1 - 2}{(f^2+g^2)\varepsilon_1 - g - f} \quad \text{et} \quad \varepsilon_4 = \frac{g\varepsilon_1 - 1}{\dfrac{f^2+g^2}{2}\varepsilon_1 - f},$$

et le générateur σ du groupe Δ est bien défini par le cycle $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$. Remarquons ici que la matrice associée au deuxième générateur du groupe Δ s'obtient en échangeant f et g.

On peut encore une fois tester l'hypothèse de congruence directement dans $\mathbb{Z}$ de façon très simple : si les racines de P_s engendrent $\mathcal{E}_K$ (ce qui est le cas pour $p > 5$), la φ-composante $\mathcal{X}^{\varphi}$ est non-libre si et seulement si

$$(\varepsilon_1 \varepsilon_2^{1-a} \varepsilon_3^{-a})^{a_p} \equiv 1 \pmod{p^2}.$$

De même, on obtient pour les composantes $\mathcal{X}^{\varphi^2}$ et $\mathcal{X}^{\varphi^3}$ les conditions

$$(\varepsilon_1 \varepsilon_3)^{a_p} \equiv 1 \pmod{p^2} \quad \text{et} \quad (\varepsilon_1 \varepsilon_2^{1+a} \varepsilon_3^{a})^{a_p} \equiv 1 \pmod{p^2}.$$

On se donne maintenant $p \equiv 3 \pmod 4$. On note toujours φ le caractère associé à ζ. Cette fois-ci les caractères φ et φ^3 sont définis sur $\mathbb{Q}_p(\zeta)$ et Δ a trois caractères $\mathbb{Q}_p$-irréductibles : le caractère trivial, le caractère φ^2 et le caractère $\varphi + \varphi^3$ de degré 2. Un raisonnement identique à celui effectué dans le cas cubique cyclique montre que la composante $\mathcal{X}^{\varphi+\varphi^3}$ est non-libre si

$$\left(\varepsilon_1^2 \varepsilon_2^2 \varepsilon_3\right)^{a_p} - 1 \equiv 0 \pmod{p^2}.$$

Les fonctions PARI/GP utilisées pour déterminer si les φ-composantes sont, ou non, libres sont construites sur le même modèle que celles de la section 4.4.1. Les programmes et les résultats obtenus en faisant varier p de 1 à 10^8 sont présentés dans le tableau en appendice B.3. Pour chaque premier $p \in \mathcal{A}_{nl}$, on précise en indice la puissance k du caractère φ pour laquelle la composante $\mathcal{X}^{\varphi^k}$ est non libre ; à noter que quand $k = 2$, cela signifie que l'obstruction provient du sous-corps quadratique réel. Dans le cas $p \equiv 3 \pmod 4$, on notera en indice $1 + 3$ dans le cas où la composante $\mathcal{X}^{\varphi+\varphi^3}$ est non libre. Pour $n = 48$, on a par exemple :

s	$\mathcal{D}$	$\mathcal{D}_{Cl}$	$\mathcal{D}_{disc}$	$\mathcal{A}_{nl}(10^8)$
-12	$\{2, 11\}$	$\{2\}$	$\{2, 11, 73\}$	$\{17_2, 19363829_3, 12690513_3, 26900513_3\}$

Les formules données plus haut pour exprimer les racines ε_2 et ε_3 du polynôme P ont des dénominateurs : les diviseurs de ces dénominateurs, renseignés dans la colonne $\mathcal{D}$ du tableau précédent, doivent être étudiés à part via l'algorithme de Pitoun-Varescon (ou alternativement de Gras). Les corps sont tous p-rationnels pour $p \in \mathcal{D} \backslash \{2\}$ et aucun n'est 2-rationnel.

Enfin, pour être complet, terminons avec les premiers $p \in \mathcal{D}_{Cl} \cup \mathcal{D}_{disc} \backslash \mathcal{D}$: aucune situation n'est p-rationnelle, mais seuls les cas $(n, p) \in \{(-92604732, 5_2), (-92604732, 37_1), (1781520, 5_1)\}$ ont un régulateur normalisé non-trivial.

APPENDICE A

CALCUL LOCAL DES CUP-PRODUITS ET CRITÈRE (LMS_f) : PHILOSOPHIE DU CODE PARI-GP

A.1. Premiers auxiliaires

Soient S un ensemble fini de premiers de K de normes congrues à 1 modulo p. On rappelle que pour un élément V de S, le premier auxiliaire p_v est choisi tel que :

- p_v est inerte dans l'extension $\mathrm{K}_v^{p,el}/\mathrm{K}$,
- p_v est totalement décomposé dans l'extension $\mathrm{K}_w^{p,el}/\mathrm{K}$ pour $w \in S, w \neq v$.

Il s'agit donc en fait de calculer la ramification d'un premier p_v de K dans une extension p-élémentaire $\mathrm{K}_w^{p,el}$ de K pour $w \in S$. Par définition, p_v est ramifié dans l'extension $\mathrm{K}_w^{p,el}/\mathrm{K}$ si et seulement si p_v est égal à w. Dans les autres cas on utilise la théorie du corps de classes : le symbole d'Artin donne un isomorphisme entre le groupe de Galois de l'extension $\mathrm{K}_w^{p,el}/\mathrm{K}$ et le corps de classes de K de rayon w, noté L, donné par `L=bnrinit(K,w,0)`. On calcule alors l'image du Frobenius de p_v dans la p-partie du groupe de classes de K de rayon w :

```
frob(L,p,pv)=
{Fpv=vector(#L.clgp.cyc,i,(bnrisprincipal(L,pv,0)[i]%p)*(L.clgp.cyc[i]%p==0));}
```

Si `Fpv` est le vecteur nul, alors p_v est décomposé dans $\mathrm{K}_w^{p,el}$, sinon p_v est inerte dans $\mathrm{K}_w^{p,el}$. Il suffit ensuite de tester systématiquement les premiers de K jusqu'à en trouver un qui convienne, $p_v =$`praux(K,S,p,v)`.

Remarque A.1.1. — Si le corps de base est $\mathbb{Q}$, il est plus efficace d'utiliser le code suivant :

```
ramQ(p,pv,w)=
 {my(r);
  r=w^((pv-1)/p);
  if(r%pv==1,0,if((r^p)%pv==1,1,-1));}
```

qui renvoie $0, 1$ ou -1 suivant si le premier p_v est décomposé, inerte ou ramifié dans l'extension $\mathbb{Q}_w^{p,el}/\mathbb{Q}$.

A.2. Calcul local des cup-produits

Soient v, w deux éléments de S. D'après la proposition 3.3.1, le *linking number* l_{vw} est donné par l'égalité $F_v = F_{p_w}^{l_{vw}}$ dans le groupe de Galois $\mathrm{Gal}(\mathrm{K}_w^{p,el}/\mathrm{K})$, où p_w est le premier auxiliaire associé à w et F_v, F_{p_w} sont les Frobenius de v et p_w. Là encore on utilise le symbole d'Artin pour comparer non pas les Frobenius eux-mêmes, mais leurs images dans le groupe des classes de K de rayon w.

```
linkingnumber(K,S,p,v,w)=
{my(pw,L,l,Fpw,Fv,k);
 pw=praux(K,S,p,w);
 L=bnrinit(K,w,0);l=#L.clgp.cyc;
 Fpw=frob(L,p,pw);
 Fv=frob(L,p,v);
```

```
 k=0;
 while(Fv!=(k*Fpw)%p,k=k++);
 k;}
```

On obtient ainsi la composante locale en w du cup-produit $\widetilde{\chi}_w \cup \widetilde{\chi}_v$, ce qui permet de construire une matrice Cup =`cupproduits(K,S,p)` renseignant chacune des composantes locales (en colonnes) de chacun des cup-produits (en ligne) de la famille $\{\widetilde{\chi}_v, v \in S\}$.

A.3. Critère (LMS_f)

Une fois les cup-produits calculés localement, on peut écrire une fonction `candidats(K,S,p)` renvoyant la liste `V` des ensembles `V[i]` d'éléments de S dont les cup-produits associés sont tous nuls. En reprenant les notations de la proposition 3.3.4, on aura à i fixé t =`#V[i]` et $\{v_j, 1 \leqslant j \leqslant t\}$ =`V[i]`. Il reste alors à extraire de `Cup=cupproduits(K,S,p)` la sous-matrice C puis à tester si elle vérifie la deuxième condition de la proposition 3.3.4 (la première étant vérifiée par construction). La commande suivante donne la liste des décompositions $S = \mathcal{V} \cup \mathcal{U}$ pour lesquelles le corps K vérifie le critère de Labute-Minac-Schmidt par rapport à S.

```
LabuteMinacSchmidt(K,S,p)=
 {my(Cup,V,U,R,M);
  Cup=cupproduits(K,S,p);
  V=candidats(K,S,p);
  U=vector(#V);
  R=List();
  for(i=1,#V,U[i]=setminus(Set(S),Set(V[i]));M=matrix(1,#S);
     for(j=1,#V[i],
        for(k=1,#U[i],
           for(l=1,#S,if(S[l]==V[i][j],v=l);if(S[l]==U[i][k],w=l));
           M=matconcat([M;C[(v-1)*#S+w,\rdbrack );
        );
     );
     if(matrank(M)==#S, R=concat(R,[V[i],U[i]]));
  );
  R;}
```

APPENDICE B

STATISTIQUES SUR LA LIBERTÉ DES φ-COMPOSANTES

Cet appendice présente les programmes et les résultats numériques issus des études menées dans la section 4.4. Tous les calculs sont effectués sous la conjecture de Leopoldt.

B.1. Extensions cubiques cycliques

Les extensions cubiques cycliques que l'on considère dans la section 4.4.1 proviennent toutes de familles de polynômes bien particulières : les familles de polynômes données par Balady dans [**2**]. À partir de la donnée de deux polynômes à coefficients entiers f et g (ordonnés selon leurs degrés) et d'un entier $n \in \mathbb{Z}\backslash\{-1\}$, le programme suivant renvoie 0 si le polynôme $P_n = X^3 + a(n)X^2 + \lambda(n)X - 1$ ne vérifie pas les conditions de Balady. Dans le cas contraire, il renvoie un vecteur `T=[P,R]`, où P est le polynôme P_n et R le triplet (16) des racines de P_n.

```
polynomeBalady(f,g,n)=
{my(T,lam,lambda,coeffa,a,D,S,P,b,q,p,delta,d,r2,r3);
T=0;
lambda=(f^3+g^3+1)/(f*g);
if(type(lambda)=="t_POL",
 D=poldegree(lambda);
 S=sum(i=1,D,type(polcoeff(lambda,i))=="t_INT");
 if(S==D,
  x=n;lam=eval(lambda);x='x;
  coeffa=3*(f^2+g^2-f*g)-lambda*(f+g);x=n;a=eval(coeffa);x='x;
  P=x^3+a*x^2+lam*x-1;
  b=3*a+lam^2;
  if((vecmax(factor(b)[,2])==1)&&(polisirreducible(P)==1),
   q=2*a^3/27-a*lam/3-1;p=lam-a^2/3;
   delta=factor(-27*q^2-4*p^3);d=factorback(delta[,1],delta[,2]/2);
   r2=1/2*(6*p*(x+a/3)^2/d-9*q*(x+a/3)/d+4*p^2/d-(x+a/3))-a/3;
   r3=1/2*(-6*p*(x+a/3)^2/d+9*q*(x+a/3)/d-4*p^2/d-(x+a/3))-a/3;
   T=[P,[x, r2, r3]}
  )
 )
);
T;}
```

Il reste à ordonner les racines de P_n par ordre croissant pour fixer le générateur du groupe $\Delta = \mathrm{Gal}(\mathrm{K}_n/\mathbb{Q})$, où K_n est l'extension cubique cyclique engendrée par le polynôme P_n. On suppose pour la suite que cette fonction de réordonnement est intégrée à la fonction `polynomeBalady`.

On se donne maintenant un premier $p > 3$ non exceptionnel (c'est-à-dire qui ne divise pas le nombre de classes du corps K_n). On suppose, pour s'assurer que les racines de P_n sont inversibles modulo p, que p ne divise pas le discriminant du polynôme P (donné par `delta` dans `polynomeBalady`). On note f_p le degré résiduel de p dans l'extension K/$\mathbb{Q}$.

La liberté de chacune des φ-composantes du module $\mathcal{X}$ associé à la pro-p extension $K_{\mathbb{Q},S_p}$ est alors testée par l'un des programmes suivants, où l'entrée P est donnée par la fonction `polynomeBalady` :

Si 3 *divise* $p-1$. — Dans ce cas, le groupe Δ a deux caractères $\mathbb{Q}_p$-irréductibles non-triviaux : φ et φ^2. On rappelle que φ est associé à un relèvement a d'une racine cubique de l'unité modulo p.

```
torsionZ3(pol,p,a,fp)=
{my(T,P,E,e1,e2,K,Emodp2);
T=[0,0];
P=pol[1];K=bnfinit(P);
E=pol[2];e1=Mod(Mod(E[1],P),p^2);e2=Mod(Mod(E[2]^(-1),P),p^2);
T[1]=lift((e1*e2^a)^(p^fp-1)-1)==Mod(0,p^2);
T[2]=lift((e1*e2^(a^2))^(p^fp-1)-1)==Mod(0,p^2);
T;}
```

La première (resp. deuxième) composante de `T` vaut 0 ou 1 suivant si le module $\mathcal{X}^{\varphi}$ (resp. $\mathcal{X}^{\varphi^2}$) est libre ou non.

Si 3 *ne divise pas* $p-1$. — Ici, le groupe Δ n'a qu'un unique caractère $\mathbb{Q}_p$-irréductible non trivial, de degré 2.

```
torsionZ3(pol,p,a,fp)=
{my(T,P,K,R,E);
P=pol[1];K=bnfinit(P);
R=pol[2];E=Mod(Mod(R,P),p^2);
T=lift((E[1]^2*E[2])^(p^fp-1)-1)==Mod(0,p^2));
T;}
```

B.1.1. Résultats numériques : famille de polynômes de Balady. — Pour les notations, voir la section 4.4.1.1. Pour $X = 15 \times 10^7$, et pour la famille de polynômes de Balady donnée par $f = -n^2$ et $g = n^3 - 1$, on obtient :

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{A}_{nl}(15\times 10^7)$
1	$\{19\}$	$\varnothing$	$\{67_{29^2}, 193_{84}, 337_{128^2}, 7321_{308^2}\}$
2	$\{11, 13, 79\}$	$\{3\}$	$\{19_{7^2}, 439_{171}, 2887_{698^2}, 59060857_{26994113}, 122648623_{5895446}\}$
4	$\{13, 19, 79, 571\}$	$\{3, 13\}$	$\varnothing$
7	$\{17, 23, 2383, 3769\}$	$\{3, 7, 223\}$	$\{199_{92}, 277_{116}\}$
10	$\{7, 13, 157, 1051, 9973\}$	$\{3, 7, 991\}$	$\{43_{6^2}, 14783491_{4865581}\}$
11	$\{19, 769, 1451, 19429\}$	$\{2, 3, 7, 97\}$	$\{631_{43}\}$
14	$\{2939, 38377, 47911\}$	$\{2, 3, 19, 2143\}$	$\{13_3, 43_6, 60765967_{27581956}\}$
16	$\{19, 79, 181, 229, 439, 829\}$	$\{2, 3, 7, 2053\}$	$\{43_6, 43933_{9824}\}$
17	$\{7, 13, 31, 743, 3229, 6421\}$	$\{2, 3, 7, 37\}$	$\{157_{12^2}, 937_{322}\}$
19	$\{7, 79, 277, 7219, 130267\}$	$\{2, 3, 7, 1303\}$	$\varnothing$
20	$\{7, 19, 37, 73, 227, 313, 9817\}$	$\{2, 3, 31, 67\}$	$\{1666783_{517555^2}\}$
22	$\{307, 877, 11131, 234193\}$	$\{3, 1466473\}$	$\{7_{4^2}, 31_{52}, 139627_{11986^2}\}$
25	$\{16249, 390553, 441403\}$	$\{3, 43, 619, 691\}$	$\{19_7, 229_{94^2}, 409_{53}\}$
26	$\{7, 18251, 73417, 456901\}$	$\{3, 367, 10651\}$	$\{13_{3^2}, 91513_{30403}\}$
29	$\{25229, 707197, 785671\}$	$\{3, 57875563\}$	$\varnothing$
31	$\{7, 13, 23, 79, 191, 433, 11689\}$	$\{3, 7, 66523\}$	$\varnothing$
32	$\{67, 15649, 33791, 1153219\}$	$\{2, 3, 3863473\}$	$\{79_{23}\}$
34	$\{7, 40459, 190891, 1461391\}$	$\{2, 3, 3197533\}$	$\{37_{10}, 3181_{440^2}, 236503_{5480^2}, 83666173_{602656^2}\}$
35	$\{11, 19, 61, 211, 26833, 1500523\}$	$\{3, 757, 75931\}$	$\{13_{3^2}, 54499_{23608^2}\}$
37	$\{103, 769, 2437, 19753, 52021\}$	$\{2, 3, 19, 193, 463\}$	$\{73_8, 331_{31}, 811_{130}, 1052203_{452608}, 29322691_{4854914}\}$
40	$\{7, 181, 14143, 65599, 394549\}$	$\{2, 3, 43, 331\}$	$\{19_{7^2}, 674977_{1170352}\}$
44	$\{13, 181, 20707, 87119, 308887\}$	$\{2, 3, 1033, 4129\}$	$\{43_{6^2}, 2341_{1106}\}$
46	$\{11, 127, 349, 9041, 12829, 37657\}$	$\{3, 31, 3563467\}$	$\{67_{29}, 97_{35^2}, 11503_{467}, 417649_{174641}, 4198807_{268994}\}$
49	$\{13, 19, 31, 127, 2389, 15217, 120049\}$	$\{2, 3, 7, 61609\}$	$\{19801_{2184^2}\}$
50	$\{59, 67, 241, 2161, 25933, 99109\}$	$\{2, 3, 7, 9130117\}$	$\{331_{31}\}$
52	$\{7, 59, 79, 347, 98101, 7311463\}$	$\{2, 3, 13, 229, 71419\}$	$\varnothing$
55	$\{7, 2749, 3517, 169399, 1307209\}$	$\{2, 3, 7, 14667403\}$	$\{97_{35^2}, 4243_{298^2}, 260047_{18194}\}$
56	$\{13, 43, 277, 823, 2731, 4157, 12613\}$	$\{3, 7, 67, 127, 2719\}$	$\{62434681_{26935694}\}$

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{A}_{nl}(8\times 10^7)$
59	{7, 31, 29837, 390877, 12754741}	{2, 3, 31, 127, 1327}	$\{19_7, 43_6, 19699_{7417^2}, 25357_{9006^2}, 4296091_{2113223}\}$
61	$\{7, 19, 271, 281, 821, 2689, 2078497\}$	$\{3, 613, 388057\}$	$\{37_{10}\}$
62	$\{7, 13, 242171, 1193443, 2110879\}$	$\{3, 31, 3633403\}$	$\{223_{39^2}\}$
64	$\{127, 138493, 266239, 16777027\}$	$\{3, 5011, 129517\}$	$\{43_{6^2}\}$
65	$\{278849, 17850433, 18700243\}$	$\{3, 19, 547, 57697\}$	$\{7_{4^2}, 331_{31}, 3694459_{45444}\}$
67	$\{13, 61, 383, 571, 797, 25411, 36919\}$	$\{3, 7, 1117, 74797\}$	$\varnothing$
70	$\{13, 1933, 12421, 347899, 1928371\}$	$\{2, 3, 4003, 126151\}$	$\{503287_{112593^2}\}$
71	$\{433, 2683, 9883, 58687, 362951\}$	$\{2, 3, 340422079\}$	$\{7_4\}$
74	$\{59, 6961, 29986357, 31235551\}$	$\{2, 3, 109, 457, 133873\}$	$\{73_{8^2}, 3207019_{467011}\}$
76	$\{7, 23, 61, 317, 823, 5791, 34714219\}$	$\{2, 3, 127, 11237029\}$	$\{19_7, 794641_{291733}, 3728983_{905060^2}, 82044439_{14812302}\}$
77	$\{19, 23, 3583, 9811, 20107, 1924141\}$	$\{3, 1457126959\}$	$\{7_{4^2}, 148942621_{71590090}\}$
79	$7\{11, 31, 67, 45389, 581341, 1305391\}$	$\{3, 19, 211, 433, 3631\}$	$\{37_{10^2}, 103_{46^2}\}$
80	{7, 13, 19, 31, 67, 103, 719, 20479, 165829}	{2, 3, 7, 52667059}	$\{73_8, 46687_{16066}, 228901_{55529^2}, 41448541_{53565652}\}$
82	$\{7, 13, 79, 271, 313, 558091, 3477841\}$	$\{3, 13, 1777, 41467\}$	$\varnothing$
85	$\{19, 31, 107, 277, 5807, 6079, 2846677\}$	$\{2, 3, 7, 313, 691, 997\}$	$\varnothing$
86	$\{167, 3853, 54700561, 56653879\}$	$\{2, 3, 7, 17713, 51043\}$	$\{73_{8^2}, 6199_{2645}\}$
89	$\{7, 61, 712889, 1028557, 9272173\}$	$\{2, 3, 127, 48593539\}$	$\{31_5, 211_{14^2}\}$
91	$\{631, 829, 919, 2503, 27397, 112339\}$	$\{2, 3, 1483, 52567\}$	$\{73_8\}$
92	$\{17, 19, 373, 2437, 198463, 71639023\}$	$\{2, 3, 61, 193, 542197\}$	$\{103_{46^2}\}$
94	$\{7, 37, 463, 78074617, 90620231\}$	$\{3, 8929, 36396301\}$	$\{67_{29}, 367_{83}, 829_{125}\}$
95	$\{13, 79, 79309, 866399, 84077473\}$	$\{2, 3, 31, 37, 631, 2113\}$	$\varnothing$
97	$\{7, 223, 56713, 922081, 91324339\}$	$\{2, 3, 763707067\}$	$\{19_7, 97_{35^2}, 487_{232}\}$
100	$\{23, 43913, 99999703, 103060603\}$	$\{3, 57709, 1882459\}$	$\{11670859_{4550018}, 54250591_{7365^2}\}$

B.1.2. Résultats numériques : famille de polynômes de Lecacheux. — Voir section 4.4.1.1. Pour la famille de polynômes de Lecacheux **[33]** que l'on retrouve à partir de la famille de Balady pour $f=-1$ et $g=-n$, et pour $X=15\times 10^6$, on obtient :

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{A}_{nl}(15\times 10^7)$
14	$\{13, 157, 199\}$	$\{3, 13\}$	$\{43_{6^2}, 397849_{136077^2}\}$
16	$\{3, 5, 7, 37, 211\}$	$\{3, 43\}$	$\{62347_{4200^2}\}$
22	$\{3, 7, 421, 487\}$	$\{3, 439\}$	$\{151_{32}\}$
26	$\{5, 7, 97, 601\}$	$\{2, 3, 7\}$	$\{523_{60}\}$
28	$8\{3, 19, 37, 787\}$	$\{3, 5\}$	$\{331_{31^2}, 1669_{248}, 640483_{42506}\}$
34	$\{3, 7, 11, 19, 61, 151\}$	$\{3, 7, 19\}$	$\{31_5, 43_{6^2}\}$
38	$\{31, 37, 43, 1447\}$	$\{3, 229\}$	$\{13_{3^2}, 73_8\}$
40	$\{3, 7, 13, 229, 1483\}$	$\{3, 709\}$	$\{73_{8^2}, 28051_{2374^2}, 588277_{199858}\}$
44	$\{7, 13, 43, 139, 277\}$	$\{2, 3, 19\}$	$\{17923_{613}, 8436997_{3980782^2}\}$
46	$\{3, 5, 7, 13, 163, 283\}$	$\{3, 7, 13\}$	$\{31_5\}$
50	$\{7, 13, 181, 2503\}$	$\{2, 3, 37\}$	$\{45439_{2225}, 1602529_{510444^2}\}$
52	$\{3, 17, 2551, 2707\}$	$\{2, 3, 919\}$	$\{7_4, 157_{12^2}, 10453_{270^2}\}$
56	$\{5, 11, 43, 73, 2971\}$	$\{3, 13\}$	$\{7_{4^2}\}$
58	$\{3, 7, 13, 19, 31, 37, 103\}$	$\{3, 17\}$	$\{2221_{543}, 725209_{1202492}\}$
62	$\{7, 61, 523, 3847\}$	$\{2, 3, 157\}$	$\{13_{3^2}, 14737_{4341}\}$
64	$\{3, 7, 3907, 4099\}$	$\{3, 7, 127\}$	$\{103_{46^2}, 601_{24}\}$
68	$\{7, 67, 661, 4423\}$	$\{3, 13, 31\}$	$\{4621_{1763}\}$
74	$\{7, 73, 751, 5479\}$	$\{3, 19, 127\}$	$\{43_6, 107815549_{14774937}\}$
76	$\{3, 5, 7, 13, 61, 5779\}$	$\{3, 1381\}$	$\{400339_{160715^2}\}$
80	$\{19, 79, 337, 6163\}$	$\{3, 7, 43\}$	$\{61_{13^2}\}$
88	$\{3, 7, 29, 61, 127, 1069\}$	$\{2, 3, 7, 151\}$	$\varnothing$
92	$\{7, 13, 8191, 8467\}$	$\{3, 1669\}$	$\{367_{83}\}$
94	$\{3, 31, 43, 199, 8839\}$	$\{2, 3, 2851\}$	$\varnothing$
98	$\{13, 67, 97, 139, 739\}$	$\{2, 3, 7, 13\}$	$\{12919_{5520^2}, 247309_{37071}\}$
100	$\{3, 7, 11, 31, 313, 1429\}$	$\{2, 3, 7, 211\}$	$\{13_{3^2}, 6037_{509^2}, 145316557_{17730502^2}\}$

B.2. Extensions diédrales

La section 4.4.2 se concentre sur les extensions diédrales K_n obtenues à partir des polynômes $P_n = X^3+nX+1$ de discriminant d_n sans facteurs carrés. On considère toujours un premier $p>3$ et on suppose que p ne divise ni le nombre de classes de K_n ni la quantité $20n^2-d_n$. On peut alors tester la liberté de la φ-composante du module $\mathcal{X}$ associé à la représentation irréductible de degré 2 du groupe $\Delta=\mathrm{Gal}(K_n/\mathbb{Q})$. On suppose que les entrées dans la fonction suivante vérifient les hypothèses mentionnées au début de ce paragraphe. On note toujours f_p le degré résiduel de p dans l'extension $\mathrm{K}/\mathbb{Q}$.

```
torsionZ3(P,p,fp)=
{my(d,Q,K,eps,R,T);
d=poldisc(P);
Q=polcompositum(P,x^2-d)[1];
K=bnfinit(Q);
eps=X/(40*n^2-2*d)*(12*n*x^2-9*x+16*n^2)-x/2;
R=Mod(Mod(Mod([x,eps],P),X^2-d),p^2);
T=lift(lift((R2[1]*R2[2]^2)^(p^fp-1)-1))==Mod(0,p^2));
T;}
```

B.3. Extensions cycliques de degré 4

Les applications numériques de la section 4.4.3 proviennent de la famille de polynômes donnée par Balady et Washington dans [**3**]. Le code suivant renvoie 0 lorsque le polynôme P_s ne vérifie pas les hypothèses de [**3**, th. 1]. Dans le cas contraire, on obtient un vecteur $[P_s, R]$, où R est le quadruplet des racines de P ordonnées conformément aux choix faits dans la section 4.4.3.

```
polynomeBW(s)=
{my(T,c,b,c,t,B,f,g,P,eps2,eps3,eps4);
T=0;
a=s^2+2;
b=factor(3*s^2-4*s+4);c=b[,2]%2;
t=(vecmax(c)==0)*(vecmax(factor(a)[,2])==1);
if(t==1,
 B=factorback(b[,1],b[,2]/2);
 f=(s+B)/2; g=(s-B)/2;
 P=x^4+4*(s^3-s^2+2*s-1)*x^3+6*(-s^2-1)*x^2+4*x+1;
 eps2=Mod((f*x-1)/((f^2+g^2)/2*x-g),P);
 eps3=Mod(((f+g)*x-2)/((f^2+g^2)*x-g-f),P);
 eps4=Mod((g*x-1)/((f^2+g^2)/2*x-f),P);
 T=[P,[x,lift([esp2,eps3,esp4])]);
T;}
```

Considérons maintenant un premier p congru à 1 modulo 4. On suppose qu'il n'est pas exceptionnel et qu'il ne divise aucun des dénominateurs des coefficients des racines `eps2` et `eps3` obtenues de `polynomeBW`. Soit φ un caractère $\mathbb{Q}_p$-irréductible non trivial du groupe de Galois du corps de décomposition de P. On note a un relèvement de la racine quatrième de l'unité modulo p associée à φ et f_p le degré résiduel de p dans l'extension K/$\mathbb{Q}$. Dans le code suivant, la composante $T[i]$ vaut 0 si la φ^i-composante de $\mathcal{X}$ est libre, 1 sinon.

```
torsionBW(pol,p,a,fp)=
{my(T,P,E2,E3,e2,e3,eps2,eps3);
T=[0,0,0];
P=pol[1];sgn=sign(1-a);
E2=Mod(pol[2][2],P);e2=Mod(E2,p^2);eps2=Mod(E2^(sgn),p^2);
E3=Mod(pol[2][3],P);e3=Mod(E3,p^2);eps3=Mod(E3^(-1),p^2);
T[1]=lift((x*eps2^abs(1-a)*eps3^(a))^(p^fp-1))==Mod(1,p^2);
T[2]=lift((x*e3)^(p^fp-1))==Mod(1,p^2);
T[3]=lift((x*e2^(1+a)*e3^(a))^(p^fp-1))==Mod(1,p^2);
T;}
```

Si le premier p est congru à 3 modulo 4, le groupe de Galois du corps de décomposition de P n'a plus que deux caractères $\mathbb{Q}_p$-irréductibles : le caractère $\mathcal{X}^{\varphi^2}$ de degré 1 et le caractère $\mathcal{X}^{\varphi+\varphi^3}$ de degré 2. Le

programme pour tester leur liberté est construit sur le même modèle que le précédent ; la composante $T[i]$ correspond cette fois au caractère irréductible de degré i.

```
torsionBW(pol,p,fp)=
{my(T,P,E2,E3,e2,e3,eps2,eps3);
T=[0,0];
P=pol[1];
E2=Mod(pol[2][2],P);e2=Mod(E2,p^2);
E3=Mod(pol[2][3],P);e3=Mod(E3,p^2);
T[1]=lift((x*e3)^(p^fp-1))==Mod(1,p^2);
T[2]=lift((x^2*e2^2*e3)^(p^fp-1))==Mod(1,p^2);
T;}
```

B.3.1. Résultats numériques : cas cyclique de degré 4. — Voir la section 4.4.3.

s	$\mathcal{D}$	$\mathcal{D}_{Cl}$	$\mathcal{D}_{disc}$	$\mathcal{A}_{nl}(10^8)$
-34272	{2, 67, 443}	{2, 3, 5, 131, 1597}	{2, 67, 443, 587284993}	$\{193_1, 313_3, 389_3, 37511_2,$ $88969_1, 3019229_3, 14771837_1\}$
-2460	$\{2, 2131\}$	$\{2, 3, 5, 13\}$	$\{2, 113, 2131, 26777\}$	$\{491_2\}$
-12	$\{2, 11\}$	$\{2\}$	$\{2, 11, 73\}$	$\{17_2, 19363829_3, 12690513_3, 26900513_3\}$
48	$\{2, 41\}$	$\{2\}$	$\{2, 41, 1153\}$	$\{13_1, 379849_3, 763597_2, 2152957_2\}$
660	$\{2, 571\}$	$\{2, 5, 13\}$	$\{2, 353, 571, 617\}$	$\{349_2, 1949_1, 9137_3, 25652023_2, 25652023_2\}$
127908	$\{2, 110771\}$	$\{2, 7, 13, 17, 9337\}$	$\{2, 73, 110771, 112057921\}$	$\{3_2, 5_3, 29_1, 1117_3, 117889_2\}$
1781520	$\{2, 1542841\}$	$\{2, 5, 11, 47, 677208593\}$	$\{2, 1542841, 1586906755201\}$	$\{7_2, 29_2\}$

INDEX DES NOTATIONS

Notations générales

p	nombre premier impair
K	corps de nombres
$\overline{\mathrm{K}}$	clôture algébrique de K (fixée)
$\mathcal{O}_{\mathrm{K}}$	anneau des entiers de K
E_{K}	$\mathcal{O}_{\mathrm{K}}^{\times}$, groupe des unités de K
$\mathrm{Cl}(\mathrm{K})$	groupe des classes de K
$\mathrm{Reg}_{\mathrm{K}}$	régulateur de K
$\mathrm{Disc}_{\mathrm{K}}$	discriminant de K
Pl_{K}	ensemble des places de K
S_p	ensemble des places de K au-dessus de p
$\mu_{p^\infty}(\mathrm{K})$	groupe des racines de l'unité d'ordre une puissance de p contenues dans K
$\mu_p(\mathrm{K})$	racines de l'unité d'ordre divisant p contenues dans K
μ_{p^∞}	$\mu_{p^\infty}(\overline{\mathrm{K}})$
μ_p	$\mu_p(\overline{\mathrm{K}})$

Corps globaux

K^{nr}	extension non-ramifiée maximale de K
$v^{(1)}, \ldots, v^{(g)}$	premiers divisant v dans une extension L/K lorsque v est un premier de K
$D_{v^{(i)}}(\mathrm{L}/\mathrm{K})$	groupe de décomposition de $v^{(i)}$ dans l'extension L/K
$I_{v^{(i)}}(\mathrm{L}/\mathrm{K})$	groupe d'inertie de $v^{(i)}$ dans l'extension L/K
K_S^T	pro-p extension maximale de K non-ramifiée en dehors de S et T-décomposée
$G_{\mathrm{K},S}^T$	$\mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$
K_S	pro-p extension non-ramifiée en dehors de S maximale de K
$G_{\mathrm{K},S}$	$\mathrm{Gal}(\mathrm{K}_S^{\varnothing}/\mathrm{K})$
$\mathrm{K}_S^{p,el}$	p-extension élémentaire maximale de K non ramifiée en dehors de S
$\mathrm{K}_v^{p,el}$	$\mathrm{K}_{\{v\}}^{p,el}$
Γ_v	$\mathrm{Gal}(\mathrm{K}_v^{p,el}/\mathrm{K})$
$\mathrm{L}_v^{p,el}$	$\mathrm{L}_{\{v^{(1)},\ldots,v^{(g)}\}}^{p,el}$ lorsque v est un premier de K

Corps locaux

K_v	complété de K pour $\lvert\cdot\rvert_v$
$\mathcal{M}_v/\mathrm{K}_v$	réunion des complétés des sous-extensions finies de $\mathcal{M}/\mathrm{K}$ lorsque $\mathcal{M}/\mathrm{K}$ est infinie
$\overline{\mathrm{K}_v}$	pro-p extension maximale de K_v
G_v	$\mathrm{Gal}((\mathrm{K}_S)_v/\mathrm{K}_v)$
$\overline{G_v}$	$\mathrm{Gal}(\overline{\mathrm{K}_v}/\mathrm{K}_v)$

Notations p-adiques

$\mathcal{R}_{\mathrm{K}}$	$\mathbb{Z}_p \otimes \mathrm{K}^\times$
$\mathcal{R}_v$	complétion p-adique de K_v, $v \in Pl_{\mathrm{K}}$
$\mathcal{U}_v$	complétion p-adique de $\mathcal{O}_{\mathrm{K}_v}$, $v \in Pl_{\mathrm{K}}$
$\mathcal{J}_{\mathrm{K}}$	$\prod_{v \in Pl_{\mathrm{K}}}^{res} \mathcal{R}_v$
$\mathcal{E}_S$	$\mathbb{Z}_p \otimes E_{\mathrm{K}}$
E_S^T	$E_{\mathrm{K}}^T \cap \ker\left(E \to \prod_{v \in S} \mathcal{U}_v\right)$
ι	plongement diagonal

Pro-p groupes (pour un pro-p groupe G fixé)

$[G,G]$	sous-groupe fermé normal de G engendré par ses commutateurs
G^{ab}	$G/[G,G]$
G^p	sous-groupe de G engendré par les puissances p-èmes
$G^{ab,p}$	$G/G^p[G,G]$
F_d	pro-p groupe libre à d générateurs
$H^k(G)$	$H^k(G,\mathbb{F}_p)$, k-ème groupe de cohomologie de G à valeurs dans $\mathbb{F}_p$
$d(G)$	$\dim_{\mathbb{F}_p} H^1(G)$
$r(G)$	$\dim_{\mathbb{F}_p} H^2(G)$
$Ш(G_{S,\mathrm{K}}^T)$	$\mathrm{Ker}\left(H^2(G_{\mathrm{K},S}^T) \to \bigoplus_v H^2(\overline{G_v})\right)$, noyau de Shafarevich

$\mathbb{Z}_p$-modules

$\mathrm{rg}_{\mathbb{Z}_p} M$	$\dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$, le $\mathbb{Z}_p$-rang de M
$\mathrm{Tor}_{\mathbb{Z}_p} M$	$\{x \in M,\ \exists p^k,\ p^k x = 0\}$, sous-module de torsion de M
$M[p]$	$\{x \in M,\ px = 0\}$, ensemble des éléments de p-torsion de M
$d_p M$	$\dim_{\mathbb{F}_p} \mathbb{F}_p \otimes_{\mathbb{Z}_p} M$, nombre minimal de générateurs de M

$\mathbb{Z}_p[\Delta]$-modules

I_Δ	$\langle \sigma - 1, \sigma \in \Delta \rangle$, idéal d'augmentation de l'algèbre $\mathbb{Z}_p[\Delta]$
M^Δ	$\{x \in M,\ \sigma \cdot x = x,\ \forall \sigma \in \Delta\}$, sous-groupe des invariants de M sous l'action de Δ
M_Δ	$M/I_\Delta M$, coinvariants de M sous l'action de Δ, plus grand quotient de M sur lequel Δ agit trivialement.

Si Δ d'ordre premier à p

$\mathbb{1}$	caractère trivial de Δ, *i.e.* caractère du module $M = \mathbb{Z}_p$
Rg	caractère de la représentation régulière, *i.e.* caractère de $M = \mathbb{Z}_p[\Delta]$
$\mathrm{Irr}(\Delta, \mathbb{Q}_p)$	ensemble des caractères $\mathbb{Q}_p$-irréductibles de Δ
$\mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$	$\mathrm{Irr}(\Delta, \mathbb{Q}_p) \backslash \{\mathbb{1}\}$
e_φ	$\frac{\psi(1)}{\lvert\Delta\rvert} \sum_{s \in \Delta} \varphi(s) s^{-1}$ pour $\varphi \in \mathrm{Irr}(\Delta, \mathbb{Q}_p)$ et $\psi \in \mathrm{Irr}(\Delta, \mathbb{C}_p), \psi \lvert \varphi$
$(e_\varphi)_{\varphi \in \mathrm{Irr}(\Delta, \mathbb{Q}_p)}$	système fondamental d'idempotents orthogonaux
M^φ	$e_\varphi M$

BIBLIOGRAPHIE

[1] D. J. Anick – « Noncommutative graded algebras and their Hilbert series », *J. Algebra* **78** (1982), no. 1, p. 120–140.

[2] S. Balady – « Families of cyclic cubic fields », *J. Number Theory* **167** (2016), p. 394–406.

[3] S. Balady & L. C. Washington – « A family of cyclic quartic fields with explicit fundamental units », *prépublication* (2017).

[4] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman & Y. Zhao – « Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves », *prépublication* (2017).

[5] A. Brumer – « Pseudocompact algebras, profinite groups and class formations », *J. Algebra* **4** (1966), p. 442–470.

[6] A. Brumer & K. Kramer – « The rank of elliptic curves », *Duke Math. J.* **44** (1977), no. 4, p. 715–743.

[7] C. W. Curtis & I. Reiner – *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing, Providence, RI, 2006, Reprint of the 1962 original.

[8] T. W. Cusick – « Lower bounds for regulators », in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, p. 63–73.

[9] J. S. Ellenberg, L. B. Pierce & M. Matchett Wood – « On ℓ-torsion in class groups of number fields », *ArXiv e-prints* (2016).

[10] J. S. Ellenberg & A. Venkatesh – « Reflection principles and bounds for class group torsion », *Int. Math. Res. Not. IMRN* (2007), no. 1, p. Art. ID rnm002, 18.

[11] P. Erdös – « Arithmetical properties of polynomials », *J. London Math. Soc.* **28** (1953), p. 416–425.

[12] P. Forré – « Strongly free sequences and pro-p-groups of cohomological dimension 2 », *J. Reine Angew. Math.* **658** (2011), p. 173–192.

[13] G. Frei & P. J. Roquette (éds.) – *Emil Artin and Helmut Hasse—the correspondence 1923–1958*, Contributions in Mathematical and Computational Sciences, vol. 5, Springer, Heidelberg, 2014, Translated from the German original by Franz Lemmermeyer.

[14] G. Gras – « A program to test the p-rationality of any number field », *prépublication* (2017).

[15] ———, « The p-adic kummer-leopoldt constant - normalized p-adic regulator », *Int. J. Number Theory* **à paraître** (2018).

[16] G. Gras – « Théorèmes de réflexion », *J. Théor. Nombres Bordeaux* **10** (1998), no. 2, p. 399–499.

[17] ———, *Class field theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003, From theory to practice, Translated from the French manuscript by Henri Cohen.

[18] ———, « On the T-ramified, S-split p-class field towers over an extension of degree prime to p », *J. Number Theory* **129** (2009), no. 11, p. 2843–2852.

[19] ———, « Les θ-régulateurs locaux d'un nombre algébrique : conjectures p-adiques », *Canad. J. Math.* **68** (2016), no. 3, p. 571–624.

[20] G. Gras & J.-F. Jaulent – « Sur les corps de nombres réguliers », *Math. Z.* **202** (1989), no. 3, p. 343–365.

[21] R. Greenberg – « Galois representations with open image », *Ann. Math. Qué.* **40** (2016), no. 1, p. 83–119.

[22] F. Hajir & C. Maire – « Analytic lie extensions of number fields with cyclic fixed points and tame ramification », *prépublication* (2017).

[23] F. Harary – *Graph theory*, Addison-Wesley Publishing Co., Reading, Mass.-Menlo Park, Calif.-London, 1969.

[24] H. Heilbronn – « On the 2-classgroup of cubic fields », in *Studies in Pure Mathematics (Presented to Richard Rado)*, Academic Press, London, 1971, p. 117–119.

[25] H. A. Helfgott & A. Venkatesh – « Integral points on elliptic curves and 3-torsion in class groups », *J. Amer. Math. Soc.* **19** (2006), no. 3, p. 527–550.

[26] J.-F. Jaulent & T. Nguyen Quang Do – « Corps p-rationnels, corps p-réguliers, et ramification restreinte », *J. Théor. Nombres Bordeaux* **5** (1993), no. 2, p. 343–363.

[27] J.-F. Jaulent – « Théorie ℓ-adique globale du corps de classes », *J. Théor. Nombres Bordeaux* **10** (1998), no. 2, p. 355–397.

[28] Y. Kishi – « A family of cyclic cubic polynomials whose roots are systems of fundamental units », *J. Number Theory* **102** (2003), no. 1, p. 90–106.

[29] H. Koch – *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer.

[30] J. Labute – « Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$ », *J. Reine Angew. Math.* **596** (2006), p. 155–182.

[31] J. Labute & J. Miná˘ c – « Mild pro-2-groups and 2-extensions of $\mathbb{Q}$ with restricted ramification », *J. Algebra* **332** (2011), p. 136–158.

[32] S. Lang – *Algebraic number theory*, second éd., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[33] O. Lecacheux – « Units in number fields and elliptic curves », in *Advances in number theory (Kingston, ON, 1991)*, Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, p. 293–301.

[34] C. Maire – « Compléments à un résultat de Safarevic », *Math. Nachr.* **198** (1999), p. 149–168.

[35] ———, « On the $\mathbb{Z}_l$-rank of abelian extensions with restricted ramification », *J. Number Theory* **92** (2002), no. 2, p. 376–404.

[36] ———, « Sur la dimension cohomologique des pro-p-extensions des corps de nombres », *J. Théor. Nombres Bordeaux* **17** (2005), no. 2, p. 575–606.

[37] ———, « Une estimation de la dimension de Krull des anneaux de déformations et ramification incomplète », in *Algèbre et théorie des nombres. Années 2003–2006*, Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. Nr., Lab. Math. Besançon, Besançon, 2006, p. 129–141.

[38] ———, « Sur la structure galoisienne de certaines pro-p-extensions de corps de nombres », *Math. Z.* **267** (2011), no. 3-4, p. 887–913.

[39] ———, « Some examples of fab and mild pro-p-groups with trivial cup-product », *Kyushu J. Math.* **68** (2014), no. 2, p. 359–376.

[40] J. S. Milne – *étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[41] A. Movahhedi & T. Nguyen-Quang-Do – « Sur l'arithmétique des corps de nombres p-rationnels », in *Séminaire de Théorie des Nombres, Paris 1987–88*, Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, p. 155–200.

[42] J. Neukirch, A. Schmidt & K. Wingberg – *Cohomology of number fields*, second éd., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[43] T. Nguyen-Quang-Do – « Formations de classes et modules d'Iwasawa », in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, p. 167–185.

[44] M. Ozaki – « Construction of maximal unramified p-extensions with prescribed Galois groups », *Invent. Math.* **183** (2011), no. 3, p. 649–680.

[45] L. B. Pierce – « The 3-part of class numbers of quadratic fields », *J. London Math. Soc. (2)* **71** (2005), no. 3, p. 579–598.

[46] L. B. Pierce – « A bound for the 3-part of class numbers of quadratic fields by means of the square sieve », *Forum Math.* **18** (2006), no. 4, p. 677–698.

[47] F. Pitoun & F. Varescon – « Computing the torsion of the p-ramified module of a number field », *Math. Comp.* **84** (2015), no. 291, p. 371–383.

[48] M. Rougnant – « Sur la propagation de la propriété *mild* au-dessus d'une extension quadratique imaginaire de $\mathbb{Q}$ », *Ann. Math. Qué.* **41** (2017), no. 2, p. 309–335.

[49] A. Schmidt – « Rings of integers of type $K(\pi, 1)$ », *Doc. Math.* **12** (2007), p. 441–471 (electronic).

[50] ———, « Über pro-p-fundamentalgruppen markierter arithmetischer kurven », *J. Reine Angew. Math.* **640** (2010), p. 203–235.

[51] J.-P. Serre – *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[52] ———, *Cohomologie galoisienne*, fifth éd., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994.

[53] J. Tate – « Nilpotent quotient groups », *Topology* **3** (1964), no. suppl. 1, p. 109–111.

[54] The PARI Group – Univ. Bordeaux, *PARI/GP version* `2.9.0`, 2016, available from `http://pari.math.u-bordeaux.fr/`.

[55] D. Vogel – « Circular sets of primes of imaginary quadratic number fields », preprint, 2006.

[56] K. Wingberg – « Free quotients of demushkin groups with operators », *prépublication* (2014).

[57] K. Wingberg – « Galois groups of local and global type », *J. Reine Angew. Math.* **517** (1999), p. 223–239.

Sur quelques aspects des extensions à ramification restreinte

Soit p un nombre premier, soit K/k une extension galoisienne finie de corps de nombres de degré premier à p et soit S un ensemble fini de premiers de k. Le groupe de Galois $G_{\mathrm{K},S}$ de la pro-p extension maximale de K non ramifiée en dehors de S est l'objet central de ce mémoire.

On se place dans un premier temps dans le cas modéré : on suppose que S ne contient pas les places divisant p. Les travaux combinés de Labute, Minac et Schmidt sur les pro-p groupes *mild* ont permis d'exhiber les premiers exemples de groupes $G_{\mathrm{K},S}$ de dimension cohomologique 2. En implémentant un corollaire de leur critère dans le logiciel PARI/GP, on observe un phénomène de propagation : si $\mathrm{k} = \mathbb{Q}$ et si le groupe $G_{\mathbb{Q},S}$ est *mild*, un fort pourcentage des groupes $G_{\mathrm{K},S}$ l'est également, pour K quadratique imaginaire. En associant au groupe $G_{\mathrm{K},S}$ deux graphes orientés dont les arcs sont définis par la ramification dans des extensions p-élémentaires, on démontre un critère théorique pour que ce phénomène de propagation ait lieu.

On considère ensuite le cas sauvage : toutes les places au-dessus de p sont contenues dans S. Le groupe de Galois $\Delta := \mathrm{Gal}(\mathrm{K}/\mathrm{k})$ agit sur $G_{\mathrm{K},S}$; on note G le plus grand quotient de $G_{\mathrm{K},S}$ sur lequel Δ agit trivialement et $\mathcal{H}$ le sous-groupe fermé de $G_{K,S}$ correspondant. Maire a étudié la liberté du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{H}^{ab}$. Nous poussons plus loin ses résultats en considérant les φ-composantes de $\mathcal{H}^{ab}$ sous l'action de Δ. Sous de bonnes hypothèses et sous la conjecture de Leopoldt, on démontre une condition nécessaire et suffisante pour que les φ-composantes soient libres ou non. La théorie du corps de classes permet de ramener cette condition à l'étude du régulateur normalisé, et donc à la p-rationalité du corps K. Les expérimentations faites sur PARI/GP dans des familles d'extensions cubiques cycliques, diédrales et cycliques de degré 4 du corps des rationnels corroborent une conjecture de Gras selon laquelle tout corps de nombres est p-rationnel pour p suffisant grand.

Mots-clefs : Extensions de corps de nombres à ramification restreinte ; Pro-p groupes G_S ; Pro-p groupes *mild* ; Algèbre d'Iwasawa ; Corps p-rationnels.

On some aspects of pro-p extensions with restricted ramification

Let p be a prime number, let K/k be a Galois extension of number fields and let S be a finite set of primes of K. We suppose that the degree of K/k is finite and coprime to p. We denote by $G_{K,S}$ the Galois group of the pro-p maximal extension of K unramified outside S. We focus on this thesis on two differents aspects of this pro-p group.

We are first interested in the tame case : we suppose that S does not contain any place above p. The works of Labute, Minac and Schmidt about mild pro-p groups brought the first examples of groups $G_{K,S}$ of cohomological dimension less two. Using a corollary of their criterium, we compute some examples with PARI/GP and we observe a propagation phenomenum : if we take $\mathrm{k} = \mathbb{Q}$ and if we suppose that $G_{\mathbb{Q},S}$ is mild, a large part of the pro-p groups $G_{\mathrm{K},S}$ with K imaginary quadratic are mild too. We then associate two oriented graphs to $G_{\mathrm{K},S}$ and we show a theoretical criterium proving mildness of some imaginary quadratic fields.

We then consider the wild case where all the places dividing p belong to S. The Galois group $\Delta := \mathrm{Gal}(\mathrm{K}/\mathrm{k})$ acts on $G_{\mathrm{K},S}$. The action of Δ is trivial on some quotients of $G_{\mathrm{K},S}$; we denote by G the maximal one and by $\mathcal{H}$ the corresponding closed subgroup of $G_{\mathrm{K},S}$. Maire has studied the $\mathbb{Z}_p[\![G]\!]$-freeness of the module $\mathcal{H}^{ab}$. We extend his results considering the φ-component of $\mathcal{H}^{ab}$ under the action of Δ. In a favourable context and under Leopoldt's conjecture, we show a necessary and sufficient condition for the freeness of the φ-components. This condition is connected to p-rational fields by class field theory. We present experiments with PARI/GP in some families of cubic cyclic, dihedral and quartic cyclic extensions of $\mathbb{Q}$ which support the following conjecture from Gras : every number field is p-rational for sufficiently large p.

Keywords : Extensions with restricted ramification ; Mild pro-p groups ; Iwasawa algebra ; p-rational fields.

MSC 2010 : 11R37, 11R29, 11R34, 12G10, 11R11.