UFR Sciences et Techniques
École Doctorale Louis Pasteur
Université de Franche-Comté – Besançon

Thèse de Doctorat

présentée par

Frédéric Pitoun

pour obtenir le grade de
Docteur de Mathématiques de l'Université de Franche-Comté

Calculs théoriques et explicites en théorie d'Iwasawa

Thèse soutenue le 17 septembre 2010 à Besançon, devant le jury composé de :

Bruno Anglès (rapporteur)	Professeur à l'Université de Caen
Jean-Robert Belliard (directeur)	Maître de Conférences à l'Université de Franche-Comté
Emmanuel Hallouin	Maître de Conférences à Université Toulouse II-Le Mirail
Christian Maire (directeur)	Professeur à l'Université de Franche-Comté
Bernadette Perrin-Riou (rapporteur et président du jury)	Professeur à l'Université Paris XI
Thong Nguyen Quang Do	Professeur à l'Université de Franche-Comté

Remerciements

Je tiens à remercier en tout premier lieu mes directeurs de thèse sans qui cette thèse n'aurait jamais abouti.
D'une part Jean Robert Belliard, qui m'a accompagné lors de mes premiers pas en théorie algébrique des nombres, que j'ai effectués par le biais du DEA du centre de télé-enseignement de l'université de Besançon et qui par la suite a accepté de m'encadrer en thèse. Je le remercie notamment pour les nombreux trajets entre Bordeaux et Toulouse qu'il a effectués, n'hésitant pas à se lever à l'aube pour me voir me débattre au beau milieu des ϕ-parties et ϕ-quotients, tronçonner allègrement la suite exacte de Coleman ou invoquer le "NSW" comme on invoque un texte cabalistique.
D'autre part, Christian Maire qui m'a dans un premier temps accueilli dans les locaux de feu le GRIMM et m'a patiemment écouté me plaindre des foncteurs qui n'étaient pas exacts, des H^1 non-triviaux et autre joyeusetés cohomologiques. J'ai également une pensée pour les membres permanents du GRIMM, J-M Couveignes, M. Perret, E. Hallouin et T. Henocq, qui m'ont accueilli pendant plusieurs années au sein de leur laboratoire. Les nombreux séminaires que j'ai suivis durant cette période et leur précieuse bibliothèque m'ont grandement aidé. Cette période fut également celle du TAM-TAM, groupe de travail étudiant, au cours duquel j'ai eu de fructueux échanges avec mes collègues doctorants : Landry, Alain, Lara, Cécile, Tony, Mourad et Magyd. J'ai également une pensée pour les doctorants de l'université de Besançon, que j'ai malheureusement trop peu côtoyés pour de triviales raisons géographiques.
Je remercie E. Hallouin d'avoir accepté d'être membre de mon jury, ainsi que T. Nguyen Quand Do qui, non-content d'être également membre de mon jury, a également accepté d'encadrer mon mémoire de DEA et m'a fait partager sa grande expérience de la théorie d'Iwasawa.
J'ai également beaucoup appris lors des discussions informelles qui ont lieu un peu partout lors des conférences. Je pense notamment à celles que j'ai eues avec B. Anglès et D. Solomon, que je remercie de l'attention qu'ils ont portés à mes modestes travaux.
Enfin je tiens à remercier tout particulièrement Bernadette Perrin-Riou et Bruno Anglès d'avoir accepté de rapporter mes travaux de recherches. J'en profite également pour remercier Bernadette Perrin-Riou des nombreuses aides qu'elle m'a apportées dans un cadre tout à fait différent. En effet, je l'ai rencontrée il y a près d'une dizaine d'années lors d'un colloque WIMS et depuis elle a toujours été là pour répondre à mes questions relatives à l'utilisation de WIMS.

Table des matières

Introduction

En 1637, Fermat énonça le célèbre théorème qui porte aujourd'hui son nom :

Théorème (Fermat-Wiles,1994)**.** *Pour tout entier naturel, $n \geq 3$, l'équation $X^n + Y^n = Z^n$ ne possède pas de solutions entières non-triviales.*

Ce théorème a été l'objet de nombreuses recherches depuis sa formulation jusqu'à sa démonstration en 1994 par Taylor-Wiles.
En marge de ce théorème, Fermat aurait laissé une appréciation laissant entendre qu'il disposait d'une preuve merveilleuse de ce résultat.
Si quelques preuves relativement simples existent pour des valeurs particulières de n, comme $n = 3$ (Euler, 1770) ou $n = 5$ (Dirichlet et Legendre, 1825), l'étude de ce théorème dans un cadre général s'est avérée être un problème très ardu. La première avancée significative a été faite par Kummer en 1847. Il démontre en effet le théorème de Fermat pour tous les nombres premiers p pour lesquels l'anneau des entiers de $\mathbb{Q}(\zeta_p)$ est factoriel. La factorialité de l'anneau des entiers de $\mathbb{Q}(\zeta_p)$ constitue la clé de voûte de sa preuve et c'est probablement en cherchant à généraliser sa démonstration qu'il découvre le premier exemple d'anneau d'entiers cyclotomiques, qui ne soit pas factoriel : $\mathbb{Z}[\zeta_{23}]$.
Dedekind, qui rencontre Kummer en 1859 à Berlin, formalisa en 1871 la notion d'idéal premier et introduisit la notion d'anneau de Dedekind. Cette notion généralise en un certain sens celle d'anneau factoriel. En effet dans un anneau de Dedekind, à l'instar de ce qui se passe dans le cas factoriel, tout idéal se décompose de façon unique en produit d'idéaux premiers.
Cherchant à mesurer le "défaut de principalité" des anneaux d'entiers des corps de nombres, Kummer introduisit la notion de groupe des classes. Rappelons brièvement, en termes modernes, comment définir ce groupe des classes : la multiplication induit sur l'ensemble des idéaux de O_K, anneau des entiers d'un corps de nombres K une loi de composition interne. Symétrisant cette loi, on obtient un groupe, appelé groupe des idéaux fractionnaires de K. Les idéaux principaux engendrent naturellement un sous-groupe P du groupe des idéaux fractionnaires Id de K. Le quotient Id/P est appelé groupe des classes d'idéaux associé au corps K. Le groupe des classes d'idéaux $Cl(K)$, qui est trivial si et seulement si l'anneau O_K est principal, permet donc de

quantifier le défaut de principalité de O_K. Utilisant ce concept, Kummer put alors généraliser la démonstration qu'il avait élaborré en 1847 aux nombres premiers p pour lesquels l'ordre de $Cl(\mathbb{Z}[\zeta_p])$ n'est pas divisible par p, comme par exemple $p = 23$. Cette démonstration, datant de 1857, fut primée par l'académie des sciences de Paris.
Les travaux de Kummer relatifs au théorème de Fermat l'amenèrent également à étudier l'existence de lois de réciprocité d'ordre quelconque, définies sur les anneaux d'entiers cyclotomiques. Cette quête l'amena à l'étude des extensions abéliennes de $\mathbb{Q}$. Dans le même temps Eisenstein s'intéressa aux extensions abélienne de $\mathbb{Q}(i)$.
Dans un article paru en 1897, Hilbert fit d'une part la synthèse des travaux de Kummer et d'Eisenstein sur les extensions abéliennes, qu'il relia à ceux de Kronecker-Weber et d'autre part introduisit ses propres idées. Il conjectura puis démontra l'existence de ce que l'on appelle aujourd'hui le corps de Hilbert d'un corps de nombre K :

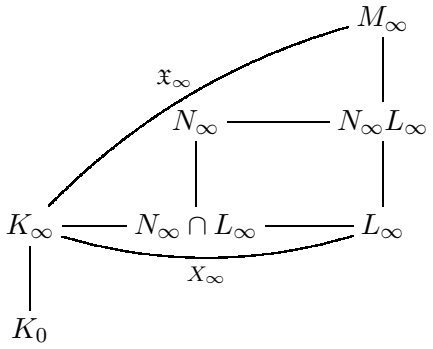
Théorème (Hilbert,1907)**.** *Étant donné un corps de nombre K, dont le groupe des classes est noté $Cl(K)$, il existe une unique extension abélienne H_K de K telle que :*

1. *H_K/K soit non ramifiée.*
2. *toute extension abélienne non-ramifiée de K est contenue dans H_K*
3. *$Gal(H_K/K) \simeq Cl(K)$*

Il faudra par suite attendre 1920 et les travaux d'Artin et de Takagi pour obtenir une généralisation de la loi de réciprocité quadratique à un corps de nombres quelconque. Ces travaux sont le fondement de ce que l'on appelle aujourd'hui la théorie du Corps de Classe. Comme le disait Chevalley en 1940, *L'objet de la théorie du Corps de Classes est de montrer comment les extensions abéliennes d'un corps de nombres algébriques K peuvent être déterminées par des éléments tirés de la connaissance de K lui même ; ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possède en soi les éléments de son propre dépassement.*
Lors d'un séjour à Princeton en 1952, Artin rencontra Iwasawa et poussa ce dernier à s'intéresser à la théorie algébrique des nombres. Iwasawa adapta à la théorie des nombres de nombreuses idées venues de l'étude des variétés algébriques.
Iwasawa, qui s'intéressera entre autre au groupe des classes d'idéaux d'un corps de nombres K, développa une théorie qui aujourd'hui porte son nom. L'un des objectifs de cette théorie est l'étude de modules d'Iwasawa, objets arithmétiques associés à une $\mathbb{Z}_p$-extension K_∞ d'un corps de nombres K. L'étude de ces modules permet d'obtenir des informations sur l'arithmétique de K_0, informations jusque là inaccessibles. C'est en ce sens que la théorie d'Iwasawa fut considérée comme révolutionnaire.
Un des principaux module d'Iwasawa est le module X_∞, qui est le groupe de

Galois de la pro-p-extension abélienne non-ramifiée maximale de K_∞ et peut donc être considéré comme une généralisation au niveau infini du groupe de classes d'idéaux. Ce module, comme tous les modules d'Iwasawa, possède une structure de Λ-module de type fini, Λ désignant l'anneau des séries formelles à une indéterminée à coefficients dans $\mathbb{Z}_p$. On peut par conséquent définir les invariants λ, μ et ρ, associés au Λ-module X_∞.
Ces invariants furent étudiés par de nombreux mathématiciens, dont Greenberg, qui fut l'élève d'Iwasawa en 1967. Ce dernier conjectura dans [8] la nullité de l'invariant λ associé au module X_∞, dans le cas où le corps K est totalement réel. Cette conjecture encore ouverte à l'heure actuelle est le point de départ de la présente thèse et en constitue l'arrière plan.

Précisons maintenant le cadre théorique de cette thèse. Initialement on se donne un premier impair p et un corps de nombres K_0, contenant une racine primitive p-ième de l'unité, ζ_p.
Le n-ième étage de la $\mathbb{Z}_p$-extension cyclotomique de K_0 sera noté K_n et on définit les extensions L_∞ et M_∞ de K_∞ comme étant les pro-p-extensions abéliennes de K_∞, qui sont respectivement non-ramifiées et non-ramifiées en dehors de p et maximales pour ces propriétés. Les groupes de Galois sur K_∞ des extensions L_∞ et M_∞, notés respectivement X_∞ et $\mathfrak{X}_\infty$, sont naturellement munis d'une structure de Λ-module, l'anneau Λ étant l'anneau des séries formelles à coefficients dans $\mathbb{Z}_p$.
L'invariant μ de X_∞ est conjecturalement nul, cette conjecture a été démontrée en 1979 par Ferrero et Washington ([5]) dans le cas où l'extension $K_0/\mathbb{Q}$ est abélienne. Le module X_∞ étant de Λ-torsion, son invariant ρ est nul. L'invariant λ quant à lui est en général non-nul, même si sa nullité fut conjecturée par Greenberg dans le cas où le corps K_0 est totalement réel.
Enfin, on définit N_∞ comme le compositum des extensions de K_∞ de la forme $K_\infty(u^{\frac{1}{p^a}})$ avec u unité de K_∞ et a entier naturel, de sorte que le radical kummérien associé à l'extension N_∞/K_∞ n'est autre que $U_{K_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p$.
Les extensions N_∞, L_∞ et M_∞ sont reliées entre elles de la façon suivante :



Dans [8], Greenberg montre en outre que la nullité de l'invariant λ de X_∞^+ est équivalente à la capitulation des groupes de classe d'idéaux de K_n^+, i.e.

à la trivialité de la limite inductive $A_\infty^+ = \varinjlim A_n^+$, A_n désignant la p-partie de $Cl(K_n)$.
L'extension N_∞ est fortement reliée à l'extension L_∞. En effet dans [13], Iwasawa démontre que $\mathrm{Gal}(M_\infty/N_\infty) \simeq \mathrm{Hom}(A_\infty, \mu_{p^\infty})$. Cet isomorphisme permet de donner une interprétation kummérienne de la conjecture de Greenberg, la véracité de cette conjecture impliquant la trivialité de la partie $-$ de $\mathrm{Gal}(M_\infty/N_\infty)$.
H. Ichimura s'est dans ses travaux beaucoup intéressé au problème de l'existence d'une base normale d'entiers pour une extension de degré p non-ramifiée, L d'un corps de nombres K, contenant ζ_p. Il montre dans [11] que l'existence d'une telle base est équivalente au fait que l'extension L soit engendrée par un élément de la forme $u^{\frac{1}{p}}$ avec $u \in U_K$, groupe des unités de K. Ce problème d'existence de base normale d'entiers se traduit donc également de façon kummérienne.
Par suite, dans [10], il étudie l'existence de base normales d'entiers pour des extensions non-ramifiées de degré p de K_n, n-ième étage de la $\mathbb{Z}_p$-extension cyclotomique de K et montre que dans le cas semi-simple, l'existence de telles bases pour $n >> 0$ est fortement reliée à l'invariant λ de X_∞^+. En particulier la véracité de la conjecture de Greenberg implique que pour tout entier $n >> 0$, les extensions de degré p de K_n sont engendrées par des racines p-ièmes d'unités et par conséquent possèdent des bases normales d'entiers.

On se propose dans le premier chapitre de cette thèse d'essayer de généraliser les résultats obtenus par Ichimura dans le cas non-semi-simple. Pour n entier, notons $H_n(p)$ l'extension abélienne non-ramifiée d'exposant p maximale de K_n et N_n l'extension de K_n engendrée par des racines p-ièmes d'unités. Le résultat initial d'Ichimura relie pour $n >> 0$, le $\mathbb{F}_p$-rang de la Φ^*-partie du radical kummérien associé à l'extension $H_n(p)/H_n(p) \cap N_n$ à λ_Φ, invariant λ de la Φ-partie de X_∞, Φ désignant un caractère de $\mathrm{Gal}(K_0/\mathbb{Q})$. En particulier ce $\mathbb{F}_p$-rang est nul si et seulement si $\lambda_\Phi = 0$.
Le premier écueil rencontré lors de la tentative de généralisation du théorème précédent a été la définition de la notion de Φ-partie au cas non-semi-simple. Même s'il existe une définition communément admise de la notion de Φ-partie et de celle de Φ-quotient dans le cas non-semi-simple, les résultats algébriques relatifs à ces notions, même s'ils sont bien connus de tous les spécialistes, n'apparaissent que de façon éparse dans la littérature et ne sont pas systématiquement démontrés. Ce chapitre commence donc par un recueil des résultats algébriques connus sur les notions de Φ-partie et de Φ-quotient, résultats que nous avons choisis de redémontrer en utilisant une approche aussi élémentaire que possible. Ces préliminaires acquis, nous avons généralisé au cas non-semi-simple certains des résultats obtenus par Ichimura dans [10]. Nous obtenons dans le cas non-semi-simple un résultat au niveau infini, analogue à celui obtenu par Ichimura au niveau fini. Plus précisément,

nous démontrons le théorème suivant :

Théorème. *Soit Φ un caractère pair de $Gal(K_0/\mathbb{Q})$. On note λ_Φ l'invariant λ du Λ-module $X_\infty(K_0)$ et $\deg(\Phi)$ le degré de l'extension $\mathbb{Q}_p(\Phi(G))/\mathbb{Q}_p$. Alors :*

$$\mathrm{Corang}_{\mathbb{Z}_p}(\mathcal{H}_\infty/\mathcal{E}_\infty)^\Phi = \lambda_\phi.\deg(\Phi).$$

Le point clé de la démonstration étant la trivialité de la Φ-partie du module $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^\Phi$ pour tout caractère impair Φ.
Au préalable, il a fallu généraliser la notion de Φ-partie au cas non-semi-simple. Etant donné un $\mathbb{Z}_p$-module M, on peut naturellement définir la Φ-partie M^Φ de M en utilisant l'idempotent $e_\Phi = \frac{1}{|G|}\sum_{g\in G}\Phi(g)g^{-1} \in \mathbb{Q}_p[G]$ de la façon suivante :

- $M^\Phi = e_\Phi(M \otimes \mathbb{Z}_p)$ si M est de type fini,
- $M^\Phi = e_\Phi(\mathrm{Div}(M)$ si M est de torsion, $\mathrm{Div}(M)$ désignant le sous-module divisible maximale de M.

Nous avons choisi une approche différente et défini la notion de Φ-partie de façon fonctorielle. Les deux principaux avantages d'une telle démarche sont d'une part que l'on obtient une définition unifiée de la notion de Φ-partie et d'autre part que cette définition peut être utilisée dans le cas où M est un $\mathbb{Z}_p$-module de torsion de type fini. Le résultat que l'on obtient, sur la trivialité de la partie $-$ de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$ permet de traduire la conjecture de Greenberg en termes kummériens. Plus précisément, la finitude de la partie $+$ de X_∞ implique que la partie $-$ de X_∞ coïncide avec $\mathrm{Gal}(L_\infty \cup N_\infty/K_\infty)^-$. En d'autres termes, toute p-extension cyclique de K_∞, non-ramifiée contenue dans L_∞^-, est engendrée par une racine p-primaire d'unités. Ce qui constitue bien une généralisation au niveau infini du résultat obtenu par Ichimura au niveau fini.

Dans le second chapitre de cette thèse, nous avons regardé ce qui se passait au niveau fini. Reprenant les travaux effectués par G. Gras dans [6], nous décrivons une méthode permettant de calculer explicitement le radical kummérien associé au corps de Hilbert d'un corps de nombre K_0, contenant ζ_p. Cette méthode une fois implémentée avec le logiciel pari-gp nous permet d'observer dans une famille de corps K_0 donnée, ceux pour lesquels il existe des unités dont les racines p-primaires engendrent des extensions non-ramifiées. Malheureusement, nous n'avons pu effectuer ces calculs que pour un nombre relativement petit de corps et cela pour des raisons inhérentes au logiciel utilisé. Les résultats obtenus laissent toutefois penser que, dans la famille considérée, la densité de corps possédant des unités dont les racines p-primaires engendrent des extensions non-ramifiées est non-nulle. On obtient par ailleurs, dans le cas non-semi-simple, une version faible du résultat d'Ichimura. En effet, dans ce cas la véracité de la conjecture de Greenberg implique que toute extension non-ramifiée de degré p de K_n est engendrée par un élément de la forme $u^{\frac{1}{p}}$ avec $u \in U_{K_m}$

pour $m \geq n$.

La conjecture de Greenberg s'énonçant en termes de capitulation de groupe de classes d'idéaux, de nombreux auteurs s'intéressant à cette conjecture ont donc étudié l'application naturelle $j_n : A_n \to A_\infty^{\Gamma_n}$ et plus particulièrement ses noyaux et conoyaux. Dans [19], M. Le-Floch, C. Movaheddi et T. Nguyen-Quang-Do s'intéressent au conoyau de cette application et montre que celui ci est galoisiennement isomorphe au groupe de Galois d'une certaine extension de K_∞, convenablement tordue. Par ailleurs dans [11], H. Ichimura relie, dans le cas semi-simple, la partie $+$ de ce conoyau de capitulation à la $\mathbb{Z}_p$-torsion du module d'Iwasawa $Y_\infty^- := \mathrm{Gal}(N_\infty \cap L_\infty / K_\infty)^-$. L'objectif du troisième chapitre de cette thèse est de généraliser ce dernier résultat au cas non semi-simple en utilisant les techniques développées par M. Le-Floch, C. Movaheddi et T. Nguyen-Quang-Do dans [19].

Dans le dernier chapitre de cette thèse, qui se situe au niveau fini, on s'intéresse à la pro-p-extension abélienne non-ramifiée en dehors de p maximale de K_0, notée M_0 et l'on expose dans une méthode permettant de calculer effectivement la $\mathbb{Z}_p$-torsion du groupe de Galois $\mathfrak{X}_0 := \mathrm{Gal}(M_0/K_0)$. La détermination explicite de $tor_{\mathbb{Z}_p}(\mathfrak{X}_0)$ permet entre autres d'obtenir des informations sur la p-rationalité du corps K_0, ainsi que sur la Λ-liberté de $\mathfrak{X}_\infty$, sous réserve que le corps K_0 vérifie la conjecture de Leopoldt. Une fois la méthode justifiée du point de vue théorique, nous l'implémentons utilisant le logiciel pari-gp et déterminons effectivement $tor_{\mathbb{Z}_p}(\mathfrak{X}_0)$ lorsque le corps K_0 varie dans différentes familles de corps. Après avoir rappelé les heuristiques de Cohen-Lenstra, nous confrontons les résultats numériques obtenus aux résultats théoriques prédits par ces heuristiques. Pour finir, un ensemble de p-places S étant donné, nous nous sommes intéressés à la structure de $\mathbb{Z}_p$-module de $\mathfrak{X}_S := \mathrm{Gal}(M_S/K_0)$, où M_S désigne la pro-p-extension abélienne non-ramifiée en dehors de S de K_0. De nombreuses formules théoriques permettant de calculer le $\mathbb{Z}_p$-rang de $\mathfrak{X}_S$ existent, notamment dans [7] et [17]. Cependant l'implémentation de ces formules en langage pari-gp est peu aisée. Nous verrons à la fin de ce chapitre qu'en utilisant les techniques développées pour le calcul effectif de la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_0$, on obtient une méthode permettant de calculer effectivement la torsion du $\mathbb{Z}_p$-module de $\mathfrak{X}_S$, sous réserve que l'on connaisse son $\mathbb{Z}_p$-rang.

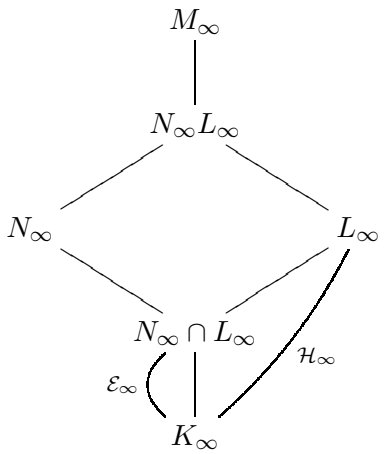
Chapitre 1

Φ-partie d'un module non-semi-simple.

1.1 Introduction

Soit p un nombre premier impair. Considérons une extension abélienne totalement réelle F de $\mathbb{Q}$, modérément ramifiée en p, et notons $K_0 = F(\zeta_p)$, ζ_p désignant une racine primitive p-ième de l'unité. Pour $n \in \mathbb{N}$, on note F_n (respectivement K_n) le n-ième étage de la $\mathbb{Z}_p$-extension cyclotomique de F (respectivement K_0). Du fait que $\zeta_p \in K_0$, on a $K_n = K_0(\zeta_{p^{n+1}})$, $\zeta_{p^{n+1}}$ désignant une racine primitive p^{n+1}-ième de l'unité.
Le corps K_n contenant les racines p^{n+1}-ièmes de l'unité, la théorie de Kummer permet d'établir une correspondance bi-univoque entre les extensions de K_n d'exposant p^{n+1} et les sous-groupes de $K_n^* \otimes \mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$. A toute extension de K_n d'exposant p^{n+1}, on peut donc associer un sous groupe de $K_n^* \otimes \mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$, appelé radical kummérien. De même, au niveau infini, la théorie de Kummer permet d'établir l'existence d'un accouplement non dégénéré entre $K_\infty^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ et l'abélianisé du groupe de Galois de la pro-p-extension maximale de K_∞ à valeurs dans le groupe des racines p-primaires de l'unité, noté μ_{p^∞}. Les relations entre radicaux kummériens et extensions galoisiennes sont étudiées par exemple dans [11] et [19].
La connaissance du radical Kummérien $\mathcal{R}$, associé à une extension R de K_∞, permet d'obtenir des informations sur la ramification dans l'extension R/K_∞. Par exemple si $\mathcal{R} = (u \otimes \frac{1}{p^n})$ pour une certaine p-unité u de K_∞, alors l'extension R/K_∞ est non-ramifiée en dehors de p. D'un autre côté, si l'on se donne une p-extension R de K_∞, non-ramifiée en dehors de p, la théorie de Kummer affirme l'existence d'éléments du type $u_i^{\frac{1}{p^{n_i}}}$ engendrant cette extension. Cependant, en général, il est très difficile d'expliciter les u_i et il n'existe aucune raison pour que ces éléments u_i soient des p-unités. En d'autres termes, la connaissance d'une extension n'apporte que très peu d'informations sur le radical Kummérien associé.

Un des objets centraux en théorie d'Iwasawa est le module d'Iwasawa $X_\infty(K_0)$, que l'on peut interpréter comme le groupe de Galois de la pro-p-extension abélienne non-ramifiée maximale de K_∞, notée L_∞. Le module $X_\infty(K_0)$ est un $\mathbb{Z}_p$-module sur lequel le groupe $\Gamma := \mathrm{Gal}(K_\infty/K_0)$ agit, il est donc muni d'une structure de $\mathbb{Z}_p[[T]]$-module. L'anneau $\mathbb{Z}_p[[T]]$ est habituellement noté Λ.
Ces généralités rappelées, on peut maintenant introduire les notations et définitions des principaux objets que l'on va étudier dans ce chapitre, les relations entre ces différents objets étant résumées dans le diagramme ci-dessous :



- L_∞ désigne la pro-p-extension abélienne non-ramifiée maximale de K_∞.
- M_∞ désigne la pro-p-extension abélienne non-ramifiée en dehors de p maximale de K_∞.
- N_∞ est l'extension de K_∞ engendrée par des éléments du type $u^{\frac{1}{p^n}}$ avec u unité de K_∞.
  Le fait que u soit inversible assure que cette extension est non-ramifiée en dehors de p. Les extensions N_∞ et L_∞ sont donc toutes deux contenues dans la pro-p-extension abélienne, non-ramifiée en dehors de p, M_∞.
- $\mathcal{E}_\infty$ et $\mathcal{H}_\infty$ désignent les radicaux kummériens respectivement associés aux extensions $N_\infty \cap L_\infty$ et L_∞.

Le fait que p soit modérément ramifié dans F, et donc dans K_0, implique que le groupe de Galois $\mathrm{Gal}(K_\infty/\mathbb{Q})$ est produit direct de $\Gamma := \mathrm{Gal}(K_\infty/K_0)$ et de $G = \mathrm{Gal}(K_0/\mathbb{Q})$. Le groupe G s'identifie donc à un sous-groupe de $\mathrm{Gal}(K_\infty/\mathbb{Q})$ et on peut le faire opérer sur les modules d'Iwasawa $\mathrm{Gal}(L_\infty/K_\infty)$ et $\mathrm{Gal}(M_\infty/K_\infty)$, qui sont par conséquent munis d'une structure de $\Lambda[G]$-module. Un caractère Φ de G étant fixé, on peut parler de la Φ-partie de ces modules. La première partie de ce chapitre a pour but de définir les notions de Φ-partie et de Φ-quotient d'un $\mathbb{Z}_p[G]$-

module et d'étudier les propriétés algébriques de ces notions dans le cas où G est un groupe abélien, d'ordre quelconque.
Dans [11], Ichimura montre que dans le cas semi-simple (p ne divise pas $[F : \mathbb{Q}]$), les modules $((\mathcal{E}_\infty/\mathcal{H}_\infty)^\Phi)^\vee$ et $X_\infty(K_0)^\Phi$ ont même $\mathbb{Z}_p$ rang. L'objectif de ce chapitre est de généraliser au cas non semi-simple ce résultat d'Ichimura. Plus précisément, on démontre le théorème suivant :

Théorème. *Soit Φ un caractère pair de $Gal(K_0/\mathbb{Q})$. On note λ_Φ l'invariant λ du Λ-module $X_\infty(K_0)$ et $\deg(\Phi)$ le degré de l'extension $\mathbb{Q}_p(\Phi(G))/\mathbb{Q}_p$. Alors :*

$$\mathrm{Corang}_{\mathbb{Z}_p}(\mathcal{H}_\infty/\mathcal{E}_\infty)^\Phi = \lambda_\phi.\deg(\Phi).$$

La théorie de Kummer permet de ramener la démonstration de ce théorème à l'étude de la Φ^*-partie d'un certain groupe de Galois, Φ^* désignant le caractère miroir de Φ.
En effet, l'extension associée au radical kummérien $\mathcal{H}_\infty/\mathcal{E}_\infty$ est $L_\infty/N_\infty \cap L_\infty$. Le groupe de Galois de cette extension est isomorphe à $\mathrm{Gal}(N_\infty L_\infty/N_\infty)$. Par ailleurs, la théorie de Kummer permet d'établir l'existence d'un pseudo-isomorphisme entre $\mathrm{Gal}(M_\infty/N_\infty)$ et $X_\infty(K_0)$. Le groupe de Galois $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$ représente en quelque sorte la différence entre le radical kummérien $\mathcal{H}_\infty/\mathcal{E}_\infty$ et $X_\infty(K_0)$. La démonstration de l'égalité des rangs annoncée se ramène donc à la démonstration de la trivialité de la Φ^*-partie de ce groupe de Galois, pour un caractère pair Φ de G. Pour démontrer cette trivialité, on adoptera la démarche suivante :
Le groupe de Galois $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$, que l'on considère, est muni d'une structure de Λ-module, comme sous Λ-module de $\mathrm{Gal}(M_\infty/K_\infty)$. Pour montrer la trivialité de la Φ^*-partie de ce module, on va montrer que sa série caractéristique est triviale. Notons $\overline{U}_\infty$ la limite projective relativement à la norme des $\overline{U}_{K_n}$, pro-p-complété des unités de K_n et $\mathcal{U}_\infty = \prod_v \overline{U}_{\infty,v}$, v parcourant l'ensemble des p-places de K_∞ et $\overline{U}_{\infty,v}$ désignant le pro-p-complété du groupe des unités de $K_{\infty,v}$, v-complété de K_∞. La suite exacte de la théorie du Corps de Classes au niveau infini :

$$1 \longrightarrow \overline{U}_\infty \longrightarrow \mathcal{U}_\infty \longrightarrow \mathrm{Gal}(M_\infty/L_\infty) \longrightarrow 1,$$

permet d'obtenir des informations sur la série caractéristique de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$, connaissant celle de $\mathcal{U}_\infty$. On verra que pour un caractère pair Φ, on peut effectivement calculer la série caractéristique de la Λ-torsion de $\mathcal{U}_\infty^{\Phi^*}$, le caractère Φ^* désignant le caractère miroir de Φ. L'ingrédient principal nécessaire pour ce calcul est la suite exacte de Coleman.
Pour finir, on verra que les résultats obtenus permettent de reformuler la conjecture de Greenberg ([8]), qui prédit la finitude de la partie + de $X_\infty(K_0)$.

Corollaire. *Les invariants λ_ϕ des modules $X_\infty(K_0)^\Phi$ sont nuls pour tout caractère pair Φ de G si et seulement si $Gal(L_\infty/N_\infty \cap L_\infty)$ est fini.*

Notons enfin, que les résultats que nous obtenons peuvent être obtenus en utilisant une approche totalement différente. En effet, les idempotents étant dans le cas non-semi-simple des éléments de $\mathbb{Q}_p[G]$, on peut définir la Φ-partie en utilisant ces idempotents de la façon suivante :

- Pour un $\mathbb{Z}_p[G]$-module M, de type fini qui n'est pas de $\mathbb{Z}_p$-torsion, on définit la Φ-partie de M en posant $M^\Phi = e_\Phi(M \otimes \mathbb{Q}_p)$.
- Pour un $\mathbb{Z}_p[G]$-module M de $\mathbb{Z}_p$-torsion, on définit la Φ-partie de M en posant $M^\Phi = e_\Phi(\mathrm{Div}(M))$, $\mathrm{Div}(M)$ désignant le sous-module divisible maximal de M.

L'intérêt de la démarche que nous avons choisie est de proposer une définition unifiée de la notion de Φ-partie, plus générale que celle exposée précédemment dans le sens ou elle peut s'appliquer aux modules de type fini et de $\mathbb{Z}_p$-torsion. Qui plus est, les résultats relatifs aux Φ-parties et Φ-quotients que nous utilisons apparaissent fréquemment dans la litératture, mais ne sont démontrés que rarement et de façon éparse. Nous avons donc choisi de les redémontrer en utilisant une approche aussi élémentaire que possible.

Dans toute la suite, les produits tensoriels, sauf mention expresse du contraire, sont relatifs à $\mathbb{Z}_p$.

1.2 Propriétés algébriques de la Φ-partie

Dans cette section, on considère un groupe abélien fini G, M un $\mathbb{Z}_p[G]$-module de type fini et Φ un caractère $\mathbb{C}_p$-irréductible de G. On va dans cette partie définir la Φ-partie et le Φ-quotient d'un module dans le cas non semi-simple (p divise l'ordre de G). Bien évidemment, les définitions que l'on va introduire restent valable dans le cas semi-simple et coïncident avec la définition usuelle de la Φ-partie.
Par analogie avec le cas semi-simple, on va définir la Φ-partie de M comme "la plus grande partie" de M sur laquelle G agit via Φ. De même le Φ-quotient de M sera "le plus grand quotient" de M sur lequel G agit via Φ.
Une fois ces notions définies, on étudiera certaines de leurs propriétés algébriques, dans le but de pouvoir utiliser ces notions dans le contexte qui nous intéresse.
Les principaux résultats de cette section sont bien connus des spécialistes et par exemple sont énoncés dans [25].
Si Φ désigne un caractère de G, i.e. un morphisme de groupe de G dans $\mathbb{C}_p^*$, on notera $\mathbb{Z}_p[\Phi]$ l'anneau des entiers de $\mathbb{Q}_p(\Phi(G))$.

Définition 1.2.1. *Soit M un $\mathbb{Z}_p[\Phi][G]$-module. On dit que G agit sur M via Φ si l'on a $g.m = \Phi(g)m$ pour tout $(g, m) \in G \times M$.*

On va voir dans un premier temps qu'il existe plusieurs définitions équivalentes de la Φ-partie. Pour alléger les démonstrations, on supposera

dans un premier temps que le groupe G est cyclique, puis on verra que les propriétés obtenues se généralisent sans peine au cas où G est abélien.

1.2.1 Définitions équivalentes de la Φ-partie

Rappelons dans un premier temps, la définition de la Φ-partie d'un $\mathbb{Z}_p[G]$-module dans le cas semi-simple. Dans le cas où l'ordre de G est premier à p, tout $\mathbb{Z}_p[G]$-module M possède une décomposition de la forme $\oplus_\Phi M^\Phi$, Φ parcourant l'ensemble des caractères $\mathbb{C}_p$-irréductible de G. Plus précisément, le module M^Φ est l'image du module M par la multiplication par l'idempotent $e_\Phi = \frac{1}{|G|}\sum_{g\in G}\Phi(g)^{-1}g$. Le fait que l'ordre de G soit premier à p implique que $e_\Phi \in \mathbb{Z}_p[G]$.
Dans le cas non semi-simple, l'idempotent e_Φ est dans $\mathbb{Q}_p[G]$. Si l'on veut utiliser ces idempotents, on doit donc considérer le module $M \otimes \mathbb{Q}_p$, qui est trivial dans le cas où le module M est de torsion et de type fini.
On doit donc, dans le cas non semi-simple, utiliser une autre approche si l'on désire définir la notion de Φ-partie pour un $\mathbb{Z}_p$-module quelconque.
A priori M est un $\mathbb{Z}_p$ module, si l'on veut munir M d'une structure de $\mathbb{Z}_p[\Phi]$-module, il faut considérer le produit tensoriel $M \otimes \mathbb{Z}_p[\Phi]$. L'action de G sur $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Phi]$, peut être définie de deux façons (au moins) :

- En posant pour $g \in G$ et $m \otimes z \in M \otimes \mathbb{Z}_p[\Phi]$:

$$g \star (m \otimes z) = (gm) \otimes (\Phi(g)^{-1}z) \quad \text{(Action } \star\text{)}.$$

- En posant pour $g \in G$ et $m \otimes z \in M \otimes \mathbb{Z}_p[\Phi]$:

$$g.(m \otimes z) = (gm) \otimes z \quad \text{(Action } \odot\text{)}.$$

L'action de G sur $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$ est définie classiquement de la façon suivante :

- On définit pour $(g, f) \in G \times \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$, l'élément $g * f \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$ par

$$g * f(z) = gf(g^{-1}z) \quad \text{(action } *\text{)}.$$

De sorte que $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)^G = \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$.
Par ailleurs, on peut naturellement définir une action de G sur $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$, en définissant pour $(g, f) \in G \times \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$, l'élément $g.f \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$ par

$$g.f(z) = gf(z) \quad \text{(action naturelle)}.$$

On a alors $g.f(z) = g.f(\Phi(g^{-1})\Phi(g)z) = f(\Phi(g)z)$, de sorte que G agit sur $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$ via Φ, avec la structure naturelle de $\mathbb{Z}_p[\Phi]$-module sur $\mathrm{Hom}(\mathbb{Z}_p[\Phi], M)$: $g.f(z) = f(\Phi(g)z)$.
De façon générale, si A et B sont deux $\mathbb{Z}_p[G]$-modules, l'action naturelle

de G sur $\mathrm{Hom}_{\mathbb{Z}_p}(A,B)$ sera l'action $*$, définie de la façon suivante : pour $(g,h) \in G \times \mathrm{Hom}_{\mathbb{Z}_p}(A,B)$, on définit :

$$\begin{array}{rccc} g*h: & A & \to & B \\ & a & \mapsto & gh(g^{-1}a) \end{array}$$

Cas où G est cyclique

Supposons que G est un groupe cyclique et fixons un générateur g de G. Notons $\mathbb{Z}_p[\Phi]$ l'anneau des entiers de $\mathbb{Q}_p(\Phi(G))$, $n = |\Phi(G)|$ et $P_n(X)$ le n-ième polynôme cyclotomique.

Proposition 1.2.2. *Soit M un $\mathbb{Z}_p[G]$-module et Φ un caractère de G. Alors les trois modules suivants peuvent être munis d'une structure de $\mathbb{Z}_p[\Phi]$-module et sont $\mathbb{Z}_p[G]$-isomorphes.*

i) $(M \otimes \mathbb{Z}_p[\Phi])^G$, *les invariants étant pris relativement à l'action* $\star$;

ii) $M^{P_n} := \{m \in M \text{ tels que } P_n(g)m = 0\}$;

iii) $Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$.

Démonstration. Au préalable, remarquons que $(M \otimes \mathbb{Z}_p[\Phi])^G$ est l'ensemble des éléments $\sum_i m_i \otimes z_i \in M \otimes \mathbb{Z}_p[\Phi]$ tels que $\forall g \in G, \sum_i (gm_i) \otimes z_i = \sum_i m_i \otimes (\Phi(g) z_i)$.
On va dans un premier temps construire un morphisme de $Z_p[G]$-module $F_1 : (M \otimes \mathbb{Z}_p[\Phi])^G \to M^{P_n}$.
Posons $n' = \varphi(n) - 1$. Alors $\{\Phi(g^i), 0 \le i \le n'\}$ est une $\mathbb{Z}_p$-base de $\mathbb{Z}_p[\Phi]$. Il s'ensuit que $M \otimes \mathbb{Z}_p[\Phi] = \oplus_{i=0}^{n'} M \otimes \Phi(g^i)$.
Soit donc $m = \sum_{i=0}^{n'} m_i \otimes \Phi(g^i) \in M \otimes \mathbb{Z}_p[\Phi]$. Par définition de $(M \otimes \mathbb{Z}_p[\Phi])^G$, on a

$$m \in (M \otimes \mathbb{Z}_p[\Phi])^G \Leftrightarrow \sum_{i=0}^{n'} (gm_i) \otimes \Phi(g^i) = \sum_{i=0}^{n'} m_i \otimes \Phi(g^{i+1}).$$

Si l'on écrit $P_n(X)$ sous la forme $P_n(X) = X^{n'+1} - \sum_{i=0}^{n'} a_i X^i$, on en déduit le système suivant :

$$m \in (M \otimes \mathbb{Z}_p[\Phi])^G \Leftrightarrow \begin{cases} gm_0 & = & a_0 m_{n'} \\ m_0 + a_1 m_{n'} & = & gm_1 \\ m_1 + a_2 m_{n'} & = & gm_2 \\ \vdots & & \vdots \\ m_{n'-1} + a_{n'} m_{n'} & = & gm_{n'} \end{cases} \tag{1.1}$$

Ce système comporte $n'+1$ équations. On peut utiliser les n' premières équations pour exprimer $m_1 \cdots, m_{n'}$ en fonction de m_0, la dernière équation

donnera une contrainte sur m_0. On obtient donc :

$$\begin{array}{rcll} m_{n'} & = & \frac{g.m_0}{a_0} & (E_{n'}) \\ m_1 & = & \frac{g^{-1}}{a_0}(a_0 m_0 + a_1 g.m_0) & (E_1) \\ m_2 & = & \frac{g^{-2}}{a_0}(a_0 m_0 + a_1 g.m_0 + a_2 g^2.m_0) & (E_2) \\ \vdots & = & \vdots & \\ m_i & = & \frac{g^{-i}}{a_0}(a_0 m_0 + a_1 g.m_0 + \cdots \quad a_i g^i.m_0) & (E_i) \\ \vdots & = & \vdots & \\ m_0 & = & g^{-(n'+1)}(\sum_{i=0}^{n'} a_i g^i m_0) & (C) \end{array}$$

Or il est clair que $(C) \Leftrightarrow P_n(g)m_0 = 0$. On peut donc définir un morphisme de $\mathbb{Z}_p$-modules $F_1 : (M \otimes \mathbb{Z}_p[\Phi])^G \to M^{P_n}$, en posant $F(m) = m_0$. Ce morphisme est clairement injectif. De plus les équations $(E_1, \cdots, E_{n'})$ permettent de calculer explicitement l'image réciproque d'un élément $m_0 \in M^{P_n}$ par F_1. Ce morphisme est donc surjectif. On en déduit donc que les modules $i)$ et $ii)$ sont $\mathbb{Z}_p$-isomorphes. Par ailleurs, il est clair que F_1 est G linéaire. En effet, soit $m = \sum_{i=0}^{n'} m_i \otimes \Phi(g^i) \in (M \otimes \mathbb{Z}_p[\Phi])^G$. On a alors $F_1(gm) = F_1(\sum_{i=0}^{n'}(gm_i) \otimes \Phi(g^i)) = gm_0 = gF_1(m)$. Finalement F_1 est bien $\mathbb{Z}_p[G]$-linéaire (l'action de G sur $(M \otimes \mathbb{Z}_p[\Phi])^G$ étant l'action $\odot$).

Donnons nous maintenant un élément $m_0 \in M^{P_n}$ et définissons $f \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$ en posant

$$f(\Phi(g^i)) = g^i.m_0$$

pour $0 \leq i \leq n'$. Nous devons montrer que f est $\mathbb{Z}_p[G]$-linéaire. Par $\mathbb{Z}_p$-linéarité de f et par cyclicité de G, il suffit de vérifier que $f(\Phi(g^{i+1})) = g^{i+1}.m_0$ pour $i \in \{0, \cdots, n'\}$. Ces égalités découlent de la définition de f pour $i = 0, \cdots, n'-1$. De plus

$$\begin{array}{rcll} f(\Phi(g^{n'+1})) & = & f(\sum_{i=0}^{n'} a_i g^i) & \\ & = & a_i f(\sum_{i=0}^{n'} g^i) & \\ & = & \sum_{i=0}^{n'} a_i g^i m_0 & \\ & = & g^{n'+1} m_0 & (\text{ du fait que } m_0 \in M^{P_n}) \\ & = & g f(\Phi(g^{n'})). & \end{array}$$

Le morphisme f est donc bien $\mathbb{Z}_p[G]$-linéaire. Par ailleurs, le calcul précédent montre que l'élément $f \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$ est $\mathbb{Z}_p[G]$-linéaire du fait que $f(1) \in M^{P_n}$. On peut donc définir de façon évidente un $\mathbb{Z}_p$-morphisme $F_2 : M^{P_n} \to \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$, qui est clairement injectif. De plus, étant donné $f \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$, on a par $\mathbb{Z}_p[G]$-linéarité de f, $P_n(g)f(1) = 0$. Il est alors clair que $f = F_2(f(1))$. Le morphisme F_2 est donc surjectif. Les modules $ii)$ et $iii)$ sont donc bien $\mathbb{Z}_p$-isomorphes. Par ailleurs F_2 est clairement G-linéaire, l'action de G sur $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$ étant l'action naturelle définie précédemment. □

Définition 1.2.3. *Soit M un $\mathbb{Z}_p[G]$-module et Φ un caractère de G. On définit la Φ-partie de M, que l'on note M^Φ, par :*

$$M^\Phi = (M \otimes \mathbb{Z}_p[\Phi])^G,$$

les invariants étant pris relativement à l'action $\star$.

Exemple 1.2.4. *Considérons $M = \mathbb{Z}_p^3$ et $G = \mathbb{Z}/3\mathbb{Z}$. Si g désigne un générateur de G, on définit l'action de G sur M en posant*

$$\rho(g) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}.$$

Considérons le caractère Φ de G, défini par $\Phi(g) = j$.
Si on veut déterminer M^Φ en utilisant la définition ii), il suffit de calculer le noyau de $id + \rho(g) + \rho(g)^2 = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, alors que si l'on utilise la définition i), on doit calculer le noyau de $j^2\rho_(g) - id = \begin{bmatrix} j^2-1 & 0 & 0 \\ 0 & -1 & -j^2 \\ 0 & j^2 & -j^2-1 \end{bmatrix}$. La définition ii) permet donc, dans le cas où G est cyclique, de déterminer M^ϕ avec des calculs plus simples.

Par ailleurs, de la définition *ii*) de la Φ-partie, on déduit les corollaires suivants :

Corollaire 1.2.5. *Soit M un $\mathbb{Z}_p[G]$-module et Φ un caractère $\mathbb{C}_p$-irréductible de G, groupe cyclique fini. Alors M^Φ s'injecte de façon naturelle dans M.*

Corollaire 1.2.6. *Soit M un $\mathbb{Z}_p[G]$-module, Φ et Φ' deux caractères $\mathbb{C}_p$-irréductible de G, groupe cyclique fini, tels qu'il existe $\sigma \in Gal(\mathbb{Q}_p(\Phi(G))/\mathbb{Q}_p)$ vérifiant $\Phi' = \sigma \circ \Phi$. Alors M^Φ et $M^{\Phi'}$ sont canoniquement isomorphes.*

Cas où G est abélien

On a vu comment définir la Φ-partie d'un $\mathbb{Z}_p[G]$-module, lorsque G est un groupe cyclique.
On va maintenant généraliser les définitions précédentes, dans le cas où G est abélien. Soit donc G un groupe abélien, Φ un caractère $\mathbb{C}_p$-irréductible de G et $G_1 = \ker(\Phi)$, de sorte que : $\Phi(G) \simeq G/G_1$. Le groupe G/G_1 est cyclique, car isomorphe à un groupe de racines de l'unité. Rappelons aussi que tout G-module sur lequel G_1 agit trivialement peut être muni d'une structure naturelle de $\mathbb{Z}_p[\Phi(G)]$-module.

Lemme 1.2.7. *Soit M un $\mathbb{Z}_p[G]$-module, on munit $M \otimes \mathbb{Z}_p[\Phi]$ de l'action $\star$. Alors :*

i) $(M \otimes \mathbb{Z}_p[\Phi])^G = (M^{G_1} \otimes \mathbb{Z}_p[\Phi])^{G/G_1}$,

ii) $Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M) = Hom_{\mathbb{Z}_p[G/G_1]}(\mathbb{Z}_p[\Phi], M^{G_1})$.

Démonstration. Soit $m = \sum_{i=0}^{n'} m_i \otimes \Phi(g^i) \in (M \otimes \mathbb{Z}_p[\Phi])^G$. Le fait que m soit G-invariant relativement à l'action $\star$ et le fait que G_1 agisse trivialement sur $\mathbb{Z}_p[\Phi]$ impliquent que $\sum_{i=0}^{n'} gm_i \otimes \Phi(g^i) = \sum_{i=0}^{n'} m_i \otimes \Phi(g^i), \forall g \in G_1$. Il s'ensuit que $m_i \in M^{G_1}, \forall i \in \{0, \cdots, n'\}$. Pour l'action $\star$ des deux côtés, on constate aussi des égalités :

$$(M \otimes \mathbb{Z}_p[\Phi])^G = (M^{G_1} \otimes \mathbb{Z}_p[\Phi])^G = (M^{G_1} \otimes \mathbb{Z}_p[\Phi])^{G/G_1}.$$

Soit maintenant $f \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$. L'action de G_1 sur $\mathbb{Z}_p[\Phi]$ étant triviale, on a pour $g \in G_1$, $gf(z) = f(z)$ et donc $f(\mathbb{Z}_p[\Phi]) \subset M^{G_1}$. On peut alors définir de façon naturelle un $\mathbb{Z}_p$-isomorphisme

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M) \to \mathrm{Hom}_{\mathbb{Z}_p[G/G_1]}(\mathbb{Z}_p[\Phi], M^{G_1}),$$

qui est clairement G-linéaire. (A priori le module de gauche est un $\mathbb{Z}_p[G]$-module et celui de droite un $\mathbb{Z}_p[G/G_1]$-module, cependant l'action de G_1 étant triviale sur le module de gauche, il est naturellement muni d'une structure de $\mathbb{Z}_p[G/G_1]$-module.)

□

Proposition 1.2.8. *Soient M un $\mathbb{Z}_p[G]$-module, Φ un caractère de G, $G_1 = \ker(\Phi)$ et n l'ordre de G/G_1. Alors les trois modules suivants sont $\mathbb{Z}_p[G]$-isomorphes :*

i) $(M \otimes \mathbb{Z}_p[\Phi])^G$, *les invariants étant pris relativement à l'action* $\star$,

ii) $(M^{G_1})^{P_n} := \{m \in M^{G_1}$ *tels que* $P_n(g)m = 0\}$,

iii) $Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$.

Démonstration. D'après le lemme précédent, on dispose de $\mathbb{Z}_p[G]$-isomorphismes

$$(M \otimes \mathbb{Z}_p[\Phi])^G \to (M^{G_1} \otimes \mathbb{Z}_p[\Phi])^{G/G_1}$$

et

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M) \to \mathrm{Hom}_{\mathbb{Z}_p[G/G_1]}(\mathbb{Z}_p[\Phi], M^{G_1}).$$

Or d'après la proposition 1.2.2,

$$(M^{G_1} \otimes \mathbb{Z}_p[\Phi])^{G/G_1} \simeq (M^{G_1})^{P_n} \simeq \mathrm{Hom}_{\mathbb{Z}_p[G/G_1]}(\mathbb{Z}_p[\Phi], M^{G_1}),$$

les isomorphismes étant $\mathbb{Z}_p[G/G_1]$-linéaires. On en déduit l'existence d'isomorphismes $(M \otimes \mathbb{Z}_p[\Phi])^G \simeq (M^{G_1})^{P_n} \simeq \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$. Ces trois modules sont des $\mathbb{Z}_p[G]$-modules, sur lesquels G_1 agit trivialement, ce sont donc des $\mathbb{Z}_p[G/G_1]$-modules et les isomorphismes considérés sont clairement $\mathbb{Z}_p[G/G_1]$-linéaires et donc $\mathbb{Z}_p[G]$-linéaires. □

On déduit de cette propriété le corollaire suivant :

Corollaire 1.2.9. *Soit G un groupe abélien et M un $\mathbb{Z}_p[G]$-module, alors M^Φ s'injecte canoniquement dans M.*

1.2.2 Définition du Φ-quotient

On a vu que la Φ-partie d'un module M pouvait être définie comme l'ensemble des éléments de $M \otimes \mathbb{Z}_p[\Phi]$, qui sont G-invariants, l'action de G étant l'action $\star$. On va voir que $(M \otimes \mathbb{Z}_p[\Phi])_G$ peut être considéré comme le Φ-quotient de M, dans le sens où c'est le plus grand quotient de $M \otimes \mathbb{Z}_p[\Phi]$ sur lequel G agit via Φ. Par ailleurs, il existe aussi dans ce cas, deux définitions équivalentes du Φ-quotient, le Φ-quotient d'un $\mathbb{Z}_p[G]$-module M étant défini naturellement de la façon suivante :

Définition 1.2.10. *Soit M un $\mathbb{Z}_p[G]$-module et Φ un caractère de G. Le Φ-quotient de M, que l'on note M_Φ, est par définition :*

$$M_\Phi = (M \otimes \mathbb{Z}_p[\Phi])_G,$$

les coinvariants étant pris relativement à l'action $\star$.

Proposition 1.2.11. *Soit M un $\mathbb{Z}_p[G]$-module. Les modules suivants sont $\mathbb{Z}_p[G]$-isomorphes :*

1. *$(M \otimes \mathbb{Z}_p[\Phi])_G$, l'action de G sur $M \otimes \mathbb{Z}_p[\Phi]$ étant l'action $\star$,*
2. *$M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\Phi]$.*

Démonstration. Une fois que l'on a pris les G-coinvariants, l'action de G sur $(M \otimes \mathbb{Z}_p[\Phi])_G$ induite par l'action $\star$ est triviale. Cependant l'action $\odot$ induit également une action de G sur $(M \otimes \mathbb{Z}_p[\Phi])_G$. Dans la suite, on considérera que cette action est l'action naturelle de G sur $(M \otimes \mathbb{Z}_p[\Phi])_G$.
Considérons le diagramme suivant, dans lequel la projection p_2 est clairement surjective :

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ & & & & \ker(p_2) & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & I_G(M \otimes \mathbb{Z}_p[\Phi]) & \longrightarrow & M \otimes \mathbb{Z}_p[\Phi] & \xrightarrow{p_1} & M_\Phi & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle p_2} & & & & \\ & & & & M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\Phi] & & & & \\ & & & & \downarrow & & & & \\ & & & & 0 & & & & \end{array}$$

Montrons que $\ker(p_1) = \ker(p_2)$.
Soit $m = (g-1) \star (\sum_i m_i \otimes z_i) \in I_G(M \otimes \mathbb{Z}_p[\Phi])$. On a alors dans

$M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\Phi]$:

$$\begin{array}{rcll} p_2(m) & = & \sum_i (gm_i) \otimes \Phi(g^{-1}) z_i - \sum_i m_i \otimes z_i & \\ & = & \sum_i m_i \otimes z_i - \sum_i m_i \otimes z_i & \text{par } \mathbb{Z}_p[G] - \text{linéarité} \\ & = & 0 & \end{array}$$

Donc $\ker(p_1) \subset \ker(p_2)$.
Réciproquement, soit $m \in \ker(p_2)$. On peut écrire m sous la forme $m = \sum_i m_i \otimes \Phi(g_i)$. On a $p_2(m) = 0 \Leftrightarrow \sum_i m_i \otimes \Phi(g_i) = 0 \Leftrightarrow \sum_i g_i m_i \otimes 1 = 0$ (ces calculs étant effectués dans $M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\Phi]$), on a par conséquent $\sum_i g_i m_i = 0$. Or

$$\begin{array}{rcl} \sum_i m_i \otimes \Phi(g_i) & = & \sum_i m_i \otimes \Phi(g_i) - \sum_i g_i m_i \otimes 1 \\ & = & \sum_i m_i \otimes \Phi(g_i) - \sum_i g_i \star (m_i \otimes \Phi(g_i)) \\ & = & \sum_i (1 - g_i) \star (m_i \otimes \Phi(g_i)). \end{array}$$

On a donc $m \in I_G(M \otimes \mathbb{Z}_p[\Phi]) = \ker(p_2)$ et finalement $\ker(p_2) \subset \ker(p_1)$.
On déduit donc de la surjectivité de p_2 et de l'égalité $\ker(p_1) = \ker(p_2)$, l'existence d'un $\mathbb{Z}_p$-isomorphisme canonique entre M_Φ et $M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\Phi]$. De plus cet isomorphisme est clairement G-linéaire pour l'action $\odot$. □

1.2.3 Interprétation cohomologique des Φ-parties et Φ-quotients.

Étant donné un $\mathbb{Z}_p[G]$-module M et un caractère $\mathbb{C}_p$-irréductible Φ de G, on a vu que M^Φ et M_Φ étaient respectivement définis comme les G-invariants et G-coinvariants du module $M \otimes \mathbb{Z}_p[\Phi]$, muni de l'action $\star$. En d'autres termes $M^\Phi = H^0(G, M \otimes \mathbb{Z}_p[\Phi])$ et $M_\Phi = H_0(G, M \otimes \mathbb{Z}_p[\Phi])$. Par conséquent, on dispose d'un morphisme naturel $M_\Phi \to M^\Phi$, dont les noyaux et conoyaux sont tués par l'ordre de G. On va voir que dans le cas où M est un $\Lambda[G]$-module et sous certaines hypothèses, ce morphisme réalise un quasi-isomorphisme entre M_Φ et M^Φ. Ces $\Lambda[\Phi]$-modules auront alors même invariants.
Pour alléger les notations, introduisons la définition suivante :

Définition 1.2.12. *Soit M un $\mathbb{Z}_p[G]$-module et Φ un caractère de G. On note $M^\bullet$ le module $M \otimes \mathbb{Z}_p[\Phi]$, muni de l'action $\star$.*

On dispose alors d'une suite exacte :

$$1 \longrightarrow \hat{H}^{-1}(G, M^\bullet) \longrightarrow H_0(G, M^\bullet) \xrightarrow{N_G} H^0(G, M^\bullet) \longrightarrow \hat{H}^0(G, M^\bullet) \longrightarrow 1 \,, \tag{1.2}$$

où $N_G = \sum_{g \in G} g \in \mathbb{Z}_p[G]$. En conséquence, $\ker(N_G)$ et $\mathrm{coker}(N_G)$ sont tués par l'ordre de G.

Application aux Λ-modules

Notons Λ l'anneau $\mathbb{Z}_p[[T]]$. On va voir que la suite exacte 1.2 permet d'établir quelques résultats relatifs aux Φ-parties et Φ-quotients d'un Λ-module M. Rappelons que si deux Λ-modules M et N sont pseudo-isomorphes, on note $M \sim N$. Le théorème suivant donne alors la structure d'un Λ-module de type fini.

Théorème 1.2.13. *Soit M un Λ-module de type fini. Il existe alors des entiers m_i et des polynômes distingués f_j tels que :*

$$M \sim \Lambda^r \oplus (\oplus_i \Lambda/p^{m_i}) \oplus (\oplus_j \Lambda/f_j).$$

Les nombres $\mu = \sum_i m_i$ et $\lambda = \sum_j deg(f_j)$ ne dépendent que du module M, on les appelle invariants λ et μ du module M.
La série caractéristique de M est par définition $f = \prod_j f_j$, elle est définie au produit par un élément de Λ^* près et est notée $sc(M)$.

Proposition 1.2.14. *Soit M un $\Lambda[G]$-module de type fini et de Λ-torsion, dont l'invariant μ est nul. Alors M^Φ et M_Φ sont pseudo-isomorphes.*

Démonstration. Compte tenu de la suite exacte 1.2, il suffit de vérifier que $\hat{H}^{-1}(G, M^\bullet)$ et $\hat{H}^0(G, M^\bullet)$ sont finis. Or le fait que M soit de type fini, de Λ-torsion et que $\mu(M) = 0$ implique que M^Φ et M_Φ sont de type fini, de Λ-torsion et que leurs invariants μ sont nuls. Par conséquent $\hat{H}^{-1}(G, M^\bullet)$ et $\hat{H}^0(G, M^\bullet)$ sont des Λ-modules de torsion, de type fini et leurs invariants μ sont nuls. Comme ils sont tués par l'ordre de G, ils sont nécessairement finis. L'application N_G apparaissant dans la suite exacte 1.2 est donc un quasi-isomorphisme entre M_Φ et M^Φ. □

Corollaire 1.2.15. *Soit M un $\mathbb{Z}_p$-module de type fini, alors M_Φ et M^Φ ont même $\mathbb{Z}_p$-rang.*

Démonstration. Si on fait agir Γ de façon triviale sur M, on le munit d'une structure de Λ-module. D'après la proposition précédente, M_Φ et M^Φ sont quasi-isomorphes. Le corollaire découle du fait que le $\mathbb{Z}_p$-rang de M_Φ (respectivement M^Φ) n'est autre que l'invariant λ de M_Φ (respectivement M^Φ). □

1.3 Caractères et dualité de Kummer

Lorsque l'on utilise la théorie de Kummer, on obtient en général des accouplements non-dégénérés $G \times \mathcal{H} \to \mu_{p^\infty}$, où G désigne le groupe de Galois d'une pro-p- extension de K_∞, $\mathcal{H}$ le radical Kummérien associé et μ_{p^∞}, le groupe des racines p-primaires de l'unité. De ces accouplements, on déduit un isomorphisme entre G et $\mathrm{Hom}(\mathcal{H}, \mu_{p^\infty})$. Or $\mathrm{Hom}(\mathcal{H}, \mu_{p^\infty})$ est le

dual de Pontryagin de $\mathcal{H}$, sur lequel l'action de Γ a été tordu une fois à la Tate via le caractère cyclotomique (la définition de l'action tordue est donnée définition 1.3.5). Si l'on veut pouvoir utiliser les outils algébriques introduits précédemment (Φ-partie et Φ-quotient), dans le cadre de la théorie de Kummer, il est naturel d'une part de s'intéresser aux relations existant entre Φ-partie et dual de Pontryagin et d'autre part de comprendre la Φ-partie d'un module tordu.

1.3.1 Φ-partie, Φ-quotient et dual de Pontryagin

Dans cette partie, G désigne un groupe abélien et M désigne un $\mathbb{Z}_p[G]$-module, qui est compact ou discret. Le but de cette partie est d'expliciter la Φ-partie et le Φ-quotient de $M^\vee := \mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$. L'action de G sur $M^\vee$ est l'action $*$, le groupe G agissant trivialement sur $\mathbb{Q}_p/\mathbb{Z}_p$.
On sait que la dualité de Pontryagin transforme les invariants en coinvariants et réciproquement, plus précisément :

Proposition 1.3.1. *Soit M un $\mathbb{Z}_p[G]$-module, alors $(M^\vee)^G = (M_G)^\vee$ et $(M^\vee)_G = (M^G)^\vee$, l'action de G sur $M^\vee$ étant l'action $*$.*

Compte tenu des définitions des Φ-parties et Φ-quotients, une première étape pour comprendre ces interactions va être de comparer $\mathbb{Z}_p[\Phi] \otimes M^\vee$ et $\mathrm{Hom}(\mathbb{Z}_p[\Phi], M)$, le groupe G agissant diagonalement sur $\mathbb{Z}_p[\Phi] \otimes M^\vee$ et via $*$ sur $\mathrm{Hom}(\mathbb{Z}_p[\Phi], M)$.
Fixons $g \in G$ tel que $\Phi(g)$ engendre $\Phi(G)$. Le degré de l'extension $\mathbb{Q}_p(\Phi(G)/\mathbb{Q}_p$ est alors $\varphi(n)$, n désignant l'ordre de $\Phi(G)$. On dispose alors d'une $\mathbb{Z}_p$-base $(1, \Phi(g), \cdots, \Phi(g^{n'})$ de $\mathbb{Z}_p[\Phi]$, avec $n' = \varphi(n)-1$. Tout élément de $f \in \mathbb{Z}_p[\Phi] \otimes M^\vee$ s'écrit de façon unique sous la forme $f = \sum_{i=0}^{n'} \Phi(g^i) \otimes f_i$, avec $f_i \in M^\vee$. Définissons alors l'élément $\theta(f) \in \mathrm{Hom}(\mathbb{Z}_p[\Phi], M)^\vee$ en posant pour $h \in \mathrm{Hom}(\mathbb{Z}_p[\Phi], M)$:

$$\theta(f)(h) = \sum_{i=1}^{n'} f_i(h(\Phi(g^i))). \tag{1.3}$$

Proposition 1.3.2. *Le $\mathbb{Z}_p$-morphisme $\theta : \mathbb{Z}_p[\Phi] \otimes M^\vee \to Hom(\mathbb{Z}_p[\Phi], M)^\vee$, défini en 1.3, est un isomorphisme de $\mathbb{Z}_p[G]$-modules.*

Démonstration. Nous devons vérifier d'une part que θ est un $\mathbb{Z}_p$-isomorphisme et d'autre part que c'est un isomorphisme de $\mathbb{Z}_p[G]$-modules.

Montrons tout d'abord que θ est injectif. Soit $f = \sum_{i=0}^{n'} \Phi(g^i) f_i$ tel que $\theta(f) = 0$. On a alors $\theta(f)(h) = 0$ pour tout $h \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$.
Définissons pour $i \in \{0, \cdots, n'\}$ l'élément $h_{m,i} \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$ par $h_{m,i}(\Phi(g^j)) = m\delta_{i,j}$.

On a alors pour $i_0 \in \{0, \cdots, n'\}$ et $m \in M$, $\theta(f)(h_{m,i_0}) = 0 \Leftrightarrow \sum_{i=0}^{n'} f_i(\delta_{i,i_0} m) = 0 \Leftrightarrow f_{i_0}(m) = 0$. On a donc $f_{i_0} = 0$ quel que soit i_0 et par suite $f = 0$. Le morphisme θ est donc bien injectif.

Montrons que θ est surjectif. Soit donc $F \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)^\vee$. On a pour $h \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$, $F(h) = \sum_{i=0}^{n'} F(h_i)$, avec $h_i = h \circ \pi_i$, π_i désignant la projection de $\mathbb{Z}_p[\Phi]$ sur $\Phi(g^i)\mathbb{Z}_p$ et dans la direction $\oplus_{j \neq i} \Phi(g^j)\mathbb{Z}_p$. Nous allons construire un antécédent de F.
Soit $m \in M$. On définit $h_m^i \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Phi], M)$ par $h_m^i(\Phi(g^j)) = m\delta_{i,j}$ pour $1 \leq i, j \leq n'$, puis un élément f_i de $M^\vee$ en posant $f_i(m) = F(h_m^i)$.
On a alors $\theta(\sum_{i=0}^{n'} \Phi(g^i) \otimes f_i)(h) = \sum_{i=0}^{n'} f_i(h(\Phi(g^i)))$. Or par définition de f_i, on a $f_i(h(\Phi(g^i))) = F(h_i)$. On en déduit que $\sum_{i=0}^{n'} \Phi(g^i) \otimes f_i$ est bien un antécédent de F et donc θ est bien surjectif.
On doit maintenant étudier la G-linéarité de θ. Rappelons au préalable la façon dont G agit sur les divers modules que l'on utilise :

- l'action de G sur les modules du type $\mathrm{Hom}_{\mathbb{Z}_p}(A, B)$ est l'action $*$.
- l'action de G sur $\mathbb{Z}_p[\Phi] \otimes M^\vee$ est l'action diagonale, G agissant sur $\mathbb{Z}_p[\Phi]$ via Φ et sur $M^\vee$ via $*$. On la notera abusivement $*$.

Remarquons que tout élément de G s'écrit sous la forme kg^a avec $k \in \ker(\Phi)$ et $a \in \mathbb{N}$, où g est un élément de G tel que $\Phi(g)$ engendre $\Phi(G)$. Pour montrer que θ est G-linéaire, on doit donc montrer que $\theta(g*f) = g*\theta(f)$ et que $\theta(k*f) = k*\theta(f)$, pour tout $k \in \ker(\Phi)$.
Soit $f = \sum_{i=0}^{n'} \Phi(g^i) \otimes f_i \in \mathbb{Z}_p[\Phi] \otimes M^\vee$.
On va dans un premier temps montrer que $\theta(g*f) = g*\theta(f)$. Pour cela, notons n l'ordre de $\Phi(G)$ et écrivons $P_n(X)$, n-ième polynôme cyclotomique, sous la forme $P_n(X) = X^{n'+1} - \sum_{i=0}^{n'} a_i X^i$. On a alors $g*f = \sum_{i=0}^{n'} \Phi(g^{i+1}) \otimes g*f_i = \sum_{i=0}^{n'-1} \Phi(g^{i+1}) \otimes g*f_i + \sum_{i=0}^{n'} a_i \Phi(g^i) \otimes g*f_{n'}$.
D'une part

$$\begin{array}{rcl} \theta(g*f)(h) & = & \sum_{i=0}^{n'-1} g*f_i(h(\Phi(g^{i+1}))) + \sum_{i=0}^{n'} g*f_{n'}(h(a_i\Phi(g^i))) \\ & = & \sum_{i=0}^{n'-1} g*f_i(h(\Phi(g^{i+1}))) + g*f_{n'}(h(\sum_{i=0}^{n'} a_i\Phi(g^i))) \\ & = & \sum_{i=0}^{n'} g*f_i(h(\Phi(g^{i+1}))) \end{array}$$

d'autre part

$$\begin{array}{rcl} g*\theta(f)(h) & = & \theta(f)(g^{-1}*h) \\ & = & \sum_{i=0}^{n'} f_i(g^{-1}*h(\Phi(g^i))) \\ & = & \sum_{i=0}^{n'} f_i(g^{-1}h(\Phi(g^{i+1}))) \\ & = & \sum_{i=0}^{n'} g*f_i(h(\Phi(g^{i+1}))). \end{array}$$

On a donc bien $g*\theta(f) = \theta(g*f)$.

Par ailleurs $k * f = \sum_{i=0}^{n'} \Phi(g^i) \otimes k * f_i$, par conséquent :

$$\begin{array}{rcl} k * (\theta(f))(h) & = & \theta(f)(k^{-1} * h) \\ & = & \sum_{i=0}^{n'} f_i(k^{-1}h(\Phi(k)\Phi(g^i))) \\ & = & \sum_{i=0}^{n'} f_i(k^{-1}h(\Phi(g^i))) \\ & = & \sum_{i=0}^{n'} k * f_i(h(\Phi(g^i))) \\ & = & \theta(\sum_{i=0}^{n'} \Phi(g^i) \otimes k * f_i)(h) \\ & = & \theta(k * f)(h). \end{array}$$

Il s'ensuit que l'on a bien $\theta(g' * f) = g' * \theta(f)$ pour tout $g' \in G$. □

Remarque. *La proposition précédente apparaît dans un cadre plus général dans [21] (cor. 5.2.9 page 232).*

Proposition 1.3.3. *Soit M un $\mathbb{Z}_p[G]$-module, compact ou discret, et Φ un caractère de G. Alors :*

i) $(M^\vee)_\Phi = (M^{\Phi^{-1}})^\vee$,

ii) $(M^\vee)^\Phi = (M_{\Phi^{-1}})^\vee$.

Démonstration. Notons $\widetilde{\mathbb{Z}_p[\Phi]}$ le module $\mathbb{Z}_p[\Phi]$ sur lequel l'opération de G est définie par :

$$\begin{array}{rcl} G \times \mathbb{Z}_p[\Phi] & \to & \mathbb{Z}_p[\Phi] \\ (g, z) & \mapsto & \Phi(g^{-1}).z \end{array} .$$

Rappelons que $M_\Phi = (\mathbb{Z}_p[\Phi] \otimes M)_G$, les G-coinvariants étant relatifs à l'action $\star$. En d'autres termes, $M_\Phi = (\widetilde{\mathbb{Z}_p[\Phi]} \otimes M)_G$, les G-coinvariants étant relatifs à l'action diagonale de G sur $\widetilde{\mathbb{Z}_p[\Phi]} \otimes M$.
De plus si G agit sur $\mathrm{Hom}_{\mathbb{Z}_p}(\widetilde{\mathbb{Z}_p[\Phi]}, M)$ via l'action $*$, alors $\mathrm{Hom}_{\mathbb{Z}_p}(\widetilde{\mathbb{Z}_p[\Phi]}, M)^G = \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widetilde{\mathbb{Z}_p[\Phi]}, M)$. Utilisant le lemme précédent, on obtient alors :

$$\begin{array}{rcl} (M^\vee)_\Phi & = & (\widetilde{\mathbb{Z}_p[\Phi]} \otimes_{\mathbb{Z}_p} M^\vee)_G \\ & = & (\mathrm{Hom}_{\mathbb{Z}_p}(\widetilde{\mathbb{Z}_p[\Phi]}, M)^\vee)_G \\ & = & (\mathrm{Hom}_{\mathbb{Z}_p}(\widetilde{\mathbb{Z}_p[\Phi]}, M)^G)^\vee \\ & = & \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widetilde{\mathbb{Z}_p[\Phi]}, M)^\vee \\ & = & (M^{\Phi^{-1}})^\vee. \end{array}$$

La partie i) du corollaire est donc démontrée. Pour la partie ii), il suffit d'appliquer la partie i) au module $M^\vee$ et d'utiliser le fait que $(M^\vee)^\vee = M$, M étant compact ou discret. □

1.3.2 Φ partie d'un module tordu

On a déjà étudié les relations entre Φ-partie et dual de Pontryagin. Or les modules apparaissant lorsque on utilise la dualité de Kummer sont des duaux de Pontryagin sur lesquels l'action de G a été tordu, via le caractère cyclotomique. Nous devons donc comprendre les relations entre Φ-partie d'un module tordu et tordu de la Φ-partie. Pour cela on doit préciser un peu le cadre dans lequel on travaille. Rappelons au préalable la définition du caractère cyclotomique κ :

Proposition 1.3.4. *L'application κ : $Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^*$, qui a un élément $g \in Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ associe l'unique élément $\kappa(g) \in \mathbb{Z}_p$ tel que $g(\zeta_{p^n}) = \zeta_{p^n}^{\kappa(g)}, \forall n \in \mathbb{N}$, est un isomorphisme de groupe appelé caractère cyclotomique.*

Rappelons que $F/\mathbb{Q}$ est une extension abélienne totalement réelle de $\mathbb{Q}$, qui est supposée modérément ramifiée.
Par conséquent l'extension $K_0/\mathbb{Q}$ est également modérément ramifiée, de sorte que $\mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq \mathrm{Gal}(K_\infty/K_0) \times \mathrm{Gal}(K_0/\mathbb{Q})$. Notons $\Gamma = \mathrm{Gal}(K_\infty/K_0)$ et $G = \mathrm{Gal}(K_0/\mathbb{Q})$. Le caractère cyclotomique κ est défini sur $\mathrm{Gal}(K_\infty/\mathbb{Q})$, car K_∞ contient les racines p-primaires de l'unité. On peut par conséquent considérer la restriction de κ à Γ et G, qui sont des sous groupes de $\mathrm{Gal}(K_\infty/\mathbb{Q})$.
Donnons nous maintenant un $\mathbb{Z}_p[\Gamma \times G]$-module M.

Définition 1.3.5. *Le module $M(i)$ est le module M sur lequel l'action de $\Gamma \times G$ est définie de la façon suivante :*

$$\begin{array}{ccc} (\Gamma \times G) \times M(i) & \to & M(i) \\ (\gamma g, m) & \mapsto & \kappa(\gamma g)^i \gamma g m \end{array} \tag{1.4}$$

On dit que $M(i)$ est le module M, sur lequel l'action de G a été tordue i-fois par le caractère cyclotomique κ.

On peut alors énoncer la propriété suivante :

Proposition 1.3.6. *Soit M un $\mathbb{Z}_p[\Gamma \times G]$-module, $M(i)$ le module M sur lequel l'action de $\Gamma \times G$ a été tordue i fois via le caractère cyclotomique. Alors pour tout caractère Φ de G, on a :*

$$(M(i))^\Phi \simeq (M^{\omega^{-i}\Phi})(i) \text{ et } (M(i))_\Phi \simeq (M_{\omega^{-i}\Phi})(i),$$

où ω désigne la restriction de κ à G.

Démonstration. Notons $M^\bullet = M \otimes \mathbb{Z}_p[\Phi]$. Par définition $M^\Phi = (M^\bullet)^G$, l'action de G sur $M^\bullet$ étant l'action $\star$. Soit maintenant $\sum_j m_j \otimes z_j \in (M(i))^\Phi$,

on a alors pour $g \in G$

$$\begin{array}{rcl} g \star \sum_j m_j \otimes z_j & = & \sum_j m_j \otimes z_j \\ \Leftrightarrow \quad \sum_j (\omega^i(g) g.m_j) \otimes (\Phi(g^{(-1)} z_j) & = & \sum_j m_j \otimes z_j \\ \Leftrightarrow \quad \sum_j (g.m_j) \otimes (\omega^i(g) \Phi(g^{(-1)} z_j) & = & \sum_j m_j \otimes z_j \\ \Leftrightarrow \quad \sum_j (g.m_j) \otimes (\omega^{-i} \Phi(g^{(-1)} z_j) & = & \sum_j m_j \otimes z_j \quad . \end{array}$$

On en déduit un isomorphisme naturel $(M(i))^\Phi \to M^{\omega^{-i}\Phi}$. On obtient de même un isomorphisme entre $(M(i))_\Phi$ et $M_{\omega^{-i}\Phi}$.

Cependant les isomorphismes que l'on obtient ne sont a priori que des $\mathbb{Z}_p$-isomorphismes. Examinons de plus près l'action de G sur chacun de ces modules. L'action naturelle de G sur M^Φ est l'action $\odot$. Par conséquent, on a pour $m = \sum_j m_j \otimes z_j \in (M(i))^\Phi$ et $\gamma g \in \Gamma \times G$: $\gamma g.m = \sum_j (\kappa(\gamma g)^i \gamma g m_j) \otimes z_j$.
Par conséquent le $\mathbb{Z}_p$-isomorphisme canonique considéré précédemment, réalise un $\mathbb{Z}_p[\Gamma \times G]$-isomorphisme entre $M(i)^\Phi$ et $M^{\omega^{-i}\Phi}(i)$.

□

1.3.3 Φ-partie, Φ-quotient et modules induits

Pour une p-place v de K_0, on note $U_{\infty,v} = \varprojlim \overline{U}_{n,v}$ la limite projective relativement à la norme des groupes $\overline{U}_{n,v}$, qui sont les pro-p-complétés des groupe des unités de $K_{n,v}$. Le module des unités semi-locales $\mathcal{U}_\infty = \prod_v U_{\infty,v}$ est un module apparaissant fréquemment en théorie d'Iwasawa. Si l'on regarde de plus près, on voit que la structure de $\mathbb{Z}_p[G]$-module est induite par la structure de $\mathbb{Z}_p[G_v]$-module de G_v, groupe de décomposition dans G d'une p-place v. On sera par la suite amené à considérer la Φ^*-partie de ce module.
Il est naturel de déterminer la relation entre Φ-partie d'un module induit et le module induit de la Φ-partie. Rappelons au préalable la définition d'un module induit :

Définition 1.3.7. *Soit H un sous groupe de G, M un $\mathbb{Z}_p[H]$-module, alors*

$$\mathrm{Ind}_G^H M = M \otimes_{\mathbb{Z}_p[H]} \mathbb{Z}_p[G] \quad .$$

Le module induit $\mathrm{Ind}_G^H M$ est le plus petit $\mathbb{Z}_p[G]$-module contenant M, comme sous $\mathbb{Z}_p[H]$-module.
Le problème qui nous intéresse est le suivant : considérons un sous groupe H de G, M un $\mathbb{Z}_p[H]$-module, Φ un caractère de G et $\phi = \Phi_{|H}$, quelles relations existe-t-il entre $(\mathrm{Ind}_G^H M)^\Phi$ et $\mathrm{Ind}_G^H(M^\phi)$? Pour cela, on va supposer dans un premier temps que le groupe G est cyclique, puis on verra que le résultat obtenu se généralise au cas où G est supposé seulement abélien.

Proposition 1.3.8. *Soient G un groupe cyclique, H un sous groupe de G, M un $\mathbb{Z}_p[H]$-module, compact ou discret, Φ un caractère de G et $\phi = \Phi_{|H}$. On dispose d'un isomorphisme de $\mathbb{Z}_p[G]$-modules :*

$$\Theta : Hom_{\mathbb{Z}_p[H]}(\mathbb{Z}_p[\phi], M) \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi] \to Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M \otimes_{\mathbb{Z}_p[H]} \mathbb{Z}_p[G]).$$

Démonstration. Posons $r = [G : H]$.
Remarquons que $\mathrm{Hom}_{\mathbb{Z}_p[H]}(\mathbb{Z}_p[\phi], M) \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi] = M^\phi \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi]$. De plus $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M \otimes_{\mathbb{Z}_p[H]} \mathbb{Z}_p[G]) = (\mathrm{Ind}_G^H M)^\phi$ est un $\mathbb{Z}_p[\Phi]$-module contenant M comme sous $\mathbb{Z}_p[\phi]$-module.
Par définition de la ϕ-partie, on a $M^\phi = (M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\phi])^H$, l'action d'un élément $h \in H$ sur un tenseur élémentaire $m \otimes z$ étant définie par $h \star (m \otimes z) = (h.m) \otimes (\phi(h)^{-1} m)$. Par conséquent, $M^\phi \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi] \simeq (M \otimes \mathbb{Z}_p[\Phi])^H$. On déduit donc du lemme de Shapiro que $M^\phi \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi] \simeq \mathrm{Ind}_G^H (M \otimes \mathbb{Z}_p[\Phi])^G$. On doit donc montrer que $\mathrm{Ind}_G^H (M \otimes \mathbb{Z}_p[\Phi])^G \simeq (\mathrm{Ind}_G^H (M) \otimes \mathbb{Z}_p[\Phi])^G$.
A cette fin, comparons les actions de G sur $\mathrm{Ind}_G^H (M \otimes \mathbb{Z}_p[\Phi])$ et sur $\mathrm{Ind}_G^H (M) \otimes \mathbb{Z}_p[\Phi]$. Il est clair qu'il existe un $\mathbb{Z}_p$-isomorphisme canonique entre $\mathrm{Ind}_G^H (M) \otimes \mathbb{Z}_p[\Phi]$ et $\mathrm{Ind}_G^H (M \otimes \mathbb{Z}_p[\Phi])$. L'action de G sur $\mathrm{Ind}_G^H (M \otimes \mathbb{Z}_p[\Phi])$ définit alors une représentation de G, que l'on notera ρ_1, à valeur dans $\mathrm{GL}(\mathrm{Ind}_G^H (M) \otimes \mathbb{Z}_p[\Phi])$. De même l'action de G sur $(\mathrm{Ind}_G^H (M) \otimes \mathbb{Z}_p[\Phi])$ définie une représentation ρ_2 à valeurs dans $\mathrm{GL}(\mathrm{Ind}_G^H (M) \otimes \mathbb{Z}_p[\Phi])$. Fixons un générateur g de G, alors $\rho_1(g)$ et $\rho_2(g)$ peuvent être représentés par une matrice $r \times r$ à coefficients dans $\mathrm{Hom}_{\mathbb{Z}_p}(M \otimes \mathbb{Z}_p[\Phi])$. Plus précisément, on a :

$$M(\rho_1(g)) = \begin{pmatrix} 0 & \cdots & 0 & \zeta^{-r} g^r \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ (0) & & 1 & 0 \end{pmatrix}$$

et

$$M(\rho_2(g)) = \begin{pmatrix} 0 & \cdots & 0 & \zeta^{-1} g^r \\ \zeta^{-1} & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ (0) & & \zeta^{-1} & 0 \end{pmatrix}.$$

Notant R_i le $\mathbb{Z}_p[G]$-module $\mathrm{Ind}_G^H M \otimes \mathbb{Z}_p[\Phi]$, sur lequel l'action de G est définie via ρ_i. On doit démontrer que $R_1^G \simeq R_2^G$. Par définition de l'induit, tout élément de $m \in \mathrm{Ind}_G^H M \otimes \mathbb{Z}_p[\Phi]$ s'écrit de façon unique sous la forme $m = \sum_{i=1}^r m_i$, avec $m_i \in g^{i-1} M \otimes \mathbb{Z}_p[\Phi]$. Soit donc $m = (m_1, \cdots, m_r) \in \mathrm{Ind}_G^H M \otimes \mathbb{Z}_p[\Phi]$. En utilisant les représentations matricielles de $\rho_1(g)$ et de

$\rho_2(g)$, il vient d'une part :

$$m \in R_1^G \Leftrightarrow \begin{cases} \zeta^{-r} g^r m_r &= m_1 \\ m_1 &= m_2 \\ \vdots & \vdots \\ m_{r-1} &= m_r \end{cases} \Leftrightarrow m_1 = \cdots = m_r \text{ et } g^r m_r = \zeta^r m_r$$

et d'autre part

$$m \in R_2^G \Leftrightarrow \begin{cases} \zeta^{-1} g^r m_r &= m_1 \\ \zeta^{-1} m_1 &= m_2 \\ \vdots & \vdots \\ \zeta^{-1} m_{r-1} &= m_r \end{cases} \Leftrightarrow m_i = \zeta^{-i} m_r \text{ et } g^r m_r = \zeta^r m_r.$$

Posons alors pour $m = (m_1, \cdots, m_r) \in R_1^G$:

$$f(m) = (\zeta^{r-1} m_r, \zeta^{r-2} m_r, \cdots, \zeta m_r, m_r).$$

L'application f est clairement à valeurs dans R_2^G, de plus il s'agit clairement d'un isomorphisme de $\mathbb{Z}_p$-modules. On en déduit donc que $R_1^G \simeq R_2^G$. □

Remarque. *Dans la démonstration précédente, l'hypothèse G est cyclique, permet de ramener le calcul des G-invariants au calcul du noyau de la multiplication par $g - 1$, g étant un générateur de G. Il semble donc peu probable que cette démonstration puisse s'adapter si l'on suppose uniquement G abélien. Toutefois on va voir que la proposition précédente reste vraie pour un groupe abélien G.*

Proposition 1.3.9. *Soit G un groupe abélien, H un sous groupe de G, M un $\mathbb{Z}_p[H]$-module, Φ un caractère de G et $\phi = \Phi_{|H}$. Alors*

$$M^\phi \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi] \simeq \mathrm{Ind}_G^H(M)^\Phi \quad .$$

Démonstration. Les groupes $\Phi(G)$ et $\Phi(H)$ étant des sous groupes finis du groupe des racines de l'unité, ils sont cycliques. Notons G_1 et H_1 les noyaux respectifs des projections canoniques de $G \to \Phi(G)$ et de $H \to \Phi(H)$.
On a d'une part $M^\phi \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi] = (M \otimes \mathbb{Z}_p[\Phi])^H = (M^{H_1} \otimes \mathbb{Z}_p[\Phi])^{\Phi(H)}$ et d'autre part $\mathrm{Ind}_G^H(M)^\Phi = (\mathrm{Ind}_G^H M \otimes \mathbb{Z}_p[\Phi])^G = ((\mathrm{Ind}_G^H M)^{G_1} \otimes \mathbb{Z}_p[\Phi])^{\Phi(G)}$.
Les groupes $\Phi(G)$ et $\Phi(H)$ étant cycliques, on en déduit que $M^\phi \otimes_{\mathbb{Z}_p[\phi]} \mathbb{Z}_p[\Phi] = (\mathrm{Ind}_{\Phi(G)}^{\Phi(H)}(M^{H_1}) \otimes \mathbb{Z}_p[\Phi])^{\Phi(G)}$. La démonstration de la proposition se ramène donc à la démonstration du lemme suivant

Lemme 1.3.10. $\mathrm{Ind}_{\Phi(G)}^{\Phi(H)}(M^{H_1}) \simeq (\mathrm{Ind}_G^H M)^{G_1}$.

Démonstration. Remarquons pour commencer que $(\mathrm{Ind}_G^H M)^{G_1}$ étant un G-module sur lequel G_1 agit trivialement, c'est naturellement un $\Phi(G)$-module. Soient maintenant $(x_1, \cdots, x_s)$ un système de représentants de G_1/H_1 dans G_1 et $(y_1, \cdots, y_t)$ un système de représentants de $\Phi(G)/\Phi(H)$ dans G. La famille $(x_i y_j, 1 \leq i \leq s, 1 \leq j \leq t)$ est un système de représentants de G/H dans G. En effet $x_i y_j \equiv x_{i'} y_{j'} (\mod H)$ implique que $\Phi(y_j) \equiv \Phi(y_{j'}) (\mod \Phi(H))$ et donc que $j = j'$. Il s'ensuit que $x_i \equiv x_{i'} (\mod H)$, x_i et $x_{i'}$ étant des éléments de G_1, on a en fait $x_i \equiv x_{i'} (\mod H_1) \Rightarrow i = i'$. De plus G/H est clairement d'ordre st. On a alors $\mathrm{Ind}_G^H M = \oplus_{i,j} x_i y_j M$.
Définissons l'application $f : M^{H_1} \to (\mathrm{Ind}_G^H M)^{G_1}$ en posant $f(m) = \sum_i x_i m$. Il s'agit d'un morphisme injectif de $\mathbb{Z}_p[\Phi(H)]$-modules, qui s'étend donc de façon naturelle en un morphisme injectif de $\mathbb{Z}_p[\Phi(G)]$-modules :

$$\tilde{f} : \mathrm{Ind}_{\Phi(G)}^{\Phi(H)} M^{H_1} \to (\mathrm{Ind}_G^H M)^{G_1}.$$

Soit $m \in (\mathrm{Ind}_G^H M)^{G_1}$. On a alors $m = \sum_{i,j} x_i y_j m_{i,j}$. Le groupe H_1 opérant diagonalement on a $m_{i,j} \in M^{H_1}$. Par ailleurs les éléments de G_1 permutent les x_i. Le fait que M soit G_1 invariant implique donc que $m_{i,j} = m_{i',j}$. Quitte à poser $m_j = m_{i,j}$, on peut alors écrire $m = \sum_{i,j} x_i y_j m_j = \sum_j y_j \sum_i x_i m_j$. En d'autres termes $m = \tilde{f}(\sum_j m_j \otimes y_j)$. Le morphisme $\tilde{f}$ défini précédemment est donc surjectif. □

La démonstration du lemme achève aussi celle de la proposition. □

1.4 Étude de la Φ^*-composante de quelques modules galoisiens

Rappelons le cadre arithmétique dans lequel on évolue. On dispose d'une extension $F/\mathbb{Q}$ modérément ramifiée. L'extension $K_0 = F(\zeta_p)$ est donc également modérément ramifiée. On supposera en outre que l'extension $K_0/\mathbb{Q}$ vérifie la conjecture de Leopoldt. Les extensions M_∞ et N_∞ de K_∞, $\mathbb{Z}_p$-extension cyclotomique de K_0, sont définies de la façon suivante :

- L_∞ désigne la pro-p-extension abélienne maximale non-ramifiée de K_∞.
- M_∞ désigne la pro-p-extension abélienne maximale non-ramifiée en dehors des p-places de K_∞.
- N_∞ désigne l'extension obtenue en ajoutant à K_∞ les racines de p^n-ièmes d'unités.

De plus, de l'hypothèse de ramification, on déduit que le groupe $G := \mathrm{Gal}(K_0/\mathbb{Q})$, peut être considéré comme un sous groupe de $\mathrm{Gal}(K_\infty/\mathbb{Q})$. Par conséquent, on peut faire agir G sur le Λ-module $\mathrm{Gal}(M_\infty/K_\infty)$, ses sous Λ-modules et ses Λ-modules quotients. Il est donc licite de parler de la Φ-partie du module $\mathrm{Gal}(M_\infty/K_\infty)$, pour un caractère Φ de G.

A partir de maintenant, fixons un caractère pair $\mathbb{C}_p$-irréductible Φ de G et définissons le caractère miroir de Φ :

Définition 1.4.1. *Soit Φ un caractère de G. Le caractère miroir de Φ est le caracère Φ^* défini par*

$$\Phi^* = \Phi^{-1}\omega,$$

où ω désigne la restriction du caractère cyclotomique κ à G.

Les outils algébriques nécessaires étant maintenant en place, on peut étudier la Φ^*-partie de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$, le but étant de montrer que lorsque Φ est pair, $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*}$ est triviale. Pour cela, on va calculer la série caractéristique de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*}$. L'idée est de plonger ce module dans deux modules, $\mathrm{Gal}(M_\infty/L_\infty)^{\Phi^*}$ et $\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*}$, pour lesquels on est en mesure d'obtenir des informations sur la série caractéristique.

1.4.1 Étude de la Φ^*-composante de $\mathrm{Gal}(M_\infty/N_\infty)$

Le but de cette section est d'obtenir des informations sur la série caractéristique de $\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*}$. La théorie de Kummer permet de ramener l'étude de $\mathrm{Gal}(M_\infty/N_\infty)$ à celle du module d'Iwasawa $X_\infty(K_0)$. Or la conjecture de Leopoldt, qui est vérifiée dans le cas d'une extension abélienne, nous donne des informations sur la série caractéristique de $X_\infty(K_0)$.

Notons μ_{p^∞} le groupe des racines p-primaires de l'unité et A_∞ la limite inductive des A_n, où A_n désigne la p-partie du groupe des classes de K_n.
Le fait que G s'identifie à un sous groupe de $\mathrm{Gal}(K_\infty/F)$ permet de munir les modules $\mathrm{Gal}(L_\infty/K_\infty)$, $\mathrm{Gal}(M_\infty/K_\infty)$ et $\mathrm{Gal}(N_\infty/K_\infty)$ d'une structure de $\mathbb{Z}_p[\Gamma \times G]$-module et par conséquent on peut considérer les Φ-parties et Φ-quotients de ces modules.
Par définition de N_∞, on dispose, via la théorie de Kummer, d'un accouplement de $\mathbb{Z}_p[G]$-modules non dégénéré :

$$\mathrm{Gal}(M_\infty/N_\infty) \times A_\infty \to \mu_{p^\infty}.$$

Il s'ensuit que $\mathrm{Gal}(M_\infty/N_\infty)$ et $\mathrm{Hom}(A_\infty, \mu_{p^\infty})$ sont $\mathbb{Z}_p[G]$-isomorphes.(Voir par exemple [26] ou [13]).

Proposition 1.4.2. *Le Λ-module $Gal(M_\infty/N_\infty)^{\Phi^*}$ est de Λ-torsion et sa série caractéristique est étrangère à $\dot{T}$.*

Démonstration. Rappelons que $\Phi^* = \Phi^{(-1)}\omega$. Notons pour $f(T) \in \Lambda$, $f(T)^\bullet = f(\dot{T})$, avec $\dot{T} = T - (\kappa(\gamma) - 1)$.
Le groupe $\Gamma \times G$ agit sur $\mathrm{Hom}(A_\infty, \mu_{p^\infty})$ via l'action $*$. Par ailleurs $\mu_{p^\infty} = \mathbb{Q}_p/\mathbb{Z}_p(1)$. Si l'on fait agir $\Gamma \times G$ de façon triviale sur $\mathbb{Q}_p/\mathbb{Z}_p$ et via $*$

sur $\mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$, on a alors $\mathrm{Hom}(A_\infty, \mu_{p^\infty}) = \mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)(1) = (A_\infty^\vee)(1)$. Il s'ensuit que :

$$\begin{aligned}
\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*} &= ((A_\infty^\vee)(1))^{\Phi^*} \\
&= ((A_\infty^\vee)^{\Phi^*\omega^{(-1)}})(1) \\
&= ((A_\infty^\vee)^{\Phi^{-1}})(1) \\
&= (((A_\infty)_\Phi)^\vee)(1) \\
&= \mathrm{Hom}((A_\infty)_\Phi, \mu_{p^\infty}).
\end{aligned}$$

On obtient de même $\mathrm{Gal}(M_\infty/N_\infty)_{\Phi^*} \simeq \mathrm{Hom}((A_\infty)^\Phi, \mu_{p^\infty})$. Il s'ensuit que la série caractéristique de $\mathrm{Gal}(M_\infty/N_\infty)_{\Phi^*}$ est égale à celle de $\mathrm{Hom}((A_\infty)^\Phi, \mu_{p^\infty})$. Or $sc(\mathrm{Hom}((A_\infty)^\Phi, \mu_{p^\infty})) = sc((A_\infty^\Phi)^\vee)^\bullet = sc(X_\infty^\Phi)^\bullet$. Le caractère Φ étant pair, la série caractéristique de X_∞^Φ est étrangère à T (c'est une conséquence de la conjecture de Leopoldt), celle de $\mathrm{Gal}(M_\infty/N_\infty)_{\Phi^*}$ est donc bien étrangère à $\dot{T}$.

□

1.4.2 Étude de la Φ^*-composante de $\mathbf{Gal}(M_\infty/N_\infty L_\infty)$

Le calcul de la série caractéristique de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$ est plus délicat. Il nécéssite l'utilisation de la théorie du Corps de Classe, ainsi que de la suite exacte de Coleman.

Théorème 1.4.3. *La Φ^*-partie de $Gal(M_\infty/N_\infty L_\infty)$ est triviale.*

Démonstration. Remarquons tout d'abord que

$$\mathrm{Gal}(M_\infty/N_\infty L_\infty) \subset \mathrm{Gal}(M_\infty/K_\infty).$$

Le Λ-module $\mathrm{Gal}(M_\infty/K_\infty)$ ne possédant pas de sous module fini, il en est de même de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$. De plus comme $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*} \hookrightarrow \mathrm{Gal}(M_\infty/N_\infty L_\infty)$, il suffit pour montrer la trivialité de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*}$ de prouver que sa série caractéristique est 1. Compte tenu de ce qui précède, il suffit de démontrer que cette série est une puissance de $\dot{T}$.
Notons U_n le groupe des unités de K_n, U_∞ la limite projective relativement à la norme des U_n.
Si v est une p-place de K_∞, $U_{n,v}$ désigne le groupe des unités de K_n, v-complété de K_n et $U_{\infty,v}$ est la limite projective des $U_{n,v}$ relativement à la norme.
On note enfin $\mathcal{U}_\infty = \prod_{v|p} U_{\infty,v}$.

Considérons la suite exacte du corps de classe

$$1 \longrightarrow \overline{U}_\infty \longrightarrow \mathcal{U}_\infty \longrightarrow \mathrm{Gal}(M_\infty/L_\infty) \longrightarrow 1\ .$$

On en déduit

$$1 \longrightarrow (\overline{U}_\infty)^{\Phi^*} \longrightarrow (\mathcal{U}_\infty)^{\Phi^*} \xrightarrow{f} (\mathrm{Gal}(M_\infty/L_\infty))^{\Phi^*} \longrightarrow H^1(G, \overline{U}_\infty \otimes \mathbb{Z}_p(\Phi]) \ .$$

Le fait que Φ^* est impair assure que $(\overline{U}_\infty)^{\Phi^*}$ est de Λ-torsion, on a donc une suite exacte :

$$1 \longrightarrow (\overline{U}_\infty)^{\Phi^*} \longrightarrow t_\Lambda((\mathcal{U}_\infty)^{\Phi^*}) \xrightarrow{f} t_\Lambda(\mathrm{Im}(f)) \longrightarrow 1 \ . \tag{1.5}$$

Par ailleurs d'après le théorème de Ferrero-Washington ([5]), comme l'invariant μ de $\mathrm{Gal}(M_\infty/K_\infty)$ est nul, il en est de même de celui de $\mathrm{Gal}(M_\infty/L_\infty)$. Le conoyau de l'injection naturelle $\mathrm{Im}(f) \hookrightarrow \mathrm{Gal}(M_\infty/L_\infty)^{\Phi^*}$, étant tué par l'ordre de G, il est donc nécessairement fini et les Λ-modules $\mathrm{Im}(f)$ et $\mathrm{Gal}(M_\infty/L_\infty)^{\Phi^*}$ sont pseudo-isomorphes. Il en est donc de même de leurs Λ-torsions. On déduit alors de cette remarque et de la suite (1.5) que la série caractéristique de $t_\Lambda(\mathrm{Gal}(M_\infty/L_\infty)^{\Phi^*})$ divise celle de $t_\Lambda((\mathcal{U}_\infty)^{\Phi^*})$. On est donc amener à calculer la série caractéristique de $t_\Lambda((\mathcal{U}_\infty)^{\Phi^*})$.

Fixons une p-place v de K_0. Le principal ingrédient du calcul de la série caractéristique de $t_\Lambda((\mathcal{U}_\infty)^{\Phi^*})$ est la suite exacte de Coleman ([3]) :

$$1 \longrightarrow \mathbb{Z}_p(1) \longrightarrow U_{\infty,v} \xrightarrow{Col} \mathbb{Z}_p[\mathrm{Gal}(K_{\infty,v}/\mathbb{Q}_p)] \longrightarrow \mathbb{Z}_p(1) \longrightarrow 1 \ . \tag{1.6}$$

Notons V l'image de $U_{\infty,v}$ par l'application de Coleman Col. On dispose alors de deux suites exactes courtes :

$$1 \longrightarrow \mathbb{Z}_p(1) \longrightarrow U_{\infty,v} \xrightarrow{Col} V \longrightarrow 1 \tag{1.7}$$

et

$$1 \longrightarrow V \longrightarrow \mathbb{Z}_p[\mathrm{Gal}(K_{\infty,v}/\mathbb{Q}_p)] \longrightarrow \mathbb{Z}_p(1) \longrightarrow 1 \ . \tag{1.8}$$

Notons Φ_v^* la restriction de Φ^* à G_v groupe de décomposition de v. Prenant la Φ_v^*-partie de la suite exacte (1.7). Il vient :

$$1 \longrightarrow (\mathbb{Z}_p(1))^{\Phi_v^*} \longrightarrow (U_{\infty,v})^{\Phi_v^*} \xrightarrow{Col} V^{\Phi_v^*}. \tag{1.9}$$

Or $(\mathbb{Z}_p(1))^{\Phi_v^*} = (\mathbb{Z}_p)^{\Phi_v^*\omega^{-1}}(1)$. Il s'ensuit que $(\mathbb{Z}_p)^{\Phi_v^*\omega^{-1}}(1) = 0$ dès que $\Phi_v^*\omega^{-1} \neq 1$. Or par définition de Φ^*, on a $\Phi^* = \Phi^{-1}\omega$ et donc $\Phi_v^*\omega^{-1} = \Phi_v^{-1}\omega\omega^{-1} = \Phi_v^{-1}$. Il s'ensuit que $\Phi_v^*\omega^{-1} = 1 \Leftrightarrow \Phi_v^{-1} = 1 \Leftrightarrow \Phi_v = 1$, où Φ_v désigne la restriction de Φ à G_v.

Dans le cas où $\Phi_v \neq 1$, on a donc une injection $(U_{\infty,v})^{\Phi_v^*} \hookrightarrow V^{\Phi_v^*}$. Par ailleurs, considérant la suite exacte (1.8), on obtient une injection $V^{\Phi_v^*} \hookrightarrow \mathbb{Z}_p[\mathrm{Gal}(K_{\infty,v}/\mathbb{Q}_p)]^{\Phi_v^*}$. Par composition, on en déduit une injection :

$$(U_{\infty,v})^{\Phi_v^*} \hookrightarrow \mathbb{Z}_p[\mathrm{Gal}(K_{\infty,v}/\mathbb{Q}_p)]^{\Phi_v^*} \quad . \tag{1.10}$$

Revenons au problème initial, qui était de déterminer la Λ-torsion des unités semi-locales $\mathcal{U}_\infty$. Pour cela, on a besoin des deux lemmes suivants :

Lemme 1.4.4. *Soit M un $\Lambda[G]$-module de type fini et $\Phi \in \hat{G}$. Alors on a $(t_\Lambda M)^\Phi = t_\Lambda(M^\Phi)$.*

Preuve du lemme. On sait que $M^\Phi = \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[\Phi], M)$. Procédons par double inclusion.
On a $t_\Lambda(M) \subset M \Rightarrow t_\Lambda(M)^\Phi \subset M^\Phi \Rightarrow t_\Lambda(M)^\Phi \subset t_\Lambda(M^\Phi)$.
Par ailleurs, si f est un élément de M^Φ de Λ-torsion, il est clair, $f(\mathbb{Z}_p[\Phi])$ étant de type fini, que $f(\mathbb{Z}_p[\Phi]) \subset t_\Lambda(M)$ et donc $t_\Lambda(M^\Phi) \subset (t_\Lambda M)^\Phi$. □

Lemme 1.4.5. *Soit M un $\Lambda[H]$-module de type fini. Alors* $\mathrm{Ind}_G^H t_\Lambda(M) = t_\Lambda(\mathrm{Ind}_G^H M)$.

Preuve du lemme. Notons r l'indice $[G : H]$ et donnons nous un système de représentants de G/H dans G, $\{g_1, \cdots, g_r\}$. Par définition, $\mathrm{Ind}_G^H M = M \otimes_{\mathbb{Z}_p[H]} \mathbb{Z}_p[G]$. Tout repose sur le fait que G/H est fini et que Λ agit diagonalement sur $\mathrm{Ind}_G^H M$. En effet soit $m = \sum_{i=1}^r g_i m_i \in t_\Lambda(\mathrm{Ind}_G^H M)$, alors il existe $f(T) \in \Lambda$ telle que $f(T).m = 0 \Rightarrow f(T).m_i = 0, \forall i$. On peut donc définir de façon naturelle une injection $t_\Lambda(\mathrm{Ind}_G^H M) \to \mathrm{Ind}_G^H t_\Lambda(M)$. Par ailleurs si $m = \sum_{i=1}^r g_i.m_i \in \mathrm{Ind}_G^H t_\Lambda(M)$, alors $\forall i$, il existe $f_i(T) \in \Lambda$ tel que $f_i(T).m_i = 0$, il s'ensuit que $\prod_{i=1}^r f_i(T)m = 0$, l'injection définie précédemment est donc bien un isomorphisme. □

On déduit alors de ces deux lemmes et de la proposition 1.3.8, que

$$t_\Lambda(\mathcal{U}_\infty)^{\Phi^*} = t_\Lambda(\mathcal{U}_\infty^{\Phi^*}) = t_\Lambda((\mathrm{Ind}_G^{G_v} U_{\infty,v})^{\Phi^*}) = t_\Lambda((\mathrm{Ind}_G^{G_v}((U_{\infty,v})^{\Phi_v^*}))\otimes\mathbb{Z}_p[\Phi]).$$

Or compte tenu de l'injection (1.10) et du fait que $\mathbb{Z}_p[\mathrm{Gal}(K_{\infty,v}/\mathbb{Q}_p)]^{\Phi_v^*} = \mathbb{Z}_p[\Phi_v^*][\Gamma] = \Lambda_{\Phi_v^*}$, la Λ-torsion de $U_{\infty,v}$ est donc triviale, lorsque $\Phi_v \neq 1$ et par conséquent $t_\Lambda(\mathcal{U}_\infty^{\Psi^*}) = 0$ dès que $\Phi_v \neq 1$.

Supposons donc maintenant que $\Phi_v = 1$. Dans ce cas $\mathbb{Z}_p(1)^{\Phi_v^*} = \mathbb{Z}_p(1)$. Les suites exactes (1.7) et (1.8) donnent alors :

$$1 \longrightarrow \mathbb{Z}_p(1) \longrightarrow (U_{\infty,v})^{\Phi_v^*} \longrightarrow V^{\Phi_v^*} \tag{1.11}$$

et

$$1 \longrightarrow V^{\Phi_v^*} \longrightarrow \Lambda_{\Phi_v} \longrightarrow \mathbb{Z}_p(1)\ .$$

Par conséquent la Λ-torsion de $V^{\Phi_v^*}$ est triviale, il s'ensuit que la Λ-torsion de l'image de la flèche de droite dans la suite (1.11) est également triviale.
Par ailleurs, le module $\mathbb{Z}_p(1)$ étant de Λ-torsion, on a pour $\Phi_v = 1 \Leftrightarrow \Phi_v^* = \omega$:

$$t_\Lambda((U_{\infty,v})^{\Phi_v^*}) = \mathbb{Z}_p(1) = \Lambda/\dot{T} \quad .$$

Et finalement, lorsque $\Phi_{|G_v} = 1$, on a

$$t_\Lambda(\mathcal{U}_\infty)^{\Phi^*} = (\Lambda/\dot{T}) \otimes \mathbb{Z}_p[\Phi] = \Lambda_\Phi/\dot{T}.$$

On a donc montré que $sc(t_\Lambda((\mathcal{U}_\infty)^{\Phi^*}) = \dot{T}^a$ avec $a = \deg(\Phi)$ ou 0 selon que $\Phi_v = 1$ ou non.

Corollaire 1.4.6. *Notons $\mathcal{F}$ l'ensemble des caractères $\mathbb{C}_p$-irréductibles $\Phi \in \hat{G}$ tels que $\Phi_{G_v} = 1$. Alors la série caractéristique de $(\mathcal{U}_\infty)^-$ est égale à $\dot{T}^n$ avec $n = \sum_{\Phi\in\mathcal{F}}[\mathbb{Z}_p[\Phi] : \mathbb{Z}_p]$.*

Démonstration. En effet $sc(\mathcal{U}_\infty)^- = \sum_{\Phi \text{ impair}} \mathcal{U}_\infty^\Phi$. Or $sc(\mathcal{U}_\infty^\Phi) = 0$ si $\Phi_{|G_v} \neq 1$ et $sc(\mathcal{U}_\infty^\Phi) = \prod_{\Phi\in\hat{G}} sc(\mathcal{U}_\infty^\Phi) = \prod_{\Phi\in\mathcal{F}} \dot{T}^{n_\Phi}$ si $\Phi_{|G_v} = 1$. □

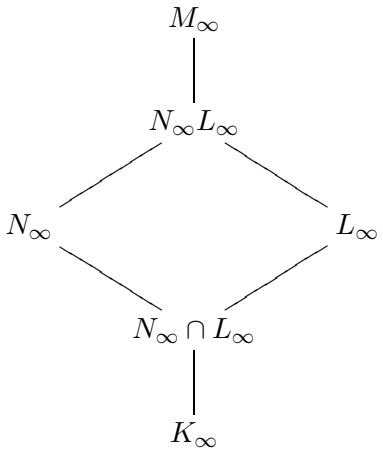
Du corollaire, on déduit que la série caractéristique de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*}$ est une puissance de $\dot{T}$. Or on a vu dans la section précédente, qu'elle était étrangère à $\dot{T}$. Cette série est donc triviale et le module $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*}$, qui s'injecte dans $\mathrm{Gal}(M_\infty/K_\infty)$ également.

□

1.5 Lien avec la théorie de Kummer

La théorie de Kummer permet d'établir une correspondance entre les extensions de K_∞ d'exposant p-primaire et les sous groupes de $(\varinjlim U_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Notons $\mathcal{H}_\infty$ le radical Kummérien associé à la pro-p-extension abélienne non-ramifiée maximale de K_∞, notée L_∞ et $\mathcal{E}_\infty$ le radical Kummérien associé à l'extension $N_\infty \cap L_\infty$. Le radical Kummérien $\mathcal{H}_\infty$ est donc constitué des éléments de la forme $u \otimes \frac{1}{p^n}$ avec u unité de K_∞, tel que u^{1/p^n} engendre une extension non-ramifiée. Le but de cette partie est de relier l'invariant λ_Φ de l'extension K_0, qui est conjecturalement nul, aux radicaux Kummériens introduits précédemment et d'observer les conséquences de la conjecture de Greenberg.
Les relations entre les diverses extensions sont résumées dans le treillis ci-

dessous :



On dispose donc d'une suite exacte

$$\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty) \hookrightarrow \mathrm{Gal}(L_\infty/K_\infty) \twoheadrightarrow \mathrm{Gal}(N_\infty \cap L_\infty/K_\infty)\ .$$

Utilisant la dualité de Kummer, on en déduit

$$\mathcal{E}_\infty \hookrightarrow \mathcal{H}_\infty \twoheadrightarrow \mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)^\vee(1)\ .$$

Par conséquent

$$(\mathcal{H}_\infty/\mathcal{E}_\infty)_\Phi = \mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)^\vee(1)_\Phi = (\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)^{\Phi^*})^\vee(1).$$

Or $\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty) \simeq \mathrm{Gal}(N_\infty L_\infty/N_\infty)$, les Φ^*-parties de ces modules sont donc égales. Considérons alors la suite exacte :

$$1 \longrightarrow \mathrm{Gal}(M_\infty/N_\infty L_\infty) \longrightarrow \mathrm{Gal}(M_\infty/N_\infty) \longrightarrow \mathrm{Gal}(N_\infty L_\infty/N_\infty) \longrightarrow 1\ .$$

On en déduit, compte tenu de la trivialité de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*}$,

$$\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*} \hookrightarrow \mathrm{Gal}(N_\infty L_\infty/N_\infty)^{\Phi^*} \longrightarrow H^1(G, \mathrm{Gal}(M_\infty/N_\infty L_\infty)^\bullet)\ .$$

D'une part les groupes $\mathrm{Gal}(M_\infty/L_\infty)$, $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$ et $\mathrm{Gal}(N_\infty L_\infty/L_\infty)$, considérés comme Λ-modules, sont de torsion et de type fini. D'autre part l'extension $K_0/\mathbb{Q}$ étant abélienne, l'invariant μ de $\mathrm{Gal}(M_\infty/K_\infty)$ est nul. Par conséquent les invariants μ des modules considérés précédemment sont également nuls.
Il s'ensuit que $H^1(G, \mathrm{Gal}(M_\infty/N_\infty L_\infty)^\bullet)$ est fini. Les modules $\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*}$ et $\mathrm{Gal}(N_\infty L_\infty/N_\infty)^{\Phi^*}$ sont donc pseudo-isomorphes.
Par conséquent :

$$(\mathcal{H}_\infty/\mathcal{E}_\infty)^\Phi \sim (\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*})^\vee(1) \quad .$$

Or d'une part $(\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*})^\vee(1) \simeq \mathrm{Gal}(M_\infty/N_\infty)^\vee(1)_\Phi$ et d'autre part $\mathrm{Gal}(M_\infty/N_\infty) \simeq A_\infty^\vee(1)$. On en déduit donc que $(\mathcal{H}_\infty/\mathcal{E}_\infty)_\Phi \sim (A_\infty)_\Phi$. On a donc démontré le résultat suivant :

Théorème 1.5.1. *Notons $\mathcal{H}_\infty$, le radical kummérien associé à l'extension L_∞/K_∞, $\mathcal{E}_\infty$ celui associé à l'extension $N \cap L_\infty/K_\infty$. Alors pour tout caractère pair $\mathbb{C}_p$-irréductible Φ de G, on a :*

$$Corang_{\mathbb{Z}_p}(\mathcal{H}_\infty/\mathcal{E}_\infty)_\Phi = \lambda_\Phi deg(\Phi).$$

Démonstration. En effet, on a vu que $\mathcal{H}_\infty/\mathcal{E}_\infty \sim (A_\infty)_\Phi$. Par conséquent $\mathrm{Corang}_{\mathbb{Z}_p}\mathcal{H}_\infty/\mathcal{E}_\infty = \mathrm{Rang}_{\mathbb{Z}_p}((A_\infty)_\Phi)^\vee$. De plus, du fait de l'existence d'un quasi-isomorphisme $f : A_\infty^\vee \to X$, on déduit $((A_\infty)_\Phi)^\vee \sim X_\Phi$. □

La conjecture de Greenberg prédit la nullité des invariants λ de $(X_\infty)^\Phi$ pour Φ pair. Dans le cadre que nous venons d'étudier elle se reformule de la façon suivante.

Corollaire 1.5.2. *Les invariants λ_ϕ des modules $X_\infty(K_0)^\Phi$ sont nuls pour tout caractère pair Φ de G si et seulement si $Gal(L_\infty/N_\infty \cap L_\infty)$ est fini.*

Démonstration. Pour montrer la finitude de $\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)$ il suffit de montrer la nullité des $\mathbb{Z}_p$-rangs de $\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)_\Phi$ pour tout caractère Φ. Si Φ est pair, cela découle de l'hypothèse $\lambda_\Phi = 0$. Pour Φ-impair, remarquons que :

$$\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)_\Phi = \mathrm{Gal}(N_\infty L_\infty/N_\infty)_\Phi \sim \mathrm{Gal}(M_\infty/N_\infty)_\Phi = (A_\infty^{\Phi^*})^\vee(1).$$

Or Φ impair implique Φ^* pair. Par hypothèse $A_\infty^{\Phi^*}$ est fini et donc $\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)_\Phi$ également.
Finalement on a bien $\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty) \sim 0$.
Réciproquement, la finitude de $\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)$ est équivalente à celle de $\mathrm{Gal}(N_\infty L_\infty/N_\infty)$. Or pour un caractère pair Φ, on a vu que $\mathrm{Gal}(M_\infty/N_\infty L_\infty)^{\Phi^*}$ était trivial, la finitude de $\mathrm{Gal}(N_\infty L_\infty/N_\infty)^{\Phi^*}$ entraîne donc celle de $\mathrm{Gal}(M_\infty/N_\infty)^{\Phi^*}$et donc celle de $X_\infty(K_0)$. □

Corollaire 1.5.3. *La conjecture de Greenberg est vérifiée pour le corps K_0 si et seulement su $Gal(L_\infty \cap N_\infty/K_\infty)^- = X_\infty^-$.*

Démonstration. L'implication directe découle tout simplement du corollaire précédent et du fait que le module X_∞^- est $\mathbb{Z}_p$-libre (prop. 13.28 de [26]).
La réciproque découle du fait que $\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty)^- \sim X_\infty^+$, ce pseudo-isomorphisme étant une conséquence directe du théorème 1.4.3. □

Chapitre 2

Radical Kummérien du corps de Hilbert : quelques observations.

2.1 Introduction

Etant donné un premier impair p et un corps de nombres K_0 contenant ζ_p, racine primitive p-ième de l'unité, on considère alors la p-extension élémentaire abélienne non-ramifiée maximale de K_0, que l'on note $H_0(p)$. Le corps K_0 contenant ζ_p, on sait, par la théorie de Kummer qu'il existe des éléments $x_1, \cdots, x_r$ de K_0 tels que l'extension $H_0(p)$ soit engendrée par les racines p-ièmes de ces éléments. Le sous-groupe de $K_0^* \otimes \mathbb{Z}/p\mathbb{Z}$ engendré par de tels éléments est appelé radical kummérien associé à l'extension $H_0(p)$. Le but de ce chapitre est de déterminer une méthode permettant de calculer effectivement ce radical à l'aide du logiciel pari-gp .
Connaissant un sous-groupe de $K_0^* \otimes \mathbb{Z}/p\mathbb{Z}$, il est facile de déterminer les places se ramifiant dans l'extension correspondante. Ce problème a été traité en détail dans [6]. Si on se donne un ensemble de places S et une S-unité u, on sait que l'extension $K_0(u^{\frac{1}{p}})/K_0$ est non-ramifiée en dehors de $S \cup S_p$, S_p désignant l'ensemble des p-places de K_0. En particulier, l'extension associée à une unité est non-ramifiée en dehors de p.
Cependant le problème inverse, i.e. déterminer effectivement le radical kummérien associé à une extension donnée, est nettement plus difficile. En effet, rien ne garantit que le radical kummérien associé à une extension non-ramifiée de K_0 est engendré par des unités. Dans un premier temps, nous allons voir que dans le cas modérément ramifié, certains critères relatifs à la ramification d'une extension kummérienne engendrée par une unité, énoncés dans [6], se simplifient et se ramènent à des calculs de valuations dans le corps K_0.
Nous verrons ensuite que toute extension non-ramifiée de K_0 peut être

engendrée par une S-unité, S désignant un ensemble de places engendrant le groupe des classes d'idéaux de K_0.
Pour finir, on montrera comment l'on peut calculer effectivement le radical kummérien associé à $H_0(p)$ lorsque le degré de $[K_0 : \mathbb{Q}]$ est relativement petit.

2.2 Critères de non-ramification d'une extension kummérienne engendrée par des racines p-ièmes d'unités

Notons K_v, le complété de K_0 relativement à une place v et O_{K_v} l'anneau des entiers de K_v. Rappelons que pour une p-place v de K, on munit K_v de l'unique valuation v prolongeant celle de $\mathbb{Q}_p$, on a donc dans K_v : $v(p) = 1$ et pour une uniformisante π_v de K_v : $v(\pi_v) = \frac{1}{e_v}$, e_v désignant l'indice de ramification de $K_v/\mathbb{Q}_p$.

Théorème 2.2.1. *(Voir par exemple [6]) Soit $x \in K_0$ et v une p-place de K_0, alors l'extension $K_0(x^{\frac{1}{p}})/K_0$ est non-ramifiée en v si et seulement si il existe $x_v \in K_v^*$ et $\eta_v \in O_{K_v}$ tels que :*

$$x = x_v^p(1 + p(\zeta_p - 1)\eta_v).$$

Si l'on note q le cardinal du corps résiduel de K_v, $q-1$ est premier à p et pour tout élément x de K_0, les extensions $K_0(x^{\frac{1}{p}})/K_0$ et $K_0(x^{\frac{q-1}{p}})/K_0$ coïncident.

Le théorème précédent peut dans le cas particulier des unités s'énoncer de la façon suivante :

Proposition 2.2.2. *Donnons nous une p-place v de K_0 telle que l'extension $K_v/\mathbb{Q}_p$ soit modérément ramifiée. Soit $u \in U_{K_0}$, alors l'extension $K_0(u^{\frac{1}{p}})/K_0$ est non-ramifiée en v si et seulement si*

$$v(u^{q-1} - 1) \geq \frac{p}{p-1}.$$

Démonstration. Il est clair que cette condition est suffisante, montrons qu'elle est également nécessaire.
Raisonnons par contraposé. Soit donc $u \in U_{K_0}$ tel que $v(u^{q-1} - 1) < \frac{p}{p-1}$ et montrons que l'extension $K_0(u^{\frac{1}{p}})/K_0$ est ramifiée en v.
Si l'extension $K_0(u^{\frac{1}{p}})/K_0$ était non-ramifiée en v, on aurait alors $u = x_v^p(1 + p(\zeta_p - 1)\eta_v)$ avec $x_v \in K_v^*$ et $\eta_v \in O_{K_v}$. Or u étant une unité, on aurait nécessairement $x_v \in U_v$ et du fait que $q-1 \in \mathbb{Z}_p^*$, on peut supposer que

$x_v \in U_v^1$. En d'autres termes, si l'extension $K_0(u^{\frac{1}{p}})/K_0$ était non-ramifiée, on aurait pour une certaine unité principale x_v : $v(ux_v^p - 1) \geq \frac{p}{p-1}$.
Les extensions engendrées par les racines p-ièmes de u et u^{q-1} coincidant, on peut toujours supposer, quitte à remplacer u par u^{q-1}, que $v(u-1) < \frac{p}{p-1}$.
En vertu de ce qui précède, montrer que l'extension $K_0(u^{\frac{1}{p}})/K_0$ est ramifiée en v revient à montrer que $v(x_v^p u - 1) < \frac{p}{p-1}$ pour tout x_v dans U_v^1.
Notons π_v, une uniformisante de K_v. On a alors $u = 1+\pi_v^a \eta_u$ et $x_v = 1+\pi_v^b \eta_x$ avec η_u et η_x unités de K_v. Avec ces notations $v(u-1) = \frac{a}{p-1}$ et $v(x-1) = \frac{b}{p-1}$. L'hypothèse $v(u-1) < \frac{p}{p-1}$ se traduit alors par $a < p$.
Explicitons x_v^p. On a $x_v^p = (1+\pi_v^b \eta_x)^p = 1 + \sum_{k=1}^{p} C_p^k \pi_v^{kb} \eta_x^{p-k}$. Or pour k entier, $1 \leq k \leq p-1$, on a $v(C_p^k \pi_v^{kb} \eta_x^{p-k}) = 1+\frac{bk}{p-1}$ et $v(\pi_v^{pb}) = \frac{pb}{p-1} = b+\frac{b}{p-1}$.
Par conséquent

$$v(x_v^p - 1) \geq \text{Min}\{1 + \frac{bk}{p-1}, 1 \leq k \leq p-1\} \cup \{b + \frac{b}{p-1}\} \geq 1 + \frac{1}{p-1}.$$

Finalement $v(x_v^p - 1) > v(u-1)$. Or on dispose du lemme suivant :

Lemme 2.2.3. *Soient $a, b \in U_v^1$ tels que $v(a-1) \neq v(b-1)$, alors $v(ab-1) = Min\{v(a-1), v(b-1)\}$.*

Démonstration. On a $a = 1 + \pi_v^\alpha x_a$ et $b = 1 + \pi_v^\beta x_b$ avec $\alpha = v(a-1)$, $\beta = v(b-1)$, $x_a, x_b \in O_{K_v}$. Par hypothèse $\alpha \neq \beta$, or

$$\begin{aligned} ab &= (1+\pi_v^\alpha x_a)(1+\pi_v^\beta x_b) \\ &= 1 + \pi_v^\alpha x_a + \pi_v^\beta x_b + \pi_v^{\alpha+\beta} x_a x_b \end{aligned}$$

Du fait que $\alpha \neq \beta$, on a nécessairement $v(ab-1) = \text{Min}(\alpha, \beta)$. □

On a donc $v(x_v^p u - 1) = \text{Min}\{v(u-1), v(x_v^p - 1)\} = v(u-1) < \frac{p}{p-1}$. □

Ce résultat ne se généralise malheureusement pas au cas où l'extension $K_0/\mathbb{Q}$ est sauvagement ramifiée : on peut trouver des exemples de corps K_0, sauvagement ramifiés, pour lesquels il existe des unités u tels que $K_0(u^{\frac{1}{p}})/K_0$ soit non-ramifiée et $v(u-1) < \frac{p}{p-1}$.
On peut toutefois, dans le cas sauvagement ramifié, obtenir une version faible de ce résultat, donnant une condition suffisante portant sur $v(u-1)$ pour que l'extension $K_0(u^{\frac{1}{p}})/K_0$ soit ramifiée en v.

Proposition 2.2.4. *Soit v une p-place de K_0, $K_0/\mathbb{Q}$ une extension sauvagement ramifiée en v. On note e (respectivement e_s) l'indice de ramification (respectivement ramification sauvage) de cette extension. Soit u une unité principale de K_0 telle que $u \equiv 1 \ [\pi_v]$, π_v désignant une uniformisante de K_v. Alors :*

1. *Si* $v(u-1) \geq \frac{p}{p-1}$, *l'extension* $K_0(u^{\frac{1}{p}})/K_0$ *est non-ramifiée en* v.
2. *Si* $v(u-1) < \frac{p}{p-1}$ *et si* $ev(u-1) \not\equiv 0 \quad [p]$, *l'extension* $K_0(u^{\frac{1}{p}})/K_0$ *est ramifiée en* v.

Remarque. *La condition 2, même si elle n'est que suffisante, est très utile lorsque l'on effectue des calculs dans le cas sauvagement ramifié. En effet, si l'on veut déterminer, avec le logiciel pari-gp , si une extension du type* $K_0(u^{\frac{1}{p}})$ *est non-ramifiée, il faut a priori utiliser la commande* ***rnfinit****. La condition 2 permet dans de nombreux cas, de conclure en effectuant uniquement des calculs sur les valuations et de ce fait d'accélérer le calcul.*

Démonstration. Le 1) découle directement du théorème 2.2.1.
Soit u une unité de K_0, principale dans K_v telle que $v(u-1) < \frac{p}{p-1}$ et $ev(u-1) \not\equiv 0 \quad [p]$. Supposons qu'il existe $x \in U_v^1$ tel que $v(x^p u - 1) \geq \frac{p}{p-1}$, i.e. que l'extension $K_0(u^{\frac{1}{p}})/K_0$ soit non-ramifiée.
Si l'on désigne par π_v une uniformisante de K_v, on a alors $u = 1 + \pi_v^a \eta_u$ et $x = 1 + \pi_v^b \eta_x$ avec η_u et η_x unités de K_v. Par hypothèse, on a $a \not\equiv 0 \quad [p]$.
Si e_s désigne l'indice de ramification sauvage, l'indice de ramification e de l'extension $K_v/\mathbb{Q}_p$ est alors $e = e_s(p-1)$.
On a alors $v(u-1) = \frac{a}{e}$. De plus, un calcul similaire à celui effectué dans la démonstration de la proposition 2.2.2, montre que $v(x^p-1) \geq \mathrm{Min}(1+\frac{b}{e}, \frac{pb}{e})$.
On a plus précisément :

$$v(x^p-1) \begin{cases} = \frac{bp}{e} & \text{si} \quad b < e_s (\Leftrightarrow \frac{pb}{e} < 1 + \frac{b}{e}) \\ \geq \frac{p}{p-1} & \text{si} \quad b \geq e_s \end{cases}$$

Dans le cas ou $b \geq e_s$, on a en vertu du lemme 2.2.3, $v(u-1) = v(x^p u - 1) \Rightarrow v(x^p u - 1) < \frac{p}{p-1}$. Or on a supposé que $v(x^p u - 1) \geq \frac{p}{p-1}$, nécessairement, $b < e_s$ et $v(x^p - 1) = \frac{bp}{e} < \frac{p}{p-1}$.
Pour que $v(x^p u - 1) \geq \frac{p}{p-1}$, il est donc nécessaire que $v(x^p - 1) = v(u-1)$. En effet, $v(x^p-1) \neq v(u-1) \Rightarrow v(x^p u - 1) = \mathrm{Min}(v(x^p-1), v(u-1)) \Rightarrow v(x^p u - 1) < \frac{p}{p-1}$. On a donc nécessairement $v(x^p-1) = v(u-1) \Leftrightarrow a = bp \Rightarrow a \equiv 0 \quad [p]$. On obtient alors une contradiction et l'extension $K_0(u^{\frac{1}{p}})/K_0$ est nécessairement ramifiée lorsque $v(u-1) < \frac{p}{p-1}$ et $ev(u-1) \not\equiv 0 \quad [p]$. □

2.3 Étude du radical kummérien de $H_0(p)$

Notons $Cl(K_0)$ le groupe des classes d'idéaux de K_0 et A_0 la p-partie de $Cl(K_0)$. La théorie du corps de classe permet d'identifier $H_0(p)$, l'extension abélienne non-ramifiée d'exposant p maximale de K_0, au groupe A_0/p.
Utilisant le théorème de structure des groupes abéliens, on obtient l'existence d'un isomorphisme de groupe abélien entre $Cl(K_0)$ et $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$.

Par conséquent, il existe des idéaux $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ tels que le sous groupe de $Cl(K_0)$ engendré par la classe de $\mathfrak{P}_i$ soit isomorphe à $\mathbb{Z}/n_i\mathbb{Z}$. Notons $S_{Cl(K_0)}$ l'ensemble des places divisant les $\mathfrak{P}_\mathfrak{i}$. Nous allons voir que le radical kummérien de $H_0(p)/p$ est engendré par des $S_{Cl(K_0)}$-unités.

Définition 2.3.1. *Une famille d'idéaux $\{\mathfrak{P}_i, 1 \leq i \leq r\}$ est une base de $Cl(K_0)$ si :*

1. *pour chaque i, le sous-groupe G_i de $Cl(K_0)$ engendré par $\mathfrak{P}_i$, est cyclique non trivial ;*
2. *le groupe $Cl(K_0)$ est produit direct des G_i.*

Dans toute cette section, on fixe une base $\{\mathfrak{P}_i, 1 \leq i \leq r\}$ de $Cl(K_0)$ et on note $S_{Cl(K_0)}$ l'ensemble des places divisant les $\mathfrak{P}_i$.

Théorème 2.3.2. *Il existe des $S_{Cl(K_0)}$-unités $u_1, \cdots, u_r$ telles que $H_0(p) = K_0(u_1^{\frac{1}{p}}, \cdots, u_r^{\frac{1}{p}})$.*

Démonstration. Soit x un élément de K_0^* engendrant une extension non-ramifiée. L'extension $K_0(x^{\frac{1}{p}})/K_0$ étant non-ramifiée, on a pour toute place $\mathfrak{p}$, $v_\mathfrak{p}(x) \equiv 0 \quad [p]$.
Notons n_i l'ordre du sous groupe cyclique de $Cl(K_0)$ engendré par la classe de$\mathfrak{P}_i$. On a alors $Cl(K_0) = \oplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$.
On a

$$(x) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(x)} = \prod_\mathfrak{p} \mathfrak{p}^{pa_\mathfrak{p}}.$$

Or pour tout idéal $\mathfrak{p}$, on a :

$$\mathfrak{p} = (y_\mathfrak{p}) \prod_i \mathfrak{P}_i^{b_{\mathfrak{p},i}},$$

avec $y_\mathfrak{p} \in O_{K_\mathfrak{p}}$ et donc

$$(x) = \prod_\mathfrak{p} (y_\mathfrak{p})^{pa_\mathfrak{p}} \prod_i \mathfrak{P}_i^{\sum_\mathfrak{p} b_{\mathfrak{p},i} pa_\mathfrak{p}} = (y)^p \prod_i \mathfrak{P}_i^{pm_i},$$

avec $y = \prod_\mathfrak{p} y_\mathfrak{p}^{a_\mathfrak{p}}$ et $m_i = \sum_\mathfrak{p} a_\mathfrak{p} b_{\mathfrak{p},i}$.
L'idéal $\mathfrak{P} = \prod_i \mathfrak{P}_i^{pm_i}$ est principal et donc $n_i | pm_i$. Si l'on note z un élément de K_0^* tel que $\mathfrak{P} = (z)$, on a alors pour une certaine unité u de K_0 :

$$x = uy^p z.$$

Les racines p-ièmes de x et uz engendrent donc la même extension et uz est bien une $S_{Cl(K_0)}$-unité. □

Remarque. *Le résultat que l'on obtient précédemment peut être affiné, dans le sens suivant : si l'on note X_i un élément de K_0 tel que $\mathfrak{P}_i^{n_i} = (X_i)$, on a alors $x = u\prod_{i=1}^{r} X_i^{a_i}$ avec $a_i \in \{0, 1, \cdots, p-1\}$.*
C'est d'ailleurs cette remarque que l'on utilisera pour calculer effectivement des générateurs du radical Kummérien associé à $H_0(p)$, le logiciel pari-gp permettant de calculer effectivement les X_i.

Si l'on observe la preuve précédente, on voit que l'on peut l'adapter au cas d'une extension p-élémentaire S-ramifiée : dans ce cas, toute extension S-ramifiée p-élémentaire peut être obtenue en extrayant des racines p-ièmes de $S \cup S_{Cl(K_0)}$-unités. La dualité n'étant pas parfaite dans le sens où des $S \cup S_{Cl(K_0)}$-unités peuvent engendrer des extensions, qui sont ramifiées en certaines places de $S \cup S_{Cl(K_0)}$.

Théorème 2.3.3. *Etant donné S un ensemble fini de places de K_0, on note $H_0(p)^S$ l'extension abélienne de K_0, non ramifiée en dehors de S, d'exposant p, maximale pour ces propriétés de K_0. Alors le radical Kummérien associé à l'extension $H_0(p)^S$ est engendré par des $S \cup S_{Cl(K_0)}$-unités.*

Démonstration. Soit donc $x \in K_0$ telle que l'extension $K_0(x^{\frac{1}{p}})/K_0$ soit non ramifiée en dehors de S.
L'idéal (x) se décompose de la façon suivante :

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}},$$

avec $a_\mathfrak{p} \equiv 0 \quad [p]$ lorsque $\mathfrak{p} \notin S$. On a alors, dans la base $(\mathfrak{P}_i)$, pour tout idéal $\mathfrak{p}$:

$$\mathfrak{p} = (y_\mathfrak{p}) \prod_i \mathfrak{P}_i^{b_{\mathfrak{p},i}}.$$

On a alors

$$(x) = \prod_{\mathfrak{p} \notin S} (y_\mathfrak{p})^{a_\mathfrak{p}} \prod_i \mathfrak{P}_i^{\sum_{\mathfrak{p} \notin S} a_\mathfrak{p} b_{\mathfrak{p},\mathfrak{i}}} \prod_{\mathfrak{p} \in S} (y_\mathfrak{p})^{a_\mathfrak{p}} \prod_i \mathfrak{P}_i^{\sum_{\mathfrak{p} \in S} a_\mathfrak{p} b_{\mathfrak{p},\mathfrak{i}}}.$$

Or pour $\mathfrak{p} \in S$, l'élément $y_\mathfrak{p}$ défini précédemment est une $S \cup S_{Cl(K_0)}$-unité : il existe alors $y \in K_0$, z une $S \cup S_{Cl(K_0)}$-unité et des entiers c_i tels que :

$$(x) = (z)(y)^p \prod_i \mathfrak{P}_\mathfrak{i}^{c_i}.$$

L'idéal $\prod_i \mathfrak{P}_\mathfrak{i}^{c_i}$ est alors principal (donc $c_i \equiv 0[n_i]$) et est engendré par une certaine $S_{Cl(K_0)}$-unité z'. Finalement, il existe une unité u telle que x s'écrive sous la forme suivante :

$$x = uzz'y^p.$$

L'extension $K_0(x^{\frac{1}{p}})$ est donc également engendrée par la racine p-ième de uzz', qui est une $S \cup S_{Cl(K_0)}$-unité. □

2.4 Radical kummérien, partie + et partie −

Supposons dans cette section que $p \neq 2$ et que K_0 est un corps CM. On définit alors K_0^+ comme le sous corps totalement réel maximal de K_0.
L'extension $H_0(p)$ est une extension abélienne de K_0, dont le groupe de Galois est muni d'une structure de $\mathbb{F}_p$-espace vectoriel. L'extension $H_0(p)$ est une extension galoisienne de K_0, comme sous-extension de H_0, qui est galoisienne et abélienne sur K_0. De plus l'extension $H_0(p)/K_0^+$ est galoisienne par maximalité de $H_0(p)$, on peut donc parler de la partie + et de la partie − de $\mathrm{Gal}(H_0(p)/K_0)$. On notera $H_0(p)^+$ et $H_0(p)^-$ les extensions de K_0 de groupes de Galois respectifs $\mathrm{Gal}(H_0(p)/K_0)^+$ et $\mathrm{Gal}(H_0(p)/K_0)^-$. Nous allons dans cette section étudier les radicaux kummériens respectifs de ces extensions.

Proposition 2.4.1. *Soit $x \in K_0^+$, telle que l'extension $K_0(x^{\frac{1}{p}})$ soit non-ramifiée. Alors $K_0(x^{\frac{1}{p}})$ est contenue dans $H_0(p)^-$.*

Démonstration. Le groupe de Galois $\mathrm{Gal}(K_0(x^{\frac{1}{p}})/K_0)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Pour $i \in \mathbb{Z}/p\mathbb{Z}$, on désigne par ϕ_i l'élément de $\mathrm{Gal}(K_0(x^{\frac{1}{p}})/K_0)$ défini par $\phi_i(x^{\frac{1}{p}}) = \zeta_p^i x^{\frac{1}{p}}$.
Notons τ la conjugaison complexe. Nous allons dans un premier temps montrer que l'extension $K_0(x^{\frac{1}{p}})$ est galoisienne sur K_0^+. Soit donc un K_0^+-plongement $\phi : K_0(x^{\frac{1}{p}}) \to \mathbb{C}$. Montrons que $K_0(x^{\frac{1}{p}})$ est stable par ϕ.
Si la restriction de ϕ à K_0 est l'identité, du fait que $K_0(x^{\frac{1}{p}})/K_0$ est galoisienne, on déduit que $K_0(x^{\frac{1}{p}})$ est stable par ϕ.
Si la restriction de ϕ à K_0 est la conjugaison complexe, on a alors $\phi(x^{\frac{1}{p}})^p = \phi(x) = x$ car $x \in K_0^+$ et donc $\phi(x^{\frac{1}{p}})$ est une racine p-ième de x et est bien un élément de $K_0(x^{\frac{1}{p}})$. Ce corps est donc bien stable par ϕ.
Soit maintenant $\phi_i \in \mathrm{Gal}(K_0(x^{\frac{1}{p}})/K_0)$. Remarquons pour commencer que $\tau(x^{\frac{1}{p}})$ est une racine p-ième de x, on a par conséquent $\tau(x^{\frac{1}{p}}) = \zeta_p^a x^{\frac{1}{p}}$ avec $a \in \{0, \cdots, p-1\}$. Montrons que $\tau \circ \phi_i \circ \tau = \phi_{-i}$:

$$\begin{aligned} \tau \circ \phi_i \circ \tau(x^{\frac{1}{p}}) &= \tau \circ \phi_i(\zeta_p^a x^{\frac{1}{p}}) \\ &= \tau \circ (\zeta_p^i \zeta_p^a x^{\frac{1}{p}}) \\ &= \zeta_p^{-i} \zeta_p^{-a} \zeta_p^a x^{\frac{1}{p}} \\ &= \zeta_p^{-i} x^{\frac{1}{p}} \\ &= \phi_{-i}(x^{\frac{1}{p}}). \end{aligned}$$

On a donc bien finalement $K_0(x^{\frac{1}{p}}) \subset H_0(p)^-$. □

Proposition 2.4.2. *Soit $x \in K_0$ tel que $x\tau(x) = 1$ et tel que l'extension $K_0(x^{\frac{1}{p}})$ soit non-ramifiée. Alors $K_0(x^{\frac{1}{p}})$ est contenue dans $H_0(p)^+$.*

Démonstration. Commençons par vérifier que $K_0(x^{\frac{1}{p}})$ est galoisienne sur K_0^+. Il suffit pour cela de vérifier que cette extension est stabilisée par τ. Or $\tau(x^{\frac{1}{p}})^p = \tau(x) = x^{-1}$. Par conséquent $\tau(x^{\frac{1}{p}})$ est une racine p-ième de x^{-1} et est donc bien un élément de $K_0(x^{\frac{1}{p}})$. On a de plus $\tau(x^{\frac{1}{p}}) = \zeta_p^a x^{\frac{-1}{p}}$.
Considérons maintenant un élément $\phi_i \in \mathrm{Gal}(K_0(x^{\frac{1}{p}})/K_0)$ et montrons que $\tau \circ \phi_i \circ \tau = \phi_i$.

$$\begin{aligned} \tau \circ \phi_i \circ \tau(x^{\frac{1}{p}}) &= \tau \circ \phi_i(\zeta_p^a x^{\frac{-1}{p}}) \\ &= \tau \circ (\zeta_p^{-i}\zeta_p^a x^{\frac{-1}{p}}) \\ &= \zeta_p^i \zeta_p^a \zeta_p^{-a} x^{\frac{1}{p}} \\ &= \zeta_p^i x^{\frac{1}{p}} \\ &= \phi_i(x^{\frac{1}{p}}). \end{aligned}$$

Et finalement, on a bien $K_0(x^{\frac{1}{p}}) \subset H_0(p)^+$. □

Il nous reste maintenant à étudier la réciproque des propositions qui précèdent.

Proposition 2.4.3. *Le radical kummérien de $(H_0(p))^-$ est engendré par des éléments de $K_0^+ \otimes \mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Notons tout d'abord que l'extension $(H_0(p))^-$ est galoisienne sur K_0^+. En effet, d'une part la conjugaison complexe agit trivialement sur $\mathrm{Gal}(H_0(p)/H_0(p)^-) = \mathrm{Gal}(H_0(p)/K_0^+)^+$ et d'autre part le groupe $\mathrm{Gal}(H_0(p)/K_0)$ est abélien. Ces deux faits assurent que $\mathrm{Gal}(H_0(p)/H_0(p)^-)$ est un sous groupe distingué de $\mathrm{Gal}(H_0(p)/K_0^+)$. L'extension $(H_0(p))^-$ est donc bien galoisienne sur K_0^+.
Soit maintenant $K_0(x^{\frac{1}{p}})/K_0$ une sous-extension de $H_0(p)^-$. Cette extension n'est pas nécessairement galoisienne sur K_0^+, cependant la clôture galoisienne de cette extension sur K_0^+ est $K_0(x^{\frac{1}{p}}, \tau(x)^{\frac{1}{p}})$, cette clôture étant bien évidemment contenue dans $H_0(p)^-$.
Deux phénomènes peuvent se produire : ou bien $K_0(x^{\frac{1}{p}}) = K_0(\tau(x)^{\frac{1}{p}})$, ou bien $K_0(x^{\frac{1}{p}}) \neq K_0(\tau(x)^{\frac{1}{p}})$.
Si $K_0(x^{\frac{1}{p}}) \neq K_0(\tau(x)^{\frac{1}{p}})$, alors $\mathrm{Gal}(K_0(x^{\frac{1}{p}}, \tau(x)^{\frac{1}{p}})/K_0) \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Or dans ce cas, $K_0(x^{\frac{1}{p}}, \tau(x)^{\frac{1}{p}})$ contiendrait comme sous-extension $K_0((\frac{x}{\tau(x)})^{\frac{1}{p}})$. Cette sous-extension est non triviale, en effet $\frac{x}{\tau(x)} \in K_0^p \Rightarrow K_0(x^{\frac{1}{p}}) = K_0(\tau(x)^{\frac{1}{p}})$, et est contenue dans la partie + de $H_0(p)$ (Cf prop 2.4.2). On a donc nécessairement $K_0(x^{\frac{1}{p}}) = K_0(\tau(x)^{\frac{1}{p}})$, l'égalité de ces extensions impliquant que $\tau(x) = x^\alpha y^p$ avec $\alpha \in \{1, \cdots, p-1\}$. Il s'ensuit que $\tau(x)^{\frac{1}{p}} = x^{\frac{\alpha}{p}} y \zeta_p^a$ avec

$a \in \{0, \cdots, p-1\}$. Nous allons montrer que $\alpha \equiv 1 \quad [p]$. En effet,

$$\begin{aligned} \tau \circ \phi_i \circ \tau(x^{\frac{1}{p}}) &= \tau \circ \phi_i(x^{\frac{\alpha}{p}} y \zeta_p^a) \\ &= \tau \circ \phi_i(x^{\frac{1}{p}})^\alpha y \zeta_p^a \\ &= \tau[\zeta_p^{\alpha i} x^{\frac{\alpha}{p}} y \zeta_p^a] \\ &= \zeta_p^{-\alpha i} \tau(x^{\frac{\alpha}{p}}) \tau(y) \zeta_p^{-a}. \end{aligned}$$

Or $\tau(x^{\frac{1}{p}}) = x^{\frac{\alpha}{p}} y \zeta_p^a \Leftrightarrow x^{\frac{1}{p}} = \tau(x^{\frac{\alpha}{p}}) \tau(y) \zeta_p^{-a}$ et par conséquent

$$\tau \circ \phi_i \circ \tau(x^{\frac{1}{p}}) = \zeta_p^{-\alpha i} x^{\frac{1}{p}}.$$

Or, comme $K_0(x^{\frac{1}{p}}) \subset H_0(p)^-$, on a $\tau \circ \phi_i \circ \tau = \phi_{-i}$ et nécessairement $\alpha \equiv 1 \quad [p]$.
On a donc finalement $\tau(x) = xy^p \Rightarrow x\tau(x) = x^2 y^p$. Les extensions $K_0(x^{\frac{1}{p}})$ et $K_0((x\tau(x))^{\frac{1}{p}})$ coïncident donc bien et l'on a ainsi trouvé un élément de K_0^+ engendrant $K_0(x^{\frac{1}{p}})$. □

Proposition 2.4.4. *Le radical kummérien de $H_0(p)^+$ est engendré par des éléments de module 1 (i.e. des éléments x tels que $x\tau(x) = 1$).*

Démonstration. Soit $x \in K_0$ tel que $K_0(x^{\frac{1}{p}}) \subset H_0(p)^+$. Si $K_0(x^{\frac{1}{p}}, \tau(x)^{\frac{1}{p}})$ était de degré p^2 sur K_0, elle contiendrait comme sous-extension non-triviale $K_0((x\tau(x))^{\frac{1}{p}})$, ce qui contredirait le fait que $K_0(x^{\frac{1}{p}}) \subset H_0(p)^+$. L'extension $K_0(x^{\frac{1}{p}})$ est donc galoisienne sur K_0^+.
Du fait que $K_0(x^{\frac{1}{p}}) = K_0(\tau(x)^{\frac{1}{p}})$, on a $\tau(x) = x^\alpha y^p$ avec $\alpha \in \{1, \cdots, p-1\}$ et $y \in K_0$. Il s'ensuit que $\tau(x)^{\frac{1}{p}} = x^{\frac{\alpha}{p}} y \zeta_p^a$. Un calcul en tout point similaire à celui effectué dans la démonstration de la proposition 2.4.3 montre alors que l'on a nécessairement $\alpha \equiv -1 \quad [p]$ et donc $x\tau(x) = y^p \Rightarrow \frac{\tau(x)}{x} = x^{-2} y^p$. Par conséquent, l'élément $\frac{x}{\tau(x)}$ est un complexe de module 1 et une de ses racines p-ième engendre bien l'extension $K_0(x^{\frac{1}{p}})$. □

2.5 Radicaux kummériens et capitulation

La conjecture de Greenberg prédit la nullité de l'invariant λ associé au module d'Iwasawa non-ramifié X_∞ d'un corps de nombres totalement réel F.
Relativement au cadre dans lequel nous évoluons, elle prédit donc la nullité de l'invariant λ associé à la partie + du module d'Iwasawa non-ramifié $X_\infty(K_0)$, qui n'est autre que le module d'Iwasawa non-ramifié associé à K_0^+.
Cette conjecture peut être reformulée en termes d'idéaux. En effet, dans [8] l'auteur montre que la nullité de l'invariant λ associé à $X_\infty(K_0)^+$ est équivalente au fait que tous les idéaux de K_n^+ sont principaux dans K_m^+,

pour m suffisamment grand. De façon formelle, la conjecture de Greenberg peut donc s'énoncer de la façon suivante :

Conjecture 1 (Greenberg). *La restriction à A_n^+ de l'application $j_{n,m} : A_n \to A_m$, induite par l'inclusion naturelle $K_n \to K_m$, est triviale pour $m >> n$.*

On sait par ailleurs que cette conjecture est également équivalente à l'égalité des modules X_∞^- et $\mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)^-$ (Il s'agit du corollaire 1.5.3 figurant au premier chapitre) . En d'autres termes, toute p-extension non-ramifiée de K_∞, sur laquelle la conjugaison complexe agit via la multiplication par -1, est engendrée par des racines p-primaires d'unités.
Nous allons dans cette section étudier la relation entre la capitulation de la p-partie de A_0^+ et le radical Kummérien associé à l'extension $H_0(p)K_n/K_n$ pour $n >> 0$.

Théorème 2.5.1. *Supposons l'application $A_0^+ \to A_n^+$ triviale. Alors il existe des unités $u_1, \cdots, u_s$ de K_n telle que $K_n H_0(p)^- = K_n(u_i^{\frac{1}{p}}, 1 \leq i \leq s)$.*

Démonstration. Soit x tel que $K_0(x^{\frac{1}{p}}) \subset H_0(p)^-$. En vertu de la proposition 2.4.3, on peut supposer que $x \in K_0^+$.
Décomposant dans K_0^+ l'idéal principal engendré par x en produit d'idéaux premiers, on obtient :

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}}.$$

L'hypothèse de non-ramification implique que $a_\mathfrak{p} \equiv 0 \quad [p]$. Or par hypothèse $A_0^+ \to A_n^+$ est triviale, les idéaux premiers $\mathfrak{p}$ sont donc principaux dans K_n^+ et a fortiori dans K_n, de sorte que l'on peut écrire $\mathfrak{p} = (y_\mathfrak{p})$ avec $y_\mathfrak{p} \in K_n$.
On a donc dans K_n :

$$(x) = \prod_{\mathfrak{p}} (y_\mathfrak{p})^{a_\mathfrak{p}},$$

ce qui implique compte tenu du fait que $a_\mathfrak{p} \equiv 0 \quad [p]$ qu'il existe une unité u_n de K_n :

$$x = y^p u_n.$$

Finalement l'extension $K_n(x^{\frac{1}{p}})$ est également engendrée par $u_n^{\frac{1}{p}}$. □

2.6 Cas de l'extension non-ramifiée en dehors de p

Notons M_0 la pro-p-extension abélienne non-ramifiée en dehors de p maximale de K_0 et considérons l'extension de K_0 dont le groupe de Galois est isomorphe à $\mathfrak{X}_0/p$. Que peut-on dire du radical kummérien de cette extension ? Si l'on se donne une p-unité u de K_0, il est clair que l'extension $K_0(u^{\frac{1}{p}})/K_0$ est non-ramifiée en dehors de p. Une première conséquence de

ce fait est que le $\mathbb{F}_p$-rang de M_0/p est supérieur ou égal à $r+s+1$, avec $r = r_1 + r_2 - 1$ et s désignant le nombre de p-places.
Réciproquement, donnons nous un élément x tel que $x \otimes \frac{1}{p}$ appartienne au radical kummérien de l'extension M_0/p et désignons par S_p l'ensemble des p-places de K_0. On a alors :

$$(x) = \prod_{\mathfrak{p} \notin S_p} \mathfrak{p}^{pb_\mathfrak{p}} \prod_{\mathfrak{p} \in S_p} \mathfrak{p}^{a_\mathfrak{p}} = (y)^p \prod_i \mathfrak{P}_i^{p \sum_{\mathfrak{p} \notin S_p} b_\mathfrak{p}} \prod_{\mathfrak{p} \in S_p} \mathfrak{p}^{a_\mathfrak{p}}.$$

Les éléments $x \otimes \frac{1}{p}$ et $xy^{-p} \otimes \frac{1}{p}$ engendrant la même extension, on en déduit que l'extension $K_0(x^{\frac{1}{p}})/K_0$ est également engendrée par la racine p-ième d'une S'-unité, où $S' := S_{Cl(K_0)} \cup S_p$.
Réciproquement, pour que la racine p-ième d'une S'-unité engendre une extension non-ramifiée en dehors de p, il est nécessaire et suffisant que la valuation de cette S'-unité en toute place ne divisant pas p soit divisible par p. Cela signifie que dans le cas non-ramifié en dehors de p, la détermination du radical Kummérien associé à l'extension de K_0 de groupe de Galois M_0/p se ramène à un simple calcul de valuations.
Avant d'énoncer le principal résultat de cette section, introduisons quelques notations. Soient $u_1, \cdots, u_r, y_1, \cdots, y_s$ une base des S'-unités telle que $u_1, \cdots, u_r$ soit une base des unités, $y_1, \cdots, y_s$ soit une base des S'-unités modulo les unités (l'extistence d'une telle base découle du théorème de Dirichlet, figurant par exemple dans [21]).
Toute S'-unité x s'écrit alors sous la forme $x = \mu u y$ avec $u = \prod_i u_i^{a_i}, v = \prod_j y_j^{b_j}$ et μ racine de l'unité. De plus la valuation en un place quelconque de x est égale à celle de v.
Notons $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ les non-p-places de S' et définissons alors la matrice $V = (v_{i,j}) \in M_{t,s}(\mathbb{Z})$ par

$$v_{i,j} = v_{\mathfrak{p}_i}(y_j).$$

Proposition 2.6.1. *Soit $x = u \prod_j y_j^{b_j}$ une S'-unité. Notons B le vecteur colonne dont les composantes sont les b_j. Alors l'extension $K_0(x^{\frac{1}{p}})$ est non-ramifiée en dehors de p si et seulement si*

$$VB \equiv 0 \quad [p].$$

Démonstration. En effet les composantes du vecteur colonne VB ne sont autre que les valuations de x en les non-p-places. □

Corollaire 2.6.2. *Notons k la dimension du noyau de V, considéré comme élément de $\mathcal{M}_{t,s}(\mathbb{F}_p)$, alors :*

$$\mathrm{Rang}_{\mathbb{F}_p} \mathfrak{X}_0/p = r + k.$$

2.7 Approche numérique

Nous avons vu que le radical kummérien associé à l'extension abélienne non-ramifiée d'exposant p maximale d'un corps de nombres K_0, contenant ζ_p, était engendré par des S-unités. Or, la conjecture de Greenberg prédit la finitude du module $\mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)$. En d'autres termes, presque toutes les p-extensions non-ramifiées abéliennes de K_∞, sont obtenues en extrayant des racines p-primaires d'unités.
Une question se pose alors naturellement : que se passe-t-il au niveau fini ? Plus précisément, si l'on considère un ensemble fini $\mathcal{F}_N$ constitué de corps K_0 contenant ζ_p, que peut on dire du rapport

$$f(\mathcal{F}_N, p) = \frac{\#\{K_0 \in \mathcal{F}_N / \exists u \in U_{K_0} \text{ t.q. } K_0(u^{\frac{1}{p}})/K_0 \text{ soit n.r.}\}}{\#\{K_0 \in \mathcal{F}_N / A_0(K_0) \neq 1\}} \quad ?$$

Nous nous intéressons aux deux cas particuliers suivants :

1) $\mathcal{F}_N$ est constitué de corps du type $\mathbb{Q}(\sqrt{d}, j)$, j désignant une racine primitive troisième de l'unité et p étant égal à 3.
2) $\mathcal{F}_N$ est constitué de corps du type $F(j)$ avec $F/\mathbb{Q}$ extension cyclique de degré 3 et $p = 3$.

2.7.1 Méthode du calcul

Soit S un ensemble quelconque de places et u une S-unité. Pour déterminer si l'extension de K_0 engendrée par $u^{\frac{1}{p}}$ est non-ramifiée nous utilisons la méthode suivante :

1. On étudie la ramification en les non-p-places, ce qui se ramène à un calcul de valuation. Si l'extension étudiée est ramifiée en une non-p-place, le calcul s'arrête.
2. Sinon, on étudie la ramification en les p-places. Pour une p-place v donnée :
   (a) On calcule $v(u)$, si $v(u) \not\equiv 0 \ [p]$, alors l'extension est nécessairement ramifiée et le calcul s'arrête.
   (b) Sinon, on distingue deux cas, suivant que l'extension $K_v/\mathbb{Q}_p$ soit modérément ramifiée ou non.
      i. Si l'extension $K_v/\mathbb{Q}_p$ est modérément ramifiée, on utilise la proposition 2.2.2 qui permet de conclure.
      ii. Si l'extension $K_v/\mathbb{Q}_p$ est sauvagement ramifiée, on utilise la seconde partie de la proposition 2.2.4, qui donne une condition suffisante de ramification. Si cette condition n'est pas vérifiée, on calcule alors explicitement l'extension $K_0(u^{\frac{1}{p}})/K_0$ utilisant la commande rnfinit.

Cette méthode est implémentée dans le programme **look.gp**, figurant en annexe de la thèse.

Utilisant le logiciel pari-gp, nous obtenons les résultats suivants.

2.7.2 Cas des corps quadratiques réels

L'ensemble $\mathcal{F}_N$ est dans ce cas constitué de l'ensemble des corps quadratiques totalement réels dont le discriminant est inférieur ou égal à N, auxquels on a adjoint j, racine primitive troisième de l'unité.

N	$f(\mathcal{F}_N, 3)$
100	0.98
500	0.90
1000	0.86
2000	0.83
5000	0.82

2.7.3 Cas des extensions cycliques de degré 3

L'ensemble $\mathcal{F}_N$ est dans ce cas constitué de l'ensemble des corps cycliques de degré 3, contenus dans $\mathbb{Q}(\zeta_n)$ pour $n \leq N$, auxquels on a adjoint j, racine primitive troisième de l'unité.

N	$f(\mathcal{F}_N, 3)$
10	1
20	0.8
30	0.76
40	0.68
50	0.63
60	0.68
70	0.66
80	0.60
90	0.63
100	0.63
110	0.64
120	0.65
130	0.63
140	0.64
150	0.67
200	0.65

Bien évidemment, il serait intéressant d'effectuer ce type de calcul pour de grandes valeurs de N. Cependant, lorsque l'on essaye des valeurs de N plus grandes le calcul n'aboutit pas pour des raisons inhérentes au logiciel pari-gp .

En effet, nous avons vu que dans le cas d'une extension $K_0/\mathbb{Q}$ sauvagement ramifiée l'étude de la ramification d'une extension du type $K_0(u^{\frac{1}{p}})$ nécessite de calculer effectivement cette extension (i.e. avec **rnfinit**). Or l'utilisation de cette commande semble problématique.

Chapitre 3

Module d'Iwasawa et conoyaux de capitulation.

3.1 Introduction

Donnons-nous un corps totalement réel F et considérons pour p nombre premier impair le corps $K_0 = F(\zeta_p)$. On notera K_∞ la $\mathbb{Z}_p$-extension cyclotomique de K_0. Les corps L_∞, L'_∞ et M_∞ désigneront les pro-p-extensions abéliennes maximales de K_∞, qui sont respectivement non-ramifiée, non-ramifiée et totalement décomposée en les p-places, non-ramifiée en dehors de p. Les groupes de Galois $X_\infty = \mathrm{Gal}(L_\infty/K_\infty), X'_\infty = \mathrm{Gal}(L'_\infty/K_\infty)$ et $\mathfrak{X}_\infty = \mathrm{Gal}(M_\infty/K_\infty)$ sont naturellement munis d'une structure de Λ-module, où Λ est l'algèbre d'Iwasawa usuelle.
On supposera en outre que tous les étages de K_∞ vérifient la conjecture de Gross. Cette conjecture, qui prédit pour tout entier n la finitude du quotient $(X'_\infty)_{\Gamma_n}$, est démontrée dans le cas abélien (voir [15]).
Le corps K_∞ contenant les racines p-primaires de l'unité, on peut utiliser la théorie de Kummer pour décrire les extensions d'exposant p-primaires de K_∞. On notera N_∞ et N'_∞ les extensions obtenues en ajoutant à K_∞ respectivement les racines p-primaires d'unités et de p-unités. Les extensions N_∞ et N'_∞ sont toutes deux contenues dans M_∞. Dans [13], Iwasawa démontre que les Λ-modules $\mathrm{Gal}(M_\infty/N_\infty)$ et $\mathrm{Gal}(M_\infty/N'_\infty)$ sont de Λ-torsion. Les extensions N_∞ et N'_∞ contiennent donc toutes deux l'extension T_∞ de K_∞, définie par $\mathrm{Gal}(M_\infty/T_\infty) = tor_\Lambda(\mathfrak{X}_\infty)$, et l'on dispose ainsi d'une tour d'extensions $K_\infty \subset T_\infty \subset N_\infty \subset N'_\infty \subset M_\infty$.
Enfin désignons par K_∞^{BP} l'extension de K_∞ dont le groupe de Galois sur K_∞ est le module de Bertrandias-Payan de K_∞. Le module de Bertrandias-Payan a notamment été défini et étudié dans [19], [22] et [1].
Désignons par A_n la p-partie du groupe des classes d'idéaux de K_n et par A_∞ la limite inductive des A_n. Dans [12], Ichimura démontre le théorème suivant :

Théorème (Ichimura). *Si le degré de F sur $\mathbb{Q}$ est étranger à p, alors la $\mathbb{Z}_p$-torsion du Λ-module $Gal(N_\infty \cap L_\infty/K_\infty)^-$ est isomorphe, en tant que que groupe abélien, à la partie $+$ du conoyau de capitulation $coker(A_0 \to A_\infty^\Gamma)^+$.*

Dans sa démonstration, Ichimura décompose le Λ-module $\mathrm{Gal}(N_\infty \cap L_\infty/K_\infty)^-$ en somme directe de ses Φ-composantes, Φ parcourant l'ensemble des caractères impairs du groupe de Galois G de K_0 sur $\mathbb{Q}$. Le point essentiel de sa démonstration est le fait que dans le cas semi-simple les Φ-parties du module des unités semi-locales sont isomorphes à Λ_Φ ou à $\Lambda_\Phi \oplus \mathbb{Z}_p(1)$, suivant que $\Phi(p) \neq 1$ ou que $\Phi(p) = 1$. En particulier, lorsque $\Phi(p) \neq 1$, le Λ_Φ-module $\mathcal{U}_\infty(\Phi)$ est monogène. Or l'on sait (voir par exemple [25] prop. 5.2) que $\mathcal{U}_\infty(\Phi)$ n'est plus monogène dans le cas non semi-simple. Il semble donc difficile d'adapter au cas non-semi-simple la démonstration d'Ichimura. De plus, le résultat qu'il obtient ne prend pas en compte la structure galoisienne des modules considérés.
Si les noyaux de capitulation ($\ker(A_n \to A_\infty)^+$) ont été abondamment étudiés, car reliés à la conjecture de Greenberg (voir [8]), les conoyaux de capitulation n'ont fait l'objet pour l'instant que de peu de publications. La principale référence sur le sujet est l'article [19], dans lequel les auteurs étudient les conoyaux de capitulation associés à $A'_\infty = \varinjlim A'_n$, où A'_n est le quotient du groupe des classes d'idéaux A_n par le sous groupe de A_n, engendré par les p-places de K_n. Les auteurs montrent sans se restreindre au cas semi-simple le théorème suivant, qui prend en compte la structure galoisienne des modules :

Théorème (Le Floc'h,Movahhedi,Nguyen). *Pour $n >> 0$, le conoyau de capitulation $coker(A'_n \to (A'_\infty)^{\Gamma_n})$ est galoisiennement isomorphe à* $\mathrm{Hom}(Gal(N'_\infty \cap K_\infty^{BP}/T_\infty), \mu_{p^\infty})$.

Afin de généraliser le résultat d'Ichimura, on se propose dans ce chapitre de démontrer que les parties $-$ des modules $\mathrm{Gal}(N_\infty \cap L_\infty/K_\infty)$ et $\mathrm{Gal}(N'_\infty \cap K_\infty^{BP}/T_\infty)$ sont galoisiennement isomorphes et l'on en déduira le théorème suivant :

Théorème. *La $\mathbb{Z}_p$-torsion du Λ-module $Gal(N_\infty \cap L_\infty/K_\infty)^-$ est isomorphe au dual de Kummer du conoyau de capitulation :*

$$\mathrm{Hom}((coker(A_n \to (A_\infty)^{\Gamma_n})^+), \mu_{p^\infty}) \quad \text{pour} \quad n >> 0.$$

Pour arriver à ce résultat, nous commençons par étudier un sous-module de $\mathrm{Gal}(N'_\infty \cap L'_\infty/K_\infty)$, dont la $\mathbb{Z}_p$-torsion est isomorphe au conoyau de capitulation. On vérifie ensuite que le quotient de $\mathrm{Gal}(N'_\infty \cap L'_\infty/K_\infty)$ par ce sous-module est sans $\mathbb{Z}_p$-torsion. On se ramène au cas non-ramifié en utilisant le fait que les modules $(X_\infty)^+$ et $(X'_\infty)^+$ sont pseudo-isomorphes.
La section 2 expose le contexte du problème que nous étudions. Après avoir précisé les différentes actions galoisiennes que nous utiliserons dans ce

chapitre, nous montrerons la Λ-liberté de la limite projective des $\mathcal{M}_{n,v}/\mu_n$, où $\mathcal{M}_{n,v}$ est le pro-p-complété de $K_{n,v}^*$ et μ_n le groupe des racines p-primaires de l'unité contenus dans $K_{n,v}^*$. S'en suivront quelques propriétés élémentaires relatives au module de Bertrandias-Payan et nous rappellerons pour finir certains résultats de la théorie de Kummer relatifs aux modules d'Iwasawa étudiés dans ce chapitre.
La section 3 reprend de nombreux résultats de [19], qui seront utilisés par la suite et propose pour certains d'entre eux des démonstrations alternatives.
La section 4 fait le lien entre les travaux d'Ichimura et ceux de Le Floc'h, Movahhedi, Nguyen-Quang-Do, travaux figurant respectivement dans [11] et [19]. On verra en outre que les méthodes de Le Floc'h, Movahhedi et Nguyen-Quang-Do permettent de généraliser les résultats d'Ichimura, d'une part parce qu'elles permettent de se passer de l'hypothèse de semi-simplicité et d'autre part parce qu'elles prennent en compte le caractère galoisien des modules considérés.
La section 5 étudie quelques implications de la conjecture de Greenberg dans le contexte que nous avons étudié.

3.2 Contexte du problème

Dans cette section et dans celle qui suit, nous survolons des résultats connus, figurant notamment dans [11], [13] ou [19]. Pour le commodité du lecteur, nous redémontrons certains de ces résultats.
Avant d'entrer dans le vif du sujet, nous allons préciser les diverses actions galoisiennes que nous utiliserons. On désignera par Γ le groupe de Galois de K_∞/K_0. Le groupe des racines p-primaires de l'unité μ_{p^∞} étant contenu dans K_∞, le groupe Γ opère sur μ_{p^∞} et le caractère cyclotomique κ est défini sur Γ.

3.2.1 Actions galoisiennes

Un $\mathbb{Z}_p[[\Gamma]]$-module M étant donné, on dispose d'une action de Γ sur M, i.e. d'un morphisme de groupe $\Gamma \to Aut(M)$. Un morphisme de $\mathbb{Z}_p[[\Gamma]]$-module est alors un morphisme de $\mathbb{Z}_p$-module, compatible avec l'action de Γ. Cependant, il arrive assez fréquemment lorsque on étudie les relations entre deux $\mathbb{Z}_p[[\Gamma]]$-modules que l'on ait affaire à des morphismes qui sont uniquement des $\mathbb{Z}_p$-morphismes et ne respectent a priori pas l'action de Γ. Dans ce cas, il est fréquent que l'on modifie l'action de Γ sur l'un des deux modules afin que le morphisme considéré devienne un morphisme de $\mathbb{Z}_p[\Gamma]$-module.
L'action de Γ sur le module M peut être tordue de différentes façons. Tout d'abord en utilisant le caractère cyclotomique κ :

Définition 3.2.1. *Le module $M(i)$ est le module M sur lequel l'action de Γ a été tordu i fois par le caractère cyclotomique, l'action de Γ sur $M(i)$ est alors défini par le morphisme qui suit :*

$$\begin{array}{ccc} \Gamma & \to & Aut(M) \\ \gamma & \mapsto & (m \mapsto \kappa(\gamma)^i \gamma.m) \end{array}$$

Il découle alors immédiatement de la définition de κ que $\mathbb{Q}_p/\mathbb{Z}_p(1) = \mu_{p^\infty}$, l'action initiale de Γ sur $\mathbb{Q}_p/\mathbb{Z}_p$ étant l'action triviale.
Par ailleurs, dans l'étude de la théorie de l'adjoint d'un module d'Iwasawa figurant dans [26] (chapitre 15), l'auteur définit le module $\widetilde{M}$, comme le module M sur lequel l'action de Γ a été inversée. Plus précisément :

Définition 3.2.2. *Étant donné un $\mathbb{Z}_p[[\Gamma]]$-module M, on note $\widetilde{M}$ le module M sur lequel l'action de Γ est définie par le morphisme qui suit :*

$$\begin{array}{ccc} \Gamma & \to & Aut(\widetilde{M}) \\ \gamma & \mapsto & (m \mapsto \gamma^{-1}.m). \end{array}$$

Remarque. *L'action définie en 3.2.2 est plus générale dans le sens où elle peut être définie pour un Λ-module quelconque. Tandis que pour définir l'action tordue (définition 3.2.1), il est nécessaire de disposer d'une action de Γ sur μ_{p^∞}.*

Enfin, si M désigne un $\mathbb{Z}_p$-module, le dual de Pontryagin de M, $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, est noté $M^\vee$. Si Γ agit sur M, on fait usuellement agir Γ sur $M^\vee$ de la façon suivante :

$$\begin{array}{ccc} \Gamma & \to & Aut(M^\vee) \\ \gamma & \mapsto & (\phi \mapsto (m \mapsto \phi(\gamma^{-1}m)). \end{array}$$

Citons enfin une propriété bien connue, découlant immédiatement de la définition de module tordu, que nous utiliserons fréquemment :

Proposition 3.2.3. *Soit M un $\mathbb{Z}_p[[\Gamma]]$-module, alors* $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mu_{p^\infty}) = M^\vee(1)$.

On sait par ailleurs que l'anneau $\mathbb{Z}_p[[\Gamma]]$ est isomorphe à l'anneau de séries formelles à une indéterminée à coefficients dans $\mathbb{Z}_p$, usuellement noté Λ. Dans toute la suite de ce chapitre, nous identifierons donc $\mathbb{Z}_p[[\Gamma]]$ et Λ, de sorte que l'on considère implicitement que l'on dispose d'une action de Λ sur μ_{p^∞}.

Utilisant l'action définie en 3.2.2, la théorie de l'adjoint permet de relier A_∞ au module d'Iwasawa non-ramifiée X_∞ de la façon suivante :

Proposition 3.2.4. *Le dual de Pontryagin de la limite inductive $A_\infty = \varinjlim A_n$ est pseudo-isomorphe à $\widetilde{X_\infty}$.*

Remarque. *Le lecteur désirant une démonstration détaillée de ce résultat peut consulter [26] page 359. Rappelons toutefois le schéma de cette preuve : utilisant les propriétés de descente de X_∞, on montre que $A_\infty^\vee$ est pseudo isomorphe à l'adjoint $\alpha(X_\infty)$ de X_∞ sur lequel l'action galoisienne a été inversée, on a donc $A_\infty^\vee \sim \widetilde{\alpha(X_\infty)}$. Le résultat découle alors du fait que l'adjoint de X_∞, qui est un Λ-module de torsion, est pseudo-isomorphe à X_∞.*

3.2.2 Λ-liberté de $\mathcal{N}_{\infty,v}$

Fixons une p-place v de K_∞ et notons $\mathcal{M}_{n,v}$ le pro-p-complété du groupe multiplicatif $K_{n,v}^*$. La limite projective relativement à la norme des $\mathcal{M}_{n,v}$ sera notée $\mathcal{M}_{\infty,v}$. Le groupe des racines de l'unité p-primaires μ_n de $K_{n,v}$ est exactement la $\mathbb{Z}_p$-torsion de $\mathcal{M}_{n,v}$. Notons $\mathcal{N}_{n,v}$ le quotient de $\mathcal{M}_{n,v}$ par μ_n, et $\mathcal{N}_{\infty,v}$ la limite projective des $\mathcal{N}_{n,v}$.
Nous allons voir ici que le module $\mathcal{N}_{\infty,v}$ est Λ-libre. Ce résultat est bien connu et figure par exemple dans [13] ou dans [21], nous le redémontrons ici par une méthode plus cohérente avec la ligne générale de ce chapitre. La Λ-liberté de $\mathcal{N}_{\infty,v}$ est équivalente à la trivialité de $\mathcal{N}_{\infty,v}^\Gamma$ et à la $\mathbb{Z}_p$-liberté de $(\mathcal{N}_{\infty,v})_\Gamma$ (voir prop. 5.3.19 de [21]).

Proposition 3.2.5. *Le module $(\mathcal{N}_{\infty,v})_\Gamma$ est $\mathbb{Z}_p$-libre.*

Démonstration. De la suite exacte

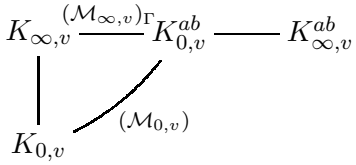
$$1 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathcal{M}_{\infty,v} \longrightarrow \mathcal{N}_{\infty,v} \longrightarrow 1\ ,$$

on déduit le diagramme suivant :

$$\begin{array}{ccccccc} & & \mathbb{Z}_p(1)_\Gamma & \longrightarrow & (\mathcal{M}_{\infty,v})_\Gamma & \longrightarrow & (\mathcal{N}_{\infty,v})_\Gamma \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 \longrightarrow & tor_{\mathbb{Z}_p}(\mathcal{M}_{0,v}) & \longrightarrow & \mathcal{M}_{0,v} & \longrightarrow & \mathcal{N}_{0,v} & \longrightarrow 1. \end{array}$$

Commençons par remarquer que $\mathbb{Z}_p(1)_\Gamma \simeq \mathbb{Z}_p/(\kappa(\gamma)-1)\mathbb{Z}_p \simeq \mu_{p^\infty}(\mathcal{M}_{0,v}) = tor_{\mathbb{Z}_p}(\mathcal{M}_{0,v})$. La flèche verticale de gauche, qui est surjective, est donc un isomorphisme. On en déduit en particulier que $\mathbb{Z}_p(1)_\Gamma$ s'injecte dans $(\mathcal{M}_{\infty,v})_\Gamma$.
La flèche verticale du milieu est injective. En effet par la théorie locale du Corps de Classes, $\mathcal{M}_{0,v}$ est isomorphe via l'application d'Artin à la pro-p-extension abélienne maximale de $K_{0,v}$, tandis que $(\mathcal{M}_{\infty,v})_\Gamma$ correspond à la pro-p-extension abélienne maximale de $K_{\infty,v}$, qui soit abélienne sur $K_{0,v}$.

Ces deux extensions coïncidant, on a :



On en déduit donc que la flèche verticale du milieu est une injection, dont le conoyau est isomorphe à $\mathbb{Z}_p$.
Finalement, l'application du lemme du serpent montre que $(\mathcal{N}_{\infty,v})_\Gamma$ s'injecte dans $\mathcal{N}_{0,v}$. Le module $\mathcal{N}_{0,v}$ étant $\mathbb{Z}_p$-libre par définition, on en déduit la $\mathbb{Z}_p$-liberté de $(\mathcal{N}_{\infty,v})_\Gamma$. □

Proposition 3.2.6. *On a* $\mathcal{N}_{\infty,v}^\Gamma = 1$.

Démonstration. Partons de la suite exacte suivante, définissant le module $\mathcal{N}_{\infty,v}$:

$$1 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathcal{M}_{\infty,v} \longrightarrow \mathcal{N}_{\infty,v} \longrightarrow 1.$$

On en déduit :

$$1 \longrightarrow \mathbb{Z}_p(1)^\Gamma \longrightarrow \mathcal{M}_{\infty,v}^\Gamma \longrightarrow \mathcal{N}_{\infty,v}^\Gamma \longrightarrow \mathbb{Z}_p(1)_\Gamma \longrightarrow (\mathcal{M}_{\infty,v})_\Gamma.$$

Or d'une part $\mathcal{M}_{\infty,v}^\Gamma = 1$: en effet soit $x = (x_n) \in \mathcal{M}_{\infty,v}^\Gamma$, on a alors $\gamma(x_n) = x_n$ pour tout entier n. Il s'ensuit que $x_n \in K_{0,v}$ pour tout entier n, or par définition de $\mathcal{M}_{\infty,v}$, on a $x_0 = N_{n,0}(x_n) = x_n^{p^n}$, l'élément x_0 de $K_{0,v}$ est donc infiniment p-divisible et nécessairement $x_0 = 1$. On montre de même que $x_n = 1$ quel que soit l'entier n et donc que $x = 1$.
Et d'autre part, on a vu que $\mathbb{Z}_p(1)_\Gamma$ s'injectait dans $(\mathcal{M}_{\infty,v})_\Gamma$, il s'ensuit que l'application naturelle $\mathcal{M}_{\infty,v}^\Gamma \to \mathcal{N}_{\infty,v}^\Gamma$ est surjective et donc $\mathcal{N}_{\infty,v}^\Gamma = 1$. □

Corollaire 3.2.7. *Le module* $\mathcal{N}_{\infty,v}$ *est* Λ*-libre.*

3.2.3 Le module de Bertrandias-Payan

L'extension K_∞^{BP} de K_∞ est caractérisée par la suite exacte suivante :

$$1 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathrm{Ind}_{G_v}^G \mathbb{Z}_p(1) \xrightarrow{A} \mathrm{Gal}(M_\infty/K_\infty) \longrightarrow \mathrm{Gal}(K_\infty^{BP}/K_\infty) \longrightarrow 1.$$

Le groupe de Galois $\mathrm{Gal}(K_\infty^{BP}/K_\infty)$ est appelé module de Bertrandias-Payan de K_∞ (pour plus de détails voir [23]).
Notons $W_\infty = \mathrm{Gal}(M_\infty/K_\infty^{BP}) = A(\mathrm{Ind}_{G_v}^G \mathbb{Z}_p(1))$ et $V_\infty = \mathrm{Gal}(M_\infty/L'_\infty)$. Le module W_∞ est clairement de Λ-torsion. Notons $\mathcal{M}_\infty = \mathrm{Ind}_{G_v}^G \mathcal{M}_{\infty,v}$, $\mathcal{N}_\infty = \mathrm{Ind}_{G_v}^G \mathcal{N}_{\infty,v}$ et $\overline{U}'_\infty$ la limite projective relativement à la norme des $\overline{U}'_{K_n}$. Les modules V_∞ et W_∞ sont reliés par le diagramme qui suit :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z}_p(1) & \longrightarrow & \mathrm{Ind}_{G_v}^{G}\mathbb{Z}_p(1) & \longrightarrow & W_\infty & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \overline{U}'_\infty & \longrightarrow & \mathcal{M}_\infty & \longrightarrow & V_\infty & \longrightarrow & 1 \end{array} \tag{3.1}$$

La flèche de gauche est injective du fait de l'inclusion triviale $L'_\infty \subset K_\infty^{BP}$. Commençons par énoncer un résultat utile pour la suite relatif à la partie moins du module quotient V_∞/W_∞ :

Proposition 3.2.8. *La partie $-$ de V_∞/W_∞ est Λ-libre.*

Démonstration. Étant donné un Λ-module M, on notera $Fr_\Lambda(M)$ le module quotient $M/tor_\Lambda(M)$.
L'application du lemme du serpent au diagramme (3.1) donne

$$1 \longrightarrow Fr_\Lambda(\overline{U}'_\infty) \longrightarrow Fr_\Lambda(\mathcal{M}_\infty) \longrightarrow V_\infty/W_\infty \longrightarrow 1.$$

Or la partie $-$ de $\overline{U}'_\infty$ est de Λ-torsion, par conséquent $Fr_\Lambda(\overline{U}'_\infty)^- = 1$ et $(V_\infty/W_\infty)^- = Fr_\Lambda(\mathcal{M}_\infty)^- = (\mathcal{N}_\infty)^-$. Or le module $\mathcal{N}_\infty$ est Λ-libre, de plus on a $(\mathcal{N}_\infty^\Gamma)^- = (\mathcal{N}_\infty^-)^\Gamma$ et $((\mathcal{N}_\infty)_\Gamma)^- = ((\mathcal{N}_\infty)_\Gamma)^-$, la Λ-liberté de $\mathcal{N}_\infty^-$ découle donc de celle de $\mathcal{N}_\infty$. □

Pour de plus amples informations sur le module de Bertrandias-Payan, le lecteur intéressé peut consulter [22] ou encore [19].

3.2.4 La conjecture de Gross

Désignons par $X'_\infty = \mathrm{Gal}(L'_\infty/K_\infty)$, qui est naturellement muni d'une structure de Λ-module. Ce module est de type fini et de Λ-torsion, on peut donc définir sa série caractéristique. La conjecture de Gross prédit que cette série caractéristique est étrangère à T, ce qui revient à dire que le quotient $(X'_\infty)_\Gamma$ est fini. Signalons enfin que cette conjecture, tout comme la conjecture de Leopoldt, a été démontrée dans le cas abélien (voir par exemple [15]).

3.2.5 Dualité de Kummer et théorie d'Iwasawa

Le corps K_∞ contenant les racines p-primaires de l'unité, on peut lui appliquer la théorie de Kummer, qui établit une dualité entre les p-extensions de K_∞ et les sous groupes de $K_\infty^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$.
Par définition, les radicaux kummériens associés aux extensions N_∞ et N'_∞ sont respectivement $U_{K_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ et $U'_{K_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Le résultat qui suit, figurant dans [13] et dans [26], permet de décrire le radical kummérien associé à M_∞, considéré respectivement comme extension de N_∞ et de N'_∞.

Proposition 3.2.9. *Les radicaux kummériens des extensions M_∞/N_∞ et M_∞/N'_∞ sont respectivement isomorphes aux limites inductives $A_\infty = \varinjlim A_n$ et $A'_\infty = \varinjlim A'_n$. En d'autres termes $Gal(M_\infty/N_\infty)^\vee(1) = A_\infty$ et $Gal(M_\infty/N'_\infty)^\vee(1) = A'_\infty$. De plus les Λ-modules $Gal(M_\infty/N_\infty)$ et $Gal(M_\infty/N'_\infty)$ sont de torsion et respectivement pseudo-isomorphes à $\widetilde{X_\infty}(1)$ et $\widetilde{X'_\infty}(1)$.*

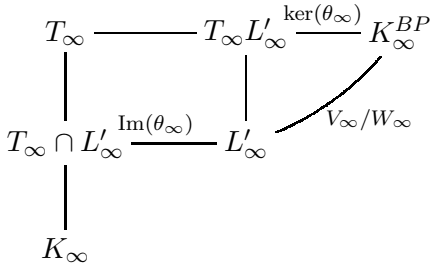
Si l'on note T_∞ l'extension de K_∞ définie par $\mathrm{Gal}(M_\infty/T_\infty) = tor_\Lambda(\mathfrak{X}_\infty)$, on a alors $T_\infty \subset N_\infty \subset N'_\infty$.

3.3 Étude de la $\mathbb{Z}_p$-torsion de $\mathbf{Gal}(N'_\infty \cap L'_\infty/K_\infty)$

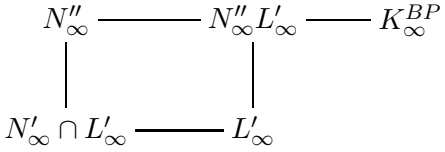
L'objectif de cette partie est de relier la $\mathbb{Z}_p$-torsion de $\mathrm{Gal}(N'_\infty \cap L'_\infty/K_\infty)$ au conoyau de capitulation $\mathrm{coker}(A'_n \to (A'_\infty)^{\Gamma_n})$.
A cette fin, désignons par $N''_\infty = N'_\infty \cap K_\infty^{BP}$. Du fait que $L'_\infty \subset K_\infty^{BP}$, on a immédiatement $N''_\infty \cap L'_\infty = N'_\infty \cap K_\infty^{BP} \cap L'_\infty = N'_\infty \cap L'_\infty$. Rappelons en outre que T_∞ est la sous-extension de M_∞ fixée par $tor_\Lambda(\mathfrak{X}_\infty)$.

Proposition 3.3.1. *La flèche naturelle $Gal(N''_\infty/T_\infty) \to Gal(N'_\infty \cap L'_\infty/T_\infty \cap L'_\infty)$ induit un isomorphisme entre les parties $-$ de ces modules, qui sont finies.*

Démonstration. Compte tenu de la proposition 3.2.9, les extensions N_∞ et N'_∞ contiennent toutes deux T_∞.
Désignons par θ_∞ la flèche naturelle $\mathrm{Gal}(K_\infty^{BP}/T_\infty) \to \mathrm{Gal}(L'_\infty/K_\infty)$. Comme indiqué par le diagramme ci-dessous, on a $\ker(\theta_\infty) = \mathrm{Gal}(K_\infty^{BP}/T_\infty L'_\infty)$ et $\mathrm{Im}(\theta_\infty) = \mathrm{Gal}(L'_\infty/T_\infty \cap L'_\infty)$:



Par ailleurs, par définition de N''_∞, on a $N''_\infty = N'_\infty \cap K_\infty^{BP}$; il découle alors immédiatement de l'inclusion $L'_\infty \subset K_\infty^{BP}$, que $N''_\infty \cap L'_\infty = N'_\infty \cap L'_\infty$. Les relations entre ces différentes extensions étant représentées dans le diagramme qui suit :



En d'autres termes l'image par θ_∞ de $\mathrm{Gal}(K_\infty^{BP}/N''_\infty)$ est $\mathrm{Gal}(L'_\infty/L'_\infty \cap N'_\infty)$. On en déduit donc que θ_∞ réalise une surjection de $\mathrm{Gal}(N''_\infty/T_\infty)$ sur $\mathrm{Gal}(L'_\infty \cap N'_\infty/L'_\infty \cap T_\infty)$.
Par définition de θ_∞, on a $\ker(\theta_\infty) \subset \mathrm{Gal}(K_\infty^{BP}/L'_\infty) = V_\infty/W_\infty$. Comme $\ker(\theta_\infty) \subset \mathrm{Gal}(K_\infty^{BP}/T_\infty)$, le noyau de θ_∞ est de Λ-torsion. De plus on a vu proposition 3.2.8 que $tor_\Lambda(V_\infty/W_\infty)^- = 1$. La partie $-$ du noyau de θ_∞ est donc triviale et θ_∞ réalise nécessairement un isomorphisme entre $\mathrm{Gal}(N''_\infty/T_\infty)^-$ et $\mathrm{Gal}(L'_\infty \cap N'_\infty/L'_\infty \cap T_\infty)^-$.
Enfin, il est connu ([19], th. 2.4) que le module $\mathrm{Gal}(L'_\infty \cap N'_\infty/L'_\infty \cap T_\infty)$ est fini.

□

La proposition précédente apparaît dans [19] (prop. 2.4) et y est démontrée plus généralement et de façon différente. Dans leur démonstration les auteurs utilisent notamment le fait que $W_\infty(-1) = tor_\Lambda(\mathfrak{X}_\infty(-1))^{\Gamma_n}$, résultat démontré dans [27]. La démonstration que nous proposons, qui se limite à la partie $-$, n'utilise pas ce résultat.
La proposition qui suit est largement inspirée de celle du corollaire 2.7 de [19] et en constitue d'ailleurs le point clé.

Proposition 3.3.2. *Le Λ-module $Gal(T_\infty \cap L'_\infty/K_\infty)^-$ est sans $\mathbb{Z}_p$-torsion.*

Démonstration. On a vu que $\mathrm{Gal}(K_\infty^{BP}/T_\infty L'_\infty)^- = 1$ et que $(V_\infty/W_\infty)^-$.
Considérons maintenant la suite exacte

$$1 \longrightarrow \mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty) \longrightarrow \mathrm{Gal}(T_\infty/K_\infty) \longrightarrow \mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty) \longrightarrow 1.$$

On en déduit :

$$\begin{array}{ccccc} (\mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty)^-)^\Gamma & \hookrightarrow & (\mathrm{Gal}(T_\infty/K_\infty)^-)^\Gamma & \longrightarrow & (\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-)^\Gamma \\ & & & & \downarrow \\ & & & & (\mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty)^-)_\Gamma \end{array}$$

Comme le module $\mathrm{Gal}(T_\infty/K_\infty)^-$ est sans Λ-torsion, $(\mathrm{Gal}(T_\infty/K_\infty)^-)^\Gamma = 1$.
Par conséquent la flèche de $(\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-)^\Gamma \to (\mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty)^-)_\Gamma$ est injective.
Par ailleurs, on a vu que $\mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty)^- = (V_\infty/W_\infty)^- = Fr_\Lambda(\mathcal{M}_\infty)^-$.
Par conséquent, $\mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty)^-_\Gamma = Fr_\Lambda(\mathcal{M}_\infty)^-_\Gamma$. Or le module $Fr_\Lambda(\mathcal{M}_\infty)$ est Λ-libre, comme induit de modules Λ_v-libres, on en déduit la $\mathbb{Z}_p$-liberté de $Fr_\Lambda(\mathcal{M}_\infty)_\Gamma$ et donc celle de $\mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty)^-_\Gamma$. De plus K_0 vérifiant la conjecture de Gross, la série caractéristique de X'_∞ est étrangère à T, celle de $\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-$ l'est également et $(\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-)^\Gamma$ est fini.
On a donc nécessairement $(\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-)^\Gamma = 1$. Les étages de la $\mathbb{Z}_p$-extension cyclotomique de K_0 vérifiant également la conjecture de Gross,

on a de même $(\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-)^{\Gamma_n} = 1$ pour tout entier n. Le sous Λ-module fini maximal de $\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-$ est donc trivial et ce module est donc sans $\mathbb{Z}_p$-torsion.

□

Proposition 3.3.3. *La $\mathbb{Z}_p$-torsion de $Gal(N'_\infty \cap L'_\infty/K_\infty)^-$ est isomorphe à $Gal(L'_\infty \cap N'_\infty/L'_\infty \cap T_\infty)^-$.*

Démonstration. Considérons la suite exacte tautologique

$$\mathrm{Gal}(L'_\infty \cap N'_\infty/T_\infty \cap L'_\infty) \hookrightarrow \mathrm{Gal}(L'_\infty \cap N'_\infty/K_\infty) \twoheadrightarrow \mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty).$$

Le Λ-module $\mathrm{Gal}(L'_\infty \cap T_\infty/K_\infty)^-$ étant sans $\mathbb{Z}_p$-torsion, il ne possède pas de sous Λ-module fini. De plus, il est de type fini sur $\mathbb{Z}_p$ car son invariant μ est nul (voir [5]), sa $\mathbb{Z}_p$-torsion est donc triviale et il est $\mathbb{Z}_p$-libre.
On en déduit immédiatement, en tenant compte de la prop. 3.3.1, que

$$\begin{aligned} \mathrm{Gal}(L'_\infty \cap N'_\infty/T_\infty \cap L'_\infty)^- &= tor_{\mathbb{Z}_p}(\mathrm{Gal}(L'_\infty \cap N'_\infty/T_\infty \cap L'_\infty)^-) \\ &= tor_{\mathbb{Z}_p}(\mathrm{Gal}(L'_\infty \cap N'_\infty/K_\infty)^-) \end{aligned}$$

□

Nous sommes maintenant en mesure de donner une démonstration alternative du théorème suivant, qui n'est autre que le corollaire 2.8 de [19] :

Théorème 3.3.4. *Pour $n >> 0$, on a :*

$$tor_{\mathbb{Z}_p}(Gal(L'_\infty \cap N'_\infty/K_\infty))^- \simeq (coker(A'_n \to A'^{\Gamma_n}_\infty)^+)^\vee(1)$$

Démonstration. Le théorème 2.4 de [19] montre que

$$\mathrm{coker}(A'_n \to A'^{\Gamma_n}_\infty)^\vee(1) \simeq \mathrm{Gal}(N''_\infty/T_\infty).$$

On en déduit immédiatement que

$$\begin{aligned} \mathrm{Gal}(N''_\infty/T_\infty)^- &= (coker(A'_n \to A'^{\Gamma_n}_\infty)^\vee(1))^- \\ &= (coker(A'_n \to A'^{\Gamma_n}_\infty)^\vee)^+(1) \\ &= (coker(A'_n \to A'^{\Gamma_n}_\infty)^+)^\vee(1) \end{aligned}$$

Or nous avons vu respectivement dans les propositions 3.3.1 et 3.3.3 que

$$\mathrm{Gal}(N''_\infty/T_\infty)^- = \mathrm{Gal}(L'_\infty \cap N'_\infty/L'_\infty \cap T_\infty)^-$$

et que

$$tor_{\mathbb{Z}_p}(\mathrm{Gal}(N_\infty \cap L'_\infty/K_\infty)^-) \simeq \mathrm{Gal}(L'_\infty \cap N'_\infty/L'_\infty \cap T_\infty)^-.$$

On déduit de ces isomorphismes le résultat annoncé, à savoir :

$$tor_{\mathbb{Z}_p}(\mathrm{Gal}(L'_\infty \cap N'_\infty/K_\infty)^- \simeq (coker(A'_n \to A'^{\Gamma_n}_\infty)^+)^\vee(1).$$

□

Corollaire 3.3.5. *S'il n'y a qu'une seule p-place dans K_0, alors le module $Gal(N'_\infty \cap L'_\infty/K_\infty)$ est $\mathbb{Z}_p$-libre.*

Démonstration. En effet, le fait qu'il n'y ait qu'une seule p-place assure que la flèche naturelle $\varinjlim X'_{\Gamma_n} \to A'_\infty$ est un isomorphisme. Or on sait que le conoyau de capitulation $\mathrm{coker}(A'_n \to (A'_\infty)^{\Gamma_n})$ est le noyau de cette flèche (voir par exemple [19]). □

3.4 Cas du module non-ramifié

Nous allons voir dans cette section que si l'on considère le module d'Iwasawa non ramifié X_∞, on obtient des résultats en tous points similaires. On suppose dans cette section que tous les étages de K_n vérifient la conjecture de Leopoldt. Notons $N^0_\infty = N_\infty \cap K^{BP}_\infty$, qui est l'analogue dans le cas non-ramifié du module N''_∞.
Comparons dans un premier temps $\mathrm{Gal}(N''_\infty/T_\infty)$ et $\mathrm{Gal}(N^0_\infty/T_\infty)$.

Proposition 3.4.1. *La partie $-$ du Λ-module $Gal(N''_\infty/N^0_\infty)$ est triviale.*

Démonstration. Cette preuve comporte deux ingrédients principaux : d'une part la finitude de la partie $-$ de $\mathrm{Gal}(N'_\infty/N_\infty)$ et d'autre part le fait que $\mathrm{Gal}(N'_\infty/K_\infty)$ ne possède pas de sous module de $\mathbb{Z}_p$-torsion.
Commençons par vérifier que la partie $-$ du Λ-module $\mathrm{Gal}(N'_\infty/N_\infty)$ est finie. Considérons la suite exacte :

$$1 \longrightarrow \mathrm{Gal}(M_\infty/N'_\infty)^- \longrightarrow \mathrm{Gal}(M_\infty/N_\infty)^- \longrightarrow \mathrm{Gal}(N'_\infty/N_\infty)^- \longrightarrow 1.$$

D'après la proposition 3.2.9, les modules $\mathrm{Gal}(M_\infty/N_\infty)^-$ et $\mathrm{Gal}(M_\infty/N'_\infty)^-$ sont respectivement isomorphes à $(A^+_\infty)^\vee(-1)$ et $((A'_\infty)^+)^\vee(-1)$. Or $(A^+_\infty)^\vee(-1)$ et $((A'_\infty)^+)^\vee(-1)$ sont respectivement pseudo-isomorphes à $X^+_\infty(1)$ et $(X'_\infty)^+(1)$. Les invariants λ de ces deux modules étant égaux (prop. 11.4.7 de [21]), les deux termes initiaux de la suite exacte considérée sont des $\mathbb{Z}_p$-modules de même rang et le troisième terme de la suite est nécessairement fini.
Par ailleurs $\mathrm{Gal}(N'_\infty/K_\infty)$ ne possède pas de sous module de $\mathbb{Z}_p$-torsion (une preuve détaillée de ce résultat est donnée dans [13], th. 15, nous nous contenterons d'en donner l'idée : de l'isomorphisme $\mathrm{Gal}(N'_\infty/K_\infty) \simeq A^\vee_\infty(-1)$, on déduit que $\mathrm{Gal}(N'_\infty/K_\infty)$ est l'adjoint d'un certain module d'Iwasawa et comme tel ne possède pas de sous module fini), le module $\mathrm{Gal}(N'_\infty/N_\infty)^-$ est donc nécessairement trivial. □

Corollaire 3.4.2. *La surjection canonique $A_\infty \twoheadrightarrow A'_\infty$ induit un isomorphisme entre les parties $+$ de ces modules et les conoyaux de capitulation $coker(A_n \to (A_\infty)^{\Gamma_n})^+$ et $coker(A'_n \to (A'_\infty)^{\Gamma_n})^+$ sont naturellement isomorphes.*

Démonstration. En effet, on a vu dans la démonstration de la proposition 3.4.1 que $\mathrm{Gal}(N'_\infty/N_\infty)^- = 1$. Par conséquent les modules $\mathrm{Gal}(M_\infty/N_\infty)^-$ et $\mathrm{Gal}(M_\infty/N'_\infty)^-$ sont galoisiennement isomorphes. Les radicaux kummériens associés à ces modules, qui sont respectivement $(A_\infty)^+$ et $(A'_\infty)^+$ sont donc également isomorphes.
La seconde partie du corollaire découle de l'application du lemme du serpent au diagramme qui suit :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \ker(A_n \to A'_n)^+ & \longrightarrow & (A_n)^+ & \longrightarrow & (A'_n)^+ & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 1 = \varinjlim \ker(A_n \to A'_n)^+ & \longrightarrow & (A^+_\infty)^{\Gamma_n} & \longrightarrow & ((A'_\infty)^+)^{\Gamma_n} & \longrightarrow & 1 \end{array}$$

□

Remarque. *Le résultat qui précède est bien connu des spécialistes et figure par exemple dans [26] ou [21].*

On déduit immédiatement de la proposition 3.4.1 le corollaire suivant :

Corollaire 3.4.3. *La surjection naturelle $Gal(N''_\infty/T_\infty) \to Gal(N^0_\infty/T_\infty)$ induit un isomorphisme entre les parties $-$ de ces modules.*

Finalement, la conjonction des corollaires 3.4.2 et 3.4.3 et du théorème 3.3.4 permet de relier le conoyau de capitulation $\mathrm{coker}(A_n \to A_\infty^{\Gamma_n})^+$ au module $\mathrm{Gal}(N^0_\infty/T_\infty)^-$ de la façon suivante :

Corollaire 3.4.4. *Pour $n >> 0$, on a :*

$$(coker(A_n \to A_\infty^{\Gamma_n})^+)^\vee(1) \simeq Gal(N^0_\infty/T_\infty)^-$$

Pour généraliser le théorème 3.3.4, nous devons maintenant relier la $\mathbb{Z}_p$-torsion du module $\mathrm{Gal}(N_\infty \cap L_\infty/K_\infty)^-$ au module $\mathrm{Gal}(N^0_\infty/T_\infty)^-$. On a l'analogue de la proposition 3.3.3.

Proposition 3.4.5. *Le Λ-module $Gal(T_\infty \cap L_\infty/K_\infty)^-$ est sans $\mathbb{Z}_p$-torsion.*

Démonstration. Notons α_∞ l'application de restriction naturelle

$$\alpha_\infty : \mathrm{Gal}(K^{BP}_\infty/K_\infty) \to \mathrm{Gal}(T_\infty/K_\infty).$$

L'image de $\mathrm{Gal}(L_\infty/L'_\infty)$ par α_∞ est alors $\mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty)$. De plus $\ker(\alpha_\infty) = \mathrm{Gal}(K^{BP}_\infty/T_\infty)$.
Considérons le diagramme suivant, où les flèches verticales sont induites par α_∞ :

$$\begin{array}{ccccc} \mathrm{Gal}(K^{BP}_\infty/L_\infty) & \hookrightarrow & \mathrm{Gal}(K^{BP}_\infty/L'_\infty) & \twoheadrightarrow & \mathrm{Gal}(L_\infty/L'_\infty) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Gal}(T_\infty/T_\infty \cap L_\infty) & \hookrightarrow & \mathrm{Gal}(T_\infty/T_\infty \cap L'_\infty) & \twoheadrightarrow & \mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty) \end{array}$$

Le morphisme α_∞ induit un morphisme $\mathrm{Gal}(L_\infty/L'_\infty) \to \mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty)$. L'application du lemme du serpent au diagramme précédent montre alors que le noyau de ce morphisme est $\mathrm{Gal}(T_\infty L_\infty/T_\infty L'_\infty)$. Par ailleurs, on sait que $\mathrm{Gal}(K_\infty^{BP}/T_\infty L'_\infty)^- = 1$ (c'est la trivialité de $\ker(\theta_\infty)^-$, vue à la proposition 3.3.1), il s'ensuit que $\mathrm{Gal}(T_\infty L_\infty/T_\infty L'_\infty)^- = 1$. Le morphisme α_∞ induit alors un isomorphisme entre $\mathrm{Gal}(L_\infty/L'_\infty)^-$ et $\mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty)^-$. Or le module $\mathrm{Gal}(L_\infty/L'_\infty)^-$ est $\mathbb{Z}_p$-libre (prop. 13.28 de [26]), le module $\mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty)^-$ l'est donc également. On en déduit que $\mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty)^-$ est $\mathbb{Z}_p$-libre.
Pour finir, considérons la suite exacte :

$$\mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty)^- \hookrightarrow \mathrm{Gal}(T_\infty \cap L_\infty/K_\infty)^- \twoheadrightarrow \mathrm{Gal}(T_\infty \cap L'_\infty/K_\infty)^-.$$

On vient de voir $\mathrm{Gal}(T_\infty \cap L_\infty/T_\infty \cap L'_\infty)^-$ est $\mathbb{Z}_p$-libre, par ailleurs on a vu (proposition 3.3.2) que $\mathrm{Gal}(T_\infty \cap L'_\infty/K_\infty)$ était également $\mathbb{Z}_p$-libre. Les termes extrémaux de cette suite sont donc sans $\mathbb{Z}_p$-torsion, on en déduit que $\mathrm{Gal}(T_\infty \cap L_\infty/K_\infty)^-$ l'est également.

□

Théorème 3.4.6. *Pour $n >> 0$,*

$$tor_{\mathbb{Z}_p}(Gal(L_\infty \cap N_\infty/K_\infty)^-) = (coker(A_n \to A_\infty)^{\Gamma_n})^+)^\vee(1)$$

Démonstration. En effet, on vient de voir que $\mathrm{Gal}(T_\infty \cap L_\infty/K_\infty)^-$ était sans $\mathbb{Z}_p$-torsion. On en déduit immédiatement de la suite exacte

$$\mathrm{Gal}(L_\infty \cap N_\infty/T_\infty \cap L_\infty)^- \hookrightarrow \mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)^- \twoheadrightarrow \mathrm{Gal}(T_\infty \cap L_\infty/K_\infty)^-$$

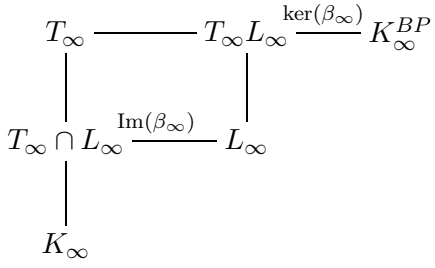
que

$$tor_{\mathbb{Z}_p}(\mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)^-) = tor_{\mathbb{Z}_p}(\mathrm{Gal}(L_\infty \cap N_\infty/L_\infty \cap T_\infty)^-) \quad (3.2)$$

On sait (corollaire 3.4.4) que

$$(\mathrm{coker}(A_n \to A_\infty^{\Gamma_n})^+)^\vee(1) \simeq \mathrm{Gal}(N_\infty^0/T_\infty)^-,$$

il suffit donc pour démontrer le théorème, de montrer que les parties $-$ des modules $\mathrm{Gal}(N_\infty^0/T_\infty)$ et $\mathrm{Gal}(L_\infty \cap N_\infty/L_\infty \cap T_\infty)$ sont isomorphes.
Notons β_∞ le morphisme de restriction $\mathrm{Gal}(K_\infty^{BP}/T_\infty) \to \mathrm{Gal}(L_\infty/K_\infty)$.



On a vu proposition 3.3.1, que $\ker(\theta_\infty)^-$ était trivial. Or $\ker(\beta_\infty) = \mathrm{Gal}(K_\infty^{BP}/T_\infty L_\infty)$ s'injecte dans $\ker(\theta_\infty) = \mathrm{Gal}(K_\infty/T_\infty L'_\infty)$. La trivialité de $\ker(\theta_\infty)^-$ implique donc celle de $\ker(\beta_\infty)^-$. Par suite le morphisme β_∞ induit un isomorphisme entre les parties $-$ des modules $\mathrm{Gal}(K_\infty^{BP}/T_\infty)$ et $\mathrm{Gal}(L_\infty/T_\infty \cap L_\infty)$. De l'application du lemme du serpent au diagramme suivant :

$$\begin{array}{ccccc}
\mathrm{Gal}(K_\infty^{BP}/N_\infty^0) & \hookrightarrow & \mathrm{Gal}(K_\infty^{BP}/T_\infty) & \twoheadrightarrow & \mathrm{Gal}(N_\infty^0/T_\infty) \\
\downarrow & & \downarrow{\scriptstyle \beta_\infty} & & \downarrow \\
\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty) & \hookrightarrow & \mathrm{Gal}(L_\infty/L_\infty \cap T_\infty) & \twoheadrightarrow & \mathrm{Gal}(L_\infty \cap N_\infty/T_\infty \cap L_\infty),
\end{array}$$

on déduit que $\mathrm{Gal}(N_\infty^0/T_\infty)^- = \mathrm{Gal}(L_\infty \cap N_\infty/T_\infty \cap L_\infty)^-$. Le résultat annoncé découle immédiatement de cet isomorphisme et de (3.2). □

3.5 Conséquences de la conjecture de Greenberg

La conjecture de Greenberg prédit sous sa forme la plus connue, la nullité de l'invariant λ du Λ-module X_∞^+. Dans [8], l'auteur montre entre autre que la nullité de cet invariant est équivalente au fait que les applications naturelles $A_n^+ \to A_m^+$ sont triviales pour $m >> n$. En d'autres termes, la conjecture de Greenberg est vérifiée si et seulement si la limite inductive A_∞^+ est triviale, cette conjecture implique donc a fortiori la trivialité des conoyaux de capitulation $\mathrm{coker}(A_n \to A_\infty)^+$. On en déduit immédiatement que :

Proposition 3.5.1. *Si le corps K_0 vérifie la conjecture de Greenberg, alors le module $Gal(L_\infty \cap N_\infty/K_\infty)^-$ est $\mathbb{Z}_p$-libre.*

Démonstration. Ce module est de type fini comme $\mathbb{Z}_p$-module, la $\mathbb{Z}_p$-torsion de sa partie $-$ est triviale en vertu du théorème 3.4.6. □

Par ailleurs, on sait ([13]), que $\mathrm{Gal}(M_\infty/N_\infty) \simeq (A_\infty)^\vee(1)$. Par conséquent, la conjecture de Greenberg est équivalente à la trivialité de la partie $-$ de $\mathrm{Gal}(M_\infty/N_\infty)$. Or $\mathrm{Gal}(M_\infty/N_\infty) \twoheadrightarrow \mathrm{Gal}(L_\infty/N_\infty \cap L_\infty)$; on en déduit le résultat suivant :

Proposition 3.5.2. *Le corps K_0 vérifie la conjecture de Greenberg si et seulement si le module $Gal(L_\infty/L_\infty \cap N_\infty)$ est fini.*

Démonstration. D'après ce que l'on vient de rappeler, la conjecture de Greenberg implique la trivialité de $\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty)^-$ et la finitude de $\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty)^+$.
Réciproquement, si $\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty)$ est fini, sa partie $-$ est triviale et donc $\mathrm{Gal}(N_\infty L_\infty/N_\infty)^- = 1$. Or, on sait que la partie $-$ de $\mathrm{Gal}(M_\infty/N_\infty L_\infty)$ est

triviale (Il s'agit du théorème 1.4.3 figurant dans le premier chapitre.) Or la trivialité de $\mathrm{Gal}(N_\infty L_\infty/N_\infty)^-$ implique celle de $\mathrm{Gal}(M_\infty/N_\infty)^-$ et donc celle de A_∞^+. □

Notons que dans [23], Nguyen-Quang-Do démontre que la conjecture de Greenberg implique la trivialité de $\mathrm{Gal}(L'_\infty/L'_\infty \cap N'_\infty)$.

Dans [18], les auteurs donnent une méthode permettant de déterminer si un corps quadratique totalement réel donné, vérifie effectivement la conjecture de Greenberg. S'inspirant des résultats énoncés dans ce chapitre, on peut ébaucher une démarche pour vérifier numériquement la conjecture de Greenberg pour des corps de degré 3.

En effet, dans le cas où le corps K_0 ne contient qu'une seule p-place, on sait que les conoyaux de capitulation sont triviaux. Dans ce cas, le module $\mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)$ est $\mathbb{Z}_p$-libre. On peut donc en déterminant, à l'étage n de la $\mathbb{Z}_p$-extension cyclotomique de K_0, des systèmes d'unités multiplicativement indépendantes engendrant des extensions non-ramifiées de K_n, obtenir une minoration de l'invariant λ du module $\mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)$. Par ailleurs, la formule de Riemann-Hurwitz (Corollaire 11.4.11 de [21]), permet de calculer effectivement l'invariant λ^- de X_∞. Si l'on dispose de suffisamment d'unités, on pourrait donc démontrer l'égalité des invariants λ des modules $\mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)$ et $\mathrm{Gal}(L_\infty/K_\infty)^-$ et donc en déduire la trivialité de $\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty)^-$, qui implique celle de A_∞^+. On dispose donc d'une méthode algorithmique permettant de déterminer si un corps donné vérifie la conjecture de Greenberg.

Malheureusement, cet algorithme à l'heure actuelle n'est pas effectif. En effet, les invariants λ^- peuvent être relativement grands et l'utilisation de cet algorithme nécessiterait de faire des calculs dans des étages trop élevés de la $\mathbb{Z}_p$-extension cyclotomique.

Chapitre 4

Calcul explicicte de la $\mathbb{Z}_p$ torsion de $\mathfrak{X}_0$.

4.1 Introduction

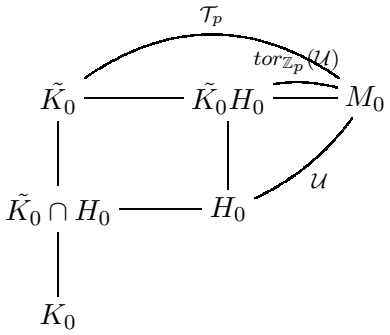
Fixons un nombre premier p et un corps de nombres K_0 vérifiant la conjecture de Leopoldt. Désignons par M_0 la pro-p-extension abélienne non-ramifiée en dehors de p, maximale de K_0. L'objectif de ce chapitre est d'étudier le $\mathbb{Z}_p$-module $\mathfrak{X}_0 = \mathrm{Gal}(M_0/K_0)$ et de déterminer une méthode permettant de calculer effectivement la structure de ce $\mathbb{Z}_p$-module. Ce module est décrit par la suite exacte suivante, issue de la théorie du Corps de Classes :

$$1 \longrightarrow \overline{U}_{K_0} \longrightarrow \prod_{v|p} U_v^1 \longrightarrow \mathfrak{X}_0 \longrightarrow \mathrm{Gal}(H_0/K_0) \longrightarrow 1 \qquad (4.1)$$

On déduit immédiatement de cette suite exacte que le $\mathbb{Z}_p$-rang de $\mathfrak{X}_0$ est égal à $r_2 + 1$, r_2 désignant le nombre de plongements complexes, à conjugaison près de K_0. Le théorème de structure des $\mathbb{Z}_p$-modules de type fini, nous dit alors que $\mathfrak{X}_0$ est produit direct d'une partie libre, $\mathbb{Z}_p^{r_2+1}$ et d'une partie de torsion, que l'on notera $\mathcal{T}_p$. Nous nous intéresserons dans ce chapitre au calcul explicite de ce module de torsion.
Afin d'éviter toute ambiguïté, précisons d'emblée que par calcul explicite, nous entendons *écrire un programme pari-gp calculant $\mathcal{T}_p$, un corps K_0 et un premier p étant donné.*
Dans son livre ([7]), G. Gras étudie le module $\mathcal{T}_p$. Son approche est la suivante : notons $\tilde{K_0}$ le compositum de toutes les $\mathbb{Z}_p$-extensions de K_0 et H_0 la p-extension abélienne non-ramifiée maximale de K_0. On sait, via la théorie du Corps de Classes, que le groupe d'inertie $\mathrm{Gal}(M_0/H_0)$ est isomorphe au quotient $\mathcal{U} := \prod_{v|p} U_v^1/\overline{U}_{K_0}$. Le module de torsion $\mathcal{T}_p$ est alors décrit par la suite exacte suivante :

$$1 \longrightarrow tor_{\mathbb{Z}_p}(\mathcal{U}) \longrightarrow \mathcal{T}_p \longrightarrow \mathrm{Gal}(H_0\tilde{K_0}/\tilde{K_0}) \longrightarrow 1. \qquad (4.2)$$

La situation entre les différentes extensions apparaissant dans la suite exacte (4.2) étant résumée par le diagramme suivant :



(4.3)

Une première idée pour déterminer explicitement $\mathcal{T}_p$ est de calculer les termes extrémaux de la suite exacte (4.2). Le calcul pratique de $tor_{\mathbb{Z}_p}(\mathcal{U})$ peut se faire aisément dans le cas où l'extension $K_0/\mathbb{Q}$ est non-ramifiée en p. En effet, dans ce cas là, le groupe des unités principales U_v^1 est contenu dans le disque de convergence de la fonction $\log_p$ et cette fonction permet de ramener le calcul de $tor_{\mathbb{Z}_p}(\mathcal{U})$ à celui d'une base adaptée d'un $\mathbb{Z}_p$-module. Malheureusement le procédé utilisé dans le cas non-ramifié peut difficilement être généralisé à une extension quelconque. Qui plus est, hormis dans le cas où l'extension K_0 est totalement réelle, la détermination explicite de $\mathrm{Gal}(H_0/\tilde{K}_0 \cap H_0)$ est loin d'être aisée, même si cette détermination est traitée dans le cas théorique dans [7] (th. 2.6).
Nous avons donc abordé le problème sous un autre angle. Partant du fait que le $\mathbb{Z}_p$-module $\mathfrak{X}_0$ est la limite projective des p-parties des groupes de classe de rayon p^n, $Cl_{p^n}(K_0)$, nous avons étudié les propriétés de stabilisation de ces groupes, ainsi que le comportement des facteurs invariants de $Cl_{p^n}(K_0)$ lorsque n croit. De cette étude, nous avons déduit une méthode permettant de déterminer explicitement $\mathcal{T}_p$.
Avant d'aborder la partie technique de ce chapitre, à savoir le calcul effectif de $\mathcal{T}_p$, nous allons voir que la connaissance de $\mathcal{T}_p$ permet d'obtenir de nombreuses informations sur le corps K_0. Ces motivations étant exposées, nous rappellerons la définition ainsi que quelques propriétés élémentaires du groupe de classe de rayon p^n.
Une fois la méthode de calcul théoriquement justifiée, nous l'utiliserons dans quelques cas particuliers et tenterons de donner une explication heuristique aux phénomènes observés.
Pour finir nous verrons que la méthode utilisée pour le calcul de $\mathcal{T}_p$ permet de déterminer explicitement la torsion du $\mathbb{Z}_p$-module de $\mathfrak{X}_S$, groupe de Galois de M_S, pro-p-extension abélienne non-ramifiée en dehors de S maximale de K_0 et cela pour un ensemble de p-places quelconque S, sous réserve que l'on connaisse le $\mathbb{Z}_p$-rang de ce module.

4.2 Motivation du problème

Nous allons voir, dans cette partie, que bien qu'intéressant de façon intrinsèque, le calcul de $\mathcal{T}_p$ permet d'obtenir des informations d'une part sur la p-rationalité du corps K_0 et d'autre part sur la Λ-liberté du module d'Iwasawa non-ramifié en dehors de p, $\mathfrak{X}_\infty$ associé au corps K_0.
Rappelons au préalable que nous nous sommes placés dans le cadre où le corps K_0 vérifie la conjecture de Leopoldt.

4.2.1 Corps p-rationnels

Notons G_{S_p}, le groupe de Galois de la pro-p-extension, non-ramifiée en dehors de p, maximale de K_0, de sorte que $G_{S_p}^{ab} = \mathfrak{X}_0$.

Définition 4.2.1. *On dit que le corps K_0 est p-rationnel si et seulement si le groupe G_{S_p} est libre.*

Les corps p-rationnels ont été étudiés par de nombreux auteurs (voir par exemple [14]). Déterminer si un corps donné est p-rationnel revient donc à étudier la liberté du groupe G_{S_p}, qui est caractérisée par la proposition suivante (pour plus d'informations sur l'étude de G_{S_p} on pourra consulter [17]) :

Proposition 4.2.2. *Le groupe G_{S_p} est libre si et seulement si*

$$\begin{cases} H^2(G_{S_p}, \mathbb{Q}_p/\mathbb{Z}_p) &= 1 \\ \text{et} & \\ H^2_{cont}(G_{S_p}, \mathbb{Z}_p) &= 1 \end{cases}$$

La trivialité du groupe de cohomologie $H^2(G_{S_p}, \mathbb{Q}_p/\mathbb{Z}_p)$ est équivalente à la conjecture de Leopoldt (cette équivalence est traitée en détail dans [21] ou dans [24]). Dans le cas abélien, où cette conjecture est démontrée (voir [5]), la liberté de G_{S_p} est donc équivalente à la trivialité de $H^2_{cont}(G_{S_p}, \mathbb{Z}_p)$. Or ce groupe de cohomologie continue est relié au module $\mathfrak{X}_0$ de la façon suivante :

Proposition 4.2.3. *Soit K_0 un corps vérifiant la conjecture de Leopoldt. Alors la $\mathbb{Z}_p$-torsion du module d'Iwasawa $\mathfrak{X}_0$ est isomorphe au dual de Pontryagin du groupe de cohomologie continue $H^2_{cont}(G_{S_p}, \mathbb{Z}_p)$.*

Démonstration. Faisons agir G_{S_p} trivialement sur $\mathbb{Q}_p/\mathbb{Z}_p$ et considérons la suite exacte :

$$1 \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 1.$$

On obtient par passage à la cohomologie et tenant compte de la conjecture de Leopoldt :

$$H^1(G_{S_p}, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p^n} H^1(G_{S_p}, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^2(G_{S_p}, \mathbb{Z}/p^n\mathbb{Z}) \longrightarrow 1.$$

L'action de G_s sur $\mathbb{Q}_p/\mathbb{Z}_p$ étant triviale, on a

$$H^1(G_{S_p}, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(G_{S_p}, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(G_{S_p}^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) = (G_{S_p}^{ab})^\vee,$$

la dernière égalité étant l'objet du corollaire 2.7.6 de [21]. On obtient donc en considérant la suite duale de la suite précédente :

$$1 \longrightarrow H^2(G_{S_p}, \mathbb{Z}/p^n\mathbb{Z})^\vee \longrightarrow G_{S_p}^{ab} \xrightarrow{p^n} G_{S_p}^{ab}.$$

Par conséquent $(H^2(G_{S_p}, \mathbb{Z}/p^n\mathbb{Z}))^\vee = G_{S_p}^{ab}[p^n]$, on en déduit que $tor_{\mathbb{Z}_p}(G_{S_p}^{ab}) = \varinjlim (H^2(G_{S_p}, \mathbb{Z}/p^n\mathbb{Z}))^\vee = (\varprojlim H^2(G_{S_p}, \mathbb{Z}/p^n\mathbb{Z}))^\vee = H^2_{cont}(G_{S_p}, \mathbb{Z}_p)^\vee$. On a donc bien

$$H^2_{cont}(G_{S_p}, \mathbb{Z}_p)^\vee = \mathcal{T}_p.$$

□

En conséquence, pour un corps K_0 donné, vérifiant la conjecture de Leopoldt, le calcul de la $\mathbb{Z}_p$-torsion du groupe de Galois $\mathfrak{X}_0$, permet de déterminer si le corps considéré est p-rationnel.

4.2.2 Λ-liberté de $\mathfrak{X}_\infty$

Rappelons brièvement une construction de $\mathfrak{X}_\infty$. Pour $n \in \mathbb{N}$, on note K_n le n-ième étage de la $\mathbb{Z}_p$-extension cyclotomique de K_0 et M_n la pro-p-extension abélienne non-ramifiée en dehors de p maximale de K_n. La limite inductive des M_n, notée M_∞, correspond à la pro-p-extension abélienne non-ramifiée en dehors de p maximale de K_∞. Notons $\mathfrak{X}_\infty = \mathrm{Gal}(M_\infty/K_\infty)$, la limite projective relativement à la norme des $\mathfrak{X}_n = \mathrm{Gal}(M_n/K_n)$. Le groupe de Galois $\mathfrak{X}_\infty$ est un $\mathbb{Z}_p$-module sur lequel $\Gamma := \mathrm{Gal}(K_\infty/K_0)$ opère. Il est donc naturellement muni d'une structure de Λ-module, où Λ désigne l'anneau $\mathbb{Z}_p[[T]]$ des séries formelles en T à coefficients dans $\mathbb{Z}_p$.
La conjecture de Leopoldt, dont nous avons donné précédemment une version cohomologique, s'énonce également relativement à la série caractéristique du Λ-module $\mathfrak{X}_\infty$ (pour cette équivalence, on peut consulter [21] ou [26]) :

Proposition 4.2.4. *Le corps K_0 vérifie la conjecture de Leopoldt si et seulement si la série caractéristique de la Λ-torsion de $\mathfrak{X}_\infty$ est étrangère à T.*

On sait par ailleurs (voir par exemple [21] ou [26]) que la dimension Λ-projective de $\mathfrak{X}_\infty$ est inférieure ou égale à 1. En d'autre termes, $\mathfrak{X}_\infty$ ne possède pas de sous Λ-module fini. On en déduit immédiatement le corollaire suivant :

Corollaire 4.2.5. *Soit K_0 un corps de nombres vérifiant la conjecture de Leopoldt, alors $\mathfrak{X}_\infty^\Gamma = 1$.*

Par ailleurs, on sait caractériser la Λ-liberté d'un module de type fini en termes d'invariants et de co-invariants relativement à l'action de Γ. Plus précisément, on dispose du résultat suivant (voir [21], prop. 5.3.19) :

Proposition 4.2.6. *Soit M un Λ-module de type fini. Alors M est Λ-libre si et seulement si :*

$$\begin{cases} M^{\Gamma} = 1 \\ \text{et} \\ M_{\Gamma} \text{ est } \mathbb{Z}_p \text{ libre .} \end{cases}$$

En conséquence, pour un corps K_0 vérifiant la conjecture de Leopoldt, étudier la Λ-liberté de $\mathfrak{X}_\infty$ revient à étudier la $\mathbb{Z}_p$-liberté de $(\mathfrak{X}_\infty)_\Gamma$. Nous allons maintenant voir que la $\mathbb{Z}_p$-liberté de $(\mathfrak{X}_\infty)_\Gamma$ est équivalente à celle de $\mathfrak{X}_0$ et donc à la trivialité de $\mathcal{T}_p$.

Proposition 4.2.7. *Soit K_0 un corps de nombres. Alors $(\mathfrak{X}_\infty)_\Gamma$ est $\mathbb{Z}_p$-libre si et seulement si $\mathfrak{X}_0$ est $\mathbb{Z}_p$-libre.*

Démonstration. En effet, la sous-extension de M_∞, ayant pour groupe de Galois sur K_∞ le quotient $(\mathfrak{X}_\infty)_\Gamma$, est la pro-$p$-extension non ramifiée en dehors de p de K_∞, abélienne sur K_0 et qui soit maximale pour ces propriétés. En d'autres termes, on a $(\mathfrak{X}_\infty)_\Gamma = \mathrm{Gal}(M_0/K_\infty)$. On dispose donc d'une suite exacte :

$$1 \longrightarrow (\mathfrak{X}_\infty)_\Gamma \longrightarrow \mathfrak{X}_0 \longrightarrow \Gamma \longrightarrow 1.$$

Considérant la $\mathbb{Z}_p$-liberté de Γ, on déduit que $tor_{\mathbb{Z}_p}((\mathfrak{X}_\infty)_\Gamma) = tor_{\mathbb{Z}_p}(\mathfrak{X}_0)$ et le résultat annoncé en découle. □

Finalement, pour un corps K_0 vérifiant la conjecture de Leopoldt, calculer effectivement $tor_{\mathbb{Z}_p}(\mathfrak{X}_0)$ permet de déterminer si le module $\mathfrak{X}_\infty$ est Λ-libre.

4.3 Groupe de classes de rayon p^n

Nous rappelons dans cette section la définition du groupe de classes de rayon p^n, via la théorie du Corps de Classes. Notons que comme le corps de Hilbert, le groupe de classes de rayon p^n peut être considéré comme quotient d'un certain groupe d'idéaux (Cf [7]).
Introduisons pour commencer quelques notations générales. Dans O_{K_0}, anneau des entiers de K_0, l'idéal engendré par p, s'écrit comme produit d'idéaux premiers :

$$(p) = \prod_{v|p} \mathfrak{p}_v^{e_v}.$$

Pour chaque p-place v de K_0, fixons une uniformisante π_v dans K_v, v-complété de K. On munit K_v de l'unique valuation prolongeant celle de $\mathbb{Q}_p$, de sorte que $v(p) = 1$ dans K_v et $v(\pi_v) = \frac{1}{e_v}$. On notera en outre

$e = \mathrm{Max}\{e_v, v|p\}$.

La théorie globale du Corps de Classes décrit les extensions abéliennes d'un corps de nombres K_0. Or nous ne considérons ici que des p-extensions abéliennes, qui sont décrites par la théorie p-adique du Corps de Classes ([16]). Cette théorie est en tous points similaire à la théorie globale dans laquelle les corps locaux K_v^* seraient remplacés par leurs pro-p-complétés.

Sur les pro-p-complétés.

Par définition, le pro-p-complété d'un $\mathbb{Z}$-module M est la limite projective des quotiens M/p^n. Dans le cas où M est de type fini sur $\mathbb{Z}$, cette limite projective est isomorphe au produit tensoriel sur $\mathbb{Z}$ de M par $\mathbb{Z}_p$.
On conviendra de noter $\overline{M}$ le pro-p-complété d'un $\mathbb{Z}$-module M.
Pour une place v quelconque, $\overline{U}_v$ désignera donc le pro-p-complété du groupe des unités U_v de K_v. On a par conséquent :

$$\overline{U}_v = \begin{cases} U_v^1 & \text{si} \quad v|p \\ \mu_{p^\infty}(K_v) & \text{si} \quad v \nmid p \end{cases},$$

où $\mu_{p^\infty}(K_v)$ est le groupe des racines p-primaires de l'unité contenues dans K_v.
Pour une p-place v et n entier naturel non nul, U_v^n désigne le groupe des unités u de K_v tels que $u \equiv 1[\pi_v^n]$ (compte tenu du fait que $v(p) = 1$, on a $u \in U_v^n \Leftrightarrow v(u-1) \geq \frac{n}{e_v}$). Le groupe, U_v^n est naturellement muni d'une structure de $\mathbb{Z}_p$-module et est donc pro-p-complet, en d'autres termes $\overline{U}_v^n = U_v^n$.

La notion de groupe de classes de rayon est fortement liée à celle de conducteur d'une extension, nous commencerons donc cette partie par de brefs rappels sur la notion de conducteur.

4.3.1 Conducteur d'une extension

La notion de conducteur est une notion locale dans le sens où elle est définie initialement pour une extension locale.

Définition 4.3.1. *Le conducteur d'une extension abélienne de corps locaux L_v/K_v est le minimum des entiers n tels que $U_v^n \subset N_{L_v/K_v}(L_v^*)$.*

Remarque. *En particulier une extension abélienne L_v/K_v est non-ramifiée si et seulement si son conducteur est nul.*

Définition 4.3.2. *Le conducteur d'une extension abélienne de corps globaux L/K est l'idéal $\mathfrak{m} = \prod_{\mathfrak{p}_v} \mathfrak{p}_v^{n_v}$, où $\mathfrak{p}_v$ parcourt l'ensemble des idéaux premiers de K et où n_v est le conducteur de l'extension L_v/K_v.*

Notons que la définiton précédente ne prend pas en compte une éventuelle ramification des places à l'infini.
La proposition suivante découle immédiatement de ces définitions :

Proposition 4.3.3. *Soit $K \subset L \subset M$ une tour d'extensions de degrés finis, telle que M/K soit abélienne. Alors le conducteur de l'extension L/K divise le conducteur de l'extension M/K.*

Démonstration. Cela découle tout simplement du fait que pour toute place v de M, on a $N_{M_v/K_v}(M_v^*) \subset N_{L_v/K_v}(L_v^*)$. □

Énonçons pour finir un lemme, qui nous sera fort utile dans la suite :

Lemme 4.3.4. *Soit $K_v \subset L_v \subset M_v$ une tour d'extensions de $\mathbb{Q}_p$ telle que l'extension M_v/K_v soit abélienne et l'extension M_v/L_v de degré p. Notons n_M et n_L les conducteurs respectifs des extensions M_v/K_v et L_v/K_v. Alors, si $n_L > \frac{e_v}{p-1}$, où e_v désigne l'indice de ramification de p dans l'extension $K_v/\mathbb{Q}_p$, on a :*

$$n_M \leq n_L + e_v.$$

Démonstration. Par définition n_L est le plus petit entier n tel que $U_v^n \subset N_{L_v/K_V}(L_v^*)$.
De la théorie locale du Corps de Classes, on déduit le diagramme suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N_{M_v/K_v}(M_v^*) & \longrightarrow & K_v^* & \longrightarrow & \mathrm{Gal}(M_v/K_v) & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & N_{L_v/K_v}(L_v^*) & \longrightarrow & K_v^* & \longrightarrow & \mathrm{Gal}(L_v/K_v) & \longrightarrow & 1 \end{array}$$

L'application du lemme du serpent au diagramme précédent donne alors immédiatement la suite exacte suivante :

$$1 \longrightarrow N_{M_v/K_v}(M_v^*) \longrightarrow N_{L_v/K_v}(L_v^*) \longrightarrow \mathrm{Gal}(M_v/L_v) = \mathbb{Z}/p\mathbb{Z} \longrightarrow 1.$$

Par conséquent $N_{M_v/K_v}(M_v^*)$ est un sous-groupe d'indice p de $N_{L_v/K_v}(L_v^*)$. Soient $n \in \mathbb{N}, n \geq n_L + e_v$ et $x \in U_v^n$. On va montrer que $x \in N_{M_v/K_v}(M_v^*)$. On a $x = 1 + \pi_v^n y$ avec $v(y) \geq 0$, par conséquent $v(x-1) \geq nv(\pi_v) = \frac{n}{e_v}$. Or $n \geq n_L + e_v \Rightarrow \frac{n}{e_v} \geq \frac{n_L}{e_v} + 1 > \frac{1}{p-1}$, la fonction logarithme p-adique réalise donc un isomorphisme de groupes entre $(U_v^n, \times)$ et $(\pi_v^n O_{K_v}, +)$. Par conséquent $\frac{1}{p}\log_p(x) \in \pi_v^{n-e_v} O_{K_v}$. Or par hypothèse, $\frac{n_L}{e_v} > \frac{1}{p-1}$, on peut définir à l'aide de la fonction $\exp_p$, l'élément $x^{\frac{1}{p}} \in U_v^{n-e_v}$. Or $n - e_v \geq n_L \Rightarrow x^{\frac{1}{p}} \in N_{L_v/K_v}(L_v^*)$. Pour finir, comme $N_{M_v/K_v}(M_v^*)$ est d'indice p dans $N_{L_v/K_v}(L_v^*)$, on en déduit que $x \in N_{M_v/K_v}(M_v^*)$. On a donc $U_v^n \subset N_{M_v/K_v}(M_v^*)$ pour tout entier n tel que $n \geq n_L + e_v$. On en déduit en particulier que $U_v^{n_L+e_v} \subset N_{M_v/K_v}(M_v^*)$ et, par définition du conducteur, que $n_M \leq n_L + e_v$.

□

4.3.2 Définition du groupe de classes de rayon p^n

Une façon de définir le Corps de Classes de rayon p^n est d'utiliser la théorie globale du Corps de Classes.
La théorie du Corps de Classes locale établit l'existence d'une correspondance entre les sous-groupes d'indice fini de K_v^* et les extensions abéliennes de K_v. Dans la théorie globale, le groupe des idéles de K_0 joue un rôle analogue à celui joué par K_v^* dans le cas local. Ce groupe des idéles, noté $\mathcal{I}_{K_0}$, est le produit restreient des K_v^*, v parcourant l'ensemble des p-places de K_0. Un élément de $x \in \mathcal{I}_{K_0}$ est la donnée d'un élement $x_v \in \prod_v K_v^*$ tel que x_v soit une unité pour toutes les places, excepté peut être un nombre fini.
La théorie globale du Corps de Classes permet donc de décrire les extensions abéliennes d'un corps de nombres K_0 en termes de suites exactes.

Définition 4.3.5. *On désignera par :*

- $\tilde{H}_0$ *l'extension abélienne non-ramifiée maximale de* K_0,
- $\tilde{H}_0^{p^n}$ *le compositum de toutes les extensions abéliennes de* K_0, *dont le conducteur divise* p^n,
- H_0 *la pro-p-extension abélienne non-ramifiée maximale de* K_0,
- $H_0^{p^n}$ *le compositum de toutes les p-extensions de* K_0, *dont le conducteur divise* p^n.

De sorte que les groupes de Galois $Gal(H_0/K_0)$ *et* $Gal(H_0^{p^n}/K_0)$ *sont isomorphes aux p-parties respectives des groupes* $Gal(\tilde{H}_0/K_0)$ *et* $Gal(\tilde{H}_0^{p^n}/K_0)$.

Proposition 4.3.6. *Les suites exactes suivantes, issues de la théorie globale du Corps de Classes, permettent de caractériser les corps* $\tilde{H}_0^{p^n}$ *et* $\tilde{H}_0$ *:*

$$1 \longrightarrow K^* \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v} \longrightarrow \mathcal{I}_{K_0} \longrightarrow Gal(\tilde{H}_0^{p^n}/K_0) \longrightarrow 1$$

$$1 \longrightarrow K^* \prod_{v} U_v \longrightarrow \mathcal{I}_{K_0} \longrightarrow Gal(\tilde{H}_0/K_0) \longrightarrow 1$$

Le groupe de Galois $Gal(H_0^{p^n}/K_0)$ *sera noté* $Cl_{p^n}(K_0)$ *et est la p-partie du groupe de Galois* $Gal(\tilde{H}_0^{p^n}/K_0)$, *groupe de classes de rayon* p^n *de* K_0.

On déduit quasi immédiatement de la définition de $H_0^{p^n}$ les propriétés suivantes :

Proposition 4.3.7. *Soit n un entier non-nul :*

i) On dispose d'une inclusion naturelle $H_0^{p^n} \subset H_0^{p^{n+1}}$.

ii) La limite inductive $\varinjlim H_0^{p^n}$ *est égale à* M_0.

iii) La limite projective $\varprojlim Cl_{p^n}(K_0)$ *est égale à* $\mathfrak{X}_0$.

La suite exacte définissant le Corps de Classes de rayon p^n fait intervenir le groupe des idèles $\mathcal{I}_{K_0}$. Or ce groupe étant un produit infini, il est très peu commode à utiliser dès que l'on veut étudier numériquement le corps $H_0^{p^n}$. Pour pallier cette difficulté, nous allons voir que le corps $H_0^{p^n}$ peut être défini par une suite exacte analogue à la suite exacte (4.1), définissant le module $\mathfrak{X}_0$.

Proposition 4.3.8. *Pour n, entier non nul, les extensions $\tilde{M}_0$ et $\tilde{H}_0^{p^n}$ de K_0 sont reliées entre elles par la suite exacte suivante :*

$$1 \longrightarrow U_{K_0}^{(p^n)} \longrightarrow \prod_{v|p} U_v^{ne_v} \longrightarrow Gal(\tilde{M}_0/K_0) \longrightarrow Gal(\tilde{H}_0^{p^n}/K_0) \longrightarrow 1,$$

où $U_{K_0}^{(p^n)} = \{u \in U_{K_0}$ telle que $u \in U_v^{ne_v}, \forall v, v|p\}$.

Démonstration. De la définition des extensions $\tilde{M}_0$ et $\tilde{H}_0^{p^n}$, on déduit le diagramme

$$\begin{array}{ccccccc}
1 & \longrightarrow & K_0^* \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v} & \longrightarrow & \mathcal{I}_{K_0} & \longrightarrow & \mathrm{Gal}(\tilde{H}_0^{p^n}/K_0) \longrightarrow 1 \\
 & & \uparrow & & \| & & \uparrow \\
1 & \longrightarrow & K_0^* \prod_{v\nmid p} U_v \prod_{v|p} 1 & \longrightarrow & \mathcal{I}_{K_0} & \longrightarrow & \mathrm{Gal}(\tilde{M}_0/K_0) \longrightarrow 1
\end{array}$$

Il découle immédiatement du lemme du serpent que :

$$\ker(\mathrm{Gal}(\tilde{M}_0/K_0) \to \mathrm{Gal}(\tilde{H}_0^{p^n}/K_0)) = (K^* \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v})/(K^* \prod_{v\nmid p} U_v \prod_{v|p} 1).$$

Définissons alors l'application :

$$\theta : (K^* \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v}) \to \prod_{v|p} U_v^{ne_v}/U_{K_0}^{(p^n)},$$

en posant pour $k(u_v) \in K^* \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v}$: $\theta(k(u_v)) = \overline{(u_v)_{v|p}}$, où $\overline{(u_v)_{v|p}}$ désigne la classe de $(u_v)_{v|p}$ dans $\prod_{v|p} U_v^{ne_v}/U_{K_0}^{(p^n)}$.

Commençons par vérifier que l'application θ est bien définie, i.e. que si $k(u_v) = k'(u'_v)$ dans $K^* \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v}$, alors $\theta(k(u_v)) = \theta(k'(u'_v))$. Par définition, $k(u_v) = k'(u'_v) \Leftrightarrow i_v(k)u_v = i_v(k')u'_v, \forall v$, où i_v désigne le plongement de K dans K_v. On en déduit que $i_v(k'k^{-1}) \in U_v, \forall v$ et que $i_v(k'k^{-1}) \in U_v^{ne_v}, \forall v, v|p$. On a donc $k'k^{-1} \in U_{K_0}^{(p^n)}$ et $\overline{(u_v)_{v|p}} = \overline{(u'_v)_{v|p}}$. L'application θ est donc bien définie.

Il est clair que $(K^* \prod_{v\nmid p} U_v \prod_{v|p} 1) \subset \ker(\theta)$ et que l'application θ est surjective. Nous allons montrer que $(K^* \prod_{v\nmid p} U_v \prod_{v|p} 1) = \ker(\theta)$. Soit donc

$k(u_v) \in \ker(\theta)$, il existe $x \in U_{K_0}^{(p^n)}$ tel que $u_v = i_v(x), \forall v, v|p$. Considérons alors l'élément $x(u'_v)$, où $u'_v = 1$, si $v|p$ et $u'_v = i_v(x)^{-1}u_v$, si $v \nmid p$. On a alors $x(u'_v) = (u_v) \Rightarrow k(u_v) = kx(u'_v)$ et comme $kx(u'_v) \in (K^* \prod_{v\nmid p} U_v \prod_{v|p} 1)$, on en déduit que l'on a bien $(K^* \prod_{v\nmid p} U_v \prod_{v|p} 1) \subset \ker(\theta)$ et finalement

$$(K^* \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v})/(K^* \prod_{v\nmid p} U_v \prod_{v|p} 1) \simeq \prod_{v|p} U_v^{ne_v}/U_{K_0}^{(p^n)}.$$

La suite exacte

$$1 \longrightarrow U_{K_0}^{(p^n)} \longrightarrow \prod_{v|p} U_v^{ne_v} \longrightarrow \mathrm{Gal}(\tilde{M}_0/K_0) \longrightarrow \mathrm{Gal}(\tilde{H}_0^{p^n}/K_0) \longrightarrow 1 \tag{4.4}$$

en découle. □

Corollaire 4.3.9. *Les extensions $H_0^{p^n}$ et M_0 sont reliées entre elle via la suite exacte suivante :*

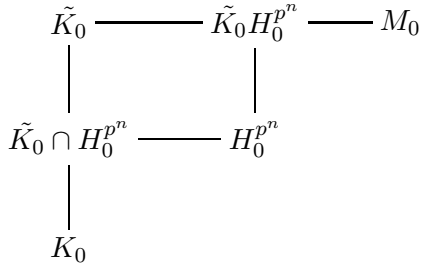
$$1 \longrightarrow \overline{U}_{K_0}^{(p^n)} \longrightarrow \prod_{v|p} U_v^{ne_v} \longrightarrow \mathfrak{X}_0 \longrightarrow Cl_{p^n}(K_0) \longrightarrow 1,$$

où $\overline{U}_{K_0}^{(p^n)}$ désgine le pro-p-complété de $U_{K_0}^{(p^n)}$.

Démonstration. Cette suite exacte s'obtient en considérant la suite pro-p-complétée de la suite exacte de la proposition 4.3.8, reliant $\tilde{H}_0^{p^n}$ et $\tilde{M}_0$. □

4.4 Calcul explicite de $tor_{\mathbb{Z}_p}(\mathfrak{X}_0)$

Le but de cette section est d'exposer une méthode permettant de calculer effectivement $\mathcal{T}_p$. Après la présentation d'un exemple générique, nous donnerons des arguments théoriques justifiant cette méthode empirique. L'idée principale de cette méthode est que la connaissance de $Cl_{p^n}(K_0)$ pour $n >> 0$ permet de déterminer la structure de $\mathcal{T}_p$.
Notons $\tilde{K}_0$, le compositum de toutes les $\mathbb{Z}_p$-extensions de K_0. Les extensions $H_0^{p^n}, M_0$ et $\tilde{K}_0$ sont reliées entre elles suivant le diagramme d'extensions suivant :



S'il est clair que pour $n >> 0$, $\mathrm{Gal}(H_0^{p^n}/\tilde{K}_0 \cap H_0^{p^n}) \simeq \mathcal{T}_p$, la détermination explicite d'un entier n_0 tel que $\mathrm{Gal}(H_0^{p^{n_0}}/\tilde{K}_0 \cap H_0^{p^{n_0}}) \simeq \mathcal{T}_p$ est a priori difficile.

Après avoir exposé une méthode permettant de déterminer explicitement un tel entier, nous verrons que la connaissance pour $n \geq n_0$, des facteurs invariants des groupes $Cl_{p^n}(K_0)$ et $Cl_{p^{n+1}}(K_0)$ permet de déterminer ceux de $\mathcal{T}_p$.
Par commodité , nous allons commencer par donner un exemple générique afin d'expliciter les raisons qui nous ont conduites à étudier les propriétés de stabilisation de $Cl_{p^n}(K_0)$.

4.4.1 Un exemple générique dans le cas $p = 3$

Considérons le corps $K = \mathbb{Q}(\sqrt{-129})$. Utilisant le logiciel pari-gp , on voit que les 3-parties des groupes de classe de rayon 3^n de K pour $n = 0, 1, 2, 3, 4, 5$ sont respectivement :

n	$Cl_{p^n}(K_0)$
0	$\mathbb{Z}/3\mathbb{Z}$
1	$\mathbb{Z}/9\mathbb{Z}$
2	$\mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2$
3	$\mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/81\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
5	$\mathbb{Z}/243\mathbb{Z} \times \mathbb{Z}/81\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Cet exemple générique incite à penser que la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_0$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et que pour déterminer cette p-torsion, il suffit de calculer $H_0^{p^n}$ pour n suffisamment grand. A partir de cet exemple, on peut légitimement se poser la question suivante :

Question 1. *Pour $n >> 0$, le noyau de la surjection canonique $Cl_{p^{n+1}}(K_0) \twoheadrightarrow Cl_{p^n}(K_0)$ est-il toujours isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$?*

Par ailleurs, si l'on regarde un peu plus précisément les relations existantes entre les extensions $H_0^{p^n}$ et $H_0^{p^{n+1}}$, résumées dans le diagramme suivant :

$$\begin{array}{ccccc}
\tilde{K_0} & \text{———} & \tilde{K_0}H_0^{p^n} & \text{═══} & \tilde{K_0}H_0^{p^{n+1}} \text{ ═══ } M_0 \ , \\
| & & | & & | \\
\tilde{K_0} \cap H_0^{p^{n+1}} & \text{——} & H_0^{p^n}(\tilde{K_0} \cap H_0^{p^{n+1}}) & \text{═══} & H_0^{p^{n+1}} \\
| & & | & & \\
\tilde{K_0} \cap H_0^{p^n} & \text{———} & H_0^{p^n} & & \\
| & & & & \\
K_0 & & & &
\end{array} \qquad (4.5)$$

l'exemple étudié nous amène à nous poser la question suivante :

Question 2. *Supposons que le noyau de la surjection canonique* $Cl_{p^{n+1}}(K_0) \twoheadrightarrow Cl_{p^n}(K_0)$ *soit isomorphe à* $(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. *A-t-on*

$$\mathcal{T}_p \simeq Gal(H_0^{p^n}/H_0^{p^n} \cap \tilde{K}_0) \qquad ?$$

Relativement au diagramme qui précède, notons que du fait que $\mathfrak{X}_0$ est un $\mathbb{Z}_p$-module abélien de type fini, il est produit direct de sa partie libre, par sa partie de torsion. En d'autres termes, il existe une extension finie M_0' de K_0 telle que $\tilde{K}_0 M_0' = M_0$ et $\mathrm{Gal}(M_0'/K_0) \simeq \mathcal{T}_p$. L'extension M_0' étant non-ramifiée en dehors de p, on a pour $n >> 0$: $M_0' \subset H_0^{p^n}$, et par conséquent $\tilde{K}_0 H_0^{p^n} = M_0$.

4.4.2 Propriétés de stabilisation de $Cl_{p^n}(K_0)$

L'objectif est ici de démontrer la proposition suivante, qui répond à la première question posée.

Proposition 4.4.1. *Pour tout entier* n *tel que* $p^n > \frac{e}{p-1}$, *le noyau de la surjection canonique*

$$Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)$$

se surjecte sur $(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$.

Démonstration. Considérons le diagramme suivant :

$$\begin{array}{ccccc} \tilde{K}_0 \cap H_0^{p^{n+1}} & \text{——} & H_0^{p^n}(\tilde{K}_0 \cap H_0^{p^{n+1}}) & \text{——} & H_0^{p^{n+1}} \\ | & & | & & \\ \tilde{K}_0 \cap H_0^{p^n} & \text{————} & H_0^{p^n} & & \\ | & & & & \\ K_0 & & & & \end{array} \tag{4.6}$$

Notons tout d'abord que K_0 vérifiant la conjecture de Leopoldt, $\mathrm{Gal}(\tilde{K}_0/K_0) = \mathbb{Z}_p^{r_2+1}$.

Il est clair que $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \twoheadrightarrow \mathrm{Gal}(\tilde{K}_0 \cap H_0^{p^{n+1}}/\tilde{K}_0 \cap H_0^{p^n})$. Or $\mathrm{Gal}(\tilde{K}_0/\tilde{K}_0 \cap H_0^{p^n})$ est un sous $\mathbb{Z}_p$-module de $\mathrm{Gal}(\tilde{K}_0/K_0) = \mathbb{Z}_p^{r_2+1}$ de corang nul, il est donc isomorphe à $\mathbb{Z}_p^{r_2+1}$. Il existe donc r_2+1 extensions, disons $M_1, M_2, \cdots, M_{r_2+1}$ de $\tilde{K}_0 \cap H_0^{p^n}$, contenues dans $\tilde{K}_0$ telles que $\mathrm{Gal}(M_i/\tilde{K}_0 \cap H_0^{p^n}) \simeq \mathbb{Z}/p\mathbb{Z}$ et $\mathrm{Gal}(M_1 \cdots M_{r_2+1}/\tilde{K}_0 \cap H_0^{p^n}) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. Or le conducteur de l'extension $\tilde{K}_0 \cap H_0^{p^n}/K_0$ divise $p^n = \prod_{v|p} \mathfrak{p}_v^{ne_v}$. De plus l'hypothèse $p^n > \frac{e}{p-1}$ assure que l'on peut utiliser le lemme 4.3.4 et par conséquent le conducteur de l'extension M_i/K_0 divise $\prod_{v|p} \mathfrak{p}_v^{ne_v+e_v} = p^{n+1}$. En d'autres termes, $M_i \subset H_0^{p^{n+1}}$ pour tout $i \in \{1, \cdots, r_2+1\}$. La surjection annoncée en découle.

□

On en déduit immédiatement le corollaire suivant :

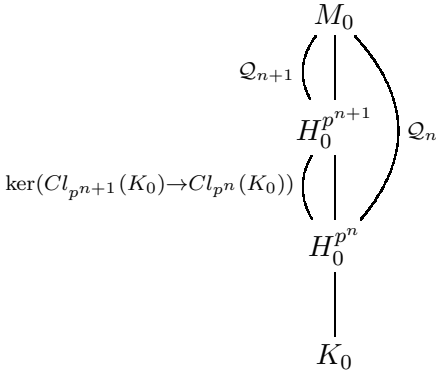
Corollaire 4.4.2. *Supposons que pour un entier n tel que $p^n > \frac{e}{p-1}$, le cardinal de* $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$ *soit exactement* p^{r_2+1}. *Alors* $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \simeq Gal(\tilde{K_0} \cap H_0^{p^{n+1}}/\tilde{K_0} \cap H_0^{p^n})$.

Démonstration. En effet d'après le diagramme (4.6), on dispose d'une surjection $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \twoheadrightarrow \mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/\tilde{K_0} \cap H_0^{p^n})$. Or on vient de voir que $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/\tilde{K_0} \cap H_0^{p^n}) \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. Ces groupes étant finis et par hypothèse équipotents, les surjections considérées sont des isomorphismes. □

Il nous reste maintenant à vérifier que si $\ker(Cl_{p^{n_0+1}}(K_0) \to Cl_{p^{n_0}}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ pour un certain n_0, alors $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ pour tout entier $n \geq n_0$. A cette fin, considérons la suite exacte définissant la p-partie du groupe de classe de rayon p^n :

$$1 \longrightarrow \overline{U}_{K_0}^{(p^n)} \longrightarrow \prod_{v|p} U_v^{ne_v} \longrightarrow \mathfrak{X}_0 \longrightarrow Cl_{p^n}(K_0) \longrightarrow 1,$$

et notons $\mathcal{Q}_n = \prod_{v|p} U_v^{ne_v}/\overline{U}_{K_0}^{(p^n)}$. On a alors $\mathcal{Q}_n = \mathrm{Gal}(M_0/H_0^{p^n})$. Par conséquent $\mathcal{Q}_n/\mathcal{Q}_{n+1} = \ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \simeq \mathrm{Gal}(H_0^{p^{n+1}}/H_0^{p^n})$. Les relations entre toutes ces extensions étant rappelées dans le diagramme qui suit :



Proposition 4.4.3. *L'élévation à la puissance p induit, via l'application d'Artin, une surjection* $\ker(Cl_{p^{n+2}}(K_0) \to Cl_{p^{n+1}}(K_0))$ *sur* $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$.

Démonstration. Rappelons que $\mathcal{Q}_n = \prod_{v|p} U_v^{ne_v}/\overline{U}_{K_0}^{(p^n)} = \ker(\mathfrak{X}_0 \to Cl_{p^n}(K_0))$ et considérons le diagramme suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{Q}_{n+1} & \longrightarrow & \mathfrak{X}_0 & \longrightarrow & Cl_{p^{n+1}}(K_0) & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & \mathcal{Q}_n & \longrightarrow & \mathfrak{X}_0 & \longrightarrow & Cl_{p^n}(K_0) & \longrightarrow & 1 \end{array}$$

On en déduit que $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) = \mathcal{Q}_n/\mathcal{Q}_{n+1}$. Or, n non-nul implique trivialement que $n > \frac{1}{p-1}$, l'élévation à la puissance p réalise un isomorphisme de $\prod_{v|p} U_v^{ne_v}$ sur $\prod_{v|p} U_v^{ne_v+e_v}$. Cet isomorphisme induit donc une surjection $\mathcal{Q}_n$ sur $\mathcal{Q}_{n+1}$. Considérons finalement le diagramme suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{Q}_{n+1} & \longrightarrow & \mathcal{Q}_n & \longrightarrow & \mathcal{Q}_n/\mathcal{Q}_{n+1} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle (.)^p} & & \downarrow{\scriptstyle (.)^p} & & \downarrow{\scriptstyle (.)^p} & & \\ 1 & \longrightarrow & \mathcal{Q}_{n+2} & \longrightarrow & \mathcal{Q}_{n+1} & \longrightarrow & \mathcal{Q}_{n+1}/\mathcal{Q}_{n+2} & \longrightarrow & 1 \end{array}$$

On déduit du lemme du serpent que la flèche verticale de droite est une surjection de $\mathcal{Q}_n/\mathcal{Q}_{n+1}$ sur $\mathcal{Q}_{n+1}/\mathcal{Q}_{n+2}$, i.e. de $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$ sur $\ker(Cl_{p^{n+2}}(K_0) \to Cl_{p^{n+1}}(K_0))$. □

On déduit trivialement de cette proposition, le corollaire suivant :

Corollaire 4.4.4. *Notons $q_n = \#\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$. La suite (q_n) est décroissante et donc asymptotiquement constante.*

Nous sommes maintenant en mesure de répondre à la première question posée :

Théorème 4.4.5. *Il existe un entier n_0 tel que $\ker(Cl_{p^{n_0+1}}(K_0) \to Cl_{p^{n_0}}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. De plus pour tout entier $n \geq n_0$, le module $\mathcal{Q}_n = Gal(M_0/H_0^{p^n})$ est $\mathbb{Z}_p$-libre de rang r_2+1 et :*

$$\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}.$$

Démonstration. Le $\mathbb{Z}_p$-module de type fini $\mathfrak{X}_0$ est isomorphe au produit direct de sa torsion et de $\mathbb{Z}_p^{r_2+1}$. Un isomorphisme étant fixé, on peut identifier $\mathbb{Z}_p^{r_2+1}$ à un sous groupe de $\mathfrak{X}_0$ et donc définir, via la théorie de Galois, une extension M_0' de K_0 telle que $\mathrm{Gal}(M_0'/K_0) \simeq \mathcal{T}_p$ et $\tilde{K_0}M_0' = M_0$. Cette extension étant non-ramifiée en dehors de p, il existe un entier n_1 tel que $M_0' \subset H_0^{p^{n_1}}$ et par conséquent $H_0^{p^{n_1}}\tilde{K_0} = M_0$. De plus pour tout entier $n \geq n_1$, $\mathrm{Gal}(M_0/H_0^{p^n})$ est un sous-module de corang nul de $\mathrm{Gal}(M_0/M_0') = \mathbb{Z}_p^{r_2+1}$, par conséquent $\mathcal{Q}_n = \mathrm{Gal}(M_0/H_0^{p^n}) \simeq \mathbb{Z}_p^{r_2+1}$. Le $\mathbb{Z}_p$-module $\mathcal{Q}_n$ est donc libre de rang r_2+1.
Par ailleurs, on sait qu'il existe un entier n_2 tel que $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$ se surjecte sur $(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ pour tout entier $n \geq n_2$ (on peut choisir pour n_2 le minimum des entiers n tels que les conducteurs des extensions $\tilde{K_0} \cap H_0^{p^n}/K_0$ soit supérieurs ou égaux à $\frac{e}{p-1}$ et cela pour toute p-place v).
Enfin remarquons que du fait que l'élévation à la puissance p réalise un isomorphisme entre $U_v^{ne_v}$ et $U_v^{ne_v+e_v}$, le quotient $\mathcal{Q}_n/\mathcal{Q}_{n+1}$, qui est isomorphe à $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$, est tué par p.
Posons $n_0 = \mathrm{Max}(n_1, n_2)$ et donnons nous maintenant un entier $n \geq n_0$.
Le noyau $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$ est donc un quotient de $\mathbb{Z}_p^{r_2+1}$, qui

se surjecte sur $(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ et qui est tué par p. On a alors nécessairement $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) = (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. Il s'ensuit que pour tout entier $n, n \geq n_0$, on a :

$$\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}.$$

□

4.4.3 Comportement asymptotique des facteurs invariants de $Cl_{p^n}(K_0)$

Commençons par rappeler la définition des facteurs invariants d'un groupe abélien G :

Définition 4.4.6. *Étant donné un groupe abélien fini G, on sait qu'il existe une unique suite $a_1, \cdots, a_t$ telle que :*
- $G \simeq \prod_{i=1}^{t} \mathbb{Z}/a_i\mathbb{Z}$
- $a_{i+1}|a_i$ *pour* $i \in \{1, \cdots, t-1\}$

Les a_i sont appelés facteurs invariants du groupe G et ne dépendent que de la classe d'isomorphisme de G.

Notons que contrairement à l'usage, nous avons choisi d'utiliser la convention $a_{i+1}|a_i$ pour des raisons pratiques. C'est en effet cette forme, qui est utilisée par le logiciel pari-gp .
Si G est un p-groupe, ses facteurs invariants sont des puissances de p. Pour alléger la rédaction de la suite du paragraphe, introduisons la notation suivante :
Notation : Si les facteurs invariants d'un groupe G sont $a_1, \cdots, a_n$, on notera $\mathcal{FI}(G) = [a_1, \cdots, a_t]$.
En pratique, nous sommes en mesure de déterminer les facteurs invariants de $Cl_{p^n}(K_0)$. Nous allons voir dans cette sous-section que la connaissance des facteurs invariants de $Cl_{p^n}(K_0)$ pour $n >> 0$, combinée à l'utilisation des propriétés de stabilisation de $Cl_{p^n}(K_0)$, permet de déterminer explicitement les facteurs invariants et donc la structure de $\mathcal{T}_p$.
Rappelons que pour $n >> 0$, $Cl_{p^n}(K_0)$ est isomorphe au produit direct de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^n}/K_0)$ et de $\mathrm{Gal}(H_0^{p^n}/\tilde{K_0} \cap H_0^{p^n}) = \mathcal{T}_p$. Nous allons donc au préalable étudier un peu plus finement la structure de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^n}/K_0)$.

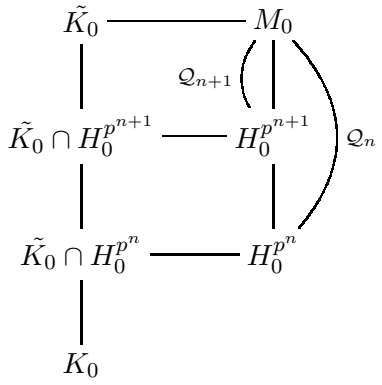
Proposition 4.4.7. *Soit n_0 tel que $p^{n_0} > \frac{e}{p-1}$ et*

$$\ker(Cl_{p^{n_0+1}}(K_0) \to Cl_{p^{n_0}}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}.$$

Alors pour tout entier $n \geq n_0$,

$$Gal(\tilde{K_0}/\tilde{K_0} \cap H_0^{p^{n+1}}) = pGal(\tilde{K_0}/\tilde{K_0} \cap H_0^{p^n}).$$

Démonstration. En vertu du théorème 4.4.5, d'une part le module $\mathcal{Q}_n$ est $\mathbb{Z}_p$-libre de rang r_2+1 et d'autre part $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) = \mathcal{Q}_n/\mathcal{Q}_{n+1} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. On a alors nécessairement $\mathcal{Q}_{n+1} = p\mathcal{Q}_n$. Considérant alors le digramme suivant,



on en déduit l'isomorphisme annoncé. □

Corollaire 4.4.8. *Soit n_0 entier tel que $p^{n_0} > \frac{e}{p-1}$ et $\ker(Cl_{p^{n_0+1}}(K_0) \to Cl_{p^{n_0}}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. Alors pour tout entier $n \geq n_0$, les facteurs invariants de $Gal(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$ sont égaux aux facteurs invariants de $Gal(\tilde{K_0} \cap H_0^{p^n}/K_0)$, multipliés par p.*

Démonstration. En effet, considérons une $\mathbb{Z}_p$-base $(e_1, \cdots, e_r)$ de $\mathrm{Gal}(\tilde{K_0}/K_0)$ adaptée au sous $\mathbb{Z}_p$-module $\mathrm{Gal}(\tilde{K_0}/\tilde{K_0} \cap H_0^{p^n})$. Il existe alors $p^{a_1}, \cdots, p^{a_{r_2+1}}$ tels que $(p^{a_i}e_i)$ soit une $\mathbb{Z}_p$-base de $\mathrm{Gal}(\tilde{K_0}/\tilde{K_0} \cap H_0^{p^n})$. Les p^{a_i} sont alors exactement les facteurs invariants de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^n}/K_0)$. Or $\mathrm{Gal}(\tilde{K_0}/\tilde{K_0} \cap H_0^{p^{n+1}}) = p\mathrm{Gal}(\tilde{K_0}/\tilde{K_0} \cap H_0^{p^n})$, on en déduit donc que $(p^{a_i+1}e_i)$ est une $\mathbb{Z}_p$-base de $\mathrm{Gal}(\tilde{K_0}/\tilde{K_0} \cap H_0^{p^{n+1}})$ et donc les facteurs invariants de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$ sont exactement les p^{a_i+1}. □

Or, du fait que $\mathfrak{X}_0 \simeq \mathbb{Z}_p^{r_2+1} \times \mathcal{T}_p$, le groupe de classe de rayon p^n, $\mathrm{Gal}(H_0^{p^n}/K_0)$, est isomorphe au produit direct des deux p-groupes $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^n}/K_0)$ et de $\mathrm{Gal}(H_0^{p^n}/\tilde{K_0} \cap H_0^{p^n})$. Les facteurs invariants de $\mathrm{Gal}(H_0^{p^n}/K_0)$ s'obtiennent donc en concaténant les facteurs invariants des deux groupes composant ce produit direct.
Nous sommes maintenant en mesure d'énoncer le résultat permettant de déterminer explicitement la structure du p-groupe $\mathcal{T}_p$:

Théorème 4.4.9. *Soit n tel que $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) = (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ et $p^n > \frac{e}{p-1}$. On suppose d'une part que*

$$\mathcal{FI}(Cl_{p^n}(K_0)) = [a_1, \cdots, a_{r_2+1}, b_1, \cdots, b_t]$$

avec $\mathrm{Min}(v_p(a_i)) > \mathrm{Max}(v_p(b_i)) + 1$, *et d'autre part que :*

$$\mathcal{FI}(Cl_{p^{n+1}}(K_0)) = [pa_1, \cdots, pa_{r_2+1}, b_1, \cdots, b_t].$$

Alors, on a :

$$\mathcal{FI}(\mathcal{T}_p) = [b_1, \cdots, b_t].$$

Démonstration. En effet, du fait que

$$\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1},$$

on a $Cl_{p^n}(K_0) \simeq tor_{\mathbb{Z}_p}(\mathfrak{X}_0) \times \mathrm{Gal}(\tilde{K_0} \cap H_0^{p^n}/K_0)$ et $Cl_{p^{n+1}}(K_0) \simeq tor_{\mathbb{Z}_p}(\mathfrak{X}_0) \times \mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$. Or on a vu que les facteurs invariants de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$ étaient exactement égaux à p fois ceux de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^n}/K_0)$. Par conséquent, si a est un facteur invariant de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$, on a nécessairement $a = pa_i$ ou $a = pb_i$. Or comme $\mathrm{Min}(v_p(a_i)) > \mathrm{Max}(v_p(b_i))+1$, aucun des facteurs invariants de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$ n'est de la forme pb_i. Les facteurs invariants de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$ sont donc exactement les $pa_1, \cdots, pa_{r_2+1}$. Le résultat découle alors du fait que $Cl_{p^{n+1}}(K_0)$ est isomorphe au produit direct de $\mathcal{T}_p$ et de $\mathrm{Gal}(\tilde{K_0} \cap H_0^{p^{n+1}}/K_0)$. □

Exemple 4.4.10. *Pour le corps* $\mathbb{Q}(\sqrt{-129})$, *on a* $Cl_{p^3}(K_0) = [27, 9, 3]$ *et* $Cl_{p^4}(K_0) = [81, 18, 3]$. *On en déduit donc que la* $\mathbb{Z}_p$*-torsion de* $\mathfrak{X}_0$ *est exactement* $\mathbb{Z}/3\mathbb{Z}$.

4.5 Approche heuristique

Nous sommes maintenant en mesure de calculer $\mathcal{T}_p$. L'idée de cette section est d'essayer de donner une explication heuristique des résultats numériques que l'on obtient. Bien évidemment, la principale référence sur le sujet est [2], mais on on pourra aussi regarder [4].
L'idée principale des heuristiques de Cohen-Lenstra peut se vulgariser de la façon suivante : "plus un groupe G possède un gros groupe d'automorphismes, moins il apparaît dans la nature". Commençons par rappeler les principaux résultats que nous utiliserons.

4.5.1 Rappels sur les heuristiques de Cohen-Lenstra

La $\mathbb{Z}_p$-torsion de $\mathfrak{X}_0$ est le groupe de Galois d'une certaine extension de K_0. Si l'on suppose l'extension $K_0/\mathbb{Q}$ galoisienne, le module $\mathcal{T}_p$ est alors muni d'une structure de $\mathbb{Z}[\Delta]$-module, où $\Delta := \mathrm{Gal}(K_0/\mathbb{Q})$.
Cependant, si l'on note $N_\Delta = \sum_{\delta \in \Delta} \delta$, on a $N_\Delta(\mathcal{T}_p) = 1$, par conséquent $\mathcal{T}_p$ est en fait un $\mathbb{Z}_p[\Delta]/(N_\Delta)$-module.

Dans le cas où le groupe Δ est cyclique d'ordre premier l, $\mathbb{Z}_p[\Delta]/(1+\delta+\cdots\delta^{o(\Delta)-1})$ est isomorphe à l'anneau des entiers de $\mathbb{Q}(\zeta_l)$, que l'on notera O_l.
Dans cette section, nous supposerons donc que K_0 est une extension cyclique de degré premier l de $\mathbb{Q}$. La $\mathbb{Z}_p$-torsion de $\mathfrak{X}_0$ est alors naturellement munie d'une structure de O_l-module.
D'une façon générale, on sait que tout O_l-module G peut s'écrire de façon non canonique sous la forme $\oplus_{i=1}^{q} O_l/\mathfrak{a}_i$, où les $\mathfrak{a}_i$ sont des idéaux de O_l. Cependant l'idéal $\mathfrak{a} = \prod_{i=1}^{q} \mathfrak{a}_i$ ne dépend lui que de la classe d'isomorphie de G, considéré comme O_l-module. Cet invariant, noté $\mathfrak{a}(G)$, peut être considéré comme une généralisation de la notion de cardinal. On a d'ailleurs $N_{\mathbb{Q}(\zeta_l)}(\mathfrak{a}(G)) = \#G$.

Pour alléger les notations on notera :
- $\sum_{G,N} = \sum_{G, N(\mathfrak{a}(G))\leq N}$, la somme portant sur les classes d'isomorphie de G.
- $\sum_{\mathfrak{a},N} = \sum_{\mathfrak{a}, N(\mathfrak{a})\leq N}$.
- $\sum_{\mathfrak{a}',N} = \sum_{\mathfrak{a}', N(\mathfrak{a}')\leq N \text{ et } \mathfrak{a}'\wedge p=1}$.
- $\sum_{\mathfrak{p},N} = \sum_{\mathfrak{p}, N(\mathfrak{p})\leq N \text{ et } \mathfrak{p}\in S_p}$, où S_p désigne l'ensemble des p-places de O_l.

Nous allons maintenant définir la notion de cardinalité asymptotique pour un ensemble de O_l-module donné. Pour cela, considérons une fonction f, définie sur l'ensemble des classes d'isomorphies de O_l-modules (typiquement f sera une fonction caractéristique). On pose alors

$$\begin{aligned} S_N(f) &= \sum_{G,N} \frac{f(G)}{\#Aut_{O_l}(G)} \\ S_N &= \sum_{G,N} \frac{1}{\#Aut_{O_l}(G)} \end{aligned}$$

Définition 4.5.1. *La moyenne de f est si elle existe la limite lorsque $N \to \infty$ du quotient*

$$\frac{S_N(f)}{S_N}$$

Elle sera notée $M_l(f)$.

Dans le cas où f est la fonction caractéristique d'une certaine propriété, le quotient $\frac{S_N(f)}{S_N}$ peut s'interpréter de la façon suivante : considérons l'ensemble des classes d'isomorphie des groupes de cardinal inférieur ou égal à N, le quotient $\frac{S_N(f)}{S_N}$ peut être considéré comme le rapport du cardinal de l'ensemble des groupes vérifiant la propriété f sur le cardinal de l'ensemble total des groupes considérés initialement, chaque classe d'isomorphie étant compté avec la pondération $\frac{1}{\#Aut_{O_l}(G)}$.

Suivant [2], introduisons la notation suivante :

Notation : Étant donné un idéal $\mathfrak{a}$ de O_l, on note

$$w(\mathfrak{a}) = \sum_{G,\mathfrak{a}(G)=\mathfrak{a}} \frac{1}{\#Aut_{O_l}(G)}$$

Dans [2], Cohen et Lenstra donnent une relation permettant de calculer effectivement $w(\mathfrak{a})$:

Proposition 4.5.2. *Soit $n \in \mathbb{N}$, alors :*

$$w(\mathfrak{a}) = \frac{1}{N_{\mathbb{Q}(\zeta_l)}(\mathfrak{a})} \left(\prod_{\mathfrak{p}^\alpha || \mathfrak{a}} \prod_{k=1}^{\alpha} (1 - \frac{1}{N_{O_l}(\mathfrak{p})^k}) \right)^{-1}.$$

La notation $\mathfrak{p}^\alpha || \mathfrak{a}$ signifiant que $\mathfrak{p}^\alpha | \mathfrak{a}$ et que $\mathfrak{p}^{\alpha+1} \nmid \mathfrak{a}$.
Par conséquent la fonction w, définie sur l'ensemble des idéaux de O_l, est multiplicative.

Notation : Notons $\mathcal{F}_p$ la fonction caractéristique de l'ensemble des classes d'isomorphies de groupe, dont la p-partie est non-triviale.

Proposition 4.5.3. *Notons $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ les p-places de O_l, la moyenne de $\mathcal{F}_p$ existe et on a :*

$$M_l(\mathcal{F}_p) = 1 - \prod_{i=1}^{g} \prod_{k \geq 1} 1 - \frac{1}{p^{k f_i}},$$

où les f_i désignent les degrés des extensions résiduelles $O_l/\mathfrak{p}_i$ sur $\mathbb{F}_p$.

Démonstration. Notons tout d'abord que ce résultat peut être démontré de façon plus rapide en utilisant les fonctions ζ, nous avons toutefois pris le parti d'en donner une démonstration élémentaire.
Par définition de $\mathcal{F}_p$, on a $\mathcal{F}_p(G) = 1$ si et seulement si $\mathfrak{a}(G)$ est divisible par une p-place, il s'ensuit que :

$$\begin{array}{rcl} S_N(\mathcal{F}_p) & = & \sum_{G, \#G \leq N \text{ et } p | \#G} \frac{1}{\#Aut_{O_l}(G)} \\ & = & \sum_{G,N} \frac{1}{\#Aut_{O_l}(G)} - \sum_{\mathfrak{a}',N} \frac{1}{\#Aut_{O_l}(G)}. \end{array}$$

Ainsi

$$\frac{S_N(f)}{S_N} = 1 - \frac{\sum_{\mathfrak{a}',N} \frac{1}{\#Aut_{O_l}(G)}}{\sum_{G,N} \frac{1}{\#Aut_{O_l}(G)}}.$$

L'idée pour déterminer la limite du quotient $\frac{S_N(f)}{S_N}$ est d'utiliser la multiplicativité de la fonction w. Remarquons pour commencer que $\sum_{G,N} \frac{1}{\#Aut_{O_l}(G)} = \sum_{\mathfrak{a},N} w(\mathfrak{a})$.

Notons $Q_N(\mathcal{F}_p) = \frac{\sum_{\mathfrak{a}',N} w(\mathfrak{a}')}{\sum_{\mathfrak{a},N} w(\mathfrak{a})}$, de sorte que $\frac{S_N(\mathcal{F}_p)}{S_N} = 1 - Q_n(\mathcal{F}_p)$.
Par multiplicativité de w, on a :

$$\sum_{\mathfrak{a},N} w(\mathfrak{a}) \leq \sum_{\mathfrak{a}',N} w(\mathfrak{a}') \sum_{\mathfrak{p},N} w(\mathfrak{p}),$$

il s'ensuit que

$$Q_N(\mathcal{F}_p) \geq \frac{1}{\sum_{\mathfrak{p},N} w(\mathfrak{p})}. \tag{4.7}$$

Par ailleurs, donnons nous un $\epsilon > 0$:

$$\begin{aligned} Q_n(\mathcal{F}_p) &= \frac{\sum_{\mathfrak{a}',N} w(\mathfrak{a}')}{\sum_{\mathfrak{a},N} w(\mathfrak{a})} \\ &= \frac{\sum_{\mathfrak{a}',N} w(\mathfrak{a}') \sum_{\mathfrak{p},N^\epsilon} w(\mathfrak{p})}{\sum_{\mathfrak{a},N} w(\mathfrak{a}) \sum_{\mathfrak{p},N^\epsilon} w(\mathfrak{p})}. \end{aligned}$$

On a alors :

$$Q_n(\mathcal{F}_p) \leq \frac{\sum_{\mathfrak{a},N^{1+\epsilon}} w(\mathfrak{a})}{\sum_{\mathfrak{a},N} w(\mathfrak{a}) \sum_{\mathfrak{p},N^\epsilon} w(\mathfrak{p})}. \tag{4.8}$$

Or lorsque $x \to +\infty$, $\sum_{\mathfrak{a},x} w(\mathfrak{a}) \simeq C_\infty \log(x)$ (lemme 5.3 de [2]), avec $C_\infty = \kappa \prod_{s \geq 2} \zeta_{\mathbb{Q}(\zeta_l)}(s)$, κ désignant le résidu en $s = 1$ de la fonction $\zeta_{\mathbb{Q}(\zeta_l)}$. Il en découle que

$$\lim_{N \to +\infty} \frac{\sum_{\mathfrak{a},N^{1+\epsilon}} w(\mathfrak{a})}{\sum_{\mathfrak{a},N} w(\mathfrak{a})} = 1 + \epsilon.$$

Par conséquent, pour déterminer la limite lorsque $N \to +\infty$ de $Q_n(\mathcal{F}_p)$, il suffit de déterminer la limite lorsque $N \to +\infty$ de $\sum_{\mathfrak{p},N} w(\mathfrak{p})$, ce qui est l'objet du lemme qui suit :

Lemme 4.5.4. *La suite de terme général $\sum_{\mathfrak{p},N} w(\mathfrak{p})$ est convergente.*

Démonstration. Notons $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ les p-places de O_l et considérons la série de terme général $w(\mathfrak{p}_i^k)$. Désignons par f_i, le degré de l'extension résiduelle $O_l/\mathfrak{p}_i$ sur $\mathbb{F}_p$. On a d'après la proposition 4.5.2 :

$$w(\mathfrak{p}_i^k) = \frac{1}{p^{f_i k}} \left(\prod_{a=1}^{k} (1 - \frac{1}{p^{f_i a}}) \right)^{-1}.$$

Or il découle d'une identité d'Euler, cité dans [9], que :

$$\sum_{k \geq 0} w(\mathfrak{p}_i^k) = \frac{1}{\prod_{k \geq 1} 1 - \frac{1}{p^{k f_i}}}.$$

Notons $l_i = \sum_{k \geq 0} w(\mathfrak{p}_i^k)$, nous allons montrer que la limite lorsque $N \to +\infty$ de $\sum_{\mathfrak{p},N} w(\mathfrak{p}) = \prod_{i=1}^{g} l_i$. D'une part, par multiplicativité de w, on a $\sum_{\mathfrak{p},N} w(\mathfrak{p}) \leq \prod_{i=1}^{g} l_i$. On en déduit donc la convergence lorsque $N \to +\infty$

de $\sum_{\mathfrak{p},N} w(\mathfrak{p})$. D'autre part $\sum_{\mathfrak{p},N} w(\mathfrak{p}) \geq \prod_{i=1}^{g} \sum_{k=0,N_i} w({\mathfrak{p}_i}^k)$, où $N_i = E(\frac{\log(N)}{gf_i \log(p)})$ (concrètement $N(\mathfrak{p}_i^k) \leq N^{\frac{1}{g}} \Leftrightarrow k \leq N_i$). On en déduit donc finalement que

$$\prod_{i=1}^{g} \sum_{k\geq 0} w(\mathfrak{p}_i^k) \geq \sum_{\mathfrak{p},N} w(\mathfrak{p}) \geq \prod_{i=1}^{g} \sum_{k=0,N_i} w({\mathfrak{p}_i}^k)$$

et on a bien

$$\lim_{N\to+\infty} \sum_{\mathfrak{p},N} w(\mathfrak{p}) = \prod_{i=1}^{g} l_i.$$

□

Notons α_p la limite en $+\infty$ de $\sum_{\mathfrak{p},N} w(\mathfrak{p})$.Des invégalités 4.7 et 4.8, on déduit que $\limsup Q_N(\mathcal{F}_p) \leq (1+\epsilon)\frac{1}{\alpha_p}$, $\forall \epsilon > 0$. Ce qui implique que $\limsup Q_N(\mathcal{F}_p) \leq \frac{1}{\alpha_p}$. De plus $\liminf Q_N(\mathcal{F}_p) \geq \frac{1}{\alpha_p}$. On en déduit donc que $\lim Q_N(\mathcal{F}_p) = \frac{1}{\alpha_p}$ et donc que $M_l(\mathcal{F}_p) = 1 - \frac{1}{\alpha_p}$. Plus précisément :

$$M_l(\mathcal{F}_p) = 1 - \prod_{i=1}^{g} \prod_{k\geq 1} 1 - \frac{1}{p^{kf_i}}.$$

Dans le cas où l'extension K_0 est galoisienne, tous les degrés résiduels sont égaux à f et dans ce cas

$$M_l(\mathcal{F}_p) = 1 - \left(\prod_{k\geq 1} 1 - \frac{1}{p^{kf}} \right)^g.$$

□

Remarque. *Le réel $M_l(\mathcal{F}_p)$ lorsque il existe est couramment appelé 0-moyenne de $\mathcal{F}_p$. La notion de 0-moyenne se généralise en celle de u-moyenne. Les formules permettant de calculer effectivement la u-moyenne de $\mathcal{F}_p$ s'obtiennent en substituant $k+u$ à k dans les formules relatives à la 0-moyenne. Pour de plus amples informations sur la notion de u-moyenne, il conviendra de consulter [2] ou [4]. Nous donnons ci-dessous les valeurs approchées des u-moyennes de $\mathcal{F}_p$ pour $u = 1,2,3$ et $p \in \{2,3,5,7,11,13,17,19\}$.*

Valeurs théoriques des u-moyennes :

p	1-moyenne	2 -moyenne	3-moyenne
3	0.1598	0.0547	0.0184
5	0.0495	0.0099	0.0020
7	0.0237	0.0033	0.0005
11	0.0090	0.0008	0.0001
13	0.0064	0.0004	0.0000
17	0.003	0.0002	0.0000
19	0.0029	0.0001	0.0000

4.5.2 Comparaison avec les résultats numériques obtenus

Pour calculer effectivement la $\mathbb{Z}_p$-torsion du module $\mathfrak{X}_0$, il suffit d'utiliser le théorème 4.4.9 de la façon suivante :

1. On calcule les p-parties des groupes de classes de rayon p^n et p^{n+1}, dont les cardinaux respectifs sont notés q_n et q_{n+1}.
2. Si le quotient $\frac{q_{n+1}}{q_n}$ vaut p^{r_2+1}, on est en mesure d'utiliser le théorème 4.4.9 et donc de déterminer la structure de la $\mathbb{Z}_p$-torsion du module $\mathfrak{X}_0$.
3. Sinon, on incrémente la valeur de n, le corollaire 4.4.4 assurant l'existence d'un entier n pour lequel le quotient $\frac{q_{n+1}}{q_n}$ vaudra effectivement p^{r_2+1}.

Cette méthode est implémentée dans le script **torclass.gp** figurant en annexe de la thèse.

Cas des corps quadratiques réels

Dans ce cas $O_l = \mathbb{Z}$ et donc $l = 2$.
Principe du calcul : Étant donné un entier N, on considère tous les corps quadratiques du type $\mathbb{Q}(\sqrt{d})$ avec d entier naturel sans facteur carré et $d \leq N$. On obtient ainsi un ensemble $\mathcal{K}_N$ de corps quadratiques. Ensuite, on calcule la proportion de corps appartenant à $\mathcal{K}_N$, pour lesquels la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_0$ est non triviale. Cette proportion est notée f_{exp}. L'écart absolu $|f_{exp} - M_2(\mathcal{F}_p)|$ entre f_{exp} et $M_2(\mathcal{F}_p)$ est noté δ. On donne ci-dessous, les tables comportant les résultats obtenus pour $N = 10^4$ et $N = 10^5$.
Notons que si l'on considère comme ensemble $\mathcal{K}_N$ l'ensemble des corps du type $\mathbb{Q}(\sqrt{d})$, dont le discriminant est inférieur ou égal à N, on obtient des résultats en tous points similaires.

$N = 10^4$

p	$M_2(\mathcal{F}_p)$	f_{exp}	δ(Écart)
3	0.43987	0.43933	0.00054
5	0.23967	0.21210	0.02757
7	0.16320	0.14683	0.01637
11	0.09916	0.08796	0.01120
13	0.08284	0.07498	0.00786
17	0.06228	0.05788	0.00440
19	.05540	0.05508	0.00032

$$N = 10^5$$

p	$M_2(\mathcal{F}_p)$	f_{exp}	δ(Écart)
3	0.43987	0.46619	0.02632
5	0.23967	0.22244	0.01723
7	0.16320	0.15632	0.00688
11	0.09916	0.09238	0.00678
13	0.08284	0.08045	0.00239
17	0.06228	0.05930	0.00298
19	0.05540	0.05413	0.00126

Cas des corps cubiques

Dans ce cas $O_l = \mathbb{Z}[j]$ et $l = 3$.

Principe du premier calcul : Étant donné un entier N, on considère tous les sous-corps cycliques de degré 3 de $\mathbb{Q}(\zeta_n)$ pour $1 \leq n \leq N$. On obtient ainsi un ensemble $\mathcal{K}_N$ de corps cubiques.
Ensuite, on calcule la proportion de corps appartenant à $\mathcal{K}_N$, pour lesquels la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_0$ est non triviale. Cette proportion est notée f_{exp}. L'écart relatif $|f_{exp} - M_3(\mathcal{F}_p)|$ entre f_{exp} et $M_3(\mathcal{F}_p)$ est noté δ. On obtient pour $N = 20000$, un ensemble $\mathcal{K}_N$ de cardinal 3165, comprenant tous les corps cycliques de degré 3 dont le discriminant est inférieur ou égal à 399960001. De plus :

p	$M_3(\mathcal{F}_p)$	f_{exp}	δ(Écart)
2	0.3115	0.4088	0.0973
5	0.04160	0.04202	0.00042
7	0.29977	0.29953	0.00024
11	0.00833	0.00758	0.00075
13	0.15881	0.16114	0.0023
17	0.00347	0.00190	0.00157
19	0.10773	0.11438	0.00665

Principe du second calcul : Nous avons ici utilisé les tables de corps de nombres disponibles sur le site dédié au logiciel pari-gp . Nous avons considéré les 10000 premiers corps de nombres de degré 3 (non nécessairement cycliques) de signature $(3,0)$ figurant dans ces tables. Dans ce cas, la $\mathbb{Z}_p$-torsion du module $\mathfrak{X}_0$ n'est a priori muni que d'une structure de $\mathbb{Z}$-module et les résultats que l'on obtient qui semblent être en adéquation avec les heuristiques énoncées précédemment.

p	$M_2(\mathcal{F}_p)$	f_{exp}	δ(Écart)
2	0.7112	0.3644	0.347
5	0.23967	0.23244	0.01723
7	0.16320	0.15896	0.00688
11	0.09916	0.0980	0.00678
13	0.08284	0.0817	0.00239
17	0.06228	0.06214	0.00298
19	0.05540	0.05671	0.00126

Extensions cycliques de degré 5

Principe du premier calcul : Dans ce cas, $O_l = \mathbb{Z}[\zeta_5]$ et $l = 5$. Le principe du calcul est identique à celui utilisé pour les extensions cycliques de degré 3, dans le sens ou l'on a dans un premier temps examiner toutes les extensions cycliques de degré 5, qui sont des sous extensions de $\mathbb{Q}(\zeta_n)$ pour $n \leq 20000$. On obtient dans ce cas les résultats suivants, que l'on compare aux fréquences expérimentales attendues pour un $\mathbb{Z}[\zeta_5]$-module.

p	$M_5(\mathcal{F}_p)$	f_{exp}	δ(Écart)
2	0.0664	0.2137	0.1473
3	0.01250	0.01430	0.00180
7	0.00042	0.00091	0.00049
11	0.34147	0.33830	0.00317
13	0.00003	0	0.00003
17	0.00001	0	0.00001
19	0.00555	0.00639	0.00084

Principe du second calcul : Nous avons ici utilisé les tables de corps de nombres disponibles sur le site dédié au logiciel pari-gp . Nous avons considéré les 10.000 premiers corps de nombres de degré 5, de signature $(5,0)$ figurant dans ces tables. Ici encore, la $\mathbb{Z}_p$-torsion du module $\mathfrak{X}_0$ n'est a priori munie que d'une structure de $\mathbb{Z}$-module et les résultats que l'on obtient semblent être en adéquation avec les heuristiques énoncées précédemment.

p	$M_2(\mathcal{F}_p)$	f_{exp}	δ(Écart)
2	0.7112	0.35910	0.3521
3	0.43987	0.4027	0.02632
7	0.16320	0.1609	0.00688
11	0.09916	0.0990	0.00678
13	0.08284	0.0878	0.00239
17	0.06228	0.0636	0.00298
19	0.05540	0.0549	0.00126

4.5.3 Incidence de la signature du corps

Pour l'instant, nous n'avons effectué que des calculs pour des corps de signatures constantes. Dans cette section, nous étudions l'incidence de la signature du corps sur la fréquence d'apparition du module $\mathcal{T}_p$. Nous avons, utilisant les tables de nombres disponibles sur le site dédié à pari-gp , calculé les fréquences d'apparition de $\mathcal{T}_p$ pour des corps de nombres de degré 3 et 5, dont les signatures sont respectivement $(1,1)$ et $(3,0)$ d'une part et $(1,2),(3,1)$ et $(5,0)$ d'autre part.
Nous tentons ensuite d'interpréter les résultats obtenus en termes de u-moyennes (relativement à la notion de u-moyenne, qui généralise celle de 0-moyenne, on pourra consulter [2] ou [4]) et constatons que pour les corps n'ayant qu'une seule place complexe la fréquence expérimentale obtenue est de l'ordre de la 1-moyenne de $\mathcal{F}_p$.

Les résultats obtenus sont consignés dans les tableaux ci-dessous :

Cas des corps de degré 3.

p	$f_{exp}(1,1)$	$f_{exp}(3,0)$
3	0.2044	0.4729
5	0.0401	0.23224
7	0.0190	0.15896
11	0.0069	0.0980
13	0.0061	0.0817
17	0.0028	0.06214
19	0.0023	0.05671

Cas des corps de degré 5 :

p	$f_{exp}(1,2)$	$f_{exp}(3,1)$	$f_{exp}(5,0)$
3	0.1071	0.1548	0.4027
5	0.0057	0.0341	0.2281
7	0.0023	0.0204	0.1609
11	0.0007	0.0099	0.0990
13	0.0003	0.0054	0.0878
17	0.0003	0.0035	0.0636
19	0.0002	0.0028	0.0549

Nous observons alors que les fréquences théoriques obtenues pour les corps cubiques de signature $(1,1)$ et pour les corps quintiques de signature $(3,1)$ sont de l'ordre de la 1-moyenne de $\mathcal{F}_p$, comme le montre le tableau ci-dessous :

p	1-moy.	$f_{exp}(1,1)$	$f_{exp}(3,1)$
3	0.1598	0.2044	0.1548
5	0.0495	0.0401	0.0341
7	0.0237	0.0190	0.0204
11	0.0090	0.0069	0.0099
13	0.0064	0.0061	0.0054
17	0.003	0.0028	0.0035
19	0.0029	0.0023	0.0028

4.5.4 Synthèse

Dans le cas quadratique réel et plus généralement dans le cas où le module $\mathcal{T}_p$ n'est muni que d'une strcture de $\mathbb{Z}$-module, les résultats obtenus numériquement semblent être en accord avec les heuristiques de Cohen-Lenstra.
d

Par ailleurs dans [7], page 330, l'auteur se demande si étant donné un corps K_0, le produit $\prod_p \mathcal{T}_p$ est fini ou infini. Les calculs que nous avons effectués, ne permettent sans doute pas de se faire une idée relativement à ce problème très ardu, toutefois il est intéressant de noter que dans le cadre des heuristiques que l'on a effectué, nous avons fait comme si $\mathcal{T}_p$ était la p-partie d'un groupe abélien fini G, relié "aléatoirement" au corps K_0. Cette hypothèse semble corroboré par l'expérience dans le cas où K_0 est un corps quadratique réel.

4.6 Calcul du $\mathbb{Z}_p$-rang de $\mathfrak{X}_S$

Une façon de généraliser l'étude que nous venons de faire est de considérer en lieu et place de l'extension M_0, l'extension M_S, pro-p-extension abélienne maximale non-ramifiée en dehors de S de K_0, pour un ensemble de p-places

S de K_0.
Donnons nous donc un ensemble de p-places S et désignons par $\mathfrak{X}_S$ le groupe de Galois sur K_0 de M_S. On va dans cette section essayer de déterminer une méthode permettant de calculer explicitement la structure du $\mathbb{Z}_p$-module $\mathfrak{X}_S$, i.e. son $\mathbb{Z}_p$-rang et sa torsion.
Effectuant des calculs similaires à ceux effectués lors de la démonstration de la proposition 4.3.8, on montre aisément que les extensions M_S et H_0 sont reliés entre elles, via la suite exacte qui suit :

$$\overline{U}_{K_0}^S \xrightarrow{i_S} \prod_{v\in S} U_v^1 \longrightarrow \mathfrak{X}_S \longrightarrow \mathrm{Gal}(H_0/K_0) \longrightarrow 1, \qquad (4.9)$$

où $\overline{U}_{K_0}^S = \{u \in \overline{U}_{K_0} \text{ t.q. } i_v(u) \in U_v^1, \forall v \in S\}$.
Dans l'étude initiale que nous avons effectuée, nous nous sommes placés dans le cas d'un corps de nombres K_0 vérifiant la conjecture de Leopoldt, qui est équivalente à l'injectivité de i_{S_p}.
Cette hypothèse présentait un double intérêt : d'une part elle permet de ramener la liberté du groupe G_{S_p} à la $\mathbb{Z}_p$-liberté du module $\mathfrak{X}_0$ et d'autre part elle permet de calculer le $\mathbb{Z}_p$-rang de $\mathfrak{X}_0$, qui est $r_2 + 1$.
En outre, on a vu lors du calcul effectif de $\mathcal{T}_p$ que la suite des cardinaux de $\ker(Cl_{p^{n+1}}(K_0) \to Cl_{p^n}(K_0))$ était asymptotiquement égale à p^{r_2+1}. En d'autres termes la connaissance du $\mathbb{Z}_p$-rang de $\mathfrak{X}_0$ nous permet de déterminer effectivement la limite de cette suite et par suite la structure de $\mathcal{T}_p$.
Si l'on veut être en mesure de calculer la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_S$ en utilisant la démarche adoptée initialement, il est donc nécessaire de connaître le $\mathbb{Z}_p$-rang de $\mathfrak{X}_S$, que l'on notera d_S.
Dans le cas où l'application i_S est injective, la valeur de d_S se déduit immédiatement de la suite exacte (4.9). Dans [20], l'auteur donne de nombreux exemples d'extensions $K/\mathbb{Q}$ pour lesquelles l'application i_S est injective. Par ailleurs, il existe des formules "explicites" permettant de calculer ce rang, comme par exemple le th. 11.8 de [17]. Ce théorème ramène le calcul du $\mathbb{F}_p$-rang de $\mathfrak{X}_S$ au calcul du $\mathbb{F}_p$-rang de $V_S/(K_0^*)^p$, où $V_S = \{a \in K_0^* | a \in (K_v^*)^p, \forall v \in S\}$. Dans l'optique qui nous intéresse, à savoir calculer effectivement le $\mathbb{Z}_p$-rang de $\mathfrak{X}_S$, l'utilisation de cette formule dans un cas pratique semble très ardue dans la mesure où le calcul effectif du $\mathbb{F}_p$-rang de $V_S/(K_0^*)^p$ est au moins aussi difficile que le calcul du $\mathbb{Z}_p$-rang de $\ker(i_S)$.
Dans le cas d'une extension non-ramifiée, la détermination de $\ker(i_S)$ se ramène, via la fonction $\log_p$, à la détermination du noyau d'une matrice à coefficients dans $\mathbb{Z}_p$. Cette méthode, si elle est facilement implémentable, possède deux gros défauts. D'une part l'hypothèse de non-ramification est très restrictive, d'autre part lorsque on l'implémente effectivement, l'utilisation de la fonction $\log_p$ impose l'utilisation de valeurs approchées.
Après avoir donné un exemple de calcul théorique de d_S, nous calculerons effectivement la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_S$ pour une famille de corps $\mathcal{F}$ constituée de

corps pour lesquels nous connaissons d_S.

4.6.1 $\mathfrak{X}_S$ comme limite projective de groupes de classes de rayon.

Pour une p-place $v \in S$ désignons par $\mathfrak{p}_v$ l'idéal premier sous jacent. On définit alors l'idéal $\mathfrak{m}$ comme le produit des idéaux $\mathfrak{p}_v^{e_v}$, où e_v désigne l'indice de ramification de v dans $K_0/\mathbb{Q}$. La p-partie du groupe de classes de rayon $\mathfrak{m}^n$ est alors caractérisée, via la théorie globale du corps de Classes, par la suite exacte suivante :

$$1 \longrightarrow \overline{K^*} \prod_{v\in S} \overline{U}_v^{ne_v} \prod_{v\notin S} \overline{U}_v \longrightarrow \overline{\mathcal{I}_{K_0}} \longrightarrow \mathrm{Gal}(H_0^{\mathfrak{m}^n}/K_0) \longrightarrow 1, \tag{4.10}$$

où $\overline{\mathcal{I}_{K_0}} = \prod_v \overline{K_v}^*$. On en déduit que l'extension M_S peut être obtenue comme limite inductive des corps de classes de rayon $\mathfrak{m}^n$, le groupe de Galois $\mathfrak{X}_S$ étant alors la limite projective des $Cl_{\mathfrak{m}^n}(K_0) := \mathrm{Gal}(H_0^{\mathfrak{m}^n}/K_0)$.

4.6.2 Propriétés de stabilisation de $Cl_{\mathfrak{m}^n}(K_0)$

Notons d_S le $\mathbb{Z}_p$-rang de $\mathfrak{X}_S$ et notons K_S le compositum de toutes les $\mathbb{Z}_p$-extensions de K_0 contenues dans M_S. Il est immédiat que $\mathrm{Gal}(K_S/K_0) = \mathbb{Z}_p^{d_s}$ et que $tor_{\mathbb{Z}_p}(\mathfrak{X}_S) \simeq \mathrm{Gal}(M_S/K_S)$.
De façon similaire à la proposition 4.4.1, on démontre que :

Proposition 4.6.1. *Pour tout entier $n >> 0$, le noyau de la surjection naturelle $\ker(Cl_{\mathfrak{m}_{n+1}}(K_0) \to Cl_{\mathfrak{m}_n}(K_0)$ se surjecte sur $\mathbb{Z}/p\mathbb{Z}^{d_S}$.*

De plus, considérant les suites exactes issues de la théorie globale du Corps de Classes caractérisant les corps $H_0^{\mathfrak{m}^n}$ et $H_0^{\mathfrak{m}^{n+1}}$, on montre que

$$\ker(Cl_{\mathfrak{m}^{n+1}}(K_0) \to Cl_{\mathfrak{m}^n}(K_0)) \quad \simeq \quad \prod_{v\in S} U_v^{ne_v}/i_S(\overline{U}_{K_0}^{\mathfrak{m}^n}).$$

L'élévation à la puissance p induit donc une surjection $\ker(Cl_{\mathfrak{m}^{n+1}}(K_0) \to Cl_{\mathfrak{m}^n}(K_0))$ sur $\ker(Cl_{\mathfrak{m}^{n+2}}(K_0) \to Cl_{\mathfrak{m}^{n+1}}(K_0))$ et de façon similaire au cas où $S = S_p$, on en déduit la proposition suivante :

Proposition 4.6.2. *Supposons qu'il existe un entier n_0 tel que le cardinal de $\ker(Cl_{\mathfrak{m}^{n+1}}(K_0) \to Cl_{\mathfrak{m}^n}(K_0))$ soit égal à p^{d_S}, alors pour tout entier $n \geq n_0$, on a $\ker(Cl_{\mathfrak{m}^{n+1}}(K_0) \to Cl_{\mathfrak{m}^n}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{d_S}$.*

La détermination explicite de $tor_{\mathbb{Z}_p}(\mathfrak{X}_S)$ peut donc s'effectuer en utilisant la méthode élaborée pour la détermination de $\mathcal{T}_p$ sous réserve que l'on connaisse d_S.

Calcul effectif de $tor_{\mathbb{Z}_p}(\mathfrak{X}_S)$

Supposons que le $\mathbb{Z}_p$-rang d_S de $\mathfrak{X}_S$ soit connu, alors le théorème suivant permet de calculer effectivement $tor_{\mathbb{Z}_p}(\mathfrak{X}_S)$

Théorème 4.6.3. *Soit n tel que $\ker(Cl_{\mathfrak{m}^{n+1}}(K_0) \to Cl_{\mathfrak{m}^n}(K_0)) \simeq (\mathbb{Z}/p\mathbb{Z})^{d_S}$. On suppose d'une part que*

$$\mathcal{FI}(Cl_{\mathfrak{m}^n}(K_0)) = [a_1, \cdots, a_{d_S}, b_1, \cdots, b_t],$$

avec $\mathrm{Min}(v_p(a_i)) > \mathrm{Max}(v_p(b_i)) + 1$, et d'autre part que :

$$\mathcal{FI}(Cl_{\mathfrak{m}^{n+1}}(K_0)) = [pa_1, \cdots, pa_{d_S}, b_1, \cdots, b_t].$$

Alors, on a :

$$\mathcal{FI}(tor_{\mathbb{Z}_p}(\mathfrak{X}_S)) = [b_1, \cdots, b_t].$$

4.6.3 Un exemple de calcul théorique de d_S

Nous donnons dans cette section un exemple de calcul théorique de d_S .

Cas de certains corps CM.

On suppose ici que K_0 est un corps CM dans lequel p est non-décomposé dans K_0^+ et décomposé dans K_0/K_0^+, de sorte que l'on a $p = \mathfrak{p}\overline{\mathfrak{p}}$. On considère $S = \{\mathfrak{p}\}$.

Proposition 4.6.4. *L'application i_S est injective et le $\mathbb{Z}_p$-rang de $\mathfrak{X}_S$ est égal à 1.*

Démonstration. De la suite exacte 4.9, on déduit que le $\mathbb{Z}_p$-rang d_S de $\mathfrak{X}_S$ vaut :

$$d_S = rk_{\mathbb{Z}_p} U_{\mathfrak{p}}^1 + rk_{\mathbb{Z}_p}(\ker(i_S) - rk_{\mathbb{Z}_p}\overline{U}_{K_0} = 1 + rk_{\mathbb{Z}_p}(\ker(i_S)$$

Le corps K_0 étant CM, on sait (th. 4.12 de [26]) que $\mu(K_0)U_{K_0^+}$ est d'indice 1 ou 2 dans U_{K_0}, $\mu(K_0)$ désignant le sous groupe des racines de l'unité contenues dans K_0. Soit donc $u \in \ker(i_S)$, quitte à remplacer u par u^2, on peut toujours supposer que $u \in \mu_{p^\infty}(K_0) \times \overline{U}_{K_0^+}$, où $\mu_{p^\infty}(K_0) = \mu(K_0) \otimes \mathbb{Z}_p$. Par conséquent $u^{p^a} \in \overline{U}_{K_0^+}$, où p^a est l'exposant de $\mu_{p^\infty}(K_0)$. Par hypothèse, on a $i_S(u^{p^a}) = 1$, i.e. $i_{\mathfrak{p}}(u^{p^a}) = 1$. Or du fait que $u \in K_0^+$, on a $i_{\overline{\mathfrak{p}}}(u^{p^a}) = i_{\mathfrak{p}}(\overline{u^{p^a}}) = i_{\mathfrak{p}}(u^{p^a}) = 1$, par conséquent $u^{p^a} \in \ker(i_{S_p}) = 1$. Le $\mathbb{Z}_p$-module $\ker(i_S)$ étant $\mathbb{Z}_p$-libre, on a nécessairement $u = 1$. Ce module est donc trivial et l'application i_S est injective. Il s'en suit que $d_S = 1$. □

Si l'exemple précédent montre qu'il est possible de calculer théoriquement le $\mathbb{Z}_p$-rang de $\mathfrak{X}_S$, il montre aussi que de tels calculs nécessitent des hypothèses très restrictives.

4.6.4 Une approche numérique

Dans cette section, on note $\mathcal{F}_N$ l'ensemble des corps cycliques de degré 3 totalement réels, dans lesquels p est non décomposé, qui sont des sous corps de $\mathbb{Q}(\zeta_n)$ avec n entier, $n \leq N$.
Pour un entier d tel que p soit décomposé dans $\mathbb{Q}(\sqrt{-d})$, on note $\mathcal{K}_{N,d}$ l'ensemble des corps $F.\mathbb{Q}(\sqrt{-d})$, F parcourant $\mathcal{F}_N$. On sait alors en vertu de la proposition 4.6.4 que pour $K \in \mathcal{K}_{N,d}$, le $\mathbb{Z}_p$-rang de $\mathfrak{X}_S(K)$, lorsque S est constitué d'une unique p-place, est égal à 1. On peut donc utilisant le théorème 4.6.3 déterminer la structure de $tor_{\mathbb{Z}_p}(\mathfrak{X}_S)$.
Le nombre d'éléments de $\mathcal{K}_{N,d}$ pour lesquels la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_S$ est non-triviale sera noté $C^S_{N,d}$, le nombre total d'éléments de $\mathcal{K}_{N,d}$ sera noté $C_{N,d}$ et le rapport $\frac{C^S_{N,d}}{C_{N,d}}$ sera noté $f^S_{N,d}$.

Utilisant le logiciel pari-gp , on obtient les résultats suivants pour $N = 20000$ et $p = 3$:

Valeur de d	$C^S_{N.d}$	$C_{N.d}$	$f^S_{N.D}$
2	97	116	0.84
5	95	116	0.82
8	97	116	0.84
11	94	116	0.81
14	96	116	0.83
17	101	116	0.87
20	95	116	0.82
23	115	116	0.99
26	115	116	0.99
29	115	116	0.99
32	97	116	0.84
35	95	116	0.82
38	115	116	0.99
41	98	116	0.84
44	94	116	0.81
47	97	116	0.84
50	97	116	0.84
53	115	116	0.99
56	96	116	0.83
59	115	116	0.99
62	93	116	0.8
65	93	116	0.8
68	101	116	0.87
71	91	116	0.78
74	95	116	0.82
77	96	116	0.83
80	95	116	0.82
83	115	116	0.99
86	97	116	0.84
89	115	116	0.99
92	115	116	0.99
95	96	116	0.83
98	97	116	0.84

Chapitre 5

Annexe : programmes pari-gp .

5.1 Calcul du radical kummérien

Nom du script : look(bnf,base,p).

Paramètres du script :

- bnf est un corps de nombres, défini par *bnfinit*.
- base est un ensemble de places du corps de nombres considéré.
- p est un nombre premier.

Description du script : Ce script détermine toutes les S-unités u, telles que l'élément $u^{\frac{1}{p}}$ engendre une extension non-ramifiée, S désignant l'ensemble des places étrangères à p contenues dans "base".

Sortie du script : Ce script retourne un vecteur à deux composantes, la première composante étant la liste des élément de $U_{K_0}^S/p$ engendrant des extensions non-ramifiées et la seconde le nombre de tels éléments.

Dépendances : plan_proj.gp.

Code source du script :

```
look(bnf,base,p)=                                                    1
{                                                                    2
local(r,proj,lproj,u,ul,u2,unif,vu,a,b,c,dec,e,f,g,tc                3
   ,tv,mu,rnf,vdr,cpt,lk,tvp,tvnp,npid,pbase,snpid,
   lnpid,Mval,Mu,Mvu);
read("plan_proj.gp");                                                4
cpt=0;                                                               5
r=matsize(base)[2];                                                  6
/*Nous allons déterminer la liste des idéaux                         7
   étrangers à p, divisant les élements de base*/
pbase=prod(a=1,r,base[a]);                                           8
/*On fait le produit de tous les éléments de base*/                  9
npid=idealfactor(bnf,pbase);                                         10
```

```
/*On décompose ce produit en produit d'idéaux premiers*/
snpid=matsize(npid)[1];
/*On compte ces idéaux*/
lnpid=[];
if(snpid>0,
        /*On va sélectionner dans snpid les idéaux étrangers à p*/
        for(a=1,snpid,
                if(npid[a,1][1]<>p,lnpid=concat(lnpid,[npid[a,1]]));
        );
        if(matsize(lnpid)[1]>0,
        Mval=matrix(matsize(lnpid)[1],r,i,j,idealval(bnf,base[j],lnpid[i]));
        );
);
proj=plan_proj(r,p);
lproj=matsize(proj)[1];
/*proj contient le plan projectif, paramétrant l'ensemble des p-extensions élémentaires associé au radical kummérien base*/
mu=-1*subst(nffactor(bnf,x^2+x+1)[1,1],x,0);
dec=idealprimedec(bnf,p);
e=dec[1][3];
f=dec[1][4];
g=matsize(dec)[2];
lk=[];
/*lk contiendra les éléments du radical kummerien associe a l'extension non-ramifiee*/
for(a=1,lproj,
        u=mu^proj[a,1]*prod(b=1,r,base[b]^proj[a,b+1]);
        /*u est un élément générique de base tenseur Fp*/
        /*On va commencer par regarder la ramification en les non-p-places*/
        if(matsize(lnpid)[1]>0,
        Mu=matrix(r,1,i,j,proj[a,i+1]);
        Mvu=Mval*Mu;
        Mvu=Mod(Mvu,p);
        Mvu=lift(Mvu);
        tvnp=mattranspose(Mvu)*Mvu
        ,
```

```
        tvnp=0;                                                  45
        );                                                       46
if(tvnp==0,                                                      47
        tc=vector(g);                                            48
        tv=vector(g);                                            49
        /* On va dans la boucle qui suit examiner la             50
           ramification en les p-places*/
        for(b=1,g,                                               51
                unif=bnf.zk*dec[b][2];                           52
                /*unif est une uniformisante associée            53
                    à la p-place étudiée*/
                vu=idealval(bnf,u,dec[b]);                       54
                tvp=lift(Mod(vu,p));                             55
                /*Si la valuation de u en une p-place            56
                    est non divisible par p, alors l'
                   extension est ramifiée en cette p-
                   place*/
                if(tvp==0,                                       57
                        ul=u/unif^vu;                            58
                        ul=ul^(p^f-1);                           59
                        tv[b]=idealval(bnf,ul-1,dec[b            60
                           ])/e;
                              if(tv[b]>=p/(p-1),tc[              61
                                 b]=1);
                              if(lift(Mod(e,p))==0               62
                                 & lift(Mod(tv[b]*e
                                 ,p))==0,
                                    rnf=rnfinit(                 63
                                       bnf,x^p-u)
                                       ;
                                    vdr=idealval(                64
                                       bnf,rnf
                                       [3][1],dec
                                       [b]);
                                    /*vdr est la                 65
                                       valuation
                                       du
                                       discriminant
                                        de l'
                                       extension
                                       relative
                                       en une p-
                                       place*/
                                    if(vdr==0,tc[                66
```

```
                                                    b]=1);
                                          );                          67
                    );                                                68
          );                                                          69
          if(prod(b=1,g,tc[b])>0,cpt=cpt+1;lk=concat(lk               70
              ,u););
);                                                                    71
);                                                                    72
return([lk,cpt]);                                                     73
}                                                                     74
```

5.2 Paramétrisation de $P^n(\mathbb{F}_p)$

Nom du script : plan_proj(n,p).
Paramètres du script :
– n est un nombre entier.
– p est un nombre premier.
Description du script : Ce script détermine tous les éléments de l'espace projectif $P^n(\mathbb{F}_p)$.

Sortie du script : Ce script retourne un vecteur dont les composantes sont les élément de $P^n(\mathbb{F}_p)$.

Dépendances : aucune.

Code source du script :

```
  plan_proj(n,p)=                                                     1
{                                                                     2
local(P,F,M,N,l);                                                     3
P=vector(n+1);                                                        4
if(n==0,P[1]=matrix(p-1,1,a,ba),                                      5
                                                                      6
F=vector(n);                                                          7
F[1]=matrix(p,1,i,j,i-1);                                             8
P[1]=matrix(1,1,i,j,1);                                               9
for(a=2,n,                                                            10
l=matsize(F[a-1])[1];                                                 11
for(b=0,p-1,                                                          12
          if(b==0,F[a]=concat(F[a-1],matrix(l,1,i,j,b))               13
              ,M=concat(F[a-1],matrix(l,1,i,j,b));N=
              concat(mattranspose(F[a]),mattranspose(M))
              ;F[a]=mattranspose(N);
```

```
        );
);
);
for(a=1,n,
l=matsize(P[a])[1];
m=matsize(F[a])[1];
P[a+1]=concat(P[a],matrix(l,1,i,j,0));
M=concat(F[a],matrix(m,1,i,j,1));
N=concat(mattranspose(P[a+1]),mattranspose(M));
P[a+1]=mattranspose(N);
);

);
return(P[n+1]);
}
```

5.3 Calcul des polynômes, qui engendrent des extensions cycliques de degré p

Nom du script : liste(N,p).

Paramètres du script :

– N est un nombre entier.

– p est un nombre premier.

Description du script : Ce script détermine tous les polynômes engendrant des extensions cycliques de degré p contenues dans $\mathbb{Q}(\zeta_n)$ pour tous les entiers $n \leq N$.

Sortie du script : Ce script retourne un vecteur constitué de polynômes de degré p.

Dépendances : aucune.

Code source du script :

```
  liste(N,p)=
{
local(j,t,lp,pol,n,q,a,b,c,lpt);
lp=[];
for(j=3,N,
t=eulerphi(j);
t=lift(Mod(t,p));
        if(t==0,
        pol=polsubcyclo(j,p);
```

```
                if(type(pol)=="t_VEC",n=matsize(pol)[2];
                for(a=1,n,q=pol[a];lp=concat(lp,q)),
                lp=concat(lp,pol);
                );
        );
);
t=matsize(lp)[2];
lpt=concat([],lp[1]);
for(a=2,t,
        c=1;b=1;
        while(b<> 0 & c <= matsize(lpt)[2],b=lp[a]-lpt[c];c=c+1;);
        if(b<>0,lpt=concat(lpt,lp[a]););
);
return(lpt);
}
```

5.4 Calcul de la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_0$

Nom du script : torclass(K,p)

Paramètres du script :

– K est un corps de nombres défini par la commande *bnfinit*.

– p est un nombre premier.

Description du script : Ce script détermine la partie de $\mathbb{Z}_p$ torsion du module $\mathfrak{X}_0$ associé au corps de nombres K.

Sortie du script : Ce script retourne un vecteur à deux composantes. La première est un vecteur contenant les composantes cycliques de la partie de $\mathbb{Z}_p$-torsion du module $\mathfrak{X}_0$ et la seconde l'ordre de cette partie de $\mathbb{Z}_p$-torsion.

Dépendances : ppart.gp.

Code source du script :

```


  torclass(K,p)=
{
local(a,b,c,r2,n,tor,h1,h2,ordre);
read("ppart.gp");
a=0;
n=1;
r2=K.sign[2];
c=p^(r2+1);
```

```
while(a==0,                                                    11
h1=bnrclass(K,p^n);                                            12
h2=bnrclass(K,p^(n+1));                                        13
t=p^valuation(h2[1],p)/p^valuation(h1[1],p);                   14
h1=ppart(h1[2],p);                                             15
h2=ppart(h2[2],p);                                             16
        if(t==c,                                               17
        a=1;                                                   18
        tor=vector(matsize(h2)[2]-r2-1);                       19
                if(matsize(tor)[2]>0,                          20
                for(b=r2+2,matsize(h2)[2],tor[b-r              21
                   2-1]=h2[b]);
                );                                             22
        ,n=n++;                                                23
        );                                                     24
);                                                             25
if(matsize(tor)[2]>0,ordre=prod(a=1,matsize(tor)[2],           26
   tor[a]),ordre=1);
return([tor,ordre]);                                           27
}                                                              28
```

5.5 Calcul de la p-partie d'un vecteur

Nom du script : ppart(v,p).

Paramètres du script :

– v est un vecteur.

– p est un nombre premier.

Description du script : Ce script détermine la p-partie du vecteur v.

Sortie du script : Ce script retourne un vecteur dont les compsantes sont les p-parties des composantes du vecteur initial.

Dépendances : aucune.

Code source du script :

```
  ppart(v,p)=                                                  1
{                                                              2
local(a,n,w1,w2);                                              3
n=matsize(v)[2];                                               4
if(n>0,                                                        5
        w1=vector(n);                                          6
        for(a=1,n,w1[a]=p^valuation(v[a],p));                  7
        w2=[];                                                 8
        for(a=1,n,if(w1[a]<>1,w2=concat(w2,w1[a])));           9
```

```
        return(w2),/*else*/
        return([1]);
);
}
```

5.6 Calcul de la $\mathbb{Z}_p$-torsion de $\mathfrak{X}_S$

Nom du script : Storclass(K,S).

Paramètres du script :

– K est un corps de nombres, défini par *bnfinit*.

– S est un ensemble de p-places du corps de nombres K.

Description du script : Ce script détermine la partie de $\mathbb{Z}_p$-torsion du module $\mathfrak{X}_S$ associé à K, sous réserve que l'application naturelle $i_S : U_K \to \prod_{v \in S} U_v^1$ soit injective.

Sortie du script : Ce script retourne un vecteur à deux composantes. La première est un vecteur contenant les composantes cycliques de la partie de $\mathbb{Z}_p$-torsion du module $\mathfrak{X}_S$ et la seconde l'ordre de cette partie de $\mathbb{Z}_p$-torsion.
Dépendances : ppart.gp.

Code source du script :

```
  Storclass(K,S)=
{
/*K est un corps de nombres, S un ensemble de p
   places de S*/
local(a,b,c,r2,n,tor,h1,h2,ordre,l,hn,hn1,dS,dec,e,f,
   p,Nid,prod_id,M0,Mn,Mn1);
l=matsize(S)[2];/*l est le nombre de p places dans S
   */
if(l>1,prod_id=S[1];a=2;while(a<=l,prod_id=idealmul(K
   ,prod_id,S[a]);a=a+1),prod_id=S[1];);
/*prod_id contient le produit des places de S*/
read("ppart.gp");
r1=K.sign[1];
r2=K.sign[2];
Nid=idealnorm(K,S[1]);
p=factor(Nid)[1,1];
/*On détermine le premier p associé à l'ensemble S*/
e=idealval(K,p,S[1]);
f=valuation(Nid,p);
ds=e*f*l-r1-r2+1;
/*ds est le Zp rang du X_S sous l'hyptohèse i_S
   injective*/
```

```
M0=idealpow(K,prod_id,e);
Mn=M0;
a=0;
n=1;
Mn=1;
while(a==0 & n<12,
Mn=idealmul(K,Mn,M0);
Mn1=idealmul(K,Mn,M0);
/*Mn et Mn1 sont respectivement égaux à M0^n et M0^(n+1)*/
hn=bnrclass(K,Mn);
hn1=bnrclass(K,Mn1);
t=p^valuation(hn1[1],p)/p^valuation(hn[1],p);
print("Le kn vaut", t," pour n=",n);
/*t est le cardinal de ker(Cl(M_{n+1})->Cl(M_n)*/
hn=ppart(hn[2],p);
hn1=ppart(hn1[2],p);
        if(t==p^ds,
                if(ds==0,tor=hn[2];ordore=hn[1];a=1,
                a=1;
                tor=vector(matsize(hn1)[2]-ds);
                        if(matsize(tor)[2]>0,
                        for(b=ds+1,matsize(hn1)[2],
                           tor[b-ds]=hn1[b]);
                        ordre=prod(a=1,matsize(tor)
                           [2],tor[a]);
                        ,tor=[];ordre=1;
                        );
                );
        ,n=n++;
        );
);
return([tor,ordre]);
}
```

Notations

Nous précisons dans cette partie les notations communes à l'ensemble de cette thèse. Les éventuelles hypothèses supplémentaires inhérentes à un chapitre particulier seront précisées par la suite.

- Notations globales :
  - $\overline{\mathbb{Q}}$ désigne une clôture algébrique de $\mathbb{Q}$.
  - p est un nombre premier impair et ζ_p désignera une racine primitive p-ième de l'unité.
  - μ_{p^∞} désigne le groupe des racines p-primaires de l'unité de $\overline{\mathbb{Q}}$.
  - K_0 désigne un corps de nombres.
  - K_n est le n-ième étage de la $\mathbb{Z}_p$-extension cyclotomique associé à K_0.
  - Γ désigne le groupe de Galois $\mathrm{Gal}(K_\infty/K_0)$, de sorte que $\Gamma \simeq \mathbb{Z}_p$.
  - Γ_n désigne le groupe de Galois $\mathrm{Gal}(K_\infty/K_n)$.
  - $Cl(K_n)$ est le groupe des classes d'idéaux de K_n.
  - A_n est la p-partie de $Cl(K_n)$.
  - La limite inductive des A_n sera notée A_∞.
  - H_n est la p-extension abélienne non-ramifiée maximale de K_n, de sorte que $\mathrm{Gal}(H_n/K_n) \simeq A_n$ via l'application d'Artin.
  - M_n est la p-extension abélienne non-ramifiée en dehors de p maximale de K_n, le groupe de Galois $\mathrm{Gal}(H_n/K_n)$ sera noté $\mathfrak{X}_n$.
  - L_∞ est la pro-p-extension abélienne non-ramifiée maximale de K_∞.
  - M_∞ est la pro-p-extension abélienne non-ramifiée en dehors de p maximale de K_∞.
  - $X_\infty = \mathrm{Gal}(L_\infty/K_\infty)$.
  - $\mathfrak{X}_\infty = \mathrm{Gal}(M_\infty/K_\infty)$.
- Notations locales :pour une place v donnée, K_v désigne le v-complété de K.
  - U_v désigne le groupe des unités de K_v.
  - U_v^1 désigne le groupe des unités principales de K_v.
  - $\overline{U}_v$ désigne le pro-p-complété de U_v.
  - π_v désigne une uniformisante de K_v.
  - Si v est une p-place, on munira K_v de l'unique valuation prolongeant celle de $\mathbb{Q}_p$, de sorte que dans K_v, l'on a $v(p) = 1$.
- Notations relatives aux caractères.
  - κ désigne le caractère cyclotomique ; $\kappa : \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \to \mathbb{C}_p^*$.

  - ω désigne le caractère de Teichmüller ; $\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{Z}_p^*$.
  - Si K_0 est un corps contenant ζ_p et Φ un caractère de $\mathrm{Gal}(K_0/\mathbb{Q})$, le caractère miroir de Φ est le caractère $\Phi^* := \Phi^{-1}\omega$.
  - Etant donné un caractère Φ, défini sur un groupe G, on note $\mathbb{Z}_p[\Phi]$ l'anneau des entiers de $\mathbb{Q}_p(\Phi(G))$.
- Notations algébriques.
  - L'anneau des séries formelles à une indéterminée à coefficients dans $\mathbb{Z}_p$ est noté Λ.
  - La série caractéristique d'un Λ-module de type fini M est notée $sc(M)$.
  - Etant donné un Λ-module de type fini M, le quotient $M/tor_\Lambda(M)$ est noté $Fr(M)$.
  - Etant donné deux Λ-modules M et N, on dit que M et N sont pseudo-isomorphes s'il existe un morphisme $f : M \to N$ dont les noyaux et conoyaux sont finis et on note $M \sim N$.
  - Etant donné un $\mathbb{Z}_p$-module M, le dual de Pontryagin de M $\mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ est noté $M^\vee$.

Bibliographie

[1] J. Assim et T. N. Quang Do – « Sur la constante de Kummer-Leopoldt d'un corps de nombres », *Manuscripta Math.* **115** (2004), p. 55–72.

[2] H. Cohen et H. W. Lenstra, Jr. – « Heuristics on class groups of number fields », Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, 1984, p. 33–62.

[3] R. F. Coleman – « Division values in local fields », *Invent. Math.* **53** (1979), no. 2, p. 91–116.

[4] C. Delaunay – « Heuristics on class groups and on Tate-Shafarevich groups : the magic of the Cohen-Lenstra heuristics », Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, 2007, p. 323–340.

[5] B. Ferrero et L. C. Washington – « The Iwasawa invariant μ_p vanishes for abelian number fields », *Ann. of Math. (2)* **109** (1979), no. 2, p. 377–395.

[6] G. Gras – « Théorèmes de réflexion », *J. Théor. Nombres Bordeaux* **10** (1998), no. 2, p. 399–499.

[7] — , *Class field theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003, From theory to practice, Translated from the French manuscript by Henri Cohen.

[8] R. Greenberg – « On the Iwasawa invariants of totally real number fields », *Amer. J. Math.* **98** (1976), no. 1, p. 263–284.

[9] P. Hall – « A partition formula connected with Abelian groups », *Comment. Math. Helv.* **11** (1938), no. 1, p. 126–129.

[10] H. Ichimura – « On a power integral basis problem over cyclotomic $\mathbb{Z}_p$ extensions », *Journal of Algebra* **234** (2000), p. 90–100.

[11] — , « On a quotient of the unramified Iwasawa module over an abelian number field », *J. Number Theory* **88** (2001), p. 175–190.

[12] — , « On a quotient of the unramified Iwasawa module over an abelian number field. II », *Pacific J. Math.* **206** (2002), no. 1, p. 129–137.

[13] K. Iwasawa – « On $\mathbf{Z}_l$-extensions of algebraic number fields », *Ann. of Math. (2)* **98** (1973), p. 246–326.

[14] J.-F. Jaulent et T. Nguyen Quang Do – « Corps p-rationnels, corps p-réguliers, et ramification restreinte », *J. Théor. Nombres Bordeaux* **5** (1993), no. 2, p. 343–363.

[15] J.-F. Jaulent – « Sur l'indépendance l-adique de nombres algébriques », *J. Number Theory* **20** (1985), no. 2, p. 149–158.

[16] — , « Théorie l-adique globale du corps de classes », *J. Théor. Nombres Bordeaux* **10** (1998), no. 2, p. 355–397.

[17] H. Koch – *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer.

[18] J. S. Kraft et R. Schoof – « Computing Iwasawa modules of real quadratic number fields », *Compositio Math.* **97** (1995), p. 135–155, Special issue in honour of Frans Oort.

[19] M. Le Floc'h, A. Movahhedi et T. Nguyen Quang Do – « On capitulation cokernels in Iwasawa theory », *Amer. J. Math.* **127** (2005), no. 4, p. 851–877.

[20] C. Maire – « On the $\mathbb{Z}_l$-rank of abelian extensions with restricted ramification », *J. Number Theory* **92** (2002), no. 2, p. 376–404.

[21] J. Neukirch, A. Schmidt et K. Wingberg – *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000.

[22] T. Nguyen-Quang-Do – « Sur la $\mathbf{Z}_p$-torsion de certains modules galoisiens », *Ann. Inst. Fourier (Grenoble)* **36** (1986), no. 2, p. 27–46.

[23] T. Nguyen-Quang-Do – « Sur la torsion de certains modules galoisiens.(ii) », *Séminaire de Théorie des Nombres, Paris 1986–87* **75** (1988), p. 271–297.

[24] T. Nguyen Quang Do – « Galois module structure of p-class formations », Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, p. 123–138.

[25] T. Tsuji – « Semi-local units modulo cyclotomic units », *J. Number Theory* **78** (1999), no. 1, p. 1–26.

[26] L. C. Washington – *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982.

[27] K. Wingberg – « Duality theorems for Γ-extensions of algebraic number fields », *Compositio Math.* **55** (1985), no. 3, p. 333–381.