Invariants d'Iwasawa dans les extensions de Lie p-adiques des corps de nombres

Guillaume Perbet

▶ **To cite this version:**

Guillaume Perbet. Invariants d'Iwasawa dans les extensions de Lie p-adiques des corps de nombres. Mathématiques générales [math.GM]. Université de Franche-Comté, 2011. Français. NNT : 2011BESA2024 . tel-00839578

HAL Id: tel-00839578

https://theses.hal.science/tel-00839578

Submitted on 28 Jun 2013

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

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

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

Thèse de Doctorat

présentée par

Guillaume PERBET

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

Invariants d'Iwasawa dans les extensions de Lie p-adiques des corps de nombres

---

Thèse soutenue le 6 décembre 2011, devant le jury composé de :

Jean-François Jaulent (président du jury, rapporteur), *Professeur à l'Université de Bordeaux*

Christian Maire (directeur), *Professeur à l'Université de Franche-Comté*

Farshid Hajir (rapporteur), *Professeur à l'University of Massachusetts Amherst (USA)*

Jean-Robert Belliard, *Maître de Conférences à l'Université de Franche-Comté*

Christophe Delaunay, *Professeur à l'Université de Franche-Comté*

François Laubie, *Professeur à l'Université de Limoges*

Jérôme Poineau, *Maître de Conférences à l'Université de Strasbourg*

REMERCIEMENTS

Mes remerciements se portent tout d'abord vers mon directeur de thèse, Christian Maire. Il m'a placé devant des problèmes mathématiques suscitant mon intérêt, et présentant le parfait équilibre entre profondeur et accessibilité souhaité dans tout travail de doctorat. Il a su, lors de nos entretiens brefs et instructifs, me faire profiter de ses impressionnantes connaissances dans le domaine de la théorie des nombres.

Merci à Jean-François Jaulent, qui a fait une place dans son emploi du temps de directeur de laboratoire dans le but de revenir avec moi sur ses précédents écrits. Il m'a fait l'honneur de rapporter ce travail, ainsi que de présider mon jury de thèse. J'exprime ma gratitude envers Farshid Hajir pour avoir accepté d'être rapporteur, tout en regrettant qu'il n'ait pas pu être présent le jour de la soutenance.

Je suis reconnaissant envers Jean-Robert Belliard, Christophe Delaunay, François Laubie et Jérôme Poineau pour avoir constitué ce jury. Ils ont, à travers l'attention qu'ils ont porté à mon travail, contribué à l'achèvement de cette thèse.

J'ai également une pensée pour tous les gens du laboratoire de mathématiques de Besançon, et de l'Université en général, que j'ai eu l'occasion de cotoyer. Ils m'excuseront si je ne les cite pas un par un car la liste serait trop longue. L'ambiance sympathique qui règne entre compagnons de promo, enseignants puis collègues, membres de l'équipe de recherche, doctorants, étudiants et personnel administratif a été pour moi un moteur. La preuve en est ces dix années passées avec plaisir à l'Université de Franche Comté.

TABLE DES MATIÈRES

INTRODUCTION

Histoire du groupe des classes

L'étude du groupe des classes d'un corps de nombres prend sa source dans la résolution d'équations diophantiennes. Une méthode de résolution consiste à factoriser l'équation dans l'anneau des entiers d'une extension algébrique finie de $\mathbb{Q}$ appropriée. Cette méthode est très efficace lorsque l'anneau d'entiers dans lequel on mène les calculs est factoriel, ce qui n'est hélas pas toujours le cas. Ce défaut a été initialement repéré par Kummer en 1844 dans ses travaux sur le dernier théorème de Fermat, et a été formalisé par Dedekind en 1876 avec l'apparition de la notion d'idéal fractionnaire. Etant donné un corps de nombres, il exhibe un groupe fini, le groupe des classes d'idéaux, qui mesure le défaut de factorialité de l'anneau des entiers correspondant. Pour un corps de nombres donné, il existe des méthodes pour déterminer son nombre de classes. Cependant, la complexité des algorithmes qui en ressortent dépasse vite la capacité de calcul des machines actuelles et il est difficile de savoir à quoi s'attendre si on passe d'un corps à un autre.

Les travaux d'Iwasawa

Les travaux d'Iwasawa dans la deuxième partie du vingtième siècle [**16**], [**17**] permettent, d'un coup d'un seul, d'obtenir des renseignements sur le nombre de classes d'une famille infinie de corps de nombres. La théorie dont il pose les bases construit des limites d'objets arithmétiques, attachés à des corps de nombres prenant place dans une extension galoisienne infinie. On obtient de cette façon ce qu'on appelle des modules d'Iwasawa, qui sont mieux compris que les objets de départ. Il est ensuite possible de faire le chemin inverse et de reconstruire les objets au niveau fini à partir du module d'Iwasawa correspondant, c'est le procédé de descente, et ainsi d'obtenir des informations a priori inaccessibles. Un exemple d'application de cette théorie nous intéresse tout particulièrement, c'est le théorème d'Iwasawa sur le comportement asymptotique du nombre de classes le long d'une $\mathbb{Z}_p$-extension d'un corps de nombres. Si on note X_n la p-partie du groupe des classes du n-ième étage K_n d'une $\mathbb{Z}_p$-extension K_∞/K, ce théorème affirme qu'il existe des constantes entières μ, λ et ν telles que, pour n assez grand, on a $\#(X_n) = p^{\mu p^n + \lambda n + \nu}$. Les constantes μ et λ proviennent de la structure de la limite projective des X_n pour les applications norme.

Généralisations du groupe des classes

La démonstration de ce résultat utilise fortement l'interprétation de X_n comme groupe de Galois de la p-extension abélienne non ramifiée maximale de K_n, donnée par la théorie du corps de classes. On est alors en droit de se demander s'il existe des résultats similaires lorsqu'on modifie les contraintes de ramification sur la p-extension de K_n qui intervient. Plus précisément, si S et T sont

deux ensembles finis de places de K, que l'on peut supposer disjoints sans perte de généralité, la théorie du corps de classes donne une bonne interprétation du groupe de Galois de la p-extension abélienne S-ramifiée et T-décomposée maximale de K_n, noté $X_{S,n}^T$. La principale obstruction lorsqu'on veut utiliser les arguments d'Iwasawa vient du fait que ce groupe n'est pas toujours fini, tout du moins lorsque S contient des places p-adiques. L'idée de Jaulent [**22**] pour y remédier fut de s'intéresser aux quotients $X_{S,n}^T/p^n$, qui eux sont finis. La limite projective des $X_{S,n}^T$ est un module d'Iwasawa auquel on associe des invariants ρ_S^T, μ_S^T et λ_S^T. Il est toujours possible, comme dans le cas non ramifié, de redescendre aux étages finis. Il faut cependant prendre beaucoup de précautions avec l'énoncé du théorème de descente (théorème 2.1.7). C'est un résultat classique qui donne le module $X_{S,n}^T$ comme un quotient $X_{S,\infty}^T/\big(\omega_{n,e}(\omega_e X_{S,\infty}^T + Y_e)\big)$ du module à l'infini correspondant, où Y_e est un sous-$\mathbb{Z}_p$-module de $X_{S,\infty}^T$ appelé défaut de descente. Il se trouve que ce n'est pas forcément un sous-module si on prend en compte l'action galoisienne. Cette précision joue effectivement un rôle lorsque l'invariant ρ_S^T est non trivial et fait apparaître une perturbation κ_S^T dans la formule asymptotique qui en découle (théorème 2.3.1) :

Théorème. — *Soit K_∞/K une $\mathbb{Z}_p$-extension du corps de nombres K et S et T deux ensembles finis de places de K. Si K_∞/K n'est pas S-ramifiée et T-décomposée, il existe un plus petit entier e tel que, dans l'extension K_∞/K_e, les places ramifiées qui ne sont pas contenues dans S sont totalement ramifiées et les places de T qui ne sont pas totalement décomposées ne sont pas décomposées du tout. On a la formule asymptotique suivante concernant les p-groupes de T-classes S-infinitésimales des étages de la tour K_∞/K :*

$$\#\left(X_{S,n}^T/p^n\right) = p^{\rho_S^T np^n + \mu_S^T p^n + (\lambda_S^T - \kappa_S^T)n + \mathcal{O}(1)},$$

où ρ_S^T, μ_S^T et λ_S^T sont les invariants structurels du module d'Iwasawa $X_{S,\infty}^T$, et où κ_S^T est un entier naturel vérifiant $\kappa_S^T \leqslant \rho_S^T p^e$.
On notera $\tilde{\lambda}_S^T$ la quantité $\lambda_S^T - \kappa_S^T$ qui apparaît dans la formule.

Cette formule corrige celle initialement donnée par Jaulent et a comme particularité que le paramètre $\tilde{\lambda}_S^T$ peut se retrouver négatif. On montre tout de même que la quantité κ_S^T est majorée par $\rho_S^T p^e$, et que cette borne peut être atteinte :

Exemple. — *Soit p un nombre premier irrégulier. On considère la $\mathbb{Z}_p$-extension $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)$ et les ensembles de places $S = \{p\}$ et $T = \{q_1, q_2\}$, avec q_1, q_2 les deux premiers de $\mathbb{Q}(\zeta_p)$ au dessus d'un nombre premier q totalement décomposé dans $\mathbb{Q}(\zeta_{p^{e+1}})/\mathbb{Q}$ et inerte dans $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_{p^{e+1}})$. Alors*

$$\tilde{\lambda}_S^T = -(p-1)p^e/2.$$

Le cadre non commutatif

Une autre manière d'étendre le cadre d'application du théorème d'Iwasawa a été abordée par Cuoco et Monsky [**4**]. Ils se sont intéréssés au cas des $\mathbb{Z}_p$-extensions multiples. L'analyse de l'algèbre d'Iwasawa, qui est dans ce cadre une algèbre de séries formelles à plusieures indéterminées, leur a permi de dégager des invariants d'Iwasawa généralisant ceux existant en dimension 1. Ils ont alors obtenu des formules asymptotiques, pour les p-groupes des classes au sens classique, le long de $\mathbb{Z}_p^d$-extensions. Là encore, ces formules ont pour paramètres les invariants d'Iwasawa de l'extension.

Dans le cadre des développements récents dans l'étude des extensions de Lie p-adiques des corps de nombres, Howson [**15**] et Venjakob [**38**] introduisent une notion d'invariants ρ et μ attachés à des modules de type fini sur l'algèbre d'Iwasawa d'un groupe de Lie p-adique. On leur ajoutera un troisième invariant r, correspondant tout comme μ au sous-module de $\mathbb{Z}_p$-torsion. Ces invariants généralisent ceux précédemment introduits par Iwasawa et Cuoco-Monsky pour des extensions abéliennes, et il se pose la question de l'existence de formules asymptotiques pour les groupes des classes généralisés le long de telles extensions.

Dans le but de pouvoir définir des étages avec une certaine régularité, on se limite à des pro-p-extensions K_∞/K dont le groupe de Galois G est p-valué de type fini au sens de Lazard [**26**]. On note d sa dimension. On peut alors construire une filtation entière $(G_n)_{n\in\mathbb{N}}$ du groupe G, qui fixe des sous-extensions K_n dont le degré vérifie $[K_n : K] = Cp^{nd}$ pour n assez grand. On veut alors estimer le cardinal des groupes finis $X_{S,n}^T/p^n$, en fonction des invariants d'Iwasawa ρ_S^T et μ_S^T de la limite projective $X_{S,\infty}^T = \varprojlim X_{S,n}^T$.

Le théorème principal

Les résultats qui suivent ont donné lieu à une publication dans Algebra and Number Theory [**34**], dont voici le théorème principal (théorème 2.2.8) :

Théorème. — *Soit K_∞/K une extension du corps de nombres K dont le groupe de Galois G est un pro-p-groupe p-valué, de dimension d, et dans laquelle seul un nombre fini de places de K se ramifient. On fixe S et T deux ensembles finis de places de K.*

Alors les p-groupes des T-classes S-infinitésimales attachés aux étages K_n de l'extension vérifient :

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}^T) = \rho_S^T(G : G_n) + \mathcal{O}(p^{n(d-1)}),$$

$$\dim_{\mathbb{F}_p}(X_{S,n}^T/p) = (\rho_S^T + r_S^T)(G : G_n) + \mathcal{O}(p^{n(d-1)})$$

et

$$\#(X_{S,n}^T/p^n) = p^{(\rho_S^T n + \mu_S^T)(G:G_n) + \mathcal{O}(np^{n(d-1)})}.$$

Où ρ_S^T, μ_S^T et r_S^T sont les invariants d'Iwasawa du module $X_{S,\infty}^T$.

L'hypothèse de ramification finie est classique en théorie d'Iwasawa non commutative et a pour conséquence le fait que le Λ-module à l'infini est de type fini, sans quoi on ne peut pas parler de ses invariants d'Iwasawa. Cette hypothèse est automatiquement vérifiée pour les extensions provenant de la géométrie, mais aussi pour les extensions que l'on construit dans la partie 1.2.
Il y a deux principales étapes dans la démonstration de ce théorème.
La première est la descente, qui permet de retrouver des infos sur les groupes $X_{S,n}^T$ à partir de $X_{S,\infty}^T$.
La seconde est l'analyse algébrique du Λ-module $X_{S,\infty}^T$. Elle utilise les résultats de structure de Venjakob [**38**] et de Coates-Schneider-Sujatha [**3**], concernant la classification des Λ-modules modulo pseudo-isomorphisme. La notion de module pseudo-nul est délicate à manipuler dans le cadre non commutatif, mais on montre que ces modules sont négligeables au vues des formules asymptotiques que l'on développe. La démonstration de ce fait s'appuie sur une formule de Harris [**13**] concernant les coïnvariants d'un Λ-module, que l'on étend au cas des groupes p-valués, ainsi qu'aux groupes d'homologie supérieurs dans la partie 2.2.1.

Formules de réflexion

Les formules asymptotiques obtenues relient les invariants d'Iwasawa d'une extension de Lie p-adique à une suite d'objets arithmétiques attachés à des sous-extensions K_n, de degré fini sur $\mathbb{Q}$. Il sera donc possible d'obtenir des informations sur ces invariants en travaillant au niveau fini. Le dernier chapitre de cette thèse illustre comment les formules de réflexion de Gras [**10**] conduisent à des théorèmes de dualité concernant les invariants d'Iwasawa, lorsque l'on interchange les ensembles de places S et T, qui seront dorénavant supposés disjoints. Les théorèmes du miroir utilisés reposent sur une double interprétation, par le corps de classes et par la théorie de Kummer, des groupes de classes généralisés et nécéssitent de ce fait la présence de racines de l'unité. On obtient le théorème suivant (corollaire 3.2.2 dans le texte) :

Théorème. — *Soit K_∞/K une extension du corps de nombres K dont le groupe de Galois G est un pro-p-groupe p-valué et dans laquelle seul un nombre fini de places de K se ramifient. On suppose que K contient les racines $2p$-ièmes de l'unité et que K_∞ contient la $\mathbb{Z}_p$-extension cyclotomique de K. On fixe S et T deux ensembles finis disjoints de places de K dont l'union contient les places p-adiques.*
Alors

$$\rho_S^T + \frac{\delta_T}{2} = \rho_T^S + \frac{\delta_S}{2},$$
$$r_S^T = r_T^S,$$
$$\mu_S^T = \mu_T^S.$$

Ici, δ_S désigne la somme sur toutes les places p-adiques v de S des degrés locaux $[K_v : \mathbb{Q}_p]$.

Ces formules rejoingnent celles données par Jaulent et Maire pour la $\mathbb{Z}_p$-extension cyclotomique **[23]** et les travaux de cette thèse à propos des $\mathbb{Z}_p$-extensions permettent de les corriger, en remplaçant l'invariant λ par le paramètre $\tilde{\lambda}$ (théorème 3.1.1).
La présence de la $\mathbb{Z}_p$-extension cyclotomique est nécéssaire pour faire apparaître l'invariant μ dans les formules de réflexion. On peut néanmoins se passer de cette hypothèse et aboutir tout de même à un résultat. Les hypothèses sont les mêmes sauf qu'on ne suppose plus que K_∞ contient la $\mathbb{Z}_p$-extension cyclotomique de K (théorèmes 3.2.7 et 3.2.6) :

Théorème. — *Si p est impair. On a la formule suivante concernant les invariants ρ et r :*

$$\rho_S^T + r_S^T + \frac{\delta_T}{2} + t^{dec} = \rho_T^S + r_T^S + \frac{\delta_S}{2} + s^{dec}.$$

Si $p = 2$ et que $S \cup T$ contient les places réelles, on a :

$$\rho_S^T + r_S^T + \frac{\delta_T}{2} + t^{dec} + \frac{t_{\mathbb{R}}}{2} = \rho_T^S + r_T^S + \frac{\delta_S}{2} + s^{dec} + \frac{s_{\mathbb{R}}}{2}.$$

Avec s^{dec} le nombre de places de S totalement décomposées dans K_∞/K et $s_{\mathbb{R}}$ est le nombre de places réelles de S.

Calcul des invariants
Ce travail s'achève par des calculs sur les invariants d'Iwasawa, en présence de la $\mathbb{Z}_p$-extension cyclotomique. On démontre d'abord que les invariants ρ_S^T, μ_S^T et r_S^T ne dépendent que des places p-adiques contenues dans S (théorème 3.2.8).
On effectue ensuite le calcul explicite de ρ_S^T dans le cas d'une extension totalement réelle ou CM (théorème 3.2.9), en se ramenant à des problèmes de plongement d'unités. On obtient l'annulation de cet invariant dans le cas totalement réel et sa valeur dans le cas CM est donnée par $\frac{\delta_{\hat{S}}}{2}$, avec $\hat{S}$ le plus grand sous-ensemble de S stable par conjugaison complexe.
Concernant les invariants μ_S^T et r_S^T. On montre que, dans le cas CM et lorsque le sous-ensemble des places p-adiques de S est stable par conjugaison complexe, ils sont majorés par les invariants μ et r correspondant au cas $S = T = \emptyset$ (proposition 3.2.10).

CHAPITRE 1

EXTENSIONS DE LIE p-ADIQUES D'UN CORPS DE NOMBRES

Ce premier chapitre est tout d'abord une mise en place des outils utilisés tout au long de cette thèse. On commence par introduire la notion de groupe de Lie p-adique. Ces groupes, et plus particulièrement les groupes p-valués, interviendrons dans la suite comme groupe de Galois d'extensions infinies de corps de nombres. On se restreindra vite aux groupes p-valués, dont l'algèbre d'Iwasawa possède des propriétés agréables. Ces propriétés sont listées dans ce chapitre et éclaircissent la structure des modules de type fini sur cette algèbre, modulo pseudo-isomorphisme. Ces résultats de structure seront un point clef des démonstrations futures. On expliquera aussi comment construire des extensions de Lie p-adiques d'un corps de nombres, vérifiant des contraintes arithmétiques supplémentaires nécessaires à l'application des résultats des chapitres suivants.

1.1. Groupes de Lie p-adiques

Le contenu de ce paragraphe est issu principalement de **[6]** et **[26]** .

1.1.1. Variétés analytiques sur $\mathbb{Q}_p$. — Soit p un nombre premier et $\mathbb{Q}_p$ le corps des nombres p-adiques.
Le but de cette première section est de donner la définition de variété analytique sur $\mathbb{Q}_p$. Elle repose sur la notion de fonction analytique :

Définition 1.1.1. — Une application $f : \mathbb{Q}_p^n \to \mathbb{Q}_p$ est dite (localement) analytique si pour tout $x \in \mathbb{Q}_p^n$, il existe un voisinage $B(x, p^{-r}) = x + p^r\mathbb{Z}_p^n$ de x sur lequel f est donnée par une série convergente à coefficients dans $\mathbb{Q}_p$:

$$f(x + p^r z) = \sum_{i \in \mathbb{N}^n} a_i z^i.$$

Une application $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ est dite analytique si chacune de ses composantes est analytique.

Une variété analytique sur $\mathbb{Q}_p$ est une variété sur $\mathbb{Q}_p$ au sens géométrique, pour laquelle les applications de changement de carte sont analytiques. Plus précisément :

Définition 1.1.2. — Soit V un espace topologique.
Un atlas de cartes sur V est la donnée d'un recouvrement $\{U_i\}_i$ de V par des ouverts et d'homeomorphismes $\{\varphi_i : U_i \to \varphi_i(U_i)\}_i$ entre U_i et un ouvert de $\mathbb{Z}_p^n$ vérifiant la condition de compatibilité suivante : l'application $\varphi_i \circ \varphi_j^{-1}$ est analytique sur l'ouvert $\varphi_j(U_i \cap U_j)$. Les couples (U_i, φ_i) sont appelés cartes de V.
Deux atlas sont dit compatibles si leur union forme toujours un atlas et une structure de variété analytique sur V est la donnée d'une classe d'équivalence d'atlas compatibles.
L'entier n est appelé dimension de la variété.

Cette définition vient avec une notion de fonction analytique entre deux variétés.

Définition 1.1.3. — Soient V et V' deux variétés analytiques sur $\mathbb{Q}_p$. Une fonction $f : V \to V'$ est dite analytique si pour toutes cartes (U, φ) de V et (U', φ') de V' :
- l'image réciproque $f^{-1}(U')$ est un ouvert de V.
- l'application $\varphi' \circ f \circ \varphi^{-1}$ est analytique sur $\varphi(U \cap f^{-1}(U'))$.

1.1.2. Groupes de Lie p-adiques. — Un groupe de Lie p-adique, aussi appelé groupe analytique p-adique, est un ensemble sur lequel sont mêlés structure de groupe et de variété analytique sur $\mathbb{Q}_p$.

Définition 1.1.4. — Un groupe de Lie p-adique est un groupe topologique $(G, .)$, muni d'une structure de variété analytique sur $\mathbb{Q}_p$ telle que les opérations de groupe $(x, y) \mapsto x.y$ et $x \mapsto x^{-1}$ soient des fonctions analytiques.

Les exemples canoniques de groupes de Lie p-adiques sont $(\mathbb{Z}_p^n, +)$ et $(\mathbb{Q}_p^n, +)$. On va maintenant donner la structure de groupe de Lie p-adique sur le groupe linéaire $(\mathrm{GL}_n(\mathbb{Q}_p), .)$. La topologie est la topologie naturelle, qui est l'induite de la topologie produit sur $\mathrm{M}_n(\mathbb{Q}_p) \simeq \mathbb{Q}_p^{n^2}$. L'ouvert $\mathrm{GL}_n(\mathbb{Q}_p)$ hérite, de ce fait, de la structure de variété analytique de $\mathbb{Q}_p^{n^2}$. Il suffit alors de voir que les opérations de produit matriciel et d'inversion sont analytiques. En ce qui concerne le produit, les coefficients de la matrice produit sont donnés par des applications polynômiales (donc analytiques) en les coefficients des matrices de départ. Il en est de même de l'inversion grâce à la formule de la comatrice. Les sous-groupes ouverts de $\mathrm{GL}_n(\mathbb{Q}_p)$ sont également des groupes analytiques p-adiques, en particulier $\mathrm{GL}_n(\mathbb{Z}_p)$. Sa dimension est n^2.

La structure de groupe de Lie p-adique sur $\mathrm{SL}_n(\mathbb{Q}_p)$ se décrit de la façon suivante. Tout d'abord, $\mathrm{SL}_n(\mathbb{Q}_p)$ est le noyau du morphisme $det : \mathrm{GL}_n(\mathbb{Q}_p) \to \mathbb{Q}_p^\times$ qui envoie la matrice (a_{ij}) sur $\sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$. Il suit que si on pose $U_\sigma = \left\{(a_{ij}) \in \mathrm{SL}_n(\mathbb{Q}_p) \mid \prod_{i=1}^n a_{i\sigma(i)} \neq 0\right\}$, la famille d'ouverts $\{U_\sigma\}_{\sigma \in S_n}$ recouvre $\mathrm{SL}_n(\mathbb{Q}_p)$. On associe à chacun de ces ouverts l'application $\varphi_\sigma : U_\sigma \to \mathbb{Q}_p^{n^2-1}$ qui envoie (a_{ij}) sur $(a_{ij})_{(i,j)\neq(1,\sigma(1))}$. Pour $\sigma \in S_n$ et $(a_{ij}) \in U_\sigma$, l'élément $a_{1\sigma(1)}$ est déterminé de manière unique par les autres coefficients de la matrice, *via* la formule du déterminant. Il en résulte que l'application φ_σ est un isomorphisme entre U_σ et l'ouvert de $\mathbb{Q}_p^{n^2-1}$ déterminé par les conditions $a_{i\sigma(i)\neq 0}$ pour $i \neq 1$. On vérifie que l'ensemble des couples $\{(U_\sigma, \varphi_\sigma)\}_\sigma$ forme bien un atlas sur $\mathrm{SL}_n(\mathbb{Q}_p)$, qui est par conséquent un groupe de Lie p-adique de dimension $n^2 - 1$. Il en est de même de $\mathrm{SL}_n(\mathbb{Z}_p)$.

1.1.3. Groupes p-valués. — La structure analytique d'un groupe de Lie p-adique peut être déterminée de manière algébrique. En effet, il est équivalent pour un groupe topologique profini de posséder une structure analytique p-adique et de posséder un sous-groupe d'indice fini qui est un pro-p-groupe avec de bonnes propriétés. Ce sont ces bonnes propriétés qui sont décrites dans la définition de groupe p-valué.

Définition 1.1.5. — Un groupe G est dit p-valué s'il est muni d'une application $\nu : G \to \mathbb{R}_+^* \cup \{+\infty\}$, appelée valuation, vérifiant les axiomes :

i) $\nu(xy^{-1}) \geqslant \min(\nu(x), \nu(y))$,

ii) $\nu(x^{-1}y^{-1}xy) \geqslant \nu(x) + \nu(y)$,

iii) $\nu(x) = +\infty \Leftrightarrow x = 1$,

iv) $\nu(x) > (p-1)^{-1}$,

v) $\nu(x^p) = \nu(x) + 1$.

Théorème 1.1.6. — *Un groupe est p-adique analytique si et seulement s'il possède un sous-groupe ouvert qui est un pro-p-groupe p-valué de type fini.*

Un groupe p-valué est donc un prototype intéressant de groupe analytique. Remarquons que l'on peut exiger une condition plus forte sur le sous-groupe p-valué. On peut lui demander d'être uniforme, c'est à dire d'être un pro-p-groupe de type fini tel que le quotient par son sous-groupe engendré par les puissances p-ièmes soit abélien et que les quotients successifs de la suite centrale descendante soient de cardinal constant. C'est le point de vue adopté dans [**6**]. On se concentrera sur la notion de groupe p-valué, qui a l'avantage d'être un peu plus générale.

Pour $(\mathbb{Q}_p^n, +)$, il suffit de considérer le sous-groupe ouvert $(\mathbb{Z}_p^n, +)$, pour la valuation donnée par le minimum des valuations p-adiques sur chaque composante.
Pour l'exemple de $G = \mathrm{GL}_n(\mathbb{Z}_p)$, on peut prendre comme pro-p-sous-groupe p-valué le premier sous-groupe de congruences $G_1 = \mathrm{Id}_n + p\mathrm{M}_n(\mathbb{Z}_p)$ si p est impair. Si $p = 2$, on prend $G_2 = \mathrm{Id}_n + 4\mathrm{M}_n(\mathbb{Z}_2)$. Il est p-valué pour la valuation induite par sa filtration par les sous-groupes $G_i = \mathrm{Id}_n + p^i\mathrm{M}_n(\mathbb{Z}_p)$.

Les groupes de Galois que l'on va considérer dans la suite seront toujours profinis et de type fini. Voici quelques propriétés des groupes p-valués satisfaisant ces hypothèses (voir **[26]**).

Proposition 1.1.7. — *Soit G un groupe p-valué profini de type fini. Alors :*

1. *Le groupe G est un pro-p-groupe analytique sans élément d'ordre fini.*
2. *La valuation ν est discrète.*

Si la valuation sur le groupe p-valué G sera, dans notre cas, toujours discrète ; il est possible de la grossir pour la rendre à valeurs entières. On pose pour $n \in \mathbb{N}^*$:

$$G_n = \{x \in G \mid \nu(x) > (p-1)^{-1} + n - 1\}.$$

La filtration de G par les sous-groupes G_n conduit à une valuation à valeurs entières ν', en posant $\nu'(x) = \sup\{n \in \mathbb{N} \mid x \in G_n\}$.
L'indice des G_n dans G est alors d'une certaine régularité :

Proposition 1.1.8. — *Soit G un pro-p-groupe p-valué de type fini de dimension d et G_n les sous-groupes de G définis ci-dessus. Il existe une constante C telle que les indices des G_n dans G vérifient, pour n assez grand :*

$$(G : G_n) = Cp^{nd}.$$

Démonstration. — On utilise les résultats et le vocabulaire de **[26]**.
Pour n_0 assez grand, le groupe G_{n_0} est p-saturé de dimension d (**[26]**, *III* 3.1.13). En particulier, $(G_{n_0} : G_{n_0+k}) = p^{kd}$ (**[26]**, *III* 3.1.8) et on a pour $n \geqslant n_0$

$$(G : G_n) = (G : G_{n_0})(G_{n_0} : G_n) = p^{c+(n-n_0)d}.$$

□

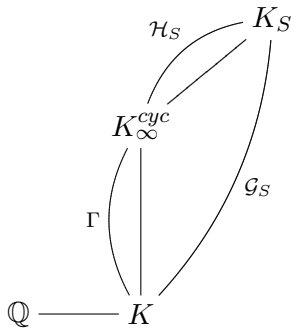
Lorsque G est uniforme, on a $G_n = G^{p^n}$ et la constante C de la proposition 1.1.8 est égale à 1.

1.2. Constructions d'extensions de Lie

Les groupes de Lie p-adiques introduits dans la section précédente nous intéressent particulièrement lorsqu'ils apparaîssent comme groupe de Galois d'une extension d'un corps de nombre, appelée alors extension de Lie p-adique. L'objet de cette partie est la construction d'extensions de Lie p-adiques, vérifiant certaines contraintes importantes pour les applications arithmétiques. On exigera que l'extension contiennent la $\mathbb{Z}_p$-extension cyclotomique du corps de base et que seul un nombre fini de places du corps de base se ramifient dans l'extension de Lie.

Outre l'exemple historique des $\mathbb{Z}_p$-extensions et $\mathbb{Z}_p$-extensions multiples, qui sont abéliennes, certaines extensions de Lie p-adiques non commutatives sont souvent prises en exemple pour illustrer la théorie. C'est le cas de la fausse courbe de Tate, donnée par l'extension $\mathbb{Q}(\zeta_{p^\infty}, \sqrt[p^\infty]{p})/\mathbb{Q}(\zeta_p)$. Son groupe de Galois est isomorphe à un produit semi-direct $\mathbb{Z}_p \rtimes \mathbb{Z}_p$. Dans ces premiers exemples, seules les places au-dessus de p sont ramifiées.
On obtient des extensions de Lie p-adiques d'un corps de nombres K en regardant l'action du groupe de Galois absolu $G_K = \mathrm{Gal}(\overline{K}/K)$ sur les objets géométriques $H^i_{et}(\overline{Y}, \mathbb{Q}_p)(j)$, où Y est une variété projective lisse absolument irréductible définie sur K. Lorsque Y est une courbe elliptique non CM fixée, on réalise ainsi des $\mathrm{GL}_2(\mathbb{Z}_p)$-extensions, à part pour un nombre fini de premiers p (voir **[37]**). Ces extensions sont non-ramifiées en dehors de p et des places de mauvaise réduction de Y.

On donne ici une construction galoisienne d'extensions de Lie p-adiques. Le point de départ est l'existence d'extensions de groupe de Galois pro-p-libre au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres.
Soit K un corps de nombres totalement réel et soit K_∞^{cyc} sa $\mathbb{Z}_p$-extension cyclotomique. On se donne aussi un ensemble fini S de places de K contenant l'ensemble Pl_p des places p-adiques. On écrira K_S pour la pro-p-extension S-ramifiée maximale de K. C'est une extension galoisienne contenant K_∞^{cyc}. Le treillis suivant fixe les notations pour les différents groupes de Galois :



On renvoie à la partie 2.1 pour la définition des invariants d'Iwasawa μ et λ qui interviennent dans la proposition suivante :

Proposition 1.2.1. — *Sous la conjecture d'Iwasawa $\mu(K_\infty^{cyc}/K) = 0$, le groupe $\mathcal{H}_S$ est pro-p-libre de rang égal à l'invariant d'Iwasawa $\lambda_S(K_\infty^{cyc}/K)$.*

Démonstration. — Considérons la suite exacte longue de $\mathcal{H}_S$-cohomologie de

$$0 \to \mathbb{F}_p \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

Elle conduit à

$$H^1(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p} H^1(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(\mathcal{H}_S, \mathbb{F}_p) \to H^2(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p).$$

On fait plusieures remarques concernant les termes de cette suite.
Tout d'abord, la conjecture de Leopoldt faible, valable ici, prédit l'annulation du dernier terme $H^2(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p)$ (voir [**33**]).
Ensuite, l'action de $\mathcal{H}_S$ sur $\mathbb{Q}_p/\mathbb{Z}_p$ étant triviale, le groupe $H^1(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p)$ n'est autre que le dual de Pontryagin de l'abélianisé de $\mathcal{H}_S$. On a donc

$$H^1(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p) = X_S^\vee,$$

avec X_S le module d'Iwasawa S-ramifié de l'extension cyclotomique. On sait que ce module d'Iwasawa est de $\Lambda(\Gamma)$-rang nul car K est totalement réel ; qu'il est également d'invariant μ_S nul par hypothèse ; et qu'il ne possède pas de sous-module fini non nul. C'est donc, d'après le théorème de structure, un $\mathbb{Z}_p$-module libre de rang λ_S. Son dual de Pontryagin $X_S^\vee$ est alors p-divisible ce qui entraîne que la multiplication par p dans la suite exacte longue est surjective.

On en déduit que le module $H^2(\mathcal{H}_S, \mathbb{F}_p)$ des relations de $\mathcal{H}_S$ est nul. Le pro-p-groupe $\mathcal{H}_S$ est donc libre et son rang est égal au $\mathbb{Z}_p$-rang de son abélianisé, soit λ_S. □

Remarquons que la conjecture d'Iwasawa est démontrée pour un corps de base abélien sur $\mathbb{Q}$ (voir [**7**]).

Plaçons nous maintenant sous les hypothèses de la proposition 1.2.1 et considérons un pro-p-groupe p-valué de rang inférieur à λ_S. On remarque que le

corollaire 3.1.2 à venir assure que λ_S peut être aussi grand que voulu. On le note P et on appelle ν sa valuation. La propriété universelle des pro-p-groupes libres fournit une surjection $\mathcal{H}_S \twoheadrightarrow P$ et permet d'introduire un sous-corps L de K_S, tel que le groupe de Galois de l'extension L/K_∞^{cyc} soit isomorphe à P. On va construire, à partir de L, une extension galoisienne de K dont le groupe de Galois est un groupe de Lie p-adique. Pour cela, on va étudier les conjugués de P sous l'action de Γ.
Soit $\gamma \in \Gamma$. On note $\tilde{\gamma}$ un relèvement de γ à $\mathcal{G}_S$ et on démontre le résultat suivant.

Lemme 1.2.2. — *Le corps $\tilde{\gamma}(L)$ ne dépend pas du relèvement de γ et son groupe de Galois sur K_∞^{cyc}, que l'on note P^γ, est un groupe p-valué isomorphe à P.*

Démonstration. — La première assertion est immédiate. Deux relèvements de γ diffèrent d'un élément $h \in \mathcal{H}_S$, qui est un automorphisme lorsqu'on le restreint à L.

On obtient un isomorphisme entre P et P^γ en associant à $x \in P$ la restriction à $\gamma(L)$ de $\tilde{\gamma}x\tilde{\gamma}^{-1}$. Cet isomorphisme dépend du choix du relèvement de γ.
Le groupe P^γ est alors p-valué pour la valuation ν_γ définie par

$$\nu_\gamma(x) = \nu((\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}).$$

Bien que l'isomorphisme entre P et P^γ dépende du relèvement de γ, la valuation ν_γ est canonique, ce qui justifie l'absence du tilde dans son écriture. En effet, prenons $\tilde{\gamma}h$ un autre relèvement de γ, avec $h \in \mathcal{H}_S$ et soit $x \in P^\gamma$. Il vient :

$$\begin{aligned}
\nu\left(((\tilde{\gamma}h)^{-1}x(\tilde{\gamma}h))_{|L}\right) &= \nu\left(h_{|L}^{-1}(\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}h_{|L}\right) \\
&\geqslant \min\left(\nu\left(h_{|L}^{-1}(\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}h_{|L}(\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}^{-1}\right), \nu\left((\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}\right)\right) \\
&\geqslant \min\left(\nu(h_{|L}) + \nu\left((\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}\right), \nu\left((\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}\right)\right) \\
&= \nu\left((\tilde{\gamma}^{-1}x\tilde{\gamma})_{|L}\right).
\end{aligned}$$

L'inégalité réciproque se démontre par symétrie. □

On introduit alors le corps L', défini comme le composé des corps $\gamma(L)$ lorsque γ parcourt Γ.

Proposition 1.2.3. — *L'extension L'/K est galoisienne et le groupe de Galois $P' = \mathrm{Gal}(L'/K_\infty^{cyc})$ est p-valué.*

Démonstration. — L'extension L'/K est galoisienne par construction. Il s'agit alors de voir que P' est p-valué.

Pour tout $\gamma \in \Gamma$, il existe un surjection canonique $\pi_\gamma : P' \twoheadrightarrow P^\gamma$. On va vérifier que l'application

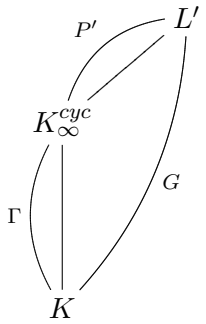
$$\nu' : x \in P' \mapsto \inf_{\gamma \in \Gamma} (\nu_\gamma(\pi_\gamma(x)))$$

est bien une p-valuation sur P'.
Par construction, les valuations ν_γ prennent toutes leurs valeurs dans l'ensemble $\nu(P)$, qui est discret (proposition 1.1.7). Par conséquent, l'inf est en fait un minimum et l'axiome iv) de la définition 1.1.5 est vérifié.
Les axiomes i), ii) et v) découlent d'un calcul direct utilisant la validité de ces mêmes relations pour toutes les valuations ν_γ.
En ce qui concerne l'axiome iii), on a $\nu'(x) = +\infty$ si et seulement si $\nu_\gamma(\pi_\gamma(x)) = +\infty$ pour tout $\gamma \in \Gamma$; donc si et seulement si $\pi_\gamma(x) = 1$ pour tout γ. Cette dernière condition est équivalente au fait que la restriction de x à chacun des corps $\gamma(L)$ est triviale. Comme L' est la composée des corps $\gamma(L)$, on obtient

$$\nu'(x) = +\infty \Longleftrightarrow x = 1.$$

□

On a donc construit l'extension suivante :



dans laquelle le groupe P' est un pro-p-groupe p-valué de type fini et G est un groupe de Lie p-adique en tant qu'extension de groupes de Lie.
On sait, d'après le théorème 1.1.6, qu'il existe une extension finie F de K telle que le groupe de Galois de L'/F est un pro-p-groupe p-valué de type fini.

1.3. Structure des Λ-modules

On peut construire l'algèbre d'Iwasawa d'un groupe profini de la façon suivante :

Définition 1.3.1. — Soit G un groupe profini. L'algèbre d'Iwasawa de G à coefficients dans $\mathbb{Z}_p$, notée $\Lambda(G)$ ou Λ, est la limite projective :

$$\Lambda(G) = \mathbb{Z}_p[[G]] = \varprojlim_{U \lhd_o G} \mathbb{Z}_p[G/U],$$

où U parcout l'ensemble des sous-groupes distingués d'indice fini de G.
On sera aussi amené à considérer l'algèbre complète de G sur $\mathbb{F}_p$:

$$\Omega = \Omega(G) = \mathbb{F}_p[[G]] = \varprojlim_{U \lhd_o G} \mathbb{F}_p[G/U].$$

Etant donnée une extension de Lie p-adique K_∞/K de groupe de Galois G, certains $\mathbb{Z}_p$-modules attachés à K_∞ sont naturellement munis d'une action continue de G, et donc d'une structure de $\Lambda(G)$-module. On portera, dans la suite, une attention toute particulière aux modules d'Iwasawa construits à partir des p-groupes de classes généralisés.
On ne sait que très peu de choses sur l'algèbre d'Iwasawa d'un groupe de Lie p-adique quelconque, en particulier si celui-ci possède des éléments d'ordre fini. Nous mettrons donc des restrictions sur les groupes étudiés. Après avoir donné les résultats pour $G \simeq \mathbb{Z}_p$, on se penchera sur le cas d'un pro-p-groupe p-valué de type fini. On rappelle que le théorème 1.1.6 assure que tout groupe de Lie p-adique de dimension non nulle possède un sous-groupe ouvert avec cette propriété, ce sous-groupe étant d'indice fini si le groupe de Lie est compact.

1.3.1. Le cas $\mathbb{Z}_p$. — On peut se référer à **[36]** pour cette section. On considère ici un groupe Γ isomorphe à $\mathbb{Z}_p$.

Proposition 1.3.2. — *L'algèbre d'Iwasawa $\Lambda(\Gamma)$ est isomorphe à une algèbre de séries formelles à une indéterminée à coefficients dans $\mathbb{Z}_p$:*

$$\Lambda(\Gamma) \simeq \mathbb{Z}_p[[T]].$$

L'isomorphisme s'obtient en fixant un générateur topologique γ de Γ et en lui associant le polynôme $T + 1$.
Ce résultat permet de donner la structure des modules de type fini sur $\Lambda(\Gamma)$ à pseudo-isomorphisme près :

Théorème 1.3.3 **(Iwasawa, [36], théorème 7)**. — *Soit X un $\Lambda(\Gamma)$-module de type fini. Il existe des entiers naturels ρ ; $(\alpha_i)_{i=1,\cdots,r}$; $(\beta_j)_{j=1,\cdots,s}$; ainsi que des polynômes distingués irréductibles $(f_j)_{j=1,\cdots,s}$; uniques à permutation près, tels qu'on ait un morphisme de $\Lambda(\Gamma)$-modules à noyau et conoyau finis :*

$$\varphi : X \to E = \Lambda(\Gamma)^\rho \oplus (\oplus_{i=1,\cdots,r} \Lambda(\Gamma)/p^{\alpha_i}) \oplus \left(\oplus_{j=1,\cdots,s} \Lambda(\Gamma)/f_j^{\beta_j}\right).$$

Les entiers ρ, $\mu = \sum_{i=1}^{r} \alpha_i$ *et* $\lambda = \deg \prod_{j=1}^{s} f_j^{\beta_j}$ *sont appelés les invariants d'Iwasawa de* X.

Le polynôme $F_X = p^{\mu} \prod_{j=1}^{s} f_j^{\beta_j}$ *est dit série caractéristique du module* X.

Un $\Lambda(\Gamma)$*-module ayant la forme de* E *sera appelé module élémentaire.*

1.3.2. Le cas p-valué. — Lorsque G est isomorphe à $\mathbb{Z}_p$, on vient de voir que l'algèbre d'Iwasawa correspondante est une algèbre de séries formelles. Cette forme explicite permet de connaître la structure des Λ-modules dans ce cadre. On regroupe dans un premier temps différentes propriétés de l'algèbre d'Iwasawa d'un pro-p-groupe p-valué de type fini G, de dimension d strictement positive. Nous verrons ensuite ce que l'on peut dire des modules de type fini sur cette algèbre.

1.3.2.1. Algèbre d'Iwasawa d'un groupe p-valué. — Les résultats qui suivent, tout comme le nom de groupe p-valué, sont tirés des travaux de Lazard **[26]**. On rapelle d'abord la notion d'idéal d'augmentation.

Définition 1.3.4. — Soit G un groupe profini et U un sous-groupe d'indice fini de G. On définit l'idéal d'augmentation I_U de $\Lambda(G)$ (ou de $\Omega(G)$ de manière similaire) comme le noyau de la réduction modulo U :

$$I_U = \ker(\Lambda(G) \twoheadrightarrow \mathbb{Z}_p[G/U]).$$

Proposition 1.3.5 **(Lazard, [26],** *II* 2.2.2**)**. — *Soit* G *un pro-*p*-groupe* p*-valué de type fini. Les algèbres correspondantes* Λ *et* Ω *sont locales, d'idéaux maximaux respectifs* $p\Lambda + I_G$ *et* I_G.

Etant donné G un pro-p-groupe p-valué de type fini, on peut construire une algèbre graduée à partir de son algèbre d'Iwasawa. On considère la chaîne d'idéaux I_G^k de Λ (ou de Ω). L'algèbre graduée $\mathrm{Gr}(\Lambda)$ (ou $\mathrm{Gr}(\Omega)$) est alors la somme directe $\bigoplus_{k=0}^{\infty} I_G^k/I_G^{k+1}$. Il se trouve que cette algèbre possède de très bonnes propriétés, qui se reflètent sur l'algèbre d'Iwasawa correspondante.

Proposition 1.3.6 **(Lazard, [26],** *III* 2.3.3**)**. — *Soit* G *un pro-*p*-groupe* p*-valué de type fini de dimension* d*. Les algèbres graduées* $\mathrm{Gr}(\Lambda)$ *et* $\mathrm{Gr}(\Omega)$ *sont des algèbres de polynômes à respectivement* $d+1$ *et* d *variables.*

Corollaire 1.3.7. — *Soit* G *un pro-*p*-groupe* p*-valué de type fini. Les algèbres correspondantes* Λ *et* Ω *sont noethériennes à droite et à gauche et intègres.*

1.3.2.2. Invariants des Λ-modules. — A partir de maintenant, Λ désignera l'algèbre d'Iwasawa d'un pro-p-groupe p-valué de type fini G, de dimension $d \geqslant 1$. On s'intéresse aux Λ-modules de type fini, c'est-à-dire aux $\mathbb{Z}_p$-modules topologiques avec une action continue de G, qui sont de type fini pour leur structure de Λ-module étendant l'action de G. On va commencer par définir trois invariants pour de tels modules. Ils généralisent les invariants d'Iwasawa ρ, μ et r qui apparaissent dans le théorème de structure (théorème 1.3.3), lorsque le groupe G est isomorphe à $\mathbb{Z}_p$. Les invariants ρ et μ ont déjà fait l'objet d'études de la part de Harris [**12**], Venjakob [**38**] et Howson [**15**].

Définition 1.3.8. — Soit M un Λ-module de type fini. On définit les invariants d'Iwasawa de M de la façon suivante :

$$\rho(M) = \mathrm{rk}_\Lambda(M) = \dim_F(F \otimes_\Lambda M),$$

avec F le corps gauche des fractions de Λ (voir [**27**]). C'est le rang de M.

$$r(M) = \mathrm{rk}_\Omega(M[p]).$$

$$\mu(M) = \sum_{i \geq 0} \mathrm{rk}_\Omega(M[p^{i+1}]/M[p^i]).$$

Pour $i \in \mathbb{N}$, $M[p^i]$ désigne les éléments de M tués par p^i.

L'invariant ρ est additif sur les suites exactes de Λ-modules et un Λ-module M est de torsion si et seulement si $\rho(M) = 0$. Quant aux invariants r et μ, ils mesurent la $\mathbb{Z}_p$-torsion de M. L'invariant μ ne dépend que du sous-module de $\mathbb{Z}_p$-torsion de M et est additif sur les suites exactes de modules de Λ-torsion ([**38**] corollaire 3.37), tandis que r ne dépend que de $M[p]$ et est additif sur les suites exactes de modules tués par p. Ces deux derniers invariants sont aussi donnés par les formules suivantes :

Lemme 1.3.9. — *Pour M un Λ-module de type fini, on a*

$$\begin{aligned} r(M) &= \mathrm{rk}_\Omega(\mathrm{tor}_{\mathbb{Z}_p}(M)/p) \\ &= \mathrm{rk}_\Omega(\mathrm{tor}_\Lambda(M)/p). \\ \mu(M) &= \sum_{i \geq 0} \mathrm{rk}_\Omega(p^i \mathrm{tor}_{\mathbb{Z}_p}(M)/p^{i+1}\mathrm{tor}_{\mathbb{Z}_p}(M)) \\ &= \sum_{i \geq 0} \mathrm{rk}_\Omega(p^i \mathrm{tor}_\Lambda(M)/p^{i+1}\mathrm{tor}_\Lambda(M)). \end{aligned}$$

Démonstration. — Notons dans cette preuve $T = \mathrm{tor}_{\mathbb{Z}_p}(M)$.
L'anneau Λ étant noethérien, il existe un entier α tel que $T = M[p^\alpha]$.
Quotienter par p la suite exacte

$$0 \to pT \to T \to T/p \to 0$$

conduit à la suite exacte de Ω-modules :

$$0 \to (pT)[p] \to T[p] \to T/p \to (pT)/p \to T/p \to T/p \to 0.$$

La somme alternée des Ω-rangs nous informe que

$$\mathrm{rk}_\Omega(T[p]) - \mathrm{rk}_\Omega(T/p) = \mathrm{rk}_\Omega((pT)[p]) - \mathrm{rk}_\Omega((pT)/p).$$

Il est possible d'itérer les calculs en remplaçant T par pT. On obtient, pour tout entier i :

$$\mathrm{rk}_\Omega(T[p]) - \mathrm{rk}_\Omega(T/p) = \mathrm{rk}_\Omega((p^iT)[p]) - \mathrm{rk}_\Omega((p^iT)/p) = 0,$$

la nullité provenant du cas $i = \alpha$.
On justifie la première égalité du lemme pour r et μ en notant que

$$T[p^{i+1}]/T[p^i] \simeq p^i(T[p^{i+1}]) = (p^iT)[p].$$

Enfin, pour voir que l'on peut calculer μ et r à partir du sous-module $\mathrm{tor}_\Lambda(M)$, on regarde pour tout $i \in \mathbb{N}$ la suite exacte

$$0 \to p^iT \to p^i\mathrm{tor}_\Lambda(M) \to p^i\mathrm{tor}_\Lambda(M)/p^iT \to 0.$$

Le dernier terme de cette suite, que l'on note N, est un Λ-module de torsion sans p-torsion. Quotienter par p donne donc

$$0 \to p^iT/p^{i+1}T \to p^i\mathrm{tor}_\Lambda(M)/p^{i+1}\mathrm{tor}_\Lambda(M) \to N/p \to 0,$$

où N/p est un Ω-module de torsion. L'additivité du rang permet de conclure que

$$\mathrm{rk}_\Omega(p^iT/p^{i+1}T) = \mathrm{rk}_\Omega(p^i\mathrm{tor}_\Lambda(M)/p^{i+1}\mathrm{tor}_\Lambda(M)).$$

□

1.3.2.3. Résultats de structure. — Beaucoup de résultats de la théorie d'Iwasawa classique reposent sur le théorème de structure des Λ-modules de type fini à pseudo-isomorphisme près (théorème 1.3.3). Coates, Schneider et Sujatha, dans **[3]**, ainsi que Venjakob, dans **[38]**, ont ouvert la voie vers une généralisation au cas non-commutatif de ce théorème. On rappelle la notion de pseudo-nullité qu'ils ont introduite dans ce contexte, notion qui se ramène à la finitude lorsque $G \simeq \mathbb{Z}_p$. La notation $\mathrm{Ext}_\Lambda(-,-)$ désignera les dérivés du bifoncteur $\mathrm{Hom}_\Lambda(-,-)$ des homomorphismes continus entre Λ-modules de type fini.

Définition 1.3.10. — Un Λ-module de type fini M est dit pseudo-nul si

$$\mathrm{Ext}^0_\Lambda(M,\Lambda) = \mathrm{Ext}^1_\Lambda(M,\Lambda) = 0.$$

Un morphisme $\varphi : M \to N$ entre deux Λ-modules de type fini est appelé pseudo-isomorphisme si le noyau et le conoyau de φ sont pseudo-nuls.

Le lemme suivant indique que la sous-catégorie des modules pseudo-nuls vérifie la condition de Serre, et permet de considérer la catégorie quotient.

Lemme 1.3.11. — *Tout sous-module et tout quotient d'un module pseudo-nul est pseudo-nul.*

Démonstration. — C'est la proposition 3.6 de **[38]**. □

On démontre alors la proposition suivante, qui met en évidence le fait que les invariants d'Iwasawa se comportent bien vis-à-vis des pseudo-isomorphismes.

Proposition 1.3.12. — *Soit M et N deux Λ-modules de type fini pseudo-isomorphes. Alors $\rho(M) = \rho(N)$, $\mu(M) = \mu(N)$ et $r(M) = r(N)$.*

Démonstration. — La condition $\mathrm{Ext}^0_\Lambda(A, \Lambda) = \mathrm{Hom}_\Lambda(A, \Lambda) = 0$ indique que tout Λ-module pseudo-nul A est de torsion. Ceci entraîne que $\rho(A) = 0$ et, comme ρ est aussi additif sur les suites exactes, il est invariant modulo pseudo-isomorphisme.

En ce qui concerne r, on écrit la suite exacte donnée par le pseudo-isomorphisme :

$$0 \to A \to M \xrightarrow{\varphi} N \to B \to 0$$

et on note $Z = \mathrm{Im}(\varphi)$. Le lemme du serpent permet d'extraire les deux suites exactes

$$A[p] \to M[p] \to Z[p] \to A/p$$

et

$$0 \to Z[p] \to N[p] \to B[p].$$

D'après le lemme 1.3.11, les termes extrémaux de ces deux suites sont des modules pseudo-nuls tués par p. Le lemme 1.3.13 ci-dessous donne alors $r(M) = r(Z) = r(N)$ en regardant les Ω-rangs des termes des deux suites.

Lemme 1.3.13. — *Soit A un Λ-module pseudo-nul tué par p, alors A est un Ω-module de torsion.*

Démonstration. — Soit A un Λ-module pseudo-nul tué par p. La suite exacte $0 \to \Lambda \xrightarrow{p} \Lambda \to \Omega \to 0$ conduit à l'encadrement

$$\mathrm{Ext}^0_\Lambda(A, \Lambda) \to \mathrm{Hom}_\Lambda(A, \Omega) \to \mathrm{Ext}^1_\Lambda(A, \Lambda).$$

La pseudo-nullité de A entraîne la nullité de $\mathrm{Hom}_\Lambda(A, \Omega)$, qui coïncide avec $\mathrm{Hom}_\Omega(A, \Omega)$. Le Ω-module A est donc de torsion. □

En ce qui concerne μ, on utilise des arguments similaires exposés dans la preuve de la proposition 3.34 de **[38]**. □

Le premier des deux résultats importants que l'on énonce ici donne, à pseudo-isomorphisme près, la structure de la $\mathbb{Z}_p$-torsion d'un Λ-module de type fini. Il permet, comme dans le cadre de la théorie commutative, de lire les invariants μ et r sur un module élémentaire.

Théorème 1.3.14 **(Venjakob, [38], théorème** 3.40**)**

Soit M un Λ-module de type fini. Il existe des uniques entiers naturels $\alpha_1, ..., \alpha_r$ tels que l'on ait un pseudo-isomorphisme :

$$\mathrm{tor}_{\mathbb{Z}_p}(M) \to \bigoplus_{i=1}^{r} \Lambda/p^{\alpha_i}.$$

De plus, $r(M) = r$ et $\mu(M) = \sum_{i=1}^{r} \alpha_i$.

L'autre résultat de structure que l'on expose permet de séparer les parties de torsion et sans torsion d'un Λ-module de type fini, en se plaçant dans la catégorie quotient par la sous-catégorie des modules pseudo-nuls (lemme 1.3.11). On note Q le foncteur canonique de passage au quotient.

Proposition 1.3.15 **(Coates, Schneider, Sujatha, [3], proposition** 6.4**)**

Soit M un Λ-module de type fini.
On a un isomorphisme dans la catégorie quotient :

$$Q(M) \simeq Q(\mathrm{tor}_\Lambda(M)) \oplus Q(\overline{M}),$$

où $\overline{M}$ désigne le quotient de M par son sous-module de Λ-torsion.

Remarquons que $\mathrm{tor}_\Lambda(M)$ est un Λ-module de torsion dont les invariants μ et r sont égaux à ceux de M, tandis que $\overline{M}$ est un Λ-module sans torsion de même rang que M.

CHAPITRE 2

FORMULES ASYMPTOTIQUES POUR LES GROUPES DES CLASSES

On se focalise dans cette section sur un certain type de modules d'Iwasawa, construits à partir de variations sur le groupe des classes. Le résultat motivant le travail effectué dans cette thèse est une formule asymptotique concernant l'ordre des p-groupes des classes le long d'une $\mathbb{Z}_p$-extension d'un corps de nombres.

Théorème 2.0.16 **(Iwasawa, [36], théorème** 2**).** — *Soit K_∞/K une $\mathbb{Z}_p$-extension du corps de nombres K et soit X_n le p-groupe des classes du n-ième étage K_n de la tour. Alors, pour n assez grand, on a :*

$$\#(X_n) = p^{\mu p^n + \lambda_n + \nu},$$

avec μ et λ les invariants d'Iwasawa du module à l'infini $X_\infty = \varprojlim X_n$ et ν un entier relatif.

Sa démonstration utilise fortement les techniques de montée-descente de la théorie d'Iwasawa. Après avoir défini les variantes du groupe des classes sur lesquelles on va se pencher dans la suite, nous verrons comment la théorie du corps de classes permet de relier ces groupes, attachés aux étages d'une extension de corps de nombres, aux coïnvariants d'un Λ-module à l'infini. Les théorèmes de structure du premier chapitre appliqués à ce module d'Iwasawa conduirons alors à des formules asymptotiques semblables au théorème d'Iwasawa ci-dessus.

2.1. Descente pour les groupes des classes

2.1.1. Le p-groupe des T-classes S-infinitésimales. — Commençons par donner une définition des p-groupes des classes généralisés en terme d'idèles.

Fixons un corps de nombres K et notons $\mathcal{I}$ son p-groupe des idèles. C'est l'ensemble des éléments du produit des pro-p-complétés des groupes multiplicatifs $\prod_v \mathcal{K}_v^\times$ des complétés de K en chacune de ses places v, qui sont des unités pour presque tout v. Soit $\mathcal{U}$ son sous-groupe unité (éléments qui sont des unités en chaque place). Le plongement de K dans ses complétés permet de voir $\mathbb{Z}_p \otimes K^\times$ comme un sous-groupe de $\mathcal{I}$. C'est le sous-groupe des p-idèles principaux que l'on notera $\mathcal{R}$. Le quotient du p-groupe des idèles par le sous-groupe engendré par les idèles unités et les idèles principaux est alors isomorphe au p-groupe des classes de K. Cet isomorphisme respecte l'action du groupe de Galois de $K/\mathbb{Q}$ sur le groupe des classes et sur le groupe des idèles :

$$\mathrm{Cl}(K)_p \simeq \mathcal{I}/\mathcal{U}\mathcal{R}.$$

Soient maintenant S et T deux ensembles finis de places de K. Nous allons définir le p-groupe des T-classes S-infinitésimales de K. Pour ce faire, on introduit le sous-groupe $\mathcal{I}_S^T$ des T-idèles S-infinitésimales. Il est constitué des idèles qui sont des unités aux places étrangères à T et S et qui valent 1 sur les places de S. Remarquons que dans le cas $S = T = \emptyset$, on a $\mathcal{I}_\emptyset^\emptyset = \mathcal{U}$.

Définition 2.1.1. — Soient S et T deux ensembles finis de places du corps de nombres K. On définit le p-groupe des T-classes S-infinitésimales de K comme le quotient

$$X_S^T = \mathcal{I}/\mathcal{I}_S^T\mathcal{R}$$

Ce groupe possède aussi une description en terme de groupe de classes de rayon (voir [**20**] $II.2$).
La finitude du groupe des classes classique $\mathrm{Cl}(K)$ conduit au résultat suivant.

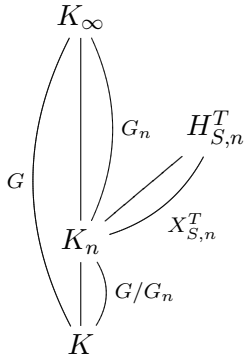
Proposition 2.1.2. — *Soient S et T deux ensembles finis de places du corps de nombres K. Alors le p-groupe des T-classes S-infinitésimales de K est un $\mathbb{Z}_p$-module de type fini.*

Le résultat fondamental de la théorie du corps de classes interprète ces p-groupes de classes généralisés en terme de groupes de Galois de p-extensions abéliennes de K. Une extension de K sera dite S-ramifiée et T-décomposée lorsque, dans cette extension, les places ramifiées sont contenues dans S et les places de T sont totalement décomposées. Une place réelle sera dite ramifiée si elle se complexifie, et non-ramifiée (ou totalement décomposée) dans le cas contraire.

Théorème 2.1.3. — *Soient S et T deux ensembles finis de places du corps de nombres K. Le p-groupe des T-classes S-infinitésimales X_S^T de K est isomorphe, en tant que module galoisien, au groupe de Galois de la p-extension abélienne S-ramifiée et T-décomposée maximale H_S^T de K.*

Démonstration. — voir **[20]**, théorème $II.2.21$ et proposition $II.2.38$. □

2.1.2. Le module d'Iwasawa $X_{S,\infty}^T$. — Soit K_∞/K une extension de Lie p-adique du corps de nombres K, de groupe de Galois G. On la suppose donnée par une tour d'extensions finies de K, dont les étages K_n sont les sous-corps de K_∞ fixés par des sous-groupes distingués ouverts G_n de G. Si G est p-valué, on peut prendre pour G_n la filtration entière de G. On fixe deux ensembles finis S et T de places de K et on notera toujours S et T pour les places d'une extension de K qui sont au-dessus de celles de S et T.
On peut associer à chaque étage K_n de la tour son p-groupe des T-classes S-infinitésimales, noté $X_{S,n}^T$.
Le treillis suivant résume les notations, en tenant compte de l'interprétation de $X_{S,n}^T$ comme groupe de Galois :



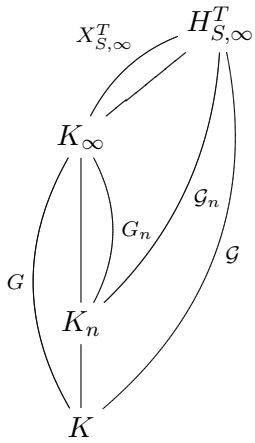
Construisons alors le système projectif $(X_{S,n}^T)_{n\in\mathbb{N}}$ dont la limite projective donne le Λ-module $X_{S,\infty}^T$.
Chacun des $X_{S,n}^T$ est muni d'une action de G/G_n de la façon suivante. Soit $g \in G/G_n$ et $x \in X_{S,n}^T$. On fixe un relèvement $\tilde{g}$ de g à $H_{S,n}^T$. Le conjugué $\tilde{g}x\tilde{g}^{-1}$ est un automorphisme de $\tilde{g}(H_{S,n}^T)$ qui laisse fixe le sous-corps K_n et qui est indépendant du choix du relèvement de g par abélianité de $H_{S,n}^T/K_n$. L'extension ainsi obtenue $\tilde{g}(H_{S,n}^T)/K_n$ reste abélienne, S-ramifiée et T-décomposée de telle sorte que c'est une sous-extension de $H_{S,n}^T/K_n$ par maximalité. Les corps $H_{S,n}^T$ et $\tilde{g}(H_{S,n}^T)$ étant isomorphes, ils sont égaux et $\tilde{g}x\tilde{g}^{-1} \in X_{S,n}^T$ est l'image de x sous l'action de g.
Maintenant, la composition de $H_{S,n}^T$ et de K_{n+1} forme un sous-corps de $H_{S,n+1}^T$ par maximalité. Les applications de transition $X_{S,n+1}^T \to X_{S,n}^T$ sont alors données par la restriction des automorphismes de $H_{S,n+1}^T$ à $H_{S,n}^T$. En terme d'idèles, ces applications correspondent à la norme au niveau des extensions locales.

On dispose donc d'un système projectif $(X_{S,n}^T)_{n\in\mathbb{N}}$ de $\mathbb{Z}_p$-modules de type fini munis d'une action galoisienne. Le passage à la limite projective fait ressortir un module $X_{S,\infty}^T$ sur l'algèbre d'Iwasawa Λ. Il est isomorphe au groupe de Galois de la p-extension abélienne S-ramifiée et T-décomposée maximale $H_{S,\infty}^T$ de K_∞. Ce module n'est pas de type fini en général, mais le sera sous les hypothèses de la section suivante.

2.1.3. Théorèmes de descente. — Ce paragraphe illustre en quoi l'étude des modules d'Iwasawa à l'infini permet d'obtenir des informations sur les objets arithmétiques au niveau fini. On reprend les notations de la section précédente en supposant de plus que :

- Le groupe $G = \mathrm{Gal}(K_\infty/K)$ est un pro-p-groupe p-valué de type fini de dimension $d \geqslant 1$.
- Il n'y a qu'un nombre fini de places de K ramifiées dans K_∞/K.

On munit G de sa filtation entière par les sous-groupes G_n (voir en 1.1.3) et on prend pour K_n le sous-corps de K_∞ fixé par G_n.
Pour S et T deux ensembles finis de places de K, on a introduit dans le paragraphe précédent le Λ-module $X_{S,\infty}^T$, qui s'interprète comme groupe de Galois d'une extension $H_{S,\infty}^T/K_\infty$. Par maximalité, l'extension $H_{S,\infty}^T$ est galoisienne sur le corps de base K, ainsi que sur chacun des étages K_n. Le treillis suivant fixe les notations pour les groupes de Galois correspondants :



Pour appliquer au Λ-module $X_{S,\infty}^T$ les résultats de structure de la section 1.3, on doit voir qu'il est de type fini. La prochaine proposition affirme que c'est le cas, et autorise ainsi à parler des invariant d'Iwasawa ρ_S^T, μ_S^T et r_S^T de $X_{S,\infty}^T$, aussi appelés invariants d'Iwasawa de l'extension K_∞/K relatifs au couple (S,T).

Proposition 2.1.4. — *Sous les hypothèses de cette section, le Λ-module $X_{S,\infty}^T$ est de type fini.*

Démonstration. — Le résultat peut se voir sur le diagramme du lemme 4.3 de [**19**] mais on en donne une preuve plus directe ici.
On obtient la suite exacte

$$H_2(G,\mathbb{F}_p) \to H_1(X_{S,\infty}^T,\mathbb{F}_p)_G \to H_1(\mathcal{G},\mathbb{F}_p)$$

en appliquant la suite exacte d'inflation-restriction à coefficients dans $\mathbb{F}_p$ à la suite exacte $0 \to X_{S,\infty}^T \to \mathcal{G} \to G \to 0$.

Le groupe abélien $H_2(G,\mathbb{F}_p)$ est de type fini du fait que G est analytique. Ce terme de gauche étant également tué par p, il est fini. Concernant le terme de droite, l'extension $H_{S,\infty}^T/K$ est non-ramifiée en dehors de l'ensemble fini Σ, composé des places de S et des places ramifiées dans K_∞/K. Le groupe $\mathcal{G}$ est donc un quotient de G_Σ : groupe de Galois de la pro-p-extension maximale de K qui est non-ramifiée en dehors des places de Σ. D'après la théorie du corps de classes G_Σ est de type fini donc $\mathcal{G}$ aussi. Le terme de droite est ainsi lui aussi fini et on en déduit que le terme médian, $(X_{S,\infty}^T)_G/p$, est fini. D'après le lemme de Nakayama (voir [**1**]), $X_{S,\infty}^T$ est de type fini sur Λ. □

Le résultat suivant réalise la descente de $X_{S,\infty}^T$ à $X_{S,n}^T$ dans une pro-p-extension de groupe de Galois p-valué. Il nous informe que le comportement asymptotique des G_n-coïnvariants du module à l'infini $X_{S,\infty}^T$ est proche de celui des $X_{S,n}^T$. Le module des G_n-coïnvariants d'un Λ-module M est noté M_{G_n} et s'obtient comme le quotient $M/I_{G_n}M$. C'est le plus grand quotient de M sur lequel G_n agit trivialement.

Théorème 2.1.5 **(descente dans une extension de Lie)**
Sous les hypothèses de ce paragraphe, on a les relations suivantes :

$$\#((X_{S,\infty}^T)_{G_n}/p^n) = \#(X_{S,n}^T/p^n)p^{\mathcal{O}(np^{n(d-1)})},$$

$$\dim_{\mathbb{F}_p}((X_{S,\infty}^T)_{G_n}/p) = \dim_{\mathbb{F}_p}(X_{S,n}^T/p) + \mathcal{O}(p^{n(d-1)}),$$

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,\infty}^T)_{G_n} = \mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}^T) + \mathcal{O}(p^{n(d-1)}).$$

Démonstration. — Cette preuve s'appuie sur une variante d'un résultat de Harris, qui sera démontrée dans la partie 2.2.1.
Dans un soucis de clareté, on va se concentrer uniquement sur la première équivalence et oublier les indices S et T.

La suite exacte d'inflation-restriction à coefficients dans $\mathbb{Z}/p^n\mathbb{Z}$, appliquée à la suite exacte

$$0 \to X_\infty \to \mathcal{G}_n \to G_n \to 0,$$

conduit à

$$H_2(G_n, \mathbb{Z}/p^n\mathbb{Z}) \to (X_\infty)_{G_n}/p^n \to \mathcal{G}_n^{ab}/p^n \to H_1(G_n, \mathbb{Z}/p^n\mathbb{Z}) \to 0.$$

Le corollaire 2.2.7, appliqué à $M = \mathbb{Z}_p$, nous indique que le cardinal de $H_i(G_n, \mathbb{Z}/p^n\mathbb{Z})$ évolue en $p^{\mathcal{O}(np^{n(d-1)})}$. On en déduit que

$$\#((X_\infty)_{G_n}/p^n) = \#(\mathcal{G}_n^{ab}/p^n)p^{\mathcal{O}(np^{n(d-1)})}.$$

Il reste donc à comparer $\mathcal{G}_n^{ab}$ à X_n. On s'inspire de ce qui est fait dans [**40**], théorème 13.13, pour $G \simeq \mathbb{Z}_p$ et $S = T = \emptyset$.
La situation galoisienne nous informe que X_n s'obtient comme le quotient de $\mathcal{G}_n^{ab}$ par son sous-groupe $\mathcal{D}_n$, engendré par l'inertie des places hors de S et la décomposition des places de T. Soit D_{v_n} l'un des sous-groupes d'inertie ou de décomposition non triviaux qui interviennent. Le groupe D_{v_n} est alors associé à une place v_n de K_n, située au dessus d'une place v de K qui n'est pas totalement décomposée dans K_∞/K. On a une injection de D_{v_n} dans G_n, qui implique que le nombre minimal de générateurs de D_{v_n} est inférieur à d dès que n assez grand pour que G_n soit p-saturé ([**26**], III 3.1.13). Le p-rang de $D_{v_n}^{ab}$ est donc inférieur à d. On en déduit que le p-rang de $\mathcal{D}_n$ est borné par d fois le cardinal de l'ensemble des places v_n que l'on considère. La place v n'étant pas totalement décomposée dans K_∞/K_n, le nombre de places v_n au dessus de v évolue en $\mathcal{O}(p^{n(d-1)})$ d'après le lemme :

Lemme 2.1.6 **(Hachimori, Sharifi, [11], lemme** 4.2**)**
Soit K_∞/K une extension du corps de nombres K de groupe de Galois un pro-p-groupe p-valué de type fini et soit K_n les étages de cette extension. Pour v une place de K qui n'est pas totalement décomposée dans K_∞/K, on note V_n l'ensemble des places de K_n divisant v. Alors

$$\#(V_n) = \mathcal{O}(p^{n(d-1)}).$$

Démonstration. — On fixe une place w de K_∞ au dessus de v. La place v n'étant pas totalement décomposée et G étant sans torsion, on en déduit que le sous-groupe de décomposition $G_v \subset G$, associé à $w|v$, est de dimension $d_v > 0$. On note $G_{v,n}$ la filtration de G_v induite par la filtration G_n de G. La proposition 1.1.8 nous informe que, pour n assez grand, il existe des constantes C et C' telles que

$$(G : G_n) = Cp^{nd},$$
$$(G_v : G_{v,n}) = C'p^{nd_v}.$$

Mais

$$\#(V_n) = (G/G_n : G_v/G_{v,n}) = \frac{C}{C'}p^{n(d-d_v)}.$$

□

Finalement, comme les places v à considérer sont en nombre fini, $\#(\mathcal{D}_n/p^n) = p^{\mathcal{O}(np^{n(d-1)})}$ et

$$\#(\mathcal{G}_n^{ab}/p^n) = \#(X_n/p^n)p^{\mathcal{O}(np^{n(d-1)})}.$$

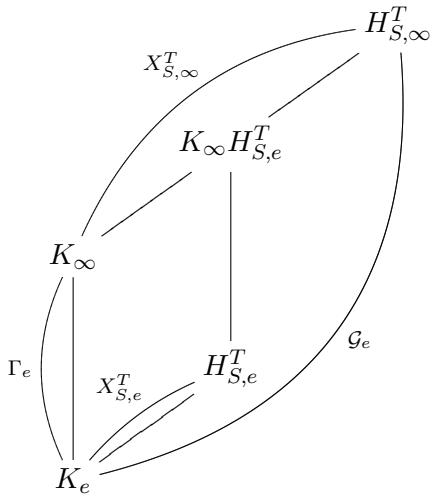
La démonstration des deux autres égalités est similaire. □

On clos ce paragraphe en donnant les théorèmes de descente pour les $\mathbb{Z}_p$-extensions. Dans ce cadre restreint, on peut retrouver les p-groupes $X_{S,n}^T$ directement comme quotient du module d'Iwasawa $X_{S,\infty}^T$. Les résultats sont donc plus précis que ceux démontrés dans le cas général, qui se contentent de comparer des rangs. La descente dans les $\mathbb{Z}_p$-extensions consiste en deux théorèmes, suivant que la $\mathbb{Z}_p$-extension K_∞/K est elle même S-ramifiée et T-décomposée ou non.
On commence par traiter le cas où la $\mathbb{Z}_p$-extension K_∞/K n'est pas S-ramifiée et T-décomposée, appelé "cas général". On aura besoin de quelques notations. On appelle Γ le groupe de Galois de K_∞/K, isomorphe à $\mathbb{Z}_p$, et on en fixe un générateur topologique γ. Pour tout entier naturel n, on pose $\omega_n = \gamma^{p^n} - 1 \in \Lambda$ et $\omega_{m,n} = \frac{\omega_m}{\omega_n}$ pour $m \geqslant n$. Pour tout n, le sous-groupe Γ_n est engendré topologiquement par γ^{p^n} et les Γ_n-coïnvariants d'un Λ-module M sont alors donnés par $M_{\Gamma_n} = M/\omega_n M$.
Notons R l'ensemble des places de K ramifiées dans K_∞/K et T^{fd} l'ensemble des places de T qui sont finiment décomposées dans K_∞/K. Dans le cas général, l'union de l'ensemble des places de R qui ne sont pas contenues dans S et de T^{fd} forme un ensemble fini non vide. On appelle e le plus petit entier tel que le comportement de ces places se stabilise à partir de K_e, c'est à dire tel que les places de R non contenues dans S soient totalement ramifiées et celles de T^{fd} soient non décomposées dans K_∞/K_e. Notons P_e l'ensemble fini des places de K_e dont il est question.
Le théorème suivant est classique dans le cas $S = T = \emptyset$ (voir par exemple [**40**], lemme 13.18). Nous en rappelons néanmoins la démonstration, en insistant sur le fait que le défaut de descente Y_e n'est pas forcément un sous-Λ-module de $X_{S,\infty}^T$.

***Théorème 2.1.7* (descente dans le cas général).** — *Dans le cas général, il existe un sous-$\mathbb{Z}_p$-module noethérien Y_e de $X_{S,\infty}^T$ tel que la somme $\omega_e X_{S,\infty}^T + Y_e$ soit un sous-Λ-module de $X_{S,\infty}^T$ et tel que, pour tout $n \geqslant e$, on ait :*

$$X_{S,n}^T \simeq X_{S,\infty}^T / \left(\omega_n X_{S,\infty}^T + \omega_{n,e} Y_e\right).$$

Démonstration. — On est dans la situation suivante :



Par sa définition en tant que p-extension abélienne S-ramifiée et T-décomposée maximale de K_e, le corps $H^T_{S,e}$ est la sous-extension de $H^T_{S,\infty}/K_e$ fixée par les commutateurs de $\mathcal{G}_e$ et par les sous-groupes $D_{v^x_\infty}$ que l'on va maintenant définir. Pour chaque place $v \in P_e$, choisissons une place v_∞ de $H^T_{S,\infty}$ qui soit au-dessus, puis notons D_{v_∞} son sous-groupe de décomposition dans $\mathcal{G}_e$ si v_∞ est au-dessus de T^{fd} et d'inertie sinon. Par choix de e, chacun de ces groupes est isomorphe à Γ_e et d'intersection triviale avec $X^T_{S,\infty}$. On fixe l'une de ces places v°_∞, qui permet d'écrire $\mathcal{G}_e$ comme le produit semi-direct

$$\mathcal{G}_e = X^T_{S,\infty} \rtimes D_{v^\circ_\infty}.$$

Fixons un générateur $\gamma_\circ$ de $D_{v^\circ_\infty}$ qui relève γ^{p^e} dans $\mathcal{G}_e$. Chacun des D_{v_∞} possède un générateur topologique de la forme $\gamma_\circ x_{v_\infty}$, avec $x_{v_\infty} \in X^T_{S,\infty}$ et $x_{v^\circ_\infty} = 1$. Toute autre place au dessus de v est conjuguée à v_∞ par un élément $x \in X^T_{S,\infty}$, on la note v^x_∞. Le groupe $D_{v^x_\infty}$ est alors topologiquement engendré par le conjugugué $x(\gamma_\circ x_{v_\infty})x^{-1} = x\gamma_\circ x^{-1} x_{v_\infty} = x^{(1-\gamma^{p^e})}\gamma_\circ x_{v_\infty}$ par commutativité de $X^T_{S,\infty}$, l'action de γ sur $X^T_{S,\infty}$ se faisant par relèvement et conjugaison.
Déterminons les commutateurs $[\mathcal{G}_e, \mathcal{G}_e]$ comme dans **[40]**, lemme 13.14. Un calcul permet de voir que si αx et βy sont deux éléments de $\mathcal{G}_e$, avec $x, y \in X^T_{S,\infty}$ et $\alpha, \beta \in D_{v^\circ_\infty}$, alors

$$[\alpha x, \beta y] = (x^\alpha)^{1-\beta}(y^\beta)^{\alpha-1}.$$

Prendre $\beta = 1$ et $\alpha = \gamma_\circ$ dans cette dernière égalité prouve que

$$(X^T_{S,\infty})^{\gamma^{p^e}-1} \subset [\mathcal{G}_e, \mathcal{G}_e].$$

Si on écrit α sous la forme $\alpha = \gamma_\circ^a$ avec $a \in \mathbb{Z}_p$, on obtient

$$\alpha - 1 = (\gamma_\circ - 1 + 1)^a - 1 = \left(\sum_{n=0}^{\infty} \binom{a}{n} (\gamma_\circ - 1)^n \right) - 1 = \sum_{n=1}^{\infty} \binom{a}{n} (\gamma_\circ - 1)^n.$$

On en déduit que $(y^\beta)^{\alpha-1} \in (X_{S,\infty}^T)^{\gamma^{p^e}-1}$. Le même calcul montre que $(x^\alpha)^{1-\beta} \in (X_{S,\infty}^T)^{\gamma^{p^e}-1}$. Ainsi, $[\alpha x, \beta y] \in (X_{S,\infty}^T)^{\gamma^{p^e}-1}$ ce qui prouve l'inclusion réciproque

$$[\mathcal{G}_e, \mathcal{G}_e] \subset (X_{S,\infty}^T)^{\gamma^{p^e}-1}.$$

Les commutateurs de $\mathcal{G}_e$ sont donc donnés par $(X_{S,\infty}^T)^{\gamma^{p^e}-1}$.
Si on quotiente $\mathcal{G}_e$ par ses commutateur et les sous-goupes $D_{v_\infty^x}$ pour retrouver $X_{S,e}^T$, il reste $X_{S,\infty}^T/(X_{S,\infty}^T)^{\gamma^{p^e}-1} Y_e$, avec Y_e le sous-groupe de $X_{S,\infty}^T$ engendré par les x_{v_∞}. C'est le résultat anoncé pour $n = e$ en passant en notations additives.

Ce point acquis, le passage de K_e à K_n pour $n \geqslant e$ se fait en remplaçant γ^{p^e} par γ^{p^n} au départ. On a alors

$$[\mathcal{G}_n, \mathcal{G}_n] = \omega_n X_{S,\infty}^T.$$

Aussi, le relévement $\gamma_\circ$ devient $\gamma_\circ^{p^{n-e}}$ et les générateurs $\gamma_\circ x_{v_\infty}$ deviennent

$$\begin{array}{rcl} (\gamma_\circ x_{v_\infty})^{p^{n-e}} & = & \gamma_\circ^{p^{n-e}} (\gamma_\circ^{-(p^{n-e}-1)} x_{v_\infty} \gamma_\circ^{(p^{n-e}-1)}) \cdots (\gamma_\circ^{-1} x_{v_\infty} \gamma_\circ) x_{v_\infty} \\ & = & \gamma_\circ^{p^{n-e}} (x_{v_\infty})^{\omega_{n,e}}. \end{array}.$$

On en déduit que $Y_n = \omega_{n,e} Y_e$ ce qui donne, comme annoncé :

$$X_{S,n}^T \simeq X_{S,\infty}^T / \left(\omega_n X_{S,\infty}^T + \omega_{n,e} Y_e \right).$$

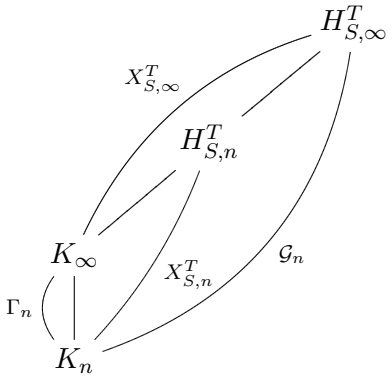
□

Le cas où K_∞/K est S-ramifiée et T-décomposée est appelé "cas spécial". La descente est alors plus simple et s'exprime de la façon suivante.

***Théorème 2.1.8* (descente dans le cas spécial).** — *Dans le cas spécial, on a pour tout entier n :*

$$X_{S,n}^T \simeq X_{S,\infty}^T / \omega_n X_{S,\infty}^T \oplus \Gamma_n.$$

Démonstration. — Dans le cas spécial, l'extension $H_{S,n}^T$ contient K_∞, ce qui donne la situation galoisienne :



On a ainsi $\mathcal{G}_n \simeq X^T_{S,\infty} \rtimes \Gamma_n$ et le corps $H^T_{S,n}$ s'obtient comme celui fixé par les commutateurs $[\mathcal{G}_n, \mathcal{G}_n]$. Ces commutateurs ont été calculés dans la démonstration précédente et sont donnés par $\omega_n X^T_{S,\infty}$, d'où le résultat. □

2.2. Formules asymptotiques dans les extensions de Lie p-adiques

Ce paragraphe à pour but la démonstration du théorème 2.2.8, qui donne des formules asymptotiques portant sur les p-groupes des classes généralisés des étages d'une extension de corps de nombres de groupe de Galois un pro-p-groupe p-valué de type fini. Le travail de descente à déjà été effectué dans la section précédente et il reste à estimer les coïnvariants du module d'Iwasawa correspondant.

2.2.1. Un théorème de Harris. — Cette partie est purement algébrique et a pour objectif la démonstration du théorème 2.2.1 et de ses corollaires, qui sont des variantes d'un théorème de Harris. Ces résultats forment la clef de voûte des calculs menés dans la suite. Ils permettront surtout de négliger les quantités provenant de modules pseudo-nuls, et ainsi d'appliquer les théorèmes de structure de la section 1.3.2.3 au module d'Iwasawa $X^T_{S,\infty}$.
Soit G un pro-p-groupe p-valué de type fini et G_n sa filtration entière. Rappelons que Ω désigne l'algèbre complète de G sur $\mathbb{F}_p$.

Théorème 2.2.1 **(Harris, [13], théorème** 1.10**).** — *Si M est un Ω-module de type fini. Alors*

$$\dim_{\mathbb{F}_p}(M_{G_n}) = \mathrm{rk}_\Omega(M)(G : G_n) + \mathcal{O}(p^{n(d-1)}).$$

Supposons dans un premier temps que le module M est de torsion. Il existe alors des éléments non nuls $f_1, ..., f_s$ de Ω donnant une surjection

$$\bigoplus_{i=1}^{s} \Omega/\Omega f_i \twoheadrightarrow M.$$

On peut donc se ramener à un module de la forme $M = \Omega/\Omega f$ et démontrer que le p-rang de ses coïnvariants, $\dim_{\mathbb{F}_p}(\Omega/(I_{G_n} + \Omega f))$, évolue en $\mathcal{O}(p^{n(d-1)})$.

Pour tout entier naturel n, les idéaux I_{G_n} et I_G^n sont stables par f. La multiplication par f induit donc des endomorphismes f_n de $\Omega_{G_n} = \Omega/I_{G_n}$ et $\overline{f}_n$ de $\mathrm{Gr}(\Omega)/\mathrm{Gr}(I_{G_n})$. On va montrer que la quantité $\dim_{\mathbb{F}_p}(\mathrm{coker}(f_n))$, que l'on cherche à estimer, est inférieure à $\dim_{\mathbb{F}_p}(\mathrm{coker}(\overline{f}_n))$. Pour cela, on démontre le lemme suivant qui compare les idéaux I_G^n et I_{G_n}.

Lemme 2.2.2. — *Pour tout $n \in \mathbb{N}$ et pour tout $k \geqslant dp^n$, on a*

$$I_G^k = (I_G^k \cap I_{G_n}) + I_G^{k+1}.$$

Démonstration. — Fixons $g_1, \cdots, g_d$ un système minimal de générateurs de G. L'idéal I_G est alors engendré par les éléments $g_1 - 1, \cdots, g_d - 1$.
Comme le quotient I_G^k/I_G^{k+1} est commutatif pour tout k, il est engendré par tous les produits de k facteurs parmis les éléments $\overline{g_1 - 1}, \cdots, \overline{g_d - 1}$. Si k est supérieur à dp^n, on est assuré de retrouver au moins p^n fois le même facteur dans chacun des générateurs, qui sont donc de la forme

$$\overline{(g-1)^{p^n} x} = \overline{(g^{p^n} - 1)x} \in (I_G^k \cap I_{G_n})/I_G^{k+1},$$

puisqu'on est en caractéristique p et que $g^{p^n} \in G_n$. □

Ce lemme étant démontré, on en tire tout d'abord :

$$\begin{aligned} \mathrm{coker}(\overline{f}_n) &= \bigoplus_{\substack{k=0 \\ dp^n}}^{\infty} I_G^k/((I_G^k \cap I_{G_n}) + I_G^{k+1} + fI_G^k) \\ &= \bigoplus_{k=0}^{\infty} I_G^k/((I_G^k \cap I_{G_n}) + I_G^{k+1} + fI_G^k). \end{aligned}$$

En découpant le conoyau de f_n selon la filtration I_G^k, on a de même :

$$\begin{aligned} \dim_{\mathbb{F}_p}(\mathrm{coker}(f_n)) &= \bigoplus_{\substack{k=0 \\ dp^n}}^{\infty} \dim_{\mathbb{F}_p}\left(I_G^k/(I_G^k \cap (I_{G_n} + f\Omega) + I_G^{k+1})\right) \\ &= \bigoplus_{k=0}^{\infty} \dim_{\mathbb{F}_p}\left(I_G^k/(I_G^k \cap (I_{G_n} + f\Omega) + I_G^{k+1})\right). \end{aligned}$$

L'inclusion $(I_G^k \cap I_{G_n}) + fI_G^k \subset I_G^k \cap (I_{G_n} + f\Omega)$ nous donne immédiatement l'inégalité

$$\dim_{\mathbb{F}_p}(\mathrm{coker}(f_n)) \leqslant \dim_{\mathbb{F}_p}(\mathrm{coker}(\overline{f}_n)).$$

On va désormais calculer la quantité $\dim_{\mathbb{F}_p}(\mathrm{coker}(\overline{f}_n))$ en utilisant l'identification de $\mathrm{Gr}(\Omega)$ avec une algèbre de polynômes (proposition 1.3.6).
Le calcul précédent montre que

$$\mathrm{coker}(\overline{f}_n) = \mathrm{Gr}(\Omega)/(\mathrm{Gr}(I_{G_n}) + \mathrm{Gr}(I_G^{dp^n}) + f\mathrm{Gr}(\Omega)).$$

En terme de polynômes, l'idéal $\mathrm{Gr}(I_G^{dp^n})$ correspond à l'idéal engendré par les polynômes homogènes de degré dp^n. On notera $\mathcal{P}_{dp^n}$ l'ensemble des polynômes homogènes de degré dp^n et $< \mathcal{P}_{dp^n} >$ l'idéal engendré par cet ensemble.
On a ainsi une surjection :

$$\mathbb{F}_p[X_1, ..., X_d]/(< \mathcal{P}_{dp^n} > +(f)) \twoheadrightarrow \mathrm{coker}(\overline{f}_n).$$

Le théorème pour un module de Ω-torsion M découlera d'une estimation de la $\mathbb{F}_p$-dimension du quotient de l'algèbre de polynômes ci-dessus, via le résultat suivant :

Théorème 2.2.3 **(Polynôme de Hilbert, [14] Chapitre I, théorème 7.5)**
Soit g un polynôme homogène de $\mathbb{F}_p[X_1, ..., X_d]$. Il existe un polynôme χ de degré $d-2$ tel que la dimension sur $\mathbb{F}_p$ de $\mathcal{P}_k/(\mathcal{P}_k \cap (g))$ est donnée, pour k assez grand, par $\chi(k)$. Le polynôme χ est appelé polynôme de Hilbert de $\mathbb{F}_p[X_1, ..., X_d]/(g)$.

On va se ramener à f homogène.
Remarquons tout d'abord que $\mathbb{F}_p[X_1, ..., X_d]/\big(< \mathcal{P}_{dp^n} > +(f)\big)$ est isomorphe à $\big(\mathbb{F}_p[X_1, ..., X_d]/ < \mathcal{P}_{dp^n} > \big)/\big((f)/ < \mathcal{P}_{dp^n} > \cap(f)\big)$.
Si g désigne la somme des monômes de plus haut degré de f, l'application $\mathbb{F}_p$-linéaire $fh \mapsto gh$ induit une surjection

$$(f)/\big(< \mathcal{P}_{dp^n} > \cap(f)\big) \twoheadrightarrow (g)/\big(< \mathcal{P}_{dp^n} > \cap(g)\big).$$

Aux vues de la remarque qui précède, cette surjection entraîne :

$$\dim_{\mathbb{F}_p}\big(\mathbb{F}_p[X_1, ..., X_d]/\big(< \mathcal{P}_{dp^n} > +(f)\big)\big) \leqslant \dim_{\mathbb{F}_p}\big(\mathbb{F}_p[X_1, ..., X_d]/\big(< \mathcal{P}_{dp^n} > +(g)\big)\big).$$

Il suffit donc de calculer la dimension de $\mathbb{F}_p[X_1, ..., X_d]/\big(< \mathcal{P}_{dp^n} > +(g)\big)$, où g est maintenant un polynôme homogène.

Selon le théorème 2.2.3, la dimension de chaque graduation $\mathcal{P}_k/(\mathcal{P}_k \cap (g))$ de l'algèbre $\mathbb{F}_p[X_1, ..., X_d]/(g)$ est donnée, pour $k \geqslant l$ assez grand, par le polynôme de Hilbert $\chi(k) = \chi_0 + \chi_1 k + ... + \chi_{d-2}k^{d-2}$. La dimension du quotient $\mathbb{F}_p[X_1, ..., X_d]/\big(< \mathcal{P}_{dp^n} > +(g)\big)$ est donc égale, à une constante près, à

$$\sum_{k=l}^{dp^n-1} \chi(k) = \sum_{k=l}^{dp^n-1} \sum_{i=0}^{d-2} \chi_i k^i.$$

A i fixé, la somme sur les k devient

$$\begin{aligned}\sum_{k=l}^{dp^n-1} \chi_i k^i &\leqslant \chi_i \sum_{k=l}^{dp^n-1} (dp^n-1)^i \\ &= \chi_i (dp^n-1)^i (dp^n-l) \\ &= \mathcal{O}(p^{n(i+1)}) \\ &= \mathcal{O}(p^{n(d-1)}).\end{aligned}$$

Revenons maintenant au cas général, dans lequel le Ω-module M n'est plus supposé de torsion.
On commence par isoler la partie de torsion de M grâce à la suite exacte ci-dessous, où $\overline{M}$ désigne le quotient $M/\mathrm{tor}_\Omega(M)$ de M par son sous-module de torsion :

$$0 \to \mathrm{tor}_\Omega(M) \to M \to \overline{M} \to 0.$$

Le passage aux G_n-coïnvariants conduit à

$$(\mathrm{tor}_\Omega(M))_{G_n} \to M_{G_n} \to \overline{M}_{G_n} \to 0.$$

D'après ce qui précède, le premier terme est asymptotiquement négligeable et on est ramené au calcul des coïnvariants du Ω-module sans torsion $\overline{M}$. On utilise le lemme suivant pour comparer un module sans torsion à un module libre.

Lemme 2.2.4. — *Soit M un Λ-module de type fini, sans torsion, et de rang ρ. Il existe des suites exactes*

$$0 \to \Lambda^\rho \to M \to T_1 \to 0$$

et

$$0 \to M \to \Lambda^\rho \to T_2 \to 0$$

où T_1 et T_2 sont de Λ-torsion.
Le même résultat est valable si on remplace Λ par Ω.

Démonstration. — Soit $m_1, ..., m_r$ un système générateur de M et soit $F = \mathrm{Frac}(\Lambda)$. Le F-espace vectoriel $F \otimes_\Lambda M$ est de dimension ρ et l'on peut ordonner les m_i de telle sorte que $(1 \otimes m_1, ..., 1 \otimes m_\rho)$ forme une base de $F \otimes_\Lambda M$.

La première suite exacte s'obtient alors en envoyant le i-ième vecteur de base de Λ^ρ sur m_i. Cette application est injective par choix de l'ordre des m_i et on en déduit que le conoyau est de torsion par un calcul de rang.

En ce qui concerne la deuxième suite, pour tout $\rho < i \leqslant r$ et $1 \leqslant k \leqslant \rho$, on obtient l'existence de coefficients $\alpha_{i,k}$, $\beta_{i,k} \in \Lambda$ tels que

$$m_i = \sum_{k=1}^{\rho} \alpha_{i,k} \beta_{i,k}^{-1} m_k.$$

On va montrer qu'il existe des dénominateurs communs β_k et des $\gamma_{i,k}$ de Λ tels que $m_i = \sum_{k=1}^{\rho} \gamma_{i,k}\beta_k^{-1} m_k$. Le module M sera alors contenu dans le sous-Λ-module libre de $F \otimes_\Lambda M$ engendré par les $\beta_k^{-1} \otimes m_k$. Le conoyau de cette application est de Λ-torsion donc le noyau aussi par un calcul de rang (il est donc nul car M est sans torsion).
L'existence de ces éléments est une conséquence du lemme suivant.

Lemme 2.2.5. — *Soit A un anneau noethérien à droite et intègre. Soit $a_1, ..., a_n$ des éléments non nuls de A. Alors $a_1A \cap ... \cap a_nA \neq 0$.*

Démonstration. — Il suffit de le démontrer pour deux éléments a et b de A. En effet, supposons que $a_1A \cap ... \cap a_{n-1}A \neq 0$. Un élément non nul c de cette intersection fournit un élément non-nul $d \in cA \cap a_nA \subset a_1A \cap ... \cap a_nA$. On obtient donc le cas général de n éléments par récurrence.

Supposons que $aA \cap bA = 0$. Soient $x_0, ..., x_n$ des éléments de aA tels que

$$x_0 + bx_1 + ... + b^n x_n = 0.$$

On a $x_0 \in aA \cap bA = 0$ et, en utilisant l'intégrité de A, on en déduit de proche en proche que tous les x_i sont nuls.
Ceci signifie que la somme d'idéaux $aA + baA + b^2aA + ...$ est directe, ce qui contredit la noethérianité de A. □

Appliqué aux éléments $\beta_{\rho+1,k}, ..., \beta_{r,k}$ de Λ, le lemme 2.2.5 nous informe qu'il existe $\gamma'_{\rho+1,k}, ..., \gamma'_{r,k} \in \Lambda$ tels que

$$\beta_{\rho+1,k}\gamma'_{\rho+1,k} = ... = \beta_{r,k}\gamma'_{r,k} := \beta_k.$$

On obtient les éléments cherchés en posant $\gamma_{i,k} = \alpha_{i,k}\gamma'_{i,k}$. □

Les suites exactes du lemme 2.2.4 appliquées au Ω-module $\overline{M}$ et passées aux G_n-coïnvariants donnent

$$\mathbb{F}_p[G/G_n]^{\mathrm{rk}_\Omega(\overline{M})} \to \overline{M}_{G_n} \to (T_1)_{G_n} \to 0$$

et

$$\overline{M}_{G_n} \to \mathbb{F}_p[G/G_n]^{\mathrm{rk}_\Omega(\overline{M})} \to (T_2)_{G_n} \to 0.$$

La $\mathbb{F}_p$-dimension des termes de droite est asymptotiquement négligeable car T_1 et T_2 sont de Ω-torsion. On obtient donc une majoration et une minoration de la quantité $\dim_{\mathbb{F}_p}(\overline{M}_{G_n})$ par $\dim_{\mathbb{F}_p}(\mathbb{F}_p[G/G_n]^{\mathrm{rk}_\Omega(\overline{M})})$ à $\mathcal{O}(p^{n(d-1)})$ près, d'où le résultat annoncé :

$$\dim_{\mathbb{F}_p}(M_{G_n}) = \mathrm{rk}_\Omega(M)(G : G_n) + \mathcal{O}(p^{n(d-1)}).$$

On termine ce paragraphe par deux corollaires au théorème 2.2.1. Ce sont des extensions aux groupes d'homologie supérieurs, dont on rappelle la définition. Pour i et n des entiers naturels, les groupes d'homologie de G_n à coefficients dans un Λ-module de type fini M sont définis par

$$H_i(G_n, M) = \mathrm{Tor}_i^{\Lambda(G_n)}(\mathbb{Z}_p, M),$$

où $\mathrm{Tor}_i^{\Lambda(G_n)}(-,-)$ désignent les dérivés du bifoncteur $-\hat{\otimes}_{\Lambda(G_n)}-$.
Lorsque M est aussi muni d'une structure de Ω-module, le théorème 2.2.1 donne des renseignements sur $H_0(G_n, M) = M_{G_n}$. En effet, on a dans ce cas $H_i(G_n, M) = \mathrm{Tor}_i^{\Lambda(G_n)}(\mathbb{Z}_p, M) \simeq \mathrm{Tor}_i^{\Omega(G_n)}(\mathbb{F}_p, M)$ (voir **[35]**, lemme 6.3.5). On va voir que, pour un Ω-module de torsion, le même résultat est valable pour tout $i \in \mathbb{N}$.

Corollaire 2.2.6. — *Soit M un Ω-module de type fini et de torsion. Pour tout $i \geqslant 0$, on a*

$$\dim_{\mathbb{F}_p}(H_i(G_n, M)) = \mathcal{O}(p^{n(d-1)}).$$

Démonstration. — On procède par récurrence sur i, le cas $i = 0$ étant donné par le théorème 2.2.1.

Le Ω-module M étant de type fini et de torsion, il existe un Ω-module de torsion A et des éléments non nuls $f_1, \cdots, f_r \in \Omega$ prenant place dans la suite exacte :

$$0 \to A \to \bigoplus_j \Omega/f_j \to M \to 0.$$

Cette suite conduit à l'encadrement

$$H_i(G_n, \bigoplus_j \Omega/f_j) \to H_i(G_n, M) \to H_{i-1}(G_n, A).$$

L'hypothèse de récurrence appliquée à A permet de se ramener au cas $M = \Omega/f$ car elle entraîne que $\dim_{\mathbb{F}_p}(H_{i-1}(G_n, A)) = \mathcal{O}(p^{n(d-1)})$.

On calcule les groupes d'homologie de Ω/f à partir de sa résolution $\Omega(G_n)$-libre :

$$0 \to \Omega \xrightarrow{f} \Omega \to \Omega/f \to 0.$$

On obtient immédiatement $H_i(G_n, \Omega/f) = 0$ pour $i > 1$, ainsi que les renseignements suivants sur le H_1 :

$$\begin{aligned} \dim_{\mathbb{F}_p}(H_1(G_n, \Omega/f)) &= \dim_{\mathbb{F}_p}(\ker(\Omega_{G_n} \xrightarrow{f} \Omega_{G_n})) \\ &= \dim_{\mathbb{F}_p}(\mathrm{coker}(\Omega_{G_n} \xrightarrow{f} \Omega_{G_n})) \\ &= \dim_{\mathbb{F}_p}((\Omega/f)_{G_n}) \\ &= \mathcal{O}(p^{n(d-1)}), \end{aligned}$$

la dernière égalité provenant du théorème 2.2.1. □

Corollaire 2.2.7. — *Soit M un Λ-module de type fini tel que M/p est un Ω-module de torsion. Alors, pour tout $i \geqslant 0$,*

$$\#(H_i(G_n, M/p^n)) = p^{\mathcal{O}(np^{n(d-1)})}.$$

Démonstration. — On va découper M/p^nM selon les $p^kM/p^{k+1}M$.
Le corollaire 2.2.6 fournit des constantes C_k, indépendantes de n, telles que $\#H_i(G_n, p^kM/p^{k+1}M) \leqslant p^{C_kp^{n(d-1)}}$.

Pour $k < n$, la G_n-homologie de la suite exacte

$$0 \to p^{k+1}M/p^nM \to p^kM/p^nM \to p^kM/p^{k+1}M \to 0$$

entraîne les inégalités

$$\#H_i(G_n, p^kM/p^nM) \leqslant \#H_i(G_n, p^{k+1}M/p^nM)p^{C_kp^{n(d-1)}}.$$

Elles conduisent à

$$\#H_i(G_n, M/p^nM) \leqslant p^{(C_1+\cdots+C_n)p^{n(d-1)}}.$$

Pour k assez grand, le module p^kM est sans p-torsion par noethérianité. Ainsi $p^kM/p^{k+1}M \simeq p^{k+1}M/p^{k+2}M$ et les constantes C_k sont majorées par une constante C' indépendante de k. On en tire

$$\#H_i(G_n, M/p^nM) \leqslant p^{C'np^{n(d-1)}}.$$

□

2.2.2. Le théorème principal. — On se donne une extension de Lie p-adique K_∞/K du corps de nombres K, dont le groupe de Galois est un pro-p-groupe p-valué de type fini G et dans laquelle seul un nombre fini de places de K se ramifient. On peut définir ses étages K_n comme en 2.1.3. Le théorème de descente (théorème 2.1.5) relie les p-groupes des T-classes S-infinitésimales des étages $X_{S,n}^T$ aux G_n-coïnvariants du module d'Iwasawa à l'infini $X_{S,\infty}^T$. L'obtention de formules asymptotiques pour les groupes des classes généralisés sera conséquente à une étude algébrique approfondie du Λ-module $X_{S,\infty}^T$, initiée dans la section précédente.
Cette partie utilise la plupart du matériel mis en place jusqu'à présent. Elle a pour but la démonstration du théorème :

Théorème 2.2.8. — *Soit ρ_S^T, μ_S^T et r_S^T les invariants d'Iwasawa du module $X_{S,\infty}^T$. On a les trois identités :*

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}^T) = \rho_S^T(G : G_n) + \mathcal{O}(p^{n(d-1)}),$$

$$\dim_{\mathbb{F}_p}(X_{S,n}^T/p) = (\rho_S^T + r_S^T)(G : G_n) + \mathcal{O}(p^{n(d-1)})$$

et

$$\#(X_{S,n}^T/p^n) = p^{(\rho_S^T n + \mu_S^T)(G:G_n) + \mathcal{O}(np^{n(d-1)})}.$$

Les formules qui constituent ce théorème font intervenir les invariants d'Iwasawa du module à l'infini associé et peuvent être comparées au théorème d'Iwasawa pour les p-groupes des classes le long d'une $\mathbb{Z}_p$-extension (théorème 2.0.16). Des généralisations de ce résultat historique ont déjà été mises en lumière par Cuoco et Monsky pour les $\mathbb{Z}_p$-extensions multiples **[4]**, et par Jaulent pour les p-groupes des classes généralisés le long d'une $\mathbb{Z}_p$-extension **[22]**.

Nous démontrerons les trois points du théorème 2.2.8 indépendemment et dans l'ordre de l'énoncé.

• Le $\mathbb{Z}_p$-rang de $X_{S,n}^T$ est relié, par le théorème de descente (2.1.5), à celui de $(X_{S,\infty}^T)_{G_n}$. Le comportement asymptotique de ce dernier est donné directement par le théorème 1.10 de **[13]**, qui affirme que

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,\infty}^T)_{G_n} = \rho_S^T(G : G_n) + \mathcal{O}(p^{n(d-1)}).$$

• Toujours d'après le théorème de descente, la $\mathbb{F}_p$-dimension de $X_{S,n}^T/p$ est asymptotiquement égale à celle de $(X_{S,\infty}^T)_{G_n}/p$.
Le théorème 2.2.1 appliqué à $X_{S,\infty}^T/p$ donne l'estimation

$$\dim_{\mathbb{F}_p}((X_{S,\infty}^T)_{G_n}/p) = \mathrm{rk}_\Omega(X_{S,\infty}^T/p)(G : G_n) + \mathcal{O}(p^{n(d-1)}).$$

Le corollaire 1.10 de **[15]** relie la valeur de $\mathrm{rk}_\Omega(X_{S,\infty}^T/p)$ aux invariants d'Iwasawa de $X_{S,\infty}^T$ de la façon suivante :

$$\mathrm{rk}_\Omega(X_{S,\infty}^T/p) = \mathrm{rk}_\Omega(X_{S,\infty}^T[p]) + \mathrm{rk}_\Lambda(X_{S,\infty}^T) = r_S^T + \rho_S^T.$$

La combinaison de ces deux résultats donne la deuxième formule du théorème 2.2.8.

• La démonstration de la troisième formule est plus délicate. La stratégie de départ est la même, à savoir se ramener au calcul du cardinal de $(X_{S,\infty}^T)_{G_n}/p^n$ via le théorème de descente. Pour calculer cette quantité, on va utiliser les résultats de structure modulo pseudo-isomorphisme pour le Λ-module $X_{S,\infty}^T$. Notons que les arguments à suivre fournissent également une preuve de la deuxième formule du théorème 2.2.8.
On commence par remarquer que les calculs peuvent être menés modulo pseudo-isomorphisme :

Proposition 2.2.9. — *Soient M et N deux Λ-modules de type fini pseudo-isomorphes. Alors*

$$\#(M_{G_n}/p^n) = \#(N_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})}.$$

Démonstration. — Soit

$$0 \to A \to M \xrightarrow{\varphi} N \to B \to 0$$

la suite exacte donnée par le pseudo-isomorphisme et $Z = \mathrm{Im}(\varphi)$. On en déduit par passage au quotient les suites exactes

$$A_{G_n}/p^n \to M_{G_n}/p^n \to Z_{G_n}/p^n \to 0$$

et

$$B[p^n] \longrightarrow Z/p^n \xrightarrow{\quad\theta\quad} N/p^n \longrightarrow B/p^n \longrightarrow 0.$$

$$\mathrm{Im}(\theta)$$

Cette dernière se découpe pour donner

$$B[p^n]_{G_n} \to Z_{G_n}/p^n \to \mathrm{Im}(\theta)_{G_n} \to 0$$

et

$$H_1(G_n, B/p^n) \to \mathrm{Im}(\theta)_{G_n} \to N_{G_n}/p^n \to B_{G_n}/p^n \to 0.$$

Par noethérianité, la suite de sous-modules $(B[p^n])_n$ se stabilise en $B[p^\alpha]$ pour un entier α assez grand. On en déduit que pour $n \geqslant \alpha$, on a $B[p^n]_{G_n} = B[p^\alpha]_{G_n}/p^n$. Le lemme 1.3.13 permet d'appliquer le corollaire 2.2.7 à tout module pseudo-nul, en particulier à A, B et $B[p^\alpha]$. Ceci fournit successivement :

$$\begin{aligned} \#(M_{G_n}/p^n) &= \#(Z_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})} \\ &= \#(\mathrm{Im}(\theta)_{G_n})p^{\mathcal{O}(np^{n(d-1)})} \\ &= \#(N_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})}. \end{aligned}$$

□

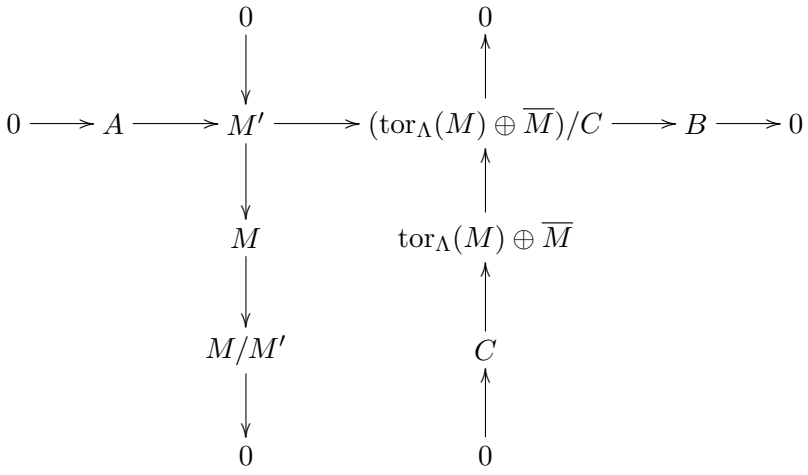
Il est maintenant possible d'utiliser les théorèmes de structure modulo pseudo-isomorphisme. Le théorème 1.3.15 permet un dévissage en étudiant un Λ-module de torsion d'une part et un sans torsion d'autre part. Ce fait est une traduction de la proposition suivante :

Proposition 2.2.10. — *Soit M un Λ-module de type fini. On note $\overline{M}$ le quotient de M par son sous-module de Λ-torsion. Alors :*

$$\#(M_{G_n}/p^n) = \#(\mathrm{tor}_\Lambda(M)_{G_n}/p^n)\#(\overline{M}_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})}.$$

Démonstration. — L'isomorphisme dans la catégorie quotient qui apparaît dans le théorème 1.3.15 signifie qu'il existe des modules pseudo-nuls A, B,

C et un sous-module M' de M, avec M/M' pseudo-nul, prenant place dans le diagramme suivant (voir [**8**], chapitre III) :



On a donc des pseudo-isomorphismes entre M' et M, entre M' et $(\mathrm{tor}_\Lambda(M)\oplus \overline{M})/C$ et entre $\mathrm{tor}_\Lambda(M)\oplus\overline{M}$ et $(\mathrm{tor}_\Lambda(M)\oplus\overline{M})/C$.

On applique alors la proposition 2.2.9 pour obtenir :

$$\begin{aligned}
\#(M_{G_n}/p^n) &= \#(M'_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})} \\
&= \#((\mathrm{tor}_\Lambda(M)\oplus\overline{M}/C)_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})} \\
&= \#((\mathrm{tor}_\Lambda(M)\oplus\overline{M})_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})} \\
&= \#(\mathrm{tor}_\Lambda(M)_{G_n}/p^n)\#(\overline{M}_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})}.
\end{aligned}$$

□

On détermine, grâce au lemme suivant, l'impact de la partie de torsion $\#(\mathrm{tor}_\Lambda(X^T_{S,\infty})_{G_n}/p^n)$.

Lemme 2.2.11. — *Soit T un Λ-module de type fini, de torsion et d'invariant μ. Alors*

$$\#(T_{G_n}/p^n) = p^{\mu(G:G_n)+\mathcal{O}(np^{n(d-1)})}.$$

Démonstration. — On dévisse le problème en s'intéressant à la suite exacte

$$0 \to \mathrm{tor}_{\mathbb{Z}_p}(T) \to T \to \widetilde{T} \to 0,$$

où $\widetilde{T} = T/\mathrm{tor}_{\mathbb{Z}_p}(M)$ est un module de Λ-torsion sans $\mathbb{Z}_p$-torsion.
Le module $\widetilde{T}$ étant sans $\mathbb{Z}_p$-torsion, quotienter par p^n conserve l'exactitude de cette suite et conduit à la suite exacte d'homologie :

$$H_1(G_n, \widetilde{T}/p^n) \to \mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n \to T_{G_n}/p^n \to \widetilde{T}_{G_n}/p^n \to 0.$$

Le corollaire 2.2.7 pour le module $\widetilde{T}$ permet d'obtenir la relation

$$\#(T_{G_n}/p^n) = \#(\mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n)p^{\mathcal{O}(np^{n(d-1)})}.$$

Il suffit donc de contôler le cardinal de $\mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n$ à l'aide du théorème 1.3.14, qui fournit un pseudo-isomorphisme

$$\mathrm{tor}_{\mathbb{Z}_p}(T) \to \bigoplus_{i=1}^{r} \Lambda/p^{\alpha_i},$$

avec $\mu = \sum \alpha_i$.
La proposition 2.2.9 nous informe qu'alors :

$$\begin{aligned} \#(\mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n) &= \#\left(\bigoplus_{i=1}^{r} \mathbb{Z}_p[G/G_n]/(p^{\alpha_i}, p^n)\right) p^{\mathcal{O}(np^{n(d-1)})} \\ &= p^{\mu(G:G_n)+\mathcal{O}(np^{n(d-1)})}. \end{aligned}$$

□

Il reste à évaluer la partie sans torsion $\#(\overline{X^T_{S,\infty}}_{G_n}/p^n)$. C'est l'objet du lemme :

Lemme 2.2.12. — *Soit M un Λ-module de type fini, sans-torsion et de rang ρ. Alors*

$$\#(M_{G_n}/p^n) = p^{\rho n(G:G_n)+\mathcal{O}(np^{n(d-1)})}.$$

Démonstration. — Tout Λ-module sans torsion est contenu dans un module libre de même rang (lemme 2.2.4). On a donc une suite exacte

$$0 \to M \to \Lambda^\rho \to T \to 0,$$

qui conduit à la suite exacte de Ω-modules

$$0 \to T[p] \to M/p \to \Omega^\rho \to T/p \to 0.$$

La somme alternée des Ω-rangs nous informe que $\mathrm{rk}_\Omega(M/p) = \rho$.
Le théorème 2.2.1 appliqué au Ω-module M/p donne alors une suite bornée $(c_n)_n$ telle que

$$\dim_{\mathbb{F}_p}(M_{G_n}/p) = \rho(G : G_n) + c_n p^{n(d-1)}.$$

Pour calculer $\#(M_{G_n}/p^n)$, on signale les isomorphismes suivants, qui proviennent du fait que M est sans torsion :

$$M/pM \xrightarrow{p^i}_{\sim} p^i M/p^{i+1}M.$$

On a ainsi

$$\begin{aligned}\#(M_{G_n}/p^n) &= \prod_{i=0}^{n} \#(p^i M/p^{i+1}M)_{G_n} \\ &= (\#(M_{G_n}/p))^n \\ &= p^{\rho n(G:G_n)+c_n n p^{n(d-1)}} \\ &= p^{\rho n(G:G_n)+\mathcal{O}(np^{n(d-1)})}.\end{aligned}$$

□

La mise en commun, via la proposition 2.2.10, des résultats fournis par les lemmes 2.2.11 et 2.2.12 appliqués respectivement à $\mathrm{tor}_\Lambda(X_{S,\infty}^T)$ et à $\overline{X_{S,\infty}^T}$ constitue une preuve du dernier point du théorème 2.2.8.

2.3. Formules asymptotiques le long d'une $\mathbb{Z}_p$-extension

On se replace dorénavant dans le cadre classique de la théorie d'Iwasawa. On considère donc une $\mathbb{Z}_p$-extension K_∞/K du corps de nombres K, dont on note le groupe de Galois Γ. On fixe S et T deux ensembles finis de places de K. La notation $X_{S,n}^T$ vaudra encore pour le p-groupe des T-classes S-infinitésimales attaché au n-ième étage K_n de la tour. Le théorème 2.2.8 s'applique dans ce cadre et donne, entre autre, la formule suivante :

$$\#(X_{S,n}^T/p^n) = p^{(\rho_S^T n+\mu_S^T)p^n+\mathcal{O}(n)}.$$

Dans [**22**] (théorème 2.2), il est annoncé une formule qui précise le $\mathcal{O}(n)$ en faisant apparaître l'invariant d'Iwasawa λ_S^T : il existe une constante α_S^T telle que, pour n assez grand,

$$\#(X_{S,n}^T/p^n) = p^{(\rho_S^T n+\mu_S^T)p^n+\lambda_S^T(+1)n+\alpha_S^T},$$

le paramètre λ_S^T devant être augmenté de 1 dans le cas spécial.
Cependant, il se trouve que ce résultat peut être pris en défaut. L'erreur conduisant à la formule de Jaulent est de considérer le défaut de descente Y_e, dans le théorème 2.1.7, comme un sous-Λ-module de $X_{S,\infty}^T$. On corrigera les calculs en tenant compte de cette remarque. Il en découlera l'apparition d'un paramètre $\tilde{\lambda}_S^T$ à la place de l'invariant d'Iwasawa λ_S^T, la différence entre ces deux entiers pouvant être maîtrisée. Nous isolerons ensuite un certain nombre de cas pour lesquels ces deux quantités coïncident et nous donnerons des exemples concrets dans lesquels le paramètre $\tilde{\lambda}_S^T$ est négatif.
Le contenu de cette partie est issu d'un travail en commun avec Jean-François Jaulent et Christian Maire.

2.3.1. La formule corrigée. — Dans cette section, on suppose que la $\mathbb{Z}_p$-extension K_∞/K n'est pas elle même S-ramifiée et T-décomposée. Autrement dit, on se place dans le cas général. La suite du paragraphe est dédiée à la démonstration du théorème suivant.

Théorème 2.3.1. — *Soit K_∞/K une $\mathbb{Z}_p$-extension et S et T deux ensembles finis de places de K. Dans le cas général, on a la formule asymptotique suivante concernant les p-groupes de T-classes S-infinitésimales des étages de la tour K_∞/K :*

$$\#\left(X_{S,n}^T/p^n\right) = p^{\rho_S^T np^n + \mu_S^T p^n + (\lambda_S^T - \kappa_S^T)n + \mathcal{O}(1)},$$

où ρ_S^T, μ_S^T et λ_S^T sont les invariants structurels du module d'Iwasawa $X_{S,\infty}^T$, et où κ_S^T est un entier naturel vérifiant $\kappa_S^T \leqslant \rho_S^T p^e$, avec e l'entier correspondant à l'étage à partir duquel les places se stabilisent (voir la partie 2.1.3*).*
On notera $\tilde{\lambda}_S^T$ la quantité $\lambda_S^T - \kappa_S^T$ qui apparaît dans la formule.

Tout d'abord, le résultat de descente dans ce cadre (théorème 2.1.7) permet de se ramener au calcul de $\left(X_{S,\infty}^T : (\nabla_n X_{S,\infty}^T + \omega_{n,e} Y_e)\right)$, où la notation ∇_n vaut pour l'idéal de Λ engendré par ω_n et p^n.
On va effectuer le calcul de cet indice en se ramenant à un module cyclique de la forme de ceux qui apparaîssent dans le théorème de structure (théorème 1.3.3), via le lemme suivant :

Lemme 2.3.2. — *Soit $\varphi : M \to E$ un pseudo-isomorphisme entre Λ-modules, avec E un module élémentaire. Soit Y un sous-$\mathbb{Z}_p$-module de M et $\mathcal{Y} = \varphi(Y)$. Lorsque n varie, on a*

$$(M : (\nabla_n M + \omega_{n,e} Y)) = (E : (\nabla_n E + \omega_{n,e} \mathcal{Y})) + \mathcal{O}(1).$$

Démonstration. — On utilise la démonstration du lemme 1.12 de [**22**] pour obtenir les suites exactes suivantes, pour n assez grand :

$$0 \to A_n \to M/\nabla_n M \xrightarrow{\varphi_n} E/\nabla_n E \to B \to 0,$$

avec A_n et B des modules finis tels que la suite des cardinaux de A_n est stationnaire. Détaillons ce passage.
Le pseudo-isomorphisme φ passe au quotient et fournit un morphisme φ_n, pour tout n, entre $M/\nabla_n M$ et $E/\nabla_n E$. Notons respectivement A et B les noyau et conoyau du pseudo-isomorphisme φ et prenons n assez grand pour que $\nabla_n E \subset \varphi(M)$ (ce qui est possible car la suite d'idéaux $(\nabla_n)_n$ forme une base de voisinage de l'unité dans Λ et $\varphi(M)$ est d'indice fini dans E). Ceci entraîne en particulier que $\operatorname{coker}(\varphi_n) = B$ pour n assez grand.

Reste à voir que les noyaux des φ_n, notés A_n, sont de cardinal stationnaire. On a $A_n = \varphi^{-1}(\nabla_n E)/\nabla_n M$. Analysons le morphisme

$$\varphi^{-1}(\nabla_n E)/\nabla_n M \xrightarrow{\varphi} \nabla_n E/\nabla_n \varphi(M).$$

L'inclusion $\nabla_n E \subset \varphi(M)$ assure sa surjectivité car on a $\varphi(\varphi^{-1}(\nabla_n E)) = \nabla_n E$. Quant à son noyau, il est égal à $A/(A \cap \nabla_n M)$. Quitte à augmenter n, on peut supposer que $A \cap \nabla_n M = \{0\}$ car A est fini. On en déduit que pour n assez grand :

$$(\varphi^{-1}(\nabla_n E) : \nabla_n M) = \#(A)(\nabla_n E : \nabla_n \varphi(M)).$$

Ainsi, il suffit de voir que l'indice $(\nabla_n E : \nabla_n \varphi(M))$ est stationnaire, ce qui est une conséquence du lemme 2.3.3 qui va suivre.

A partir des morphismes φ_n, on obtient les morphismes :

$$M/(\nabla_n M + \omega_{n,e} Y) \xrightarrow{\varphi_n} E/(\nabla_n E + \omega_{n,e} \mathcal{Y}),$$

de conoyaux B et de noyaux $A_n/(A_n \cap \omega_{n,e} Y)$.
La stationnarité des cardinaux des A_n, met en évidence que les noyaux sont de cardinal borné, et achève la démonstration. □

Lemme 2.3.3. — *Soit E un Λ-module élémentaire et F un sous-module d'indice fini de E. Alors la suite des indices $(\nabla_n E : \nabla_n F)$ est stationnaire.*

Démonstration. — Posons d'abord quelques notations utilisées dans la démonstration de ce résultat. Pour un Λ-module M, on pose $\partial_n M = p^n M \cap \omega_n M$. On notera également M^{tor} le sous-module de Λ-torsion de M et $\pi : M \to M/M^{tor}$ la projection canonique.

On remarque, dans un premier temps, que la stationnarité de $(\nabla_n E : \nabla_n F)$ est équivalente à celle de $(\partial_n E : \partial_n F)$.
En effet, ces deux quantités sont reliées par la suite exacte

$$0 \to \partial_n E/\partial_n F \to p^n E/p^n F \oplus \omega_n E/\omega_n F \to \nabla_n E/\nabla_n F \to 0.$$

Le terme médiant est clairement fini et décroissant car F est d'indice fini dans E. Il est donc stationnaire et il suffit bien de démontrer la stationnarité de $(\partial_n E : \partial_n F)$.

Le calcul suivant permet de se ramener à des modules libres d'une part, et de torsion d'autre part :

$$\begin{aligned}(\partial_n E : \partial_n F) &= (\partial_n E : \partial_n E^{tor} + \partial_n F)(\partial_n E^{tor} + \partial_n F : \partial_n F) \\ &= (\pi(\partial_n E) : \pi(\partial_n F))(\partial_n E^{tor} : \partial_n F^{tor}).\end{aligned}$$

Concernant $(\pi(\partial_n E) : \pi(\partial_n F))$, on a $\pi(\partial_n E) = \Lambda^\rho$ et, par factorialité de Λ, on en déduit que

$$\pi(\partial_{n+1} E) = \pi(p^{n+1}\omega_{n+1} E) = p\frac{\omega_{n+1}}{\omega_n}\pi(\partial_n E).$$

D'autre part, $p\frac{\omega_{n+1}}{\omega_n}\pi(\partial_n F) \subset \pi(\partial_{n+1}F)$ ce qui nous permet de dire que

$$\begin{array}{rcl}(\pi(\partial_{n+1}E) : \pi(\partial_{n+1}F)) & \leq & (p\frac{\omega_{n+1}}{\omega_n}\pi(\partial_n E) : p\frac{\omega_{n+1}}{\omega_n}\pi(\partial_n F)) \\ & \leq & (\pi(\partial_n E) : \pi(\partial_n F)).\end{array}$$

La suite $(\pi(\partial_n E) : \pi(\partial_n F))$ est donc décroissante et, par suite, stationnaire.

Intérressons nous maintenant à la partie de torsion. Notons T la partie donnant l'invariant λ de la décomposition en modules cycliques de E^{tor}, c'est à dire la somme des modules de la forme $\Lambda/(f)$ où f est un polynôme distingué. Pour n assez grand, on a $p^n E^{tor} = p^n T$ donc aussi $\partial_n E^{tor} = \partial_n T$. Le lemme 1.6 de **[22]** nous informe, quitte à augmenter n, que $\frac{\omega_{n+1}}{\omega_n}T = pT$ et conduit à la relation

$$\partial_{n+1}T = pp^n T \cap \omega_n \frac{\omega_{n+1}}{\omega_n}T = p\,\partial_n T.$$

On en déduit que $\partial_{n+1}E^{tor} = p\,\partial_n E^{tor}$ et, de la même façon, que $\partial_{n+1}F^{tor} = p\,\partial_n F^{tor}$.
Ceci à l'incidence suivante sur la valeur des indices :

$$(\partial_{n+1}E^{tor} : \partial_{n+1}F^{tor}) = (p\,\partial_n E^{tor} : p\,\partial_n F^{tor}) \leq (\partial_n E^{tor} : \partial_n F^{tor}).$$

La suite $(\partial_n E^{tor} : \partial_n F^{tor})$ est donc elle aussi stationnaire ce qui termine la démonstration du lemme. □

Le théorème 1.3.3 assure l'existence d'un pseudo-isomorphisme $\varphi : X_{S,\infty}^T \to E$ entre $X_{S,\infty}^T$ et un Λ-module élémentaire E, d'invariants ρ_S^T, μ_S^T et λ_S^T. Ceci étant, le lemme 2.3.2 affirme qu'à une quantité bornée près, l'indice $\Big(X_{S,\infty}^T : (\nabla_n X_{S,\infty}^T + \omega_{n,e}Y_e)\Big)$ que l'on cherche à estimer est asymptotiquement égal à l'indice $\big(E : (\nabla_n E + \omega_{n,e}\varphi(Y_e))\big)$, qui peut se calculer explicitement. C'est en déterminant cet indice que l'on fait apparaître les invariants d'Iwasawa de $X_{S,\infty}^T$, ainsi que la perturbation κ_S^T dans la formule du théorème 2.3.1.
La correction apportée au théorème de descente (*ie.* Y_e n'est pas en général un sous-Λ-module de $X_{S,\infty}^T$) entraîne que l'intersection de $\varphi(Y_e)$ avec la partie libre du module élémentaire E n'est pas forcément triviale, et complique quelque peu les calculs initiaux de Jaulent. Nous allons estimer séparément les contibutions respectives de la partie libre $L = \Lambda^{\rho_S^T}$ et du sous-module de torsion T de E en écrivant :

$$\big(E : (\nabla_n E + \omega_{n,e}\varphi(Y_e))\big) \;=\; \big(E : (T + \nabla_n E + \omega_{n,e}\varphi(Y_e))\big)\,\big(T : T \cap (\nabla_n E + \omega_{n,e}\varphi(Y_e))\big),$$

et en évaluant séparément les deux facteurs.

- Attachons nous tout d'abord à la détermination de la partie libre. On a

$$\big(E : (T + \nabla_n E + \omega_{n,e}\varphi(Y_e))\big) = \big(L : (\nabla_n L + \omega_{n,e}\mathcal{Y})\big),$$

où $\mathcal{Y}$ désigne l'image de $\varphi(Y_e)$ dans le quotient $E/T \simeq L$.

On note $Z = \omega_e L + \mathcal{Y}$ et on découpe le calcul de la façon suivante :

$$\big(L : (\nabla_n L + \omega_{n,e}\mathcal{Y})\big) = \big(L : (p^n L + Z)\big)\big(Z : (p^n L \cap Z + \omega_{n,e} Z)\big).$$

Pour déterminer le premier indice $\big(L : (p^n L + Z)\big)$, on écrit un pseudo-isomorphisme donné par le théorème de structure :

$$L/Z \to \bigoplus_{i=1}^{r} \Lambda/(g_i^{\alpha_i}),$$

où les g_i sont des polynômes irréductibles divisant ω_e.
Quotienter par p^n donne l'égalité

$$\begin{aligned} \big(L : (p^n L + Z)\big) &= \prod_{i=1}^{r} \#\big(\Lambda/(g_i^{\alpha_i}, p^n)\big) + \mathcal{O}(1) \\ &= p^{\deg(\prod g_i^{\alpha_i})n + \mathcal{O}(1)}. \end{aligned}$$

Un calcul de $\mathbb{Z}_p$-rangs permet d'obtenir l'inégalité

$$\begin{aligned} \rho_S^T p^e &= \mathrm{rk}_{\mathbb{Z}_p}(L/\omega_e L) \\ &\geqslant \mathrm{rk}_{\mathbb{Z}_p}(L/Z) \\ &= \mathrm{rk}_{\mathbb{Z}_p}(\oplus_{i=1}^{r} \Lambda/(g_i^{\alpha_i})) \\ &= \deg(\textstyle\prod g_i^{\alpha_i}). \end{aligned}$$

Le calcul du second indice est un peu plus technique. On se ramène au calcul des deux premiers termes de la suite exacte

$$0 \to (p^n L \cap Z + \omega_{n,e} Z)/(p^n Z + \omega_{n,e} Z) \to Z/(p^n Z + \omega_{n,e} Z) \to Z/(p^n L \cap Z + \omega_{n,e} Z) \to 0.$$

Le Λ-module Z est sans torsion, de rang ρ_S^T, donc il existe un pseudo-isomorphisme $Z \to \Lambda^{\rho_S^T}$. Ceci nous renseigne sur le terme central de cette dernière suite exacte :

$$\big(Z : (p^n Z + \omega_{n,e} Z)\big) = p^{\rho_S^T n p^n - \rho_S^T p^e n + \mathcal{O}(1)}.$$

On va voir que le noyau est stationnaire. On a

$$(p^n L \cap Z + \omega_{n,e} Z)/(p^n Z + \omega_{n,e} Z) \simeq (p^n L \cap Z)/(p^n Z + p^n L \cap \omega_{n,e} Z).$$

Notons $p^{-n} Z = \{x \in L \mid p^n x \in Z\}$, de telle sorte que la suite $(p^{-n} Z)_n$ est une suite croissante de sous-Λ-modules de L. Cette suite est stationnaire par noethérianité donc il existe un entier α tel que $p^{-n} Z = p^{-\alpha} Z$ pour $n \geqslant \alpha$. Pour de tels n, on a $p^n L \cap Z = p^n (p^{-\alpha} Z)$ et $p^n L \cap \omega_{n,e} Z = \omega_{n,e} p^n (p^{-\alpha} Z)$ par factorialité de L.
Ainsi,

$$\begin{aligned} (p^n L \cap Z)/(p^n Z + p^n L \cap \omega_{n,e} Z) &= p^n (p^{-\alpha} Z)/p^n (Z + \omega_{n,e}(p^{-\alpha} Z)) \\ &\simeq p^{-\alpha} Z/(Z + \omega_{n,e}(p^{-\alpha} Z)), \end{aligned}$$

Le dernier isomorphisme se justifiant par l'absence de torsion. Le noyau est stationnaire dès lors que le quotient $p^{-\alpha} Z/Z$ est fini.

Mais $L/\omega_e L$ est de type fini sur $\mathbb{Z}_p$. Son sous-module $p^{-\alpha}Z/\omega_e L$ l'est donc aussi et, par suite, il en est de même de son quotient $p^{-\alpha}Z/Z$. Ce dernier quotient étant par définition tué par p^α, il est fini.

Finalement, on a

$$\big(E : (T + \nabla_n E + \omega_{n,e}\varphi(Y_e))\big) = p^{\rho_S^T n p^n - \kappa_S^T n + \mathcal{O}(1)},$$

avec $\kappa_S^T = \rho_S^T p^e - \prod \deg(g_i^{\alpha_i})$ compris entre 0 et $\rho_S^T p^e$.

• Etudions maintenant le second facteur $\big(T : T \cap (\nabla_n E + \omega_{n,e}\varphi(Y_e))\big)$. C'est évidemment une fonction décroissante du module de descente $\varphi(Y_e)$. Nous en obtenons donc une majoration très simple en remplaçant Y_e par 0, et une minoration en remplaçant $\varphi(Y_e)$ par la somme directe de ses projections sur chaque facteur cyclique de E. Nous allons voir que les deux bornes obtenues dans cet encadrement different seulement d'une quantité bornée en n. Notons $T = \oplus_i \Lambda/(f_i)$, chaque élément f_i étant une puissance de p ou d'un polynôme distingué irréductible. On appelle $\mathcal{Y}_i$ la projection de $\varphi(Y_e)$ sur le i-ième facteur direct de cette somme, ce sont des $\mathbb{Z}_p$-modules de type fini.
On obtient :

$$\big(T : T \cap (\nabla_n E + \omega_{n,e} \oplus_i \mathcal{Y}_i)\big) = \prod_i \big(\Lambda : (\nabla_n + f_i\Lambda + \omega_{n,e}\mathcal{Y}_i)\big).$$

Si $f_i = p^\alpha$, on a pour $n \geqslant \alpha$:

$$\begin{array}{rcl}(\nabla_n + p^\alpha\Lambda + \omega_{n,e}\mathcal{Y}_i)/(\nabla_n + p^\alpha\Lambda) & \simeq & \omega_{n,e}\mathcal{Y}_i/(\omega_{n,e}\mathcal{Y}_i \cap (p^\alpha\Lambda + \omega_n\Lambda)) \\ & \simeq & \mathcal{Y}_i/(\mathcal{Y}_i \cap (p^\alpha\Lambda + \omega_e\Lambda).\end{array}$$

Le dernier isomorphisme se justifie par le fait que $\mathcal{Y}_i$ est sans non-p-torsion et débouche sur un objet fini qui ne dépend pas de n.
Si $f_i = f^\beta$ avec f distingué irréductible, le lemme 1.6 de [**22**] donne, pour $n \geqslant n_\circ \geqslant e$ assez grand :

$$\begin{array}{rcl}(\nabla_n + f^\beta\Lambda + \omega_{n,e}\mathcal{Y}_i)/(\nabla_n + f^\beta\Lambda) & \simeq & \omega_{n,e}\mathcal{Y}_i/(\omega_{n,e}\mathcal{Y}_i \cap (\nabla_n + f^\beta\Lambda)) \\ & \simeq & p^{n-n_\circ}\omega_{n_\circ,e}\mathcal{Y}_i/p^{n-n_\circ}(\omega_{n_\circ,e}\mathcal{Y}_i \cap (\nabla_{n_\circ} + f^\beta\Lambda)) \\ & \simeq & \omega_{n_\circ,e}\mathcal{Y}_i/(\omega_{n_\circ,e}\mathcal{Y}_i \cap (\nabla_{n_\circ} + f^\beta\Lambda)).\end{array}$$

Le dernier isomorphisme se justifie par le fait que $\mathcal{Y}_i$ est sans p-torsion et débouche également sur un objet fini qui ne dépend pas de n.
Ces calculs montrent que pour tout i :

$$\big(\Lambda : (\nabla_n + f_i\Lambda + \omega_{n,e}\mathcal{Y}_i)\big) = \big(\Lambda : (\nabla_n + f_i\Lambda)\big) + \mathcal{O}(1),$$

et permettent de se ramener au cas $\varphi(Y_e) = 0$.
L'indice $\big(\Lambda : (\nabla_n + f_i\Lambda)\big)$ se calcule explicitement et vaut $p^{\alpha p^n}$ lorsque $f_i = p^\alpha$ et $p^{\deg(f^\beta)n+c}$, avec c une constante, lorsque $f_i = f^\beta$ (voir [**22**] section 1.2 pour les détails de ce calcul).

La contribution de la partie de torsion est donc

$$\big(T : T \cap (\nabla_n E + \omega_{n,e}\varphi(Y_e))\big) = p^{\mu_S^T p^n + \lambda_S^T n + \mathcal{O}(1)}.$$

Les arguments qui précèdent fournissent la formule :

$$\#\left(X_{S,n}^T/p^n\right) = p^{\rho_S^T n p^n + \mu_S^T p^n + (\lambda_S^T - \kappa_S^T)n + \mathcal{O}(1)},$$

qui est le résultat annoncé dans le théorème 2.3.1.

2.3.2. Trivialité de κ_S^T. — Le théorème principal de la section précédente (théorème 2.3.1) donne une formule asymptotique portant sur les groupes de classes généralisés le long d'une $\mathbb{Z}_p$-extension. Ce qui est remarquable est l'intervention d'une perturbation inattendue de l'invariant d'Iwasawa λ_S^T, provenant d'un défaut de descente. Cette section isole des situations dans lesquelles cette perturbation est triviale. La première correspond au cas spécial, dans lequel la $\mathbb{Z}_p$-extension est elle même S-ramifiée et T-décomposée.

Théorème 2.3.4. — *Soient S et T deux ensembles finis de places d'un corps de nombres K et soit K_∞/K une $\mathbb{Z}_p$-extension. Dans le cas spécial, les p-groupes des T-classes S-infinitésimales attachés aux étages de K_∞/K vérifient, pour n assez grand :*

$$\#\left(X_{S,n}^T/p^n\right) = p^{\rho_S^T n p^n + \mu_S^T p^n + (\lambda_S^T + 1)n + c},$$

avec ρ_S^T, μ_S^T et λ_S^T les invariants d'Iwasawa de $X_{S,\infty}^T$ et $c \in \mathbb{Z}$ une constante.

Démonstration. — La descente se fait de la façon suivante (théorème 2.1.8) :

$$X_{S,n}^T \simeq X_{S,\infty}^T/\omega_n X_{S,\infty}^T \oplus \Gamma_n.$$

Les calculs de la section précédente, en se ramenant à un module élémentaire, permettent de voir que $\#\big(X_{S,\infty}^T/(\omega_n X_{S,\infty}^T + p^n X_{S,\infty}^T)\big) = p^{\rho_S^T n p^n + \mu_S^T p^n + \lambda_S^T n + c}$ et le $+1$ provient du cardinal de Γ_n/p^n. □

Dans le cas général, l'analyse de la preuve du théorème 2.3.1 montre que la quantité κ_S^T provient de la contribution du sous-$\mathbb{Z}_p$-module de descente Y_e dans la partie libre du module à l'infini $X_{S,\infty}^T$. On en déduit donc les résultats suivants :

Corollaire 2.3.5. — *Soient S et T deux ensembles finis de places d'un corps de nombres K et soit K_∞/K une $\mathbb{Z}_p$-extension telle que l'union de l'ensemble des places de K_∞ au dessus de $R-S$ et de l'ensemble de celles au dessus de T^{fd} est un singleton. Alors les p-groupes des T-classes S-infinitésimales attachés aux étages de K_∞/K vérifient, pour n assez grand :*

$$\#\left(X_{S,n}^T/p^n\right) = p^{\rho_S^T n p^n + \mu_S^T p^n + \lambda_S^T n + c},$$

avec ρ_S^T, μ_S^T et λ_S^T les invariants d'Iwasawa de $X_{S,\infty}^T$ et $c \in \mathbb{Z}$ une constante.

Démonstration. — Cette fois-ci, les hypothèses de ramification conduisent à un $\mathbb{Z}_p$-module de descente Y_e trivial. Le résultat est alors une conséquence des calculs menés dans la section 2.3.1 et de la remarque qui précède l'énoncé du corollaire. □

Corollaire 2.3.6. — *Soient S et T deux ensembles finis de places d'un corps de nombres K et soit K_∞/K une $\mathbb{Z}_p$-extension. On suppose que le module d'Iwasawa à l'infini $X_{S,\infty}^T$ est de torsion. Alors, pour n assez grand :*

$$\#\left(X_{S,n}^T/p^n\right) = p^{\mu_S^T p^n + \lambda_S^T n + \mathcal{O}(1)},$$

avec μ_S^T et λ_S^T les invariants d'Iwasawa de $X_{S,\infty}^T$.

Démonstration. — La partie libre de $X_{S,\infty}^T$ est nulle donc la perturbation κ_S^T, ainsi que l'invariant ρ_S^T le sont aussi. □

On remarque que les hypothèses du dernier corollaire sont vérifiées lorsque S ne contient que des places modérées.

2.3.3. Valeurs négatives de $\tilde{\lambda}_S^T$. — On expose ici une situation dans laquelle le paramètre $\tilde{\lambda}_S^T$, qui apparaît dans l'énoncé du théorème 2.3.1, peut être rendu aussi négatif que voulu.

• On prend $p = 2$, $K = \mathbb{Q}(i)$ et on considère K_∞ la $\mathbb{Z}_2$-extension cyclotomique de K. Le travail déjà effectué fournit certaines conditions nécessaires sur S et T pour obtenir un paramètre $\tilde{\lambda}_S^T$ négatif. Plus précisément, la borne $\rho_S^T p^e$ sur κ_S^T devra atteindre des valeurs aussi grandes que voulues. Ceci force l'ensemble S à contenir des places 2-adiques. Dans le cas contraire, les modules $X_{S,n}^T$ sont de $\mathbb{Z}_2$-torsion et leur limite projective $X_{S,\infty}^T$ est de Λ-torsion, ce qui entraîne $\kappa_S^T = 0$. Dans l'exemple qui va suivre, l'invariant ρ_S^T sera toujours égal à 1. La borne sur κ_S^T sera donc rendue grande en jouant sur l'entier e, c'est à dire en imposant d'assez fortes congruences sur les places de T pour qu'elles soient décomposées dans K_e/K.
On met dans S l'unique place 2-adique de K et dans T les deux places de K au dessus d'un premier q totalement décomposé dans $K_e/\mathbb{Q}$ et inerte dans K_∞/K_e, pour un entier naturel e arbitraire. Le premier q vérifie la congruence $q \equiv 1 + 2^{e+1} (mod\, 2^{e+2})$.

Déterminons tout d'abord le module à l'infini $X_{S,\infty}^T$. Comme on est au-dessus de la $\mathbb{Z}_2$-extension cyclotomique, on a $X_{S,\infty}^T = X_{S,\infty}$. En effet, les places modérées non ramifiées sont totalement décomposées au-dessus de K_∞ du fait que K_∞/K est localement la p-extension non ramifiée maximale de K en les places modérées.
Il est bien connu que $X_{S,\infty}$ est de Λ-rang égal au nombre de places complexes $r_2(K) = 1$ ([**40**], théorème 13.31) donc $\rho_S^T = \rho_S = 1$.

La descente pour $X_{S,\infty}$ s'écrit $X_{S,\infty}/(\omega_0) \oplus \mathbb{Z}_2 \simeq X_{S,0}$ car K_∞/K est S-ramifiée. Donc $X_{S,\infty}/(\omega_0, 2) \oplus \mathbb{Z}/2\mathbb{Z} \simeq X_{S,0}/(2)$.
On évalue $X_{S,0}/(2)$ en utilisant la dualité de Kummer. Le radical kummérien correspondant est $E'(K)/E'(K)^2$, où $E'(K)$ désigne les 2-unités de K. On a $E'(K) \simeq \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ ce qui entraîne $E'(K)/E'(K)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$.
Le $\mathbb{Z}/2\mathbb{Z}$-module $X_{S,\infty}/(\omega_0, 2)$ est ainsi cyclique et, par le lemme de Nakayama, $X_{S,\infty}$ est un Λ-module cyclique.
En résumé, on a $X_{S,\infty}^T \simeq \Lambda$ et $\rho_S^T = 1$, $\mu_S^T = \lambda_S^T = 0$.

Ce point acquis, pour tout $n \geqslant e$, la descente pour $X_{S,\infty}^T$ s'écrit :

$$X_{S,n}^T \simeq X_{S,\infty}^T/\omega_{n,e}(\omega_e X_{S,\infty}^T + Y_e).$$

Il se trouve que le module $X_{S,e}^T$ est fini. En effet, la théorie p-adique du corps de classes (voir **[21]**) l'interprète comme le quotient $\mathcal{U}_2(K_e)/s_2(\mathcal{E}^T(K_e))$ du 2-groupe des unités locales en l'unique place 2-adique de K_e par l'image canonique du $\mathbb{Z}_2$-tensorisé du groupe des T-unités de K_e. Or, à un fini près, $\mathcal{U}_2(K_e)$ définit la représentation régulière du groupe de Galois $\mathrm{Gal}(K_e/\mathbb{Q})$ et $\mathcal{E}^T(K_e)$ contient aussi cette représentaion régulière du fait que q est totalement décomposé dans $K_e/\mathbb{Q}$. La conjecture de Leopoldt, qui est vérifiée ici puisque $\mathrm{Gal}(K_e/\mathbb{Q})$ est abélien, nous assure que $s_2(\mathcal{E}^T(K_e))$ la contient encore. Ceci montre que le groupe $X_{S,e}^T$ est fini.
On obtient donc un pseudo-isomorphisme :

$$(\omega_e X_{S,\infty}^T + Y_e) \hookrightarrow X_{S,\infty}^T,$$

puis un pseudo-isomorphisme

$$X_{S,n}^T \twoheadrightarrow X_{S,\infty}^T/\omega_{n,e}X_{S,\infty}^T \simeq \Lambda/\omega_{n,e}\Lambda.$$

On en déduit que $\#(X_{S,n}^T/(2^n)) = \#(\Lambda/(\omega_{n,e}, 2^n)) + \mathcal{O}(1) = 2^{n2^n - n2^e + \mathcal{O}(1)}$, donc que $\tilde{\lambda}_S^T = -2^e$. Cet exemple montre que la borne sur κ_S^T est optimale.

• Cet exemple peut être développé aussi pour p un premier impair irrégulier. On prend pour corps de base le corps cyclotomique $K = \mathbb{Q}(\zeta_p)$ et on considère sa $\mathbb{Z}_p$-extension cyclotomique K_∞. On fixe aussi un entier naturel e. L'ensemble de places S est constitué de l'unique place p-adique de K et T contient les $p-1$ places de K au dessus d'un nombre premier q totalement décomposé dans $K_e/\mathbb{Q}$ et inerte dans K_∞/K_e (q vérifie la congruence $q \equiv 1 + p^e (mod\, p^{e+1})$).
Introduisons le groupe de Galois $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ et notons Δ^* le groupe des caractères p-adiques de Δ. A chaque élément φ de Δ^* correspond un idempotent primitif e_φ de l'algèbre de groupe $\mathbb{Z}_p[\Delta]$, ce qui permet d'écrire canoniquement tout $\Lambda[\Delta]$-module comme somme directe de ses φ-composantes. Ceci vaut en particulier pour le module $X_{S,\infty}^T = X_{S,\infty}$. On note X_φ la φ-composante de $X_{S,\infty}^T$, c'est un module sur $\Lambda_\varphi \simeq \Lambda$ que l'on peut déterminer selon la parité du caractère φ.

– Si φ est pair (c'est à dire si φ prend la valeur $+1$ sur la conjugaison complexe τ), l'hypothèse de régularité entraîne la trivialité de X_φ.
– Si φ est impair ($\varphi(\tau) = -1$), il vient que X_φ est libre de rang 1 sur Λ_φ. Donc $X_\varphi \simeq \Lambda$.

On en déduit que $\rho_S^T = (p-1)/2$, $\mu_S^T = 0$ et $\lambda_S^T = 0$.
Les arguments développés dans l'exemple précédent donnent une perturbation égale à $-p^e$ pour chaque caractère φ impair, soit au total $\tilde{\lambda}_S^T = -p^e(p-1)/2$.

CHAPITRE 3

FORMULES DE RÉFLEXION

Dans [**23**], les formules asymptotiques sur les p-groupes de classes généralisés le long d'une $\mathbb{Z}_p$-extension sont exploitées à l'aide des formules de réflexion de Gras (voir [**10**] ou [**9**]). Le but est d'obtenir des informations sur les invariants d'Iwasawa et le principe est le suivant. Les formules asymptotiques relient les invariants d'un module d'Iwasawa à l'infini à des objets attachés aux étages finis de la tour. En présence de racines de l'unité, ces objets au niveau fini possèdent une double interprétation en terme de groupe de classes et en terme de radicaux kummeriens. On peut supposer sans restriction que les ensembles de places S et T sont disjoints, il suffit d'enlever les places de l'intersection de S et les modules correspondants sont les mêmes. Si S et T sont disjoints et que leur union contient toutes les places p-adiques, on peut donner un lien explicite entre les objets finis correspondant au couple (S,T) et ceux correspondant au couple (T,S). Arithmétiquement, ceci traduit une dualité entre ramification et décomposition qui peut être retranscrite au niveau des invariants d'Iwasawa. Nous donnerons, dans ce chapitre, les formules de réflexion sur les invariants d'Iwasawa pour la $\mathbb{Z}_p$-extension cyclotomique qui tiennent compte des corrections apportées à l'article [**23**]. Aussi, l'obtention de formules asymptotiques pour des extensions de Lie p-adiques nous autorise à étendre ces formules aux extensions de dimension supérieure. Nous en déduirons le calcul de l'invariant d'Iwasawa ρ dans certains cas particuliers.

3.1. Cas de la $\mathbb{Z}_p$-extension cyclotomique

On se contente ici de donner une version corrigée du théorème 6 de [**23**]. La démonstration qui s'y trouve est parfaitement valable si on remplace l'invariant d'Iwasawa λ_S^T par l'invariant $\tilde{\lambda}_S^T$ qui apparaît effectivement dans la formule asymptotique (théorèmes 2.3.1 et 2.3.4 dans lequel $\tilde{\lambda}_S^T = \lambda_S^T + 1$). On

utilisera d'ailleurs cette démonstration pour traiter le cas des extensions de Lie p-adiques dans la section 3.2.1.
Pour un ensemble fini S de places d'un corps de nombres K, on pose $\delta_S = \sum_{v \in S_p} [K_v : \mathbb{Q}_p]$ la somme des degrés locaux des localisés de K en les places p-adiques de S. On notera aussi s_∞ le nombre de places au dessus de S d'une $\mathbb{Z}_p$-extension K_∞ de K.

Théorème 3.1.1 **(Jaulent, Maire, [23], théorème 6)**

Soit K un corps de nombres contenant les racines $2p$-ièmes de l'unité et soit K_∞ la $\mathbb{Z}_p$-extension cyclotomique de K. On se donne deux ensembles finis disjoints S et T de places de K dont l'union contient les places p-adiques. Alors les invariants associés à K_∞/K vérifient les identités du miroir :

(i) $\rho_S^T + \dfrac{\delta_T}{2} = \rho_T^S + \dfrac{\delta_S}{2}$,

(ii) $\mu_S^T = \mu_T^S$,

(iii) $\tilde{\lambda}_S^T + t_\infty = \tilde{\lambda}_T^S + s_\infty$.

Ce théorème permet d'obtenir des informations sur les invariants ρ_S^T et μ_S^T, que l'on exposera dans le cas général traité dans la partie 3.2.3.
Une conséquente immédiate sur l'invariant λ_S^T est l'existence d'une minoration très simples lorsque S contient les places p-adiques.

Corollaire 3.1.2. — *Soit K un corps de nombres contenant les racines $2p$-ièmes de l'unité et soit K_∞ sa $\mathbb{Z}_p$-extension cyclotomique. On se donne S un ensemble fini de places de K qui contient l'ensemble des places p-adiques et T un ensemble fini de places modérées disjoint de S. Alors*

$$\lambda_S^T \geqslant s_\infty - 1.$$

En particulier, λ_S^T est arbitrairement grand avec S.

Démonstration. — Les identités du miroir nous donnent pour $T = \emptyset$:

$$\lambda_S + 1 = \tilde{\lambda}_S = \tilde{\lambda}^S + s_\infty = \lambda^S + s_\infty \geqslant s_\infty,$$

puisque, dans le cas spécial, $\tilde{\lambda}_S = \lambda_S + 1$ et que, pour le module de Λ-torsion X_∞^S, le paramètre effectif $\tilde{\lambda}^S$ coïncide avec l'invariant d'Iwasawa λ^S (voir le théorème 2.3.4 et le corollaire 2.3.6).
La montée dans la $\mathbb{Z}_p$-extension cyclotomique ayant épuisé toute possibilité d'inertie aux places modérées, on a banalement $X_{S,\infty}^T = X_{S,\infty}$, donc $\lambda_S^T = \lambda_S$. □

3.2. Cas des extensions de Lie

A partir de maintenant on fixe un nombre premier p et un corps de nombres K contenant les racines $2p$-ièmes de l'unité. On considère une extension K_∞/K dont le groupe de Galois G est un pro-p-groupe p-valué de type fini et dans laquelle seul un nombre fini de places de K se ramifie. On fixe deux ensembles finis disjoints S et T de places de K dont l'union contient les places p-adiques. Ce cadre permet d'appliquer les théorèmes de réflexion pour comparer la S-ramification et T-décomposition à la T-ramification et S-décomposition au niveau fini, puis d'utiliser le théorème 2.2.8 pour en tirer des conséquences sur les invariants d'Iwasawa à l'infini. On supposera d'abord, que le corps K_∞ contient la $\mathbb{Z}_p$-extension cyclotomique de K (ce cas couvre la situation de la section 3.1). Ensuite, nous verrons ce que l'on peut dire sans cette hypothèse.

3.2.1. En présence de la $\mathbb{Z}_p$-extension cyclotomique. — On suppose dans cette section que K_∞ contient la $\mathbb{Z}_p$-extension cyclotomique de K, donc $K(\mu_{p^\infty}) \subset K_\infty$ car $\mu_{2p} \in K$. Cette hypothèses assurent que, pour k assez grand, le corps K_{k+n} contient les racines p^n-ièmes de l'unité. En effet, G est produit semi-direct du groupe de Galois de la $\mathbb{Z}_p$-extension cyclotomique de K, noté Γ, par un sous-groupe distingué H de G. Prenons k assez grand pour que G_k soit p-saturé, de telle sorte que $G_{k+n} = G_k^{p^n}$. Pour tout n, les racines p^n-ièmes de l'unité sont fixées par H et par Γ^{p^n}, donc par $G_k^{p^n}$. Autrement dit, $\mu_{p^n} \subset K_{k+n}$. On fixe cette constante k dans la suite, en remarquant qu'elle est nulle si G est un groupe uniforme.

On aura besoin d'un certain nombre de notations qui servirons à énoncer le théorème fondamental de cette partie, qui exprime une lien entre le groupe des classes associé à la S-ramification, T-décomposition d'une part, et le radical kummerien associé à la T-ramification, S-décomposition d'autre part. On pourra se référer à [**21**] pour les définitions des objets de la théorie p-adique du corps de classes et on oubliera souvent l'indice n pour ne pas surcharger les notations. La notation $\mathfrak{m}$ vaut pour un certain diviseur, construit sur les places de $S(K_{k+n})$. Le module $\mathcal{R}$ est le p-adifié des idéles principaux de K_{k+n} et $\mathcal{R}_\mathfrak{m}$ est son sous-module des idéles congrues à 1 modulo $\mathfrak{m}$. On appelle $\mathcal{E}_\mathfrak{m}^T$ le p-adifié des T-unités de K_{k+n} qui sont congrues à 1 modulo $\mathfrak{m}$. Comme expliqué dans [**23**], le diviseur $\mathfrak{m}$ a été choisi de telle sorte que le quotient d'ordre p^n du p-groupe des T-classes de rayon $\mathfrak{m}$ de K_{k+n}, noté $\mathrm{Cl}_\mathfrak{m}^T$, soit isomorphe au quotient d'ordre p^n du groupe de Galois de sa pro-p-extension abélienne S-ramifiée T-décomposée maximale $X_{S,k+n}^T$, et que le radical kummérien du quotient de l'extension duale, T-ramifiée et S-décomposée, soit donné par $\mathrm{Rad}_\mathfrak{m}^T$. Enfin, $\mathfrak{R}_\mathfrak{m}^T[p^n]$ est un pseudo-radical qui permet de faire le lien entre les deux suites

du théorème suivant et qui est défini par

$$\mathfrak{R}_{\mathfrak{m}}^{T}[p^n] = \{p^n \otimes x \in p^{-n}\mathbb{Z}_p/\mathbb{Z}_p \otimes \mathcal{R}_{\mathfrak{m}} | x \in \mathcal{J}^T \mathcal{J}^{p^n}\},$$

où $\mathcal{J}$ est le p-groupe des idèles de K_{k+n} et $\mathcal{J}^T$ son sous-groupe des T-idèles.

***Théorème 3.2.1* (Jaulent, Maire, [23], théorème 4)**

A chaque étage K_{k+n} de la tour K_∞/K, on a les suites exactes du miroir :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (\mathcal{R}/\mathcal{R}_{\mathfrak{m}})[p^n]/\mu_{p^n} & \longrightarrow & \mathfrak{R}_{\mathfrak{m}}^{T}[p^n] & \longrightarrow & \mathrm{Rad}_{\mathfrak{m}}^{T}[p^n] & \longrightarrow & 1 \\ & & & & \| & & & & \\ 1 & \longrightarrow & \mathcal{E}_{\mathfrak{m}}^{T}/p^n & \longrightarrow & \mathfrak{R}_{\mathfrak{m}}^{T}[p^n] & \longrightarrow & \mathrm{Cl}_{\mathfrak{m}}^{T}[p^n] & \longrightarrow & 1 \end{array}$$

Le corollaire suivant résulte du calcul des cardinaux des termes des suites exactes du miroir, conjointement au théorème 2.2.8. Il donne les mêmes information sur ρ et μ que le théorème 3.1.1 et les notations y sont identiques.

Corollaire 3.2.2. — *Si $\mu_{2p} \subset K$ et que K_∞ contient la $\mathbb{Z}_p$-extension cyclotomique de K. On a les formules suivantes, lorsque $S \cup T$ contient les places p-adiques :*

$$\begin{aligned} \rho_S^T + \frac{\delta_T}{2} &= \rho_T^S + \frac{\delta_S}{2}, \\ r_S^T &= r_T^S, \\ \mu_S^T &= \mu_T^S. \end{aligned}$$

Démonstration. — Dans cette démonstration, les modules qui interviennent sont attachés au corps K_{k+n}.

• Tout d'abord, on fait apparaître les invariants d'Iwasawa en regardant les cardinaux des termes de droite des deux suites. En effet, $\mathrm{Cl}_{\mathfrak{m}}^{T}$ étant un groupe fini, on en déduit, d'après la théorie du corps de classes, que

$$\#(\mathrm{Cl}_{\mathfrak{m}}^{T}[p^n]) = \#(\mathrm{Cl}_{\mathfrak{m}}^{T}/p^n) = \#(\mathrm{Cl}_{S}^{T}/p^n) = \#(X_{S,k+n}^{T}/p^n).$$

D'autre part, utilisant la théorie de Kummer,

$$\#(\mathrm{Rad}_{\mathfrak{m}}^{T}[p^n]) = \#(\mathrm{Rad}_{S}^{T}[p^n]) = \#(\mathrm{Hom}(X_{T,k+n}^{S}/p^n, \mu_{p^n})) = \#(X_{T,k+n}^{S}/p^n).$$

La preuve du théorème 2.2.8 peut être modifiée pour tenir compte du décalage de k et conduit à la formule :

$$\#(X_{S,k+n}^{T}/p^n) = p^{(\rho_S^T n + \mu_S^T)(G:G_{k+n}) + \mathcal{O}(np^{n(d-1)})}.$$

Les invariants ρ_S^T, μ_S^T et ρ_T^S, μ_T^S interviennent donc dans les cardinaux de $\mathrm{Cl}_{\mathfrak{m}}^{T}[p^n]$ et de $\mathrm{Rad}_{\mathfrak{m}}^{T}[p^n]$ respectivement.

Il reste à calculer les cardinaux des termes de gauche. On s'appuie sur ce qui est fait dans **[23]**.

• Le lemme d'approximation nous permet de voir que $(\mathcal{R}/\mathcal{R}_{\mathfrak{m}})[p^n] \simeq \mathcal{U}^S/p^n$, où $\mathcal{U}^S$ désigne le produit sur les places de $S(K_{k+n})$ des complétés p-adiques des unités locales :

$$\mathcal{U}^S/p^n \simeq \prod_{v\in S_p(K_{k+n})} \mathbb{Z}/p^n\mathbb{Z}^{[K_{k+n,v}:\mathbb{Q}_p]} \prod_{v\in S(K_{k+n})} \mu_{p^n}.$$

La partie racines de l'unité contribue en $p^{\mathcal{O}(np^{n(d-1)})}$. En effet, comme K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique, aucune place n'est totalement décomposée dans K_∞/K. On fait alors appel au lemme 2.1.6 pour conclure que $\#(S(K_{k+n})) = \mathcal{O}(p^{n(d-1)})$.
Quant au produit restant, son cardinal est donné par $p^{\delta_S n(G:G_{k+n})}$.
Le quotient par les racines globales de l'unité ne change rien (cardinal en $p^{\mathcal{O}(n)}$) et on en déduit que

$$\#((\mathcal{R}/\mathcal{R}_{\mathfrak{m}})[p^n]/\mu_{p^n}) = p^{\delta_S n(G:G_{k+n})+\mathcal{O}(np^{n(d-1)})}.$$

• Le dernier cardinal à calculer et celui de $\mathcal{E}^T_{\mathfrak{m}}/p^n$. On a $\#(\mathcal{E}^T_{\mathfrak{m}}/p^n) = \#(\mathcal{E}^T/p^n)p^{\mathcal{O}(n)}$ car les $\mathbb{Z}_p$-modules $\mathcal{E}^T$ et $\mathcal{E}^T_{\mathfrak{m}}$ sont de même rang (regarder l'injection $\mathcal{E}^T/\mathcal{E}^T_{\mathfrak{m}} \hookrightarrow \prod_{v|\mathfrak{m}} U_v/U_v^{\mathfrak{m}_v}$) et leur torsion est composée de racines globales de l'unité, dont le cardinal évolue en $p^{\mathcal{O}(n)}$.
On trouve le cardinal voulu en appliquant le théorème de Dirichlet sur les T-unités qui donne

$$\#(\mathcal{E}^T/p^n) = p^{\frac{1}{2}[K:\mathbb{Q}]n(G:G_{k+n})+\mathcal{O}(np^{n(d-1)})}.$$

• Finalement, mettant ces calculs ensemble, il vient

$$\begin{array}{c} \rho_S^T + \frac{1}{2}[K:\mathbb{Q}] = \rho_T^S + \delta_S \\ \mu_S^T = \mu_T^S \end{array}.$$

La formule symétrique de l'énoncé concernant ρ provient du fait que $S \cup T$ contient les places p-adiques, ce qui implique $[K:\mathbb{Q}] = \delta_S + \delta_T$.

L'égalité entre r_S^T et r_T^S s'obtient en recoupant la formule sur ρ avec le théorème 3.2.7 à venir (et le théorème 3.2.6 pour $p = 2$). □

On peut déduire de ce résultat une formule de réflexion concernant le $\mathbb{Z}_p$-rang des modules $X^T_{S,n}$.

Corollaire 3.2.3. — *Sous les mêmes hypothèses, on a*

$$\mathrm{rk}_{\mathbb{Z}_p}(X^S_{T,n}) - \mathrm{rk}_{\mathbb{Z}_p}(X^T_{S,n}) = \left(\frac{\delta_T}{2} - \frac{\delta_S}{2}\right)(G:G_n) + \mathcal{O}(p^{n(d-1)}).$$

Démonstration. — Le corollaire 3.2.2 donne un lien entre ρ_S^T et ρ_T^S. On sait, d'après le théorème 2.2.8, que l'invariant ρ contrôle le $\mathbb{Z}_p$-rang de X_n d'où le résultat. □

3.2.2. Sans la $\mathbb{Z}_p$-extension cyclotomique. — On garde les mêmes hypothèses sur K_∞/K que dans la section précédente, sauf que K_∞ ne contient pas forcément la $\mathbb{Z}_p$-extension cyclotomique de K. Il est toujours possible d'appliquer les théorèmes de réflexion mais sur les quotients $X_{S,n}^T/p$ seulement (au lieu des quotients par p^n) car K_n ne contient en général que les racines p-ièmes de l'unité.
On utilisera les notations suivantes pour un ensemble fini S de places de K. On notera $s_\circ$ le nombre de places finies de S et $s_\mathbb{R}$ le nombre de places réelles de S. Etant donné une extension K_∞/K, on notera s^{dec} le nombre de places finies de S totalement décomposées dans K_∞/K.
La formule de réflexion sur laquelle on se base est la suivante :

Théorème 3.2.4 **(Gras, [9], théorème** $I.4.6$**).** — *Soit p un premier et K un corps de nombres contenant μ_p, de signature (r_1, r_2). On se donne S et T deux ensembles finis disjoints de places de K tels que $S \cup T$ contient les places p-adiques et les places réelles. On a alors la formule suivante, concernant les p-groupes des classes généralisés associés à K :*

$$\dim_{\mathbb{F}_p}(X_S^T/p) - \dim_{\mathbb{F}_p}(X_T^S/p) = s_\circ - t_\circ + \delta_S - r_1 - r_2 + \delta_{2,p}\, s_\mathbb{R},$$

où δ_S est le degré p-adique en S et où $\delta_{2,p} = 1$ ou 0 suivant que $p = 2$ ou non.

Prenant en compte la nature de cette dernière formule, on traitera séparément les cas $p = 2$ et $p \neq 2$.

- Cas $p = 2$:

On remarque tout d'abord que les places à l'infini n'ont aucune incidence sur l'invariant ρ.

Proposition 3.2.5. — *Pour un ensemble de places S, on note $S_\circ$ le sous-ensemble des places finies de S. Alors*

$$\rho_S^T = \rho_{S_\circ}^{T_\circ}.$$

Démonstration. — Il est clair que $X_{S,\infty}^T = X_{S_\circ,\infty}^{T'}$, avec T' l'ensemble de places T auquel on ajoute toutes les places réelles non contenues dans S.
Ecrivant T'_∞ pour l'ensemble des places réelles de K_∞ au dessus de T', la théorie du corps de classes donne une suite exacte

$$\bigoplus_{T'_\infty} \mathbb{Z}/2\mathbb{Z} \to X_{S_\circ,\infty}^{T_\circ} \to X_{S_\circ,\infty}^{T'} \to 0.$$

Elle conduit au résultat car le premier terme est de Λ-torsion. □

Théorème 3.2.6. — *Pour $p = 2$ et lorsque $S \cup T$ contient les places au dessus de 2 et les places réelles, les invariants d'Iwasawa de l'extension K_∞/K vérifient :*

$$\rho_S^T + r_S^T + \frac{\delta_T}{2} + t^{dec} + \frac{t_{\mathbb{R}}}{2} = \rho_T^S + r_T^S + \frac{\delta_S}{2} + s^{dec} + \frac{s_{\mathbb{R}}}{2}.$$

Démonstration. — Le théorème 3.2.4 nous indique que, pour tout n, la différence $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$ est donnée par :

$$s_\circ(K_n) - t_\circ(K_n) + \delta_S(K_n) - r_1(K_n) - r_2(K_n) + s_{\mathbb{R}}(K_n).$$

Il faut remarquer ici que l'on a

$$\begin{aligned} r_1(K_n) + r_2(K_n) &= \tfrac{1}{2}(r_1(K_n) + 2r_2(K_n) + r_1(K_n)) \\ &= \tfrac{1}{2}\left(\delta_S(K_n) + \delta_T(K_n) + s_{\mathbb{R}}(K_n) + t_{\mathbb{R}}(K_n)\right). \end{aligned}$$

Le passage à la deuxième ligne se justifie grâce à l'hypothèse sur l'ensemble de places $S \cup T$.
La quantité $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$ est alors égale à :

$$s_\circ(K_n) - t_\circ(K_n) + \frac{\delta_S(K_n)}{2} - \frac{\delta_T(K_n)}{2} + \frac{s_{\mathbb{R}}(K_n)}{2} - \frac{t_{\mathbb{R}}(K_n)}{2}.$$

Asymptotiquement, on a $\delta_S(K_n) = \delta_S(G : G_n)$ et $s_\circ(K_n) = s^{dec}(G : G_n) + \mathcal{O}(p^{n(d-1)})$, car le lemme 2.1.6 permet de négliger les places qui ne sont pas totalement décomposées. Le groupe G est sans torsion donc les places réelles de S sont totalement décomposées dans K_∞/K. On en déduit que $s_{\mathbb{R}}(K_n) = s_{\mathbb{R}}(G : G_n)$. Les mêmes considérations pour T conduisent à la formule suivante pour $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$:

$$\left(s^{dec} - t^{dec} + \frac{\delta_S}{2} - \frac{\delta_T}{2} + \frac{s_{\mathbb{R}}}{2} - \frac{t_{\mathbb{R}}}{2}\right)(G : G_n) + \mathcal{O}(p^{n(d-1)}).$$

On obtient la formule de l'énoncé en comparant avec le comportement asymptotique de $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$ donné par le théorème 2.2.8. □

- Cas $p \neq 2$:

La complexification des places réelles ne produit que de la 2-torsion dans les p-groupes $X_{S,n}^T$. Comme p est différent de 2 ici, les places réelles ne jouent aucun rôle et on peut considérer que S et T ne contiennent que des places finies.

Théorème 3.2.7. — *Si p est impair. On suppose que $\mu_p \subset K$ et que $S \cup T$ contient les places p-adiques. On a alors la formule suivante concernant les invariants ρ et r :*

$$\rho_S^T + r_S^T + \frac{\delta_T}{2} + t^{dec} = \rho_T^S + r_T^S + \frac{\delta_S}{2} + s^{dec}.$$

Démonstration. — Sous ces hypothèses, le terme de droite de la formule du théorème 3.2.4 devient :

$$s(K_n) - t(K_n) + \delta_S(K_n) - \frac{1}{2}[K_n : \mathbb{Q}].$$

La relation $[K_n : \mathbb{Q}] = \delta_S(K_n) + \delta_T(K_n)$ provenant de l'hypothèse sur $S \cup T$, ainsi que le lemme 2.1.6 qui permet de négliger les places qui ne sont pas totalement décomposées donnent alors l'évolution suivante pour $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$:

$$(s^{dec} - t^{dec} + \frac{\delta_S}{2} - \frac{\delta_T}{2})(G : G_n) + \mathcal{O}(p^{n(d-1)}).$$

On conclut en invoquant le théorème 2.2.8, qui donne l'évolution asymptotique de $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$. □

3.2.3. Calcul des invariants. — Dans **[23]**, les formules de réflexion débouchent sur le calcul de l'invariant ρ_S^T dans le cas CM, ainsi que sur des inégalités concernant les invariants μ_S^T lorsque S et T varient. Nous allons exhiber des résultats de ce type dans le cadre non-commutatif.
On suppose dans cette section que $p \neq 2$ ou que K est totalement imaginaire. On fait aussi l'hypothèse que K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique, ce qui assure les deux propriétés essentielles suivantes :

– Aucune place finie de K n'est totalement décomposée dans K_∞/K.
– L'extension K_∞/K vérifie la condition de Leopoldt faible.

La condition de Leopoldt faible exprime le fait que le groupe d'homologie $H_2(G_S(K_\infty), \mathbb{Z}_p)$ est nul dès lors que S contient les places p-adiques, avec $G_S(K_\infty)$ le groupe de Galois de la pro-p-extension S-ramifiée maximale de K_∞. Il est démontré dans **[33]** que cette condition est vérifiée en présence de la $\mathbb{Z}_p$-extension cyclotomique. On va utiliser une formulation équivalente de cette condition, en terme de rang d'unités, que l'on peut trouver dans **[29]** (proposition 4.9). On donne ici les grandes lignes de la démonstration. Pour un ensemble fini S de places de K contenant les places p-adiques et les places ramifiées dans K_∞/K, on note K_S la pro-p-extension maximale S-ramifiée de K et $G_S(K) = \mathrm{Gal}(K_S/K)$. Le corps K_∞ est alors inclu dans K_S et on a $X_{S,\infty} = \mathrm{Gal}(K_S/K_\infty)^{ab} = G_S(K_\infty)^{ab}$. La condition $H_2(G_S(K_\infty), \mathbb{Z}_p) = 0$ permet de relier le Λ-rang de $X_{S,\infty}$ à la caractéristique d'Euler-Poincaré de $G_S(K)$ qui est connue. On en déduit ensuite une formule pour $\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n})$ grâce au théorème 2.2.8, que l'on relie au défaut de Leopoldt $\mathcal{E}_{S,n} = \ker(\mathcal{E}_n \to \mathcal{U}_n^S)$ via la théorie du corps de classes. On rappelle que $\mathcal{E}_n$ est le tensorisé par $\mathbb{Z}_p$ du groupe des unités globales de K_n et que $\mathcal{U}_n^S$ désigne le produit des p-adifiés des unités locales en toutes les S-places de K_n (voir les notations avant le théorème 3.2.1).

On en déduit l'expression suivante de la condition de Leopoldt faible,

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{E}_{S,n}) = \mathcal{O}(p^{n(d-1)}).$$

Cette condition est bien évidemment vérifiée si on admet la conjecture de Leopoldt pour les étages K_n.

• Indépendance en T et en $S - S_p$.

Dans le cas de la $\mathbb{Z}_p$-extension cyclotomique, les invariants ρ_S^T et μ_S^T ne dépendent que de l'ensemble des places p-adiques de S, noté S_p. L'argument, provenant de la théorie du corps de classes, étant que les p-adifiés des sous-groupes de décomposition des places au-dessus de T et d'inertie des places de $S - S_p$ dans $X_{S,\infty}$ sont des $\mathbb{Z}_p$-modules de rang au plus 1. C'est toujours vrai dans le cas général mais les places à considérer sont alors en nombre infini, ce qui empêche de conclure directement. Il faut alors redescendre à $X_{S,n}^T$ pour démontrer :

Théorème 3.2.8. —

$$\begin{aligned} \rho_S^T &= \rho_{S_p}, \\ \mu_S^T &= \mu_{S_p}, \\ r_S^T &= r_{S_p}. \end{aligned}$$

Démonstration. — Comme remarqué juste avant, les sous-groupes de décomposition et d'inertie des places de $T \cup S - S_p$ dans $X_{S,n}$ sont de p-rang au plus 1. Ces sous-groupes sont asymptotiquement au nombre de $\mathcal{O}(p^{n(d-1)})$ car les places en question ne sont pas totalement décomposées dans K_∞/K (lemme 2.1.6). On peut conclure dans ce cas que

$$\#(X_{S,n}^T/p^n) = \#(X_{S_p,n}/p^n)p^{\mathcal{O}(np^{n(d-1)})}$$

et que

$$\dim_{\mathbb{F}_p}(X_{S,n}^T/p) = \dim_{\mathbb{F}_p}(X_{S_p,n}/p) + \mathcal{O}(p^{n(d-1)}).$$

Le théorème 2.2.8 permet d'en déduire les égalités annoncées. □

• Calcul de ρ_S^T.

On calcule l'invariant ρ_S^T lorsque les corps K_n sont totalement réels ou CM pour tout n, toujours en présence de la $\mathbb{Z}_p$-extension cyclotomique.

Pour le cas CM, on note τ la conjugaison complexe et $\hat{S} = S \cap S^\tau$. On a :

Théorème 3.2.9. —

i) Si K_∞ est totalement réel, alors

$$\rho_S^T = 0.$$

ii) Si K_n est CM pour tout n, alors

$$\rho_S^T = \frac{\delta_{\hat{S}}}{2}.$$

Démonstration. — Le théorème 3.2.8 permet de se limiter au calcul de ρ_S pour S un ensemble de places p-adique de K.
On obtient des informations sur ρ_S à l'aide de la formule

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}) = \rho_S(G : G_n) + \mathcal{O}(p^{n(d-1)})$$

du théorème 2.2.8.
La théorie du corps de classes relie cette quantité à un problème de plongement d'unités grâce à la suite exacte :

$$\mathcal{E}_n \to \mathcal{U}_n^S \to X_{S,n} \to X_n \to 0.$$

Les modules X_n sont les p-groupes des classes au sens classique et sont en particulier de $\mathbb{Z}_p$-torsion. On en déduit

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}) = \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)).$$

C'est ce dernier conoyau que l'on va calculer.

i) On commence par traiter le cas totalement réel.
On a

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)) \leqslant \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^{\mathrm{Pl}_p})),$$

avec Pl_p l'ensemble des places p-adiques.
Asymptotiquement, le $\mathbb{Z}_p$-rang du noyau de cette dernière application évolue en $\mathcal{O}(p^{n(d-1)})$ d'après la condition de Leopoldt. Comme les corps K_n sont totalement réels, $\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{E}_n) = [K : \mathbb{Q}](G : G_n) - 1$ d'après le théorème de Dirichlet et $\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^{\mathrm{Pl}_p}) = [K : \mathbb{Q}](G : G_n)$. On en tire que le $\mathbb{Z}_p$-rang de ce dernier conoyau évolue en $\mathcal{O}(p^{n(d-1)})$, donc que $\rho_S = 0$.

ii) On suppose maintenant que K_n est CM pour tout n et on commence par traiter le cas où S est stable par τ.
La composante $\mathbb{Z}_p$-libre de l'image de $\mathcal{E}_n \to \mathcal{U}_n^S$ est contenue dans la partie $+$ des unités locales. On a ici $\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{E}_n) = r_2(G : G_n) - 1$ et $\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^{\mathrm{Pl}_p})^+ = r_2(G : G_n)$. La condition de Leopoldt permet de conclure que

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to (\mathcal{U}_n^S)^+)) &\leqslant \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to (\mathcal{U}_n^{\mathrm{Pl}_p})^+)) \\ &= \mathcal{O}(p^{n(d-1)}). \end{aligned}$$

On a alors

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)) &= \mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^S)^- + \mathcal{O}(p^{n(d-1)}) \\ &= \tfrac{\delta_S}{2}(G : G_n) + \mathcal{O}(p^{n(d-1)}). \end{aligned}$$

Ainsi, $\rho_S = \frac{\delta_S}{2}$.

A partir de maintenant, on ne suppose plus que S est stable par τ.
Pour une place v d'un corps CM, l'action de τ nous informe qu'une unité d'image triviale dans U_v est aussi d'image triviale dans U_{v^τ}. Notons $\check{S} = S \cup S^\tau$,

de telle sorte que pour tout n, $\mathcal{E}_{S,n} = \ker(\mathcal{E}_n \to \mathcal{U}_n^S)$ et $\mathcal{E}_{\check{S},n} = \ker(\mathcal{E}_n \to \mathcal{U}_n^{\check{S}})$ sont égaux.
Le diagramme suivant permet de comparer $\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)$ à $\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^{\check{S}})$, qui est connu car $\check{S}$ est stable par τ :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{E}_{S,n} & \longrightarrow & \mathcal{E}_n & \longrightarrow & \mathcal{U}_n^S & \longrightarrow & \mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S) \longrightarrow 0 \\ & & \| & & \| & & & & \\ 0 & \longrightarrow & \mathcal{E}_{\check{S},n} & \longrightarrow & \mathcal{E}_n & \longrightarrow & \mathcal{U}_n^{\check{S}} & \longrightarrow & \mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^{\check{S}}) \longrightarrow 0. \end{array}$$

On a donc

$$\begin{array}{rcl} \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)) & = & \mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^S) - \mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^{\check{S}}) + \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^{\check{S}})) \\ & = & (\delta_S - \delta_{\check{S}} + \frac{\delta_{\check{S}}}{2})(G : G_n) + \mathcal{O}(p^{n(d-1)}) \\ & = & (\frac{\delta_{\hat{S}} - \delta_{\check{S}}}{2} + \frac{\delta_{\check{S}}}{2})(G : G_n) + \mathcal{O}(p^{n(d-1)}) \\ & = & \frac{\delta_{\hat{S}}}{2}(G : G_n) + \mathcal{O}(p^{n(d-1)}), \end{array}$$

d'où $\rho_S = \frac{\delta_{\hat{S}}}{2}$. □

- Calcul de μ_S^T et r_S^T.

Les calculs sur l'invariant μ contenus dans **[23]** sont encore valables ici et peuvent être étendus à r. Nous les retraçons succintement, les démonstrations étant identiques à celles dans le cas de la $\mathbb{Z}_p$-extension cyclotomique.
On se place dans le cadre cyclotomique, c'est-à-dire que l'on suppose que K contient les racines p-ièmes de l'unité (μ_4 si $p = 2$) et que K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique. Cette condition est ici nécessaire pour obtenir des informations sur μ et r via les formules de réflexion.

Proposition 3.2.10. — *Notons* Pl_p *l'ensemble des places p-adiques et* $S_p = S \cap \mathrm{Pl}_p$. *Sous les hypothèses précédentes, on a :*

i)
$$\mu_S^T = \mu_{S_p} = \mu_{\mathrm{Pl}_p - S_p},$$
$$r_S^T = r_{S_p} = r_{\mathrm{Pl}_p - S_p}.$$

ii) Si de plus K_n *est CM pour tout n et* S_p *est stable par conjugaison complexe, alors*
$$\mu_S^T \leqslant \mu,$$
$$r_S^T \leqslant r,$$
où μ *et* r *sont les invariants correspondant au cas* $S = T = \emptyset$.

Démonstration. — *i)* On utilise le théorème 3.2.8 et le corollaire 3.2.2 pour écrire :
$$\mu_S^T = \mu_{S_p} = \mu_{S_p}^{\mathrm{Pl}_p - S_p} = \mu_{\mathrm{Pl}_p - S_p}^{S_p} = \mu_{\mathrm{Pl}_p - S_p},$$

ainsi que les mêmes égalités pour r.

ii) Les hypothèses permettent d'utiliser la preuve du théorème 13 de [**23**] sans changement. □

BIBLIOGRAPHIE

[1] P.N. Balister, S. Howson, "Note on Nakayama's Lemma for Compact Λ-modules", *Asian Math. Jour.,* 1, 224 – 229, 1997.

[2] A. Brumer, "Pseudocompact algebras, profinite groups and class formations", *J. Algebra,* 4, 442 – 470, 1966.

[3] J. Coates, P. Schneider, R. Sujatha, "Modules over Iwasawa algebras", *Journal of the inst. of math. Jussieu, no.* 2, 73 – 108, 2003.

[4] A. Cuoco, P. Monsky, "Class numbers in $\mathbb{Z}_p^d$-extensions.", *Math. Ann.,* 255, *no.* 2, 235 – 258, 1981.

[5] P. Deligne, K. Ribet, "Values of abelian L-functions at negative integers over totally real fields.", *Invent. Math.* 59, *no.* 3, 227 – 286, 1980.

[6] J.D. Dixon, M.P.F. Du Sautoy, A. Mann, D. Segal, "Analytic pro-p groups", *Cambridge studies in advanced math., Second edition tome* 61, 1999.

[7] B. Ferrero, L. Washington, "The Iwasawa invariant μ_p vanishes for abelian number fields.", *Ann. of Math. (2)* 109, *no.* 2, 377 – 395, 1979.

[8] P. Gabriel, "Des catégories abéliennes", *Bull. Soc. Math. France,* 90, 323 – 448, 1962.

[9] G. Gras, "Class Field Theory", *Springer,* 2003.

[10] G. Gras, "Théorèmes de réflexion", *Jour. Th. Nombres de Bordeaux,* 10 *no.* 2, 399 – 499, 1998.

[11] Y. Hachimori, R. Sharifi, "On the failure of pseudo-nullity of Iwasawa modules", *J. Algebraic Geom.,* 14, *no.* 3, 567 – 591, 2005.

[12] M. Harris, "p-adic representations arising from descent on abelian varieties", *Compositio Math., tome* 39*, no.* 2*,* 177 − 245*,* 1979.

[13] M. Harris, "Correction to p-adic representations arising from descent on abelian varieties", *Compositio Math., tome* 121*,* 105 − 108*,* 2000.

[14] R. Hartshorne, "Algebraic Geometry", *Grad. text in adv. math., Springer,* 2000.

[15] S. Howson, "Euler characteristics as invariants of Iwasawa modules", *Proc. London Math. Soc., (*3*),* 85*,* 634 − 658*,* 2002.

[16] K. Iwasawa, "On $\mathbb{Z}_l$-extension of algebraic number fields", *Ann. of Math.,* 98*,* 246 − 326*,* 1973.

[17] K. Iwasawa, "On Γ-extensions of algebraic number fields", *Bull. Amer. Math. Soc.* 65*,* 183 − 226*,* 1959.

[18] K. Iwasawa, "Lectures on p-adic L-functions.", *Annals of Mathematics Studies, No.* 74*. Princeton University Press; University of Tokyo Press,* 1972.

[19] U. Jannsen, "Iwasawa modules up to isomorphism", *Adv. Stud. in pure math.* 17*, Alg. Numb. Th. - In honor of K. Iwasawa,* 171 − 207*,* 1989.

[20] J-F Jaulent, "L'arithmétique des l-extensions" (Thèse d'état) *Pub. Math. Fac. Sci. Besançon Th. Nombres* 1985 − 86*,* 1986.

[21] J-F Jaulent, "Théorie l-adique globale du corps de classes" *Jour. Th. Nombres Bordeaux,* 10*, no.* 2*,* 355 − 397*,* 1998.

[22] J-F. Jaulent, "Généralisation d'un théorème d'Iwasawa", *Jour. Th. Nombres de Bordeaux,* 17 *no.* 2*,* 2005.

[23] J-F. Jaulent, C. Maire, "Sur les invariants d'Iwasawa des tours cyclotomiques", *Canadian Math. Bull.* 46*,* 178 − 190*,* 2003.

[24] J-F. Jaulent, C. Maire, G.Perbet, "Sur les formules asymptotiques le long des $\mathbb{Z}_\ell$-extensions", *preprint,* 2011.

[25] M. Kakde, "The main conjecture of Iwasawa theory for totally real fields", *preprint,* 2011.

[26] M. Lazard, "Groupes analytiques p-adiques", *Publ. math. IHES, no.*26*,* 389 − 603*,* 1965.

[27] L. Lesieur et R. Croisot, "Sur les anneaux premiers noethériens à gauche", *Ann. Sci. ENS, no.* 76*,* 161 − 183*,* 1959.

[28] C. Maire, "Sur la dimension cohomologique des pro-p-extensions des corps de nombres", *Jour. Th. Nombres de Bordeaux,* 17*, no.* 2*,* 575 − 606*,* 2005.

[29] C. Maire, "Plongements locaux et extensions de corps de nombres", *Int. Jour. of Num. Th., no.* 7*,* 721 − 738*,* 2011.

[30] B. Mazur, A. Wiles, "Class fields of abelian extensions of $\mathbb{Q}$.", *Invent. Math.* 76*, no.* 2*,* 179 − 330*,* 1984.

[31] J. Neukirch, A. Schmidt et K. Wingberg, "Cohomology of number fields", *Springer-Verlag,* 2000.

[32] A. Neumann, "Completed group algebras without zero divisors", *Arch. Math. no.*51*,* 496 − 499*,* 1988.

[33] T. Nguyen Quang Do, "Formations de classes et modules d'Iwasawa", *Lecture Notes in Math., Number theory, Noordwijkerhout* 1983*, no.* 1068*,* 167 − 185*,* 1983.

[34] G. Perbet, "Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques", *Algebra and Number Theory, à paraître.*

[35] L. Ribes et P. Zalesskii, "Profinite groups", *Springer-Verlag,* 2000.

[36] J-P. Serre, d'après K. Iwasawa "Classes des corps cyclotomiques", *Séminaire Bourbaki, décembre* 1958.

[37] J-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.", *Invent. Math.* 15*, no.* 4*,* 259 − 331*,* 1972.

[38] O. Venjakob, "On the structure theory of the Iwasawa algebra of a p-adic Lie group ", *J. Eur. Math. Soc. (JEMS)* 4*, no.* 3*,* 271 − 311*,* 2002.

[39] O. Venjakob, "On the Iwasawa theory of p-adic Lie extensions", *Compos. Math.* 138*,* 1 − 54*,* 2003.

[40] L. Washington, "Introduction to cyclotomic fields. Second edition", *Springer-Verlag,* 1997.

[41] A. Wiles, "The Iwasawa conjecture for totally real fields.", *Ann. of Math. (2)* 131*, no.* 3*,* 493 − 540*,* 1990.