THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par *l'Université Toulouse III - Paul Sabatier*
Discipline ou spécialité : *MATHÉMATIQUES PURES*

Présentée et soutenue par *Landry Salle*
Le *16 Juin 2008*

Titre : *Présentations de groupes de Galois de pro-p-extensions de corps de nombres*

JURY
MCF Jean-Robert Belliard, Membre - PR Jean-Marc Couveignes, Membre - PR Jean-François Jaulent, Rapporteur - PR Christian Maire, Directeur - PR Abbas Chazad Movahhedi, Membre - PR Marc Reversat, Directeur

---

Ecole doctorale : *Mathématiques Informatique et Télécommunications de Toulouse*
Unité de recherche : *Institut de Mathématiques de Toulouse, UMR 5580, UFR MIG*
Directeur(s) de Thèse : *PR Christian Maire - PR Marc Reversat*
Rapporteurs : *PR Manabu Ozaki, Rapporteur*

THÈSE
présentée pour le diplôme de
docteur de l'université Toulouse III – Paul Sabatier
en MATHÉMATIQUES PURES

par

Landry Salle

intitulée

Présentations de groupes de Galois de pro-p-extensions de corps de nombres.

soutenue le 16 Juin 2008 devant le jury composé de

Jean-Robert Belliard	Université de Franche-Comté	Examinateur
Jean-Marc Couveignes	Université de Toulouse	Examinateur
Jean-François Jaulent	Université de Bordeaux	Rapporteur
Christian Maire	Université de Franche-Comté	Directeur
Abbas Chazad Movahhedi	Université de Limoges	Examinateur
Marc Reversat	Université de Toulouse	Directeur

Institut de Mathématiques de Toulouse, UMR 5580, UFR MIG
Laboratoire Émile Picard,
Université Paul Sabatier 31062 TOULOUSE Cédex 9

Remerciements

Je tiens à remercier à travers ces quelques lignes toutes les personnes qui ont rendu possible la réalisation de ces travaux. Y compris celles qui ne rentrent pas dans les catégories traditonnellement acceptables pour des remerciements de thèse.

En premier lieu, Christian Maire a su, pendant ces trois années, ainsi que l'année de DEA qui les a précédées, surveiller mes progrès de manière attentive, tout en me laissant la possibilité d'acquérir petit à petit de l'autonomie. Sa disponibilité, son implication, accomodées de libéralisme, ont donc établi des conditions on ne peut plus favorables au déroulement de cette thèse. Marc Reversat a complété ce travail d'encadrement avec une gentillesse jamais prise en défaut.

Jean-François Jaulent et Manabu Ozaki ont chacun écrit un rapport sur ce mémoire. Ils m'avaient auparavant donné l'occasion, ainsi que Jean-Robert Belliard, Yasushi Mizusawa et Thong Nguyen Quang Do, d'exposer de manière informelle devant eux mes travaux en cours. Les fort pertinents conseils délivrés - et parfois répétés - en ces diverses occasions ont été très profitables. Jean-Marc Couveignes et Abbas Chazad Movahhedi ont accepté d'être membres du jury. Je les en remercie.

Beaucoup d'autres personnes ont joué un rôle dans le contexte plus général dans lequel s'est déroulée cette thèse : que ce soient les doctorants de l'Institut de mathématiques, les membres de l'ancienne équipe Grimm, les enseignants (« devenus collègues ») et personnels du département de mathématiques et de l'Institut, ou encore les mathématiciens croisés ou rencontrés à l'occasion d'une conférence ou d'un colloque. Ces divers éléments composent un tableau dont je tiens à souligner la richesse humaine.

Table des matières

Chapitre I

Introduction.

I.1 Contexte.

I.1.1 Théorie p-adique du corps de classes.

La théorie du corps de classes a pour objet la description des extensions abéliennes d'un corps, global (corps de nombres, corps de fonctions), ou local (corps de nombres p-adiques, corps de séries de Laurent), en fonction d'invariants de ce corps. Ces invariants sont de nature arithmétique et/ou cohomologique. Par exemple, un énoncé typique de la théorie est :

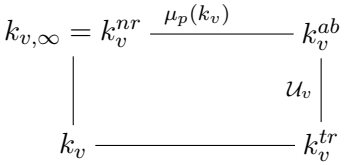
Théorème I.1.1. *Soit k un corps de nombres, et $L(k)$ son corps de Hilbert, c'est-à-dire son extension abélienne non ramifiée maximale. Alors, le symbole d'Artin $\left(\frac{\cdot}{L(k)/k}\right)$ fournit un isomorphisme entre le groupe des classes de k et le groupe de Galois* $\mathrm{Gal}(L(k)/k)$.

On rappelle que le symbole d'Artin est défini comme suit : pour chaque idéal premier $\mathfrak{p}$ de k, soit $\mathfrak{P}$ un idéal premier au-dessus de $\mathfrak{p}$ dans $L(k)$. Le symbole d'Artin $\left(\frac{\mathfrak{p}}{L/k}\right)$ est l'unique élément du sous-groupe de décomposition de $\mathrm{Gal}(L(k)/k)$ en la place $\mathfrak{P}$ dont l'image dans le groupe de Galois de l'extension de corps résiduels (corps finis de caractéristique $\mathfrak{p} \cap \mathbb{Z}$) soit le morphisme de Frobenius.
Comme l'indique le titre de cette section, donner une présentation accessible de la théorie du corps de classes n'est pas dans nos objectifs. Nous nous contenterons de donner quelques résultats de sa formulation p-adique due à Jaulent (voir [10]), c'est-à-dire adaptée à l'étude des extensions abéliennes finies dont le cardinal est une puissance de p, et de leurs unions, éventuellement infinies ; donc, en général, des pro-p-extensions abéliennes. La restriction à de telles extensions permet d'éliminer, via un formalisme adapté, certains phénomènes de la théorie générale, comme l'obligation de quotienter par la composante connexe de l'identité pour obtenir une bonne notion de groupe de classes.

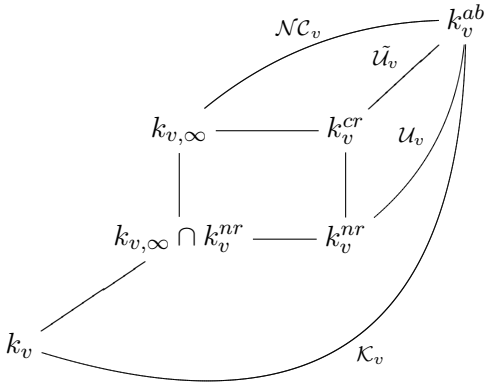
Correspondance locale.

On introduit d'abord les objets locaux suivants. Certaines notations diffèrent de celles de Jaulent, notamment pour le groupe des normes cyclotomiques locales.

Pour une place non archimédienne v, on définit $\mathcal{K}_v$ comme le compactifié p-adique du groupe multiplicatif $k_v^\times$ du localisé k_v de k en la place v, c'est-à-dire $\mathcal{K}_v = \varprojlim k_v^\times/(k_v^\times)^{p^n}$, pour les morphismes naturels de transition.
Son sous-groupe unité est noté $\mathcal{U}_v$. Suivant que la place v est au-dessus de p ou non, la structure de ce sous-groupe varie : si $v \in \mathrm{Pl}_p(k)$, alors $\mathcal{U}_v$ s'identifie au produit direct du groupe fini $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v avec un $\mathbb{Z}_p$-module libre de rang $[k_v : \mathbb{Q}_p]$. Si, au contraire, $v \notin \mathrm{Pl}_p(k)$, alors $\mathcal{U}_v$ est le groupe cyclique $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v.
Un autre sous-groupe remarquable est $\mathcal{NC}_v$, le groupe des normes cyclotomiques locales, défini comme le noyau d'une valuation logarithmique. Dans le cas où $v \notin \mathrm{Pl}_p(k)$, ce sous-groupe coïncide avec $\mathcal{U}_v$. En revanche, si $v \in \mathrm{Pl}_p(k)$, alors $\mathcal{NC}_v$ est produit direct du groupe fini $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v avec un $\mathbb{Z}_p$-module libre de rang $[k_v : \mathbb{Q}_p]$.
L'intersection des deux sous-groupes précédents sera notée $\tilde{\mathcal{U}}_v = \mathcal{U}_v \cap \mathcal{NC}_v$. C'est le ($p$-adifié du) groupe des unités qui sont normes cyclotomiques. Dans le cas où $v \in \mathrm{Pl}_p(k)$, c'est le produit direct du groupe fini $\mu_p(k_v)$ des racines p-primaires de l'unité dans k_v avec un $\mathbb{Z}_p$-module libre de rang $[k_v : \mathbb{Q}_p] - 1$, chacun des deux quotients $\mathcal{U}_v/\tilde{\mathcal{U}}_v$ et $\mathcal{NC}_v/\tilde{\mathcal{U}}_v$ étant un $\mathbb{Z}_p$-module libre de rang 1. Dans le cas où $v \notin \mathrm{Pl}_p(k)$, ce groupe coïncide avec $\mathcal{U}_v$.
La théorie p-adique du corps de classes locale établit alors des isomorphismes entre ces groupes et des groupes de Galois d'extensions abéliennes de k_v. Dans le cas où $v \notin \mathrm{Pl}_p(k)$, en supposant que k_v contienne le groupe des racines p-èmes de l'unité, ces isomorphismes sont donnés dans le diagramme suivant :



Le corps k_v^{ab} est la pro-p-extension abélienne maximale de k_v. Sa sous-extension $k_v^{nr} = k_{v,\infty}$ admet deux descriptions naturelles : c'est d'une part la pro-p-extension non ramifiée maximale de k_v, et d'autre part sa $\mathbb{Z}_p$-extension cyclotomique (voir définition I.1.4, plus bas). Le corps k_v^{tr} est une p-extension cyclique totalement ramifiée. Dans le cas où $v \in \mathrm{Pl}_p(k)$, la situation est différente : par exemple les $\mathbb{Z}_p$-extensions non ramifiée et cyclotomique sont linéairement disjointes (leur intersection est une extension finie de k_v). Le diagramme d'extensions de corps suivant résume la situation :



Ici, k_v^{ab} est encore la pro-p-extension abélienne maximale de k_v, k_v^{nr} sa pro-p-extension non ramifiée maximale et $k_{v,\infty}$ sa $\mathbb{Z}_p$-extension cyclotomique. On note k_v^{cr} le compositum de ces deux dernières. Le corps k_v admet en général d'autres $\mathbb{Z}_p$-extensions non incluses dans k_v^{cr} ; le nombre de $\mathbb{Z}_p$-extensions linéairement indépendantes étant $[k_v : \mathbb{Q}_p] + 1$, soit le $\mathbb{Z}_p$-rang de $\mathcal{K}_v$.

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

Correspondance globale.

Les objets arithmétiques en correspondance avec les extensions abéliennes d'un corps de nombres peuvent être considérés de deux façons : soit en tant que groupes des classes et groupes des classes de rayon, comme dans le théorème I.1.1, soit comme des groupes de classes d'idèles. La formulation p-adique se base sur cette deuxième manière de considérer les objets.

On introduit donc $\mathcal{J}_k$ (ou simplement $\mathcal{J}$), le p-adifié du groupe d'idèles, comme le produit des $\mathcal{K}_v$, restreint aux $\mathcal{U}_v$. Son sous-groupe associé à la $\mathbb{Z}_p$-extension cyclotomique de k sera noté $\tilde{\mathcal{J}}_k$. C'est le noyau de la formule du produit pour les valeurs absolues p-adiques.
Le sous-groupe de $\mathcal{J}_k$ des idèles principaux est $\mathcal{R}_k = \mathbb{Z}_p \otimes k^*$. Le sous-groupe des unités globales est $\mathcal{E}_k = \mathbb{Z}_p \otimes E_k$.
Le sous-groupe des idèles unités noté $\mathcal{U}_k$ (ou simplement $\mathcal{U}$) est le produit des $\mathcal{U}_v$. On note $\tilde{\mathcal{U}}_v$ le produit des $\mathcal{U}_v$, c'est-à-dire des idèles unités qui sont partout localement normes cyclotomiques.
Pour tout ensemble fini B de places, on note par ailleurs $\mathcal{K}_B$ le produit $\prod_{v\in B}\mathcal{K}_v$, $\mathcal{NC}_B$, le produit $\prod_{v\in B}\mathcal{NC}_v$, $\mathcal{U}_B$ le produit $\prod_{v\in B}\mathcal{U}_v$, et $\tilde{\mathcal{U}}_B$ le produit $\prod_{v\in B}\tilde{\mathcal{U}}_v$. On note de même $\mathcal{K}_{\overline{B}}$, $\mathcal{NC}_{\overline{B}}$, $\mathcal{U}_{\overline{B}}$, et $\tilde{\mathcal{U}}_{\overline{B}}$ les produits (restreint aux sous-groupes unités pour $\mathcal{K}_{\overline{B}}$ et $\mathcal{NC}_{\overline{B}}$) respectivement des $\mathcal{K}_v$, $\mathcal{NC}_v$, $\mathcal{U}_v$, et $\tilde{\mathcal{U}}_v$, pour v parcourant les places en dehors de B. En particulier, si $B = \mathrm{Pl}_p(k)$ est l'ensemble des places au-dessus de p, on notera $\mathcal{U}_p = \mathcal{U}_{\mathrm{Pl}_p(k)}$ et $\tilde{\mathcal{U}}_p = \tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)}$.

La correspondance du théorème I.1.1 se reformule alors en un isomorphisme entre le groupe de Galois de la p-extension abélienne non ramifiée maximale de k et le groupe quotient $\mathcal{J}_k/\mathcal{R}_k\mathcal{U}_k$. Plus généralement, soit G_S^T le groupe de Galois de la pro-p-extension S-ramifiée T-décomposée maximale de k (c'est-à-dire le compositum des p-extensions abéliennes non ramifiées aux places en dehors de S et totalement décomposées aux places de T). Alors la correspondance du corps de classes permet de décrire son abélianisé par l'isomorphisme :

$$(G_S^T)^{ab} \simeq \mathcal{J}_k/\mathcal{R}_k\mathcal{U}_{\overline{S\cup T}}\mathcal{K}_T.$$

I.1.2 Extensions de corps locaux.

La structure des groupes de Galois de la p-clôture algébrique d'une extension finie k du corps q-adique $\mathbb{Q}_q$ est connue. Au moins dans le cas $p \neq 2$, elle dépend de deux conditions : l'une porte sur le fait que le corps contienne ou non les racines p-èmes

de l'unités ; l'autre porte sur l'égalité $p = q$. Les cas où le corps k ne contient pas les racines p-èmes de l'unité sont dus à Chafarevitch ([38], consulté dans [40] ; on a uniformisé, dans la bibliographie, la transcription en anglais de Chafarevitch en Shafarevich au détriment de Šafarevič), les cas où k contient les racines p-èmes de l'unité à Demuchkin ([1]), pour le cas p impair, et à Serre puis Labute pour le cas $p = 2$ ([37], [17]).

Théorème I.1.2. *Soit p et q deux nombres premiers et k une extension finie du corps $\mathbb{Q}_q$. Alors le groupe de Galois $\overline{G}$ de la pro-p-extension maximale $\overline{k}$ de k vérifie :*

1. *Si $p \neq q$:*
   (a) *Si k ne contient pas les racines q-èmes de l'unité, alors $\overline{G} = \mathrm{Gal}(k^{nr}/k)$ est isomorphe à $\mathbb{Z}_p$.*
   (b) *Si k contient les racines q-èmes de l'unité, alors $\overline{G}$ admet la présentation :*
   $$< \sigma, \tau | \sigma\tau\sigma^{-1} = \tau^{N\mathfrak{q}} >,$$
   où σ est un relevé du Frobenius de $\mathrm{Gal}(k^{nr}/k)$, τ est un générateur du sous-groupe procyclique $\mathrm{Gal}(\overline{k}/k^{nr})$ et $\mathfrak{q}$ est l'unique idéal maximal de l'anneau des entiers de k.
2. *Si $p = q$ et si k ne contient pas les racines q-èmes de l'unité, alors $\overline{G}$ est un pro-p-groupe libre à $n + 1 = [k : \mathbb{Q}_q] + 1$ générateurs $\sigma, \tau_1, \cdots, \tau_n$ (obtenus comme relevés d'éléments de $\mathrm{Gal}(k_v^{ab}/k_v)$, à savoir le Frobenius pour σ, et, pour les τ_i, $n = [k : \mathbb{Q}_q]$ automorphismes correspondant à une base du $\mathbb{Z}_p$-module $\mathcal{U}_k$ des unités).*

Le cas restant ($p = q$, k contenant les racines p-èmes de l'unité) est le plus intéressant. Deux types d'énoncés sont disponibles pour la description du groupe $\overline{G}$: une simple description algébrique par générateurs et relations, ou une description dans un système de générateurs provenant d'une famille génératrice arithmétiquement remarquable de l'abélianisé (donc du groupe multiplicatif du corps par la théorie du corps de classes). On renvoie à [16], section 10, pour cette deuxième description, plus fine, et on se limite au résultat suivant, sans envisager les cas exceptionnels dus à Serre et Labute :

Théorème I.1.3. *Soit k une extension finie de $\mathbb{Q}_p$, de degré n, et $\tilde{p}$, qu'on suppose > 2 (donc n est pair), la plus grande puissance de p telle que k contienne les racines $\tilde{p}$-èmes de l'unité. Alors, le groupe de Galois $\overline{G}$ de la pro-p-extension maximale de k admet comme pro-p-présentation minimale :*

$$< x_1, \ldots x_{n+2} | x_1^{\tilde{p}} [x_1, x_2][x_3, x_4] \ldots [x_{n+1} x_{n+2}] > .$$

C'est un groupe de Demuchkin, c'est-à-dire un pro-p-groupe de type fini à une relation, tel que le cup-produit :

$$H^1(\overline{G}, \mathbb{F}_p) \times H^1(\overline{G}, \mathbb{F}_p) \to H^2(\overline{G}, \mathbb{F}_p),$$

qui est une forme bilinéaire sur le $\mathbb{F}_p$-espace vectoriel de dimension finie $H^1(G, \mathbb{F}_p)$, est non dégénéré.

Enfin, la structure du groupe de Galois absolu d'un corps p-adique k est en général connue (sous l'hypothèse que $k(i)/k$ est non ramifiée si $p = 2$) : voir [24], théorème 7.5.10.

I.1.3 Tours de corps de classes.

Le problème des tours de corps de classes est énoncé classiquement de la façon suivante : soit k un corps de nombres, $L(k)$ son corps de classes de Hilbert, puis, pour chaque n, $L_n(k)$, le corps de classes de Hilbert de $L_{n-1}(k)$. Cette suite se stabilise-t-elle pour n'importe quel corps de nombres k ? Une autre formulation est : l'extension non ramifiée prorésoluble maximale du corps k est-elle finie ? En remplaçant dans ce qui précède « corps de classes de Hilbert » par « p-corps de classes de Hilbert », on obtient le problème des p-tours de corps de classes (la reformulation devient ici plus simplement, grâce à la résolubilité des p-groupes finis : la pro-p-extension non ramifiée maximale d'un corps de nombres k est-elle finie ?). De même, on peut parler de tours de corps de classes de rayon.

Le problème des p-tours de corps de classes a reçu une réponse négative (et donc a fortiori le problème des tours de corps de classes), suite aux travaux de Chafarevitch et Golod (l'original [5] et [40] pour une traduction en anglais). Ceux-ci démontrent, pour tout p-groupe fini G, que le nombre minimal de générateurs $d(G)$ et le nombre minimal de relations $r(G)$ vérifient l'inégalité :

$$r(G) > \left(\frac{d(G)-1}{2}\right)^2.$$

Par ailleurs, Chafarevitch montre dans [39] (consulté dans [40]) l'inégalité suivante :

$$r(G) \leq d(G) + r_1 + r_2 - 1 + \delta,$$

où r_1 et r_2 sont respectivement le nombre de plongements réels et de couples de plongements complexes conjugués du corps de nombres considéré, et δ vaut 1 ou 0 suivant que celui-ci contient ou non les racines p-èmes de l'unité. Il suffit donc pour obtenir un exemple de p-tour de corps de classes infini de trouver un corps k, et un nombre premier p, avec :

$$d(G) + r_1 + r_2 - 1 + \delta \leq \left(\frac{d(G)-1}{2}\right)^2.$$

L'exemple donné par Chafarevitch et Golod est le corps quadratique imaginaire $k = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$, pour le nombre premier 2 (avec $d(G) = 7$ et $r_1 + r_2 - 1 + \delta = 1$).

Ce travail a fait l'objet de nombreux développements que nous n'aborderons pas : amélioration des bornes dans des familles de corps de nombres (par exemple les corps quadratiques imaginaires), calculs explicites pour $p = 2$ sur un corps quadratique imaginaire, utilisation de tours de corps de classes infinie pour l'estimation des discriminants des corps de nombres. On renvoie à l'appendice de [16] pour un tour d'horizon de ces résultats.

I.1.4 Extensions globales à ramification restreinte : résultats classiques.

Formules de Chafarevitch.

Plus généralement, dans [39], Chafarevitch exprime le nombres de générateurs et majore le nombre de relations du groupe de Galois G_S de la pro-p-extension S-ramifiée maximale d'un corps k, pour S un ensemble fini de places de k (dont on suppose qu'il ne contient aucune place complexe), en fonctions d'objets arithmétiques attachés à ce corps. Pour énoncer ces résultats, on introduit :

Définition I.1.1. *Soit k un corps de nombres et S un ensemble fini de places de k. On note :*

$$V_S = \mathcal{R}_k \cap \mathcal{U}_{\overline{S}} \mathcal{J}_k^p,$$

et on appelle groupe de Kummer le groupe quotient $V_S/\mathcal{R}_k^p$, qui est naturellement un $\mathbb{F}_p$-espace vectoriel. Pour $S = \emptyset$, on notera simplement V.

Le résultat de Chafarevitch est alors :

Théorème I.1.4 (Chafarevitch). *Les nombres minimaux de générateurs et de relations du groupe G_S vérifient :*

$$d(G_S) = \dim_{\mathbb{F}_p} V_S/\mathcal{R}_k^p + \sum_{v \in S_p} [k_v : \mathbb{Q}_p] + \sum_{v \in S} \delta(k_v) - \delta(k) - r_1 - r_2 + 1,$$

$$r(G_S) \leq \dim_{\mathbb{F}_p} V_S/\mathcal{R}_k^p - \delta(k) + \sum_{v \in S} \delta(k_v),$$

ce dernier majorant devant être augmenté de 1 si S est vide et $\delta(k) = 1$.

Le cas des corps p-rationnels.

Le théorème I.1.4 admet pour corollaire qu'une condition suffisante pour que le groupe G_S soit un pro-p-groupe libre est :

$$V_S/\mathcal{R}_k^p = 0, \ \sum_{v \in S_p} \delta(k_v) = \delta(k).$$

Un cas particulier important étudié par de nombreux auteurs (Gras, Jaulent, Movahhedi, Nguyen-Quang-Do, Wingberg), est celui où $S = \mathrm{Pl}_p(k)$. On se contente ici de citer [6] (partie III, théorème 4.2.5 et partie IV, théorème 3.5), où plus de références sont données, et les articles originaux [12] et [22].

Théorème I.1.5. *Soit k un corps de nombres, p un nombre premier et $\mathrm{Pl}_p(k)$ l'ensemble des places de k au-dessus de p. Alors on a équivalence entre :*

1. *le groupe de Galois de la pro-p-extension p-ramifiée (i.e., $\mathrm{Pl}_p(k)$-ramifiée) maximale de k est libre.*
2. *$V_{\mathrm{Pl}_p(k)}/\mathcal{R}_k^p = 0$ et $\sum_{v \in \mathrm{Pl}_p(k)} \delta(k_v) = \delta(k)$.*
3. *le groupe de Galois de la pro-p-extension abélienne p-ramifiée maximale de k est libre de rang $r_2 + 1$.*

4. *la conjecture de Leopoldt en k pour le nombre premier p est vérifié, et le groupe de Galois de la pro-p-extension abélienne p-ramifiée maximale de k est sans torsion.*

Un corps vérifiant ces propriétés est dit p-rationnel.

Rappelons un énoncé de la conjecture de Leopoldt (voir par exemple [24], section X,3 pour des énoncés équivalents) :

Conjecture (Leopoldt)**.** *Soit k un corps de nombres et p un nombre premier. Soit E_k le groupe des unités du corps k, alors le morphisme diagonal de $E_k \otimes_{\mathbb{Z}} \mathbb{Z}_p$ dans $\prod_{v\in \mathrm{Pl}_p(k)} \mathcal{U}_{k_v}$ est injectif.*

Cette conjecture a été démontrée notamment pour toute extension abélienne du corps $\mathbb{Q}$ à la suite de travaux d'Ax et Brumer sur l'indépendance de nombres algébriques.

La propriété de p-rationalité se propage bien sûr le long des p-extensions p-ramifiées (un sous-groupe d'un groupe libre est libre) ; on trouve ainsi en particulier une méthode de propagation de la conjecture de Leopoldt dans des extensions non abéliennes. Elle se propage aussi dans certaines extensions S-ramifiées, quand S vérifie une propriété dite de primitivité : si S est un ensemble de places contenant $\mathrm{Pl}_p(k)$, notons $S_0 = S - \mathrm{Pl}_p(k)$, alors S est primitif si la pro-p-extension abélienne p-ramifiée S_0-décomposée maximale de k est libre de rang $r_2 + 1 - \#S_0$. Dans ce cas, le groupe de Galois G_S de la pro-p-extension S-ramifiée maximale de k se présente comme un pro-p-produit libre (pour simplifier, on suppose que S ne contient aucune place réelle de k si $p = 2$) :

$$*_{v\in S_0} \overline{G_v} * F,$$

où F est un pro-p-groupe libre sur $r_2 + 1 - \#S_0$ générateurs. Plus généralement, dès que S contient les places au-dessus de p dans k et les places à l'infini, et si k est de plus totalement imaginaire dans le cas $p = 2$, le groupe de Galois G_S a dimension cohomologique inférieure à 2.

Présentations de Koch.

La démonstration du théorème I.1.4 est reformulée par Koch dans [16] dans un style plus moderne (voir aussi par exemple [24], section VIII, 7), et constitue sous cette forme un modèle pour plusieurs résultats de cette thèse. L'objet clef dans cette preuve est le noyau de Chafarevitch, c'est-à-dire le noyau $Ш^2(G_S, \mathbb{F}_p)$ du morphisme :

$$H^2(G_S, \mathbb{F}_p) \to \prod_{v\in S} H^2(\overline{G_v}, \mathbb{F}_p),$$

obtenu par restriction cohomologique de G_S à ses sous-groupes de décomposition en $v \in S$, puis inflation aux p-groupes de Galois absolus des localisés k_v. L'examen d'un diagramme commutatif obtenu par comparaison des situations locales et globales d'une part, par des suites de Hochschild-Serre d'autre part, permet d'obtenir une injection :

$$Ш^2(G_S, \mathbb{F}_p) \hookrightarrow V_S/\mathcal{R}_k^p.$$

Ceci fournit une condition suffisante de nature arithmétique à l'annulation du noyau de Chafarevitch. Or, l'annulation de ce noyau entraîne qu'un certain principe local-global est vérifié. En effet, les groupes de cohomologie $H^2(\cdot, \mathbb{F}_p)$ codent une information sur les relations des groupes concernés : par exemple,

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

néanmoins, l'information contenue est encore plus précise, si bien que l'annulation du noyau de Chafarevitch permet d'obtenir toutes les relations globales à partir de relations locales (voir [16], section 6.2, et en particulier théorème 6.14, pour un énoncé précis). Ceci aboutit à une présentation du groupe G_S ayant une forme remarquable, dans le cas où $V_S/\mathcal{R}_k^p = 0$. Décrire précisément l'obtention d'une présentation sur des générateurs arithmétiquement pertinents est long, et on se contente de renvoyer à [16], section 11.4. Toutefois, la forme de ces présentations motive la définition ([18], [44]) :

Définition I.1.2. *Une pro-p-présentation d'un pro-p-groupe :*

$$< \alpha_1, \ldots, \alpha_d | \omega_1, \ldots, \omega_r >,$$

est dite de type Koch si $r \leq d$ et si les congruences suivantes sont vérifiées dans le pro-p-groupe libre F engendré par les α_i :

$$\omega_i \equiv \alpha_i^{pa_i} \prod_{j \neq i} [\alpha_j, \alpha_i]^{l_{ij}} \mod F_3,$$

avec des exposants $a_i \in \mathbb{Z}_p$ et $l_{ij} \in \mathbb{Z}/p\mathbb{Z}$, où pour tout i (en particulier $i = 3$), F_i est défini par $G_1 = G$, et $G_{i+1} = G_i^p[G_i, G]$ (c'est-à-dire est le i-ème terme de la p-suite centrale descendante de F).

Les résultats de Koch, si on met de côté l'interprétation arithmétique des générateurs, peuvent se formuler de la façon suivante :

Proposition I.1.6. *Soit p un nombre premier, k un corps de nombres, et S un ensemble fini de places de k tel que $V_S/\mathcal{R}_k^p$ est trivial. Alors le groupe G_S de la pro-p-extension S-ramifiée maximale de k admet une présentation de type Koch.*

Concluons cette section par la remarque suivante : les groupes $V_S/\mathcal{R}_k^p$ sont décroissants en S. En particulier, dès que $V/\mathcal{R}_k^p$ est trivial pour un certain corps k et un premier p, alors tous les $V_S/\mathcal{R}_k^p$ sont triviaux. Par ailleurs, il existe une suite exacte (rappelée lors de la preuve du théorème II.2.2) :

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

Puisque les seuls corps de nombres pour lesquels le groupes des unités est fini sont le corps $\mathbb{Q}$ des rationnels et les corps quadratiques imaginaires, on obtient par exemple que, pour $p \geq 5$, $V/\mathcal{R}_k^p$ est trivial si et seulement si k est $\mathbb{Q}$ ou un corps quadratique imaginaire dont le nombre de classes n'est pas divisible par p ($\mathbb{Q}(\zeta_3)$ devant aussi être exclu pour $p = 3$).

I.1.5 Extensions globales à ramification restreinte : les groupes clément.

Les résultats de Labute.

Dans [18], Labute donne un critère combinatoire pour qu'un pro-p-groupe admettant une présentation de type Koch soit « *mild* » (aucune traduction de ce mot dans ce contexte n'est à notre connaissance fixée, on propose d'employer le mot « clément »).

Pour définir la notion de groupe clément, on introduit quelques objets. Soit F un pro-p-groupe libre (p impair) sur la famille finie $(\alpha_i)_{i=1,\dots,d}$. On considère les $gr_n(F) = F_n/F_{n+1}$, où les F_n sont les termes de la p-suite centrale descendante de F. Notons en particulier, pour chaque i, a_i l'image de α_i dans $gr_1(F)$. Chaque $gr_n(F)$ est un $\mathbb{F}_p$-espace vectoriel de dimension finie (donnée par la formule de Witt). On considère le $\mathbb{F}_p$-espace vectoriel gradué :

$$gr(F) = \oplus_{n\geq 1} gr_n(F).$$

Deux structures supplémentaires apparaissent naturellement sur $gr(F)$: d'une part, le crochet induit par le crochet de commutation dans F le munit d'une structure d'algèbre de Lie, et, d'autre part, il s'agit d'un $\mathbb{F}_p[\pi]$-module, où l'action de π provient de l'élévation à la puissance p dans F. Alors $gr(F)$ est l'algèbre de Lie libre engendrée par les a_i sur $\mathbb{F}_p[\pi]$. Ceci permet d'énoncer :

Définition I.1.3. *Soit p un nombre premier impair, et G un pro-p-groupe admettant une présentation :*

$$< \alpha_1, \dots, \alpha_d | \omega_1, \dots, \omega_r > .$$

Soit F un pro-p-groupe libre sur les α_i, on considère les ω_i comme des éléments de F, puis comme des éléments de $gr_{n_i}(F)$, en choisissant, pour chaque i, n_i comme le plus grand entier tel que $w_i \in F_{n_i}$. On note w_i l'élément de $gr(F)$ obtenu à partir de ω_i par cette voie. Soit W l'idéal de $gr(F)$ engendré par les w_i, $\mathfrak{g}$ l'algèbre de Lie quotient $gr(F)/W$, et $U_\mathfrak{g}$ son algèbre enveloppante obtenue via la représentation adjointe.
La présentation est dite fortement libre si $U_\mathfrak{g}$ est un $\mathbb{F}_p[\pi]$-module libre et si $W/[W,W]$, qui est muni d'une structure de $U_\mathfrak{g}$-module, est librement engendré par les classes de w_i. Si un pro-p-groupe admet une présentation fortement libre, alors on dit qu'il est clément.

On renvoie à [18], théorème 1.2, pour la description de fortes propriétés algébriques d'un groupe clément. Pour faire le lien avec ce qui a été dit précédemment sur les groupes G_S, quand k est p-rationnel et que S contient $\mathrm{Pl}_p(k)$, notons seulement qu'un tel groupe est de dimension cohomologique au plus 2.

Soit maintenant un pro-p-groupe admettant une présentation de type Koch :

$$< \alpha_1, \dots, \alpha_d | \omega_1, \dots, \omega_r >,$$

avec donc des congruences :

$$\omega_i \equiv \alpha_i^{pa_i} \prod_{j\neq i} [\alpha_j, \alpha_i]^{l_{ij}} \mod F_3.$$

A une telle présentation peut être associé un graphe orienté et pondéré, appelé graphe d'enlacement par analogie avec la théorie des nœuds : chaque sommet est associé à un générateur α_i, et une arête est tracée du sommet α_i vers le sommet α_j si le coefficient l_{ij} de la présentation est non nul dans $\mathbb{F}_p$. Dans ce cas, l'arête est pondérée par ce coefficient.
Une numérotation $v_1, \ldots, v_d, v_{d+1} = v_1$ des sommets du graphe d'enlacement forme un circuit régulier si elle vérifie :

1. pour chaque i, il y a une arête de v_i vers v_{i+1},
2. si i et j sont tous deux impairs, alors il n'y a pas d'arête tracée entre v_i et v_j (ni dans une direction ni dans l'autre),
3. $\prod_{i=1}^{d} l_{i,i+1} \neq \prod_{i=1}^{d} l_{i+1,i}$.

En particulier, la troisième condition est trivialement satisfaite dès que la première l'est et qu'il existe deux sommets v_i et v_{i+1} tels qu'il n'y ait pas d'arête tracée entre v_{i+1} et v_i. De manière tout aussi évidente, ces conditions impliquent que les nombres de générateurs d et de relations r soient égaux (rappelons que pour une présentation de type Koch, on a déjà $r \leq d$), et pairs.
Labute montre alors :

Théorème I.1.7 (Labute). *Soit p un nombre premier impair, et soit un groupe admettant une pro-p-présentation de type Koch telle que le graphe d'enlacement associé admette un circuit régulier. Alors la présentation est fortement libre, et le groupe est clément. Il est donc en particulier de dimension cohomologique au plus* 2.

Ce théorème est notamment adapté au cas des pro-p-extensions S-ramifiées de $\mathbb{Q}$, avec S un ensemble de nombres premiers ne contenant pas p (cas modéré) : il s'applique par exemple au cas $p = 3$, $S = \{7, 19, 61, 163\}$. D'autres conditions suffisantes portant sur le graphe d'enlacement pour qu'une présentation de type Koch soit fortement libre sont données dans [18], dont certaines adaptées notamment au cas où S contient des places au-dessus de p : voir les théorèmes 3.17, 3.18 et 3.19. Labute remarque par ailleurs qu'un nombre premier p et un ensemble S de places de $\mathbb{Q}$ étant fixés, un nombre premier q peut être ajouté à S de manière à ce que les arêtes supplémentaires du graphe d'enlacement admettant ce nouveau point comme extrémité soient arbitrairement prescrites. Ceci repose sur le théorème de densité de Chebotarev.

Les travaux ultérieurs.

Les résultats de Labute sont le point de départ d'une série de publications dues à divers auteurs. Citons d'abord Vogel, qui dans [41] puis [42] exhibe des groupes cléments comme groupes de Galois de pro-p-extensions à ramification restreinte au-dessus d'un corps quadratique imaginaire. Wingberg cherche dans [44] des pro-p-groupes cléments comme groupes de Galois G_S^T de la pro-p-extension S-ramifiée T-décomposée maximale d'un corps de nombres k. Il montre alors que, si le corps k est p-rationnel, que S contient toutes les places au-dessus de p, et qu'en les places de T une certaine propriété de déploiement des morphismes de localisation est vérifiée, alors le groupe de Galois G_S^T admet une présentation de type Koch. En particulier, les résultats de Labute sont susceptibles de s'appliquer, et Wingberg montre à l'aide

du théorème de Chebotarev, un théorème de prescription arbitraire des arêtes supplémentaires ajoutées au graphe d'enlacement du groupe lorsqu'on ajoute des places dans S.

Schmidt propose quant à lui diverses améliorations des résultats de Labute, portant sur des considérations de nature arithmétique et géométrique. Sans entrer dans le détail de ces travaux, qu'il nous soit permis d'essayer d'en faire ressortir les grandes lignes. Dans [30], Schmidt considère le cas d'une pro-p-extension S-ramifiée maximale de $\mathbb{Q}$, avec S ne contenant pas p : à partir d'un ensemble S de places modérées auquel le théorème I.1.7 s'applique, il montre que le groupe $G_{S\cup S'}$ est encore de dimension cohomologique 2 dès que le graphe d'enlacement associé à $S \cup S'$ est tel que chaque sommet de S' soit l'origine d'une arête ayant pour but un point de S. Il montre donc une propagation de la propriété « avoir dimension cohomologique 2 » sous une condition qui n'assure pas la propagation de la clémence. Schmidt remarque encore que dans cette situation, le fait que la dimension cohomologique de G_S soit 2 suffit à assurer un isomorphisme naturel entre la cohomologie galoisienne du groupe G_S et la cohomologie étale du schéma $\mathrm{Spec}(\mathbb{Z}) - S$. On dit dans ce cas que ce schéma vérifie la propriété « $K(\pi, 1)$ » en p. Schmidt étudie cette propriété $K(\pi, 1)$ pour les schémas $\mathrm{spec}(\mathcal{O}_k) - S$, dans [31] quand S ne contient aucune place au-dessus de p, puis dans [33] dans le cas général (voir aussi le plus récent [32]). D'une part Schmidt obtient des résultats de densité, de la forme :

> un nombre premier p, un corps k et un ensemble de places S sont donnés d'une part, un autre ensemble de places S', assez gros, d'autre part. Alors, sous certaines conditions, il existe un sous-ensemble fini $S'' \subset S'$ tel que le schéma $\mathrm{spec}(\mathcal{O}_k) - (S \cup S'')$ vérifie la propriété $K(\pi, 1)$;

d'autre part il montre des conséquences arithmétiques de la propriété $K(\pi, 1)$, comme des théorèmes de réalisation globale d'extension locale, ou de déploiement de groupes de Galois (dont un prototype a été énoncé précédemment dans le cas des corps p-rationnels). Wingberg dans [45] approfondit le lien entre théorème de déploiement et propriété $K(\pi, 1)$.

I.1.6 Théorie d'Iwasawa.

La théorie d'Iwasawa (voir [8] pour l'article historique, [36], un exposé de Serre au séminaire Bourbaki, et [43], pour un exposé dans un ouvrage didactique moderne) a pour objet de dégager des structures dans les objets arithmétiques attachés à un corps de nombres lorsque celui-ci varie dans des familles particulières. Le cas le plus classique, et le seul qui sera abordé dans cette thèse, est celui où la famille de corps de nombres est constituée des étages d'une $\mathbb{Z}_p$-extension (c'est-à-dire d'une extension galoisienne dont le groupe de Galois est isomorphe en tant que groupe topologique au groupe additif de l'anneau des entiers p-adiques) d'un corps de nombres fixé. L'exemple le plus important est celui de la $\mathbb{Z}_p$-extension cyclotomique :

Définition I.1.4. *Soit p un nombre premier. On définit la $\mathbb{Z}_p$-extension cyclotomique de $k = \mathbb{Q}(\mu_{2p})$ comme la tour d'extensions $k_n = \mathbb{Q}(\mu_{2p^{n+1}})$, $n \geq 0$, ou simplement*

comme l'union de cette tour $k_\infty = \bigcup_{n\geq 0} k_n = \mathbb{Q}(\mu_{2p^\infty})$. *On a alors les isomorphismes :*

$$\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_p,\ \mathrm{Gal}(k_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p^\times.$$

En particulier, le groupe $\mathrm{Gal}(k_\infty/\mathbb{Q})$ *admet un unique quotient isomorphe à* $\mathbb{Z}_p$, *dont le sous-corps fixe, noté* $\mathbb{B}_\infty$, *est une extension galoisienne de* $\mathbb{Q}$, *appelée* $\mathbb{Z}_p$*-extension cyclotomique, dont le groupe de Galois est isomorphe à* $\mathbb{Z}_p$.
La $\mathbb{Z}_p$*-extension cyclotomique d'un corps de nombres* K *est alors le compositum* $K \cdot \mathbb{B}_\infty$.

Remarque I.1.8. *Si* p *est impair, le groupe de Galois* $\mathrm{Gal}(\mathbb{Q}(\mu_{2p^\infty})/\mathbb{B}_\infty)$ *est isomorphe à* $\mathbb{Z}/(p-1)\mathbb{Z}$, *et il est isomorphe à* $\mathbb{Z}/2\mathbb{Z}$ *si* $p = 2$.

Le compositum des $\mathbb{Z}_p$-extensions d'un corps de nombres k est une extension de k dont le groupe de Galois est isomorphe à $\mathbb{Z}_p^{r_2+1+\delta}$, où r_2 est le nombre de couples de plongements complexes conjugués de k, et δ est un entier dont trivialité pour tout premier p et tout corps de nombres k est une forme de la conjecture de Leopoldt I.1.4. Le lien entre ces deux énoncés de la conjecture est un exercice facile en théorie du corps de classes ([43], théorème 13.4).
Le résultat emblématique et fondamental de la théorie d'Iwasawa porte sur le comportement des p-sous-groupes de Sylow des groupes des classes des étages d'une $\mathbb{Z}_p$-extension d'un corps de nombres.

Théorème I.1.9 (Iwasawa). *Soit* k_∞/k *une* $\mathbb{Z}_p$*-extension d'un corps de nombres* k, *et, pour chaque* n, *soit* $A(k_n)$ *le* p*-sous-groupe de Sylow du groupes des classes de* k_n. *La valuation* p*-adique des cardinaux des groupes* $A(k_n)$ *vérifie une formule asymptotique :*

$$e_n = \mu p^n + \lambda n + \nu,$$

où μ *et* λ *sont des entiers naturels, et* ν *est un entier relatif.*

Esquisse de démonstration. Cette formule provient de la structure de la limite projective des groupes $A(k_n)$ suivant les applications normes, $\varprojlim A(k_n)$: l'action des groupes de Galois $\mathrm{Gal}(k_n/k)$ sur les $A(k_n)$ passe naturellement à la limite projective en une structure de $\mathbb{Z}_p[[\Gamma]]$-module, où $\Gamma = \mathrm{Gal}(k_\infty/k)$. Ce dernier anneau est isomorphe à $\Lambda = \mathbb{Z}_p[[T]]$, via l'identifiation d'un progénérateur de Γ à $1+T$. L'anneau Λ est un anneau de hauteur 2, dont l'unique idéal maximal est (p, T), et dont les autres idéaux premiers non triviaux sont, outre celui engendré par p, ceux engendrés par les polynômes irréductibles distingués du sous-anneau $\mathbb{Z}_p[T]$. Il existe un théorème de structure des Λ-modules de type fini, à pseudo-isomorphisme près, c'est-à-dire qu'on s'autorise noyau et conoyau finis entre un module abstrait et son modèle canonique :

$$\Lambda^r \oplus \bigoplus_{i=1}^{m} \Lambda/(p^{g_i}) \oplus \bigoplus_{j=1}^{l} \Lambda/(f_j)^{a_j},$$

pour f_j des polynômes irréductibles distingués. Le polynôme $\prod_i p^{g_i} \prod_j f_j^{a_j}$ est appelé polynôme caractéristique du Λ-module.
En interpétant par la théorie du corps de classes les groupes $A(k_n)$ comme des groupes de Galois d'extensions de k_n en premier lieu (précisément, de la p-extension abélienne non ramifiée maximale), puis grâce au lemme de Nakayama, on montre que $\varprojlim A(k_n)$

est un Λ-module de type fini et de torsion (donc $r = 0$). Le théorème d'Iwasawa se déduit alors du théorème de structure des Λ-modules, en particulier, les invariants d'Iwasawa de la tour sont :

$$\mu = \sum_{i}^{m} g_i,\ \lambda = \sum_{j=1}^{l} a_j \deg f_j.$$

□

Une conjecture importante sur les invariants d'Iwasawa, est la conjecture de Greenberg, qui porte sur le cas où le corps de base est totalement réel (voir [7]), et n'admet donc, sous la conjecture de Leopoldt, qu'une unique $\mathbb{Z}_p$-extension :

Conjecture (Greenberg)**.** *Soit k un corps de nombres totalement réel, et k_∞/k sa $\mathbb{Z}_p$-extension cyclotomique. Alors :*

$$\lambda = \mu = 0.$$

Sous l'hypothèse supplémentaire que le corps k est une extension abélienne du corps des rationnels, la conjecture $\mu = 0$ est un théorème, initialement prouvé par Ferrero et Washington ([3]), par des arguments d'approximation diophantienne. En revanche, les résultats disponibles sur l'invariant λ restent confinés à ce jour à un bien moindre degré de généralité (voir par exemple [26]).
Plus généralement, soit S et T deux ensembles finis disjoints de places de k, et pour chaque n, $A_S^T(k_n)$ la p-sous-groupe de Sylow du quotient par les places de $T(k_n)$ du $S(k_n)$-groupe des classes de rayon de k_n (qui correspond par la théorie du corps de classes à la p-extension abélienne S-ramifiée, T-décomposée maximale de k_n). Alors, la limite projective des groupes $A_S^T(k_n)$ a encore une structure de Λ-module de type fini. Elle n'est en revanche pas en général de torsion, en particulier lorsque S contient des places au-dessus de p (et les groupes $A_S^T(k_n)$ ne sont pas forcément finis).

Un pan crucial et classique de la théorie d'Iwasawa ne sera pas évoqué dans cette thèse : c'est l'utilisation d'outils analytiques, les « fonctions L p-adiques », et leur identification aux polynômes caractéristiques des modules d'Iwasawa. Des énoncés de telle nature sont généralement encore désignés comme relevant de la « conjecture principale », même si des résultats généraux sont disponibles depuis les travaux de Mazur et Wiles.
On se contente de mentionner incidemment les développements suivants : la « théorie d'Iwasawa des courbes elliptiques », où est considéré le comportement du groupe des points rationnels d'une courbe elliptique dans une $\mathbb{Z}_p$-extension ; la « théorie d'Iwasawa non commutative », encore largement conjecturale, où les corps de bases ne varient plus parmi les étages d'une $\mathbb{Z}_p$-extension (ou d'une $\mathbb{Z}_p^d$-extension), mais parmi ceux d'une extension de groupe de Galois p-adique analytique.

Attardons-nous un peu plus sur la « théorie d'Iwasawa non abélienne », développée par Ozaki dans [25]. Il s'agit de considérer, pour chaque n, le groupe de Galois $G(k_n)$ de $L^\infty(k_n)$, la pro-p-extension non ramifiée maximale de k_n, puis de définir la suite centrale descendante $C_i(G(k_n))$ de ces groupes :

$$C_1(G) = G,\ C_{i+1}(G) = [C_i(G), G].$$

Par la théorie de Galois, on en déduit une suite d'extensions de corps : pour tout i, $L^{(i)}(k_n)$ est le sous-corps de $L^{\infty}(k_n)$ fixé par $C_{i+1}(G(k_n))$. En particulier, pour $i = 1$, il s'agit du p-corps de classes de Hilbert, la p-extension abélienne non ramifiée maximale de k_n. Cette tour d'extensions diffère cependant de la classique tour de corps de classes, en cela que $L^{(i+1)}(k_n)$ n'est pas la p-extension abélienne non ramifiée maximale de $L^{(i)}(k_n)$, mais seulement sa sous-extension maximale centrale sur k_n (c'est-à-dire telle que $\mathrm{Gal}(L^{(i+1)}(k_n)/L^{(i)}(k_n))$ soit inclus dans le centre de $\mathrm{Gal}(L^{(i+1)}(k_n)/k_n)$). Notons alors :

$$X^{(i)}(k_n) = C_i(G(k_n))/C_{i+1}(G(k_n)).$$

Pour chaque i, la famille de ces p-groupes abéliens finis donne à la limite projective un Λ-module, noté $X^{(i)}$. Ozaki montre que, dans le cas où l'invariant d'Iwasawa μ est non trivial, alors ce Λ-module n'est pas de type fini, pour $i \geq 2$. La situation diffère donc fortement du cas classique. En revanche, si l'invariant μ d'Iwasawa est nul, Ozaki obtient la formule habituelle :

Théorème I.1.10 (Ozaki). *Soit k_∞/k une $\mathbb{Z}_p$-extension d'un corps de nombres telle que l'invariant μ du module d'Iwasawa non ramifié soit nul. Alors, pour chaque i, il existe un entier positif $\lambda^{(i)}$ (qui est le $\mathbb{Z}_p$-rang de $X^{(i)}$), et un entier $\nu^{(i)}$ tels que, pour chaque n :*

$$\#X^{(i)}(k_n) = p^{\lambda^{(i)}n+\nu^{(i)}}.$$

Le cas $p = 2$ au-dessus d'un corps quadratique imaginaire.

Les invariants du module d'Iwasawa non ramifié de la $\mathbb{Z}_2$-extension cyclotomique d'un corps quadratique imaginaire ont été calculés indépendamment par Ferrero et par Kida ([2], [14]). Leurs résultats peuvent s'énoncer ainsi :

Théorème I.1.11 (Ferrero, Kida). *Soit $k = \mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire avec $d \neq 1$ impair, k_∞/k sa $\mathbb{Z}_2$-extension cyclotomique. Alors, le module d'Iwasawa non ramifié $X(k_\infty/k)$ a pour invariants :*

$$\mu(k_\infty/k) = 0,\ \lambda(k_\infty/k) = -1 + \sum_{p|d} 2^{k'_p-3},$$

où $2^{k'_p}$ est la plus grande puissance de 2 divisant $p^2 - 1$.
De plus ce module est sans $\mathbb{Z}_2$-torsion sauf dans le cas où 2 est ramifié dans $k/\mathbb{Q}$ auquel cas le sous-module de $\mathbb{Z}_2$-torsion est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Mizusawa, dans [21], cherche à obtenir à partir de ce théorème une présentation du groupe de Galois de la pro-2-extension non ramifiée maximale de k_∞. Il passe pour cela par le calcul des modules d'Iwasawa d'extensions quadratiques et biquadratiques de K_∞, utilise la théorie des genres, puis établit différents lemmes de théorie des groupes. Sa méthode lui permet d'obtenir une présentation pour plusieurs familles de corps quadratiques imaginaires, dans lesquels 2 est ramifié, et dont l'invariant λ est 1 ou 2.

Théorème I.1.12 (Mizusawa). *Dans ce qui suit, p_1 et p_2 désignent des nombres premiers impairs distincts.*

1. *Soit* $k = \mathbb{Q}(\sqrt{-d})$ *un corps quadratique imaginaire avec* $d = p_1 \equiv 9 \bmod 16$, *ou* $d = p_1 p_2$, *avec* $p_1 \equiv p_2 \equiv 5 \bmod 8$ *ou* $p_1 \equiv p_2 \equiv 3 \bmod 8$. *Alors, le groupe de Galois de la pro-2-extension non ramifiée maximale de* k_∞ *a pour abélianisé un groupe isomorphe à* $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, *et admet pour pro-2-présentation :*

$$< a, b | [a, b] = a^{-2}, a^{2\#X(\mathbb{B}_\infty(\sqrt{d}))} = 1 > .$$

2. *Soit* $k = \mathbb{Q}(\sqrt{-d})$ *un corps quadratique imaginaire avec* $d = p_1 p_2$, *et* $p_1 \equiv 3 \bmod 8$, $p_2 \equiv 7 \bmod 16$. *Alors, le groupe de Galois de la pro-2-extension non ramifiée maximale de* k_∞ *a pour abélianisé un groupe isomorphe à* $\mathbb{Z}_2^2 \oplus \mathbb{Z}/2\mathbb{Z}$, *et admet pour pro-2-présentation :*

$$< a, b, c | [a, b] = a^{-2}, [b, c] = a^2, [a, c] = 1 > .$$

De cette présentation du groupe de Galois de la pro-2-extension non ramifiée maximale de k_∞, Mizusawa est en mesure, dans certains cas, de déduire une présentation du groupe de Galois de la pro-2-extension non ramifiée maximale des étages k_n ; c'est-à-dire du groupe de Galois de leur 2-tour de corps de classes.

I.2 Présentation des résultats.

L'objet de cette thèse est la recherche de nouvelles situations où des invariants algébriques (partie libre et torsion de l'abélianisé, nombres de générateurs, de relations, présentation, dimension cohomologique) du groupe de Galois d'une extension définie par des conditions arithmétiques de décomposition et de (non) ramification peuvent être calculés.

Dans le premier chapitre (qui fera l'objet de [28]), on considère la situation suivante : soit p un nombre premier, k un corps de nombres, k_∞/k sa $\mathbb{Z}_p$-extension cyclotomique, S un ensemble fini de places de k, et $L_S^\infty(k_\infty)$ la pro-p-extension S-ramifiée maximale de k. On considère le groupe de Galois $\tilde{G}_S = \mathrm{Gal}(L_S^\infty(k_\infty)/k)$. Le premier objectif est de calculer son $\mathbb{Z}_p$-rang. On introduit les notations :

Définition I.2.1. *On note :*

$$\lambda^{ab} = \mathrm{rg}_{\mathbb{Z}_p} \mathrm{Gal}(L^\infty(k_\infty)^{ab}/k_\infty),$$

le $\mathbb{Z}_p$*-rang du groupe de Galois* $\mathrm{Gal}(L^\infty(k_\infty)^{ab}/k_\infty)$. *Plus généralement, pour* S *un ensemble fini de places de* k, *on note :*

$$\lambda_S^{ab} = \mathrm{rg}_{\mathbb{Z}_p} \mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k_\infty).$$

Il s'agit du $\mathbb{Z}_p$*-rang de* $\tilde{G}_S$ *minoré de* 1 *(rang de* $\mathrm{Gal}(k_\infty/k)$*)*

La notation est motivée par le fait que λ^{ab} (ou λ_S^{ab}) est la partie de l'invariant λ d'Iwasawa qu'on voit depuis les extensions abéliennes de k. La description de λ_S^{ab} dépend de certains sous-groupes du groupe $\mathcal{E}_k$, p-adifié du groupe des unités globales de k :

Définition I.2.2. *Pour k un corps de nombres, et S un ensemble fini de places finies de k, on note $\mathcal{E}_{k,S}$ (respectivement $\tilde{\mathcal{E}}_{k,S}$) le sous-groupe de $\mathcal{E}_k$, image réciproque par l'application de localisation ϕ de $\mathcal{U}_{\overline{S}}$ (respectivement de $\tilde{\mathcal{U}}_{\overline{S}}$).*
La finitude des groupes $\tilde{\mathcal{U}}_v$ pour v ne divisant pas p permet de voir que les groupes $\mathcal{E}_{k,S}$ et $\mathcal{E}_{k,S_p}$ (respectivement $\tilde{\mathcal{E}}_{k,S}$ et $\tilde{\mathcal{E}}_{k,S_p}$) ont même $\mathbb{Z}_p$-rang.

Le premier résultat est alors :

Théorème I.2.1. *L'invariant λ_S^{ab} vaut :*

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

où ϕ_p est l'application de semi-localisation en p, δ le défaut de la conjecture de Leopoldt en p pour k.
En particulier, on a donc les inégalités :

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

et :

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

Ce résultat peut ensuite être amélioré en considérant les $\mathbb{Z}_p$-modules qui interviennent dans le calcul de λ_S^{ab} comme munis d'une action d'un certain groupe de Galois $\mathrm{Gal}(k/k_0)$. Les inégalités de rang deviennent alors des inégalités entre caractères, et, dans certaines situations, les majorants et minorants obtenus ci-dessus correspondent caractère par caractère. On obtient alors une expression complète de λ_S^{ab} en fonction du comportement des places à l'infini, et des places au-dessus de p dans l'extension k/k_0. C'est par exemple le cas si k est un corps CM, et k_0 son sous-corps totalement réel maximal, ou si k/k_0 est une extension à conjugaison p-adique. Ces cas avaient déjà été traités par Jaulent et Sands d'une part ([9]), par Jaulent d'autre part ([11]). L'apport consiste donc à avoir donné le calcul dans un contexte général, en particulier en autorisant de la ramification. On complète avec un exemple d'extension où la méthode précédente donne les valeurs exactes des rangs de certains caractères, mais pas de tous.

Dans la suite du premier chapitre, on étudie les nombres de générateurs et de relations du groupe $\tilde{G}_S$ par les méthodes de Chafarevitch et Koch. On identifie pour cela un groupe de Kummer adapté à cette situation arithmétique :

Définition I.2.3. *Pour S un ensemble fini de places finies de k, on note $\tilde{V}_S$ le sous-groupe suivant des idèles principaux :*

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

où $\tilde{\mathcal{U}}_{\overline{S}}$ est le produit direct $\prod_{v\notin S}\tilde{\mathcal{U}}_v = \prod_{v\in \mathrm{Pl}_p(k)-S_p}\tilde{\mathcal{U}}_v \prod_{v\notin \mathrm{Pl}_p(k)\cup S_0}\mathcal{U}_v$.

En particulier, dès que S contient toutes les places de $\mathrm{Pl}_p(k)$, le groupe $\tilde{V}_S/\mathcal{R}_k^p$ est égal au groupe de Kummer habituel $V_S/\mathcal{R}_k^p$. On est alors en mesure d'énoncer le théorème :

Théorème I.2.2. *Le nombre de générateurs $d(\tilde{G}_S)$ du groupe $\tilde{G}_S$ vaut :*

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

et, pour p impair, le nombre de relations vérifie l'inégalité :

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

la notation $*$ soulignant que la somme peut être diminuée de 1 si S est non vide, et que k contient les racines p-èmes de l'unité.
En particulier, la caractéristique d'Euler tronquée à l'ordre 2 de la cohomologie de $\tilde{G}_S$ à coefficients dans $\mathbb{F}_p$ admet la majoration :

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

le terme $\delta(k)$ pouvant être omis, si $S\neq\emptyset$.

On étudie ensuite quelques critères de trivialisation du groupe $\tilde{V}_S/\mathcal{R}_k^p$. On se limite au cas où le corps k est p-rationnel, et on donne, dans cette situation, des exemples où $\tilde{V}/\mathcal{R}_k^p$ est trivial, sans que k soit le corps des rationnels ou un corps quadratique imaginaire. L'hypothèse de p-rationalité est restrictive, et il serait sûrement intéressant d'étudier cette trivialisation dans un cadre plus général. Remarquons aussi que le majorant donné de $r(\tilde{G}_S)$, pour $S_p\neq\mathrm{Pl}_p(k)$, est toujours non trivial : il ne fournit donc pas de critère de liberté du groupe $\tilde{G}_S$. Au demeurant, ce groupe n'est en général pas libre, s'il n'est pas de rang 1 : en effet, s'il l'était, son sous-groupe $\mathrm{Gal}(L_S^\infty(k_\infty)/k_\infty)$ serait libre de rang infini, situation en général impossible au vu des invariants d'Iwasawa.
Une majoration est aussi donnée dans le cas $p=2$. Le majorant trouvé dépend alors d'une propriété de trivialisation d'une certaine application entre des groupes de cohomologie de groupes de Galois d'extensions de corps de nombres 2-adiques. On ne parvient pas à caractériser entièrement les cas où cette application est triviale, mais on donne quelques éléments de réponse permettant notamment de traiter les extensions abéliennes de $\mathbb{Q}_2$.
La fin du premier chapitre est dévolue à quelques remarques supplémentaires. On note que la majoration obtenue du nombre de relations peut aussi se découper suivant les caractères d'une action d'un groupe de Galois $\mathrm{Gal}(k/k_0)$; et on examine le lien entre le comportement du groupe $\tilde{G}_S(k_n)$ quand k_n varie dans la $\mathbb{Z}_p$-extension cyclotomique de k, et les invariants d'Iwasawa du module d'Iwasawa non ramifié. Le seul directement accessible par cette méthode est l'invariant ρ, comme à l'habitude.

Dans le deuxième chapitre (qui fera l'objet de [27]), on raffine les résultats de Wingberg ([44]) mentionnés dans la section I.1.5. On se limite dans ce chapitre au cas où le nombre premier p est impair ; en revanche, on donne des résultats valables sur les corps de fonctions. L'objet de base est encore un groupe de Kummer adapté à la situation arithmétique (voir par exemple [6] chapitre théorème I, 4.6) :

Définition I.2.4. *Soient S et T deux ensembles finis et disjoints de places finies de k, corps de nombres ou de fonctions. On pose :*

$$V_S^T = \mathcal{R} \cap \mathcal{J}^p \mathcal{U}_{\overline{S \cup T}} \mathcal{K}_T,$$

et on appelle groupe de Kummer le quotient $V_S^T/\mathcal{R}_k^p$.

On montre l'existence d'une majoration du nombre de relations du groupe G_S^T faisant intervenir la dimension du groupe de Kummer, du type formule de Chafarevitch I.1.4, en passant par le contrôle d'un noyau de localisation :

$$Ш^2(G_S^T, \mathbb{F}_p) \hookrightarrow V_S^T/\mathcal{R}_k^p.$$

La majoration du nombre de relations avait déjà été obtenue par Gras ([6], appendice, corollaire 3.7.2) par une autre méthode ne faisant pas intervenir ce contrôle d'un noyau de localisation (ainsi que nous l'a signalé Alexander Schmidt, elle est aussi disponible dans la seconde édition de [24]). On est alors en mesure de donner une présentation de type Koch du groupe G_S^T sous condition de trivialité du groupe de Kummer. On étudie quelques conditions de trivialité de ce groupe de Kummer, qui débordent le cas des corps p-rationnels, et sont reliées à la notion plus générale de S_p-rationalité telle qu'étudiée par Jaulent et Sauzet ([13]). Enonçons par exemple le résultat suivant dans le cas des corps de nombres :

Théorème I.2.3. *Soit p un nombre premier impair, et k un corps de nombres. Soit S un ensemble fini de places finies de k telles que $\sum_{v \in S_p}[k_v : \mathbb{Q}_p] \geq r_1 + r_2 - 1$, et soit T un ensemble fini de places finies de k tel que k n'admette aucune p-extension T-décomposée non triviale et que le morphisme de localisation en $S_p = S \cap \mathrm{Pl}_p(k)$ soit un isomorphisme du p-adifié $\mathcal{E}^T$ du groupe des T-unités dans $\mathcal{U}_{S_p}$. Supposons que les places $\{v_1, \ldots, v_d\}$ de $S - S_p$ sont telles que k_{v_i} contient les racines p-èmes de l'unité. Alors le groupe G_S^T admet une présentation de la forme :*

$$< \alpha_1, \ldots, \alpha_d | \alpha_i^{N(v_i)-1} \prod_{j \neq i} [\alpha_j, \alpha_i]^{l_{ij}} \bmod [F, F^p[F,F]] / i = 1, \ldots, d > .$$

Dans cette présentation, F est le pro-p-groupe libre sur les générateurs α_i, chaque α_i est image dans G_S^T d'un générateur du groupe procyclique $\mathrm{Gal}(\overline{k_{v_i}}/k_{v_i}^{nr})$, et les nombres d'enlacement $l_{ij} \in \mathbb{Z}/p\mathbb{Z}$ sont donnés par l'identité :

$$\pi_i \equiv \prod_j \alpha_j^{l_{ij}} \bmod (G_S^T)_2,$$

où π_i est l'image dans G_S^T d'un relevé dans $\mathrm{Gal}(\overline{k_{v_i}}/k_{v_i})$ de l'automorphisme de Frobenius du groupe procyclique $\mathrm{Gal}(k_v^{nr}/k_v)$.

Par ailleurs, une méthode est donnée pour calculer les coefficients l_{ij} dans ces présentations. Ceci permet de calculer explicitement plusieurs situations où le théorème de Labute s'applique, et où le groupe de Galois G_S^T est clément.

Enfin, le dernier chapitre de cette thèse (qui devrait être l'objet de [29]) est consacré à une extension des résultats de Mizusawa au cas de groupes de Galois

modérément ramifiés, c'est-à-dire au calcul de présentation du groupe de Galois de la pro-2-extension S-ramifiée maximale de la $\mathbb{Z}_2$-extension cyclotomique k_∞ d'un corps quadratique imaginaire k. En premier lieu, on s'intéresse à la partie abélienne de ce groupe de Galois, ce qui constitue une extension du résultat de Ferrero et Kida, et on obtient :

Théorème I.2.4. *Soit $k = \mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire avec d impair, D l'ensemble des nombres premiers qui divisent d, S un ensemble fini de nombres premiers impairs. Pour tout nombre premier impair on définit $2^{k'_p}$ comme la plus grande puissance de 2 divisant p^2-1.*
Le module d'Iwasawa S-ramifié au-dessus de la $\mathbb{Z}_2$-extension cyclotomique de $\mathbb{Q}$ a pour invariant λ :

$$\lambda_S(k_\infty) = \#(S \cup D)(\mathbb{B}_\infty) + \lambda_S(\mathbb{B}_\infty) - 1 - \delta,$$

avec $\delta \in \{0,1,2\}$. Plus précisément, si $k = \mathbb{Q}(i)$ alors $\delta = 1$, si $k \neq \mathbb{Q}(i)$ alors $\delta = 0$.
On rappelle que la nombre de places dans $\mathbb{B}_\infty$ au-dessus d'un nombre premier impair $p \in S \cup D$ est $2^{k'_p-3}$.
De plus, la $\mathbb{Z}_2$-torsion de $X_S(k_\infty)$ vérifie

$$\mathrm{Tor}_{\mathbb{Z}_2} X_S(k_\infty) \simeq \mathrm{Tor}_{\mathbb{Z}_2} X_S(\mathbb{B}_\infty),$$

lorsque 2 est inerte ou décomposé dans $k/\mathbb{Q}$.

On donne par ailleurs aussi une identité sur l'invariant λ du module d'Iwasawa S-ramifié 2-décomposé. La méthode de Mizusawa s'applique ensuite à tous les cas où le module d'Iwasawa est isomorphe en tant que $\mathbb{Z}_2$-module à $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, et on obtient :

Théorème I.2.5. *Soient p et q deux nombres premiers congrus respectivement à 5 et 3 modulo 8, et soit $S = \{q\}$. Soit k le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$ et $\mathcal{G} = \mathrm{Gal}(\tilde{L}_S(k_\infty)/k_\infty)$ le groupe de Galois de la pro-2-extension S-ramifiée maximale de k_∞. Alors $\mathcal{G}$ a pour rang 2, son abélianisé est isomorphe en tant que $\mathbb{Z}_2$-module à $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, et $\mathcal{G}$ admet pour présentation :*

$$< a, b | [a,b]a^2 > .$$

La même conclusion demeure avec $p \equiv 3 \bmod 8$ et $q \equiv 5 \bmod 8$, ou, pour $k = \mathbb{Q}(i)$ avec $q \equiv 7 \bmod 16$.

De ce résultat on déduit, dans certaines situations, une présentation du groupe de Galois de la 2-tour de corps de classes de S-rayon au-dessus de chaque étage k_n de la $\mathbb{Z}_2$-extension cyclotomique de k.

Enfin, mentionnons que le système de calcul PARI/GP a été abondamment utilisé au cours de cette thèse : par exemple pour le calcul des exemples du chapitre 3 et pour la formulation des énoncés du chapitre 4. Il est disponible à l'adresse `http ://pari.math.u-bordeaux.fr/`.

I.3 Notations.

On complète ici la liste, amorcée dans la section I.1.1, des notations utilisées tout au long de ce mémoire. Certaines autres notations, qui sont spécifiques au dernier chapitre, y seront introduites.

Généralités.

p	un nombre premier (impair dans le chapitre 3).
k	un corps de nombres (ou de fonctions, chapitre 3).
S, T	des ensembles finis et disjoints de places de k.
$\mathrm{Pl}(k)$	ensemble des places de k.

Si k est un corps de nombres :

$\mathrm{Pl}_p(k)$	ensemble des places de k au-dessus de p.
$\mathrm{Pl}_\infty(k)$	ensemble des places à l'infini de k.
$r_1(k), r_2(k), r(k)$	nombre de places réelles, de places complexes, de places à l'infini de k ($r(k) = r_1(k) + r_2(k)$).
$S_p = S \cap \mathrm{Pl}_p(k)$	ensemble des places de S au-dessus de p.
S_0	ensemble des places de S qui ne sont pas au-dessus de p.

$\mu(k)$	groupe des racines de l'unité de k.
$\mu_p(k)$	sous-groupes de $\mu(k)$ des racines de l'unité d'ordre une puissance de p.
$\delta(k)$	vaut 0 ou 1 suivant que $\mu_p(k)$ est trivial ou non.
δ	défaut de la conjecture de Leopoldt en p pour le corps k.

Pour une place $v \in \mathrm{Pl}(k)$:

$\chi(v)$	caractéristique du corps résiduel de k en la place v.
$N(v)$	cardinal du corps résiduel de k en la place v.

Notions linéaires (dimensions, abélianisés).

Pour W un $\mathbb{F}_p$-espace vectoriel de dimension finie :

$\dim_{\mathbb{F}_p} W$	$\mathbb{F}_p$-dimension de W.

Pour W un $\mathbb{Z}_p$-module de rang fini :

$\mathrm{rg}_{\mathbb{Z}_p} W = \mathrm{rk}_{\mathbb{Z}_p} W$	$\mathbb{Z}_p$-rang de W.
$\mathrm{Tor}_{\mathbb{Z}_p} W$	sous-module des éléments de $\mathbb{Z}_p$-torsion de W.
$F_{\mathbb{Z}_p} W$	quotient de W par $\mathrm{Tor}_{\mathbb{Z}_p} W$.
$W[p]$	sous-module de p-torsion de W : $\{w \in W / pw = 0\}$.

Pour G un pro-p-groupe de présentation finie :

$d(G)$	cardinal d'un système minimal de pro-p-générateurs du groupe G.
$r(G)$	cardinal d'un système de relations d'une pro-p-présentation minimale de G.
$\chi_2(G)$	caractéristique d'Euler tronquée à l'ordre 2 pour la cohomologie de G à coefficients dans $\mathbb{F}_p$ ($\chi_2(G) = 1 - d(G) + r(G)$).

G^{ab}	pro-p-quotient abélien maximal de G.
G^{ab}/p	pro-p-quotient abélien p-élémentaire maximal de G. En particulier : $d(G) = \dim_{\mathbb{F}_p} G^{ab}/p$.

Soit Δ un groupe fini, et A un $\mathbb{C}_p[\Delta]$-module :

$\chi(A)$	caractère de A.
$r_\chi(A)$	χ-rang de A, où χ est un caractère $\mathbb{C}_p$-irréductible de Δ.

Extensions de k et leurs groupes de Galois.

Si k est un corps de nombres algébriques ou ℓ-adiques (avec $\ell = p$ ou $\ell \neq p$) :

k^{ab}	pro-p-extension abélienne maximale de k.
k_∞	$\mathbb{Z}_p$-extension cyclotomique de k.

Si k est un corps de nombres algébriques :

$L(k)$	p-corps de Hilbert de k.
$L_S^T(k)$	pro-p-extension abélienne S-ramifiée T-décomposée maximale de k.
$L_S^\infty(k)$	pro-p-extension S-ramifiée maximale de k.
G_S^T	groupe de Galois de la pro-p-extension S-ramifiée T-décomposée maximale de k.
$\tilde{G}_S$	groupe de Galois de la pro-p-extension maximale de k qui est S-ramifiée au-dessus de la $\mathbb{Z}_p$-extension cyclotomique de k.

Si k est un corps de nombres ℓ-adiques :

k^{nr}	$\mathbb{Z}_p$-extension non ramifiée de k.
k^{cr}	compositum des $\mathbb{Z}_p$-extensions non ramifiées et cyclotomiques de k (qui sont distinctes seulement si $p = \ell$).

Groupes d'unités, groupes d'idèles, groupes de classes.

On renvoie à la section I.1.1 pour l'essentiel des notations. On utilisera en plus :

$\mathcal{E}^T$	p-adifié du groupe des T-unités.
$A(k)$	p-Sylow du groupe des classes de k.
$A_S^T(k)$	p-Sylow du groupe des T-classes S-infinitésimales de k (obtenu par exemple comme $\mathcal{J}_k/\mathcal{R}_k\mathcal{U}_{\overline{S\cup T}}\mathcal{K}_T$).

Chapitre II

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

Rappelons brièvement la situation pour ce chapitre (voir le chapitre introductif pour un commentaire plus détaillé). On se donne p un nombre premier, k un corps de nombres, S un ensemble fini de places finies de k, k_∞/k la $\mathbb{Z}_p$-extension cyclotomique de k. On note $L_S^\infty(k_\infty)$ la pro-p-extension S-ramifiée maximale de k_∞ et $\tilde{G}_S$ le groupe de Galois $\mathrm{Gal}(L_S^\infty(k_\infty)/k)$. Les résultats vont porter sur les nombres de générateurs et de relations du pro-p-groupe $\tilde{G}_S$, et sur le $\mathbb{Z}_p$-rang de son abélianisé. Il est commode de mettre à part la $\mathbb{Z}_p$-extension cyclotomique, qui participe bien sûr à ce rang, et d'introduire la notation :

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

II.1 Partie $\mathbb{Z}_p$-libre

II.1.1 Sur le rang

Jaulent et Sands ont donné la valeur de l'invariant λ^{ab} dans un certain nombre de cas sur l'extension $k/\mathbb{Q}$: totalement décomposée en p, ou non décomposée en p, k corps CM (voir [9]). Rappelons par exemple le résultat suivant :

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

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

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

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

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

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

Démonstration. Pour la première assertion, il suffit de remarquer que $L^\infty(k_\infty)^{ab}$ est une sous-extension de k_p^{ab}, la pro-p-extension abélienne p-ramifiée maximale de k, et il est bien connu que $\mathrm{Gal}(k_p^{ab}/k)$ est de $\mathbb{Z}_p$-rang $r_2(k)+1+\delta$. En tant que quotient, $\mathrm{Gal}(L^\infty(k_\infty)^{ab}/k)$ est de rang inférieur, et, par abélianité, on obtient le résultat sur le rang de $\mathrm{Gal}(L^\infty(k_\infty)^{ab}/k_\infty)$.
Supposons maintenant que p est totalement décomposé dans $k/\mathbb{Q}$. Soit v une place de k au-dessus de p. Alors, par hypothèse de décomposition, $k_v=\mathbb{Q}_p$; ainsi, le localisé $(k_p^{ab})_v$ est contenu dans la pro-p-extension abélienne maximale $\mathbb{Q}_p^{ab}$, et contient sa $\mathbb{Z}_p$-extension cyclotomique $\mathbb{Q}_{p,\infty}$, qui est totalement ramifiée, et qui est la sous-extension p-ramifiée maximale de $\mathbb{Q}_p^{ab}$ si p est impair, est d'indice fini dans cette extension si $p=2$. Ainsi, le groupe d'inertie $I_v(k_p^{ab}/k)\simeq I_v((k_p^{ab})_v/\mathbb{Q}_p)=\mathrm{Gal}((k_p^{ab})_v/(k_p^{ab})_v\cap\mathbb{Q}_p^{nr})$ est isomorphe à un groupe de la forme $\mathbb{Z}_p\times$ (fini) (avec partie finie triviale si p est impair). Pour chaque place v, le corps fixé par $I_v(k_p^{ab}/k)$ est donc une extension de k, dont le groupe de Galois est de $\mathbb{Z}_p$-rang $r_2(k)+\delta$. Par compositum avec k_∞, on en déduit que k_p^{ab}/k_∞ est non ramifiée en v. Ceci étant vrai pour n'importe quelle place v au-dessus de p, et k_p^{ab}/k étant par définition non ramifiée aux autres places de k, on en déduit que $k_p^{ab}=L^\infty(k_\infty)^{ab}$, d'où la deuxième assertion.
La dernière assertion s'obtient tout simplement par compositum. □

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

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

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

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

$$\mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k)\simeq \mathcal{J}_k/\mathcal{R}_k\tilde{\mathcal{U}}_{\overline{S}}.$$

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

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

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

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

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

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

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

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

Définition II.1.1. *Pour k un corps de nombres, et S un ensemble fini de places finies de k, on note $\mathcal{E}_{k,S}$ (respectivement $\tilde{\mathcal{E}}_{k,S}$) le sous-groupe de $\mathcal{E}_k$, image réciproque par l'application de localisation ϕ de $\mathcal{U}_{\overline{S}}$ (respectivement de $\tilde{\mathcal{U}}_{\overline{S}}$).*
La finitude des groupes $\tilde{\mathcal{U}}_v$ pour v ne divisant pas p permet de voir que les groupes $\mathcal{E}_{k,S}$ et $\mathcal{E}_{k,S_p}$ (respectivement $\tilde{\mathcal{E}}_{k,S}$ et $\tilde{\mathcal{E}}_{k,S_p}$) ont même $\mathbb{Z}_p$-rang.

Théorème II.1.3. *L'invariant λ_S^{ab} vaut :*

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

où ϕ_p est l'application de semi-localisation en p et δ le défaut de la conjecture de Leopoldt en p pour k.
En particulier, on a donc les inégalités :

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

et :

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

Remarque II.1.4.

1. *Pour un corps k totalement réel, vérifiant la conjecture de Leopoldt, $\lambda_S^{ab} = 0$, pour tout S.*
   De manière générale, si $S = \mathrm{Pl}_p(k)$, on trouve :
   $$\lambda_S^{ab} = r_2(k) + \delta,$$
   ce qui est bien connu, puisque toutes les $\mathbb{Z}_p$-extensions d'un corps de nombres sont non ramifiées en dehors de $\mathrm{Pl}_p(k)$.
2. *Si p est totalement décomposé dans $k/\mathbb{Q}$, le minorant dans l'inégalité ci-dessus est précisément $r_2 + \delta$, et donc, pour n'importe quelle partie S de $\mathrm{Pl}_p(k)$:*
   $$\lambda_S^{ab} = r_2 + \delta.$$
   On retrouve le résultat pour ce cas du théorème II.1.1. Remarquons que ceci provient in fine, de la finitude (et même de la trivialité pour p impair) de $\tilde{\mathcal{U}}_p$ sous ces hypothèses.
3. *Si p n'est pas décomposé dans $k/\mathbb{Q}$, et $S = \emptyset$, alors $\#\mathrm{Pl}_p(k) = 1$ et $\#S_p = 0$, et donc :*
   $$\lambda^{ab} = 0,$$
   par la majoration dans le théorème précédent. On retrouve ainsi encore un résultat de Jaulent et Sands ([9]).

Remarque II.1.5. *Le résultat est indépendant de $S_0 = S - S_p$. En particulier, si S est un ensemble fini de places dont l'intersection avec $\mathrm{Pl}_p(k)$ est vide, on trouve $\lambda_S^{ab} = \lambda^{ab}$.*

Démonstration. Nous avons de façon évidente une suite exacte :

$$1 \to \mathcal{R}_k\mathcal{U}/\mathcal{R}_k\tilde{\mathcal{U}}_{\overline{S}} \to \mathcal{J}_k/\mathcal{R}_k\tilde{\mathcal{U}}_{\overline{S}} \to \mathcal{J}_k/\mathcal{R}_k\mathcal{U} \to 1,$$

qui se traduit, *via* la correspondance p-adique du corps de classes, par la suite exacte de groupes de Galois :

$$1 \to \mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/L(k)) \to \mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k) \to \mathrm{Gal}(L(k)/k) \to 1.$$

Le dernier terme de ces deux suites est un p-groupe fini, donc de $\mathbb{Z}_p$-rang nul. Le $\mathbb{Z}_p$-rang de $\mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k)$ est donc égal à celui du premier terme, que nous simplifions :

$$N = \mathcal{R}_k\mathcal{U}/\mathcal{R}_k\tilde{\mathcal{U}}_{\overline{S}} \simeq \mathcal{U}/\mathcal{R}_k\tilde{\mathcal{U}}_{\overline{S}} \cap \mathcal{U}.$$

Or, tout idèle p-adique principal qui est partout une unité p-adique locale, est unité p-adique globale, et donc :

$$N \simeq \mathcal{U}/\mathcal{E}_k\tilde{\mathcal{U}}_{\overline{S}} = \mathcal{U}_{S\cup\mathrm{Pl}_p(k)}/\phi_{S\cup\mathrm{Pl}_p(k)}(\mathcal{E}_k)\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}.$$

La décomposition en somme directe $\left(\mathcal{U}_{S\cup\mathrm{Pl}_p(k)}/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}\right) \simeq \mathcal{U}_{S_0} \oplus \left(\mathcal{U}_p/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}\right)$, où $\mathcal{U}_{S_0}$ est fini, induit une injection à conoyau fini :

$$1 \to \mathcal{U}_p/\left(\phi_{S\cup\mathrm{Pl}_p(k)}(\mathcal{E}_k)\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \cap \mathcal{U}_p\right) \to \left(\mathcal{U}_{S\cup\mathrm{Pl}_p(k)}/\phi_{S\cup\mathrm{Pl}_p(k)}(\mathcal{E}_k)\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}\right)$$

Le premier terme s'identifie à $\mathcal{U}_p/\phi_p(\mathcal{E}_{k,S_0})\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}$, où $\mathcal{E}_{k,S_0}$ désigne le sous-groupe de $\mathcal{E}_k$ des éléments qui sont appliqués par $\phi_{\mathrm{Pl}_p(k)\cup S}$ dans $\mathcal{U}_p$, c'est-à-dire qui ont des composantes locales triviales en les places de S_0 (définition II.1.1). On utilise ensuite la suite exacte :

$$1 \to \phi_p(\mathcal{E}_{k,S_0})\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \to \mathcal{U}_p/\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \to \mathcal{U}_p/\phi_p(\mathcal{E}_{k,S_0})\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p} \to 1,$$

dont le premier terme est isomorphe à :

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

où $\tilde{\mathcal{E}}_{k,S}$ est (voir définition II.1.1) le sous-groupe des éléments de $\mathcal{E}_k$ qui ont, par le morphisme ϕ de localisation, des composantes locales triviales en les places de S, et, en les places au-dessus de p, des composantes locales appartenant aux groupes de normes cyclotomiques. Par additivité des $\mathbb{Z}_p$-rangs dans les suites exactes, puisque les groupes finis ont $\mathbb{Z}_p$-rang nul, enfin, puisque $\mathcal{E}_{k,S_0}$ et $\mathcal{E}_k$ ont même $\mathbb{Z}_p$-rang, on obtient :

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

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

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

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

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

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

□

II.1.2 Avec une action galoisienne

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

Rappel sur les structures

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

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

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

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

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

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

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

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

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

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

et en ce qui concerne les caractères :

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

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

$$\mathrm{Reg} = \mathrm{Ind}_1^{\Delta} \mathbf{1},$$

et on rappelle que son caractère est donné par :

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

la somme portant sur tous les caractères $\mathbb{C}_p$-irréductibles de Δ.
Les suites exactes obtenues dans la première partie, dont nous avons vu qu'elles sont des suites exactes aussi pour les structures de Δ-modules, montrent alors :

Proposition II.1.6.

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

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

Calculs de caractères

Le caractère des unités globales est connu par le théorème de Dirichlet galoisien :

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

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

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

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

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

Ceci concerne les structures additives des corps considérés. Pour en déduire des propriétés sur les unités, on considère le logarithme p-adique, qui lie la structure additive à la structure multiplicative. En considérant de plus les p-adifiés, $\mathcal{U}_v$ devient $[(k_0)_v : \mathbb{Q}_p]$ fois le $\mathbb{Z}_p[\Delta_w]$-module trivial, puisque Δ_w agit trivialement sur $\mathcal{U}_v$, et que ce dernier est de dimension $[(k_0)_v : \mathbb{Q}_p]$ en tant que $\mathbb{Z}_p$-module, *via* le logarithme p-adique. On en déduit que $\mathcal{U}_w$ est $[(k_0)_v : \mathbb{Q}_p]$ fois le $\mathbb{Z}_p[\Delta_w]$-module régulier.
On calcule maintenant le caractère de l'action de Δ sur $\mathcal{U}_p$, en remarquant que ce module s'écrit $\prod_{v\in \mathrm{Pl}_p(k_0)} \prod_{w\in \mathrm{Pl}_v(k)} \mathcal{U}_w$, et que chaque facteur $\prod_{w\in \mathrm{Pl}_v(k)} \mathcal{U}_w$ admet une structure de Δ-module, qui est l'induite de la structure de Δ_w-module de $\mathcal{U}_w$. On mène donc le calcul :

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

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

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

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

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

et donc :

$$\chi(\mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k)) \geq$$

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

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

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

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

Proposition II.1.7. *On a l'égalité :*

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

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

Remarque II.1.8. *Si $k = k_0$, on retrouve le théorème II.1.3.*

Il est possible que certains caractères irréductibles viennent avec un coefficient négatif dans la somme des trois premiers termes du membre de droite de l'identité. Cela implique alors que le terme $\chi_R + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S}))$ est supérieur à chacun de ces caractères, ce qui fournit en retour une amélioration de la minoration de rang obtenue en II.1.3. Le résultat général est le suivant :

Théorème II.1.9. *Le caractère virtuel :*

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

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

$$\chi_R + \chi(\phi_p(\mathcal{E}_k)) \wedge \chi(\tilde{\mathcal{U}}_{\mathrm{Pl}_p(k)-S_p}) \geq \chi_R + \chi(\phi_p(\tilde{\mathcal{E}}_{k,S})) \geq \chi_-, \text{ et}$$
$$\chi(\mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k_\infty)) \geq \chi_+.$$

En particulier, on a la minoration :

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

Si, de plus, la conjecture de Leopoldt en p pour le corps k est vraie, et que l'égalité $\chi(\tilde{\mathcal{E}}_{k,S}) = \chi_-$ est vérifiée, alors on a l'égalité $\chi(\mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k_\infty)) = \chi_+$.

Démonstration. L'écriture sous la forme $\chi_+ - \chi_-$ est un fait classique en théorie des représentations de groupes (voir [35]). Le caractère $\chi(\mathrm{Gal}(L_S^\infty(k_\infty)^{ab}/k_\infty))$ est positif et vaut alors :

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

ce qui montre l'inégalité :

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

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

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

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

Illustrations

Tous les résultats suivants seront des conséquences du théorème ci-dessus. **On suppose désormais la conjecture de Leopoldt vérifiée pour tous les corps considérés**, c'est-à-dire que $\chi_R = 0$. On est en mesure sous ces conditions de calculer entièrement l'invariant λ_S^{ab} pour n'importe quel corps CM, et donc en particulier pour toute extension abélienne de $\mathbb{Q}$, le cas des corps totalement réels ayant déjà été traité. Ce cas, pour $S = \emptyset$, était déjà traité dans l'article [9].
Par ailleurs, sous l'hypothèse $S = \emptyset$, le cas d'une extension non décomposée en p d'une extension totalement décomposée en p, peut aussi être traité ; cela donne une nouvelle formulation pour les extensions abéliennes de $\mathbb{Q}$, peut-être plus agréable.

En vertu de la remarque II.1.5, on suppose ici $S \subset \mathrm{Pl}_p(k)$.

Corollaire II.1.10. *Soit k un corps CM, et k^+ sa sous-extension totalement réelle maximale. Soit S un ensemble de places dans $\mathrm{Pl}_p(k^+)$. Soit T_1 l'ensemble des places de $\mathrm{Pl}_p(k^+) - S$ qui se décomposent dans k/k^+, T_2 celles qui ne se décomposent pas. Alors :*

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

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

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

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

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

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

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

Le caractère virtuel auquel on souhaite appliquer le théorème II.1.9 est donc :

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

En appliquant le théorème II.1.9, on trouve donc ici :

$$\chi_+ = (\sum_{v\in S}[k_v^+ : \mathbb{Q}_p] + \#T_1)\chi_c,$$

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

On remarque en particulier que le caractère χ_- ci-dessus est bien positif. On considère ensuite la majoration de $\chi(\phi_p(\tilde{\mathcal{E}}_{k,S}))$ établie dans le théorème II.1.9. Ici :

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

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

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

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

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

et on conclut par le théorème II.1.9. □

Corollaire II.1.11. *On suppose ici $S = \emptyset$. Supposons que $k_0/\mathbb{Q}$ est une extension p-décomposée, et k/k_0 une extension galoisienne non décomposée en toutes les places au-dessus de p ; ces conditions sont en particulier vérifiées pour une extension $k/\mathbb{Q}$ abélienne, avec k_0 la sous-extension p-décomposée maximale. Alors :*

$$\chi(\mathrm{Gal}(L^\infty(k_\infty)^{ab}/k_\infty)) = r_2(k_0)\mathbf{1},$$

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

Démonstration. En effet, dans ce contexte :

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

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

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

permet de montrer que le $\mathbf{1}$-rang est 1. Les places à l'infini sont au nombre de $r_1(k_0) + r_2(k_0)$, et donc, le caractère χ_+ introduit au théorème II.1.9 est :

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

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

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

On utilise ensuite la majoration de $\chi(\phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}}_p)$ établie dans le théorème II.1.9. On a d'une part :

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

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

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

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

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

puis les résultats attendus par application du théorème II.1.9. □

Remarque II.1.12. *Cette situation est celle d'un corps à conjugaison p-adique selon la terminologie de Jaulent ; le résultat est présent dans [11] (théorème 25). Dans le cas général sur S, notre méthode ne permet de fournir que des encadrements ; la raison étant qu'on ne dispose pas d'estimation satisfaisante pour les groupes $\mathcal{E}_{k,S}$, des unités globales ayant une composante triviale en S, dès que S n'est pas vide, et qui seraient voués à jouer le rôle que joue $\mathcal{E}_k$ ici pour l'estimation des χ-composantes.*

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

Corollaire II.1.13. *On suppose toujours $S = \emptyset$. Soit $k/\mathbb{Q}$ une extension galoisienne et soit k_0 l'intersection des sous-corps fixés par les groupes de décomposition D_v, pour v parcourant $S_p(k)$. On suppose qu'aucune place à l'infini ne se complexifie dans l'extension k/k_0, et que les sous-groupes de décomposition $\Delta_v(k/k_0)$, pour $v \in \mathrm{Pl}_p(k)$, sont conjugués dans $\Delta = \mathrm{Gal}(k/k_0)$. Pour chaque caractère $\mathbb{C}_p$-irréductible χ_i de Δ, notons, indépendamment de la place $v \in Pl_p(k)$, $\alpha_i = r_{\chi_i}\mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}$. Alors, pour chacun de ces caractères :*

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

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

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

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

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

Pour chaque caractère $\mathbb{C}_p$-irréductible χ_i de Δ, on introduit alors α_i comme dans l'énoncé, et on peut écrire les χ_i-rangs des caractères χ_+ et χ_- du théorème II.1.9 :

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

La minoration annoncée de $\chi(\mathrm{Gal}(L^\infty(k_\infty)^{ab}/k_\infty))$ se déduit de la première identité, et du théorème II.1.9. Par ailleurs, grâce aux estimations :

$$\chi(\phi_p(\mathcal{E}_k)) \leq \#\mathrm{Pl}_\infty(k_0)\chi(\mathrm{Reg}) \text{ et}$$
$$\chi(\tilde{\mathcal{U}_p}) = [k_0 : \mathbb{Q}](\chi(\mathrm{Reg}) - \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1}),$$

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

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

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

On va spécialiser la proposition précédente dans le cas où le groupe Δ est un groupe diédral D_n à $2n$ éléments. La minoration de λ^{ab} dans le cas n impair est à relever, puisqu'elle permet de voir que le slogan *pour un choix naturel de k_0, on a l'identité $\lambda^{ab} = r_2(k_0)$*, vrai pour une extension abélienne de $\mathbb{Q}$, tombe en défaut en général.
On rappelle les points suivants sur les caractères d'un groupe diédral (voir [35]) : si n est impair, il y a deux caractères irréductibles de degré 1, notés χ_1, χ_2, et tous les autres sont de degré 2, on les notera ψ_j, $j = 1 \ldots \frac{n-1}{2}$ (respectivement, si n est pair, χ_1, χ_2, χ_3, χ_4 les quatre caractères de degré 1, et $j = 1 \ldots \frac{n}{2} - 1$ pour ceux de degré 2). On suppose que les caractères de degré 1 sont numérotés de telle sorte que ceux d'indice pair sont ceux de trace nulle.

Exemple II.1.14. On se place dans la situation précédente et on suppose que Δ est isomorphe à D_n, le groupe diédral à $2n$ éléments. On suppose de plus que les groupes de décomposition Δ_v sont isomorphes à des relevés du quotient $\mathbb{Z}/2\mathbb{Z}$ de D_n. Alors, pour chaque caractère ψ_j de degré 2 :

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

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

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

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

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

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

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

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

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

□

II.2 Nombres de générateurs et de relations

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

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

et

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

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

$$\chi_2(\tilde{G}_S, \mathbb{F}_p) = 1 - d(\tilde{G}_S) + r(\tilde{G}_S).$$

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

II.2.1 Générateurs

On donne une expression pour le nombre minimal de générateurs des groupes considérés, en s'inspirant de l'étude par Koch dans le cas d'une pro-p-extension S-ramifiée maximale (voir [16], section 11.3). On commence par introduire les groupes de Kummer adaptés à notre situation arithmétique :

Définition II.2.1. *Pour S un ensemble fini de places finies de k, on note $\tilde{V}_S$ le sous-groupe suivant des idèles principaux :*

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

où $\tilde{\mathcal{U}}_S$ est le produit direct $\prod_{v\notin S} \tilde{\mathcal{U}}_v = \prod_{v\in \mathrm{Pl}_p(k)-S_p} \tilde{\mathcal{U}}_v \prod_{v\notin \mathrm{Pl}_p(k)\cup S_0} \mathcal{U}_v$; on remarque que $\tilde{V}_S$ est décroissant (pour l'inclusion) par rapport à S. Pour le cas $S = \emptyset$, on notera simplement $\tilde{V} = \tilde{V}_\emptyset$.
Dès que S contient toutes les places de $\mathrm{Pl}_p(k)$, le groupe $\tilde{V}_S/\mathcal{R}_k^p$ est égal au groupe de Kummer habituel $V_S/\mathcal{R}_k^p$.

Lemme II.2.1. *Pour $S \neq \emptyset$, les dimensions des $\mathbb{F}_p$-espaces vectoriels $\tilde{V}_S/\mathcal{R}_k^p$ et $\tilde{\mathcal{E}}_{k,S}/\tilde{\mathcal{E}}_{k,S}^p$ vérifient l'inégalité :*

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

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

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

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

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

et une suite exacte :

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

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

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

et on en déduit le lemme. □

Théorème II.2.2. *Le nombre minimal de générateurs du groupe de Galois* $\tilde{G}_S = \mathrm{Gal}(L_S^\infty(k_\infty)/k)$ *est :*

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

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

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

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

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

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

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

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

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

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

On note aussi les identités suivantes :

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

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

où $A(k)$, le p-Sylow du groupe des classes de k, a été identifié à un quotient du p-adifié du groupe d'idèles.
Pour évaluer $d(\tilde{G}_S)$, on souhaite compléter à gauche la suite précédente. On commence par introduire $\tilde{V}_S \subset V$, définis par :

$$V = \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k,$$

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

On dispose des isomorphismes suivants, induits par les inclusions, grâce au principe de Hasse pour les puissances p-èmes (voir par exemple [6], partie II, théorème 6.3.3) :

$$V/\mathcal{R}_k^p \simeq \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k\mathcal{J}_k^p/\mathcal{J}_k^p,$$

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

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

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

dont toutes les flèches sauf la deuxième ont déjà été définies, la deuxième associant $u \in \mathcal{U}$ à $ua \in \mathcal{U}\mathcal{J}_k^p \cap \mathcal{R}_k\mathcal{J}_k^p$, avec $u \in \mathcal{U}$, $a \in \mathcal{J}_k^p$. L'exactitude de la suite aux deuxième et troisième termes sont les seuls points à ne pas avoir déjà été vérifiés et ne soulèvent pas de difficulté.
Enfin, le calcul suivant de la dimension de $V/\mathcal{R}_k^p$ est classique (voir [16], partie 11.2). On le reproduit ici pour pouvoir s'y référer plus loin. On remarque que V admet l'écriture suivante :

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

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

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

dont on déduit :

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

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

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

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

Le terme le plus difficile dans les formules obtenues est $\tilde{V}_S/\mathcal{R}_k^p$. On souhaiterait obtenir des conditions de trivialisation de ce groupe, notamment en lien avec le théorème II.2.8 (ou, plus exactement, sa preuve), puisqu'un tel résultat fournirait la trivialisation d'un noyau de Chafarevitch. On commence par donner un corollaire bien connu du calcul habituel sur $V/\mathcal{R}_k^p$.

Corollaire II.2.3. *Si k est un corps quadratique imaginaire dont le groupe des classes a un cardinal premier à p, alors $V/\mathcal{R}_k^p$ est trivial, et donc a fortiori tous les $V_S/\mathcal{R}_k^p$ et tous les $\tilde{V}_S/\mathcal{R}_k^p$.*

La proposition suivante donne des conditions pour mener un calcul analogue sur $\tilde{V}/\mathcal{R}_k^p$. Notamment la deuxième assertion de la proposition fait intervenir des propriétés que vérifient les corps dits p-rationnels (voir par exemple [6], partie III, lemme 4.2.4, théorème 4.2.5, et partie IV, théorème 3.5, et la preuve du corollaire II.2.5), ce qui, conjugué avec les estimations des rangs des groupes $\phi_p(\tilde{\mathcal{E}}_k)$ qui découlent des preuves de la partie I, fournit des conditions suffisantes pour la trivialité de $\tilde{V}/\mathcal{R}_k^p$ (corollaire II.2.5). On espère mener ces calculs plus loin dans un travail ultérieur.

Proposition II.2.4. *Soit k un corps de nombres, on considère la restriction $\tilde{\Psi}$ à $\tilde{V}/\mathcal{R}_k^p$ de l'application Ψ de $V/\mathcal{R}_k^p$ dans $A(k)[p]$ rappelée dans la démonstration du théorème II.2.2. Les propriétés suivantes sont vérifiées :*

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

Corollaire II.2.5. *Soit k un corps p-rationnel, dont la p-partie du groupe des classes est triviale, et vérifiant l'une des deux conditions :*

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

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

Démonstration. Un corps p-rationnel vérifie la condition 2 de la proposition : cette condition est exactement le quatrième item de la caractérisation (ii) du théorème 3.5 de la partie IV du livre de Gras ([6]) ; la partie sur les racines de l'unité de notre condition étant automatiquement vérifiée. On obtient ainsi d'après la proposition un isomorphisme entre $\tilde{V}/\mathcal{R}_k^p$ et $\tilde{\mathcal{E}}_k/\tilde{\mathcal{E}}_k^p$. Sous l'une des deux hypothèses de décomposition, le groupe $\tilde{\mathcal{E}}_k$ est un $\mathbb{Z}_p$-module libre (il ne contient pas de racine p-ème de l'unité), et on montre que son $\mathbb{Z}_p$-rang est trivial en utilisant les résultats de la partie I (voir remarque II.1.4 et corollaire II.1.10). □

Exemple II.2.6. On choisit $p = 5$, et $q = 31$. La relation $5^3 \equiv 1 \mod 31$ permet de montrer que le Frobenius de $\mathbb{F}_5(\zeta_{31})/\mathbb{F}_5$ est d'ordre 3 ; ainsi la sous-extension de degré 5 de $\mathbb{Q}(\zeta_{31})/\mathbb{Q}$ est 5-décomposée et c'est une extension 31-ramifiée : il s'agit de la 5-extension (abélienne) 31-ramifiée maximale de $\mathbb{Q}$. On en déduit en particulier que la

5-partie de son groupe des classes est triviale. De plus, d'après la caractérisation des p-extensions p-rationnelles abéliennes de $\mathbb{Q}$ (voir [6], partie IV, exemple 3.5.1), il s'agit d'un corps 5-rationnel. Toujours pour $p = 5$, on a des résultats analogues pour $q = 191$ (en utilisant la relation $5^{19} \equiv 1 \mod 191$), $q = 271$ (grâce à $5^{27} \equiv 1 \mod 271$).

Démonstration. On prouve maintenant la proposition II.2.4. La première assertion de la proposition est triviale. On montre la deuxième. Le noyau considéré est l'intersection :

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

On considère $\mathcal{E}_k \cap \tilde{\mathcal{U}}\mathcal{U}^p$ qui s'injecte *via* l'application de semi-localisation ϕ_p dans $\phi_p(\mathcal{E}_k)$. Son image est alors dans $\phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}}_p\mathcal{U}^p$; soit $e = \tilde{u_1}u_2^p$ un élément de cette image.
On remarque que l'hypothèse sur la section de $\mathcal{U}_p$ implique que $\tilde{\mathcal{U}_p}$ se scinde aussi en une somme directe $\phi_p(\tilde{\mathcal{E}}_k) \oplus \tilde{\mathcal{U}}_p/\phi_p(\tilde{\mathcal{E}}_k)$. Justifions ce point. Pour chaque $\mathbb{Z}_p$-module W, on considère $\mathrm{Tor}_{\mathbb{Z}_p}W$ le sous-module de $\mathbb{Z}_p$-torsion de W et $F_{\mathbb{Z}_p}W$ un sous-module $\mathbb{Z}_p$-libre maximal de W. Dans la somme directe $\mathcal{U}_p \simeq \phi_p(\mathcal{E}_k) \oplus (\mathcal{U}_p/\phi_p(\mathcal{E}_k))$, les parties de torsion vérifient

$$\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{U}_p \simeq \mathrm{Tor}_{\mathbb{Z}_p}\phi_p(\mathcal{E}_k) \oplus \mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{U}_p/\phi_p(\mathcal{E}_k)).$$

On en vient maintenant à considérer $\tilde{\mathcal{U}_p}$ et $\phi_p(\tilde{\mathcal{E}}_k) = \phi_p(\mathcal{E}_k) \cap \tilde{\mathcal{U}_p}$. Il existe une injection naturelle de $\tilde{\mathcal{U}_p}/\phi_p(\tilde{\mathcal{E}}_k)$ dans $\mathcal{U}_p/\phi_p(\mathcal{E}_k)$. On en déduit en particulier une injection de $\mathrm{Tor}_{\mathbb{Z}_p}\tilde{\mathcal{U}_p}/\phi_p(\tilde{\mathcal{E}}_k)$ dans $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{U}_p/\phi_p(\mathcal{E}_k)$. Par ailleurs, $\mathrm{Tor}_{\mathbb{Z}_p}\tilde{\mathcal{U}_p}/\mathrm{Tor}_{\mathbb{Z}_p}\phi_p(\tilde{\mathcal{E}}_k)$ est naturellement un sous-module de torsion de $\tilde{\mathcal{U}_p}/\phi_p(\tilde{\mathcal{E}}_k)$. Il se trouve que la torsion de $\phi_p(\mathcal{E}_k)$, comme celle de $\mathcal{U}_p$, est donnée par les racines p-èmes de l'unité, globales ou locales, et ce sont des normes cyclotomiques locales. On en déduit :

$$\mathrm{Tor}_{\mathbb{Z}_p}\tilde{\mathcal{U}_p}/\mathrm{Tor}_{\mathbb{Z}_p}\phi_p(\tilde{\mathcal{E}}_k) = \mathrm{Tor}_{\mathbb{Z}_p}\mathcal{U}_p/\mathrm{Tor}_{\mathbb{Z}_p}\phi_p(\mathcal{E}_k) = \mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{U}_p/\phi_p(\mathcal{E}_k)),$$

puis l'égalité avec $\mathrm{Tor}_{\mathbb{Z}_p}(\tilde{\mathcal{U}_p}/\phi_p(\tilde{\mathcal{E}}_k))$. On a déjà vu que ce sous-module de torsion est scindé dans $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{U}_p = \mathrm{Tor}_{\mathbb{Z}_p}\tilde{\mathcal{U}_p}$; la partie libre $F_{\mathbb{Z}_p}(\tilde{\mathcal{U}_p}/\phi_p(\tilde{\mathcal{E}}_k))$ se scinde dans $F_{\mathbb{Z}_p}\tilde{\mathcal{U}_p}$. On en déduit que la propriété de section est vraie pour la suite exacte :

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

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

On en déduit le résultat suivant sur la torsion de l'abélianisé du groupe $\tilde{G_S}$.

Corollaire II.2.7. *Notons* $\mathrm{tor}(\tilde{G_S}^{ab})$ *le sous-*$\mathbb{Z}_p$*-module de torsion de* $\tilde{G_S}^{ab}$*. La dimension du* $\mathbb{F}_p$*-espace vectoriel* $\mathrm{tor}(\tilde{G_S}^{ab})/p$ *est :*

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

où δ désigne le défaut de la conjecture de Leopoldt en p pour le corps k, et où $\delta(k)$ et $\delta(k_v)$ testent l'appartenance des racines p-èmes de l'unités aux corps k et k_v.
Pour $p \geq 5$, et un corps quadratique imaginaire, cette torsion est triviale. De même, pour $p \geq 3$ et pour un corps k ne contenant pas les racines de l'unité et vérifiant les hypothèses 1 et 2 de la proposition II.2.4, si $S = \emptyset$, et pour S quelconque si de plus $k/\mathbb{Q}$ est totalement décomposée en p.

Démonstration. La première assertion résulte du théorème II.2.2, et du théorème II.1.3 (se rappeler que l'invariant λ_S^{ab} diffère du $\mathbb{Z}_p$-rang de $\tilde{G_S}^{ab}$ de 1). La deuxième assertion s'en déduit, grâce aux conditions d'annulation de $\tilde{V}_S/\mathcal{R}_k^p$ données dans le corollaire II.2.5. En particulier, on utilise le fait qu'un corps quadratique imaginaire, ni aucun de ses localisés en les places au-dessus de p, ne contiennent les racines p-èmes de l'unité dès que $p \geq 5$. □

II.2.2 Relations

On va montrer le théorème suivant :

Théorème II.2.8. *Le nombre de relations du groupe de Galois de la pro-p-extension S-ramifiée au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres vérifie, si p est impair :*

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

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

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

où ϵ_v est une quantité valant toujours 0 si l'inflation de la proposition II.2.14 est un isomorphisme et 1 sinon.

Remarque II.2.9. *La détermination générale des quantités ϵ_v reposerait sur une extension de la proposition II.2.14 ci-dessous au cas général, ce qui paraît délicat.*

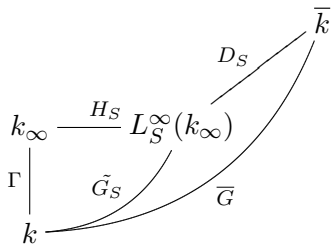
Corollaire II.2.10. *La caractéristique d'Euler tronquée à l'ordre 2 du groupe $\tilde{G_S}$ vérifie, si p est impair :*

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

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

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

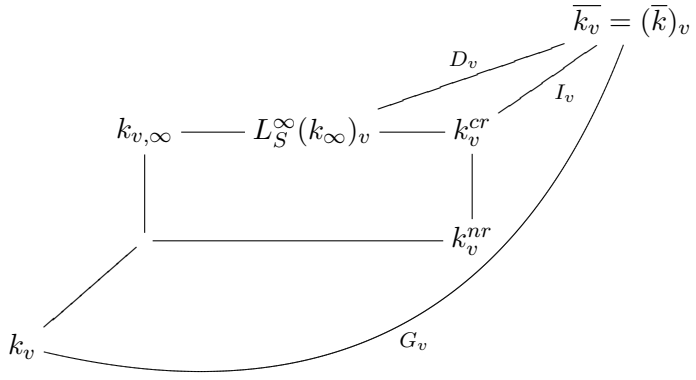
Démonstration. On introduit la pro-p-extension maximale de k, que nous notons $\overline{k}$, et on a la tour d'extensions globales suivante :



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

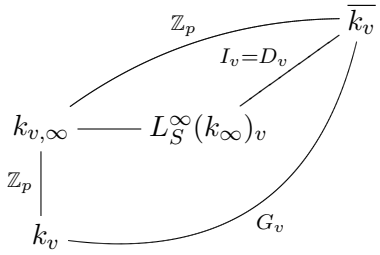
Définition II.2.2. *Si v est une place au-dessus de p, et k_v le localisé en cette place du corps de nombres k, alors k_v est une extension finie de $\mathbb{Q}_p$. On note k_v^{nr} la $\mathbb{Z}_p$-extension non ramifiée de k_v et k_v^{cr} le compositum de la $\mathbb{Z}_p$-extension cyclotomique de k_v et de k_v^{nr}. On note $\overline{k_v}$ la pro-p-extension maximale de k_v.*

On commence par décrire les localisations en les places v de k en dehors de S (c'est-à-dire qu'on s'est fixé un prolongement de la place v à $\overline{k}$, et qu'on considère l'union des complétions des sous-extensions finies de $\overline{k}/k$, voir [34], paragraphe II.6) du diagramme d'extensions précédent. En une place $v \in \mathrm{Pl}_p(k) - S_p$, on obtient le diagramme d'extensions locales suivant :



Le groupe G_v est le pro-p-groupe de Galois absolu du corps local k_v, le groupe D_v introduit ici est le sous-groupe de décomposition en la place v du groupe de Galois global D_S, quant au groupe I_v, il est à la fois le sous-groupe d'inertie en la place v du groupe D_S, et du groupe $\mathrm{Gal}(\overline{k}/k_\infty)$ (l'extension $L_S^\infty(k_\infty)/k_\infty$ étant non ramifiée en v, qu'on a choisi en dehors de S).
En une place v en dehors de $\mathrm{Pl}_p(k)$, si le corps k_v ne contient pas les racines p-èmes de l'unité (c'est-à-dire si la norme Nv de l'idéal v n'est pas congrue à 1 modulo p), la pro-p-extension maximale de k_v est sa $\mathbb{Z}_p$-extension cyclotomique, qui est non ramifiée. En de telles places, on note I_v le groupe trivial. Dans le cas où Nv est

congrue à 1 modulo p, on a en revanche le diagramme suivant :



Que v soit une place au-dessus de p ou non, on notera H_v le groupe quotient G_v/I_v. En particulier, dans le cas d'une place finie en dehors de $\mathrm{Pl}_p(k)\cup S$, le corps $L_S^\infty(k_\infty)_v$ est une extension non ramifiée de $k_{v,\infty}$ et est donc égal à $k_{v,\infty}$, ce qui implique que le groupe H_v est isomorphe à $\mathbb{Z}_p$ dans ce cas. Pour une place au-dessus de p, le groupe H_v est le groupe de Galois $\mathrm{Gal}(k_v^{cr}/k_v)$ et est isomorphe à $\mathbb{Z}_p^2$. De manière générale, on remarque que les extensions locales introduites en les places en dehors de S, correspondant aux groupes H_v, peuvent être définies de manière purement locale.

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

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

$$H^1(\tilde{G_S})\overset{inf}{\hookrightarrow} H^1(\overline{G}) \overset{res}{\longrightarrow} H^1(D_S)^{\tilde{G_S}} \overset{tra}{\longrightarrow} H^2(\tilde{G_S}) \overset{inf}{\longrightarrow} H^2(\overline{G}) \ ,$$

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

$$H^1(H_v)\overset{inf}{\hookrightarrow} H^1(G_v) \overset{res}{\longrightarrow} H^1(I_v)^{H_v} \overset{tra}{\longrightarrow} H^2(H_v) \overset{inf}{\longrightarrow} H^2(G_v) \ .$$

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

Lemme II.2.11. *Il existe une injection :*

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

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

Remarque II.2.12. *On peut se demander si cette flèche peut être naturellement incluse dans un sous-groupe du produit direct, à la manière de la proposition 21, du chapitre II du livre de Serre [34].*

Démonstration. L'extension $L_S^\infty(k_\infty)/k_\infty$ étant la sous-extension S-ramifiée non complexifiée maximale de $\overline{k}/k_\infty$, le groupe de Galois $D_S = \mathrm{Gal}(\overline{k}/L_S^\infty(k_\infty))$ est topologiquement et normalement engendré par les sous-groupes d'inertie I_v de $\mathrm{Gal}(\overline{k}/k_\infty)$, pour v décrivant les places finies de k en dehors de S, et, dans le cas $p = 2$, les places archimédiennes de k. Ceci induit une flèche entre le pro-p-produit libre des I_v et D_S

dont l'image est bien sûr fermée, et dont la clôture normale de l'image est D_S entier. On compose cette flèche avec le passage au quotient $D_S/D_S^p[D_S, \tilde{G_S}]$; la composée est alors surjective. La flèche ainsi obtenue, qui part du produit libre des I_v, se factorise alors dans le produit direct des $I_v/I_v^p[I_v, G_v]$ et fournit une application surjective :

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

Par ailleurs, si la norme de la place finie v n'est pas 0 ou 1 modulo p, le groupe I_v est trivial, et de même pour une place infinie complexe, et une place infinie réelle si p est impair ; en revanche, pour une place infinie réelle, et $p = 2$, on a $I_v = G_v = \mathbb{Z}/2\mathbb{Z}$, et donc $I_v/I_v^2[I_v, G_v] \simeq \mathbb{Z}/2\mathbb{Z}$. Le dual de Pontryagin de cette flèche est la restriction $H^1(D_S)^{\tilde{G_S}} \to \prod_{v \notin S, Nv \equiv 0,1(p), v \in \mathrm{Pl}_r(k)} H^1(I_v)^{H_v} \times \delta_{p,2}(\mathbb{Z}/2\mathbb{Z})^{r_1(k)}$, qui est donc bien une injection. □

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

Proposition II.2.13. *Si p est un nombre premier impair, alors pour chaque place v en dehors de S, l'inflation $H^2(H_v) \to H^2(G_v)$ est triviale.*

Démonstration. Si v est une place en dehors de $S \cup \mathrm{Pl}_p(k)$, alors le groupe H_v est isomorphe à $\mathbb{Z}_p$, donc est un pro-p-groupe libre, et donc $H^2(H_v)$ est trivial.
Pour $v \in \mathrm{Pl}_p(k) - S_p$, on remarque que le groupe de Galois de la pro-p-extension maximale $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$ est un pro-p-groupe libre qu'on note F. Alors, pour toute extension finie k_v de $\mathbb{Q}_p$, le pro-p-groupe de Galois absolu G_v au-dessus de k_v admet pour quotient $\mathrm{Gal}(\overline{\mathbb{Q}_p}.k_v/k_v)$, qui s'identifie à un sous-groupe ouvert de F. Par ailleurs le corps k_v^{cr} est compositum de k_v et $\mathbb{Q}_p^{cr}$, il est donc inclus dans le compositum $\overline{\mathbb{Q}_p}.k_v$, et ainsi, le groupe H_v est un quotient de $\mathrm{Gal}(\overline{\mathbb{Q}_p}.k_v/k_v)$. On a donc les inflations suivantes qui commutent :

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

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

□

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

Proposition II.2.14. *Si $p = 2$, pour chaque place v en dehors de $\mathrm{Pl}_2(k) \cup S$, en particulier les places réelles à l'infini, l'inflation $H^2(H_v) \to H^2(G_v)$ est triviale.*
Pour les places v au-dessus de 2, on considère un instant l'inflation

$$H^2(\mathrm{Gal}(K^{cr}/K)) \to H^2(\mathrm{Gal}(\overline{K}/K))$$

comme un objet purement local ; elle vérifie les propriétés suivantes dans une extension finie K/K_0 d'extensions finies de $\mathbb{Q}_2$:

1. *la trivialité et la non trivialité se propagent dans les extensions K/K_0 de degré impair.*
2. *la trivialité et la non trivialité se propagent dans les extensions K/K_0 contenues dans K^{cr}.*
3. *la trivialité se propage dans toutes les extensions K/K_0.*
4. *l'inflation est non triviale pour le corps $\mathbb{Q}_2$, et triviale pour les corps quadratiques $\mathbb{Q}_2(i)$ et $\mathbb{Q}_2(\sqrt{-2})$, et pour les autres corps quadratiques non inclus dans $\mathbb{Q}_2^{cr}$.*

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

Démonstration. On revient à la proposition. Le cas des places finies en dehors de $\mathrm{Pl}_2(k) \cup S$ se traite comme dans le cas p impair, et le cas des places réelles à l'infini provient de la trivialité de H_v.
Soit donc v une place au-dessus de 2. On oublie ici la situation globale sous-jacente pour se concentrer sur la situation locale. On dispose donc d'une extension finie $K = k_v/\mathbb{Q}_2$, et on note $H = H_v$, et $G = G_v$ les groupes intervenant dans l'inflation. On a le diagramme commutatif suivant :

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

Les deux suites horizontales définissent des formes bilinéaires non dégénérées, les groupes G et H étant des groupes de Demuchkin. On note (u_1^*, u_2^*) un système de générateurs de $H^1(H)$, qui correspond dans la théorie de Kummer à un système (u_1, u_2) de générateurs kummériens de la sous-extension 2-élémentaire maximale de K^{cr}/K. Un résultat sur le groupe de Demuchkin $H \simeq \mathbb{Z}_p^2$ (voir [24], proposition 3.9.13) montre alors que $u_1^* \cup u_2^*$ est non trivial, et est donc un générateur de $H^2(H)$. Il reste à considérer $\inf(u_1^* \cup u_2^*) = \inf(u_1^*) \cup \inf(u_2^*)$, élément du groupe $H^2(G)$. Il existe un isomorphisme canonique de ce groupe dans le groupe des racines 2-èmes de l'unité ([16], théorème 8.12), et l'élément du H^2 qui nous intéresse correspond au symbole de Hilbert local $(u_1, u_2)_2$ (en fait sa 2-partie). La trivialité de l'inflation est donc équivalente à la nullité de ce symbole.
On démontre maintenant les propriétés de propagation. Pour une extension finie K/K_0, on notera encore H et G les groupes correspondant à K, et H_0 et G_0, ceux correspondant à K_0.

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

G dans G_0. On considère alors le diagramme commutatif suivant d'inflations :

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

Il s'agit donc de démontrer que la flèche diagonale de gauche est un isomorphisme si et seulement si celle de droite en est un ; c'est-à-dire que la flèche horizontale est un isomorphisme. Les abélianisés des groupes G et G_0 s'écrivent $G^{ab} \simeq \mathbb{Z}/2^f\mathbb{Z} \oplus \mathbb{Z}_2^{d_0-1} \oplus \mathbb{Z}_2^{d-d_0}$ et $G_0^{ab} \simeq \mathbb{Z}/2^f\mathbb{Z} \oplus \mathbb{Z}_2^{d_0-1}$; en particulier, les $d - d_0$ dernières composantes de G^{ab} se trivialisent *via* la surjection sur G_0^{ab}, et les parties de torsion sont les mêmes puisqu'elles sont données par les 2-Sylow des groupes de racines de l'unité de K et K_0 respectivement, qui sont égaux puisque l'extension est supposée de degré impair. On considère $(\overline{y_i})_{i\leq d}$ un système de générateurs de G^{ab}, compatible avec l'isomorphisme précédent, qui s'envoie donc sur un système de générateurs $(\overline{x_i})$ de G_0^{ab}. En particulier, $\overline{x_i}$ est trivial pour $i > d_0$. On relève le premier en un système y_i de générateurs de G, dont on note l'image dans G_0 par x_i, et par commutativité, on en déduit que les x_i ont pour image les $\overline{x_i}$ dans G_0^{ab}. Ainsi, les systèmes $(x_i)_{i\leq d}$ puis $(x_i)_{i\leq d_0}$ (d'après, par exemple [34], proposition 25 de la partie I) sont générateurs de G_0. On considère les pro-p-groupes libres F et F_0 engendrés respectivement par $(y_i)_{i\leq d}$ et $(x_i)_{i\leq d_0}$; il existe une surjection entre eux compatible avec celle entre G et G_0, et on a donc obtenu des présentations de G et G_0 compatibles suivant le diagramme :

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

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

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

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

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

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

2. sous la condition que K est contenu dans K_0^{cr}, les groupes H et G sont des sous-groupes ouverts respectivement des groupes H_0 et G_0. Les corestrictions respectives entre les H^2 sont des isomorphismes, puisque tous ces groupes sont des groupes à dualité de Poincaré de dimension 2 (voir [34], chapitre 1, point (4) de la preuve de la proposition 30). La commutation entre corestriction et inflation permet de conclure.

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

On passe maintenant aux calculs explicites pour $\mathbb{Q}_2$, $\mathbb{Q}_2(i)$ et $\mathbb{Q}_2(\sqrt{-2})$. Une base de générateurs kummériens pour $\mathbb{Q}_2^{cr}/\mathbb{Q}_2$ est $(2,5)$. L'extension $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ est non ramifiée, et 2 est une uniformisante de $\mathbb{Q}_2$, donc le symbole d'Artin $\left(2, \mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2\right)$ est un générateur de son groupe de Galois, il agit non trivialement sur $\sqrt{5}$, ce qui montre que le symbole de Hilbert $(2,5)_2$ est non trivial, et donc la non trivialité de l'inflation considérée.
Pour $\mathbb{Q}_2(i)$, on a à nouveau le même système de générateurs kummériens. On passe par le corps global $\mathbb{Q}(i)$, et la formule du produit (voir [6], partie II, théorème 7.3) pour calculer le symbole de Hilbert. Toutes les places infinies sont complexes et les symboles correspondant sont triviaux, et en les places différentes de la place au-dessus de 2 et des deux places $(1+2i)$ et $(1-2i)$ au-dessus de 5, tant 2 que 5 sont des unités, et ont donc un symbole trivial modulo 2. En les deux places au-dessus de 5, les entiers 2 et 5 vus comme entiers 5-adiques donnent les mêmes extensions kummériennes $\mathbb{Q}_5(\sqrt[4]{2})$ et $\mathbb{Q}_5(\sqrt[4]{5})$; les deux symboles correspondant à ces deux places sont égaux, d'abord à une racine quatrième de l'unité, puis, en passant au carré puisqu'on s'intéresse au symbole modulo 2, leur produit est trivial. Par la formule du produit, on en déduit la trivialité du symbole $(2,5)_2 = (2,5)_{(1+i)}^2$, calculé dans $\mathbb{Q}_2(i)$.
Pour conclure en ce qui concerne le corps $\mathbb{Q}_2(\sqrt{-2})$, on suit la même démarche. La place 5 est cette fois-ci inerte dans $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$, et le calcul modulo cette place est trivial puisque $\sqrt{2} \in \mathbb{Q}_5(\sqrt{-2})$.
On a ainsi traité cinq extensions quadratiques de $\mathbb{Q}_2$: les trois incluses dans $\mathbb{Q}_2^{cr}$, et les deux ci-dessus. Pour les deux extensions restantes, $\mathbb{Q}_2(\sqrt{-5})$ et $\mathbb{Q}_2(\sqrt{6})$, on conclut de la façon suivante : on considère le compositum de $\mathbb{Q}_2(\sqrt{-5})$ avec $\mathbb{Q}_2(i)$; la trivialité de l'inflation dans $\mathbb{Q}_2(i)$ s'y propage puis redescend à $\mathbb{Q}_2(\sqrt{-5})$ puisqu'il s'agit d'une extension inerte de ce dernier corps, donc incluse dans $\mathbb{Q}_2(\sqrt{-5})^{cr}$; de même pour l'autre corps en prenant le compositum avec $\mathbb{Q}_2(\sqrt{-2})$.
Plus généralement pour toute extension abélienne de $\mathbb{Q}_2$, la valeur de l'inflation se lit dans la sous-pro-2-extension maximale ; cette inflation est triviale dès que l'extension contient une extension quadratique de $\mathbb{Q}_2$ dans laquelle l'inflation est triviale, et donc, d'après ce qui précède, dès qu'elle contient une extension quadratique qui n'est pas dans $\mathbb{Q}_2^{cr}$, et donc dès qu'elle n'est pas incluse dans ce corps. □

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

propriété d'exactitude, et dont les carrés sont commutatifs :

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

En oubliant la suite exacte du milieu, on obtient alors le diagramme commutatif suivant, où on introduit le noyau de Chafarevitch $Ш^2(\tilde{G}_S)$ comme noyau de la quatrième flèche verticale. L'injectivité de la flèche verticale de droite est un résultat classique ([16], théorème 11.1), et, dans le cas où k contient les racines p-èmes de l'unité cette injectivité est assurée en corestreignant la flèche à la somme directe à laquelle on a ôté un terme (*ibid*, théorème 11.2), ce qu'on souligne par la notation $\prod^*$; le noyau $Ш^{*2}(\tilde{G}_S)$ apparaissant dans le diagramme est donc *a priori* plus grand que le noyau de Chafarevitch introduit précédemment :

$$\begin{array}{ccccccccc}
 & & & & & & Ш^{*2}(\tilde{G}_S) & & 1 \\
 & & & & & & \downarrow & & \downarrow \\
H^1(\tilde{G}_S) & \hookrightarrow & H^1(\overline{G}) & \longrightarrow & H^1(D_S)^{\tilde{G}_S} & \longrightarrow & H^2(\tilde{G}_S) & \longrightarrow & H^2(\overline{G}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & \overset{\phi}{\searrow} & \downarrow \\
\prod^* H^1(H_v) & \hookrightarrow & \prod^* H^1(G_v) & \longrightarrow & \prod^* H^1(I_v)^{G_v} & \longrightarrow & \prod^* H^2(H_v) & \longrightarrow & \prod^* H^2(G_v)
\end{array}$$

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

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

et de s'assurer que le noyau $Ш^{*2}(\tilde{G}_S)$, et donc *a fortiori* le noyau de Chafarevitch $Ш^2(\tilde{G}_S)$, s'incluent dans le noyau de cette même inflation. La commutativité et la proposition II.2.13 montrent que l'image de ϕ est incluse dans le produit direct fini $\prod^*_{v\in S} H^2(G_v) \times \left(\prod_{v\in \mathrm{Pl}_2(k)-S_2} H^2(G_v)\right)^{\delta_{2,p}}$. On a donc :

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

On déduit maintenant du diagramme précédent un nouveau diagramme dont les suites horizontales ont trois termes. Puisque les groupes G_v et H_v considérés sont égaux en les places au-dessus de S, et en utilisant le lemme II.2.11, on vérifie facilement que le fait de considérer le terme $\ker\mathrm{inf}$ au lieu de $H^2(\tilde{G}_S)$ dans la suite horizontale supérieure permet de conserver l'exactitude du diagramme en ne considérant les suites locales qu'en des places en dehors de S. On utilise enfin les propositions

II.2.13 et II.2.14 pour simplifier à droite les suites locales.

$$\begin{array}{ccccccccc}
 & & & & 1 & & Ш^2(\tilde{G_S}) & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & H^1(\overline{G})/H^1(\tilde{G_S}) & \longrightarrow & H^1(D_S)^{\tilde{G_S}} & \longrightarrow & \ker\inf & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \prod_{v\notin S} H^1(G_v)/H^1(H_v) & \longrightarrow & \prod_{v\notin S} H^1(I_v)^{G_v} & \longrightarrow & \widehat{\prod_{v\notin S}} H^2(H_v) & \longrightarrow & 1
\end{array}$$

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

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

où chaque exposant α_v vaut 0 si l'inflation de la proposition II.2.14 est un isomorphisme, et vaut 1 si elle est triviale. Le lemme du serpent permet alors d'obtenir une injection du groupe de Chafarevitch dans le conoyau de la flèche verticale de gauche, qu'on note abusivement res :

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

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

$$\begin{array}{rl}
\dim_{\mathbb{F}_p} \ker\inf & \leq \dim_{\mathbb{F}_p}\mathrm{coker}(\mathrm{res}) + \widehat{\sum_{v\notin S}}\dim_{\mathbb{F}_p} H^2(H_v) \\
 & = \dim_{\mathbb{F}_p}\mathrm{coker}(\mathrm{res}) + \left\{ \begin{array}{ll} \#(\mathrm{Pl}_p(k) - S_p) & \text{si } p \neq 2 \\ \sum_{v\in \mathrm{Pl}_2(k)-S_2}(1-\epsilon_v) & \text{si } p = 2, \end{array} \right.
\end{array}$$

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

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

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

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

qui donne la suite exacte :

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

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

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

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

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

Justifions ceci : puisque le quotient $H_v = G_v/I_v$ est abélien, on a $I_v \supset [G_v, G_v]$, et puisqu'il est libre, on a $G_v^p \cap I_v = I_v^p$. On en déduit que le quotient $I_v/I_v^p[G_v, G_v]$ peut être vu comme un sous-groupe de $G_v/G_v^p[G_v, G_v]$, qui se trivialise dans H_v/H_v^p, et dont l'image dans $G_v/G_v^p[G_v, G_v]$ est la même que celle de $I_v/I_v^p[G_v, I_v]$, ce qui suffit pour écrire la seconde suite exacte. La première s'en déduit. La seconde suite exacte montre que le dual de $I_v/I_v^p[G_v, G_v]$ est bien $H^1(G_v)/H^1(H_v)$, et la suite duale de la première est donc bien celle attendue. Les propositions II.2.13 et II.2.14 fournissent alors par dualité des estimations de l'espace M_v, dans certains cas.
Le conoyau cherché est alors dual du noyau de la flèche χ_2 dans le diagramme ci-dessus. On utilise maintenant les isomorphismes de corps de classes. Le groupe $\overline{G}/\overline{G}^p[\overline{G}, \overline{G}]$ correspond par l'isomorphisme de corps de classes global à $\mathcal{J}_k/\mathcal{J}_k^p\mathcal{R}_k$, et chaque groupe $I_v/I_v^p[G_v, G_v]$ correspond à $\tilde{\mathcal{U}}_v/\tilde{\mathcal{U}}_v{}^p$. Le noyau de χ_2 est donc précisément $\tilde{\mathcal{U}}_{\overline{S}} \cap \mathcal{J}_k^p\mathcal{R}_k/\tilde{\mathcal{U}}_{\overline{S}}^p$, et fait l'objet du lemme :

Lemme II.2.15. *On a un isomorphisme :*

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

Démonstration. Soit $(a_v)^p r$ un élément de $\tilde{\mathcal{U}}_{\overline{S}} \cap \mathcal{J}_k^p\mathcal{R}_k$, avec $r \in \mathcal{R}_k$, et $(a_v) \in \mathcal{J}_k$. L'élément r est alors dans $\tilde{V}_S$. Si $(b_v)^p s$ est une autre écriture du même élément, on vérifie alors que r/s est un idèle principal qui est partout localement puissance p-ème, c'est donc une puissance p-ème d'un idèle principal : on a donc défini une flèche à valeur dans $\tilde{V}_S/\mathcal{R}_k^p$, qui est évidemment surjective.
Un élément dans le noyau est alors de la forme $r^p(a_v)^p$, sa composante en une place $v \notin S$ est donc dans $\tilde{\mathcal{U}}_v \cap \mathcal{K}_v^p$. Puisque le quotient $\mathcal{K}_v/\tilde{\mathcal{U}}_v$ est abélien libre (à 0, 1 ou 2 générateurs, suivant que v est réelle et $p = 2$, que v est finie et en dehors de $\mathrm{Pl}_p(k)$, ou que v est dans $\mathrm{Pl}_p(k)$), on en déduit que cette intersection est $\tilde{\mathcal{U}}_v{}^p$, ce qui conclut la démonstration. □

On a donc montré :

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

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

Enfin, on conclut cette partie en notant qu'il est possible de mener un calcul similaire en comparant, par la suite de Hoschschild-Serre, le groupe de Galois $\tilde{G}_S$ au groupe de Galois de la pro-p-extension $\mathrm{Pl}_p(k) \cup S$-ramifiée maximale $\tilde{L}_{\mathrm{Pl}_p(k)\cup S}(k)$, qui est de type fini, et dont on connaît exactement les nombres minimaux de générateurs et de relations. Les résultats obtenus par ce calcul sont légèrement plus faibles que ceux exposés ici, le problème majeur étant que le localisé du corps $\tilde{L}_{\mathrm{Pl}_p(k)\cup S}(k)$ en une

place v divisant p ne contient pas forcément le corps k_v^{cr}. Les théorèmes de Kuz'min (voir [24], théorème 10.6.4) et de Mukhamedov (voir [23]) donnent des conditions suffisantes pour qu'il en soit ainsi (corps global contenant les racines p-èmes de l'unité, ou corps CM, tel que toutes les places au-dessus de p sont décomposées depuis la sous-extension totalement réelle maximale). Ces théorèmes ont une portée plus générale, en cela qu'ils assurent que le localisé précédent contient toute la p-clôture algébrique du corps local k_v. On pose donc la question de savoir si des conditions plus faibles peuvent assurer que le corps k_v^{cr} soit contenu dans le localisé précédent.

II.2.3 Remarques supplémentaires

Avec une action galoisienne

On considère à nouveau une action d'un groupe de Galois $\Delta = \mathrm{Gal}(k/k_0)$, cette fois sur les divers groupes de cohomologie qui sont intervenus dans les calculs de la section précédente. On suppose que ce groupe a cardinal premier à p. On suppose aussi que l'ensemble fini S de places de k considéré est invariant sous l'action de Δ, c'est-à-dire que si une place w de k au-dessus d'une place v de k_0 est dans S, alors toutes les autres places de k au-dessus de v sont aussi dans S.
Il vient, du fait que les extensions de k considérées sont maximales pour certaines propriétés, que les extensions $L_S^\infty(k_\infty)/k_0$ et $\overline{k}/k_0$ sont galoisiennes ; notons les groupes de Galois $\overline{\mathcal{G}} = \mathrm{Gal}(\overline{k}/k_0)$ et $\mathcal{G} = \mathrm{Gal}(L_S^\infty(k_\infty)/k_0)$. Les restrictions induisent des extensions de groupes :

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

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

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

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

Les divers groupes de cohomologie étudiés dans la section précédente sont donc ainsi munis d'une structure de $\mathbb{F}_p[\Delta]$-modules. On considère leurs relevés en caractéristique zéro, pour obtenir une structure de $\mathbb{Z}_p[\Delta]$-module, qu'on tensorise ensuite par $\mathbb{C}_p$. Les caractères envisagés maintenant sont les caractères pour cette structure. L'hypothèse faite ici sur le cardinal du groupe Δ permet d'assurer que les Δ-modules considérés sont semi-simples (voir [35]).

Théorème II.2.16. *Soit p un nombre premier impair, k/k_0 une extension galoisienne de corps de nombres de degré premier à p, de groupe de Galois Δ, et $\tilde{G}_S$ le groupe de Galois de la pro-p-extension S-ramifiée maximale au-dessus de la $\mathbb{Z}_p$-extension cyclotomique de k, alors, les groupes de cohomologie de $\tilde{G}_S$ voient leurs caractères pour la structure de Δ-module vérifier :*

$$\chi(H^1(\tilde{G}_S)) = \chi(\tilde{V}_S/\mathcal{R}_k^p) + \sum_{v \in S(k_0)} \chi(\mu_p(k_v))^* + \sum_{v \in S_p(k_0)} [(k_0)_v : \mathbb{Q}_p]\chi(\mathrm{Reg}) +$$

$$+\sum_{v\in \mathrm{Pl}_p(k_0)-S_p(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} - \chi(\mu_p(k)) + \mathbf{1} - \sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1},$$

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

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

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

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

Démonstration. Les deux premiers points sont des corollaires des démonstrations des théorèmes II.2.2 et II.2.8, et des calculs de caractères effectués dans la partie 1 ; le troisième point s'en déduit immédiatement. On souligne en particulier la trivialité de l'action de Δ_v sur le groupe H_v de la démonstration du théorème II.2.8, et donc sur ses groupes de cohomologie, puisqu'il s'agit du groupe de Galois d'une extension qui provient par compositum d'une extension de $\mathbb{Q}_p$, et donc *a fortiori* de $(k_0)_v$. □

Exemple II.2.17. Soit $p \neq 2$ et k un corps CM contenant les racines p-èmes de l'unité, de sous-corps totalement réel maximal k^+, et S un ensemble de places finies de k^+. Alors :

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

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

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

$$\chi(\mu_p(k)) = \chi_c,$$

$$\sum_{v\in \mathrm{Pl}_\infty(k_0)} \mathrm{Ind}_{\Delta_v}^{\Delta}\mathbf{1} = r_1(k^+)\mathbf{1},$$

$$\sum_{v\in S_p(k^+)} [k_v^+ : \mathbb{Q}_p]\chi(\mathrm{Reg})) = \sum_{v\in S_p(k^+)} [k_v^+ : \mathbb{Q}_p](\mathbf{1} + \chi_c).$$

En remarquant la relation :

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

on trouve le résultat annoncé. □

Comportements asymptotiques

L'extension $L_S^\infty(k_\infty)^{ab}$ est une sous-extension de $L_S(k_\infty)$, la pro-p-extension abélienne S-ramifiée maximale de k_∞. La théorie d'Iwasawa munit le groupe de Galois $\mathrm{Gal}(L_S(k_\infty)/k_\infty)$ d'une structure de $\mathbb{Z}_p[[\Gamma]]$-module, où Γ désigne le groupe de Galois k_∞/k, ou encore de $\Lambda = \mathbb{Z}_p[[T]]$-module, *via* un isomorphisme qui fait correspondre à un progénérateur γ de Γ, le polynôme $T+1$; on notera alors $X_S(k_\infty) = \mathrm{Gal}(L_S(k_\infty)/k_\infty)$ ce groupe de Galois, pour faire ressortir sa structure de module d'Iwasawa. Il est pseudo-isomorphe à un module de la forme :

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

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

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

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

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

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

où le terme $O(1)$ est majoré par l'invariant λ du module d'Iwasawa $X_S(k_\infty)$.
On peut aussi considérer le nombre de générateurs des groupes $\tilde{G}_S(k_\infty)^{ab}$, en prenant les quotients p-élémentaires dans la suite exacte ci-dessus. Par le théorème II.2.2, en remarquant que les places finies sont finiment décomposées dans la $\mathbb{Z}_p$-extension cyclotomique, on obtient l'inégalité :

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

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

Puisque, si un corps k est CM, de sous-corps totalement réel k^+, les étages k_n de sa $\mathbb{Z}_p$-extension cyclotomique sont aussi des corps CM, de sous-corps totalement réel maximal k_n^+, on peut appliquer le corollaire II.1.10 à tous ces étages, et on trouve :

Corollaire II.2.18. *Si k est un corps CM de sous-corps totalement réel k^+, et S un ensemble de places au-dessus de p, alors :*

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

Démonstration. Le corollaire II.1.10 montre l'identité :

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

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

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

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

Chapitre III

On mild pro-p-groups as Galois groups over global fields

III.1 Maximal S-ramified T-split extensions of global fields

Let us assume that k is a number field or a function field over a finite field of characteristic different from p (with $p \neq 2$ in the number field case). We are interested in the Galois group of the maximal T-split, S-ramified, pro-p-extension of the field k, which we denote by G_S^T. In particular, we are interested in the local-global principle for its second cohomology group. The only places that can be ramified in a pro-p-extension are the ones with residue class field of characteristic p (in the number field case) or with residue class field which contains primitive p-th roots of unity. We assume throughout this chapter that S only contains such places. We first investigate the link between groups $V_S^T/\mathcal{R}^p$ (see the definition below), which we call Kummer group, and the group $H^2(G_S^T, \mathbb{F}_p)$ (we use the notation $H^2(G_S^T)$ for it). Presentation of this topic can be found in the appendix of [6] and in part four of [19], but these two references do not treat explicitly the question of the local-global principle (though they give many other statements we do not recover). We thus give here proofs of some well-known facts, based on the knowledge of the classical case where T is empty, as it can be found, for instance, in [16] or [24].

Let us recall the following definition :

Définition III.1.1. *For T and S disjoint finite sets of non-archimedian places of the field k, let V_S^T be :*

$$V_S^T = \mathcal{R} \cap \mathcal{J}^p \mathcal{U}_{\overline{S \cup T}} \mathcal{K}_T.$$

These groups increase with T and decrease with S. In the cases where S (respectively T) is empty, we denote $V_\emptyset^T$ by V^T (respectively $V_S^\emptyset = V_S$).

Note that another definition is sometimes used in the literature ([6], chapter I, theorem 4.6), where elements of V_S^T are asked to be prime to S. In the case where S is empty, the following lemma, which is an immediate generalisation of a very classical lemma on $V/\mathcal{R}^p$, is useful in dealing with $V^T/\mathcal{R}_k^p$. Note that the map from $V^T/\mathcal{R}^p$ to $(A/D_T)[p]$ is given as follows : let $\alpha = uj^p$ be an element of V^T, with $u \in \mathcal{U}_{\overline{S \cup T}} \mathcal{K}_T$, and $j \in \mathcal{J}_k$. Its image in A/D_T is defined as the class of the divisor $\sum_{v \notin T} v(j)v$ (it depends only on α and not on the choice of j and u).

Lemma III.1.1. *For each finite set T of non-archimedian places, there exists a short exact sequence :*

$$1 \to \mathcal{E}^T/(\mathcal{E}^T)^p \to V^T/\mathcal{R}^p \to (A/D_T)[p] \to 1,$$

so that the following identity holds :

$$\dim_{\mathbb{F}_p} V^T/\mathcal{R}^p = d(G^T) + r + \#T - 1 + \delta(k).$$

We are now in position to state the following proposition, which extends exact sequence (11.11) in [16] :

Proposition III.1.2. *There is a natural exact sequence :*

$$1 \to V_S/\mathcal{R}^p \to V_S^T/\mathcal{R}^p \to \mathcal{U}_{\overline{S\cup T}}\mathcal{K}_T/(\mathcal{U}_{\overline{S\cup T}}\mathcal{K}_T)^p\mathcal{U}_{\overline{S}} \to (G_S)^{ab}/p \to (G_S^T)^{ab}/p \to 1.$$

Its central term is isomorphic to $\mathcal{K}_T/\mathcal{K}_T^p\mathcal{U}_T \simeq \mathbb{F}_p^{\#T}$. And another exact sequence :

$$1 \to V_S^T/\mathcal{R}^p \to V^T/\mathcal{R}^p \to \mathcal{U}_{\overline{T}}\mathcal{K}_T/(\mathcal{U}_{\overline{T}}\mathcal{K}_T)^p\mathcal{U}_{\overline{S\cup T}}\mathcal{K}_T \to (G_S^T)^{ab}/p \to (G^T)^{ab}/p \to 1,$$

whose central term is isomorphic to $\mathcal{U}_S/\mathcal{U}_S^p$.

It admits as a corollary Shafarevich formulas (see again [6], chapter I, theorem 4.6) :

Corollary III.1.3. *The number of generators of the groups G_S^T, G_S and G^T are linked by the following formulas :*

$$d(G_S^T) = d(G_S) - \#T + \dim_{\mathbb{F}_p} V_S^T/\mathcal{R}^p - \dim_{\mathbb{F}_p} V_S/\mathcal{R}^p,$$

$$d(G_S^T) = d(G^T) + \sum_{v\in S}\delta(k_v) + \sum_{v\in S,\chi(v)=p}[k_v:\mathbb{Q}_p] - \dim_{\mathbb{F}_p} V^T/\mathcal{R}^p + \dim_{\mathbb{F}_p} V_S^T/\mathcal{R}^p.$$

And there is an identity :

$$d(G_S^T) = \sum_{v\in S}\delta(k_v) + \sum_{v\in S,\chi(v)=p}[k_v:\mathbb{Q}_p] + \dim_{\mathbb{F}_p} V_S^T/\mathcal{R}^p - r - \delta(k) + 1 - \#T.$$

Remark III.1.4. *In the function field case, since the characteristic is assumed to be different from p, the terms $[k_v:\mathbb{Q}_p]$ do not appear.*

In order to have information on the relation modules of the groups G_S^T, we rephrase the proofs on G_S in our more general context. We introduce some pieces of notation. We assume that for each place v of k, one place above v has been chosen in the maximal pro-p-extension of k :

- $\overline{G}$ the Galois group of the maximal pro-p-extension of k,
- D_S^T the normal subgroup of $\overline{G}$ which corresponds to the maximal T-split S-ramified subextension,
- $\overline{G_v}$ the Galois group of the maximal pro-p-extension of the local field k_v,
- G_v the decomposition subgroup of G_S^T at the place v,
- H_v for a place v in T, the trivial group, for v in S, the group $\overline{G_v}$, and for other non-archimedian places, the Galois group of the unramified $\mathbb{Z}_p$-extension of k_v (in each case H_v admits G_v as a quotient group),
- I_v the normal subgroup of $\overline{G_v}$ such that the quotient $\overline{G_v}/I_v$ is H_v.

The group D_S^T is topologically and normally generated by the subgroups $\overline{G_v}$, for v in T, and by (quotients of) I_v, for v in $\overline{S \cup T}$, so there is an epimorphism :

$$\prod_{v \in T} \overline{G_v}/\overline{G_v}^p[\overline{G_v}, \overline{G_v}] \prod_{v \notin S \cup T} I_v/I_v^p[I_v, \overline{G_v}] \twoheadrightarrow D_S^T/(D_S^T)^p[D_S^T, \overline{G}].$$

After dualizing, we obtain the injectivity of the middle vertical map in the following commutative diagram with exact rows and columns, in which we introduce the Shafarevich kernel $Ш^2(G_S^T)$:

$$\begin{array}{ccccccc}
 & & 1 & & Ш^2(G_S^T) & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
H^1(\overline{G})/H^1(G_S^T) & \hookrightarrow & H^1(D_S^T)^{\overline{G}} & \longrightarrow & H^2(G_S^T) & \longrightarrow & H^2(\overline{G}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\prod H^1(\overline{G_v})/\prod_{v \notin T} H^1(H_v) & \hookrightarrow & \prod_{v \in T} H^1(\overline{G_v}) \prod_{v \notin T \cup S} H^1(I_v)^{\overline{G_v}} & \longrightarrow & \prod_{v \in S} H^2(H_v) & \longrightarrow & \prod H^2(\overline{G_v})
\end{array}$$

In this diagram, horizontal arrows come from Hochschild-Serre exact sequences, vertical arrows are localization maps. The injectivity of the last vertical map is a well-known fact (see [16], theorems 11.1 and 11.2, for example). Moreover, one factor can be removed if the field k contains p-th roots of unity, and if S is not empty (the last of the two previous conditions ensures that the middle map is still a monomorphism). It follows that the Shafarevich kernel injects into the kernel of the inflation $H^2(G_S^T) \to H^2(\overline{G})$. The snake lemma then gives the existence of a monomorphism from this Shafarevich kernel to the cokernel of the first vertical map, and this cokernel is easily checked to be isomorphic to the dual of the group $V_S^T/\mathcal{R}^p$. Thus, we obtain :

Proposition III.1.5. *There exists a monomorphism from the Shafarevich kernel for the local-global principle on the cohomology group $H^2(G_S^T)$ into the dual of the group $V_S^T/\mathcal{R}^p$.*

Corollary III.1.6. *There is the following inequality on the number of relations of the group G_S^T :*

$$r(G_S^T) \leq \dim_{\mathbb{F}_p} V_S^T/\mathcal{R}^p + \sum_{v \in S} \delta(k_v) - \delta(k) + \theta,$$

where θ is 1 if $\delta(k) = 1$ and S is empty, and is 0 otherwise. Moreover, the partial Euler characteristic satisfies :

$$\chi_2(G_S^T) \leq \#T + \theta + r - \sum_{v \in S, \chi(v) = p} [k_v : \mathbb{Q}_p].$$

Remark III.1.7. *If one is only interested in finding an upper bound for $r(G_S^T)$ (or for $\chi_2(G_S^T)$), a more direct proof can be obtained by looking at the Hochschild-Serre exact sequence deduced from the surjection $G_S \twoheadrightarrow G_S^T$, but such a proof does not give a convenient information on the Shafarevich kernel. These bounds are given in [6], appendix, corollary 3.7.2.*

We are mainly interested in the cases where the local-global principle holds, i.e., the cases where the Shafarevich kernel is trivial. A good way to ensure this is to have the triviality of the group $V_S^T/\mathcal{R}^p$. If S and T are both empty, the only cases are those of $\mathbb{Q}$ and imaginary quadratic fields with class number not divisible by p (and, if $p = 3$ different from $\mathbb{Q}(\sqrt{-3})$, as can be seen by III.1.1). Some other cases can be found with T empty, and S big enough, depending on the field ; of particular interest are the so-called p-rational number fields for which $V_S/\mathcal{R}^p$ is trivial as soon as S contains $\mathrm{Pl}_p(k)$ (see [6], part IV, theorem 3.5). From now on, we will look for such cases with T non-empty, separately for function fields and number fields.

III.2 The function field case

III.2.1 Results

We first state the following proposition :

Proposition III.2.1. *As soon as T is non-empty, the group G_S^T satisfies the FAB property, i.e., each of its open subgroups has finite abelianization. If k contains p-th roots of unity, assume that S is not empty. If T contains exactly one place, then :*

$$d(G_S^T) = r(G_S^T).$$

Proof. Putting one place in T kills the unique $\mathbb{Z}_p$-extension. The finiteness of the abelianization of G_S^T implies the inequality $r(G_S^T) \geq d(G_S^T)$. If, moreover, T has cardinality 1, the converse inequality follows from corollary III.1.6. □

Now we state a corollary of lemma III.1.1 and corollary III.1.3 :

Corollary III.2.2. *Assume that the set T contains exactly one place such that the group A/D_T is trivial. If the field k does not contain p-th roots of unity, then the group $V^T/\mathcal{R}^p$ is trivial. If k contains p-th roots of unity, the same conclusion holds for $V_S^T/\mathcal{R}^p$, as long as there is at least one place v in S such that $\mu_p(k_v) = \mu_p(k)$. In both cases, the number of generators of G_S^T is :*

$$d(G_S^T) = \#S - \delta(k).$$

Proof. Since A/D_T is trivial, lemma III.1.1 implies that the group $V^T/\mathcal{R}^p$ is isomorphic to $\mathcal{E}^T/(\mathcal{E}^T)^p$. The fact that T contains only one place, together with the product formula, implies that the group $\mathcal{E}^T$ is equal to the group of p-power order roots of unity. Hence, the group $V^T/\mathcal{R}^p$ is a cyclic group of order $\delta(k)$, and is generated by the image of any root of unity of maximal p-power order. Such an element cannot be contained in any group V_S^T, for S non-empty, so that the conclusion on the groups V_S^T holds. Then, the assertion on $d(G_S^T)$ is a consequence of corollary III.1.3. □

We summarize our results in the function field case in the theorem :

Theorem III.2.3. *Let p be a prime number, and let k be a function field over a finite field of characteristic different from p. Let T be a set containing exactly one place of k such that the group A/D_T is trivial. Let S be a finite set of places $\{v_1, \ldots, v_d\}$, and assume that for each place v_i the local field k_{v_i} contains p-th roots of unity.*

1. *If the field k does not contain p-th roots of unity then the group G_S^T admits the following minimal presentation (of Koch type) :*

$$< \alpha_1, \ldots, \alpha_d | \alpha_i^{N(v_i)-1} \prod_{j \neq i} [\alpha_j, \alpha_i]^{l_{ij}} \bmod [F, F^p[F,F]] / i = 1, \ldots, d > .$$

In that presentation, F is the free pro-p-group on the α_i's, α_i is an image in G_S^T of a generator of the procyclic group $\mathrm{Gal}(\overline{k_{v_i}}/k_{v_i}^{ur})$, and the exponents $l_{ij} \in \mathbb{Z}/p\mathbb{Z}$ are defined by the relation :

$$\pi_i \equiv \prod_j \alpha_j^{l_{ij}} \bmod (G_S^T)_2,$$

where π_i is the image in G_S^T of a lift in $\mathrm{Gal}(\overline{k_{v_i}}/k_{v_i})$ of the Frobenius automorphism of the procyclic group $\mathrm{Gal}(k_v^{ur}/k_v)$.

2. *If the field k contains a primitive p-th root of unity, and if S contains at least one place v such that $\mu_p(k_v) = \mu_p(k)$, then one generator and the corresponding relation can be omitted.*

Moreover, the exponents l_{ij} can be explicitly computed in the way described in the proof.

Proof. For each place $v \in S$, it is known that the group $\overline{G_v}$ admits the following presentation :

$$< \alpha_v, \pi_v | \alpha_v^{Nv-1} [\alpha_v^{-1}, \pi_v^{-1}] > .$$

We denote again by α_v and π_v the images of those elements in the quotient G_v of $\overline{G_v}$ so that these elements can be seen in G_S^T. The comparison between G_S^T and G^T (see proposition III.1.2), the latter group being trivial under our hypotheses (see the proof of corollary III.2.2), shows that the elements α_v, for v in S, give a system of generators of the group G_S^T. If $\delta(k) = 0$, this system is minimal according to the formula for $d(G_S^T)$. Again by proposition III.1.2, if $\delta(k) = 1$, these generators (which correspond to primitive p-power roots of unity in completions in k at the places in S) admit a relation $\prod_v \alpha_v^{b_v} = 1 \bmod (G_S^T)_2$, coming from a root of unity in k which generates $V^T/\mathcal{R}^p$. Moreover, one of the b_i's must be invertible modulo p, according to the assumption on S. Hence, one of the generators must be removed to get a minimal system. Assume that a numbering $\{v_1, \ldots, v_d\}$ of the places in S has been chosen. Then, there exist exponents l_{ij} in $\mathbb{Z}/p\mathbb{Z}$ such that :

$$\pi_i \equiv \prod_j \alpha_j^{l_{ij}} \bmod (G_S^T)_2.$$

More precisely, the triviality of (the abelianization of) G^T implies for each i the existence of some principal idele r_i, and some idele $u_i \in \mathcal{U}_{\overline{T}} \mathcal{K}_T$, such that $\pi_i = r_i u_i$. Thus we have $\pi_i \equiv u_i \bmod (G_S^T)^p [G_S^T, G_S^T]$. In the case where the place v_i is given by a principal ideal, the idele r_i can be chosen as a generator of this ideal. As an idele in $\mathcal{J}$, the component of π_i at a place v_j, for j different from i, is trivial, hence that of u_i is $\frac{1}{r_i}$. By class field theory, the generator α_j gives a generator $\overline{\alpha_j}$ of $\mathcal{U}_{v_j}$, and so there exists an exponent $l_{ij} \in \mathbb{Z}/p\mathbb{Z}$ such that $\frac{1}{r_i} = \overline{\alpha_j}^{l_{ij}} \bmod \mathcal{U}_{v_j}^p$. In order to compute these exponents l_{ij}, the generators α_j need only to be known in $\mathcal{U}_{v_j}/\mathcal{U}_{v_j}^p$.

Then, according to corollary III.2.2, the group $V_S^T/\mathcal{R}_k^p$ is trivial, and according to proposition III.1.5 so is the Shafarevich kernel $Ш^2(G_S^T)$. It follows that (see for example [16], theorem 6.14) the local relations between the α_i's and the π_i's give rise to a system of generators of the relations module of the group G_S^T (i.e. the normal subgroup generated by these elements is precisely the kernel of the natural map from the free pro-p-group F on the α_i's to G_S^T), and, more precisely, a minimal system of relations, according to the expression for $r(G_S^T)$. We remove the relation which corresponds to the omitted generator in the case $\delta(k) = 1$. Since, for each pro-p-group G, the commutator bracket defines a bilinear map :

$$[-,-] : G/G_2 \times G/G_2 \to G_2/G_3,$$

we have found a presentation of the group G_S^T :

$$< \alpha_1, \ldots, \alpha_d | \alpha_i^{N(v_i)-1} \prod_{j \neq i} [\alpha_j, \alpha_i]^{l_{ij}} \bmod F_3 / i = 1, \ldots, d > .$$

□

III.2.2 Examples

Example III.2.4. Here is a sample computation of exponents l_{ij}, independent from our general framework on mild and Koch type pro-p-groups. We consider a function field $\mathbb{F}_\ell(X)$, for a prime number ℓ, two prime ideals in $\mathbb{F}_\ell[X]$ generated respectively by the polynomials $X + a$ and $X + b$, and α a generator of the multiplicative group $\mathbb{F}_\ell^\times$. Then there exists some integer r such that $\frac{1}{X+a} \equiv \alpha^r \bmod X + b$. It can be checked that $\frac{1}{X+b} \equiv \alpha^{r+\frac{\ell-1}{2}} \bmod X + a$. For any odd prime number p dividing $\ell - 1$, we thus obtain exponents l modulo p :

$$l_{ab} = l_{ba} = r.$$

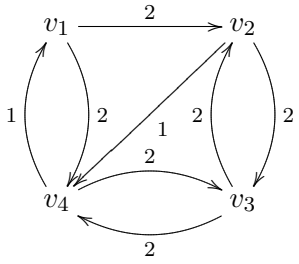
Example III.2.5. We now give an example of a mild pro-p-group obtained by application of theorems III.2.3 and I.1.7. Let $p = 3$, k be the field $\mathbb{F}_5(X)$, and the sets of places T and S be respectively $T = \{X\}$ and $S = \{X^2 + 3, X^2 + 2X + 3, X^2 + 2, X^2 + X + 2\}$. Note that the residue class field of k at any of the places in S is $\mathbb{F}_{25}$, which contains primitive third root of unity. We can choose as generators (the α's) of the unit groups of the localisation of k in the places of S the classes of $X+2$, X, $X+1$ and X, respectively. We draw the following array, which summarizes congruences needed to compute the l_{ij} :

	v_1	v_2	v_3	v_4
$\frac{1}{X^2+3}$		X^{17}	$(X+1)^{24}$	X^2
$\frac{1}{X^2+2X+3}$	$(X+2)^3$		$(X+1)^2$	X^7
$\frac{1}{X^2+2}$	$(X+2)^{12}$	X^2		X^{11}
$\frac{1}{X^2+X+2}$	$(X+2)^{10}$	X^9	$(X+1)^{11}$	

For instance, in the main box, the entry X^{17} is to be read as : $\frac{1}{X^2+3} \equiv X^{17} \bmod v_2$. Taking these powers modulo 3 yields the following identities :

$$l_{24} = l_{41} = 1,\ l_{12} = l_{14} = l_{23} = l_{32} = l_{34} = l_{43} = 2,$$

and all the other l_{ij} are zero. We thus have the following linking diagram, where the vertices are the v_i's, and an arrow is drawn from v_i to v_j if and only if l_{ij} is non-trivial in $\mathbb{Z}/3\mathbb{Z}$; we label such an arrow by the value l_{ij} :



The vertices v_1, v_2, v_3, and v_4 in this numbering then form a non-singular circuit, and theorem I.1.7 can be applied.

III.3 The number field case

III.3.1 Results

In the number field case, it is well-known (lemma III.1.1) that the group $V/\mathcal{R}^p$ cannot be trivial apart from the case of the field of rational numbers and some imaginary quadratic fields. A fortiori, the same holds for the groups $V^T/\mathcal{R}^p$. We thus seek examples with a set S containing enough places above p. The following proposition gives a general sufficient condition for $V^T_{S_p}/\mathcal{R}^p$ to be trivial. This sufficient condition is stated under two equivalent forms : the first is the easiest to check numerically, the second is the closest to the hypotheses of theorem 2.4 in Wingberg's paper [44].

Proposition III.3.1. *Assume that the group G^T is trivial. Then, the two following sets of conditions are equivalent :*

1. *the localisation map at S_p is a monomorphism from $\mathcal{E}^T$ to $\mathcal{U}_{S_p}$, and $\phi_{S_p}(\mathcal{E}^T)$ is a direct factor in $\mathcal{U}_{S_p}$.*
2. *the two following identities hold :*

$$\mathrm{rk}_{\mathbb{Z}_p}(G^T_{S_p})^{ab} = \sum_{v\in S_p}[k_v:\mathbb{Q}_p] - r + 1 - \#T,$$

$$\dim_{\mathbb{F}_p}\left(\mathrm{Tor}_{\mathbb{Z}_p}(G^T_{S_p})^{ab}\right) = \sum_{v\in S_p}\delta(k_v) - \delta(k).$$

Under these conditions, the group $V^T_{S_p}/\mathcal{R}^p$ is trivial. If, moreover, the localisation map of condition (1) is an isomorphism (which is equivalent to the triviality of the group $G^T_{S_p}$) then we have :

$$d(G^T_S) = r(G^T_S) = \sum_{v\in S}\delta(k_v) - \delta(k) = \sum_{v\in S-S_p}\delta(k_v) = \#(S - S_p).$$

Proof. By class field theory, the kernel of the surjection from $(G_{S_p}^T)^{ab}$ to $(G^T)^{ab}$ is isomorphic to $\mathcal{U}_{S_p}/\phi_{S_p}(\mathcal{E}^T)$. If condition (1) holds, then :

$$\mathrm{rk}_{\mathbb{Z}_p}\left(\mathcal{U}_{S_p}/\phi_{S_p}(\mathcal{E}^T)\right) = \mathrm{rk}_{\mathbb{Z}_p}\mathcal{U}_{S_p} - \mathrm{rk}_{\mathbb{Z}_p}\phi_{S_p}(\mathcal{E}^T) = \sum_{v\in S_p}[k_v:\mathbb{Q}_p] - r + 1 - \#T,$$

and the torsion subgroup of the latter group is $\prod_{v\in S_p}\mu_p(k_v)/\mu_p(k)$, whose number of generator is $\sum_{v\in S_p}\delta(k_v) - \delta(k)$. Hence, condition (1) implies condition (2). The converse implication follows from the same isomorphism. First note that the expression of the $\mathbb{Z}_p$-rank of $(G_{S_p}^T)^{ab}$ implies that ϕ_{S_p} is a monomorphism from the $\mathbb{Z}_p$-free part of $\mathcal{E}^T$, hence from $\mathcal{E}^T$ itself (since the torsion part is given by roots of unity). Then the expression of the dimension of the torsion part implies the remaining statement. The equivalence between the triviality of $G_{S_p}^T$ and the fact that ϕ_{S_p} is an isomorphism is shown by the same way.
Now, assume that these equivalent conditions hold and consider the exact sequence from proposition III.1.2 :

$$1 \to V_{S_p}^T/\mathcal{R}^p \to V^T/\mathcal{R}^p \to \mathcal{U}_{S_p}/p \to (G_{S_p}^T)^{ab}/p \to (G^T)^{ab}/p \to 1.$$

Under our hypotheses, the fifth term is trivial, and the second term is isomorphic to $\mathcal{E}^T/(\mathcal{E}^T)^p$, according to lemma III.1.1. Then, the second map is a quotient map of ϕ_{S_p}, and condition (1) shows that this quotient map is a monomorphism, hence that $V_{S_p}^T/\mathcal{R}^p$ is trivial.
The expression for $d(G_S^T)$ then follows from corollary III.1.3. The corollary III.1.6 gives one inequality on $r(G_S^T)$. The reverse inequality is obtained by noting that the group G_S^T has finite abelianization : the kernel of the surjection from $(G_S^T)^{ab}$ to $(G^T)^{ab}$ is isomorphic to $\mathcal{U}_S/\phi_S(\mathcal{E}^T)$ by class field theory. Since ϕ_{S_p} is an isomorphism from $\mathcal{E}^T$ to $\mathcal{U}_{S_p}$, the latter group is isomorphic to a quotient of $\prod_{v\in S-S_p}\mathcal{U}_v$, hence is finite. □

Remark III.3.2. *The two equivalent conditions of the proposition, with the further condition $\sum_{v\in S_p}\delta(k_v) = \delta(k)$ imply the freeness of $G_{S_p}^T$ (on $\sum_{v\in S_p}[k_v:\mathbb{Q}_p] - r + 1 - \#T$ generators) according to proposition III.1.5. These conditions imply in particular the S_p-rationality of the number field k, according to Jaulent and Sauzet (see [13]).*

Remark III.3.3. *Given a number field k, sets of places S and T such that the localisation map ϕ_{S_p} from the proposition is an isomorphism, we obtain further examples of groups for which a local-global principle hold by enlarging the set S or by removing places from T. In particular, if in our setting we have $\#T = 1$, we recover Vogel-like examples ([42], Definition 2.1) by taking $T = \emptyset$, provided that p does not divide the class number of k. However, note that the argument which gives the exact value of $r(G_S^T)$ is no longer valid. More precisely, removing one place from T increases the $\mathbb{Z}_p$-rank of $(G_S^T)^{ab}$ by 1.*

We now give some converse statement.

Proposition III.3.4. *Assume that G^T is trivial. If the group $V_{S_p}^T/\mathcal{R}^p$ is trivial and $\sum_{v\in S_p}\delta(k_v) = \delta(k)$, then the map ϕ_{S_p} from $\mathcal{E}^T$ to $\mathcal{U}_{S_p}$ is a monomorphism, and the image of $\mathcal{E}^T$ under this map is a direct factor in $\mathcal{U}_{S_p}$.*

Proof. We consider again the exact sequence from proposition III.1.2 :

$$1 \to V_{S_p}^T/\mathcal{R}^p \to V^T/\mathcal{R}^p \to \mathcal{U}_{S_p}/p \to (G_{S_p}^T)^{ab}/p \to (G^T)^{ab}/p \to 1.$$

Under our hypotheses, the first and fifth terms are trivial, and the second term is isomorphic to $\mathcal{E}^T/(\mathcal{E}^T)^p$. Therefore the second map is a monomorphism from that group to $\mathcal{U}_{S_p}/p$. It is a quotient map of ϕ_{S_p}, and we denote it by $\overline{\phi_{S_p}}$. The additional hypothesis ensures that ϕ_{S_p} is an isomorphism between torsion parts. It follows that none of the elements of the $\mathbb{Z}_p$-free part (we assume that a section has been chosen in $\mathcal{E}^T$) of $\mathcal{E}^T$ can be sent in the torsion part of $\mathcal{U}_{S_p}$. Together with the injectivity of $\overline{\phi_{S_p}}$, it suffices to ensure that ϕ_{S_p} itself is a monomorphism. Again by the injectivity of $\overline{\phi_{S_p}}$, the last statement holds. □

We summarize our results in the number field case :

Theorem III.3.5. *Let p be an odd prime number, and let k be a number field. Let S be a finite set of non-archimedian places in k such that $\sum_{v\in S_p}[k_v : \mathbb{Q}_p] \geq r-1$, and let T be a finite set of non-archimedian places of k such that the group G^T is trivial and the localisation map at S_p is an isomorphism from $\mathcal{E}^T$ to $\mathcal{U}_{S_p}$. Assume that the d non-p-places $\{v_1,\dots,v_d\}$ in S are such that each k_{v_i} contains p-th roots of unity. Then the group G_S^T admits the presentation given in Theorem III.2.3 (there is no special case if k contains p-th roots of unity).*

The proof follows the same pattern as that of theorem III.2.3. The main difference is that a comparison between G_S^T and $G_{S_p}^T$ must be used instead that between G_S^T and G^T. We omit the proof.

III.3.2 Examples

Example III.3.6. Let $k=\mathbb{Q}$, let $p=3$, $T=\{5\}$, and $S=\{3,7,13,79,97\}$. We choose as generators of the groups, $\mathcal{U}_7$, $\mathcal{U}_{13}$, $\mathcal{U}_{79}$ and $\mathcal{U}_{97}$: $\alpha_7=3$, $\alpha_{13}=2$, $\alpha_{79}=3$ and $\alpha_{97}=5$. We summarize the congruences needed to compute the l_{ij} in the following array :

	7	13	79	97
$\frac{1}{7}$		2	3^{25}	5^{65}
$\frac{1}{13}$	3^3		3^{44}	5^{71}
$\frac{1}{79}$	3^4	1		5^{66}
$\frac{1}{97}$	3^3	2^7	3^{72}	

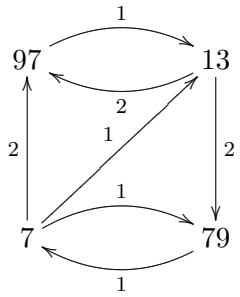
The coefficient 3^3 in the main box is, for instance, to be read as $\frac{1}{13} \equiv 3^3 \bmod 7$. Taking the powers in the array modulo 3 yields the following identities :

$$l_{13,7} = l_{97,7} = l_{79,13} = l_{97,79} = l_{79,97} = 0,$$

$$l_{79,7} = l_{7,13} = l_{97,13} = l_{7,79} = 1,$$

$$l_{13,79} = l_{7,97} = l_{13,97} = 2.$$

We thus have the following linking diagram, with the non-singular circuit $\{97, 13, 79, 7\}$; hence theorem I.1.7 can be applied :



Example III.3.7. We consider the prime number $p = 5$, and the field $k = \mathbb{Q}(z)$, where z is a primitive fifth root of unity. The field k is a totally imaginary ($r = r_2 = 2$) 5-rational number field, with trivial class group. We let T be the set of ideals :

$$T = \{(z^2 + 3), (3z + 1), (23)\}.$$

It can be checked that the Hilbert ray class field attached to the modulus 5^2 contains the compositum of the cyclic 5-ramified 5-elementary extensions of k (this compositum has Galois group over k isomorphic to $(\mathbb{Z}/5\mathbb{Z})^3$), and that its maximal T-split subextension is trivial for this choice of T. The set T thus satisfies the hypotheses of proposition III.3.1 and of theorem III.3.5.
We let S be the set :

$$S = \{(z-1), v_1 = (z^3-z^2-2), v_2 = (z^3-z^2-z), v_3 = (-2z+1), v_4 = (-z^3-2z-1)\}.$$

The first place $(z - 1)$ is of course the unique place above 5 in $k = \mathbb{Q}(z)$. This example has been computed so as to have small residue class fields at the places v_i, i.e., they are above prime numbers which are totally split in k. The norm of the place v_1 (respectively v_2, v_3 and v_4) is 41 (respectively 11, 31 and 11), and we choose 6 (respectively 2, 3 and 2) as a generator of the multiplicative group of its residue class field. As in the example above, the following array gives congruences from which exponents l_{ij} are computed :

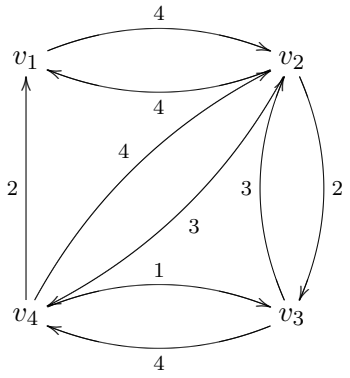
	v_1	v_2	v_3	v_4
$\frac{1}{z^3-z^2-2}$		2^9	3^{20}	2^5
$\frac{1}{z^3-z^2-z}$	6^{39}		3^7	2^3
$\frac{1}{-2z+1}$	6^{10}	2^8		2^9
$\frac{1}{-z^3-2z-1}$	6^{12}	2^9	3^{16}	

We thus get exponents l_{ij} by taking the powers in the array modulo 5 :

$$l_{31} = l_{13} = l_{14} = 0,\ l_{43} = 1,\ l_{41} = l_{23} = 2,$$

$$l_{32} = l_{24} = 3,\ l_{21} = l_{12} = l_{42} = l_{34} = 4.$$

Then the linking diagram for G_S^T is :



The vertices v_1, v_2, v_3, v_4 form a non-singular circuit, and theorem I.1.7 can be applied.

Example III.3.8. The last example is a mixed case, with decomposition. We take $k = \mathbb{Q}(\sqrt[3]{2})$. The numbers of archimedian places are $r_1 = r_2 = 1$ ($r = 2$), and the class number is 1. A fundamental unit of k is $\sqrt[3]{2} - 1$. The prime $p = 31$ is totally split in this field, and we consider two of the ideals above it, namely I_1 and I_2, which are generated respectively by $x_1 = (\sqrt[3]{2})^2 + 2\sqrt[3]{2} - 1$ and $x_2 = -2(\sqrt[3]{2})^2 + 1$. We assume that the set T contains only the unique ideal above 3 in k, which is generated by $\sqrt[3]{2} + 1$:

$$T = \{(\sqrt[3]{2} + 1)\}.$$

Hence, the group $\mathcal{E}^T$ is generated by :

$$\mathcal{E}^T =< \sqrt[3]{2} - 1, \sqrt[3]{2} + 1 > .$$

The logarithms of the 31-adic expansions of $\sqrt[3]{2}+1$ are $3*31+O(31^2)$ and $30*31+O(31^2)$ respectively in k_{I_1} and k_{I_2}. Those of $\sqrt[3]{2}-1$ are $5*31+O(31^2)$, $17*31+O(31^2)$. As the determinant $3 \cdot 17 - 5 \cdot 30 = -99$ is invertible modulo 31 the conditions of proposition III.3.1 are fulfilled.
We put four additional places in S :

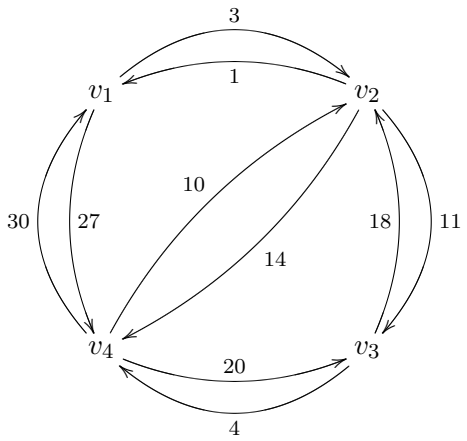
$$S = \{I_1, I_2, v_1 = (67), v_2 = (2(\sqrt[3]{2})^2 - 7), v_3 = (211), v_4 = (14(\sqrt[3]{2})^2 + 8\sqrt[3]{2} + 49)\}.$$

The places v_2 and v_4 are above the prime 311. We take as generators of the residue class fields :

$$\alpha_1 = \sqrt[3]{2} + 9, \alpha_2 = 17, \alpha_3 = \sqrt[3]{2} + 1, \alpha_4 = \sqrt[3]{2} + 1.$$

We do not give the full array of congruences as in the previous examples, since the

exponents involved are bigger. The linking diagram is :



The congruence $3 \cdot 11 \cdot 4 \cdot 30 - 1 \cdot 18 \cdot 20 \cdot 27 \equiv 6 \mod 31$ shows that the vertices v_1, v_2, v_3, v_4 form a non-singular circuit.

Chapitre IV

On maximal tamely ramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field

This chapter is divided in three sections. The first one is devoted to fixing notations and recalling some useful known results. In the second section we extend results of Ferrero and Kida to find S-ramified Iwasawa module $X_S(k_\infty)$ over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field k. The description depends on the S-ramified Iwasawa module over $\mathbb{B}_\infty$, the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. We are not able to give the general description of that module, but we exhibit a few infinite families of sets S for which it is trivial or cyclic of small order. A fact to be noticed is that $X_S(k_\infty)$ can have non-trivial torsion part even if 2 does not ramify in $k/\mathbb{Q}$. Using Mizusawa's method we finally prove the main Theorem IV.3.1 in section 3. Note that it deals with Galois groups whose abelianizations are $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, hence with $\lambda = 1$. We do not consider the cases where $\lambda = 2$. As an application of this result, we compute Galois groups of the maximal S-ramified pro-2-extension over the layers k_n of the cyclotomic $\mathbb{Z}_2$-extension of k, i.e. the S-ray 2-class field tower of k_n(Theorems IV.3.9 and IV.3.12). These results and their proofs are again inspired by Mizusawa's paper : see Proposition 4.3 in [21].

IV.1 Preliminaries.

IV.1.1 Notations

Let S and D be two finite sets of odd prime numbers in $\mathbb{Q}$. We will mainly consider the imaginary quadratic field $k = \mathbb{Q}(\sqrt{-\prod_{p_i \in D} p_i})$ and various extensions of it. For each number field K, we denote by $S(K)$ the set of places in K which are above places in S. When no confusion is possible, we will omit K.
For any place v in K, let $\mathfrak{k}_v^\times$ be the 2-adification of the multiplicative group of the residue class field of K at the place v (i.e., the 2-Sylow, since it is a cyclic group).
The notation $\mathcal{C}\ell(K)$, or simply $\mathcal{C}\ell$, stands for the ideal class group in the number field K, and $\mathcal{C}\ell_{\mathcal{M}}$ for the ray class group associated to the modulus $\mathcal{M}$. All the class

groups that we consider are taken in the ordinary sense which means that archimedean places do not complexify in the corresponding class field extensions.
Let $\mathcal{M}$ be a modulus which support is included in $S(K)$ for some K. In particular, if $\mathcal{M}_0 = \prod_{v\in S} \mathfrak{p}_v$, and if $\mathcal{M}$ is such that $\mathcal{M}_0|\mathcal{M}$, then the 2-Sylow of the ray class groups are such that $A_{\mathcal{M}} = A_{\mathcal{M}_0}$ (see Proposition IV.1.2 below). In such a situation, we omit the modulus and denote by A_S that 2-Sylow. In particular, A is the 2-Sylow of $\mathcal{C}\ell$.
D_S denotes the subgroup of A_S generated by the places above 2. When S is empty, we omit the subscript (no confusion with the discriminant of the quadratic number field seems possible). Then A'_S is the quotient group A_S/D_S (it corresponds via class field theory to the maximal 2-split S-ramified abelian 2-extension).
Following [43], section 7.3, we write $\mathbb{B}_n$ for the n-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, and K_n its compositum with any number field K. Taking inverse limits of various class groups according to norm maps from K_m to K_n for $m \geq n$, we obtain the so-called Iwasawa modules. For instance : $X(K_\infty) = \varprojlim A(K_n)$, $X'(K_\infty) = \varprojlim A'(K_n)$, $X_S(K_\infty) = \varprojlim A_S(K_n)$ and $X'_S(K_\infty) = \varprojlim A'_S(K_n)$, $\varprojlim D(K_n)$ and $\varprojlim D_S(K_n)$. Note that in general the Iwasawa module depends on the first layer of the $\mathbb{Z}_p$-extension we consider, and not only on K_∞. However, in our examples, they will be independent, and thus our notation will fit.
The notation E stands for the group of (global) units, $E_{\mathcal{M}}$ for the subgroup of units which are congruent to 1 modulo $\mathcal{M}$. Similarly, E' denotes the group of 2-units and $E'_{\mathcal{M}}$ the subgroup of 2-units which are congruent to 1 modulo $\mathcal{M}$. Then we define $\mathcal{E} = E \otimes_{\mathbb{Z}} \mathbb{Z}_2$ and $\mathcal{E}' = E' \otimes_{\mathbb{Z}} \mathbb{Z}_2$. Since the set S contains only finite non-2-places, we can define $\mathcal{E}_S$ as $E_{\mathcal{M}} \otimes_{\mathbb{Z}} \mathbb{Z}_2$ for any modulus $\mathcal{M}$ built on S and divisible by $\prod_{v\in S} \mathfrak{p}_v$ (see Proposition IV.1.2 below). The same holds for $\mathcal{E}'_S$.
Let T be either the empty set or the set of places above 2. We use T as a superscript for unit groups and class groups : for instance $\mathcal{E}_S^T$, A_S^T denote either $\mathcal{E}_S$ and A_S, or $\mathcal{E}'_S$ and A'_S, according whether T is the empty set or the set of places above 2.

IV.1.2 Some known results.

Let us recall without proof some classical results which will be used several times. First, we state a well-known result from Iwasawa theory, which is a special case of Nakayama's lemma (see for example [4], Theorem 1).

Lemma IV.1.1. *Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension of the number field K. Assume that all prime above p in K are totally ramified in K_∞/K. Let S be a finite set of finite primes in K, which are not above p. Take T to be either the empty set or* $\mathrm{Pl}_p(k)$.
If $A_S^T(K_n) = A_S^T(K_{n+1})$ for some layer K_n, then $X_S^T(K_\infty) = A_S^T(K_n)$.
Assume moreover that there is only one prime above p in K. Then $X_S^T(K_\infty)$ is trivial if and only if $A_S^T(K)$ is trivial.

The following statement is a 2-adification of Theorem 4.5 in part I of [6]. It will be used to compute S-ramified Iwasawa modules from unramified ones.

Proposition IV.1.2. *Let K be a number field. Let T be either the empty set or the set of places above 2. We recall that $\mathfrak{k}_v^\times$ denotes the 2-adification of the multiplicative*

group of the residue class field of K at the place v. Then, there is an exact sequence :

$$1 \longrightarrow \mathcal{E}^T/\mathcal{E}_S^T(K) \longrightarrow \prod_{v\in S(K)} \mathfrak{k}_v^\times \longrightarrow \ker(A_S^T(K) \to A^T(K)) \longrightarrow 1.$$

It yields the following equality :

$$\#A_S^T(K) = \#A^T(K)\frac{{}_2\phi(\mathcal{M})}{[\mathcal{E}^T : \mathcal{E}_S^T]},$$

where ${}_2\phi$ denotes the 2-part of the generalized Euler function, and $\mathcal{M}$ is any modulus whose support is S and divisible by $\mathcal{M}_0 = \prod_{v\in S(K)} \mathfrak{p}_v$.

Now we recall (a form of) the so-called genus formula which gives some information on the class group in a field L depending on the class group of a subfield K, on ramification in L/K and on norms of units (see for instance [6], part IV, Theorems 4.2 and 4.4 for the related exact sequence, and the beginning of section 4 for a sample of references).

Proposition IV.1.3. *Let L/K be a cyclic 2-extension of number fields and denote by Δ the Galois group $\mathrm{Gal}(L/K)$. Assume that L/K is disjoint from the S-ray 2-class field of K. Take T to be either the empty set or the set of places above 2. Then we have :*

$$\#A_S^T(L)^\Delta = \#A_S(K)\frac{\prod_{v\notin S\cup T} e_v \prod_{v\in T} e_v f_v}{2[\mathcal{E}_S^T(K) : \mathcal{E}_T^S(K)\cap N(\mathcal{J}_L)]},$$

where e_v and f_v denote respectively the ramification index and the inertia degree of the place v in L/K.

We will mainly use this formula in conjonction with the following well-known lemma :

Lemma IV.1.4. *With the notations of Proposition IV.1.3, assume moreover that $A_S^T(K)$ is trivial. Then, the cardinality of $A_S^T(L)^\Delta$ equals the number of generators of $A_S^T(L)$.*

Proof. Note that the non-trivial element σ of Δ acts by inversion on $A_S^T(L)$. Indeed, for each $\mathfrak{a}$, $\mathfrak{a}^{\sigma+1}$ can be seen as an element of $A_S^T(K)$, which is trivial by assumption. So $\mathfrak{a}^{\sigma+1}$ is in the same class as some principal ideal. The generator is still congruent to 1 modulo $S(L)$, hence $\mathfrak{a}^{\sigma+1}$ is trivial as well in $A_S^T(L)$. It implies that the Δ-invariants of the group $A_S^T(L)$ are exactly its elements of order lower than 2, and the result follows. □

Now we give a version of Hasse's theorem on units in CM-extensions (see [43], Theorem 4.12) for units and 2-units in layers of the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field :

Lemma IV.1.5. *Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, with $d \neq 1$ odd. Then the quotient group $\mathcal{E}(k_n)/\mathcal{E}(\mathbb{B}_n)$ is trivial. Moreover, if 2 does not split in $k/\mathbb{Q}$, the groups of 2-units $\mathcal{E}'(\mathbb{B}_n)$ and $\mathcal{E}'(k_n)$ are equal. If 2 splits in $k/\mathbb{Q}$, the quotient group $\mathcal{E}'(k_n)/\mathcal{E}'(\mathbb{B}_n)$ is infinite cyclic.*
If $k = \mathbb{Q}(i)$, then the quotient group $\mathcal{E}(k_n)/\mathcal{E}(\mathbb{B}_n)$ is cyclic of order 2^{n+1}, generated by a primitive 2^{n+2}-th root of unity, and the quotient group $\mathcal{E}'(k_n)/\mathcal{E}'(\mathbb{B}_n)$ is isomorphic to the direct product of $\mathcal{E}(k_n)/\mathcal{E}(\mathbb{B}_n)$ by a group of order 2.

Proof. See the proof of Theorem 5 in [2] if 2 ramifies in $k/\mathbb{Q}$ (the case where 2 is inert is essentially the same), and the proof of Theorem 6 if 2 splits.
For the case of $\mathbb{Q}(i)$ see for example Theorem 2 in [2] for the first assertion. The second one follows easily. □

The following lemma is an easy generalisation of a classical fact (see [43], Theorem 10.3 for instance) on capitulation in a CM-extension :

Lemma IV.1.6. *Let K be a CM-field, whose maximal real subfield we denote by K^+. Whenever S contains at least one finite place of K^+, not lying above 2, the (capitulation) kernel of the natural map $A_S(K^+) \to A_S(K)$ is trivial. If S is empty then this capitulation kernel has order 1 or 2.*
Moreover, if no place above 2 splits in K/K^+, then the same holds for $A'_S(K^+) \to A'_S(K)$.

Proof. The proof is as in the S-empty case in [43]. Let $\mathcal{M}$ be any modulus built on S divisible by at least one non-2-place of $S(K^+)$. We define $W_{\mathcal{M}}(K)$ as the set of roots of unity in K equivalent to $1 \bmod \mathcal{M}$, and $W_0(K)$ as the subset of roots of unity of the form $\sigma u/u$ where u is a unit in K, and σ denotes the non-trivial element of $\mathrm{Gal}(K/K^+)$. Let us consider the map

$$\mathrm{cap}(\mathcal{C}\ell_{\mathcal{M}}(K^+) \to \mathcal{C}\ell_{\mathcal{M}}(K)) \to W_{\mathcal{M}}(K)/W_0(K),$$

defined as follows : given an ideal $\mathfrak{a}$ of K^+, prime to S, which capitulates in $\mathcal{C}\ell_S(K)$, the image of this ideal is $\sigma\alpha/\alpha$, where $\mathfrak{a}\mathcal{O}_K = (\alpha)$. The congruence $\alpha \equiv 1 \bmod \mathcal{M}$ holds, and since S is a set of places in K^+, so does $\sigma\alpha \equiv 1 \bmod \mathcal{M}$. We deduce that $\sigma\alpha/\alpha \equiv 1 \bmod \mathcal{M}$. We can check that this element is indeed a root of unity, and that this map is injective, as in the S-empty case.
Then we notice that $W_0(K)$ contains $W_S(K)^2$, and that if S contains one finite place v lying above an odd prime p, the only roots of unity which can be equivalent to 1 modulo v are the p^n-th for $n \geq 0$, so that $W_{\mathcal{M}}(K) \subset \mu_{p^\infty}$, and the square map is an isomorphism in this group. Then the target of the previous map is trivial. Hence, for each modulus sufficiently large modulus $\mathcal{M}$, the natural map from $\mathcal{C}\ell_{\mathcal{M}}(K^+)$ is into $\mathcal{C}\ell_{\mathcal{M}}(K)$, so the same holds for $\mathcal{C}\ell_S(K^+) \to \mathcal{C}\ell_S(K)$, and for the 2-Sylow.
The same proof holds when dealing with $A'_S(K^+) \to A'_S(K)$, *mutatis mutandis.* □

IV.2 Computation of Iwasawa modules.

The main result of this section is the following :

Theorem IV.2.1. *Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. Let D be the set of prime numbers which divide d, and let S be a set of odd prime numbers in $\mathbb{Q}$. For any odd prime number p, let $2^{k'_p}$ be the largest 2-power dividing $p^2 - 1$. Take $T = \emptyset$ or $T = \mathrm{Pl}_2(k)$.*
Then the λ-invariant of the Iwasawa module $X_S^T(k_\infty)$ is :

$$\lambda_S^T(k_\infty) = \#(S \cup D)(\mathbb{B}_\infty) + \lambda_S^T(\mathbb{B}_\infty) - 1 - \delta,$$

where $\delta \in \{0,1,2\}$. More precisely, if $k = \mathbb{Q}(i)$ then $\delta = 1$, if $k \neq \mathbb{Q}(i)$, and $T = \emptyset$ or 2 does not split in $k/\mathbb{Q}$, then $\delta = 0$. In the remaining case (2 splits in $k/\mathbb{Q}$ and $T = \mathrm{Pl}_2(k)$) we only show $\delta \in \{1,2\}$ ($\delta = 1$ in the S-empty case). We recall that the number of places in $\mathbb{B}_\infty$ above an odd prime number $p \in S \cup D$ is $2^{k'_p - 3}$.
Moreover, the $\mathbb{Z}_2$-torsion part of $X_S^T(k_\infty)$ can be computed as

$$\mathrm{Tor}_{\mathbb{Z}_2} X_S^T(k_\infty) \simeq \mathrm{Tor}_{\mathbb{Z}_2} X_S^T(\mathbb{B}_\infty),$$

in the following cases : $k \neq \mathbb{Q}(i)$ and 2 inert in $k/\mathbb{Q}$, or 2 split in $k/\mathbb{Q}$ with $T = \emptyset$, or 2 ramified in $k/\mathbb{Q}$ with $T = \mathrm{Pl}_2(k)$.

Proof. We first recall the result of Ferrero and Kida (see [2] Theorems 4, 5, 6 and [14]), about the S-empty case :

$$\lambda^T(k_\infty) = \#D(\mathbb{B}_\infty) - 1 - \delta_2,$$

with $\delta_2 = 0$ apart from the case $T = \mathrm{Pl}_2(k)$, and 2 splits in $k/\mathbb{Q}$ where $\delta_2 = 1$.
We take n sufficiently large so that places in $S(\mathbb{B}_n)$ are either split or ramified in $k_n/\mathbb{B}_n$. We apply Proposition IV.1.2 for the fields $\mathbb{B}_n$ and k_n, and we find the following exact commutative diagram :

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \frac{\mathcal{E}^T(\mathbb{B}_n)}{\mathcal{E}_S^T(\mathbb{B}_n)} & \longrightarrow & \prod_{v\in S(\mathbb{B}_n)} \mathfrak{k}_v^\times & \longrightarrow & A_S^T(\mathbb{B}_n) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \phi_2} & & \\
1 & \longrightarrow & \frac{\mathcal{E}^T(k_n)}{\mathcal{E}_S^T(k_n)} & \longrightarrow & \prod_{v\in S(\mathbb{B}_n)} (\mathfrak{k}_v^\times)^{1+\delta_v} & \longrightarrow & \ker(A_S^T(k_n) \to A^T(k_n)) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \frac{\mathcal{E}^T(k_n)}{\mathcal{E}^T(\mathbb{B}_n)\mathcal{E}_S^T(k_n)} & \xrightarrow{\phi_1} & \prod_{v\in S(\mathbb{B}_n)} (\mathfrak{k}_v^\times)^{\delta_v} & \longrightarrow & \mathrm{coker}\phi_1 = \mathrm{coker}\phi_2 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

The injectivity of ϕ_2 comes from Lemma IV.1.6. The injectivity of ϕ_1 follows from the snake lemma. Here are some comments on the notations. The letter T must be replaced by $'$ or by the empty set. The quantity δ_v is 0 or 1 according whether the place v ramifies or splits in $k_n/\mathbb{B}_n$. The dependence on n has been omitted from the (2-adifications of) residue class fields, and from ϕ_1 and ϕ_2. The vertical map in the middle is a diagonal embedding at the places v which split in $k_n/\mathbb{B}_n$. The group in first row, third column is obtained from the general formula (which involves a kernel) because of the triviality of $A(\mathbb{B}_n)$.
Taking projective limit, we find first :

$$1 \to X_S^T(\mathbb{B}_\infty) \to \ker\left(X_S^T(k_\infty) \to X^T(k_\infty)\right) \to \varprojlim coker\phi_2 \to 1.$$

Then we see that there is an isomorphism of $\mathbb{Z}_2$-modules :

$$\varprojlim \prod_{v\in S(\mathbb{B}_n)} (\mathfrak{k}_v^\times)^{\delta_v} \simeq \mathbb{Z}_2^{\#S - D(\mathbb{B}_\infty)}.$$

Now, we compute $\varprojlim \frac{\mathcal{E}^T(k_n)}{\mathcal{E}^T(\mathbb{B}_n)\mathcal{E}_S^T(k_n)}$. It is free as a sub-$\mathbb{Z}_2$-module of a free $\mathbb{Z}_2$-module. If $k \neq \mathbb{Q}(i)$, and $T = \emptyset$ or 2 does not split in $k/\mathbb{Q}$, these groups are trivial by Lemma IV.1.5, hence the projective limit is trivial. If $T = \mathrm{Pl}_2(k)$ and 2 splits in $k/\mathbb{Q}$, the quotient group $\mathcal{E}'(k_n)/\mathcal{E}(\mathbb{B}_n)$ is infinite cyclic by the same lemma, hence the quotient group $\frac{\mathcal{E}'(k_n)}{\mathcal{E}'(\mathbb{B}_n)\mathcal{E}'_S(k_n)}$ is cyclic of rank at most 1, and the projective limit is either trivial or isomorphic to $\mathbb{Z}_2$.
Take now $k = \mathbb{Q}(i)$ and $T = \emptyset$. According to Lemma IV.1.5, the group $\mathcal{E}(\mathbb{B}_n(i))/\mathcal{E}(\mathbb{B}_n)$ is cyclic generated by a primitive 2^{n+2}-th root of unity ζ_n. We claim that the groups $\frac{\mathcal{E}(\mathbb{B}_n(i))}{\mathcal{E}(\mathbb{B}_n)\mathcal{E}_S(\mathbb{B}_n(i))}$ are non-trivial for n large enough (still assuming S non-empty). Assume the contrary. Then, we can write, for each n, $\zeta_n = \epsilon\epsilon_S$, with $\epsilon \in \mathcal{E}(\mathbb{B}_n)$ and $\epsilon_S \in \mathcal{E}$. Take n such that places in S are split in $\mathbb{B}_n(i)/\mathbb{B}_n$, and choose a place v in $S(\mathbb{B}_n)$, and places v_1 and v_2 above it in $\mathbb{B}_n(i)$. Hence, in the residue class fields $\mathfrak{b}_{v_1}$ and $\mathfrak{b}_{v_2}$ of $\mathbb{B}_n(i)$ at v_1 and v_2, we obtain $\bar{\zeta_n} = \bar{\epsilon}$. But $\bar{\epsilon}$ is already in the residue class field $\mathfrak{b}_v$ of $\mathbb{B}_n$ at v. Thanks to the equalities $\mathfrak{b}_v = \mathfrak{b}_{v_1} = \mathfrak{b}_{v_2}$, it follows that $\bar{\zeta_n}$ is the same in $\mathfrak{b}_{v_1}$ and in $\mathfrak{b}_{v_2}$ which is impossible. Therefore, the claim implies that the projective limit $\varprojlim \frac{\mathcal{E}(\mathbb{B}_n(i))}{\mathcal{E}(\mathbb{B}_n)\mathcal{E}_S(\mathbb{B}_n(i))}$ is isomorphic to $\mathbb{Z}_2$ by $\mathbb{Z}_2$-freeness.
Again for $k = \mathbb{Q}(i)$, take now T to be the set of places above 2. The quotient group $\mathcal{E}'(\mathbb{B}_n(i))/\mathcal{E}'(\mathbb{B}_n)$ is the direct product of the cyclic group $\mathcal{E}(\mathbb{B}_n(i))/\mathcal{E}(\mathbb{B}_n)$ with $\mathbb{Z}/2\mathbb{Z}$ according to Lemma IV.1.5. Hence, the quotient group $\frac{\mathcal{E}(\mathbb{B}_n(i))}{\mathcal{E}(\mathbb{B}_n)\mathcal{E}_S(\mathbb{B}_n(i))}$ has at most two generators. As above, we can prove the non-triviality of ζ_n in this quotient. Taking projective limit and using the argument of $\mathbb{Z}_2$-freeness, we conclude that the projective limit $\varprojlim \frac{\mathcal{E}(\mathbb{B}_n(i))}{\mathcal{E}(\mathbb{B}_n)\mathcal{E}_S(\mathbb{B}_n(i))}$ is isomorphic to $\mathbb{Z}_2$.
Thus we find an exact sequence of $\mathbb{Z}_2$-modules :

$$1 \to \mathbb{Z}_2^{\delta_1} \to \mathbb{Z}_2^{\#S-D(\mathbb{B}_\infty)} \to \varprojlim \mathrm{coker}\phi_1 \to 1,$$

with $\delta_1 \in \{0, 1\}$. More precisely, $\delta_1 = 0$ for $k \neq \mathbb{Q}(i)$ and $T = \emptyset$ or 2 not split in $k/\mathbb{Q}$, and $\delta_1 = 1$ for $k = \mathbb{Q}(i)$. Using this in the first exact sequence, we find :

$$\lambda_S^T(k_\infty) = \lambda^T(k_\infty) + \lambda_S^T(\mathbb{B}_\infty) + \#(S-D)(\mathbb{B}_\infty) - \delta_1.$$

The assertion about λ-invariants follows from this formula and the results of Ferrero and Kida that we have recalled.
Now we turn our attention to the torsion part. Whenever $\delta_1 = 0$ the projective limit $\varprojlim \mathrm{coker}\phi_1$ is free as a $\mathbb{Z}_2$-module. Hence the first exact sequence splits into a direct sum of $\mathbb{Z}_2$-modules :

$$\ker\left(X_S^T(k_\infty) \to X^T(k_\infty)\right) \simeq X_S^T(\mathbb{B}_\infty) \oplus \varprojlim \mathrm{coker}\phi_1.$$

Moreover by [2], Theorems 4, 6, if 2 does not ramify in $k/\mathbb{Q}$, the Iwasawa module $X^T(k_\infty)$ is $\mathbb{Z}_2$-free, whenever $T = \emptyset$ or $T = \mathrm{Pl}_2(k)$, and the same holds if 2 ramifies in $k/\mathbb{Q}$ with $T = \mathrm{Pl}_2(k)$. In those cases we find an isomorphism of $\mathbb{Z}_2$-modules :

$$X_S^T(k_\infty) \simeq X^T(k_\infty) \oplus X_S^T(\mathbb{B}_\infty) \oplus \varprojlim \mathrm{coker}\phi_1.$$

The assertion on torsion parts follows. □

The group $\varprojlim D_S(k_n)$ needs to be known, in particular when 2 ramifies in $k/\mathbb{Q}$.

Proposition IV.2.2. *Assume that S is non-empty and disjoint from D. Let c be such that $\varprojlim D_S(\mathbb{B}_n) \simeq \mathbb{Z}_2/2^c\mathbb{Z}_2$ (make the convention that $c = \infty$ if the group is isomorphic to $\mathbb{Z}_2$).*

- *If 2 is inert in $k/\mathbb{Q}$, then, $\varprojlim D_S(k_n) \simeq \mathbb{Z}_2/2^c\mathbb{Z}_2$.*
- *If 2 ramifies in $k/\mathbb{Q}$, then, $\varprojlim D_S(k_n) \simeq \mathbb{Z}_2/2^{c+1}\mathbb{Z}_2$ (apart from the case $D = S = \emptyset$).*
- *If c is finite and if 2 splits in $k/\mathbb{Q}$, then, $\varprojlim D_S(k_n) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2/2^c\mathbb{Z}_2$.*

Proof. First note that each $D_S(\mathbb{B}_n)$ is cyclic, generated by the unique ideal above 2 in $\mathbb{B}_n$. Hence, $\varprojlim D_S(\mathbb{B}_n)$ is procyclic.
The assumption on S implies that for each $x \equiv 1 \bmod \prod_{v\in S(\mathbb{B}_n)} \mathfrak{p}_v$, the congruence still holds in k_n : $x \equiv 1 \bmod \prod_{v\in S(k_n)} \mathfrak{p}_v$.
If 2 does not split in $k/\mathbb{Q}$, then $D_S(k_n)$ is cyclic for each n, generated by the unique ideal above 2 in k_n. If 2 is inert, we obtain $D_S(\mathbb{B}_n) = D_S(k_n)$ (using the remark above), while, if 2 is ramified, the ideal above 2 is not principal (see [2], Lemma 10, if $D \neq \emptyset$, and if $D = \emptyset$ replace the assertion by the fact that this ideal is generated by $1 - \zeta_n$, for ζ_n a primitive 2^{n+2}-root of unity, hence cannot be S-principal if $S \neq \emptyset$), and, for each n, the map of Lemma IV.1.6 induces an exact sequence :

$$1 \to D_S(\mathbb{B}_n) \to D_S(k_n) \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Taking the projective limit, we obtain the result in these cases.
If 2 splits in $k/\mathbb{Q}$, then $D_S(k_n)$ admits $D(k_n)$ as a quotient group. Since $\varprojlim D(k_n) \simeq \mathbb{Z}_2$ (see [2], Theorem 6), it follows that $\varprojlim D_S(k_n)$ admits $\mathbb{Z}_2$ as a quotient group, hence a direct summand. Moreover, each $D_S(k_n)$ is generated by the two ideals $\mathfrak{q}_n$ and $\mathfrak{q}'_n$ above 2 in k_n. Taking n sufficiently large, so that norm from $\varprojlim D_S(\mathbb{B}_m)$ to $D_S(\mathbb{B}_n)$ is an isomorphism, those ideals are linked by $(\mathfrak{q}_n\mathfrak{q}'_n)^{2^c} = 1$ in $A_S(k_n)$, where 2^c is the order of the ideal above 2 in $A_S(\mathbb{B}_n)$. Hence, for each n, the group $D_S(k_n)$ is a quotient group of $\mathbb{Z} \oplus \mathbb{Z}/2^c\mathbb{Z}$. Taking inverse limit, we obtain that $\varprojlim D_S(k_n)$ is isomorphic to some quotient of $\mathbb{Z}_2 \oplus \mathbb{Z}/2^c\mathbb{Z}$. Taking the inverse limit in Lemma IV.1.6, the group $\varprojlim D_S(\mathbb{B}_n) = \mathbb{Z}/2^c\mathbb{Z}$ is a subgroup of $\varprojlim D_S(k_n)$, and the proposition IV.2.2 follows. □

Corollary IV.2.3. *Assume that S is such that $X'_S(\mathbb{B}_\infty)$ is trivial and that 2 ramifies in $k/\mathbb{Q}$. Then :*

$$X_S(k_\infty) \simeq \mathbb{Z}_2^{\lambda_S} \oplus \mathrm{Tor},$$

with :

$$\lambda_S = -1 + \sum_{p\in S\cup D(\mathbb{Q})} 2^{k'_p-3},$$

and where the torsion part Tor *is a cyclic 2-group of order twice that of $\varprojlim D_S(\mathbb{B}_n)$ (which is given in Proposition IV.2.5).*

We are not able to compute $X_S(\mathbb{B}_\infty)$ in general. We will restrict ourselves to characterize the case when $X'_S(\mathbb{B}_\infty)$ is trivial in the following Proposition IV.2.4. Note

that much more general results of this kind have been obtained using Kummer theory (see [6], V, Theorem 2.4), from which our proposition can be deduced. However, we prefer to give an elementary proof in our situation.

Proposition IV.2.4. *Let S denote a finite set of odd prime numbers in $\mathbb{Q}$, and the set of places above it in each $\mathbb{B}_n$. The groups $A'_S(\mathbb{B}_n)$ are trivial in the following cases :*

- *S is empty.*
- *S is reduced to a single element p, with $p \neq 1 \bmod 8$.*
- *S contains two elements p_1, p_2 such that $p_2 \equiv 7 \bmod 8$ and $p_1 \equiv 3, 5 \bmod 8$ or $p_2 \equiv 3 \bmod 8$ and $p_1 \equiv 5 \bmod 8$.*

Proof. According to Lemma IV.1.1, we only have to give a characterization of the cases when the group $A'_S(\mathbb{Q})$ is trivial. We use Proposition IV.1.2. In this case, Euler function for the modulus $\mathcal{M}_0$ (using notations of the proposition) satisfies :

$$_2\phi(\mathcal{M}_0) = \prod_{p \in S} 2^{k_p} = 2^{\sum_{p \in S} k_p},$$

where 2^{k_p} denotes the greatest power of 2 dividing $p-1$. We then look at the quotient group $\mathcal{E}'/\mathcal{E}'_S$ which is seen as the subgroup generated by 2 and -1 in $\prod_{p \in S} \mathfrak{k}_p^\times$ (we recall that $\mathfrak{k}_p^\times$ is the 2-adification of the multiplicative group $\mathbb{F}_p^\times$, hence is a cyclic 2-group). In each $\mathfrak{k}_p^\times$, -1 is in the subgroup generated by 2 if and only if 2 is non-trivial. Denote its order by $o_p = 2^{a_p}$. In the product of the $\mathfrak{k}_p^\times$'s, -1 is in the subgroup generated by 2 if and only if all o_p's are equal and non-trivial. Let $\delta = 0$ if this occurs, and $\delta = 1$ if not, and take $e = 2^a$ the maximum of the o_p's (hence a is the maximum of the a_p's). Then, the order of 2 in $\mathcal{E}'/\mathcal{E}'_S$ is e, and the group $\mathcal{E}'/\mathcal{E}'_S$, generated by 2 and -1, has order $2^\delta e = 2^{\delta+a}$. Hence, we have :

$$\#A'_S(\mathbb{Q}) = 2^{\sum_{p \in S} k_p - a - \delta}.$$

It yields $\#A'_S(\mathbb{Q}) = 1$ if and only if $\sum_{p \in S} k_p = a + \delta$. For each $p \in S$, the integer $o_p = 2^{a_p}$ divides 2^{k_p}, hence $a_p \leq k_p$. One easily checks that the only cases where this equality can hold are (recall that we do not consider the case $S = \emptyset$) :

1. $S = \{p\}$, $k_p = a_p$ and (this is automatic in this case) $\delta = 0$.
2. $S = \{p\}$, $k_p = a_p + 1$ and $\delta = 1$.
3. $S = \{p_1, p_2\}$, $\delta = 1 = k_{p_2}$ and $k_{p_1} = a_{p_1}$ (making a convention on the numerotation of the two primes).

For the first case to hold, it is necessary and sufficient that 2 is not a square in $\mathbb{F}_p$, and we find that $p \equiv 3, 5 \bmod 8$ are convenient for it. To study the second case, first note that the inequality $a_p < k_p$ implies that 2 is a square in $\mathbb{F}_p$, so that $p \equiv 1, 7 \bmod 8$. If $p \equiv 7 \bmod 8$, then $k_p = 1$, $a_p = 0$ and $\delta = 1$, so that the required equality holds, whereas if $p \equiv 1 \bmod 8$, we have $k_p \geq 3$ and since either a_p or δ is trivial, the conditions cannot be fulfilled.
We end the proof by the last case. Firstly, the condition $k_{p_1} = a_{p_1}$ implies that 2 is not a square in $\mathbb{F}_{p_1}$, hence that $p_1 \equiv 3, 5 \bmod 8$. Secondly, the condition $k_{p_2} = 1$ reads as $p_2 \equiv 3, 7 \bmod 8$. As seen above, if $p_2 \equiv 7 \bmod 8$, then $a_{p_2} = 0$, hence $\delta = 1$. Thus, in all the cases with $p_1 \equiv 3, 5 \bmod 8$ and $p_2 \equiv 7 \bmod 8$ the conditions are fulfilled. We then focus on the case $p_2 \equiv 3 \bmod 8$ (for which $a_{p_2} = 1$). If $p_1 \equiv 5 \bmod 8$ then

$a_{p_1} = 2 \neq a_{p_1}$ and $\delta = 1$, so that the conditions are fulfilled, whereas if $p_1 \equiv 3 \bmod 8$, then $a_{p_1} = a_{p_2} = 1$ and the conditions are not fulfilled. □

Now, we compute the whole group $A_S(\mathbb{B}_n)$, assuming that S is such that $X'_S(\mathbb{B}_\infty)$ is trivial.

Proposition IV.2.5. *Assume that S is such that $X'_S(\mathbb{B}_\infty)$ is trivial. If S contains only one place p, and $p \equiv 3, 7 \bmod 8$ then $A_S(\mathbb{B}_n)$ is trivial for each n. If $p \equiv 5 \bmod 8$, then $A_S(\mathbb{B}_n)$ is cyclic of order 2 for each n. If S contains two places p_1 and p_2 which are respectively congruent to 3 and 7 modulo 8 then $A_S(\mathbb{B}_n)$ is cyclic of order 2 for each n, while, if p_1 and p_2 are respectively congruent to 3 and 5 or 5 and 7 modulo 8, then it is cyclic of order 4.*

Proof. First note that since the group $A'_S(\mathbb{B}_n)$ is trivial for each n under the assumptions on S, and since there is only one place above 2 in $\mathbb{B}_n$, then the group $A_S(\mathbb{B}_n) = D_S(\mathbb{B}_n)$ is cyclic for each n. To compute its cardinality, we consider the formula from Proposition IV.1.2. Since S is non-empty, the unit -1 cannot be in $E_{\mathcal{M}}$, so $[\mathcal{E} : \mathcal{E}_S] = 2$. The cardinality of ${}_2\phi(\mathcal{M}_0)$ is easily computed for each set S we consider, and the result of the proposition follows for $n = 0$. In particular, if $S = \{p\}$ with $p \equiv 3, 7 \bmod 8$, then $A_S(\mathbb{Q})$ is trivial, and so are the $A_S(\mathbb{B}_n)$'s for all n, according to Lemma IV.1.1.
For the remaining cases, we will show that $\#A_S(\mathbb{B}_1) = \#A_S(\mathbb{Q})$, in order to apply Lemma IV.1.1. The computations are therefore done in the first layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, namely $\mathbb{B}_1 = \mathbb{Q}(\sqrt{2})$. We apply Proposition IV.1.2 in that field. Assume first that $S = \{p\}$, with $p \equiv 5 \bmod 8$. We find ${}_2\phi(\mathcal{M}_0) = 8$. The group $E(\mathbb{B}_1)$ is generated by -1 and $1 - \sqrt{2}$, and the quotient group by $E_{\mathcal{M}}(\mathbb{B}_1)$ can be seen as a subgroup of the multiplicative group of the field $\mathbb{F}_{p^2}$. The greatest 2-power dividing the order of this latter group is 8. It suffices to show that $1 - \sqrt{2}$ admits a square root but not a fourth root in this group : it follows that the greatest power of 2 dividing its order is 4, so that the quotient group $E(\mathbb{B}_1)/E_{\mathcal{M}}(\mathbb{B}_1)$ is generated by $1 - \sqrt{2}$, and the 2-part of its order is 2, hence that the order of $A_S(\mathbb{B}_1)$ is 2, which concludes the proof according to Lemma IV.1.1. The square root of $1 - \sqrt{2}$ in $\mathbb{F}_{p^2}$ is $-\frac{1}{\sqrt{1+i}} + \frac{\sqrt{1+i}}{2}\sqrt{2}$, where i is the primitive fourth root of unity in $\mathbb{F}_p$ such that $2i$ has odd order (ensuring that the square root of $1+i$ exists in $\mathbb{F}_p$). A square root $a + b\sqrt{2}$ (with $a, b \in \mathbb{F}_p$) of that element would be such that :

$$\begin{cases} a^2 + 2b^2 = -\frac{1}{\sqrt{1+i}} \\ 2ab = \frac{\sqrt{1+i}}{2}. \end{cases}$$

These equations lead to :

$$b^4 + \frac{b^2}{2\sqrt{1+i}} + \frac{1+i}{32}.$$

The discriminant of the underlying quadratic equation is $\frac{1}{2}(\frac{1-i}{2})^2$. Since 2 is not a square in $\mathbb{F}_p$, and solutions are seeked in $\mathbb{F}_p$, we are done.
Now, assume that $S(\mathbb{Q})$ contains two primes p_1 and p_2. The following table gives the values of the quantities that appear in the formula for $A_S(\mathbb{B}_1)$, in the three cases for the congruence of p_1 and p_2 modulo 8. The proposition follows from the cardinalities

of the groups in the first and in the last columns, and from Lemma IV.1.1. The two columns in the middle give the 2-part of the quotient group of the units by the units which are congruent to 1 modulo, respectively, the primes above p_1 and the primes above p_2. Proofs for the values in this table are to be found below :

$p_1, p_2 \bmod 8$	${}_2\phi(\mathcal{M})$	$\mathcal{E}/\mathcal{E}_{\{p_1\}}$	$\mathcal{E}/\mathcal{E}_{\{p_2\}}$	$\mathcal{E}/\mathcal{E}_S$
$3,5$	64	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
$3,7$	32	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
$5,7$	32	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

The values in the three first columns in the table are computed as follows : the first column is simply given by decomposition rules in $\mathbb{B}_1/\mathbb{Q}$; the cardinality of the groups in the second and third columns are consequences of the values found for $A_S(\mathbb{B}_1)$ when $S(\mathbb{Q})$ contains only one prime. Whenever the group is cyclic, it comes from the fact that it can be seen as a subgroup of the multiplicative group of some finite field (as above in the case $\#S = 1$ and $p \equiv 1 \bmod 8$) ; in that case, it is generated by the class of $1 - \sqrt{2}$. The last two entries in the third column ($p_2 \equiv 7 \bmod 8$) are deduced from the fact that the group is seen as a subgroup of $\mathbb{F}_{p_2}^\times \times \mathbb{F}_{p_2}^\times$, whose 2-part is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In each case, the group $E/E_{\mathcal{M}}$ admits both E/E_{p_1} and E/E_{p_2} as a quotient group. It is generated by $1 - \sqrt{2}$ and -1. Now, the order of $1 - \sqrt{2}$ is easily checked to be respectively 8, 8 and 4 in the three cases corresponding to the three lines in the table. Then the groups in the two last entries of the fourth column are deduced from the non-cyclicity in the third column. For the remaining entry (first line, fourth column), it only needs to be noticed that -1 cannot be in the subgroup generated by $1-\sqrt{2}$ because no odd power of $(1-\sqrt{2})^{2^k}$, for any k, can be congruent to -1 modulo both p_1 and p_2, since the groups in the second and third columns of the first line do not have the same order. □

Corollary IV.2.6. *The cases with S non-empty, disjoint from D, with $X'_S(\mathbb{B}_\infty)$ trivial and $\lambda_S(k_\infty) = 1$ are :*

- *$D = \{p\}$ with $p \equiv 3 \bmod 8$ and $S = \{q\}$ with $q \equiv 3 \bmod 8$. In this case $X_S(k_\infty) \simeq \mathbb{Z}_2$.*
- *$D = \{p\}$ with $p \equiv 5 \bmod 8$ and $S = \{q\}$ with $q \equiv 3 \bmod 8$. In this case $X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$.*
- *$D = \{p\}$ with $p \equiv 3 \bmod 8$ and $S = \{q\}$ with $q \equiv 5 \bmod 8$. In this case $X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$.*
- *$D = \{p\}$ with $p \equiv 5 \bmod 8$ and $S = \{q\}$ with $q \equiv 5 \bmod 8$. In this case $X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/4\mathbb{Z}$.*
- *$D = \emptyset$ and $S = \{q\}$ with $q \equiv 7 \bmod 16$. In this case $X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$.*
- *$D = \emptyset$ and $S = \{q_1, q_2\}$ with $q_1 \equiv 3 \bmod 8$ and $q_2 \equiv 5 \bmod 8$. In this case $X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/8\mathbb{Z}$.*

IV.3 Computations of Galois groups.

IV.3.1 Presentation of Galois groups over k_∞.

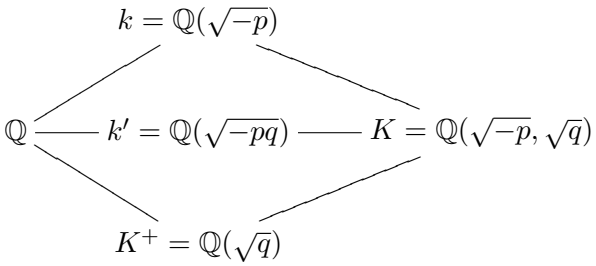
Our first aim will be to prove the following theorem.

Theorem IV.3.1. *Let p and q be two prime numbers respectively congruent to 5 and 3 modulo 8, and put $S = \{q\}$. Let k be the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$, and $\mathcal{G} = \mathrm{Gal}(L_S^\infty(k_\infty)/k_\infty)$ the Galois group of the maximal S-ramified pro-2-extension of k_∞. Then $\mathcal{G}$ has rank 2 and admits as a presentation :*

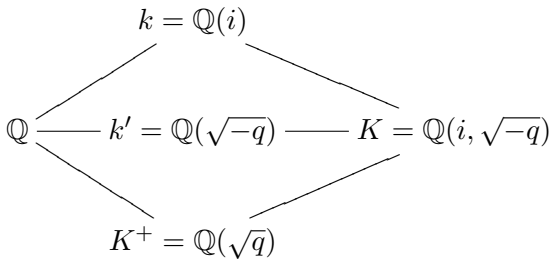
$$< a, b | [a, b]a^2 > .$$

The same holds if we assume $p \equiv 3 \bmod 8$ and $q \equiv 5 \bmod 8$, or if we take $k = \mathbb{Q}(i)$ and $q \equiv 7 \bmod 16$.

The proof is almost the same in the three cases. According to Corollary IV.2.6, the abelianization of $\mathcal{G}$ is $\mathcal{G}^{ab} = X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$. Moreover, the $\mathbb{Z}_2$-quotient of $X_S(k_\infty)$ is $X'_S(k_\infty)$. If $k = \mathbb{Q}(\sqrt{-p})$ and $S = \{q\}$ with $p, q \equiv 5, 3 \bmod 8$ or $p, q \equiv 3, 5 \bmod 8$, we introduce the following extensions :



In the case $k = \mathbb{Q}(i)$, with $S = \{q\}$ and $q \equiv 7 \bmod 16$, we put :



For each n, the extension K_n/k_n is S-ramified and 2-split. Hence, the extension K_∞/k_∞ is the subextension of $L'_S(k_\infty)$ fixed by the subgroup $2\mathbb{Z}_2$ of $X'_S(k_\infty)$. Since $L'_S(k_\infty)/k_\infty$ is procyclic, it is the maximal S-ramified 2-split pro-2-extension of k_∞. The equality $L'_S(k_\infty) = L'_S(K_\infty)$ follows, hence $X'_S(K_\infty) \simeq \mathbb{Z}_2$ as a $\mathbb{Z}_2$-module. Moreover, we have the proposition :

Proposition IV.3.2. *We have the equality $L'_S(K_\infty) = L'_S(k_\infty)$, and the S-ramified Iwasawa module over K_∞ satisfies $X_S(K_\infty) \simeq \mathbb{Z}_2^2$, where one direct summand is $X'_S(K_\infty)$.*

Proof. The first assertion has already been proved. Consider the exact sequences for all n :

$$1 \to D_S(K_n) \to A_S(K_n) \to A'_S(K_n) \to 1,$$

which give, by taking the projective limit :

$$1 \to \varprojlim D_S(K_n) \to X_S(K_\infty) \to X'_S(K_\infty) \to 1.$$

Since $X'_S(K_\infty)$ is free as a $\mathbb{Z}_2$-module, there is an isomorphism :

$$X_S(K_\infty) \simeq X'_S(K_\infty) \oplus \varprojlim D_S(K_n).$$

It remains to show that $\varprojlim D_S(K_n)$ is infinite and procyclic.
First we focus on the case $p \equiv 5 \bmod 8$ and $q \equiv 3 \bmod 8$. Consider the extension $k'_n/\mathbb{B}_n$. The prime 2 splits in this extension. Then, by the genus formula (Proposition IV.1.3), the group $A'_S(k'_n)$ is trivial for each n, hence $X_S(k'_\infty) = \varprojlim D_S(k'_n)$ holds. According to Proposition IV.2.2, the groups $D_S(k_n)$ are cyclic and their inverse limit is isomorphic to $\mathbb{Z}_2$. Then, the compositum $L_S(k'_\infty).K_\infty$ is an infinite procyclic S-ramified pro-2-extension of K_∞, and the two primes above 2 in K_∞ do not split in that extension. It is linearly disjoint from $L'_S(K_\infty)/K_\infty$.
Now, we apply Proposition IV.1.3 in the extension $K_n^+/\mathbb{B}_n$. The groups $A_S(\mathbb{B}_n)$ are trivial in this special case, and the only ramified place in $K_n^+/\mathbb{B}_n$ which is not in S is the place above 2. Hence, using Lemma IV.1.4, $A_S(K_n^+)$ is trivial. Let us write $\mathfrak{p}_{n,1}$ and $\mathfrak{p}_{n,2}$ for the places above 2 in K_n. The product $\mathfrak{p}_{n,1}\mathfrak{p}_{n,2}$ is trivial in $A_S(K_n^+)$, hence in $A_S(K_n)$ (the unique place in $S(K_n^+)$ is unramified in K_n/K_n^+, so any S-principal generator in K_n^+ is still S-principal in K_n). It follows that the subgroup $D_S(K_n)$ generated by the places above 2 is cyclic. Hence $\varprojlim D_S(K_n)$ is procyclic, and it is infinite because of the extension $L_S(k'_\infty).K_\infty/K_\infty$.
The proof in the case $k = \mathbb{Q}(i)$, $q \equiv 7 \bmod 16$ is just the same. In the case $p \equiv 3 \bmod 8$ and $q \equiv 5 \bmod 8$, some of the arguments need to be slightly adapted. The module $X_S(k'_\infty)$ is now isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$. In order to exhibit an infinite procyclic S-ramified 2-extension of K_∞ in which the primes above 2 do not split, one must replace $L_S(k'_\infty).K_\infty$ by the compositum of K_∞ with the unique infinite procyclic S-ramified pro-2-extension of k'_∞. The triviality of $A_S(K_n^+)$ comes from the fact that the field K_n^+ is the maximal S-ramified 2-extension of $\mathbb{B}_n$. □

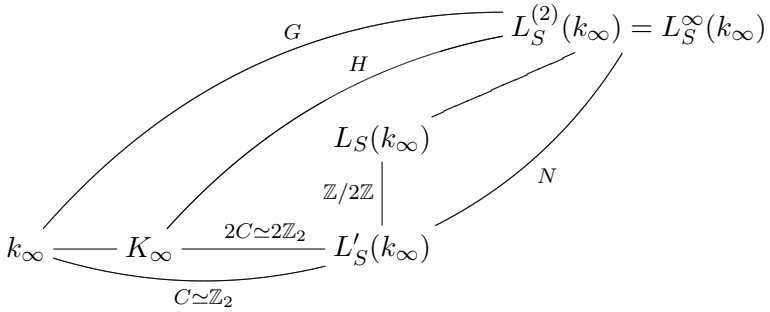
Let us now state a group theoretical proposition, whose proof can be found in [21], Section 3.2 (but the result is not explicitly stated there) :

Proposition IV.3.3. *Let G be a metabelian pro-2-group, whose abelianization G^{ab} is isomorphic to $C \oplus \mathbb{Z}/2\mathbb{Z}$, with $C \simeq \mathbb{Z}_2$. Denote by H the subgroup of G of index 2, such that $H/G_2 \simeq 2C \oplus \mathbb{Z}/2\mathbb{Z}$. If H has rank 2, then G is metacyclic. More precisely, there is a short exact sequence :*

$$1 \to N \to G \to C \to 1,$$

where N is a subgroup of H such that $H/N \simeq 2C$.

In our setting, the field extensions associated to these groups will be as follows :



We want to apply Proposition IV.3.3 to the maximal metabelian quotient $G = \mathrm{Gal}(L_S^{(2)}(k_\infty)/k_\infty)$ of the group $\mathcal{G} = \mathrm{Gal}(L_S^{\infty}(k_\infty)/k_\infty)$. We recall that there is an isomorphism $G^{ab} = \mathcal{G}^{ab} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, according to Corollary IV.2.6. Then, take $H = \mathrm{Gal}(L_S^{(2)}(k_\infty)/K_\infty)$, its abelianization is $\mathrm{Gal}(L_S(K_\infty)/K_\infty)$ which has rank 2 according to Proposition IV.3.2. Hence, the assumptions of Proposition IV.3.3 are satisified and $L_S^{(2)}(k_\infty)$ is a procyclic pro-2-extension of $L'_S(k_\infty)$. Since $L_S(K_\infty)$ is itself an infinite procyclic extension of $L'_S(k_\infty)$ (Proposition IV.3.2), we deduce the equality $L_S(K_\infty) = L_S^{(2)}(k_\infty)$. Finally, since $L_S^{(2)}(k_\infty)/L_S(k_\infty)$ is procyclic, we deduce that it is the maximal S-ramified pro-2-extension of k_∞, and that $\mathcal{G} = G$.
The group $\mathcal{G}$ is a pro-2-group of rank 2 whose abelianization is $X_S(k_\infty) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$. Let us denote by $a, b \in \mathcal{G}$ a system of representatives of generators of $X_S(k_\infty)$, such that $\bar{b} \in X_S(k_\infty)$ generates the summand $X'_S(k_\infty) \simeq \mathbb{Z}_2$, and $\bar{a}$ generates the summand $\mathbb{Z}/2\mathbb{Z}$. By restriction, the element $\bar{b}$ can be seen as a generator of the Galois group $\mathrm{Gal}(K_n/k_n)$ for each n, so it acts on the ideal $\mathfrak{p}_{n,1}$ by sending it on $\mathfrak{p}_{n,2}$ (these are the two ideals above 2 in K_n, according to the notations of Proposition IV.3.2). These ideals are each other inverses in $A_S(K_n)$, and generate $D_S(K_n)$, so $\bar{b}$ acts by inversion on $D_S(K_n)$. Taking the projective limit, we find that b acts by inversion on a. In the group $\mathcal{G}$ the following relation is satisfied :

$$[a, b]a^2 = 1.$$

The following lemma will enable us to prove that this is the only relation of the group $\mathcal{G}$:

Lemma IV.3.4. *Let $\mathcal{G}$ be a (pro-p-)group admitting as a system of generators a, b, and assume that these generators satisfy the relation $[a, b]a^2 = 1$. Then, the derived group $\mathcal{G}_2$ is included in the closed subgroup generated by a. It is in particular (pro)cyclic.*

Proof. By recursion on the minimal number of letters (among a, b, a^{-1} and b^{-1}) needed to write u, it is easily shown that each element of the form $u^{-1}au$ is in the closed subgroup generated by a. Therefore, this subgroup is normal. The derived group $\mathcal{G}_2$ is the smallest closed normal subgroup of $\mathcal{G}$ containing $[a, b]$, and that element is in the subgroup generated by a, hence the lemma follows. □

We are now in position to conclude the proof of Theorem IV.3.1. Let us denote by $\mathcal{F}$ the free pro-2-group on two generators a and b, and $\mathcal{R}$ its subgroup generated by $[a, b]a^2$. Its abelianization is easily seen to be isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$. There is a surjection $\mathcal{F}/\mathcal{R} \to \mathcal{G}$, and we deduce from it a commutative diagram :

$$\begin{array}{ccccccccc} 1 & \to & (\mathcal{F}/\mathcal{R})_2 & \to & \mathcal{F}/\mathcal{R} & \to & (\mathcal{F}/\mathcal{R})^{ab} & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathcal{G}_2 & \to & \mathcal{G} & \to & \mathcal{G}^{ab} & \to & 1 \end{array}$$

The third vertical arrow is a surjection, between two groups isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, hence it is an isomorphism. It follows that the first vertical arrow is also surjective. According to Lemma IV.3.4, and previous results on $\mathcal{G}$, the groups $(\mathcal{F}/\mathcal{R})_2$ and $\mathcal{G}$ are both procyclic, hence the first vertical arrow is an isomorphism. It follows that the map $\mathcal{F}/\mathcal{R} \to \mathcal{G}$ is actually an isomorphism, which finishes the proof of Theorem IV.3.1.

Corollary IV.3.5. *The cohomological dimension of $\mathcal{G}$ is 2. That of $\mathrm{Gal}(L_S^\infty(k_\infty)/k)$ is 3.*

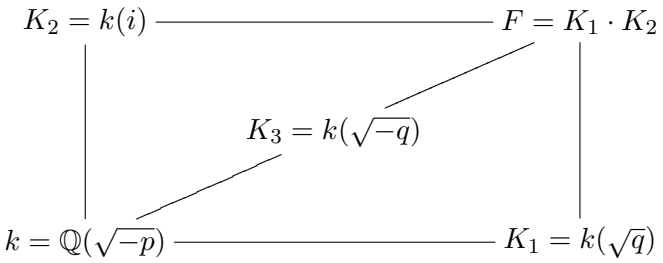
Proof. These assertions are consequences of Proposition 22 in [34]. □

IV.3.2 Presentations of Galois groups over k_n.

Our aim here is to compute the Galois groups of ray class field towers above each k_n (see Theorems IV.3.9 and IV.3.12 below). The two cases $k = \mathbb{Q}(\sqrt{-p})$ and $S = \{q\}$ with respectively $p \equiv 5 \bmod 8$ and $q \equiv 3 \bmod 8$, and $p \equiv 3 \bmod 8$ and $q \equiv 5 \bmod 8$ are again only slightly different. First we prove Theorem IV.3.9, assuming that $k = \mathbb{Q}(\sqrt{-p})$ and $S = \{q\}$ with :

$$p \equiv 5 \bmod 8,\ q \equiv 3 \bmod 8,\ \left(\frac{p}{q}\right) = -1.$$

We introduce the following notations :



Proposition IV.3.6. *Assume that the Legendre symbol $\left(\frac{p}{q}\right)$ is -1. Then the Galois group $\mathrm{Gal}(L_S^\infty(k)/k)$ is isomorphic to the quaternionic group $\mathcal{Q}_8$.*

Proof. First, we collect some lemmas :

Lemma IV.3.7. *There are isomorphisms $A(k) = \mathbb{Z}/2\mathbb{Z}$ and $A_S(k) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The Hilbert 2-class field of k is K_2, and its ray 2-class field associated to the prime q is F.*

Proof. It follows from Theorem IV.2.1 and Proposition IV.2.2, that $A(k) \simeq D(k) \simeq \mathbb{Z}/2\mathbb{Z}$ and $D_S(k) \simeq \mathbb{Z}/2\mathbb{Z}$. Since K_2 is an unramified 2-extension of k, it is the Hilbert 2-class field of k. Then we apply Proposition IV.1.2 in k : since q splits in k, the value of ${}_2\phi(\mathcal{M})$ is 4, and since $E(k)$ is generated by -1, which is not congruent to 1 modulo $\mathcal{M}$, we deduce that $\#A_S(k) = 4$. Since F is a S-ramified $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extension of k, it is its q-ray 2-class field. □

Lemma IV.3.8. *The group $A_S(\mathbb{Q}(\sqrt{p}))$ is trivial, and the groups $A_S(K_2)$ and $A_S(K_1)$ are cyclic.*

Proof. The first assertion follows easily from the genus formula in the extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, since p is the only ramified prime in this extension. Then we use the genus formula (Proposition IV.1.3) in $K_2/\mathbb{Q}(\sqrt{p})$:

$$\#A_S(K_2)^\Delta = \frac{8}{2.[\mathcal{E}_S(\mathbb{Q}(\sqrt{p})) : \mathcal{E}_S(\mathbb{Q}(\sqrt{p})) \cap N_{K_2/\mathbb{Q}(\sqrt{p})}\mathcal{J}_{K_2}]},$$

where the 8 in the numerator comes from the 3 places (the place above 2 and the two real places) which ramifiy in this extension. We use Proposition IV.1.2 in $\mathbb{Q}(\sqrt{p})$. The groups $A(\mathbb{Q}(\sqrt{p}))$ and $A_S(\mathbb{Q}(\sqrt{p}))$ are trivial, and q is inert in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, hence ${}_2\phi(\mathcal{M}) = 8$. We deduce that the quotient group $\mathcal{E}/\mathcal{E}_S(\mathbb{Q}(\sqrt{p}))$ is cyclic of order 8. Given $(\epsilon, -1)$ a system of generators of $\mathcal{E}$, linear algebra shows that the subgroups of $\mathcal{E}$ which give such a quotient are those generated by $-\epsilon^4$ and $(-1, \epsilon^8)$. The second possibility has to be excluded since -1 cannot lie in $\mathcal{E}_S$. Then $\mathcal{E}_S$ is generated by $-\epsilon^4$. This element cannot be a norm from K_2, since ϵ^4 is so and -1 is not. It follows that :

$$\#A_S(K_2)^{\Delta} = 2,$$

and we conclude that $A_S(K_2)$ is cyclic with Lemma IV.1.4.
Finally, the maximal 2-split S-ramified (abelian) 2-extension of k is a quadratic extension according to Lemma IV.3.7. Since K_1 has those properties, it is that extension. We deduce that $A'_S(K_1)$ is trivial. Hence $A_S(K_1) \simeq D_S(K_1)$ is cyclic, according to Proposition IV.3.2. □

It turns out from Lemma IV.3.7 that $\mathrm{Gal}(L_S^{\infty}(k)/k)$ has its abelianization isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. A table of maximal subgroups of such 2-groups is given for instance in [20] (Table 1, see there also for references). Our Lemma IV.3.8 together with this table ensures that the Galois group $\mathrm{Gal}(L_S^{\infty}(k)/k)$ is either abelian or isomorphic to the quaternionic group.
To conclude the proof, let us consider the ideal above p in k. It is generated by $\sqrt{-p}$. Denoting by $\mathfrak{q}_1$ and $\mathfrak{q}_2$ the prime ideals above q in k, there is a rational integer r such that $\sqrt{-p} \equiv r \mathrm{mod}\mathfrak{q}_1$ and $\sqrt{-p} \equiv -r \mathrm{mod}\mathfrak{q}_2$. It follows that no odd power of $\sqrt{-p}$ can be congruent to 1 modulo q. The ideal generated by $\sqrt{-p}$ admits another generator, namely $-\sqrt{-p}$, and the same holds for this generator. Thus, that ideal is not trivial in $A_S(k)$. The same argument holds in K_1 replacing the ideals above q, and using the fact that the 2-part of $E/E_{\mathcal{M}}$ has order 2 (for instance by Proposition IV.1.2), hence is still generated by -1. Then, there is an ideal which does not S-capitulate from k to K_1, and we conclude the proof of Proposition IV.3.6 thanks to Theorem 1 in [15] (whose adaptation to the case of ray class field towers is immediate). □

Theorem IV.3.9. *Under the assumptions of Proposition IV.3.6, for each $n \geq 0$, the group $\mathcal{G}_n = \mathrm{Gal}(L_S^{\infty}(k_n)/k_n)$ admits as a presentation :*

$$< a, b | a^2[a, b], a^{2^{n+2}}, a^{2^{n+1}} b^{-2^{n+1} w_n} >,$$

where w_n is some power of 2. Moreover, $w_0 = 1$, and, if the constant term of the Iwasawa polynomial of $X'_S(k_\infty)$ satisfies $C_0 \equiv 2 \bmod 8$, then $w_n = 1$ for all n.

Proof. Recall that the group $\mathrm{Gal}(L_S^{\infty}(k_\infty)/k_\infty)$ admits as a presentation $< a, b | a^2[a, b] >$. Each group $\mathcal{G}_n$ can be viewed as a quotient group of the former, according to the isomorphism $\mathcal{G}_n \simeq \mathrm{Gal}(L_S^{\infty}(k_n).k_\infty/k_\infty)$. Moreover, F_∞ is contained in $L_S^{\infty}(k).k_\infty$ (this follows from the proof of Proposition IV.3.6), and it is the fixed field of the subgroup of $\mathcal{G}$ generated by a^2 and b^2. This field admits three quadratic extensions, fixed respectively by $< a^4, b^2 >$, $< a^2, b^4 >$ and $< a^4, a^2 b^2 >$, and their Galois group

over k_∞ are respectively dihedral, abelian and quaternionic of order 8. Thus we have the presentation :

$$\mathcal{G}_0 \simeq < a, b | a^2[a,b], a^4, a^2b^2 > .$$

Now, denote by $H = X_S(K_\infty)$ the abelian subgroup of $\mathcal{G}$ generated by a and b^2, whose fixed field is $K_{1,\infty}$. It admits an Iwasawa module structure. There is an exact sequence :

$$1 \to < a > \to H \to X'_S(k_\infty) \to \mathrm{Gal}(K_{1,\infty}/k_\infty) \to 1.$$

Denote by $P(T)$ the Iwasawa polynomial of the Iwasawa module $X'_S(k_\infty)$. It has degree one, hence it can be written $T + C_0$ for some C_0. There is a trivial action of some generator $\gamma \in \Gamma$ on the ideal above 2 in each layer $K_{1,n}$ of the cyclotomic extension of K_1. Taking the limit, it yields a trivial action on a, hence the subgroup $< a >$ of H can be made isomorphic to $\Lambda/T\Lambda$, by the canonical identification between γ and $T-1$. Then, the exact sequence above gives a pseudo-isomorphism, with trivial kernel :

$$H \sim \Lambda/TP(T)\Lambda.$$

Through this map, the element a can be identified with $P(T)$, and b^2 with T, since it generates the image of H in $X'_S(k_\infty) \simeq \Lambda/P(T)\Lambda$. The cokernel of that pseudo-isomorphism is $\mathbb{Z}/2\mathbb{Z}$, according to the following lemma :

Lemma IV.3.10. *$C_0 \equiv 2 \bmod 4$.*

Proof. It is completely analogous to Lemma 4.4 in [21]. On the one hand, the Iwasawa module $X'_S(k_\infty)$ is isomorphic to $\Lambda/P(T)\Lambda$, and on the other hand its quotient by T is isomorphic to $A'_S(k)$ (by Lemma 13.15 in [43], since there is only one prime above 2 in k). The latter is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, hence there is an isomorphism $\Lambda/(T, P(T))\Lambda \simeq \mathbb{Z}/2\mathbb{Z}$, and it proves that the constant coefficient C_0 of P is congruent to 2 modulo 4. □

It is a classical fact of Iwasawa theory (see [43], Lemma 13.15) that the groups $\mathrm{Gal}(L_S(K_{1,\infty})/L_S(K_{1,n}).k_\infty)$ can be computed as $\nu_n(T)Y_0$, with :

$$\nu_n(T) = \frac{(1+T)^{2^n} - 1}{T},$$

$$Y_0 = \mathrm{Gal}(L_S(K_{1,\infty})/L_S(K_{1,0}).k_\infty) = < a^4, a^2b^2 > .$$

The polynomial $\nu_n(T)$ admits the expansion $2^n + 2^{n-1}(2^n-1)T + o(T)$ for each $n \geq 1$. Then, there are relations :

$$\nu_n(T) = x_n P(T) + y_n T \bmod TP(T),$$

where $x_n = 2^{n-1}u$ and $y_n = 2^n v_n$, with $u = 2/C_0 \in \mathbb{Z}_2^\times$ (according to the previous lemma), and $v_n = 2^n - 1 - u$. Using those notations, a direct computation yields :

$$\nu_n(T)Y_0 = < a^{4x_nC_0}, a^{2x_nC_0}b^{-y_nC_0} > = < a^{2^{n+2}}, a^{2^{n+1}}b^{-2^{n+1}w_n} >,$$

where w_n is the greatest 2-power dividing v_n. The last assertion follows from $v_n = 2^n - 1 - u$. □

Now we turn our attention to Theorem IV.3.12. We take now $k = \mathbb{Q}(\sqrt{-p})$ and $S = \{q\}$ with :

$$p \equiv 5 \bmod 8,\ q \equiv 3 \bmod 8,\ \left(\frac{p}{q}\right) = -1,$$

or :

$$k = \mathbb{Q}(i),\ q \equiv 7 \bmod 16.$$

We recall that $K = k(\sqrt{q})$. There is no analogous to the fields K_2 and K_3 here, and the Proposition IV.3.6 must be replaced by :

Lemma IV.3.11. *Under the assumptions above. The maximal S-ramified 2-extension of k is a cyclic extension of degree 4 which contains K. The primes above 2 have inertia degree 2 in this extension.*

Proof. It follows from Theorem IV.2.1, and Propositions IV.2.2 and IV.2.5 that the groups $D(k)$ and $A'(k)$ are trivial. Hence, the group $A(k)$ is trivial as well. By the same propositions, the group $D_S(k)$ is cyclic of order 2.
By Proposition IV.1.2, the group $A_S(k)$ is then cyclic, as a quotient group of $\prod_{v \in S(k)} \mathfrak{k}_v$, provided that $S(k)$ contains only one place, and this is true in the two cases (thanks to the assumption $\left(\frac{p}{q}\right) = -1$ in the first case). The same proposition gives the cardinality of $A_S(k)$, which turns to be 4. □

The field $L_S^\infty(k).k_\infty$ is thus a cyclic extension of degree 4 of k_∞, and it contains K_∞. The latter admits three distinct quadratic extensions, which are fixed respectively by $< a, b^4 >$, $< a^2, b^2 >$ and $< a^2, ab^2 >$. The first is 2-split over k_∞, the second one is not cyclic over that field. Hence we find :

$$Y_0 = \mathrm{Gal}(L_S(K_\infty)/L_S^\infty(k).k_\infty) =< a^2, ab^2 > .$$

By the same computation as before, we have, for $n \geq 1$:

$$\mathrm{Gal}(L_S(K_\infty)/L_S^\infty(k_n).k_\infty) = \nu_n(T)Y_0 =< a^{2x_nC_0}, a^{x_nC_0}b^{-y_nC_0} > .$$

Lemma IV.3.10 also holds in this case, and the theorem follows.

Theorem IV.3.12. *Assume that $p \equiv 3 \bmod 8$ and $S = \{q\}$ with $q \equiv 5 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$. For each $n \geq 1$, the group $\mathcal{G}_n = \mathrm{Gal}(L_S^\infty(k_n)/k_n)$ admits as a presentation :*

$$< a, b | a^2[a, b], a^{2^{n+1}}, a^{2^n} b^{-2^n w_n} >,$$

where w_n is some power of 2. Moreover, $w_0 = 1$, and, if the constant term of the Iwasawa polynomial of $X'_S(k_\infty)$ satisfies $C_0 \equiv 2 \bmod 8$, then $w_n = 1$ for all n.
The same holds if $k = \mathbb{Q}(i)$ and $q \equiv 7 \bmod 16$.

Bibliographie

[1] S. P. Demuškin. The group of a maximal p-extension of a local field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 25 :329–346, 1961.

[2] Bruce Ferrero. The cyclotomic $\mathbf{Z}_2$-extension of imaginary quadratic fields. *Amer. J. Math.*, 102(3) :447–459, 1980.

[3] Bruce Ferrero and Lawrence Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math. (2)*, 109(2) :377–395, 1979.

[4] Takashi Fukuda. Remarks on $\mathbb{Z}_p$-extensions of number fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 70(8) :264–266, 1994.

[5] E. S. Golod and Igor R. Shafarevich. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28 :261–272, 1964.

[6] Georges Gras. *Class field theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. From theory to practice, Translated from the French manuscript by Henri Cohen.

[7] Ralph Greenberg. On the Iwasawa invariants of totally real number fields. *Amer. J. Math.*, 98(1) :263–284, 1976.

[8] Kenkichi Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, 65 :183–226, 1959.

[9] Jean-François Jaulent and Jonathan W. Sands. Sur quelques modules d'Iwasawa semi-simples. *Compositio Math.*, 99(3) :325–341, 1995.

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

[11] Jean-François Jaulent. Plongements l-adiques et l-nombres de Weil. Preprint. `http://www.math.u-bordeaux.fr/~jaulent/`, 2006.

[12] Jean-François Jaulent and Thong Nguyen Quang Do. Corps p-rationnels, corps p-réguliers, et ramification restreinte. *J. Théor. Nombres Bordeaux*, 5(2) :343–363, 1993.

[13] Jean-François Jaulent and Odile. Sauzet. Pro-l-extensions de corps de nombres l-rationnels. *J. Number Theory*, 65(2) :240–267, 1997.

[14] Yûji Kida. On cyclotomic $\mathbf{Z}_2$-extensions of imaginary quadratic fields. *Tôhoku Math. J. (2)*, 31(1) :91–96, 1979.

[15] Hershy Kisilevsky. Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94. *J. Number Theory*, 8(3) :271–279, 1976.

[16] Helmut 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.

[17] John Labute. Classification of Demushkin groups. *Canad. J. Math.*, 19 :106–132, 1967.

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

[19] Christian Maire. *Extensions* T*-ramifiées modérées,* S*-décomposées*. PhD thesis, Université de Franche-Comté, 1995.

[20] Yasushi Mizusawa. On the maximal unramified pro-2-extension of $\mathbb{Z}_2$-extensions of certain real quadratic fields. II. *Acta Arith.*, 119(1) :93–107, 2005.

[21] Yasushi Mizusawa. On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field. 2006.

[22] Abbas Movahhedi and Thong Nguyen Quang Do. Sur l'arithmétique des corps de nombres p-rationnels. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 155–200. Birkhäuser Boston, Boston, MA, 1990.

[23] V. G. Mukhamedov. Local extensions associated with l-extensions of number fields with bounded ramification. *Mat. Zametki*, 35(4) :481–490, 1984.

[24] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.

[25] Manabu Ozaki. Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions. *J. Reine Angew. Math.*, 602 :59–94, 2007.

[26] Manabu Ozaki and Hisao Taya. A note on the Iwasawa λ-invariants of real abelian number fields. *Interdiscip. Inform. Sci.*, 4(2) :109–116, 1998.

[27] Landry Salle. Mild pro-p-groups as Galois groups over global fields. *A paraître : Int. J. Number Theory*.

[28] Landry Salle. Sur les pro-p-extensions à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres. *A paraître : J. Théor. Nombres Bordeaux*.

[29] Landry Salle. On maximal tamely ramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field. 2008.

[30] Alexander Schmidt. Circular sets of prime numbers and p-extensions of the rationals. *J. Reine Angew. Math.*, 596 :115–130, 2006.

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

[32] Alexander Schmidt. On pro-p-fundamental groups of marked arithmetic curves. Preprint. `http://www.mathematik.uni-regensburg.de/Schmidt/papers/schmidt32-de.htm%l`, 2008.

[33] Alexander Schmidt. On the K$(\pi, 1)$ property for rings of integers in the mixed case. Preprint. `http://www.mathematik.uni-regensburg.de/Schmidt/papers/schmidt29-en.htm%l`, 2008.

[34] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 1965 of *With a contribution by Jean-Louis Verdier. Lecture Notes in Mathematics, No. 5. Troisième édition.* Springer-Verlag, Berlin, 1965.

[35] Jean-Pierre Serre. *Représentations linéaires des groupes finis.* Hermann, Paris, revised edition, 1978.

[36] Jean-Pierre Serre. Classes des corps cyclotomiques (d'après K. Iwasawa). In *Séminaire Bourbaki, Vol. 5*, pages Exp. No. 174, 83–93. Soc. Math. France, Paris, 1995.

[37] Jean-Pierre Serre. Structure de certains pro-p-groupes (d'après Demuškin). In *Séminaire Bourbaki, Vol. 8*, pages Exp. No. 252, 145–155. Soc. Math. France, Paris, 1995.

[38] Igor R. Shafarevich. On p-extensions. *Rec. Math. [Mat. Sbornik] N.S.*, 20(62) :351–363, 1947.

[39] Igor R. Shafarevich. Extensions with prescribed ramification points. *Inst. Hautes Études Sci. Publ. Math.*, (18) :71–95, 1963.

[40] Igor R. Shafarevich. *Collected mathematical papers.* Springer-Verlag, Berlin, 1989. Translated from the Russian.

[41] Denis Vogel. Circular sets of primes of imaginary quadratic number fields. Preprint. `http://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/preprints/Vogel.htm`, 2006.

[42] Denis Vogel. p-extensions with restricted ramification - the mixed case. Preprint. `http://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/preprints/Vogel.htm`, 2006.

[43] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1997.

[44] Kay Wingberg. Arithmetical Koch groups. Preprint. `http://www.mathi.uni-heidelberg.de/~wingberg/agwingberg/paperwingberg/w%ingberg40-en.html`, 2007.

[45] Kay Wingberg. Riemann's existence theorem and the $\mathrm{K}(\pi, 1)$-property of rings of integers. Preprint. `http://www.mathi.uni-heidelberg.de/~wingberg/agwingberg/paperwingberg/w%ingberg42-en.html`, 2007.