

SUR LA PROPAGATION DE LA PROPRIÉTÉ MILD AU-DESSUS D'UNE EXTENSION QUADRATIQUE IMAGINAIRE DE Q

Marine Rougnant

▶ **To cite this version:**

Marine Rougnant. SUR LA PROPAGATION DE LA PROPRIÉTÉ MILD AU-DESSUS D'UNE EXTENSION QUADRATIQUE IMAGINAIRE DE Q. Annales mathématiques du Québec, 2016, 41 (2), pp.309–335. 10.1007/s40316-016-0071-9 . hal-01390775

HAL Id: hal-01390775
https://hal.science/hal-01390775

Submitted on 2 Nov 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

par

Marine Rougnant

Résumé. — Nous nous intéressons dans ce travail aux pro-p groupes G_S, groupes de Galois de pro-p extensions maximales de corps de nombres non ramifiées en dehors d'un ensemble fini S de places ne divisant pas p, et plus particulièrement à la propagation de la propriété *mild* au-dessus d'une extension quadratique imaginaire. Notre point de départ est le critère de Labute-Schmidt ([**12**]), basé sur l'étude du cup-produit sur le groupe de cohomologie $H^1(G_S, \mathbb{F}_p)$. Dans un contexte favorable, nous montrons par le calcul que le groupe étudié vérifie souvent une version faible (LS_f) du critère de Labute-Schmidt. Un critère théorique est ensuite établi, permettant de montrer le caractère *mild* de certains groupes auxquels le critère (LS_f) ne s'applique pas. Ce critère théorique est enfin appliqué à des exemples pour $p = 3$ et comparé aux travaux de Labute et Vogel ([**9**] et [**16**]).

Abstract. — In this work, we are interested in the pro-p groups G_S, which are Galois groups of maximal pro-p extensions of number fields unramified outside a finite set S of primes not dividing p. We focus on whether the mildness property is preserved over imaginary quadratic extensions. Our starting point is Labute-Schmidt's criterion ([**12**]), based on the study of the cup-product on the first cohomology group $H^1(G_S, \mathbb{F}_p)$. In favourable conditions, we show by computation that the group we study often satisfies a weak version (LS_f) of Labute-Schmidt's criterion. Then, a theoretical criterion is established for proving mildness of some groups to which the (LS_f) criterion does not apply. This theoretical criterion is finally illustrated by examples for $p = 3$ and compared to Labute and Vogel's works ([**9**] et [**16**]).

Table des matières

Introduction 1
1. Cadre et notations 3
2. Généralités 4
3. Calculs de cup-produits 8
4. Critère de Labute-Schmidt par rapport à S et calculs 10
5. Un critère de propagation du caractère *mild* de $G_S(\mathbb{Q})$ à $G_S(L)$ 13
6. Exemple complémentaire 19
Appendice A. Calcul local des cup-produits et critère (LS_f) : philosophie du code Pari-GP 21
Références 23

Introduction

Soit K un corps de nombres, p un nombre premier impair et S un ensemble fini de premiers de K de normes congrues à 1 modulo p. On s'intéresse au groupe de Galois $G_S(K) = \mathrm{Gal}(K_S|K)$ de la p-extension maximale de K non-ramifiée en dehors de S. Labute a montré en 2006 dans [**9**] que ces groupes peuvent

***Classification mathématique par sujets* (2000).** — 11R11, 11R34, 12G10 .
Mots clefs. — ramification restreinte, pro-p groupes G_S, pro-p groupes *mild* .

Je tiens à remercier Christian Maire pour son intérêt pour ce travail et ses remarques précieuses, ainsi que Bill Allombert pour sa patience et ses conseils dans l'élaboration des programmes.

être *mild* (définition 2.10) et donc de dimension cohomologique 2 : il détermine, dans le cas du corps des rationnels, une condition arithmétique sur S pour qu'un groupe $G_S(K)$ soit *mild* et en exhibe des exemples concrets. Ses résultats seront étendus au cas d'une extension quadratique imaginaire par Vogel ([**16**]) la même année. Ces deux articles s'appuient sur les résultats de Anick ([**1**]) et Koch ([**8**, chap. 7]), sur une description explicite du début des relations du groupe $G_S(K)$. Une autre approche, plus fonctorielle, est d'étudier le cup-produit sur le premier groupe de cohomologie de $G_S(K)$ à valeurs dans $\mathbb{F}_p$. C'est le parti pris par Schmidt dans [**13**], puis dans [**12**] pour montrer le critère de Labute-Schmidt 2.12 qui est le point de départ de ce travail.

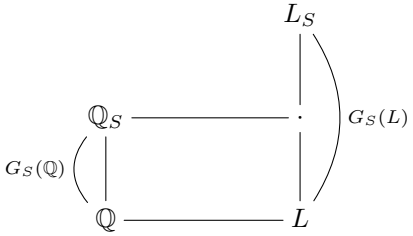
La question de la propagation du caractère *mild* d'un groupe $G_S(K)$ est vaste. Considérons une extension L de K et $G_S(L)$ le groupe de Galois correspondant, où on note par abus S l'ensemble des places de L divisant les éléments de S. Le caractère *mild* se conserve-t-il lorsque $G_S(K)$ est un quotient de $\mathrm{Gal}(L_S|K)$? 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 [**5**] permet de répondre en partie à cette dernière question, dans le cas d'une extension quadratique du corps des rationnels de p-groupe de classes trivial : en s'appuyant sur un résultat de théorie des groupes de Tate ([**15**]), le résultat de Gras montre que si les premiers de S sont inertes dans l'extension $L|K$, alors le groupe $G_S(L)$ est isomorphe à $G_S(K)$. Les groupes $G_S(K)$ et $G_S(L)$ sont donc dans ce cas simultanément *mild*.

On étudie ici le cas où L est une extension quadratique imaginaire de $\mathbb{Q}$ (différente de $\mathbb{Q}(j)$ si $p = 3$) dans laquelle tous les premiers de S se décomposent, en supposant de plus que son p-groupe de classes est trivial. Cette dernière hypothèse permet de considérer localement les éléments du deuxième groupe de cohomologie, et en particulier les cup-produits qui pourront alors être calculés grâce à des outils de théorie du corps de classes. Pour simplifier les calculs, on ne considère que des extensions quadratiques du corps des rationnels $\mathbb{Q}$, mais un raisonnement similaire est envisageable dans un cadre plus général.

La problématique est donc la suivante :

Question 0.1. — *En supposant que le groupe $G_S(\mathbb{Q})$ est mild, sous quelles conditions le groupe $G_S(L)$ conserve-t-il cette propriété ?*



Les hypothèses sous lesquelles on se place permettent de considérer une version faible (LS_f) du critère de Labute-Schmidt. Les deux critères ne sont pas équivalents, mais la version faible peut être implémentée afin de calculer des statistiques : si (LS_f) est vérifié par le groupe $G_S(\mathbb{Q})$ (on dit alors que $\mathbb{Q}$ vérifie le critère de Labute-Schmidt en respectant S), à quelle proportion de groupes $G_S(L)$ le critère (LS_f) s'applique-t-il ?

A S fixé tel que $\mathbb{Q}$ vérifie le critère de Labute-Schmidt en respectant S, on note $\mathbb{E}_S$ l'ensemble $\{d \in \mathbb{N}|\ d = \mathrm{disc}(L), L = \mathbb{Q}(\sqrt{-m}), \#\mathrm{Cl}_p(L) = 1, \forall v \in S,\ m \in \mathbb{F}_v^2\}$ des discriminants de corps quadratiques imaginaires de p-groupe de classes trivial dans lesquels éléments de S sont décomposés. On calcule grâce à la méthode des premiers auxiliaires (section 4.1) la quantité

$$P_{S,p}(X) = \frac{\#\{d \leqslant X|\ d \in \mathbb{E}_S, \text{le critère } (LS_f) \text{ s'applique à } \mathbb{Q}(\sqrt{-d})\}}{\#\{d \leqslant X|\ d \in \mathbb{E}_S\}}$$

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 définis par un élément d'un ensemble $\mathbb{E}_S$, certains ne vérifient pas le critère (LS_f), mais vérifient le critère de Labute-Schmidt 2.12. Pour étudier le caractère *mild* de ces groupes, on introduit les graphes quasi-circulaires :

Définition 0.2. — Un graphe est dit quasi-circulaire s'il admet un sous-graphe couvrant dont les sommets sont de degré entrant égal à 1.

En associant à S deux graphes bipartis $\mathcal{G}_S$ et $\mathcal{G}_S^*$ dont les sommets sont les premiers de S et dans lequel un arc relie le premier v au premier w si les premiers de L divisant v et w vérifient certaines conditions de ramification dans les p-extensions élémentaires de L non ramifiée en dehors de $u'|u$ pour $u \in S$, on montre dans la section 5.3 :

Théorème 0.3. — *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 $L|\mathbb{Q}$.*

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

Plan de l'article :

On commencera par fixer certaines notations, puis on justifiera dans une deuxième section le choix du contexte dans lequel se place ce travail en rappelant quelques généralités sur les groupes de Galois d'extensions à ramification restreinte et les groupes *mild*. Le calcul de cup-produits fera l'objet d'une troisième section, ce qui permettra d'obtenir des statistiques sur la propagation du caractère (LS_f). Nous déterminerons alors dans la cinquième section des conditions sur la ramification des premiers de S assurant au groupe $G_S(L)$ d'être *mild*, puis nous introduirons les graphes $\mathcal{G}_S$ et $\mathcal{G}_S^*$ pour enfin montrer le théorème 0.3. 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 ([**16**]).

Tous les calculs ont été effectués avec Pari/GP ([**2**])

1. Cadre et notations

A l'exception de la section 2.1, on se place dans la situation décrite dans l'introduction. 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. On suppose de plus que tout élément de S est décomposé dans l'extension $L|\mathbb{Q}$ et de norme congrue à 1 modulo p.

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

L'ensemble des premiers de L divisant les éléments de S sera noté S', ou S lorsque cela ne présentera aucune ambiguïté. On utilisera les notations suivantes :

K	corps de nombres
K^{nr}	extension non-ramifiée maximale de K
$v^{(1)}, \dots, v^{(g)}$	premiers divisant v dans une extension $L\|K$ lorsque v est un premier de K
$D_{v^{(i)}}(L\|K)$	groupe de décomposition de $v^{(i)}$ dans l'extension $L\|K$
$I_{v^{(i)}}(L\|K)$	groupe d'inertie de $v^{(i)}$ dans l'extension $L\|K$
K_S	pro-p extension non-ramifiée en dehors de S maximale de K
$G_S(K)$	$\mathrm{Gal}(K_S\|K)$
$K_S^{p,el}$	p-extension élémentaire maximale de K non ramifiée en dehors de S
$K_v^{p,el}$	$K_{\{v\}}^{p,el}$
Γ_v	$\mathrm{Gal}(K_v^{p,el}\|K)$
$L_v^{p,el}$	$L_{\{v^{(1)},\dots,v^{(g)}\}}^{p,el}$ lorsque v est un premier de K
K_v	complété de K pour $\|\cdot\|_v$
$M_v\|K_v$	réunion des complétés des sous-extensions finies de $M\|K$ lorsque $M\|K$ est infinie
$\overline{K_v}$	pro-p extension maximale de K_v
G_v	$\mathrm{Gal}((K_S)_v\|K_v)$
$\overline{G_v}$	$\mathrm{Gal}(\overline{K_v}\|K_v)$
$\mathrm{Cl}(K)$	p-groupe des classes de K
E_K	groupe des unités de $\mathcal{O}_K$
$H^k(G)$	$H^k(G, \mathbb{F}_p)$, k-ième groupe de cohomologie de G à valeurs dans $\mathbb{F}_p$
$d(G)$	$\dim_{\mathbb{F}_p} H^1(G)$
$r(G)$	$\dim_{\mathbb{F}_p} H^2(G)$
$Ш_S(G_S(K))$	$\mathrm{Ker}\left(H^2(G_S(K)) \to \bigoplus_v H^2(\overline{G_v})\right)$, noyau de Shafarevich

2. Généralités

2.1. 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.

2.1.1. Relations de $G_S(K)$. — Soit v un premier quelconque de K. L'injection $i_v : G_v \hookrightarrow G_S(K)$ et la surjection $\pi_v : \overline{G_v} \twoheadrightarrow G_v$ permettent de définir les applications :

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

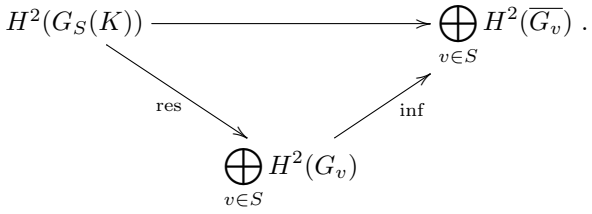
puis les applications induites :

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

où les sommes directes peuvent être restreintes aux premiers de K qui se ramifient dans $K_S|K$. En effet, si v est non-ramifié dans $K_S|K$, alors l'extension $(K_S)_v|K_v$ est non-ramifiée et on a les surjections $\overline{G_v} \twoheadrightarrow \mathrm{Gal}(K_v^{nr}|K_v)$ et $\mathrm{Gal}(K_v^{nr}|K_v) \twoheadrightarrow G_v$, où K_v^{nr} désigne la pro-p extension non-ramifiée maximale de K_v. Par transitivité de l'inflation on a alors :

$$\inf_{\overline{G_v}}^{G_v} = \inf_{\overline{G_v}}^{\mathrm{Gal}(K_v^{nr}|K_v)} \circ \inf_{\mathrm{Gal}(K_v^{nr}|K_v)}^{G_v}.$$

Mais $\mathrm{Gal}(K_v^{nr}|K_v)$ est un pro-p groupe libre, donc $H^2(\mathrm{Gal}(K_v^{nr}|K_v)) = 0$ et $\inf_{\mathrm{Gal}(K_v^{nr}|K_v)}^{G_v} : H^2(G_v) \to H^2(\mathrm{Gal}(K_v^{nr}|K_v))$ est identiquement nulle. L'application $\inf_{\overline{G_v}}^{G_v}$ est donc identiquement nulle pour tout v non-ramifié dans $K_S|K$ et on a :



Définition 2.1. — On note $Ш_S(G_S(K))$ (ou $Ш_S$) le noyau de l'application $\inf \circ \mathrm{res} : H^2(G_S(K)) \longrightarrow \bigoplus_v H^2(\overline{G_v})$. C'est le noyau de Shafarevich du groupe $G_S(K)$.

D'après le diagramme commutatif ci-dessus, lorsque le groupe $Ш_S$ est trivial, les relations du groupe $G_S(K)$ 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 [**8**], th. 10.2), il y a un réel intérêt à se placer dans une telle situation. Cependant, le groupe $Ш_S$ n'est en général pas connu. Koch, dans [**8**, th. 11.3], montre qu'il s'injecte dans le dual d'un objet bien connu.

Pour S un ensemble fini (éventuellement vide) de premiers d'un corps de nombres K de normes congrues à 1 modulo p, on note $V_S = \{\alpha \in K^\times | (\alpha) = \mathfrak{a}^p, \alpha \in K_v^p \text{ pour } v \in S\}$ où (α) désigne l'idéal fractionnaire principal engendré par α.

Théorème 2.2 **(Koch, [8])**. — *Si K est un corps de nombres, on a une injection naturelle*

$$Ш_S \hookrightarrow \left(V_S/K^{\times p}\right)^*.$$

Ce résultat permet de se placer sous un ensemble d'hypothèses annulant $Ш_S$:

Théorème 2.3. — *Si $K = \mathbb{Q}$ 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.*

Démonstration. — Par définition, pour tout $x \in V_\emptyset(K)$ il existe un idéal $\mathfrak{a}$ de $K^\times$ 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 $\overline{\varphi} : V_\emptyset(K)/K^{\times p} \to \mathrm{Cl}(K)$ de noyau E_K/E_K^p, où $\mathrm{Cl}(K)$ est le p-groupe des classes de K et E_K est le groupe des unités de $\mathcal{O}_K$. D'après le théorème des unités de Dirichlet, E_K/E_K^p est isomorphe au produit du groupe libre $\mathbb{F}_p^{r_1+r_2-1}$ et du groupe $\mu_p(K)$ des racines de l'unité contenues dans K. On a donc :

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

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

On conclut avec le théorème 2.2 en remarquant que $V_S(K)/K^{\times p}$ est un sous-groupe de $V_\emptyset(K)/K^{\times p}$. □

2.1.2. Structure de $H^1(G_S(K))$. — La formule suivante, due à Shafarevich et dont on trouve une preuve par exemple dans [**8**, th. 11.8], donne le nombre de générateurs du groupe $G_S(K)$:

***Théorème 2.4* (Formule du p-rang, [14]).** — *Soit K un corps de nombres et soit S un ensemble fini de places de K. Alors :*

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

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

On peut de plus montrer, grâce à des arguments classiques, que sous de bonnes hypothèses arithmétiques, le groupe de cohomologie $H^1(G_S(K))$ est somme directe de p-groupes.

Définition 2.5. — Pour S un ensemble (éventuellement vide) de places de K, on note $K_S^{p,el}|K$ 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 $K_v^{p,el}$ le corps $K_{\{v\}}^{p,el}$ et Γ_v le groupe $\mathrm{Gal}(K_v^{p,el}|K)$.

Théorème 2.6. — *Soit K un corps de nombres de p-groupe des classes trivial et S un ensemble fini de places de K de normes congrues à 1 modulo p. Si on suppose que les unités sont des puissances p-ièmes en les places v de S, alors on a la décomposition :*

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

En particulier $d(G_S(K)) = |S|$.

Démonstration. — La preuve repose sur la théorie ℓ-adique du corps de classes (voir par exemple [**7**]).

On a la suite exacte :

$$1 \to \textstyle\prod_{v\in S}\mathcal{U}_v\Big/\mathcal{E}_K \to \mathcal{J}_K\Big/\mathcal{R}_K\prod_{v\notin S}\mathcal{U}_v \to \mathcal{J}_K/\mathcal{R}_K\mathcal{U}_K \to 1,$$

où $\mathcal{J}_K$ désigne le p-groupe des idèles de K, $\mathcal{R}_K = \mathbb{Z}_p \otimes K^\times$, $\mathcal{E}_K = \mathbb{Z}_p \otimes E_K$ et $\mathcal{U}_v = \varprojlim_k U_v\Big/U_v^{p^k}$. De plus, on a les isomorphismes :

$$\mathcal{J}_K\Big/\mathcal{R}_K\prod_{v\notin S}\mathcal{U}_v \simeq G_S(K)^{ab} \quad \text{et} \quad \mathcal{J}_K/\mathcal{R}_K\mathcal{U}_K \simeq G_\emptyset^{ab} = \mathrm{Cl}(K).$$

Ici on suppose que le p-groupe des classes de K est trivial, donc en quotientant par les puissances p-ièmes, la suite exacte devient :

$$G_S^{p,el} \simeq \textstyle\prod_{v\in S}\mathcal{U}_v\Big/\mathcal{E}_K\mathcal{J}_K^p \cap \prod_{v\in S}\mathcal{U}_v = \prod_{v\in S}\mathcal{U}_v\Big/\mathcal{E}_K\prod_{v\in S}\mathcal{U}_v^p.$$

Les unités sont des puissances p-ièmes en les places v de S, donc finalement :

$$\prod_{v\in S}\mathcal{U}_v\Big/\mathcal{U}_v^p \simeq G_S^{p,el}.$$

En reprenant la suite exacte pour $S = \{v\}$, on obtient l'isomorphisme $\mathcal{U}_v\Big/\mathcal{U}_v^p \simeq G_v^{p,el}$, et on a bien le résultat énoncé. □

Corollaire 2.7. — *Si $K = \mathbb{Q}$ ou si K est une extension quadratique imaginaire de $\mathbb{Q}$ vérifiant les conditions décrites dans la section 1, on a la décomposition*

$$H^1(G_S) \simeq \bigoplus_{v\in S} H^1(\Gamma_v).$$

Démonstration. — Sous ces hypothèses, $\mathcal{E}_K = (1)$. On peut donc appliquer le théorème 2.6, puis conclure en dualisant. □

Remarque 2.8. — Sous les hypothèses du théorème 2.6, l'espace vectoriel $H^1(\Gamma_v)$ est de dimension 1 pour tout v dans S.

2.2. Pro-p groupes *mild* et critère de Labute-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

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

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 **[3]**, ou **[8**, 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 **[3]**.

***Définition 2.9* (Forré, [3])**. — 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 **[9]**, sans avoir recours à l'étude d'algèbres de Lie.

Définition 2.10. — 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 **[9]**, et Forré, dans **[3]**, ont démontré qu'un groupe *mild* possède des propriétés intéressantes, notamment :

***Théorème 2.11* (Labute, [9])**. — *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* $\mathrm{gr}(\mathbb{F}_\mathrm{p}[[\mathrm{G}]])$ *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 $\mathrm{gr}(\mathbb{F}_\mathrm{p}[[\mathrm{G}]])$ *est* $\dfrac{1}{1 - dt + \sum_{i=1}^{r} t^{\deg(\rho_\mathrm{i})}}$.

Montrer qu'un pro-p groupe est *mild* en appliquant la définition 2.10 nécessite d'avoir une description explicite du début des relations de G. Schmidt donne dans **[12]** un critère permettant d'établir le caractère *mild* d'un pro-p groupe en étudiant le cup-produit sur son premier groupe de cohomologie. Ce résultat repose sur un critère d'Anick et sur le travail de Labute (**[9]**), et est ensuite étendu par Gärtner dans **[4]** au cas des pro-p groupes dont le cup-produit est trivial.

***Théorème 2.12* (Critère de Labute-Schmidt, [12], [13])**. — *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 :*

- *il existe deux $\mathbb{F}_p$-espaces vectoriels U et V tels que $H^1(G) \simeq U \oplus V$,*
- *la restriction du cup-produit $\cup : H^1(G) \times H^1(G) \to H^2(G)$ à $V \otimes V$ est identiquement nulle,*
- *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 cet article, 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 $G_S(K)$ 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 2.13. — *Si il existe deux $\mathbb{F}_p$-espaces vectoriels U et V tels que :*

(i) $H^1(G_S(K)) \simeq U \oplus V$,

(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 $G_S(K)$ *est mild et* $r(G_S(K)) = \dim_{\mathbb{F}_p} H^2(G_S(K)) = |S|$.

De plus, d'après le corollaire 2.7, on a la décomposition :

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

On supposera donc naturellement que la décomposition de $H^1(G_S(K))$ vérifiant le critère de Labute-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 2.14. — *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) $H^1(G_S(K)) \simeq U \oplus V$,

(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 $G_S(K)$ *est mild et* $r(G_S(K)) = \dim_{\mathbb{F}_p} H^2(G_S(K)) = |S|$.

Définition 2.15. — On dira dans ce cas que le corps K vérifie le critère de Labute-Schmidt en respectant S. On fera référence au corollaire 2.14 par la notation (LS_f).

Remarque 2.16. — Pour que le corps K vérifie le critère de Labute-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 2.17. — Le critère de Labute-Schmidt et sa version faible (LS_f) ne sont pas équivalents (l'exemple 6.1 est un contre-exemple).

3. Calculs de cup-produits

3.1. 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 section 1), k est une extension finie de $\mathbb{Q}_v$ pour un certain $v \in S$. On note $\hat{k}$ 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-ièmes de l'unité, et on notera ζ_p une racine primitive p-ième 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-ièmes de l'unité μ_p. On suit ici ce qui est fait, par exemple, dans [**8**, chap. 10] et [**11**, chap.7].

La suite exacte de Kummer

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

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

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

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

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

Toujours d'après le théorème d'Hilbert 90, λ^* est injective. On obtient donc de la deuxième suite exacte de cohomologie la $\mathbb{F}_p$-dimension de $H^2(\overline{G},\hat{k}^\times)[p]$: $\dim_{\mathbb{F}_p} H^2(\overline{G},\hat{k}^\times)[p]=\dim_{\mathbb{F}_p} H^2(\overline{G})$. 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 **[8]**,10.2). Le groupe $H^2(\overline{G},\hat{k}^\times)[p]$ 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 $\mu_p\subset k$). On peut expliciter un tel isomorphisme. En notant

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

où $\mathrm{inv}_k : H^2(\overline{G},\hat{k}^\times)\to\mathbb{Q}/\mathbb{Z}$, la composition $\psi=\iota\circ\lambda^*$ est un isomorphisme de $H^2(\overline{G})$ sur μ_p ([**8**, sec. 8.9]).

D'autre part, si $\alpha\in k^\times$ 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

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

On peut alors montrer :

Proposition 3.1. — *L'application φ fait commuter le diagramme :*

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

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 [**11**, prop.7.2.13]. □

Corollaire 3.2. — *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 $\alpha\in k^\times/k^{\times p}$ tel que $\chi=\varphi\alpha$. Comme χ est un caractère non ramifié, α est une unité et d'après la proposition 3.1, 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 par la théorie du corps de classes à α. 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 $\dim_k H^1(G^{nr})^\perp=1$ et on a bien égalité. □

3.2. 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 la section 1 .

D'après le théorème 2.3, le groupe de cohomologie $H^2(G_S(K))$ s'injecte dans la somme $\bigoplus_{v\in S} H^2(\overline{G_v})$. On appellera « calcul local » des cup-produits de caractères de $G_S(K)$ le calcul de l'image de ces cup-produits dans $\bigoplus_{v\in S} H^2(\overline{G_v})$. La commutativité du diagramme

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

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 2.7 que le groupe $H^1(G_S(K))$ 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 3.3. — *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 :*

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

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 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 $K_w^{p,el}|K$.

□

4. Critère de Labute-Schmidt par rapport à S et calculs

4.1. 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 (LS_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 [**10**, 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 $K_v^{p,el}|K$,
- p_v est totalement décomposé dans l'extension $K_w^{p,el}|K$ pour $w \in S, w \neq v$.

Le Frobenius en p_v, noté F_{p_v}, engendre le groupe de décomposition $D_{p_v}(L_S^{p,el}|L)$. Or, par hypothèses, $D_{p_v}(K_S^{p,el}|K) = I_v(K_v^{p,el}|K)$, donc F_{p_v} engendre le groupe d'inertie $I_v(K_v^{p,el}|K)$ et la famille $\{F_{p_v}, v \in S\}$ est une base de $\mathrm{Gal}(K_S^{p,el}|K)$. 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 4.1. — *Avec les notations précédentes, si v, w sont deux éléments de S avec v inerte dans $K_w^{p,el}|K$, 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 $K_w^{p,el}|K$. D'après la proposition 3.1, $(\widetilde{\chi}_w \cup \widetilde{\chi}_v)_w = \inf \cdot \mathrm{res}_w(\widetilde{\chi}_w)(\sigma_v)$, 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 $K_w^{p,el}|K$. □

Remarque 4.2. — 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 4.3. — Les entiers l_{vw} ainsi définis sont appelés *linking numbers* par Labute dans [**9**] et Vogel dans [**16**] (voir sec. 6.2).

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

Proposition 4.4. — *Sous les hypothèses décrites dans la section 1, 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 $G_S(K)$ est mild et $r(G_S(K)) = \dim_{\mathbb{F}_p} H^2(G_S(K)) = |S|$.

4.2. 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 ([**2**]), ce procédé permet d'obtenir des exemples variés de pro-p groupes *mild*. La philosophie du code utilisé est présentée en annexe A.

Exemple 4.5. — Soit $p = 3$, $K = \mathbb{Q}$ 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 4.4 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 4.4, donc le groupe $G_S(K)$ est *mild*.

Le groupe $G_S(K)$ dépend de trois données : le corps de base K, le premier p et l'ensemble S de places de K. Soit $L|\mathbb{Q}$ une extension quadratique et S un ensemble fini de nombres premiers tels que les corps $\mathbb{Q}$ et L vérifient le critère de Labute-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 la section 1, un corps quadratique ne peut vérifier le critère de Labute-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 4.6. — Soit $S = \{31, 61, 151, 211\}$. Le corps $L = \mathbb{Q}(\sqrt{-15})$ vérifie le critère de Labute-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-Schmidt en respectant S. Les exemples suivants montrent qu'il peut exister plusieurs corps quadratiques vérifiant le critère de Labute-Schmidt en respectant S.

Exemple 4.7. — Soit $p = 3$ et $S = \{7, 13, 79, 97\}$. La proposition 4.4 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 4.8. — Soit $S = \{37, 103, 127, 139\}$ et $L = \mathbb{Q}(\sqrt{-d})$ 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-Schmidt en respectant S.

4.3. Quelques données statistiques. — Les exemples 4.7 et 4.8 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 la section 1, de discriminant borné, auquel la proposition 4.4 s'applique.
On note $\mathbb{E}_S = \{d \in \mathbb{N} |\ d = \mathrm{disc}(L), L = \mathbb{Q}(\sqrt{-m}), \#\mathrm{Cl}_p(L) = 1, \forall v \in S, m \in \mathbb{F}_v^2\}$, l'ensemble des discriminants de corps quadratiques imaginaires de p-groupe de classes trivial dans lesquels éléments de S sont décomposés.

On calcule

$$P_{S,p}(X) = \frac{\#\{d \leqslant X |\ d \in \mathbb{E}_S, \text{la proposition 4.4 s'applique à } \mathbb{Q}(\sqrt{-d})\}}{\#\{d \leqslant X |\ d \in \mathbb{E}_S\}}.$$

Les tableaux suivants présentent les valeurs de $P_{S,3}(10^5)$ et $P_{S,5}(10^4)$ pour différents exemples d'ensembles S tels que $\mathbb{Q}$ vérifie le critère de Labute-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	$P_{S,5}(10^5)$
$\{101, 131, 211, 251\}$	$\frac{1931}{2888} \simeq 0.6686$
$\{11, 31, 41, 211\}$	$\frac{1820}{2561} \simeq 0.7107$
$\{31, 181, 191, 271\}$	$\frac{1970}{2865} \simeq 0.6876$
$\{211, 251, 401, 421\}$	$\frac{1897}{2916} \simeq 0.6505$

5. Un critère de propagation du caractère *mild* de $G_S(\mathbb{Q})$ à $G_S(L)$

Soit p un nombre premier, L un corps quadratique imaginaire et S un ensemble fini de nombres premiers vérifiant les conditions énoncées dans la section 1. Afin d'alléger les notations, les groupes $G_S(\mathbb{Q})$ et $G_S(L)$ seront respectivement notés G_S et H_S dans toute cette section et les autres notations seront adaptées en conséquence.

5.1. Cup-produits d'éléments de $H^1(H_S)$. — On a vu dans la section 3.2 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 $L|\mathbb{Q}$ 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 $L|\mathbb{Q}$, 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 5.1. — *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 [**11**, prop. 1.5.3] pour le carré de gauche et [**11**, prop. 1.5.5] pour le carré de droite. □

On suppose pour la suite que le corps K vérifie le critère de Labute-Schmidt en respectant S et on notera U et V les sous-espaces vectoriels de $H^1(G_S)$ vérifiant les hypothèses du critère (LS_f). D'après le théorème 2.6, 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 $\Gamma_v = \mathrm{Gal}(K_v^{p,el}|K)$ et $\gamma_w = \mathrm{Gal}(L_w^{p,el}|L)$ 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 $H^1(\gamma_w)$.

5.1.1. 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 $L\mathbb{Q}_v^{p,el}$. Comme v est totalement ramifié dans $\mathbb{Q}_v^{p,el}|\mathbb{Q}$ et totalement décomposé dans $L|\mathbb{Q}$, $v^{(1)}$ et $v^{(2)}$ sont ramifiés dans $F|L$. L'extension $F|L$ est donc une sous-extension de $L_v^{p,el}|L$ de degré p, distincte de $L_{v^1}^{p,el}|L$ et $L_{v^2}^{p,el}|L$.

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 $L|\mathbb{Q}$, 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 5.2. — *Le diagramme suivant est commutatif :*

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

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

5.1.2. Critère de Labute-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 2.13 s'applique à $H^1(H_S) = \overline{U} \oplus \overline{V}$.

Lemme 5.3. — *On note $\overline{V} = \underline{V}$. 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-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 5.2. □

Lemme 5.4. — *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 :

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

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 digramme est commutatif d'après le lemme 5.2. D'après le théorème 2.3,

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 2.14, on a de plus la surjection $U \otimes V \twoheadrightarrow \bigoplus_{v\in S} H^2(\overline{G_v})$. D'après le lemme 5.2, la flèche du bas est donc une surjection. Les observations du paragraphe 5.1.1 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 $L_{v^1}^{p,el}|L$ et décomposé dans $L_{v^2}^{p,el}|L$, et v^1 et v^2 sont décomposés dans $L_{u_v^1}^{p,el}|L$.

(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 $L_{u^1}^{p,el}|L$, et u^1 est inerte dans $L_{v_u^i}^{p,el}|L$ et $L_{v_u^j}^{p,el}|L$.

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 $L_{v_u^1}^{p,el}|L$ et décomposé dans $L_{v_u^2}^{p,el}|L$, et v_u^1 et v_u^2 sont décomposés dans $L_{u^1}^{p,el}|L$.

(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 $L_{u_v^1}^{p,el}|L$, et u_v^1 est inerte dans $L_{v^i}^{p,el}|L$ et $L_{v^j}^{p,el}|L$.

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 5.5. — *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 3.3 :

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

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 3.3, 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 3.3 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 raisonnement 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 5.6. — 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 5.7. — *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 5.4. 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-Schmidt en respectant S et que les hypothèses sur la ramification des premiers de S considérées ci-dessus sont vérifiés, alors les lemmes 5.3 et 5.7 s'appliquent et les hypothèses du critère (LS_f) sont vérifiées.

Proposition 5.8. — *Si $\mathbb{Q}$ vérifie le critère de Labute-Schmidt en respectant S et si l'une des hypothèses $(H1)$ ou $(H2)$ est vérifée, alors le groupe H_S est mild et $d(H_S) = r(H_S) = 2|S|$.*

5.2. Utilisation de l'action galoisienne. — Le groupe de Galois $\mathrm{Gal}(L|\mathbb{Q})$, 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 $L_{u^1}^{p,el}|L$ est ramifiée (resp. décomposée, inerte) dans l'extension $\sigma(L_{u^1}^{p,el})|L$. En particulier, $\sigma(L_{u^1}^{p,el})|L$ est une extension de degré p non-ramifiée en dehors de $u^2 = \sigma(u^1)$. Par maximalité de $L_{u^2}^{p,el}$, on déduit

$\sigma(L^{p,el}_{u^1}) = L^{p,el}_{u^2}$.

Ces observations permettent de réécrire les hypothèses de la proposition 5.8. On considère l'hypothèse $(H1)$, le résultat s'étendra à $(H2)$ par symétrie. Les deux points de $(H1)$ sont stables sous l'action de $\mathrm{Gal}(L|\mathbb{Q})$. En effet, sous l'action de $\mathrm{Gal}(L|\mathbb{Q})$, 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 $L^{p,el}_{v^2}|L$ et décomposé dans $L^{p,el}_{v^1}|L$, et v^2 et v^1 sont décomposés dans $L^{p,el}_{u_v^2}|L$.

(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 $L^{p,el}_{u^2}|L$, et u^2 est inerte dans $L^{p,el}_{v_u^j}|L$ et $L^{p,el}_{v_u^i}|L$.

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 $L^{p,el}_{v^1}|L$, et v^1 est décomposé dans $L^{p,el}_{u_v^1}|L$ et $L^{p,el}_{u_v^2}|L$, 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 $L^{p,el}_{u^1}|L$, et u^1 est inerte dans $L^{p,el}_{v_u^1}|L$ et $L^{p,el}_{v_u^2}|L$, 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 $L^{p,el}_{v_u^1}|L$, et v_u^1 est décomposé dans $L^{p,el}_{u^1}|L$ et $L^{p,el}_{u^2}|L$, 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 $L^{p,el}_{u_v^1}|L$, et u_v^1 est inerte dans $L^{p,el}_{v^1}|L$ et $L^{p,el}_{v^2}|L$, 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 5.8 devient alors :

Proposition 5.9. — *Si $\mathbb{Q}$ vérifie le critère de Labute-Schmidt en respectant S et si l'une des hypothèses $(H1')$ ou $(H2')$ est vérifiée, alors le groupe H_S est mild et $d(H_S) = r(H_S) = 2|S|$.*

5.3. Graphes quasi-circulaires. — On conserve les mêmes notations. On suppose que $\mathbb{Q}$ vérifie le critère de Labute-Schmidt en respectant S pour la décomposition $S = \mathcal{U} \cup \mathcal{V}$, et on construit les graphe 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 $L^{p,el}_{v_j^1}|L$, et le premier v_j^1 est inerte dans les extensions $L^{p,el}_{v_i^1}|L$ et $L^{p,el}_{v_i^2}|L$, 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 $L^{p,el}_{v_j^1}|L$, et le premier v_j^1 est décomposé dans les extensions $L^{p,el}_{v_i^1}|L$ et $L^{p,el}_{v_i^2}|L$, 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 5.10. — 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 5.11. — 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 5.12. — *Si $\mathbb{Q}$ vérifie le critère de Labute-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 5.9 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 5.12 est équivalent à la proposition 5.9, d'où le résultat.

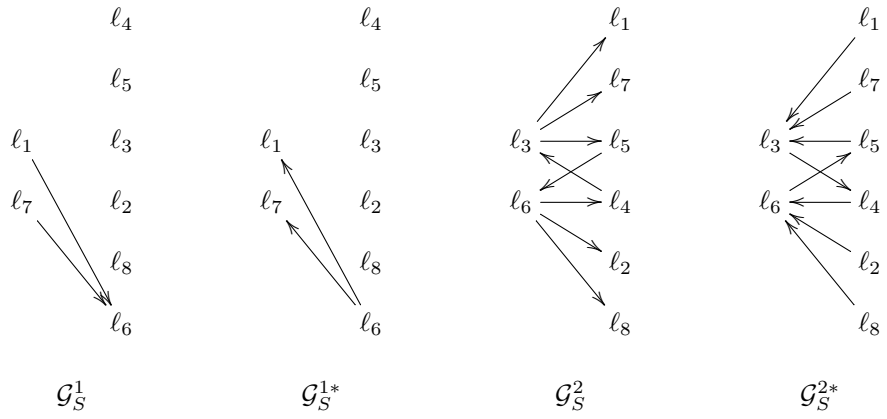
□

Remarque 5.13. — On peut montrer (voir par exemple [**6**, 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 5.14. — *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 5.15. — 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-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 5.12 peut être vérifié pour l'une des deux décomposition sans l'être pour l'autre.
  Exemple : Soit $S = \{\ell_1 = 7, \ell_2 = 43, \ell_3 = 61, \ell_4 = 103, \ell_5 = 109, \ell_6 = 163, \ell_7 = 223, \ell_8 = 241\}$, $L = \mathbb{Q}(\sqrt{-5})$ et $p = 3$. Le corps $\mathbb{Q}$ vérifie le critère de Labute-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 :



6. Exemple complémentaire

Cette section est dédiée à l'étude détaillée d'un exemple. Nous montrerons dans un premier temps, via l'étude du groupe $G_S(L)$ dans le cas où $p = 3$, $L = \mathbb{Q}(\sqrt{-5})$ et $S = \{61, 223, 229, 487\}$, qu'il existe des groupes de Galois vérifiant le théorème 5.12 auxquels on ne peut pas appliquer le critère (LS_f). Le paragraphe 6.2 prouve que les exemples de groupes *mild* obtenus par le théorème 5.12 ne vérifient pas tous le critère de Vogel ([**16**]).

Comme dans la section précédente, si $L|\mathbb{Q}$ est une extension quadratique, on notera $G_S = \mathrm{Gal}(\mathbb{Q}_S|\mathbb{Q})$ et $H_S = \mathrm{Gal}(L_S|L)$. De plus, pour $i = 1, \dots, 4$, $j = 1, 2$, on note χ_i un générateur de $H^1(G_{v_i}^{p,el})$ et Ψ_i^j un générateur de $H^1(H_{v_i^{(j)}}^{p,el})$. Les cup-produits sont calculés localement grâce à la méthode des Frobenius auxiliaires (section 4.1) et exprimés sous forme de 4-uplets (resp. 8-uplets) dans $\bigoplus_{v\in S} H^2(\overline{G_v})$ (resp. $\bigoplus_{v\in S'} H^2(\overline{H_v})$).

6.1. Un exemple de pro-p groupe *mild* ne vérifiant pas le critère 2.14. —

Exemple 6.1. — 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 $U = H^1(G_{p_2}^{p,el}) \oplus H^1(G_{p_3}^{p,el})$ et $V = H^1(G_{p_1}^{p,el}) \oplus H^1(G_{p_4}^{p,el})$, le groupe G_S vérifie les hypothèses du (LS_f). Le groupe G_S est donc *mild*.

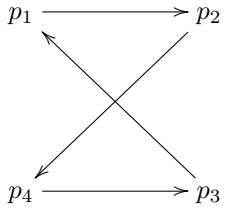
• Le groupe H_S :

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 $L_{p_i^{(l)}}^{p,el}|L$. 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 $L_{p_i^{(l)}}^{p,el}|L$.

	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 5.1.2, expliciter des ensembles $\overline{U}$ et $\overline{V}$ pour lesquels le groupe H_S vérifie le critère 2.13 :

Ici, $V = H^1(G_{p_1}^{p,el}) \oplus H^1(G_{p_4}^{p,el})$, 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 6.2. — Le corps $\mathbb{Q}(\sqrt{-5})$ ne vérifie pas le critère de Labute-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 $\overline{U} = \bigoplus_{u \in \mathcal{U}} H^1(H_u^{p,el})$, $\overline{V} = \bigoplus_{v \in \mathcal{V}} H^1(H_v^{p,el})$ 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 suivant 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 4.4 en utilisant la méthode des premiers auxiliaires (section 4.1).

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 (LS_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 (LS_f), et L ne vérifie pas le critère de Labute-Schmidt en respectant S.

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

6.2. Comparaison avec les ensembles strictement circulaires de Labute.— Dans [**9**], 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 [**16**], où il étudie de manière analogue le cas d'un corps quadratique imaginaire. Cependant, les graphes utilisés ici et dans [**16**] sont définis différemment. On renvoie à [**16**] pour les notations dans ce qui suit.

Vogel construit à partir des *linking numbers* associés aux premiers de S' (cf def. 4.3) 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 6.3. — 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 6.4* ([16])**. — *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 $\mathrm{Gal}(K_S|K)$ est un pro-p groupe mild.*

Reprenons l'exemple 6.1 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 $L = \mathbb{Q}(\sqrt{-5})$ 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 $L_{p_i^{(l)}}^{p,el}|L$.

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 $L_{\mathfrak{q}_j}^{p,el}$. 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 6.3, 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 6.3 n'est pas vérifiée. L'ensemble S' n'est donc pas strictement circulaire.

Appendice A

Calcul local des cup-produits et critère (LS_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 $K_v^{p,el}|K$,
- p_v est totalement décomposé dans l'extension $K_w^{p,el}|K$ 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-élémentaires $K_w^{p,el}$ de K pour $w \in S$. Par définition, p_v est ramifié dans l'extension $K_w^{p,el}|K$ 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 $K_w^{p,el}|K$ 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 $K_w^{p,el}$, sinon p_v est inerte dans $K_w^{p,el}$. 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. — 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 4.1, le *linking number* l_{vw} est donné par l'égalité $F_v = F_{p_w}^{l_{vw}}$ dans le groupe de Galois $\mathrm{Gal}(K_w^{p,el}|K)$, 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-même, 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 (LS_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 4.4, 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 les la deuxième condition de la proposition 4.4 (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-Schmidt par rapport à S.

```
LabuteSchmidt(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,]]);
```

```
        );
    );
    if(matrank(M)==#S, R=concat(R,[V[i],U[i]]));
);
R;}
```

Références

[1] Anick, D.J. : Noncommutative graded algebras and their Hilbert series. J. Algebra **78**(1), 120–140 (1982)

[2] Batut, C., Belabas, K., Bernardi, D., Cohen, H., Olivier, M. : User's Guide to PARI-GP. http ://pari.math.u-bordeaux.fr/ (1998)

[3] Forré, P. : Strongly free sequences and pro-p-groups of cohomological dimension 2. J. Reine Angew. Math. **658**, 173–192 (2011)

[4] Gärtner, J. : Higher Massey products in the cohomology of mild pro-p-groups. J. Algebra **422**, 788–820 (2015)

[5] Gras, G. : On the T-ramified, S-split p-class field towers over an extension of degree prime to p. J. Number Theory **129**(11), 2843–2852 (2009)

[6] Harary, F. : Graph Theory. Addison-Wesley (1969)

[7] Jaulent, J.F. : Théorie ℓ-adique globale du corps de classes. J. Théor. Nombres Bordeaux **10**(2), 355–397 (1998)

[8] Koch, H. : Galois Theory of p-Extensions. Springer (2002)

[9] Labute, J. : Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$. J. Reine Angew. Math. **596**, 155–182 (2006)

[10] Maire, C. : Some examples of fab and mild pro-p-groups with trivial cup-product. Kyushu J. Math. **68**(2), 359–376 (2014)

[11] Neukirch, J., Schmidt, A., Wingberg, K. : Cohomology of Number Fields. Springer (2000)

[12] Schmidt, A. : Rings of integers of type $K(\pi, 1)$. Doc. Math. **12**, 441–471 (electronic) (2007)

[13] Schmidt, A. : Über pro-p-fundamentalgruppen markierter arithmetischer kurven. J. Reine Angew. Math. **640**, 203–235 (2010)

[14] Shafarevich, I.R. : Extensions with prescribed ramification points. Publ. Math. Inst. Hautes Etudes Sci. **18**, 71–95 (1964)

[15] Tate, J. : Nilpotent quotient groups. Topology **3**(suppl. 1), 109–111 (1964)

[16] Vogel, D. : Circular sets of primes of imaginary quadratic number fields (2006). Preprint

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