Propriétés algébriques des unités de Stark

Coline Wiatrowski

N° d'ordre NNT : 2018LYSE1154

THÈSE DE DOCTORAT DE L'UNIVERSITÉ DE LYON
opérée au sein de
l'Université Claude Bernard Lyon 1

École Doctorale ED512
InfoMaths

Spécialité de doctorat : Mathématiques

Soutenue publiquement le 21 septembre 2018, par :
Coline WIATROWSKI

Propriétés algébriques des unités de Stark

Devant le jury composé de :

M. ANGLÈS Bruno	Professeur, Université de Caen	Rapporteur
Mme BELIAEVA Tatiana	Maîtresse de Conférences, Université de Strasbourg	Examinatrice
M. BELLIARD Jean-Robert	Maître de Conférences, Université de Franche-Comté	Codirecteur de thèse
Mme DAVID Agnès	Maîtresse de Conférences, Université de Franche-Comté	Examinatrice
M. PELLARIN Federico	Professeur, Université Jean Monnet	Examinateur
Mme PERRIN-RIOU Bernadette	Professeure Émérite, Université Paris Sud	Examinatrice
M. ROBLOT Xavier-François	Maître de Conférences, Université Lyon 1	Directeur de thèse
M. ROQUES Julien	Professeur, Université Lyon 1	Examinateur

Après avis des rapporteurs :

M. ANGLÈS Bruno	Professeur, Université de Caen
M. SANDS Jonathan	Professeur, Université du Vermont

Table des matières

Chapitre 0

Introduction

À la fin du 19ème siècle, Kronecker énonça le résultat suivant, dans un premier temps pour les extensions cycliques, puis pour les extensions abéliennes.

Théorème 0.0.1 (Théorème de Kronecker-Weber)**.** *Soit $K/\mathbb{Q}$ une extension abélienne de corps de nombres.*
Alors il existe une racine primitive de l'unité ζ telle que $K \subset \mathbb{Q}(\zeta)$.

Bien que ce théorème soit attribué à Kronecker et Weber, leurs deux démonstrations étaient incomplètes et le théorème fut démontré intégralement pour la première fois par Hilbert en 1896.
Quelques années plus tard, lors du deuxième congrès international des mathématiciens qui eut lieu à Paris en 1900, Hilbert énonça une liste de 23 problèmes ouverts, désormais connus sous le nom de problèmes de Hilbert. Parmi ces problèmes, Hilbert reformula le Kronecker Jugendtraum (rêve de jeunesse de Kronecker), que Kronecker avait mentionné dans une lettre à Dedekind en 1880 et qui cherchait à généraliser le théorème de Kronecker-Weber. Ce théorème peut être reformulé ainsi.

Théorème 0.0.2 (Reformulation du théorème de Kronecker-Weber)**.** *Considérons la fonction analytique*

$$\exp : \begin{cases} \mathbb{Q} \to \overline{\mathbb{Q}} \\ x \mapsto e^{i\pi x} \end{cases} .$$

Les valeurs de cette fonction prises en certains rationnels engendrent toutes les extensions abéliennes de $\mathbb{Q}$.

C'est cette formulation que Hilbert souhaitait voir généralisée.

12ème problème de Hilbert. *Soit k un corps de nombres.*
Existe-t-il des fonctions analytiques de k dans $\bar{k}$ dont des valeurs spéciales engendrent toutes les extensions abéliennes de k ?

Outre le théorème de Kronecker-Weber, une motivation pour cet énoncé général provient du résultat suivant pour les corps quadratiques imaginaires.

Théorème 0.0.3. *Soit k un corps de nombres quadratique imaginaire.*
Alors toutes les extensions abéliennes de k sont engendrées par des valeurs spéciales de la fonction exp*, de la fonction j et de la fonction $\wp$ de Weierstrass.*

Dans le cas général, le 12ème problème de Hilbert reste ouvert. Pour les corps de nombres totalement réels, la démonstration de la conjecture abélienne de Stark de rang 1 apporterait une solution.
On considère une extension abélienne de corps de nombres K/k de groupe de Galois G et $\mathcal{S}$ un ensemble de places de k contenant les places infinies $\mathcal{S}_\infty(k)$ de k et les places finies $\mathcal{S}_{ram}(K/k)$ qui sont ramifiées dans K/k. On note ω_K le nombre de racines de l'unité de K. Pour tout caractère χ du groupe abélien G, on définit une fonction L de Hecke en posant pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$

$$L_{K/k,\mathcal{S}}(\chi, s) = \prod_{\mathfrak{p}\notin\mathcal{S}} \frac{1}{1 - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\chi(\sigma_\mathfrak{p})}$$

puis en prolongeant analytiquement cette fonction à $\mathbb{C}$.

Conjecture 0.0.4 (Conjecture abélienne de Stark de rang 1 dans le cas infini)**.** *On suppose que $\mathcal{S}$ contient une place infinie v totalement décomposée dans K/k et on note w une place au-dessus de v dans K. On suppose également que* $\mathrm{card}(\mathcal{S}) \geq 2$*.*
Alors il existe une $\mathcal{S}$-unité $\varepsilon_{K/k,\mathcal{S},w} \in \mathcal{U}_{K/k,v}$ telle que

1. *pour tout $\sigma \in G$, on a*

$$\log\left|\sigma(\varepsilon_{K/k,\mathcal{S},w})\right|_w = -\omega_K \zeta'_{K/k,\mathcal{S}}(\sigma, 0)$$

2. *et l'extension $K\left(\varepsilon_{K/k,\mathcal{S},w}^{1/\omega_K}\right)/k$ est abélienne.*

Une telle unité s'appelle unité de Stark associée à l'extension K/k, l'ensemble de places $\mathcal{S}$ et la place w.

On suppose que le corps k est totalement réel. De plus, on suppose que la conjecture est vérifiée pour toutes les extensions abéliennes de k. On a alors le résultat suivant.

Théorème 0.0.5. *Il existe des unités de Stark ε_1, ε_2,..., ε_r, associées à $\mathcal{S} = \mathcal{S}_\infty(k) \cup \mathcal{S}_{ram}(K/k)$ telles que $K \subset k(\varepsilon_1, \varepsilon_2, ..., \varepsilon_r)$.*

Afin de mieux comprendre ces unités dont l'existence repose sur une conjecture, nous nous intéressons dans cette thèse à leurs propriétés algébriques.

Dans notre premier chapitre, nous commençons par présenter des notions de base sur les anneaux de groupe et les G-modules qui nous permettent ensuite de définir la cohomologie de Tate des groupes finis. Nous étudions ensuite la p-partie et la partie moins d'un G-module et leurs comportements respectifs vis-à-vis de la cohomologie de Tate. Enfin, nous définissons l'idéal initial de Fitting et démontrons ses propriétés.
Le deuxième chapitre constitue une mise au clair des trois notions de χ-composantes associées à un $\mathbb{Z}_p[G]$-module, χ désignant un caractère irréductible sur $\overline{\mathbb{Q}}_p$ de G. Dans un premier temps nous étudions les caractères p-adiques de G irréductibles sur $\overline{\mathbb{Q}}_p$ puis ceux qui sont irréductibles sur $\mathbb{Q}_p$. Ceci nous permet notamment d'introduire la notion d'idempotent associé à un caractère qui est centrale dans la définition de la troisième χ-composante. Les deux premières composantes, appelées χ-quotient et χ-partie, sont ici définies par propriété universelle, mais l'on donne également pour chacune d'elles deux réalisations explicites de ces propriétés universelles dont l'une qui justifie leur nom respectif de partie et de quotient. Nous démontrons que dans le cas semi-simple, ces trois notions sont canoniquement isomorphes.
Dans le chapitre suivant, on présente plus en détail et avec un peu plus de généralité que dans cette introduction la conjecture abélienne de Stark de rang 1. Nous commençons par une introduction historique autour de la formule analytique des classes de Dirichlet, afin d'en énoncer une généralisation formulée par Stark dans sa conjecture principale. Nous nous intéressons ensuite au raffinement abélien de cette conjecture, qui prédit l'existence des unités de Stark. Nous supposons pour la suite de la thèse la conjecture abélienne de Stark vérifiée, et nous pouvons alors énoncer les formules établies par Rubin et Roblot concernant l'indice de sous-groupes engendrés par des unités de Stark à l'intérieur du groupe des unités.
Dans le chapitre 4, nous nous plaçons dans le cadre suivant :
– K/k est une extension abélienne de corps de nombres,
– k est un corps de nombres totalement réel différent de $\mathbb{Q}$,
– $[K : K^+] = 2$, on note τ le générateur de $\mathrm{Gal}(K/K^+)$,
– $\mathcal{S}$ est un ensemble fini de places de k,
– il existe une unique place infinie v de k qui reste réelle dans K,
– $\mathcal{S}_\infty(k) \cup \mathcal{S}_{ram}(k) \subset \mathcal{S}$,
– tous les idéaux premiers dans $\mathcal{S}_{K^+}$ sont inertes ou ramifiés dans K/K^+.
À l'aide des formules d'indice du chapitre précédent, nous établissons le résultat suivant.

Théorème (Théorème 4.2.1 semi-simple faible)**.** *Soit p un nombre premier ne divisant pas* $\mathrm{card}(G)$.
Alors

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right).$$

Nous en déduisons alors une version plus forte.

Théorème (Théorème 4.2.7 semi-simple fort)**.** *Soit p un nombre premier ne divisant pas* card(G).
Alors on a l'isomorphisme de $\mathbb{Z}_p\,[G]$*-modules suivant*

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}\,[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p \simeq \mathbb{Z}_p\,[G]^-\,/\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(Cl_K^-\otimes\mathbb{Z}_p\right).$$

Nous formulons la conjecture locale faible 4.1.2 selon laquelle le résultat du théorème semi-simple faible reste vrai si p est un nombre premier impair divisant card(G). Nous démontrons alors un théorème moins fort de simultanée principalité.

Théorème (Théorème 4.3.1)**.** *Soit p un nombre premier impair.*
Alors les deux affirmations suivantes sont équivalentes

1. $\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}\,[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)$ *est un idéal principal de* $\mathbb{Z}_p\,[G]$ *engendré par un élément non diviseur de* 0*,*
2. $\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right)$ *est un idéal principal de* $\mathbb{Z}_p\,[G]$ *engendré par un élément non diviseur de* 0*.*

Dans le dernier chapitre, nous expliquons comment construire algorithmiquement des extensions vérifiant les conditions imposées dans le chapitre 4 en utilisant la théorie explicite du corps de classes. Nous résumons enfin les exemples numériques obtenus, pour lesquels la conjecture faible est toujours vérifiée.

Chapitre 1

Outils algébriques

Cette section a pour but d'énoncer les résultats algébriques utilisés dans cette thèse. Le nombre p y sera toujours premier.

1.1 Anneau de groupe et G-module

Dans cette section, G désigne un groupe noté multiplicativement et A un anneau commutatif.

Définition 1.1.1. *On note $A[G]$ l'ensemble des sommes formelles presque nulles*

$$\sum_{g\in G} \alpha_g g,\ \alpha_g \in A.$$

Muni de l'addition

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$$

et du produit de convolution

$$\Big(\sum_{g\in G} \alpha_g g\Big)\Big(\sum_{g\in G} \beta_g g\Big) = \sum_{(g,g')\in G^2} \alpha_g \beta_{g'}\, gg',$$

$A[G]$ est un anneau d'unité 1_G, appelé anneau de groupe de G.

Dorénavant, le groupe G est supposé abélien. L'anneau de groupe $A[G]$ est alors un anneau commutatif. Nous utiliserons dans la suite des anneaux de groupes dont l'anneau de base est $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$ ou $\mathbb{Q}_p$.

Définition 1.1.2. *On appelle morphisme d'augmentation de G le morphisme $\varepsilon : A[G] \to A$ défini par*

$$\varepsilon\Big(\sum_{g\in G} \alpha_g g\Big) = \sum_{g\in G} \alpha_g.$$

Son noyau est noté I_G et appelé idéal d'augmentation de G.

Proposition 1.1.3. *L'idéal d'augmentation I_G est engendré sur A par les $g - 1_G$, où g parcourt G.*

Démonstration. Soit $\sum_{g\in G} \alpha_g g \in I_G$. On a

$$\sum_{g\in G} \alpha_g = 0$$

donc

$$\alpha_{1_G} = -\sum_{g\in G\setminus\{1_G\}} \alpha_g$$

et

$$\sum_{g\in G} \alpha_g g = \sum_{g\in G\setminus\{1_G\}} \alpha_g (g - 1_G).$$

□

Définition 1.1.4. *On appelle G-module un $\mathbb{Z}[G]$-module. De manière équivalente, un G-module M est un groupe additif muni d'une action de G compatible avec sa loi de groupe, c'est-à-dire telle que pour tout $g \in G$ et pour tous $m, m' \in M$, on a*

$$g(m + m') = gm + gm'.$$

On dit qu'un G-module est libre s'il est libre en tant que $\mathbb{Z}[G]$-module.

On remarque que si M est un G-module et F un sous-groupe de G, alors M est également un F-module.

Définition 1.1.5. *Soit M un G-module.*
On note

$$M^G = \{m \in M \text{ tel que } gm = m \text{ pour tout } g \in G\}$$

le sous-module de M des éléments invariants par l'action de G.

Pour tout G-module M, M^G est un G-module sur lequel G agit trivialement, on peut donc le considérer comme un groupe abélien sans perdre d'information. On peut alors définir un foncteur covariant $\mathcal{F}^G$ de la catégorie des G-modules vers la catégories des groupes abéliens de la façon suivante : pour tout G-module M on note

$$\mathcal{F}^G(M) = M^G$$

et pour tout morphisme de G-modules $f : M \to N$, l'action de G commutant avec f, on a $f(M^G) \subset N^G$, donc on peut définir

$$\mathcal{F}^G(f) : M^G \to N^G$$

le morphisme de groupes abéliens obtenu à partir de f par restriction à M^G et corestriction à N^G.

Proposition 1.1.6. *Le foncteur des G-invariants $\mathcal{F}^G$ est un foncteur exact à gauche de la catégorie des G-modules vers la catégorie des groupes abéliens.*

Démonstration. Soit

$$0 \to M \xrightarrow{\varphi} N \xrightarrow{\psi} P$$

une suite exacte de G-modules. Alors $\mathcal{F}^G(\varphi)$ est injective car φ l'est. De plus

$$\mathcal{F}^G(\psi) \circ \mathcal{F}^G(\varphi) = \mathcal{F}^G(\psi \circ \varphi) = 0$$

donc

$$\mathrm{Im}(\mathcal{F}^G(\varphi)) \subset \mathrm{Ker}(\mathcal{F}^G(\psi)).$$

Soit $n \in \mathrm{Ker}(\mathcal{F}^G(\psi)) \subset \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$, il existe $m \in M$ tel que $\varphi(m) = n$. Comme $n \in N^G$, pour tout $g \in G$, on a

$$\varphi(gm) = g\varphi(m) = gn = n = \varphi(m)$$

et comme φ est injective, on en déduit que $gm = m$, et donc que $m \in M^G$. On a donc

$$\mathrm{Ker}(\mathcal{F}^G(\psi)) \subset \mathrm{Im}(\mathcal{F}^G(\varphi)).$$

Ainsi, la suite de groupes abéliens

$$0 \to M^G \to N^G \to P^G$$

est exacte. □

Dans cette thèse on adoptera la convention de Nicolas Bourbaki selon laquelle les anneaux sont supposés unitaires. Dans le cas contraire, on parlera de pseudo-anneaux.

Notation. Pour tout anneau A et tous A-modules M et N, on note $\mathrm{Hom}_A(M,N)$ l'ensemble des morphismes de A-modules de M vers N. Il s'agit d'un A-module. Pour $A = \mathbb{Z}$, on notera simplement $\mathrm{Hom}(M,N)$ l'ensemble des morphismes de groupes abéliens de M vers N.

On a le résultat classique suivant, dont on peut retrouver la démonstration dans le chapitre I.6 de [Mac67].

Proposition 1.1.7. *Soit A un anneau commutatif et M un A-module.*
Alors $\mathrm{Hom}_A(M,-)$ est un foncteur covariant exact à gauche de la catégorie des A-modules vers elle-même.

Définition 1.1.8. *Soit A un anneau commutatif et M un A-module.*
On dit que M est projectif si $\mathrm{Hom}_A(M,-)$ est un foncteur exact, autrement dit pour tout morphisme surjectif de A-modules $s : N \to P$ et tout morphisme de A-modules $f : M \to P$, il existe un morphisme de A-modules h tel que $f = s \circ h$.

Proposition 1.1.9. *Soit M et N deux G-modules.*
Alors on a

$$\mathrm{Hom}_{\mathbb{Z}[G]}(M,N) = \mathrm{Hom}(M,N)^G.$$

Et en particulier, pour tout G-module M, en considérant $\mathbb{Z}$ comme un G-module sur lequel l'action est triviale, on a

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},M) = \mathrm{Hom}(\mathbb{Z},M)^G \simeq M^G.$$

On peut retrouver ainsi l'exactitude à gauche du foncteur $\mathcal{F}^G$.
Après avoir défini le plus grand sous-module d'un G-module sur lequel G agit trivialement, nous allons nous intéresser au plus grand quotient d'un module sur lequel G agit trivialement.

Définition 1.1.10. *Soit M un G-module.*
On note

$$M_G = M/I_G M$$

le G-module des co-invariants de M.

Pour tout G-module M, M_G est un G-module sur lequel G agit trivialement, on peut donc le considérer comme un groupe abélien sans perdre d'information. On peut alors définir un foncteur covariant $\mathcal{F}_G$ de la catégorie des G-modules vers la catégories des groupes abéliens de la façon suivante : pour tout G-module M on note

$$\mathcal{F}_G(M) = M_G$$

et pour tout morphisme de G-modules $f : M \to N$, on note

$$\mathcal{F}_G(f) : M_G \to N_G$$

le morphisme de groupes abéliens obtenu à partir de f par passage au quotient :

$$\forall m \in M,\ \mathcal{F}_G(f)(m + I_G M) = f(m) + I_G N.$$

Proposition 1.1.11. *Le foncteur des G-co-invariants $\mathcal{F}_G$ est un foncteur exact à droite de la catégorie des G-modules vers la catégorie des groupes abéliens.*

Démonstration. Soit

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} P \to 0$$

une suite exacte de G-modules. Alors $\mathcal{F}_G(\psi)$ est surjective comme quotient de ψ qui est surjective. De plus $\mathcal{F}_G(\psi) \circ \mathcal{F}_G(\varphi) = \mathcal{F}_G(\psi \circ \varphi) = 0$ donc

$$\mathrm{Im}(\mathcal{F}_G(\varphi)) \subset \mathrm{Ker}(\mathcal{F}_G(\psi)).$$

Soit $n + I_G N \in \mathrm{Ker}(\mathcal{F}_G(\psi))$, on a $\psi(n) \in I_G P$, donc $\psi(n) = ap$, avec $a \in I_G$ et $p \in P$. Comme ψ est surjective, $p = \psi(n')$ avec $n' \in N$. On a alors $\psi(n) = a\psi(n') = \psi(an')$, donc $n - an' \in \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$. On a donc $n + I_G N \in \mathrm{Im}(\varphi) + I_G N = \mathrm{Im}(\mathcal{F}_G(\psi))$, et donc

$$\mathrm{Ker}(\mathcal{F}_G(\psi)) \subset \mathrm{Im}(\mathcal{F}_G(\psi)).$$

Ainsi, la suite de groupes abéliens

$$M_G \to N_G \to P_G \to 0$$

est exacte. □

Notation. Pour tout anneau A et tous A-modules M et N, on note $M \underset{A}{\otimes} N$ le produit tensoriel sur A des modules A et N. Pour $A = \mathbb{Z}$, on le notera simplement $M \otimes N$. Si M et N sont deux G-modules, alors $M \otimes N$ est doté de la structure de G-module définie par l'action diagonale de G :

$$g(m \otimes n) = gm \otimes gn.$$

Si seul M est un G-module, on peut alors doter N de l'action trivial de G. Dans ce cas, l'action diagonale de G sur $M \otimes N$ n'est autre que l'action à gauche.

Remarque. Les structures de G-modules de $M \otimes N$ et $M \underset{\mathbb{Z}[G]}{\otimes} N$ sont donc différentes puisque cette dernière est donnée par $g(m \underset{\mathbb{Z}[G]}{\otimes} n) = gm \underset{\mathbb{Z}[G]}{\otimes} n = m \underset{\mathbb{Z}[G]}{\otimes} gn$.

Proposition 1.1.12. *Soit A un anneau commutatif et M un A-module.*
Alors $M \underset{A}{\otimes} -$ est un foncteur covariant exact à droite de la catégorie des A-modules vers elle-même.

Définition 1.1.13. *Soit A un anneau commutatif et M un A-module.*
On dit que M est un A-module plat si $M \underset{A}{\otimes} -$ est un foncteur exact.

Proposition 1.1.14. *Soit M et N deux G-modules.*
Alors on a l'isomorphisme de groupes abéliens

$$M \underset{\mathbb{Z}[G]}{\otimes} N \simeq (M \otimes N)_G .$$

Et en particulier, pour tout G-module M, en considérant $\mathbb{Z}$ comme un G-module sur lequel l'action est triviale, on a l'isomorphisme de groupes abéliens

$$\mathbb{Z} \underset{\mathbb{Z}[G]}{\otimes} M \simeq M_G.$$

On peut retrouver ainsi l'exactitude à gauche du foncteur $\mathcal{F}_G$.

Définition 1.1.15. *Soit F un sous-groupe fini de G.*
On appelle norme de F l'élément

$$N_F = \sum_{g \in F} g \in \mathbb{Z}[F] \subset \mathbb{Z}[G] .$$

Si M est un G-module, on définit l'application norme de F sur M par

$$N_{F,M} : \begin{cases} M \to M \\ m \mapsto \sum\limits_{g \in F} gm \end{cases} .$$

Définition 1.1.16. *Soit X un groupe abélien. On peut alors munir le groupe abélien $\mathrm{Hom}(\mathbb{Z}[G], X)$ d'une structure de G-module en faisant agir G à la source, c'est-à-dire que pour tout $l \in \mathrm{Hom}(\mathbb{Z}[G], X)$ et pour tout $g \in G$, on pose $gl : a \mapsto l(ga)$.*
On appelle module co-induit un tel G-module.

Définition 1.1.17. *Soit X un groupe abélien. On peut alors munir le groupe abélien $\mathbb{Z}[G] \otimes X$ d'une structure de G-module en faisant agir G à gauche.*
On appelle module induit un tel G-module.

Exemple. On suppose que F est un sous-groupe distingué de G. Alors G est un F-module induit. En effet, on a les isomorphisme de $\mathbb{Z}$-modules suivants

$$\mathbb{Z}[G] \simeq \mathbb{Z}[F]^{\mathrm{card}(G/H)} \simeq \mathbb{Z}[F] \otimes \mathbb{Z}^{\mathrm{card}(G/F)}.$$

Proposition 1.1.18. *On suppose que G est un groupe fini et M un G-module. Alors M est un G-module induit si et seulement si M est un G-module co-induit.*

Démonstration. Soit X un groupe abélien. On peut définir le morphisme de G-module $\varphi : \mathrm{Hom}(\mathbb{Z}[G], X) \to \mathbb{Z}[G] \otimes X$ de la façon suivante

$$\varphi : f \mapsto \sum_{g \in G} g \otimes f(g).$$

Alors φ est un isomorphisme de G-modules de morphisme réciproque

$$\psi : \sum_{g \in G} g \otimes x_g \mapsto \left(f : \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g x_g \right).$$

□

1.2 Cohomologie de Tate

La cohomologie de Tate est une cohomologie des G-modules dans le cas où G est un groupe fini. Cette cohomologie découle d'une légère modification de la cohomologie et de l'homologie classique des groupes, que nous allons donc commencer par définir. Ce paragraphe est fortement inspiré du chapitre Cohomology of Groups rédigé par Michael Atiyah et Charles Wall dans [AW67]. Dans cette section, G désigne un groupe quelconque.

1.2.1 Cohomologie des groupes

Définition 1.2.1. *Soit M un G-module.*
Une résolution projective P de M est la donnée d'une famille de G-modules projectifs $(P_i)_{i \in \mathbb{N}}$ et d'une suite exacte infinie de G-modules

$$\ldots \to P_2 \to P_1 \to P_0 \to M \to 0.$$

Afin de définir les groupes de cohomologie d'un G-module nous avons besoin d'une résolution projective de $\mathbb{Z}$ vu comme G-module sur lequel G agit trivialement. Nous allons donc construire explicitement un exemple d'une telle résolution de $\mathbb{Z}$.
Pour tout $n \in \mathbb{N}$, on considère le G-module libre $S_n = \mathbb{Z}[G^{n+1}]$ sur lequel G agit diagonalement :

$$\forall (g_0, \ldots, g_n) \in S_n, \forall g' \in G,\ g'(g_0, \ldots, g_n) = (g'g_0, \ldots, g'g_n).$$

Pour tout $n \in \mathbb{N}^*$, on considère le morphisme de bord $d_n : S_n \to S_{n-1}$ défini par

$$\forall (g_0, ..., g_n) \in S_n,\ d_n(g_0, ..., g_n) = \sum_{i=0}^{n} (-1)^i (g_0, ..., g_{i-1}, g_{i+1}, ..., g_n),$$

et pour $n = 0$, on considère le morphisme d'augmentation

$$d_0 = \varepsilon : \mathbb{Z}[G] \to \mathbb{Z}.$$

Proposition 1.2.2. *La suite infinie de G-modules libres, donc projectifs,*

$$... \xrightarrow{d_3} S_2 \xrightarrow{d_2} S_1 \xrightarrow{d_1} S_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

est une suite exacte et S est donc une résolution projective de $\mathbb{Z}$, appelée résolution standard de $\mathbb{Z}$.

Démonstration. Pour tout $n \in \mathbb{N}^*$, on note $h_n : S_{n-1} \to S_n$ le morphisme de G-modules défini pour tout $(g_0, ..., g_{n-1}) \in P_{n-1}$ par

$$h_n(g_0, ..., g_{n-1}) = (1_G, g_0, ..., g_{n-1}).$$

On vérifie alors que pour tout $n \in \mathbb{N}^*$, on a

$$d_n \circ d_{n+1} = 0$$

et

$$h_n \circ d_n + d_{n+1} \circ h_{n+1} = \mathrm{id}_{P_n}.$$

Ainsi

$$\mathrm{Im}(d_{n+1}) \subset \mathrm{Ker}(d_n).$$

Si $(g_0, ..., g_n) \in \mathrm{Ker}(d_n)$, alors

$$(g_0, ..., g_n) = h_n \circ d_n(g_0, ..., g_n) + d_{n+1} \circ h_{n+1}(g_0, ..., g_n) = d_{n+1} \circ h_{n+1}(g_0, ..., g_n) \in \mathrm{Im}(d_{n+1}),$$

donc

$$\mathrm{Ker}(d_n) = \mathrm{Im}(d_{n+1}).$$

De plus, on a bien $\mathrm{Ker}(\varepsilon) = \mathrm{Im}(d_1)$, donc la suite considérée est bien exacte. □

À l'aide de cette résolution standard de $\mathbb{Z}$, on peut maintenant associer à tout G-module M un complexe $C_M = \mathrm{Hom}_{\mathbb{Z}[G]}(S, M)$ que l'on appelle complexe standard de M. Ce complexe est le suivant

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(S_0, M) \xrightarrow{\partial_M^0} \mathrm{Hom}_{\mathbb{Z}[G]}(S_1, M) \xrightarrow{\partial_M^1} ...$$

où pour tout $n \in \mathbb{N}$, le morphisme de cobord est donné par

$$\partial_M^n : f \mapsto f \circ d_{n+1}.$$

Cette nouvelle suite infinie vérifie $\partial_M^{n+1} \circ \partial_M^n = 0$ pour tout $n \in \mathbb{N}$, mais elle n'a pas de raison d'être exacte. Les groupes de cohomologie sont ce qui mesure cette inexactitude.

Définition 1.2.3. *Soit M un G-module.*
On définit le 0*-ième groupe de cohomologie de M par*

$$H^0(G, M) = \mathrm{Ker}(\partial_M^0)$$

et pour tout $n \in \mathbb{N}^*$, on définit le n-ième groupe de cohomologie de M de la façon suivante

$$H^n(G, M) = \mathrm{Ker}(\partial_M^n)/\mathrm{Im}(\partial_M^{n-1}).$$

Un élément de $\mathrm{Ker}(\partial_M^n)$ s'appelle un cocycle de degré n et un élément de $\mathrm{Im}(\partial_M^{n-1})$ s'appelle un cobord de degré n. Ainsi, le n-ième groupe de cohomologie de M est le quotient des cocycles de degré n par les cobords de degré n.

Proposition 1.2.4. *Soit M un G-module.*
On a

$$H^0(G, M) \simeq M^G.$$

Démonstration. Soit $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M)$, elle est déterminée par $f(1_G)$. Donc $f \in \mathrm{Ker}(\partial_M^0)$ si et seulement si pour tout $(g_0, g_1) \in \mathbb{Z}[G^2]$ on a

$$f \circ d_1(g_0, g_1) = (g_1 - g_0)f(1_G) = 0$$

donc si et seulement si $f(1_G) \in M^G$. □

Proposition 1.2.5. *Soit M et N deux G-modules.*
Pour tout $n \in \mathbb{N}$, on a

$$H^n(G, M \oplus N) = H^n(G, M) \oplus H^n(G, N).$$

Démonstration. Pour tout $n \in \mathbb{N}$, on a

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M \oplus N) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \oplus \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], N)$$

et pour tout $f = (f_M, f_N) \in \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, M \oplus N)$, on a

$$\partial_{M\oplus N}^n((f_M, f_N)) = \left(\partial_M^n(f_M), \partial_N^n(f_N)\right)$$

donc

$$\mathrm{Ker}(\partial^n_{M\oplus N}) = \mathrm{Ker}(\partial^n_M) \oplus \mathrm{Ker}(\partial^n_N),$$
$$\mathrm{Im}(\partial^{n-1}_{M\oplus N}) = \mathrm{Im}(\partial^{n-1}_M) \oplus \mathrm{Im}(\partial^{n-1}_N).$$

On en déduit donc le résultat souhaité par passage au quotient. □

Proposition 1.2.6. *Pour tout G-module co-induit M et tout $n \in \mathbb{N}^*$, on a*

$$H^n(G, M) = 0.$$

Démonstration. Soit X le groupe abélien tel que $M = \mathrm{Hom}(\mathbb{Z}[G], X)$. Soit $n \in \mathbb{N}$. Le morphisme de groupes $\varphi : \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, M) \to \mathrm{Hom}(S_n, X)$, donné par

$$\varphi : f \mapsto (a \mapsto f(a)(1_G))$$

est un isomorphisme d'isomorphisme réciproque

$$\varphi^{-1} : l \mapsto \Big(a \mapsto \big(g \mapsto f(g^{-1}a)\big)\Big).$$

De plus comme S_{n+1} et S_n sont des $\mathbb{Z}$-modules libres, la suite exacte

$$0 \to \mathrm{Ker}(d_n) \to S_n \to \mathrm{Im}(d_n) \to 0$$

est scindée, donc

$$S_{n+1} = \mathrm{Ker}(d_{n+1}) \oplus T_{n+1} = \mathrm{Im}(d_{n+2}) \oplus T_{n+1} \text{ avec } T_{n+1} \simeq \mathrm{Im}(d_{n+1}).$$

Soit $f \in \mathrm{Hom}(S_{n+1}, X)$ tel que $f \circ d_{n+2} = 0$. Définissons $h : S_{n+1} \to S_n$ en posant $h(y) = f(x)$ pour tout $y = d_{n+1}(x) \in \mathrm{Im}(d_{n+1})$ et $h(y) = 0$ pour tout $y \in T_n$. Comme $f \circ d_{n+2} = 0$, on a

$$\mathrm{Ker}(d_{n+1}) = \mathrm{Im}(d_{n+2}) \subset \mathrm{Ker}(f),$$

donc

$$h \circ d_{n+1} = f.$$

Réciproquement, si $f = h \circ d_{n+1}$, on a

$$f \circ d_{n+2} = h \circ d_{n+1} \circ d_{n+2} = 0,$$

donc on déduit de l'isomorphisme précédent que le complexe

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(S_0, M) \overset{\partial^0_M}{\to} \mathrm{Hom}_{\mathbb{Z}[G]}(S_1, M) \overset{\partial^1_M}{\to} \ldots$$

est exact en tout $\mathrm{Hom}_{\mathbb{Z}[G]}(S_n, M)$ pour $n \neq 0$. □

Soit M, N et P des G-modules. On suppose que la suite

$$0 \to M \xrightarrow{\varphi} N \xrightarrow{\psi} P \to 0$$

est exacte.
Pour tout $n \in \mathbb{N}$, comme S_n est un G-module libre donc projectif, la suite de groupes abéliens

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, M) \xrightarrow{\varphi_n} \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, N) \xrightarrow{\psi_n} \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, P) \to 0$$

est exacte. On en déduit en particulier que pour tout $n \in \mathbb{N}$, la suite

$$0 \to \mathrm{Ker}(\partial_M^n) \to \mathrm{Ker}(\partial_N^n) \to \mathrm{Ker}(\partial_P^n)$$

est exacte.
Comme pour tout G-module Q on a $\mathrm{Im}(\partial_Q^n) \subset \mathrm{Ker}(\partial_Q^{n+1})$, on a le diagramme commutatif suivant, dont les deux lignes sont exactes

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, M) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, N) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, P) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_M^n} & & \downarrow{\scriptstyle \partial_N^n} & & \downarrow{\scriptstyle \partial_P^n} & & \\
0 & \longrightarrow & \mathrm{Ker}(\partial_M^{n+1}) & \longrightarrow & \mathrm{Ker}(\partial_N^{n+1}) & \longrightarrow & \mathrm{Ker}(\partial_M^{n+1}) & &
\end{array}.$$

En appliquant le lemme du serpent, on obtient la suite exacte suivante

$$0 \to \mathrm{Ker}(\partial_M^n) \to \mathrm{Ker}(\partial_N^n) \to \mathrm{Ker}(\partial_P^n) \xrightarrow{\lambda^n} H^{n+1}(G, M) \to H^{n+1}(G, N) \to H^{n+1}(G, P).$$

Pour tout $f \in \mathrm{Ker}(\partial_P^n)$, il existe $h_f \in \mathrm{Hom}_{\mathbb{Z}[G]}(S_n, N)$ tel que

$$f = \psi_n(h_f) = \psi \circ h_f.$$

Et comme

$$\psi_{n+1}(\partial_N^n(h_f)) = \partial_P^n(\psi_n(h_f)) = \partial_P^n(f) = 0,$$

il existe une unique $l_f \in \mathrm{Ker}(\partial_M^{n+1})$ telle que

$$\partial_N^n(h_f) = \varphi_n(l_f) = \varphi \circ l_f.$$

La classe de l_f dans $H^{n+1}(G, M)$ ne dépend pas du choix de h_f, donc on peut définir le morphisme

$$\lambda^n : \mathrm{Ker}(\partial_P^n) \to H^{n+1}(G, M)$$

en posant

$$\lambda^n(f) = l_f + \mathrm{Im}(\partial_M^n).$$

Si $f \in \mathrm{Im}(\partial_P^{n-1})$, on a $f = f' \circ d_n$, avec $f' \in \mathrm{Hom}_{\mathbb{Z}[G]}(S_{n-1}, P)$, donc

$$f' = \psi_{n-1}(h') = \psi \circ h' \text{ avec } h' \in \mathrm{Hom}_{\mathbb{Z}[G]}(S_{n-1}, N).$$

Ainsi,

$$f = \psi \circ f' \circ d_n = \psi_n(f' \circ d_n),$$

donc on peut choisir $h_f = f' \circ d_n$, et comme

$$\partial_N^n(h_f) = h_f \circ d_{n+1} = f' \circ d_n \circ d_{n+1} = 0 = \varphi_n(0),$$

on a

$$\lambda^n(f) = 0,$$

donc

$$\mathrm{Im}(\partial_P^{n-1}) \subset \mathrm{Ker}(\lambda^n),$$

et λ^n induit un morphisme de connexion

$$\delta^n : H^n(G, P) \to H^{n+1}(G, M).$$

On a

$$\mathrm{Im}(\delta^n) = \mathrm{Im}(\lambda^n)$$

et

$$f + \mathrm{Im}(\partial_P^{n+1}) \in \mathrm{Ker}(\delta^n)$$

si et seulement si

$$f \in \mathrm{Ker}(\lambda^n) = \mathrm{Im}\left(\psi_n : \mathrm{Ker}(\partial_N^n) \to \mathrm{Ker}(\partial_P^n)\right)$$

donc on déduit le résultat suivant.

Théorème 1.2.7. *Soit M, N et P des G-modules. On suppose que la suite*

$$0 \to M \to N \to P \to 0$$

est exacte.
Alors la suite infinie de groupes abéliens

$$0 \to H^0(G, M) \to H^0(G, N) \to H^0(G, P) \to H^1(G, M) \to ...$$
$$\to H^n(G, P) \to H^{n+1}(G, M) \to ...$$

est exacte.

Une suite de foncteurs de la catégorie des G-modules vers celle des groupes abéliens vérifiant les propositions 1.2.4 et 1.2.6 et le théorème 1.2.7 s'appelle une extension cohomologique du foncteur $\mathcal{F}^G : M \mapsto M^G$ des G-invariants.

Théorème 1.2.8. *La suite de foncteurs $(H^n(G,-))_{n\in\mathbb{N}}$ est l'unique extension cohomologique du foncteur $\mathcal{F}^G$ à isomorphisme près.*

Démonstration. Soit $(\mathcal{F}^n)_{n\in\mathbb{N}}$ une extension cohomologique de $\mathcal{F}^G$.
Pour tout G-module M, on peut définir un morphisme injectif

$$\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)$$

en posant

$$\varphi(m)(g) = gm.$$

Ainsi, on a la suite exacte

$$0 \to M \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)/\varphi(M) \to 0.$$

D'après la proposition 1.2.6, pour tout $n \in \mathbb{N}^*$, on a $\mathcal{F}^n(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)) = 0$, et donc, d'après le théorème 1.2.7, pour tout $n \in \mathbb{N}$, on a

$$\mathcal{F}^{n+1}(M) \simeq \mathcal{F}^n(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)/\varphi(M)).$$

Donc le foncteur $\mathcal{F}^{n+1}$ est déterminé à isomorphisme près par le foncteur $\mathcal{F}^n$, et donc la proposition 1.2.4 implique l'unicité à isomorphisme près de l'extension cohomologique. □

Il existe d'autres manières de construire explicitement les groupes de cohomologie, par exemple en choisissant une résolution projective de $\mathbb{Z}$ autre que la résolution standard.

1.2.2 Homologie des groupes

Nous allons maintenant nous intéresser à une notion voisine de la cohomologie des groupes, l'homologie des groupes. La construction donnée ici reposera à nouveau sur la résolution standard de $\mathbb{Z}$ donnée au paragraphe précédent. À l'aide de cette résolution standard de $\mathbb{Z}$, on peut associer à tout G-module M un complexe de G-modules $C^M = S \underset{\mathbb{Z}[G]}{\otimes} M$ que l'on appelle complexe standard d'homologie de M.
Ce complexe est le suivant

$$\ldots \xrightarrow{\partial_3^M} S_2 \underset{\mathbb{Z}[G]}{\otimes} M \xrightarrow{\partial_2^M} S_1 \underset{\mathbb{Z}[G]}{\otimes} M \xrightarrow{\partial_1^M} S_0 \underset{\mathbb{Z}[G]}{\otimes} M \to 0$$

où pour tout $n \in \mathbb{N}^*$, le morphisme de bord est donné par

$$\partial_n^M : s \underset{\mathbb{Z}[G]}{\otimes} m \mapsto d_n(s) \underset{\mathbb{Z}[G]}{\otimes} m.$$

Cette nouvelle suite infinie vérifie $\partial_n^M \circ \partial_{n+1}^M = 0$ pour tout $n \in \mathbb{N}^*$, mais elle n'a pas de raison d'être exacte. Les groupes d'homologie sont ce qui mesure cette inexactitude.

Définition 1.2.9. *Soit M un G-module et S la résolution standard de $\mathbb{Z}$.*
On définit le 0-ième groupe d'homologie de M par

$$H_0(G, M) = S_0 \underset{\mathbb{Z}[G]}{\otimes} M/\mathrm{Im}(\partial_1^M)$$

et pour tout $n \in \mathbb{N}^*$, on définit le n-ième groupe d'homologie de M de la façon suivante

$$H_n(G, M) = \mathrm{Ker}(\partial_n^M)/\mathrm{Im}(\partial_{n+1}^M).$$

Un élément de $\mathrm{Ker}(\partial_n^M)$ s'appelle un cycle de degré n et un élément de $\mathrm{Im}(\partial_{n+1}^M)$ s'appelle un bord de degré n. Ainsi, le n-ième groupe d'homologie de M est le quotient des cycles de degré n par les bords de degré n.

Proposition 1.2.10. *Soit M un G-module.*
On a l'isomorphisme de groupes

$$H_0(G, M) \simeq M_G.$$

Démonstration. On a

$$S_0 \underset{\mathbb{Z}[G]}{\otimes} M = \mathbb{Z}[G] \underset{\mathbb{Z}[G]}{\otimes} M \simeq M$$

via

$$\varphi : g \otimes m \mapsto gm.$$

Soit $(g_0, g_1) \otimes m \in S_1 \underset{\mathbb{Z}[G]}{\otimes} M$, on a

$$\varphi \circ \partial_1^M ((g_0, g_1) \otimes m) = (g_1 - g_0)m \in I_G M,$$

donc par linéarité,

$$\varphi\left(\mathrm{Im}(\partial_{n+1}^M)\right) \subset I_G M.$$

Réciproquement si $a = \sum_g a_g g \in I_G$ et $m \in M$, on a

$$a = \sum_{g \neq g_0} a_g (g - g_0) = \varphi \circ \partial_1^M \left(\sum_{g \neq g_0} a_g (g_0, g) \otimes m \right) \in \varphi\left(\mathrm{Im}(\partial_{n+1}^M)\right),$$

donc par linéarité

$$\varphi\left(\mathrm{Im}(\partial_{n+1}^{M})\right) = I_G M.$$

Ainsi,

$$H_0(G,M) = S_0 \underset{\mathbb{Z}[G]}{\otimes} M/\mathrm{Im}(\partial_1^M) \simeq M/I_G M.$$

□

Proposition 1.2.11. *Soit M et N deux G-modules.*
Pour tout $n \in \mathbb{N}$, on a

$$H_n(G, M \oplus N) = H_n(G,M) \oplus H_n(G,N).$$

Démonstration. Pour tout $n \in \mathbb{N}$, on a

$$S_n \underset{\mathbb{Z}[G]}{\otimes} (M \oplus N) = (S_n \underset{\mathbb{Z}[G]}{\otimes} M) \oplus (S_n \underset{\mathbb{Z}[G]}{\otimes} N)$$

et pour tout $(m, m') \in M \oplus N$ et tout $s \in \S_n$, on a

$$\partial_n^{M\oplus N}(s \underset{\mathbb{Z}[G]}{\otimes} (m,m')) = \left(\partial_n^M(s \underset{\mathbb{Z}[G]}{\otimes} m), \partial_n^N(s \underset{\mathbb{Z}[G]}{\otimes} m')\right)$$

donc

$$\mathrm{Ker}(\partial_n^{M\oplus N}) = \mathrm{Ker}(\partial_n^M) \oplus \mathrm{Ker}(\partial_n^N),$$
$$\mathrm{Im}(\partial_{n+1}^{M\oplus N}) = \mathrm{Im}(\partial_{n+1}^M) \oplus \mathrm{Im}(\partial_{n+1}^N).$$

On en déduit donc le résultat souhaité par passage au quotient. □

Proposition 1.2.12. *Pour tout G-module induit M et tout $n \in \mathbb{N}^*$, on a*

$$H^n(G,M) = 0.$$

Démonstration. Soit X le groupe abélien tel que $M = \mathbb{Z}[G] \otimes X$. Soit $n \in \mathbb{N}$.
On a les isomorphismes de G-modules suivants

$$\begin{aligned} S_n \underset{\mathbb{Z}[G]}{\otimes} M &\simeq (S_n \otimes M)_G \simeq (S_n \otimes (\mathbb{Z}[G] \otimes X))_G \simeq (\mathbb{Z}[G] \otimes (S_n \otimes X))_G \\ &\simeq \mathbb{Z}[G] \underset{\mathbb{Z}[G]}{\otimes} (S_n \otimes X) \simeq S_n \otimes X. \end{aligned}$$

On s'intéresse donc au complexe suivant

$$\ldots \xrightarrow{\widetilde{\partial}_3^M} S_2 \otimes X \xrightarrow{\widetilde{\partial}_2^M} S_1 \otimes X \xrightarrow{\widetilde{\partial}_1^M} S_0 \otimes X \to 0$$

où pour tout $n \in \mathbb{N}^*$, le morphisme de bord est donné par

$$\widetilde{\partial}_n^M : s \underset{\mathbb{Z}[G]}{\otimes} x \mapsto d_n(s) \otimes x.$$

Si $n \in \mathbb{N}^*$, la suite exacte

$$0 \to \mathrm{Ker}(d_n) \to S_n \to \mathrm{Im}(d_n) \to 0$$

est scindée car $\mathrm{Im}(d_n) \subset S_{n-1}$ est libre donc projectif. On en déduit donc l'exactitude de la suite

$$0 \to \mathrm{Ker}(d_n) \otimes X \to S_n \otimes X \to \mathrm{Im}(d_n) \otimes X \to 0.$$

Or $\mathrm{Im}(d_n) \otimes X = \mathrm{Im}(\widetilde{\partial}_n^M)$, donc on en déduit que $\mathrm{Ker}(d_n) \otimes X = \mathrm{Ker}(\widetilde{\partial}_n^M)$.
Ainsi, pour tout $n \in \mathbb{N}^*$, on a

$$\mathrm{Im}(\widetilde{\partial}_{n+1}^M) = \mathrm{Im}(d_{n+1}) \otimes X = \mathrm{Ker}(d_n) \otimes X = \mathrm{Ker}(\widetilde{\partial}_n^M).$$

Donc on déduit de l'isomorphisme précédent que le complexe

$$\ldots \overset{\partial_3^M}{\to} S_2 \underset{\mathbb{Z}[G]}{\otimes} M \overset{\partial_2^M}{\to} S_1 \underset{\mathbb{Z}[G]}{\otimes} M \overset{\partial_1^M}{\to} S_0 \underset{\mathbb{Z}[G]}{\otimes} M \to 0$$

est exact en tout $S_n \underset{\mathbb{Z}[G]}{\otimes} M$ pour $n \neq 0$. □

Soit M, N et P des G-modules. On suppose que la suite

$$0 \to M \overset{\varphi}{\to} N \overset{\psi}{\to} P \to 0$$

est exacte.
Pour tout $n \in \mathbb{N}$, comme S_n est un G-module libre donc plat, la suite de groupes abéliens

$$0 \to S_n \underset{\mathbb{Z}[G]}{\otimes} M \overset{\varphi_n}{\to} S_n \underset{\mathbb{Z}[G]}{\otimes} N \overset{\psi_n}{\to} S_n \underset{\mathbb{Z}[G]}{\otimes} P \to 0$$

est exacte. On en déduit en particulier que pour tout $n \in \mathbb{N}$, la suite

$$0 \to \mathrm{Ker}(\partial_n^M) \to \mathrm{Ker}(\partial_n^N) \to \mathrm{Ker}(\partial_n^P)$$

est exacte.
Pour tout $n \in \mathbb{N}^*$, comme pour tout G-module Q on a $\mathrm{Im}(\partial_{n+1}^Q) \subset \mathrm{Ker}(\partial_n^Q)$, on a le diagramme commutatif suivant, dont les deux lignes sont exactes

$$\begin{array}{ccccccccc}
0 & \longrightarrow & S_{n+1} \underset{\mathbb{Z}[G]}{\otimes} M & \longrightarrow & S_{n+1} \underset{\mathbb{Z}[G]}{\otimes} N & \longrightarrow & S_{n+1} \underset{\mathbb{Z}[G]}{\otimes} P & \longrightarrow & 0 \\
 & & \downarrow \partial_{n+1}^M & & \downarrow \partial_{n+1}^N & & \downarrow \partial_{n+1}^P & & \\
0 & \longrightarrow & \mathrm{Ker}(\partial_n^M) & \longrightarrow & \mathrm{Ker}(\partial_n^N) & \longrightarrow & \mathrm{Ker}(\partial_n^M) & &
\end{array}.$$

En appliquant le lemme du serpent, on obtient la suite exacte suivante

$$0 \to \mathrm{Ker}(\partial^M_{n+1}) \to \mathrm{Ker}(\partial^N_{n+1}) \to \mathrm{Ker}(\partial^P_{n+1}) \xrightarrow{\lambda_n} H_n(G,M) \to H_n(G,N) \to H_n(G,P).$$

Pour tout $x \in \mathrm{Ker}(\partial^P_{n+1})$, il existe $y_x \in S_{n+1} \underset{\mathbb{Z}[G]}{\otimes} N$ tel que $x = \psi_{n+1}(y_x)$. Mais comme

$$\psi_n(\partial^N_{n+1}(y_x)) = \partial^P_{n+1}(\psi_{n+1}(y_x)) = \partial^P_{n+1}(x) = 0,$$

il existe un unique $z_x \in \mathrm{Ker}(\partial^M_n)$ tel que

$$\partial^N_{n+1}(y_x) = \varphi_n(z_x).$$

La classe de z_x dans $H_n(G,M)$ ne dépend pas du choix de y_x, on définit donc le morphisme

$$\lambda_n : \mathrm{Ker}(\partial^P_{n+1}) \to H_n(G,M)$$

en posant

$$\lambda_n(x) = z_x + \mathrm{Im}(\partial^M_{n+1}).$$

Si $x \in \mathrm{Im}(\partial^P_{n+2})$, il existe $x' \in S_{n+2} \underset{\mathbb{Z}[G]}{\otimes} P$ tel que $x = \partial^P_{n+2}(x')$. Puis il existe $y' \in S_{n+2} \underset{\mathbb{Z}[G]}{\otimes} N$ tel que $x' = \psi_{n+2}(y')$, on a alors

$$x = \partial^P_{n+2}(\psi_{n+2}(y')) = \psi_{n+1}(\partial^N_{n+2}(y')),$$

on peut donc choisir $y_x = \partial^N_{n+2}(y')$. On a donc

$$\partial^N_{n+1}(y_x) = \partial^N_{n+1}(\partial^N_{n+2}(y')) = 0 = \varphi_n(0).$$

Donc

$$\lambda_n(x) = 0$$

et

$$\mathrm{Im}(\partial^P_{n+2}) \subset \mathrm{Ker}(\lambda_n).$$

En passant au quotient, on en déduit un morphisme de connexion

$$\delta_n : H_{n+1}(G,P) \to H_n(G,M).$$

Comme

$$\mathrm{Im}(\delta_n) = \mathrm{Im}(\lambda_n)$$

et comme

$$x + \mathrm{Im}(\partial^P_{n+2}) \in \mathrm{Ker}(\delta_n)$$

si et seulement si

$$x \in \mathrm{Ker}(\lambda_n) = \mathrm{Im}\Big(\psi_{n+1} : \mathrm{Ker}(\partial^N_{n+1}) \to \mathrm{Ker}(\partial^P_{n+1})\Big),$$

on a le résultat suivant.

Théorème 1.2.13. *Soit M, N et P des G-modules. On suppose que la suite*

$$0 \to M \to N \to P \to 0$$

est exacte.
Alors la suite infinie de groupes abéliens

$$\begin{aligned} ... \to H_{n+1}(G,P) \to H_n(G,M) \to ... \\ \to H_1(G,P) \to H_0(G,M) \to H_0(G,N) \to H_0(G,P) \to 0 \end{aligned}$$

est exacte.

Une suite de foncteurs de la catégorie des G-modules vers celle des groupes abéliens vérifiant les propositions 1.2.10 et 1.2.12 et le théorème 1.2.13 s'appelle une extension homologique du foncteur $\mathcal{F}_G : M \mapsto M_G = M/I_G M$.

Théorème 1.2.14. *La suite de foncteurs $(H_n(G,-))_{n\in\mathbb{N}}$ est l'unique extension homologique du foncteur $\mathcal{F}_G : M \mapsto M_G$ à isomorphisme près.*

Démonstration. Soit $(\mathcal{F}_n)_{n\in\mathbb{N}}$ une extension homologique de $\mathcal{F}_G$.
Pour tout G-module M, on peut définir un morphisme surjectif

$$\psi : \mathbb{Z}[G] \otimes M \to M$$

en posant

$$\psi(a \otimes m) = am.$$

Ainsi, on a la suite exacte

$$0 \to \mathrm{Ker}(\psi) \to \mathbb{Z}[G] \otimes M \to M \to 0.$$

D'après la proposition 1.2.12, pour tout $n \in \mathbb{N}^*$, on a $\mathcal{F}_n(\mathbb{Z}[G] \otimes M) = 0$, et donc, d'après le théorème 1.2.13, pour tout $n \in \mathbb{N}$, on a

$$\mathcal{F}_{n+1}(M) \simeq \mathcal{F}_n(\mathrm{Ker}(\psi)).$$

Donc le foncteur $\mathcal{F}_{n+1}$ est déterminé à isomorphisme près par le foncteur $\mathcal{F}_n$, et donc la proposition 1.2.10 implique l'unicité à isomorphisme près de l'extension cohomologique. □

Il existe d'autres manières de construire explicitement les groupes d'homologie, par exemple en choisissant une résolution projective de $\mathbb{Z}$ autre que la résolution standard.

1.2.3 Cohomologie de Tate des groupes finis

La cohomologie de Tate est une cohomologie des groupes finis légèrement modifiée afin de combiner homologie et cohomologie. Dans cette partie, on suppose que le groupe G est fini. Pour tout G-module M, on a donc l'application norme

$$\mathcal{N}_{G,M} : M \to M.$$

Soit $g_0 \in G$ et $m \in M$. On a

$$\mathcal{N}_{G,M}((g_0 - 1_G)m) = \sum_{g\in G} gg_0m - \sum_{g\in G} gm = 0,$$

donc par linéarité

$$I_G M \subset \mathrm{Ker}(\mathcal{N}_{G,M}).$$

De plus

$$g_0\mathcal{N}_{G,M}(m) = \sum_{g\in G} g_0gm = \mathcal{N}_{G,M}(m),$$

donc

$$\mathrm{Im}(\mathcal{N}_{G,M}) \subset M^G.$$

Comme $H_0(G, M) = M/I_G M$ et $H^0(G, M) = M^G$, on en déduit que $\mathcal{N}_{G,M}$ induit un morphisme

$$\mathcal{N}^*_{G,M} : H_0(G, M) \to H^0(G, M).$$

Définition 1.2.15. *Soit M un G-module.*
On pose

$$\hat{H}_0(G, M) = \mathrm{Ker}(\mathcal{N}^*_{G,M}) = \mathrm{Ker}(\mathcal{N}_{G,M})/I_G M$$

et

$$\hat{H}^0(G, M) = \mathrm{Coker}(\mathcal{N}^*_{G,M}) = M^G/\mathrm{Im}(\mathcal{N}_{G,M}).$$

Exemple. Pour $M = \mathbb{Z}$ sur lequel G agit trivialement, on a $\mathcal{N}_{G,\mathbb{Z}} : m \mapsto \mathrm{card}(G)m$, donc $\mathrm{Ker}(\mathcal{N}_{G,M}) = 0$ et $\mathrm{Im}(\mathcal{N}_{G,M}) = \mathrm{card}(G)\mathbb{Z}$. On a alors $\hat{H}_0(G, \mathbb{Z}) = 0$ et $\hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/\mathrm{card}(G)\mathbb{Z}$.

À l'aide de ces zéroièmes groupes de cohomologie et d'homologie modifiés, on va pouvoir recoller l'homologie et la cohomologie à travers la cohomologie de Tate.

Définition 1.2.16. *Soit M un G-module.*
Pour tout $n \in \mathbb{Z}$, on définit le n-ième groupe de cohomologie de Tate de M de la façon suivante

$$\hat{H}^n(G, M) = H^n(G, M) \text{ pour } n \geq 1,$$

$$\hat{H}^0(G,M) = M^G/\mathrm{Im}(\mathcal{N}_{G,M}),$$
$$\hat{H}^{-1}(G,M) = \mathrm{Ker}(\mathcal{N}_{G,M})/I_G M,$$
$$\hat{H}^n(G,M) = H_{-n-1}(G,M) \text{ pour } n \leq -2.$$

Théorème 1.2.17. *Soit M, N et P des G-modules. On suppose que la suite*

$$0 \to M \to N \to P \to 0$$

est exacte.
Alors on a une suite infinie exacte de groupes abéliens

$$... \to \hat{H}^n(G,M) \to \hat{H}^n(G,N) \to \hat{H}^n(G,P) \to \hat{H}^{n+1}(G,M) \to ...$$

Démonstration. D'après les théorèmes 1.2.7 et 1.2.13, on a les deux suites infinies exactes suivantes

$$... \to \hat{H}^n(G,N) \to \hat{H}^n(G,P) \to \hat{H}^{n+1}(G,M) \to ... \to \hat{H}^{-2}(G,N) \to \hat{H}^{-2}(G,P)$$

et

$$\hat{H}^1(G,M) \to \hat{H}^1(G,N) \to ... \to \hat{H}^n(G,N) \to \hat{H}^n(G,P) \to \hat{H}^{n+1}(G,M) \to ...$$

Par ailleurs, ces théorèmes impliquent qu'on a le diagramme commutatif suivant, dont les deux lignes sont exactes

$$\begin{array}{ccccccc} & & H_0(G,M) & \longrightarrow & H_0(G,N) & \longrightarrow & H_0(G,P) \longrightarrow 0 \\ & & \downarrow \mathcal{N}^*_{G,M} & & \downarrow \mathcal{N}^*_{G,N} & & \downarrow \mathcal{N}^*_{G,P} \\ 0 & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,N) & \longrightarrow & H^0(G,P) \end{array} .$$

Donc en appliquant le lemme du serpent, on en déduit que la suite finie suivante est exacte

$$\hat{H}^{-1}(G,M) \to \hat{H}^{-1}(G,N) \to \hat{H}^{-1}(G,P) \to \hat{H}^0(G,M) \to \hat{H}^0(G,N) \to \hat{H}^0(G,P).$$

Comme on sait que la suite

$$H_1(G,N) \to H_1(G,P) \to H_0(G,M) \to H_0(G,N)$$

est exacte et que $\mathrm{Im}(H_1(G,P) \to H_0(G,M)) \subset \hat{H}^{-1}(G,M)$ on déduit un recollement de la première suite infinie avec la suite finie

$$... \to \hat{H}^{-2}(G,N) \to \hat{H}^{-2}(G,P) \to \hat{H}^{-1}(G,M) \to \hat{H}^{-1}(G,N) \to ... \to \hat{H}^0(G,P)$$

Le fait que $\hat{H}^{-1}(G,M)$ soit un sous-groupe de $H_0(G,M)$ et $\hat{H}^{-1}(G,N)$ un sous-groupe de $H_0(G,N)$ implique l'exactitude de ce recollement.
Enfin, on a la suite exacte

$$H^0(G,N) \to H^0(G,P) \to H^1(G,M) \to H^1(G,N).$$

Comme $\mathrm{Im}(\mathcal{N}_{G,M}) \subset \mathrm{Ker}(H^0(G,P) \to H^1(G,M))$ et $\hat{H}^0(G,P) = H^0(G,P)/\mathrm{Im}(\mathcal{N}_{G,M})$, on déduit un recollement avec la deuxième suite infinie

$$\ldots \to \hat{H}^0(G,N) \to \hat{H}^0(G,P) \to \hat{H}^1(G,M) \to \hat{H}^1(G,N) \to \ldots$$

Le fait que $\hat{H}^1(G,M)$ soit un quotient de $H^1(G,M)$ et $\hat{H}^1(G,N)$ un quotient de $H^1(G,N)$ implique l'exactitude de ce recollement. □

On déduit des propositions 1.2.5 et 1.2.11 le résultat suivant.

Proposition 1.2.18. *Soit M et N des G-modules.*
Pour tout $n \in \mathbb{Z}$, on a

$$\hat{H}^n(G, M \oplus N) = \hat{H}^n(G,M) \oplus \hat{H}^n(G,N).$$

Proposition 1.2.19. *Pour tout G-module induit M et tout $n \in \mathbb{Z}$, on a*

$$\hat{H}^n(G,M) = 0.$$

Démonstration. On suppose que $M = \mathbb{Z}[G] \otimes X$, avec X un groupe abélien. Les cas $n \neq 0, -1$ découlent des propositions 1.2.6 et 1.2.12.
Soit $\sum_{g \in G} g \otimes x_g \in \mathbb{Z}[G] \otimes X$. Alors pour tout $g' \in G$, on a

$$\sum_{g \in G} g'g \otimes x_g = \sum_{g \in G} g \otimes x_{g'^{-1}g} = \sum_{g \in G} g \otimes x_g.$$

Or $\mathbb{Z}[G]$ est un $\mathbb{Z}$-module libre, donc il y a unicité de l'écriture sous la forme $\sum_{g \in G} g \otimes x_g$ et on en déduit que pour tout $g \in G$, on a $x_g = x_{1_G}$. Ainsi,

$$\sum_{g \in G} g \otimes x_g = \mathcal{N}_{G,M}(1_G \otimes x_{1_G}) \in \mathrm{Im}(\mathcal{N}_{G,M}).$$

On a donc

$$\hat{H}^0(G,M) = 0.$$

Considérons maintenant $\sum_{g\in G} g\otimes x_g \in \mathrm{Ker}(\mathcal{N}_{G,M})$. On a

$$\mathcal{N}_{G,M}\Big(\sum_{g\in G} g\otimes x_g\Big) = \sum_{g\in G} g\otimes\Big(\sum_{g'\in G} x_{g'}\Big) = 0,$$

donc par unicité de l'écriture, $\sum_{g'\in G} x_{g'} = 0$, donc

$$\sum_{g\in G} g\otimes x_g = \sum_{g\in G}(g-1_G)(1_G\otimes x_g) \in I_G M.$$

On a ainsi

$$\hat{H}^{-1}(G,M) = 0.$$

□

Définition 1.2.20. *Soit M un G-module.*
On dit que M est cohomologiquement trivial si pour tout sous-groupe F de G et tout $n\in\mathbb{Z}$, on a

$$\hat{H}^n(F,M) = 0.$$

Proposition 1.2.21. *Le G-module $\mathbb{Z}[G]$ est cohomologiquement trivial.*

Démonstration. Pour tout sous-groupe F de G, G est un F-module induit, donc d'après la proposition précédente, pour tout $n\in\mathbb{Z}$, on a

$$\hat{H}^n(F,M) = 0.$$

□

Corollaire 1.2.22. *Soit M un G-module projectif.*
Alors M est un G-module cohomologiquement trivial.

Démonstration. Comme M est projectif, il existe un G-module N et un entier s tel que

$$M\oplus N \simeq \mathbb{Z}[G]^s.$$

D'après la proposition 1.2.18, pour tout sous-groupe F de G et tout $n\in\mathbb{Z}$, on a alors

$$\hat{H}^n(F,M)\oplus\hat{H}^n(F,N) \simeq \hat{H}^n(F,\mathbb{Z}[G]^s) \simeq \bigoplus_{i=1}^{s}\hat{H}^n(F,\mathbb{Z}[G]).$$

Donc d'après la proposition précédente, on a

$$\hat{H}^n(F,M)\oplus\hat{H}^n(F,N) = 0$$

donc

$$\hat{H}^n(F,M) = 0.$$

□

1.3 Produit tensoriel

Nous énonçons ici une proposition qui porte sur le produit tensoriel en général et qui nous servira ensuite dans le contexte de la p-partie.

Proposition 1.3.1. *Soit A un anneau, M un A-module et I un idéal de A.*
On a alors les isomorphismes de A-modules suivants

1. $$I \underset{A}{\otimes} M \simeq IM,$$
2. $$A/I \underset{A}{\otimes} M \simeq M/IM.$$

Démonstration. 1. Cet isomorphisme est la restriction de l'isomorphisme naturel $A \underset{A}{\otimes} M \simeq M$.

2. On définit une application A-bilinéaire surjective

$$\varphi : \begin{cases} A/I \times M \to M/IM \\ (a+I, m) \mapsto am + IM \end{cases}.$$

. Pour tout A-module N et toute application A-bilinéaire $f : A/I \times M \to N$, on définit alors une application A-linéaire

$$\tilde{h} : \begin{cases} M \to N \\ m \mapsto f(1+I, m) \end{cases}.$$

Pour tout $a \in I$ et $m \in M$, on a alors

$$\tilde{h}(am) = f(1+I, am) = f(a+I, m) = 0$$

car $a \in I$, donc $IM \subset \mathrm{Ker}(\tilde{h})$ et $\tilde{h}$ induit l'application A-linéaire

$$h : M/IM \to N.$$

On a alors $h \circ \varphi = f$ et une telle h est unique par surjectivité de φ, donc d'après la propriété universelle du produit tensoriel, on a l'isomorphisme souhaité.

□

En particulier, pour toute A-algèbre associative B, l'isomorphisme de A-modules $B \simeq A \underset{A}{\otimes} B$ induit un morphisme de A-modules $BI \simeq I \underset{A}{\otimes} B$ pour tout idéal I de A.

Proposition 1.3.2. *Soit A un anneau commutatif, M un A-module libre de type fini et N un A-module.*
On a alors l'isomorphisme de A-modules suivant

$$N \underset{A}{\otimes} \mathrm{Hom}_A(M, A) \simeq \mathrm{Hom}_A(M, N).$$

Démonstration. Soit $(\alpha_i)_i$ une base de M et $(\alpha_i^*)_i$ la base duale de $\mathrm{Hom}_A(M,A)$. Alors le morphisme

$$\varphi : \begin{cases} N \underset{A}{\otimes} \mathrm{Hom}_A(M,A) \to \mathrm{Hom}_A(M,N) \\ n \underset{A}{\otimes} f \mapsto (f_n : m \mapsto f(m)n) \end{cases}$$

a pour morphisme réciproque

$$\psi : \begin{cases} \mathrm{Hom}_A(M,N) \to N \underset{A}{\otimes} \mathrm{Hom}_A(M,A) \\ f \mapsto \sum\limits_i f(\alpha_i)\alpha_i^* \end{cases} .$$

□

1.4 p-partie

1.4.1 Propriétés générales

Notation. Pour tout $\mathbb{Z}$-module fini M, on appelle p-partie de M et on note

$$\mathrm{Syl}_p(M) = \{m \in M \text{ tel qu'il existe } r \in \mathbb{N} \text{ tel que } p^r m = 0\}$$

l'unique p-Sylow de M. La p-partie de M est un p-groupe abélien, elle a donc une structure de $\mathbb{Z}_p$-module.

Proposition 1.4.1. *Soit M un $\mathbb{Z}$-module fini.*
On a alors l'isomorphisme de $\mathbb{Z}_p$-modules suivant

$$\mathrm{Syl}_p(M) \simeq M \otimes \mathbb{Z}_p.$$

Démonstration. D'après le théorème de structure des groupes abéliens finis on a $M = \bigoplus\limits_{p' \text{ premier}} \mathrm{Syl}_{p'}(M)$, donc $M \otimes \mathbb{Z}_p = \bigoplus\limits_{p' \text{ premier}} \left(\mathrm{Syl}_{p'}(M) \otimes \mathbb{Z}_p\right)$.

– Si $p' \neq p$: p' est inversible dans $\mathbb{Z}_p$, donc

$$\mathrm{Syl}_{p'}(M) \otimes \mathbb{Z}_p = 0.$$

– Si $p' = p$: $\mathrm{Syl}_p(M)$ est un $\mathbb{Z}_p$-module, donc on a une application $\mathbb{Z}$-bilinéaire surjective

$$\varphi : \begin{cases} \mathrm{Syl}_p(M) \times \mathbb{Z}_p \to \mathrm{Syl}_p(M) \\ (m,x) \mapsto xm \end{cases} .$$

Pour tout $\mathbb{Z}$-module N et toute application $\mathbb{Z}$-bilinéaire $f : \mathrm{Syl}_p(M) \times \mathbb{Z}_p \to N$, on définit l'application $\mathbb{Z}$-linéaire

$$h : \begin{cases} \mathrm{Syl}_p(M) \to N \\ m \mapsto f(m, 1) \end{cases} .$$

Soit $m \in \mathrm{Syl}_p(M)$ et $r \in \mathbb{N}$ tels que $p^r m = 0$, pour tout $x \in \mathbb{Z}_p$, on peut écrire $x = x_0 + p^r x_1$ avec $x_0 \in \mathbb{Z}$ et $x_1 \in \mathbb{Z}_p$, on a alors

$$f(m, x) = f(m, x_0) + f(p^r m, x_1) = f(m, x_0)$$

et

$$\varphi(m, x) = \varphi(m, x_0) + \varphi(p^r m, x_1) = \varphi(m, x_0).$$

Ainsi

$$h(\varphi(m, x)) = h(\varphi(m, x_0)) = h(x_0 m) = f(x_0 m, 1) = f(m, x_0) = f(m, x).$$

Une telle application h est unique par surjectivité de φ donc d'après la propriété universelle du produit tensoriel, on a l'isomorphisme de $\mathbb{Z}$-modules

$$\mathrm{Syl}_p(M) \otimes \mathbb{Z}_p \simeq \mathrm{Syl}_p(M).$$

De plus, l'application φ est $\mathbb{Z}_p$-bilinéaire, donc l'isomorphisme obtenu est un isomorphisme de $\mathbb{Z}_p$-modules.

Ainsi, en tant que $\mathbb{Z}_p$-modules,

$$M \otimes \mathbb{Z}_p = \mathrm{Syl}_p(M) \otimes \mathbb{Z}_p \simeq \mathrm{Syl}_p(M).$$

□

Soit n un entier naturel non nul. On remarque qu'une application entre deux $\mathbb{Z}[1/n]$-modules est $\mathbb{Z}$-linéaire si et seulement si elle est $\mathbb{Z}[1/n]$-linéaire. On suppose que le nombre premier p ne divise pas n. L'anneau $\mathbb{Z}[1/n]$ est alors un sous-anneau de $\mathbb{Z}_p$. Soit r et s des entiers naturels, toute application $\mathbb{Z}$-linéaire $\varphi : \mathbb{Z}[1/n]^r \to \mathbb{Z}[1/n]^s$ peut alors s'étendre de manière unique en application $\mathbb{Z}_p$-linéaire $\varphi_p : \mathbb{Z}_p^r \to \mathbb{Z}_p^s$.

Proposition 1.4.2. *On suppose p premier ne divisant pas n fixé, et on considère $\varphi : \mathbb{Z}[1/n]^r \to \mathbb{Z}[1/n]^s$ une application $\mathbb{Z}$-linéaire.*
Alors φ est injective si et seulement si φ_p est injective.

Démonstration. On peut étendre φ en $\widetilde{\varphi} : \mathbb{Q}^r \to \mathbb{Q}^s$ et φ_p en $\widetilde{\varphi_p} : \mathbb{Q}_p^r \to \mathbb{Q}_p^s$. Comme ces deux applications ont même matrice dans la base canonique, et comme le rang de cette matrice est identique sur $\mathbb{Q}$ et $\mathbb{Q}_p$, on en déduit que $\widetilde{\varphi}$ est injective si et seulement si $\widetilde{\varphi_p}$ l'est.
On suppose φ injective. Si $\frac{a}{b} \in \ker\widetilde{\varphi}$, on a $\varphi(a) = \widetilde{\varphi}(a) = b\,\widetilde{\varphi}\left(\frac{a}{b}\right) = 0$, donc $\widetilde{\varphi}$ est injective, et $\widetilde{\varphi_p}$ également. Comme $\ker(\varphi_p) \subset \ker(\widetilde{\varphi_p})$, on en déduit que φ_p est injective.
La réciproque découle de $\ker(\varphi) \subset \ker(\varphi_p)$. □

Proposition 1.4.3. *On considère $\varphi : \mathbb{Z}[1/n]^r \to \mathbb{Z}[1/n]^s$ une application $\mathbb{Z}$-linéaire injective, et $y \in \mathbb{Z}[1/n]^s$.*
Alors $y \in \mathrm{Im}(\varphi)$ si et seulement si pour tout premier $p \nmid n$ on a $y \in \mathrm{Im}(\varphi_p)$.

Démonstration. On peut étendre φ de manière unique en une application $\mathbb{Q}$-linéaire $\widetilde{\varphi} : \mathbb{Q}^r \to \mathbb{Q}^s$. Il s'agit d'un morphisme injectif de $\mathbb{Q}$-espaces vectoriels, donc il existe un morphisme $\psi : \mathbb{Q}^s \to \mathbb{Q}^r$ tel que $\psi \circ \widetilde{\varphi} = \mathrm{id}_{\mathbb{Q}^r}$.
Pour tout premier $p \nmid n$, on étend ψ en une application $\mathbb{Q}_p$-linéaire $\psi_p : \mathbb{Q}_p^s \to \mathbb{Q}_p^r$ et φ_p en une application $\mathbb{Q}_p$-linéaire $\widetilde{\varphi_p} : \mathbb{Q}_p^r \to \mathbb{Q}_p^s$. Comme la restriction de $\psi_p \circ \widetilde{\varphi_p}$ à $\mathbb{Q}^r$ vaut $\psi \circ \widetilde{\varphi} = \mathrm{id}_{\mathbb{Q}^r}$, on a $\psi_p \circ \widetilde{\varphi_p} = \mathrm{id}_{\mathbb{Q}_p^r}$.
On suppose que pour tout p premier ne divisant pas n, $y = \varphi_p(x_p)$.
En notant $z = (z_i)_{i\in[\![1;r]\!]} = \psi(y) \in \mathbb{Q}^r$, pour tout $p \nmid n$ on a

$$z = \psi_p(y) = \psi_p(\varphi_p(x_p)) = x_p \in \mathbb{Z}_p^r,$$

donc pour tout $i \in [\![1;r]\!]$, $v_p(z_i) \geq 0$. Soit $i \in [\![1;r]\!]$, pour tout $p \nmid n$ on a $v_p(z_i) \geq 0$, et comme $z_i \in \mathbb{Q}$, on en déduit que $z_i \in \mathbb{Z}[1/n]$.
Ainsi $z \in \mathbb{Z}[1/n]^r$ et en fixant $p_0 \nmid n$, on a

$$y = \varphi_{p_0}(x_{p_0}) = \varphi_{p_0}(z) = \varphi(z) \in \mathrm{Im}(\varphi).$$

Réciproquement, si $y = \varphi(z)$ avec $z \in \mathbb{Z}[1/n]^m$, alors pour tout $p \nmid n$ on a

$$y = \varphi_p(z) \in \mathrm{Im}(\varphi_p).$$

□

Corollaire 1.4.4. *Soit M un $\mathbb{Z}$-module fini.*
On a alors l'isomorphisme de $\mathbb{Z}[1/n]$-modules suivant

$$M \otimes \mathbb{Z}[1/n] \simeq \bigoplus_{p\nmid n \text{ premier}} \left(M \otimes \mathbb{Z}_p\right) \simeq \bigoplus_{p\nmid n \text{ premier}} \mathrm{Syl}_p(M).$$

Démonstration. On a $M \otimes \mathbb{Z}[1/n] = \bigoplus_{p \text{ premier}} \left(\mathrm{Syl}_p(M) \otimes \mathbb{Z}[1/n]\right)$.

– Si $p \mid n$, alors comme p est inversible dans $\mathbb{Z}[1/n]$ et que $\mathrm{Syl}_p(M)$ est un p-groupe, on a

$$\mathrm{Syl}_p(M) \otimes \mathbb{Z}[1/n] = 0.$$

– Si $p \nmid n$, on a $\mathbb{Z}_p \otimes \mathbb{Z}[1/n] \simeq \mathbb{Z}_p$ donc d'après la proposition précédente,

$$\mathrm{Syl}_p(M) \otimes \mathbb{Z}[1/n] \simeq M \otimes \mathbb{Z}_p \otimes \mathbb{Z}[1/n] \simeq M \otimes \mathbb{Z}_p \simeq \mathrm{Syl}_p(M).$$

□

Le cas $n = 1$ n'est qu'une reformulation du théorème de structure des groupes abéliens finis.

Corollaire 1.4.5. *Soit M un $\mathbb{Z}$-module fini.*
On a alors l'isomorphisme de $\mathbb{Z}$-modules suivant

$$M \simeq \bigoplus_{p \text{ premier}} M \otimes \mathbb{Z}_p.$$

La p-partie se comporte bien vis-à-vis du quotient.

Proposition 1.4.6. *Soit M un $\mathbb{Z}$-module et N un sous module de N.*
Alors

$$(M \otimes \mathbb{Z}_p)/(N \otimes \mathbb{Z}_p) \simeq (M/N) \otimes \mathbb{Z}_p.$$

Démonstration. La suite

$$0 \to N \to M \to M/N \to 0$$

est exacte et $\mathbb{Z}_p$ est un $\mathbb{Z}$-module plat, donc la suite

$$0 \to N \otimes \mathbb{Z}_p \to M \otimes \mathbb{Z}_p \to M/N \otimes \mathbb{Z}_p \to 0$$

est également exacte. On a donc

$$(M \otimes \mathbb{Z}_p)/(N \otimes \mathbb{Z}_p) \simeq (M/N) \otimes \mathbb{Z}_p.$$

□

1.4.2 p-partie et anneau de groupe

On considère un groupe abélien G.

Proposition 1.4.7. *On suppose que n est un entier non divisible par p et on considère un $\mathbb{Z}[1/n][G]$-module M.*
On a les isomorphismes de $\mathbb{Z}_p[G]$-modules

$$M \underset{\mathbb{Z}[1/n][G]}{\otimes} \mathbb{Z}_p[G] \simeq M \underset{\mathbb{Z}[1/n]}{\otimes} \mathbb{Z}_p \simeq M \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p.$$

Démonstration. L'application $\mathbb{Z}[1/n][G]$-bilinéaire

$$\varphi_0 : \begin{cases} M \times \mathbb{Z}_p[G] \to M \underset{\mathbb{Z}[1/n]}{\otimes} \mathbb{Z}_p \\ \left(m, \sum\limits_{g \in G} \alpha_g g\right) \mapsto \sum\limits_{g \in G} g\, m \otimes \alpha_g \end{cases}$$

induit une application $\mathbb{Z}[1/n][G]$-linéaire

$$\varphi : M \underset{\mathbb{Z}[1/n][G]}{\otimes} \mathbb{Z}_p[G] \to M \underset{\mathbb{Z}[1/n]}{\otimes} \mathbb{Z}_p.$$

cette application étant également $\mathbb{Z}_p$-linéaire, elle est $\mathbb{Z}_p[G]$-linéaire.
L'application $\mathbb{Z}[1/n]$-bilinéaire

$$\psi_0 : \begin{cases} M \times \mathbb{Z}_p \to M \underset{\mathbb{Z}[1/n][G]}{\otimes} \mathbb{Z}_p[G] \\ (m, \alpha) \mapsto m \otimes \alpha 1_G \end{cases}$$

induit une application $\mathbb{Z}[1/n]$-linéaire

$$\psi : M \underset{\mathbb{Z}[1/n]}{\otimes} \mathbb{Z}_p \to M \underset{\mathbb{Z}[1/n][G]}{\otimes} \mathbb{Z}_p[G].$$

On a $\psi \circ \varphi = \mathrm{id}_{M \underset{\mathbb{Z}[1/n][G]}{\otimes} \mathbb{Z}_p[G]}$ et $\varphi \circ \psi = \mathrm{id}_{M \underset{\mathbb{Z}[1/n]}{\otimes} \mathbb{Z}_p}$, donc φ est un isomorphisme de $\mathbb{Z}_p[G]$-modules. Une application entre des $\mathbb{Z}[1/n]$-modules est $\mathbb{Z}$-linéaire (respectivement $\mathbb{Z}$-bilinéaire) si et seulement si elle est $\mathbb{Z}[1/n]$-linéaire (respectivement $\mathbb{Z}[1/n]$-bilinéaire), d'où le deuxième isomorphisme en tant que $\mathbb{Z}[1/n]$-modules. Cet isomorphisme étant compatible avec l'action de G et celle de $\mathbb{Z}_p$, on a bien un isomorphisme de $\mathbb{Z}_p[G]$-modules. □

Soit I un idéal de $\mathbb{Z}[1/n][G]$ et $p \nmid n$ un nombre premier. On définit $I_p = \mathbb{Z}_p[G]\, I$ l'idéal engendré par I dans $\mathbb{Z}_p[G]$.

Proposition 1.4.8. *On suppose que $p \nmid n$.*
On a les isomorphismes de $\mathbb{Z}_p[G]$-modules

$$I_p \simeq I \underset{\mathbb{Z}[1/n]}{\otimes} \mathbb{Z}_p \simeq I \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p.$$

Démonstration. Le deuxième isomorphisme découle de celui de la proposition précédente.
On montre le premier à l'aide de la propriété universelle du produit tensoriel.
On définit

$$\varphi : \begin{cases} I \times \mathbb{Z}_p \to \mathbb{Z}_p[G]\, I \\ (x, \alpha) \mapsto \alpha 1_G x = \alpha x \end{cases}.$$

Soit M un $\mathbb{Z}[1/n]$-module et $f : I \times \mathbb{Z}_p \to M$ une application $\mathbb{Z}[1/n]$-bilinéaire. On peut alors définir

$$h : \begin{cases} \mathbb{Z}_p[G]\, I \to M \\ \Big(\sum\limits_{g\in G} a_g g\Big)x \mapsto \sum\limits_{g\in G} f(gx, a_g) \end{cases}.$$

Soit $a = \sum\limits_{g\in G} a_g g,\ b = \sum\limits_{g\in G} b_g g \in \mathbb{Z}_p[G]$ et $x = \sum\limits_{g\in G} x_g g,\ y = \sum\limits_{g\in G} y_g g \in I \subset \mathbb{Z}[1/n][G]$ tels que $ax = by$. Alors pour tout $h \in G$ on a

$$\sum_{g\in G} a_g x_{g^{-1}h} = \sum_{g\in G} b_g y_{g^{-1}h},$$

donc comme f est $\mathbb{Z}[1/n]$-bilinéaire on a

$$\begin{aligned} \sum_{g\in G} f(gx, a_g) &= \sum_{g\in G} f\Big(\sum_{h\in G} x_{g^{-1}h} h, a_g\Big) = \sum_{h\in G} f\Big(h, \sum_{g\in G} x_{g^{-1}h} a_g\Big) = \sum_{h\in G} f\Big(h, \sum_{g\in G} y_{g^{-1}h} b_g\Big) \\ &= \sum_{g\in G} f(gy, b_g) \end{aligned}$$

donc h est bien définie. L'application h est bien $\mathbb{Z}[1/n]$-linéaire, de plus pour tout $(x, \alpha) \in I \times \mathbb{Z}_p$, on a

$$h(\varphi(x, \alpha)) = h(\alpha 1_G x) = f(1_G x, \alpha) = f(x, \alpha),$$

donc

$$h \circ \varphi = f$$

et une telle application h est unique par surjectivité de φ.
Ainsi, φ induit un isomorphisme de $\mathbb{Z}[1/n]$-modules

$$\widetilde{\varphi} : \begin{cases} I \otimes \mathbb{Z}_p \to \mathbb{Z}_p[G]\, I \\ x \otimes \alpha \mapsto \alpha x \end{cases}.$$

Cet isomorphisme commute bien avec l'action de G et la multiplication par $\mathbb{Z}_p$, c'est donc un isomorphisme de $\mathbb{Z}_p[G]$-modules. □

Proposition 1.4.9. *Tout idéal de $\mathbb{Z}\left[1/n\right][G]$ est un $\mathbb{Z}\left[1/n\right]$-module libre de type fini.*

Démonstration. En tant que $\mathbb{Z}\left[1/n\right]$-module, $\mathbb{Z}\left[1/n\right][G]$ est libre de type fini. Comme $\mathbb{Z}\left[1/n\right]$ est principal (en effet, si J est un idéal de $\mathbb{Z}\left[1/n\right]$, $J = \mathbb{Z}\left[1/n\right](J \cap \mathbb{Z})$ et $J \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ donc principal), tout sous-$\mathbb{Z}\left[1/n\right]$-module de $\mathbb{Z}\left[1/n\right][G]$ est libre de type fini, or tout idéal de $\mathbb{Z}\left[1/n\right][G]$ est un sous-$\mathbb{Z}\left[1/n\right]$-module de $\mathbb{Z}\left[1/n\right][G]$, d'où le résultat. □

Corollaire 1.4.10. *L'anneau $\mathbb{Z}\left[1/n\right][G]$ est noethérien.*

Démonstration. D'après la proposition précédente, tout idéal de $\mathbb{Z}\left[1/n\right][G]$ est de type fini sur $\mathbb{Z}\left[1/n\right]$, donc sur $\mathbb{Z}\left[1/n\right][G]$. □

Plus généralement, on montre de la même façon que $A[G]$ est noethérien pour tout anneau noethérien A.

L'idéal I admet donc une base $(v_i)_{i\in[\![1;r]\!]}$ en tant que $\mathbb{Z}\left[1/n\right]$-module.

Proposition 1.4.11. *On suppose que le nombre premier p ne divise pas n.*
L'idéal I_p de $\mathbb{Z}_p[G]$ est un $\mathbb{Z}_p$-module libre de type fini, il admet $(v_i)_{i\in[\![1;r]\!]}$ comme base.

Démonstration. D'après les propositions 1.4.8 et 1.4.9, on a les isomorphismes de $\mathbb{Z}_p$-modules suivants :

$$I_p \simeq I \underset{\mathbb{Z}\left[1/n\right]}{\otimes} \mathbb{Z}_p \simeq \mathbb{Z}\left[1/n\right]^r \underset{\mathbb{Z}\left[1/n\right]}{\otimes} \mathbb{Z}_p \simeq \mathbb{Z}_p^r,$$

donc I_p est un $\mathbb{Z}_p$-module libre de rang r.
Comme pour tout $i \in [\![1;r]\!]$, $v_i \in I \subset \mathbb{Z}_p[G]\, I$ et comme $\mathbb{Z}_p[G]\, I$ est un $\mathbb{Z}_p$-module, on a

$$\mathrm{Vect}_{\mathbb{Z}_p}\Big((v_i)_{i\in[\![1;r]\!]}\Big) \subset \mathbb{Z}_p[G]\, I.$$

De plus, pour tout $x \in I$ et $a = \sum\limits_{g\in G} a_g g \in \mathbb{Z}_p[G]$, on a $ax = \sum\limits_{g\in G} a_g(gx)$, et comme I est un idéal de $\mathbb{Z}_p[G]$, pour tout $g \in G$,

$$gx \in I = \mathrm{Vect}_{\mathbb{Z}\left[1/n\right]}\Big((v_i)_{i\in[\![1;r]\!]}\Big) \subset \mathrm{Vect}_{\mathbb{Z}_p}\Big((v_i)_{i\in[\![1;r]\!]}\Big),$$

donc

$$ax \in \mathrm{Vect}_{\mathbb{Z}_p}\Big((v_i)_{i\in[\![1;r]\!]}\Big).$$

Ainsi, la famille $(v_i)_{i\in[\![1;r]\!]}$ est génératrice de I_p comme $\mathbb{Z}_p$-module, et de cardinal le rang de I_p, c'est donc une base. □

Théorème 1.4.12. *Soit $x \in \mathbb{Z}\left[1/n\right][G]$ tel que pour tout premier $p \nmid n$, $x \in I_p$.*
Alors $x \in I$.

Démonstration. Notons $G = \{g_1, ..., g_s\}$. Pour tout $i \in [\![1; r]\!]$, il existe $(v_{i,j})_{j\in[\![1,s]\!]} \in \mathbb{Z}\left[1/n\right]^s$ tel que $v_i = \sum_{j=1}^{s} v_{i,j} g_j$.
On définit une application $\mathbb{Z}$-linéaire

$$\varphi : \begin{cases} \mathbb{Z}\left[1/n\right]^r \to \mathbb{Z}\left[1/n\right]^s \\ (\alpha_i)_{i\in[\![1;r]\!]} \mapsto \left(\sum_{i=1}^{r} \alpha_i v_{i,j} \right)_{j\in[\![1;s]\!]} \end{cases}.$$

Comme $(v_i)_{i\in[\![1;r]\!]}$ est une base de I en tant que $\mathbb{Z}\left[1/n\right]$-module, elle est $\mathbb{Z}\left[1/n\right]$-libre et φ est injective. Pour tout $p \nmid n$ premier, on l'étend en

$$\varphi_p : \mathbb{Z}_p^r \to \mathbb{Z}_p^s.$$

Notons $x = \sum_{j=1}^{s} x_j g_j$. On a $x \in I$ si et seulement si $(x_j)_{j\in[\![1;s]\!]} \in \mathrm{Im}(\varphi)$ et $x \in I_p$ si et seulement si $(x_j)_{j\in[\![1;s]\!]} \in \mathrm{Im}(\varphi_p)$, donc le résultat découle de la proposition 1.4.3. □

Corollaire 1.4.13. *Soit I et J deux idéaux de $\mathbb{Z}\left[1/n\right][G]$.*
Alors $I = J$ si et seulement si pour tout nombre premier $p \nmid n$ on a $\mathbb{Z}_p[G]\, I = \mathbb{Z}_p[G]\, J$.

Démonstration. Supposons que pour tout $p \nmid n$ premier, $\mathbb{Z}_p[G]\, I = \mathbb{Z}_p[G]\, J$.
Soit $x \in J$. Alors $x \in \mathbb{Z}\left[1/n\right][G]$, et pour tout $p \nmid n$, $x \in \mathbb{Z}_p[G]\, J = \mathbb{Z}_p[G]\, I$, donc d'après le théorème précédent, $x \in I$. Ainsi $J \subset I$ et par symétrie des rôles, $I = J$. □

En particulier, en prenant $n = 1$, on obtient le résultat suivant :

Corollaire 1.4.14. *Soit I et J deux idéaux de $\mathbb{Z}[G]$.*
Alors $I = J$ si et seulement si pour tout nombre premier p on a $\mathbb{Z}_p[G]\, I = \mathbb{Z}_p[G]\, J$.

1.4.3 p-partie et cohomologie

Dans cette section nous allons voir que cohomologie et p-partie d'une G-module commutent.

Proposition 1.4.15. *Soit M un G-module.*
Alors on a les égalités suivantes :

$$I_G(M \otimes \mathbb{Z}_p) = (I_G M) \otimes \mathbb{Z}_p,$$

$$(M \otimes \mathbb{Z}_p)^G = M^G \otimes \mathbb{Z}_p,$$
$$\mathcal{N}_{G,M\otimes\mathbb{Z}_p}(M \otimes \mathbb{Z}_p) = \mathcal{N}_{G,M}(M) \otimes \mathbb{Z}_p,$$
$$\mathrm{Ker}(\mathcal{N}_{G,M\otimes\mathbb{Z}_p}) = \mathrm{Ker}(\mathcal{N}_{G,M}) \otimes \mathbb{Z}_p.$$

Démonstration. En effet, pour tout $x \in I_G$ et tout $\sum_i m_i \otimes a_i$, on a

$$x \sum_i m_i \otimes a_i = \sum_i xm_i \otimes a_i,$$

donc par linéarité

$$I_G(M \otimes \mathbb{Z}_p) = (I_G M) \otimes \mathbb{Z}_p$$

et

$$\mathcal{N}_{G,M\otimes\mathbb{Z}_p}(M \otimes \mathbb{Z}_p) = \mathcal{N}_G\left(M \otimes \mathbb{Z}_p\right) = \mathcal{N}_G M \otimes \mathbb{Z}_p = \mathcal{N}_{G,M}(M) \otimes \mathbb{Z}_p.$$

De plus, pour tout $g \in G$, en notant

$$\varphi_g : \begin{cases} M \to M \\ m \mapsto (1_G - g)m \end{cases},$$

comme $\mathbb{Z}_p$ est un module $\mathbb{Z}$-plat, on a

$$\mathrm{Ker}(\varphi_g \otimes \mathrm{id}_{\mathbb{Z}_p}) = \mathrm{Ker}(\varphi_g) \otimes \mathbb{Z}_p,$$

donc

$$\left(M \otimes \mathbb{Z}_p\right)^G = \bigcap_{g\in G} \mathrm{Ker}(\varphi_g \otimes \mathrm{id}_{\mathbb{Z}_p}) = \bigcap_{g\in G} \left(\mathrm{Ker}(\varphi_g) \otimes \mathbb{Z}_p\right) = M^G \otimes \mathbb{Z}_p.$$

Enfin la platitude de $\mathbb{Z}_p$ implique directement

$$\mathrm{Ker}(\mathcal{N}_{G,M\otimes\mathbb{Z}_p}) = \mathrm{Ker}(\mathcal{N}_{G,M}) \otimes \mathbb{Z}_p.$$

□

Ceci va nous permettre de déduire le comportement des groupes initiaux de cohomologie vis-à-vis de la p-partie.

Corollaire 1.4.16. *Soit M un G-module.*
Alors on a les égalités suivantes

$$\hat{H}^0(G, M \otimes \mathbb{Z}_p) \simeq \hat{H}^0(G, M) \otimes \mathbb{Z}_p,$$
$$\hat{H}^{-1}(G, M \otimes \mathbb{Z}_p) \simeq \hat{H}^{-1}(G, M) \otimes \mathbb{Z}_p.$$

Démonstration. D'après la proposition 1.4.6 sur le quotient des p-parties, on déduit de la proposition précédente les égalités suivantes :

$$\begin{aligned}\hat{H}^0(G, M \otimes \mathbb{Z}_p) &= (M \otimes \mathbb{Z}_p)^G / N_{G,M\otimes\mathbb{Z}_p}(M \otimes \mathbb{Z}_p) = M^G \otimes \mathbb{Z}_p / N_{G,M}(M) \otimes \mathbb{Z}_p \\ &\simeq (M^G / N_{G,M}(M)) \otimes \mathbb{Z}_p = \hat{H}^0(G, M) \otimes \mathbb{Z}_p,\end{aligned}$$

$$\begin{aligned}\hat{H}^{-1}(G, M \otimes \mathbb{Z}_p) &= \mathrm{Ker}(N_{G,M\otimes\mathbb{Z}_p})/I_G(M \otimes \mathbb{Z}_p) = (\mathrm{Ker}(N_{G,M}) \otimes \mathbb{Z}_p)/(I_G M \otimes \mathbb{Z}_p) \\ &\simeq (\mathrm{Ker}(N_{G,M})/I_G M) \otimes \mathbb{Z}_p = \hat{H}^{-1}(G, M) \otimes \mathbb{Z}_p.\end{aligned}$$

□

Nous pouvons ensuite en déduire le comportement de tous les groupes de cohomologie.

Proposition 1.4.17. *Soit M un G-module et $i \in \mathbb{Z}$.*
Alors

$$\hat{H}^i(G, M \otimes \mathbb{Z}_p) \simeq \hat{H}^i(G, M) \otimes \mathbb{Z}_p.$$

Démonstration. Considérons une suite exacte de G-modules

$$0 \to M \to M' \to M'' \to 0.$$

Alors la suite infinie

$$\begin{aligned}... \to \hat{H}^i(G, M) \to \hat{H}^i(G, M') \to \hat{H}^i(G, M'') \to ... \to \hat{H}^0(G, M) \to \hat{H}^0(G, M') \\ \to \hat{H}^0(G, M'') \to ... \to \hat{H}^j(G, M) \to \hat{H}^j(G, M') \to \hat{H}^j(G, M'') \to ...\end{aligned}$$

est exacte. Et comme $\mathbb{Z}_p$ est un $\mathbb{Z}$-module plat, on obtient l'exactitude de la suite suivante :

$$\begin{aligned}... \to \hat{H}^i(G, M) \otimes \mathbb{Z}_p \to \hat{H}^i(G, M') \otimes \mathbb{Z}_p \to \hat{H}^i(G, M'') \otimes \mathbb{Z}_p \to ... \\ \to \hat{H}^0(G, M) \otimes \mathbb{Z}_p \to \hat{H}^0(G, M') \otimes \mathbb{Z}_p \to \hat{H}^0(G, M'') \otimes \mathbb{Z}_p \to ... \\ \to \hat{H}^j(G, M) \otimes \mathbb{Z}_p \to \hat{H}^j(G, M') \otimes \mathbb{Z}_p \to \hat{H}^j(G, M'') \otimes \mathbb{Z}_p \to ...\end{aligned}$$

Ainsi, le corollaire précédent et l'unicité de la construction des groupes de cohomologie fournissent le résultat souhaité. □

En particulier, si M est un G-module cohomologiquement trivial, $M \otimes \mathbb{Z}_p$ en est également un.

1.5 Partie moins

Dans cette section, p désigne un nombre premier impair. On suppose que G possède un élément d'ordre 2 que l'on fixe et que l'on note τ.

Définition 1.5.1. *Soit M un G-module. On appelle partie moins de M et on note M^- le sous-module de M suivant :*

$$M^- = \{m \in M \text{ tel que } \tau(m) = -m\}.$$

Le but de cette section est de donner certaines propriétés de la partie moins.

Proposition 1.5.2. *Soit M et N deux G-modules.*
Alors

$$(M \oplus N)^- = M^- \oplus N^-.$$

Démonstration. Cela provient du fait que pour tout $(m, n) \in M \oplus N$, on a

$$(1 + \tau)(m, n) = ((1 + \tau)m, (1 + \tau)n).$$

□

Proposition 1.5.3. *Soit M un G-module et F un sous-groupe de G.*
Alors

$$\left(M^F\right)^- = (M^-)^F$$

et

$$\mathrm{Ker}\,(\mathcal{N}_{F,M})^- = \mathrm{Ker}\,(\mathcal{N}_{F,M^-}).$$

Démonstration.

$$\left(M^F\right)^- = M^F \cap M^- = (M^-)^F$$

et

$$\mathrm{Ker}(\mathcal{N}_{F,M})^- = \mathrm{Ker}\,(\mathcal{N}_{F,M}) \cap M^- = \mathrm{Ker}\,(\mathcal{N}_{F,M^-}).$$

□

On remarque que si M est un $\mathbb{Z}_p[G]$-module et si $\tau \in F$, alors $\left(M^F\right)^- = 0$. En effet, si $m \in \left(M^F\right)^-$, on a $\tau(m) = m$ car $m \in M^F$ et $\tau \in F$, et $\tau(m) = -m$ car $m \in M^-$, donc $2m = 0$, et comme M est un $\mathbb{Z}_p[G]$-module avec $p \neq 2$, on a $m = 0$.

Proposition 1.5.4. *Soit M un $\mathbb{Z}_p[G]$-module.*
Alors

$$M^- = (1 - \tau)M = \frac{1 - \tau}{2}M.$$

Démonstration. Si $m \in M$, alors

$$\tau((1-\tau)m) = (\tau - 1)m = -(1-\tau)m,$$

donc $(1-\tau)m \in M^-$ et

$$(1-\tau)M \subset M^-.$$

Si $m \in M^-$, comme $p \neq 2$, alors

$$m = \frac{m - \tau(m)}{2} = (1-\tau)\frac{m}{2} \in (1-\tau)M.$$

Donc

$$M^- \subset (1-\tau)M.$$

De plus, comme $p \neq 2$ et comme M est un $\mathbb{Z}_p[G]$-module, on a

$$M = \frac{1}{2}M.$$

□

On en déduit alors que la partie moins et la p-partie commutent :

Proposition 1.5.5. *Soit M un G-module.*
Alors

$$\left(M \otimes \mathbb{Z}_p\right)^- = M^- \otimes \mathbb{Z}_p.$$

Démonstration. D'après la proposition précédente, comme $M \otimes \mathbb{Z}_p$ est un $\mathbb{Z}_p[G]$-module,

$$\left(M \otimes \mathbb{Z}_p\right)^- = (1-\tau)\left(M \otimes \mathbb{Z}_p\right) = (1-\tau)M \otimes \mathbb{Z}_p.$$

Or $(1+\tau)(1-\tau) = 0$, donc $(1-\tau)M \subset M^-$. On a alors

$$\left(M \otimes \mathbb{Z}_p\right)^- \subset M^- \otimes \mathbb{Z}_p.$$

De plus $(1+\tau)\left(M^- \otimes \mathbb{Z}_p\right) = (1+\tau)M^- \otimes \mathbb{Z}_p = 0$, donc

$$M^- \otimes \mathbb{Z}_p \subset \left(M \otimes \mathbb{Z}_p\right)^-.$$

□

Notation. On note $e^- = \frac{1-\tau}{2} \in \mathbb{Z}[1/2][G]$.

On remarque que $e^- \in \mathbb{Q}[G]$ et pour tout p premier impair, $e^- \in \mathbb{Z}_p[G]$.

Proposition 1.5.6. *Le $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p[G]^-$ muni de la multiplication de $\mathbb{Z}_p[G]$ est un anneau commutatif d'unité e^-.*

Démonstration. D'après la proposition 1.5.4, on a

$$\mathbb{Z}_p[G]^- = e^-\mathbb{Z}_p[G],$$

et

$$e^{-2} = e^-.$$

□

On a un comportement identique sur $\mathbb{Q}[G]$:

Proposition 1.5.7. *Le $\mathbb{Q}[G]$-module $\mathbb{Q}[G]^-$ muni de la multiplication de $\mathbb{Q}[G]$ est un anneau commutatif d'unité e^-.*

En revanche, le G-module $\mathbb{Z}[G]^-$ muni de la multiplication de $\mathbb{Z}[G]$ n'est pas un anneau. En effet, supposons par l'absurde que $\mathbb{Z}[G]^-$ admette une unité e, comme $1-\tau \in \mathbb{Z}[G]^-$, on a $e(1-\tau) = 1-\tau$, or $e(1-\tau) = e + e = 2e$, donc $2e = 1-\tau$, mais $\frac{1-\tau}{2} \notin \mathbb{Z}[G]$, donc $e \notin \mathbb{Z}[G]^-$, d'où la contradiction.
Ainsi, on considérera plutôt l'anneau suivant, qui n'est pas inclus dans $\mathbb{Z}[G]$:

Définition 1.5.8. *On note $\mathbb{Z}[G]^\sim = e^-\mathbb{Z}[G] \subset \mathbb{Q}[G]$ et on le munit de l'addition et de la multiplication de $\mathbb{Q}[G]$.*
C'est un anneau commutatif d'unité e^-.

On remarque que $\mathbb{Z}[G]^- = 2\mathbb{Z}[G]^\sim$.

Proposition 1.5.9. *Soit M un $\mathbb{Z}_p[G]$-module.*
Alors

$$(N_{G,M}(M))^- = N_{G,M^-}(M^-)$$

et

$$(I_G M)^- = I_G(M^-).$$

Démonstration. Comme G est abélien, on a :
– $(N_{G,M}(M))^- = (1-\tau)N_{G,M}(M) = N_{G,M}((1-\tau)M) = N_{G,M}(M^-) = N_{G,M^-}(M^-)$,
– $(I_G M)^- = (1-\tau)(I_G M) = I_G((1-\tau)M) = I_G(M^-)$.

□

Proposition 1.5.10. *Soit*

$$0 \to M_1 \overset{f_1}{\to} M_2 \overset{f_2}{\to} M_3 \to 0$$

une suite exacte de $\mathbb{Z}_p[G]$-modules.
Alors,

$$0 \to (1+\tau)M_1 \overset{\widetilde{f_1}}{\to} (1+\tau)M_2 \overset{\widetilde{f_2}}{\to} (1+\tau)M_3 \to 0$$

est exacte.

Démonstration. $\widetilde{f_1}$ et $\widetilde{f_2}$ sont les restrictions de f_1 et f_2, on a donc :
– $\widetilde{f_1}$ est injective car f_1 est injective.
– Comme $\mathrm{Im}(f_1) \subset \mathrm{Ker}(f_2)$, $f_2 \circ f_1 = 0$, donc $\widetilde{f_2} \circ \widetilde{f_1} = 0$ puis $\mathrm{Im}(\widetilde{f_1}) \subset \mathrm{Ker}(\widetilde{f_2})$.
– Soit $(1+\tau)m \in \mathrm{Ker}(\widetilde{f_2})$. Comme $\mathrm{Ker}(\widetilde{f_2}) \subset \mathrm{Ker}(f_2) = \mathrm{Im}(f_1)$, $(1+\tau)m = f_1(n)$, avec $n \in M_1$.
Or $(1+\tau)^2 = 2(1+\tau)$, donc

$$(1+\tau)m = (1+\tau)^2\frac{m}{2} = (1+\tau)\frac{f_1(n)}{2} = f_1\left((1+\tau)\frac{n}{2}\right) \in f_1((1+\tau)M_1) = \mathrm{Im}(\widetilde{f_1}).$$

Donc

$$\mathrm{Ker}(\widetilde{f_2}) \subset \mathrm{Im}(\widetilde{f_1}).$$

– Soit $m \in M_3$. L'application f_2 est surjective, donc $m = f_2(n)$, avec $n \in M_2$, donc

$$(1+\tau)m = f_2((1+\tau)n) = \widetilde{f_2}((1+\tau)n).$$

Ainsi, $\widetilde{f_2}$ est surjective.

□

Proposition 1.5.11. *Soit* $0 \to M_1 \to M_2 \to M_3 \to 0$ *une suite exacte de $\mathbb{Z}_p[G]$-modules.*
Alors, $0 \to M_1^- \to M_2^- \to M_3^- \to 0$ *est exacte.*
Autrement dit, le foncteur $\mathcal{F}^-$, défini par $\mathcal{F}^-(M) = M^-$ et $\mathcal{F}^-(f) = f^- = f\big|_{M^-}^{N^-}$ pour tous $\mathbb{Z}_p[G]$-modules M et N et tout morphisme de $\mathbb{Z}_p[G]$-modules $f : M \to N$, est un foncteur exact de la catégorie des $\mathbb{Z}_p[G]$-modules vers la catégorie des $\mathbb{Z}_p[G]$-modules.

Démonstration. D'après la proposition précédente,

$$0 \to (1+\tau)M_1 \to (1+\tau)M_2 \to (1+\tau)M_3 \to 0$$

est exacte, donc on peut appliquer le lemme du serpent aux suites

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

$$0 \to (1+\tau)M_1 \to (1+\tau)M_2 \to (1+\tau)M_3 \to 0.$$

Comme pour tout $i \in [\![1;3]\!]$,

$$\mathrm{Ker}\,(1+\tau : M_i \to (1+\tau)M_i) = M_i^-$$

et

$$\mathrm{Coker}\,(1+\tau : M_i \to (1+\tau)M_i) = 0,$$

on obtient l'exactitude de la suite

$$0 \to M_1^- \to M_2^- \to M_3^- \to 0.$$

□

On peut également démontrer directement cette proposition en utilisant le fait que pour tout $\mathbb{Z}_p[G]$-module M, on a $M^- = (1-\tau)M$ et en procédant de manière analogue à la proposition précédente.

Corollaire 1.5.12. *Soit M un $\mathbb{Z}_p[G]$-module et N un sous-module de M.*
Alors

$$(M/N)^- \simeq M^-/N^-.$$

Proposition 1.5.13. *Soit F un sous-groupe de G, M un $\mathbb{Z}_p[G]$-module et $i \in \mathbb{Z}$.*
Alors

$$\hat{H}^i(F, M^-) = \hat{H}^i(F, M)^-.$$

Démonstration. On procède de manière analogue à la preuve de 1.4.17 :
Les propositions 1.5.12, 1.5.3 et 1.5.9 permettent d'obtenir le résultat pour $i = 0$ et -1.
Puis la proposition 1.5.11 permet de construire la suite exacte infinie des groupes de cohomologie de M^- comme étant les parties moins des groupes de cohomologie de M. □

Dans le cas particulier où $\tau \in F$, ce groupe est alors trivial.

En combinant ce résultat à la proposition 1.4.17, on obtient le résultat suivant.

Proposition 1.5.14. *Soit M un G-module et F un sous-groupe de G.*
Alors, pour $i \in \mathbb{Z}$, on a

$$\hat{H}^i(F, (M^- \otimes \mathbb{Z}_p)) = (\hat{H}^i(F, M) \otimes \mathbb{Z}_p)^-.$$

Et en particulier, on a :

Proposition 1.5.15. *Le G-module $\mathbb{Z}_p[G]^-$ est cohomologiquement trivial.*

Démonstration. Soit F un sous-groupe de G et $i \in \mathbb{Z}$. Comme $\mathbb{Z}[G]$ est un G-module cohomologiquement trivial, on a $\hat{H}^i(F, \mathbb{Z}[G]) = 0$. Donc d'après la proposition précédente

$$\hat{H}^i(F, \mathbb{Z}_p[G]^-) = \hat{H}^i(F, (\mathbb{Z}[G] \otimes \mathbb{Z}_p)^-) = (\hat{H}^i(F, \mathbb{Z}[G]) \otimes \mathbb{Z}_p)^- = 0.$$

□

1.6 Idéal de Fitting

Dans cette partie, on rappelle et démontre les propriétés générales des idéaux de Fitting que l'on trouve par exemple dans l'appendice de [MW84], puis on établit un principe local-global pour les idéaux de Fitting dans le cadre des anneaux de groupe $\mathbb{Z}[1/n][G]$.
On désigne par A un anneau commutatif et par M un A-module de type fini. On note $f : A^r \to M$ une application A-linéaire surjective, où $r \in \mathbb{N}$.

Définition 1.6.1. *L'idéal de Fitting de M sur A est l'idéal de A engendré par les* $\det(v_1, ..., v_r)$ *où les* v_i *parcourent* $\mathrm{Ker}(f)$*, on le note* $\mathrm{Fitt}_A(M)$.

Il s'agit ici de l'idéal de Fitting initial, ou zéroième idéal de Fitting. Pour la définition générale du n-ième idéal de Fitting et les démonstrations de ses propriétés, on peut se référer à [Nor76].

Commençons par montrer que l'idéal de Fitting est bien défini indépendamment du choix de la surjection f.

Lemme 1.6.2. *Soit $l : A^{r+1} \to M$ une application A-linéaire telle que pour tout $(a_1, ..., a_r) \in A^r$ on a $l(a_1, ..., a_r, 0) = f(a_1, ..., a_r)$.*
Alors les surjections f et l fournissent le même idéal de Fitting.

Démonstration. Comme f est surjective, il existe $b = (b_1, ..., b_r) \in A^r$ tel que $l(0, ..., 0, 1) = f(b_1, ..., b_r)$. Pour tout $(a_1, ..., a_{r+1}) \in A^{r+1}$, on a

$$l(a_1, ..., a_{r+1}) = f(a_1 + a_{r+1}b_1, ..., a_r + a_{r+1}b_r).$$

Soit $(a_1, ..., a_{r+1}) \in \mathrm{Ker}(l)$, alors

$$(a_1 + a_{r+1}b_1, ..., a_r + a_{r+1}b_r) \in \mathrm{Ker}(f),$$

donc en notant $B = \mathrm{Ker}(f) \times \{0_A\} \cup \{(-b, 1)\}$, on a

$$(a_1, ..., a_{r+1}) = (a_1 + a_{r+1}b_1, ..., a_r + a_{r+1}b_r, 0) + a_{r+1}(-b_1, ..., -b_r, 1) \in \mathrm{Vect}_A(B)$$

et

$$\mathrm{Ker}(l) \subset \mathrm{Vect}_A(B).$$

Réciproquement,

$$l(-b, 1) = l(0, ..., 0, 1) - f(b) = 0$$

et

$$\mathrm{Ker}(f) \times \{0_A\} \subset \mathrm{Ker}(l),$$

donc par linéarité

$$\mathrm{Vect}_A(B) \subset \mathrm{Ker}(l)$$

et

$$\mathrm{Ker}(l) = \mathrm{Vect}_A(B).$$

Soit $w_1, ..., w_{r+1} \in B$. Alors si $\det(w_1, ..., w_{r+1}) \neq 0$, exactement un (w_i) est égal à $(-b, 1)$, donc on peut supposer que pour tout $i \in [\![1; r]\!]$, $w_i = (v_i, 0)$ avec $v_i \in \mathrm{Ker}(f)$ et $w_{r+1} = (-b, 1)$. En développant par rapport à la dernière ligne, on a

$$\det(w_1, ..., w_{r+1}) = \det(v_1, ..., v_r).$$

On a donc $\det(B^{r+1}) \subset \det(\mathrm{Ker}(f)^r)$, et par linéarité du déterminant,

$$\mathrm{Vect}_A(\det(\mathrm{Ker}(l)^{r+1})) = \mathrm{Vect}_A(\det(B^{r+1})) \subset \mathrm{Vect}_A(\det(\mathrm{Ker}(f)^r)).$$

Réciproquement, si $v_1, ..., v_r \in \mathrm{Ker}(f)$,

$$\det(v_1, ..., v_r) = \det((v_1, 0), ..., (v_r, 0), (-b, 1)) \in \det(\mathrm{Ker}(l)^{r+1}),$$

donc

$$\mathrm{Vect}_A(\det(\mathrm{Ker}(l)^{r+1})) = \mathrm{Vect}_A(\det(\mathrm{Ker}(f)^r)).$$

□

Proposition 1.6.3. *Soit $h : A^s \to M$ une surjection A-linéaire, où $s \in \mathbb{N}$. Alors l'idéal de Fitting de M fourni par h est égal à celui fourni par f.*

Démonstration. On définit une troisième surjection

$$l : \begin{cases} A^{r+s} \to M \\ (v, w) \mapsto f(v) + h(w) \end{cases}.$$

On déduit par récurrence du lemme précédent que l fournit le même idéal de Fitting que f d'une part, et que h d'autre part. Ainsi, f et h fournissent le même idéal de Fitting. □

L'idéal de Fitting représente un certain raffinement de l'annulateur, comme l'indique la proposition suivante.

Notation. On note

$$\mathrm{Ann}_A(M) = \{a \in A \text{ tel que } am = 0_M \text{ pour tout } m \in M\}$$

l'annulateur de M sur A.

Proposition 1.6.4. *On a*

$$\mathrm{Ann}_A(M)^r \subset \mathrm{Fitt}_A(M) \subset \mathrm{Ann}_A(M).$$

Démonstration. Soit $a_1, ..., a_r \in \mathrm{Ann}_A(M)$. Notons $(e_j)_{j\in[\![1;r]\!]}$ la base canonique de A^r et pour tout $j \in [\![1; r]\!]$, notons $v_j = a_j e_j \in A$. Alors pour tout $j \in [\![1; r]\!]$, on a $f(v_j) = a_j f(e_j) = 0_M$ car $a_j \in \mathrm{Ann}_A(M)$, donc

$$\det(v_1, ..., v_r) = a_1 ... a_r \in \mathrm{Fitt}_A(M).$$

Soit $v_1, ..., v_r \in \mathrm{Ker}(f)$, on note $V \in M_r(A)$ la matrice dont la j-ième colonne est le vecteur v_j. On note $h : A^r \to A^r$ l'application A-linéaire dont la matrice dans la base canonique est V et $l : A^r \to A^r$ celle dont la matrice est la transposée de la comatrice de V.
Pour tout $a \in A^r$, on a $h \circ l(a) = \det(V)a$, donc

$$\det(V)f(a) = f(\det(V)a) = f(h \circ l(a)) = 0_M$$

car

$$\mathrm{Im}(h) = \mathrm{Vect}_A(v_1, ..., v_r) \subset \mathrm{Ker}(f).$$

Or f est surjective, donc $\det(V) \in \mathrm{Ann}_A(M)$ et comme $\mathrm{Ann}_A(M)$ est un idéal de A, par linéarité,

$$\mathrm{Fitt}_A(M) \subset \mathrm{Ann}_A(M).$$

□

Proposition 1.6.5. *Soit N un deuxième A-module de type fini.*
Alors

$$\mathrm{Fitt}_A(M \oplus N) = \mathrm{Fitt}_A(M)\mathrm{Fitt}_A(N).$$

Démonstration. Soit $h : A^s \to N$ un morphisme A-linéaire surjectif.
On définit $l : A^{r+s} \to M \oplus N$ par $l(a, b) = (f(a), h(b))$. On a

$$\mathrm{Ker}(l) = \mathrm{Ker}(f) \times \{0_{A^s}\} \oplus \{0_{A^r} \times \mathrm{Ker}(h)\}.$$

Comme le déterminant est multilinéaire et alterné, $\mathrm{Fitt}_A(M \oplus N)$ est engendré sur A par les $\det((a_1, 0), ..., (a_{r'}, 0), (0, b_1), ..., (0, b_{s'}))$ avec $a_i \in \mathrm{Ker}(f)$ et $b_i \in \mathrm{Ker}(h)$. Pour que ces déterminants soient non nuls, on a nécessairement $r' = r$ et $s' = s$, et donc

$$\det((a_1, 0), ..., ab_r, 0), (0, b_1), ..., (0, b_s)) = \det(a_1, ..., a_r) \det(b_1, ..., b_s).$$

Donc par linéarité,

$$\mathrm{Fitt}_A(M \oplus N) = \mathrm{Fitt}_A(M)\mathrm{Fitt}_A(N).$$

□

Proposition 1.6.6. *Soit I un idéal de A.*
Alors

$$\mathrm{Fitt}_A(A/I) = I.$$

Démonstration. Soit f la projection de A sur A/I. L'application f est surjective et $\mathrm{Ker}(f) = I$, donc $\mathrm{Fitt}_A(A/I) = \mathrm{Vect}_A(\mathrm{Ker}(f)) = \mathrm{Vect}_A(I) = I$. □

En combinant les deux propositions précédentes, on obtient le résultat suivant, qui concerne en particulier les idéaux de Fitting de tout module sur un anneau principal.

Corollaire 1.6.7. *Supposons qu'il existe des idéaux $I_1, ..., I_n$ tel que M soit isomorphe à $A/I_1 \oplus ... \oplus A/I_n$ comme A-module.*
Alors

$$\mathrm{Fitt}_A(M) = I_1...I_n.$$

Dans certains cas, on peut en déduire un résultat sur les cardinaux.

Proposition 1.6.8. *Soit A un anneau principal infini et M un A-module fini.*
Alors

$$\mathrm{card}(A/\mathrm{Fitt}_A(M)) = \mathrm{card}(M).$$

Lemme 1.6.9. *Soit A un anneau principal et $c, d \in A \setminus \{0_A\}$.*
Alors

$$\mathrm{card}(A/cdA) = \mathrm{card}(A/cA)\mathrm{card}(A/dA).$$

Démonstration. Le morphisme de A-modules

$$\varphi : \begin{cases} A/cdA \to A/cA \\ a + cdA \mapsto a + cA \end{cases}$$

est surjectif, de noyau $\mathrm{Ker}(\varphi) = cA/cdA$ donc

$$\mathrm{card}(A/cdA) = \mathrm{card}(A/cA)\mathrm{card}(cA/cdA).$$

Le morphisme de A-modules

$$\psi : \begin{cases} A \to cA/cdA \\ a \mapsto ca + cdA \end{cases}$$

est surjectif. Comme A est intègre et c non nul, $\ker(\psi) = dA$, donc

$$\text{card}(cA/cdA) = \text{card}(A/dA).$$

□

Démonstration de la proposition. D'après le théorème de structure des modules de type fini sur les anneaux principaux, il existe $m \in \mathbb{N}$ et $a_1, ..., a_m \in A$ tels que

$$M \simeq A/a_1A \oplus ... \oplus A/a_mA.$$

Comme A est infini et M est fini, les a_i sont non nuls, donc d'après le lemme précédent, on déduit par récurrence que

$$\text{card}(M) = \text{card}(A/a_1A)...\text{card}(A/a_mA) = \text{card}(A/a_1...a_mA).$$

D'après le corollaire 1.6.7

$$\text{Fitt}_A(M) = a_1A...a_mA = a_1...a_mA$$

donc on a bien

$$\text{card}(A/\text{Fitt}_A(M)) = \text{card}(M).$$

□

En particulier, ce résultat s'applique sur les anneaux d'entiers de corps de nombres lorsqu'ils sont principaux, ainsi que sur les anneaux de valuation discrète.

Proposition 1.6.10. *Soit B une A-algèbre associative.*
Alors

$$\text{Fitt}_B(M \underset{A}{\otimes} B) = B\,\text{Fitt}_A(M).$$

Démonstration. Comme le produit tensoriel est exact à droite et comme $A^s \underset{A}{\otimes} B$ est isomorphe à B^s en tant que B-module, on a la suite exacte de B-modules suivante :

$$\text{Ker}(f) \underset{A}{\otimes} B \xrightarrow{h} B^s \xrightarrow{l} M \underset{A}{\otimes} B \to 0,$$

avec

$$h((a_1, ..., a_s) \otimes b) = (a_1b, ..., a_sb)$$

et

$$l(b_1, ..., b_s) = \sum_{i=1}^{s} f(e_i) \otimes b_i \text{ où } (e_i) \text{ est la base canonique de } A^s.$$

On a alors

$$\mathrm{Ker}(l) = \mathrm{Im}(h) = \mathrm{Vect}_B(\mathrm{Ker}(f)),$$

donc par multilinéarité du déterminant,

$$\mathrm{Fitt}_B(M \underset{A}{\otimes} B) = \mathrm{Vect}_B(\det(\mathrm{Vect}_B(\mathrm{Ker}(f))^s)) = \mathrm{Vect}_B(\det(\mathrm{Ker}(f)^s)) = B\,\mathrm{Fitt}_A(M).$$

□

Corollaire 1.6.11. *Soit B une A-algèbre et M un A-module.*
On a alors l'isomorphisme de A-modules suivant

$$\mathrm{Fitt}_B(M \underset{A}{\otimes} B) \simeq \mathrm{Fitt}_A(M) \underset{A}{\otimes} B.$$

Démonstration. D'après la proposition 1.3.1, on a $\mathrm{Fitt}_A(M) \underset{A}{\otimes} B \simeq B\,\mathrm{Fitt}_A(M)$ et donc le résultat découle de la proposition précédente. □

Nous pouvons également déduire de la proposition précédente un résultat concernant la partie moins.

Corollaire 1.6.12. *Soit p un nombre premier impair et M un $\mathbb{Z}_p[G]$-module.*
Alors on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}(M^-) = e^-\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M).$$

Démonstration. D'après la proposition 1.6.10, comme $\mathbb{Z}_p[G]^-$ est une $\mathbb{Z}_p[G]$-algèbre associative, on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}(M \underset{\mathbb{Z}_p[G]}{\otimes} \mathbb{Z}_p[G]^-) = \mathbb{Z}_p[G]^- \ \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = e^-\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M).$$

Or

$$M \underset{\mathbb{Z}_p[G]}{\otimes} \mathbb{Z}_p[G]^- = M \underset{\mathbb{Z}_p[G]}{\otimes} e^-\mathbb{Z}_p[G] = e^-M \underset{\mathbb{Z}_p[G]}{\otimes} \mathbb{Z}_p[G] \simeq e^-M,$$

donc

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}(M^-) = \mathrm{Fitt}_{\mathbb{Z}_p[G]^-}(M \underset{\mathbb{Z}_p[G]}{\otimes} \mathbb{Z}_p[G]^-) = e^-\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M).$$

□

On en déduit également un principe local-global sur les idéaux de Fitting.

Théorème 1.6.13 (Principe local-global des idéaux de Fitting.)**.** *Soit M un $\mathbb{Z}\left[1/n\right][G]$-module de type fini et I un idéal de $\mathbb{Z}\left[1/n\right][G]$.*
Alors

$$\mathrm{Fitt}_{\mathbb{Z}[1/n][G]}(M) = I$$

si et seulement si pour tout $p \nmid n$ premier

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M \otimes \mathbb{Z}_p) = \mathbb{Z}_p\left[G\right] I.$$

Démonstration. D'après la proposition 1.4.13, on a

$$\mathrm{Fitt}_{\mathbb{Z}[1/n][G]}(M) = I$$

si et seulement si pour tout $p \nmid n$ premier

$$\mathbb{Z}_p\left[G\right] \mathrm{Fitt}_{\mathbb{Z}[1/n][G]}(M) = \mathbb{Z}_p\left[G\right] I.$$

D'après la proposition 1.6.10, on a

$$\mathbb{Z}_p\left[G\right] \mathrm{Fitt}_{\mathbb{Z}[1/n][G]}(M) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M \underset{\mathbb{Z}[1/n][G]}{\otimes} \mathbb{Z}_p\left[G\right]),$$

et comme $M \underset{\mathbb{Z}[1/n][G]}{\otimes} \mathbb{Z}_p\left[G\right]$ et $M \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p$ sont isomorphes en tant que $\mathbb{Z}_p\left[G\right]$-modules, on a

$$\mathbb{Z}_p\left[G\right] \mathrm{Fitt}_{\mathbb{Z}[1/n][G]}(M) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p),$$

d'où le résultat. □

Chapitre 2

χ-composantes

Soit G un groupe abélien fini, p un nombre premier, $G_p = \mathrm{Syl}_p(G)$ le p-Sylow de G et Δ un supplémentaire de G_p.

2.1 Caractères p-adiques et idempotents

2.1.1 Caractères irréductibles sur $\mathbb{Q}_p[\chi]$

Soit $\chi : G \to \overline{\mathbb{Q}}_p^\times$ un $\overline{\mathbb{Q}}_p$-caractère irréductible de G. Comme G est abélien et $\overline{\mathbb{Q}}_p$ algébriquement clos, il s'agit d'un caractère linéaire.

Notation. On note $\mathbb{Q}_p[\chi]$ l'extension de $\mathbb{Q}_p$ engendrée par les valeurs prises par χ, $\mathbb{Q}_p[\chi]$ est donc un corps cyclotomique local. On note $\mathbb{Z}_p[\chi]$ son anneau des entiers, qui est engendré sur $\mathbb{Z}_p$ par les valeurs prises par χ.

On dit que χ est un $\mathbb{Q}_p[\chi]$-caractère irréductible. Et comme les valeurs prises par χ sont des racines de l'unité, on a $\chi : G \to \mathbb{Z}_p[\chi]^\times$ et on peut aussi parler de $\mathbb{Z}_p[\chi]$-caractère irréductible.

Notation. On note X_{irr} l'ensemble des $\overline{\mathbb{Q}}_p$-caractères irréductibles de G.

Définition 2.1.1. *On dit que deux $\overline{\mathbb{Q}}_p$-caractères irréductibles $\chi : G \to \overline{\mathbb{Q}}_p^\times$ et $\chi' : G \to \overline{\mathbb{Q}}_p^\times$ sont conjugués s'il existe $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ tel que $\chi' = \sigma\chi$.*
Il s'agit d'une relation d'équivalence et on note C_χ la classe d'équivalence d'un caractère χ.

On remarque que deux caractères χ et χ' sont conjugués si et seulement s'il existe $\sigma \in \mathrm{Gal}(\mathbb{Q}_p[\chi]/\mathbb{Q}_p)$ tel que $\chi' = \sigma\chi$, ce qui implique en particulier que si deux caractères χ et χ' sont conjugués, on a $\mathbb{Q}_p[\chi] = \mathbb{Q}_p[\chi']$.
On a donc

$$C_\chi = \left\{\sigma\chi, \text{ avec } \sigma \in \mathrm{Gal}(\mathbb{Q}_p[\chi]/\mathbb{Q}_p)\right\}.$$

Définition 2.1.2. *On définit ainsi l'idempotent associé à χ*

$$e_\chi = \frac{1}{\mathrm{card}(G)} \sum_{g\in G} \chi(g^{-1})g \in \mathbb{Q}_p[\chi][G].$$

Si p ne divise pas l'ordre de G, on a $e_\chi \in \mathbb{Z}_p[\chi][G]$.

Proposition 2.1.3. *La famille composée des e_χ pour tous les $\chi \in X_{\mathrm{irr}}$ est un système fondamental d'idempotents orthogonaux :*

1. *pour tout $\chi \in X_{\mathrm{irr}}$, on a $e_\chi^2 = e_\chi$,*
2. *pour tout $\chi \neq \chi' \in X_{\mathrm{irr}}$, on a $e'_\chi e_\chi = 0$,*
3. *on a $\sum_{\chi\in X_{\mathrm{irr}}} e_\chi = 1_G$.*

Démonstration. Soit $\chi, \chi' \in X_{\mathrm{irr}}$, on a

$$\begin{aligned} e'_\chi e_\chi &= \tfrac{1}{\mathrm{card}(G)^2} \sum_{g\in G}\sum_{h\in G} \chi(g^{-1})\chi'(h^{-1})gh = \tfrac{1}{\mathrm{card}(G)^2} \sum_{g\in G}\sum_{h\in G} \chi(hg^{-1})\chi'(h^{-1})g \\ &= \tfrac{1}{\mathrm{card}(G)^2} \sum_{g\in G}\Big(\sum_{h\in G} \chi(h)\chi'(h^{-1})\Big)\chi(g^{-1})g \end{aligned}$$

Si $\chi = \chi'$, on a $\sum_{h\in G} \chi(h)\chi(h^{-1}) = \mathrm{card}(G)$ donc $e_\chi^2 = e_\chi$.
Si $\chi \neq \chi'$, on a $\sum_{h\in G} \chi(h)\chi'(h^{-1}) = 0$, donc $e'_\chi e_\chi = 0$.
On a $\sum_{\chi\in X_{\mathrm{irr}}} e_\chi = \frac{1}{\mathrm{card}(G)} \sum_{g\in G}\Big(\sum_{\chi\in X_{\mathrm{irr}}} \chi(g^{-1})\Big)g$.
Or $\sum_{\chi\in X_{\mathrm{irr}}} \chi(1_G) = \mathrm{card}(X_{\mathrm{irr}}) = \mathrm{card}(G)$ et $\sum_{\chi\in X_{\mathrm{irr}}} \chi(g) = 0$ pour tout $g \neq 1_G$, donc $\sum_{\chi\in X_{\mathrm{irr}}} e_\chi = 1_G$. □

2.1.2 Caractères irréductibles sur $\mathbb{Q}_p$

On s'intéresse dans cette section à des caractères ψ qui sont irréductibles sur $\mathbb{Q}_p$, dont la dimension n'est donc en général plus égale à 1. Dans un premier temps, on se placera dans un cadre plus général que $\mathbb{Q}_p$ qui pourra ainsi s'appliquer aussi bien à $\mathbb{Q}$ qu'à $\mathbb{Q}_p$. On suppose donc que K est un corps de caractéristique 0.

Notation. Pour tout χ caractère irréductible de G sur $\overline{K}$, on note $K[\chi]$ l'extension de K engendrée par les valeurs de χ, G_χ le groupe de Galois de $K[\chi]/K$ et

$$\psi_\chi = \mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p}(\chi) = \sum_{\sigma \in G_\chi} \sigma\chi$$

la somme des conjugués galoisiens de χ.

On va chercher à démontrer que ψ_χ est un caractère de G irréductible sur K.

Lemme 2.1.4. *Soit χ un caractère de G irréductible sur $\overline{K}$.*
Alors ψ_χ est un caractère de G défini sur K.

Démonstration. Notons ζ une racine primitive de l'unité telle que $K[\chi] = K(\zeta)$, $m = [K[\chi] : K]$ et $\sigma_1, ..., \sigma_m$ les éléments de $G_\chi = \mathrm{Gal}(K[\chi]/K) = \mathrm{Gal}(K(\zeta)/K)$. Pour tout $j \in [\![1; m]\!]$, on pose $\chi_j = \sigma_j\chi$ et ρ_j la représentation de $K[\chi]$ de dimension 1 associée. On définit la représentation $\rho_\chi = \rho_1 \oplus ... \oplus \rho_m$ de dimension m dans la base canonique de $K[\chi]^m$.
Pour tout $i \in \mathbb{N}^*$, posons $v_i = \left(\sigma_j(\zeta)^{i-1}\right)_{j \in [\![1;m]\!]}$.
Comme

$$\det(v_1, ..., v_m) = \prod_{j \neq j'} \left(\sigma_j(\zeta) - \sigma_{j'}(\zeta)\right) \neq 0,$$

les vecteurs $v_1, ..., v_m$ forment une base de $K[\chi]^m$.
De plus, pour tout $i > m$, il existe $a_1, ..., a_m \in K$ tels que $\zeta^i = a_1 + a_2\zeta + ... + a_m\zeta^{m-1}$. Comme les conjugués galoisiens de ζ vérifient la même relation, pour tout $j \in [\![1; m]\!]$, on a

$$\sigma_j(\zeta)^i = a_1 + a_2\sigma_j(\zeta) + ... + a_m\sigma_j(\zeta)^{m-1},$$

donc

$$v_i = a_1v_1 + a_2v_2 + ... + a_mv_m \in \mathrm{Vect}_K(v_1, ...v_m).$$

Soit $g \in G$, il existe $d \in [\![0, n-1]\!]$ tel que $\chi(g) = \zeta^d$. Pour tout $j \in [\![1; m]\!]$, on a

$$\chi_j(g) = \sigma_j(\zeta^d) = \sigma_j(\zeta)^d.$$

Soit $i \in [\![1; m]\!]$, on a

$$\begin{aligned}\rho_\chi(g)(v_i) &= \left(\rho_j(g)\left(\sigma_j(\zeta)^{i-1}\right)\right)_{j \in [\![1;m]\!]} = \left(\chi_j(g)\sigma_j(\zeta)^{i-1}\right)_{j \in [\![1;m]\!]} = \left(\sigma_j(\zeta)^{d+i-1}\right)_{j \in [\![1;m]\!]} \\ &= v_{d+i} \in \mathrm{Vect}_K(v_1, ...v_m).\end{aligned}$$

En exprimant la représentation ρ_χ dans la base $v_1, ..., v_m$, on montre donc qu'elle est définie sur K, ce qui prouve que $\psi_\chi = \sum_{\sigma \in G_\chi} \sigma\chi$ est un caractère défini sur K. □

Lemme 2.1.5. *Soit ψ un caractère de G défini sur K et $\psi = \chi_1 + ... + \chi_s$ sa décomposition en caractères irréductibles sur $\overline{K}$. On note ψ_1 le caractère de G sur K défini par $\psi_1 = \sum_{\sigma \in G_{\chi_1}} \sigma\chi_1$.*
Alors il existe un caractère ψ'_1 de G sur K tel que $\psi = \psi_1 + \psi'_1$.

Démonstration. Comme ψ est un caractère défini sur K, pour tout $\sigma \in G_{\chi_1}$ on a $\sigma\psi = \psi$, donc par unicité de la décomposition en caractères irréductibles sur $\overline{K}$, il existe $j_\sigma \in [\![1; s]\!]$ tel que $\sigma\chi_1 = \chi_{j_\sigma}$. Or les $\sigma\chi_1$ sont distincts, donc $\psi = \psi_1 + \psi'_1$, avec $\psi'_1 = \sum_j \chi_j$ où la somme parcourt les indices qui ne sont pas des j_σ.
Soit ρ une représentation sur K de G de caractère ψ. Comme la décomposition en caractères irréductibles de ψ_1 sur $K[\chi_1]$ ne fait intervenir que des caractères présents dans celle de ψ, ψ_1 est associé à une sous-représentation ρ_1 de ρ sur $K[\chi_1]$. D'après le lemme précédent, ψ_1 est un caractère de G défini sur K donc sa représentation associée ρ_1 est une représentation définie sur K, c'est donc une sous-représentation de ρ sur K. On note ρ'_1 une sous-représentation de ρ orthogonale à ρ_1, son caractère est ψ'_1, donc ψ'_1 est bien un caractère de G sur K. □

On en déduit immédiatement le résultat suivant.

Corollaire 2.1.6. *Soit ψ un caractère de G irréductible sur K et χ_ψ un caractère de la décomposition de ψ en caractères irréductibles sur $\overline{K}$.*
Alors

$$\psi = \sum_{\sigma \in G_{\chi_\psi}} \sigma\chi_\psi.$$

On peut alors démontrer le résultat souhaité.

Proposition 2.1.7. *Soit χ un caractère de G irréductible sur $\overline{K}$.*
Alors ψ_χ est un caractère de G irréductible sur K.

Démonstration. On a démontré dans le lemme 2.1.4 que ψ_χ est un caractère de G défini sur K. Soit ψ le sous-caractère irréductible sur K de ψ_χ dont la décomposition en caractères irréductibles sur $\overline{K}$ contient χ. D'après le corollaire précédent, on a alors

$$\psi = \sum_{\sigma \in G_{\chi_\psi}} \sigma\chi = \psi_\chi,$$

donc ψ_χ est irréductible sur K. □

Notation. Si $\psi : G \to \mathbb{Q}_p$ est un $\mathbb{Q}_p$-caractère irréductible, χ_ψ désigne un $\overline{\mathbb{Q}}_p$-caractère irréductible tel que $\psi = \sum_{\chi' \in C_{\chi_\psi}} \chi'$. On note alors $C_\psi = C_{\chi_\psi}$, qui ne dépend que de ψ et non du choix de χ_ψ.

Définition 2.1.8. *Soit $\psi : G \to \mathbb{Q}_p$ un caractère de G irréductible sur $\mathbb{Q}_p$. On définit ainsi l'idempotent associé à ψ*

$$e_\psi = \sum_{\chi \in C_\psi} e_\chi = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \psi(g^{-1}) g \in \mathbb{Q}_p[G].$$

Si p ne divise pas l'ordre de G, on a $e_\psi \in \mathbb{Z}_p[G]$.

Notation. On note $X_{\mathrm{irr},\mathbb{Q}_p}$ l'ensemble des $\mathbb{Q}_p$-caractères irréductibles de G.

Proposition 2.1.9. *La famille composée des e_ψ pour tous les $\psi \in X_{\mathrm{irr},\mathbb{Q}_p}$ est un système fondamental d'idempotents orthogonaux :*

1. *pour tout $\psi \in X_{\mathrm{irr},\mathbb{Q}_p}$, on a $e_\psi^2 = e_\psi$,*
2. *pour tout $\psi \neq \psi' \in X_{\mathrm{irr},\mathbb{Q}_p}$, on a $e_\psi e'_\psi = 0$,*
3. *on a $\sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi = 1_G$.*

Démonstration. On déduit cette proposition de la proposition 2.1.3 sur l'idempotence des caractères $\overline{\mathbb{Q}}_p$-irréductibles.
Soit $\psi \in X_{\mathrm{irr},\mathbb{Q}_p}$, on a

$$e_\psi^2 = \Big(\sum_{\chi \in C_{\chi_\psi}} e_\chi \Big)^2 = \sum_{\chi \in C_{\chi_\psi}} e_\chi = e_\psi.$$

Soit $\psi \neq \psi' \in X_{\mathrm{irr},\mathbb{Q}_p}$. Comme $C_\psi \cap C_{\psi'} = \emptyset$, pour tout $\chi \in C_\psi$ et tout $\chi' \in C_{\psi'}$, on a $e_\chi e_{\chi'} = 0$, on en déduit

$$e_\psi e'_\psi = \Big(\sum_{\chi \in C_\psi} e_\chi \Big) \Big(\sum_{\chi' \in C_{\psi'}} e_{\chi'} \Big) = 0.$$

Enfin,

$$\sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi = \sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} \sum_{\chi \in C_\psi} e_\chi = \sum_{\chi \in X_{\mathrm{irr}}} e_\chi = 1_G.$$

□

2.2 χ-composantes

Dans toute cette section, G désigne un groupe abélien fini et $\chi : G \to \overline{\mathbb{Q}}_p^\times$ désigne un caractère p-adique irréductible de G.

Définition 2.2.1. *Soit M un $\mathbb{Z}_p[\chi]$-module.*
On peut munir M d'une structure de $\mathbb{Z}_p[G]$-module en faisant agir G via χ : pour tout $m \in M$ et $g \in G$, on pose $gm = \chi(g)m$.
Un $\mathbb{Z}_p[\chi][G]$-module dont l'action de G est donné par χ est dit χ-isotypique.
Lorsqu'on munit $\mathbb{Z}_p[\chi]$ de sa structure de $\mathbb{Z}_p[\chi][G]$-module χ-isotypique, on le note $\underline{\mathbb{Z}_p[\chi]}$.

Définition 2.2.2. *On note I_χ l'idéal de $\mathbb{Z}_p[\chi][G]$ engendré par les éléments $\chi(g) - g$ où g parcourt G.*

Remarques. – Un $\mathbb{Z}_p[\chi][G]$-module est χ-isotypique si et seulement si son annulateur contient I_χ.
– Si M et N sont deux $\mathbb{Z}_p[\chi][G]$-modules χ-isotypiques, $f : M \to N$ est un morphisme de $\mathbb{Z}_p[G]$-modules si et seulement si c'est un morphisme de $\mathbb{Z}_p[\chi]$ modules.

Il existe plusieurs manières d'associer un $\mathbb{Z}_p[\chi][G]$-module χ-isotypique à un $\mathbb{Z}_p[G]$-module. Ces $\mathbb{Z}_p[\chi][G]$-modules s'appellent les χ composantes du module et sont définies dans les paragraphes qui suivent.

2.2.1 χ-quotient

Théorème-Définition 2.2.3. *Soit M un $\mathbb{Z}_p[G]$-module.*
Il existe un $\mathbb{Z}_p[\chi]$-module M_χ et une application $\mathbb{Z}_p[G]$-linéaire $\varphi : M \to M_\chi$ vérifiant la propriété universelle suivante :
pour tout $\mathbb{Z}_p[\chi][G]$-module χ-isotypique N et pour toute application $\mathbb{Z}_p[G]$-linéaire $f : M \to N$, il existe une unique application $\mathbb{Z}_p[\chi]$-linéaire $h : M_\chi \to N$ telle que $h \circ \varphi = f$.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \varphi} & \nearrow{\scriptstyle h} & \\ M_\chi & & \end{array}$$

Ce $\mathbb{Z}_p[\chi]$-module M_χ est unique à isomorphisme près, il s'agit de $M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]}$ et l'application $\varphi = \varphi_\chi^M : M \to M_\chi$ est donnée par $\varphi(m) = m \otimes 1$. La structure de $\mathbb{Z}_p[\chi]$-module de $M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]}$ est donnée par multiplication à droite :

$$\forall \lambda \in \mathbb{Z}_p[\chi],\ \lambda(m \otimes a) = m \otimes \lambda a.$$

On appelle $M_\chi = M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]}$ le χ-quotient de M.

L'appellation de χ-quotient sera justifiée par une autre caractéristation donnée par la proposition 2.2.8.
On remarque que la structure de $\mathbb{Z}_p[\chi]$-module de $M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]}$ est bien compatible avec sa structure de $\mathbb{Z}_p[G]$-module : si $g \in G$, on a $\chi(g)(m \otimes a) = m \otimes \chi(g)a = g(m \otimes a)$. M_χ est donc un $\mathbb{Z}_p[\chi][G]$-module χ-isotypique.

Démonstration. Montrons d'abord l'unicité à isomorphisme de $\mathbb{Z}_p[\chi]$-modules près.
Soit $\widetilde{M_\chi}$ un $\mathbb{Z}_p[\chi]$-module et $\widetilde{\varphi} : M \to \widetilde{M_\chi}$ vérifiant également la propriété universelle. D'après la propriété universelle de M_χ, il existe $h : M_\chi \to \widetilde{M_\chi}$ telle que $h \circ \varphi = \widetilde{\varphi}$. D'après celle de $\widetilde{M_\chi}$ il existe $\widetilde{h} : \widetilde{M_\chi} \to M_\chi$ telle que $\widetilde{h} \circ \widetilde{\varphi} = \varphi$, donc

$$\widetilde{h} \circ h \circ \varphi = \varphi.$$

Or d'après la propriété universelle de M_χ, il y a une unique application $\mathbb{Z}_p[\chi]$-linéaire $\psi : M_\chi \to M_\chi$ telle que $\psi \circ \varphi = \varphi$, c'est l'identité, donc $\widetilde{h} \circ h = \mathrm{id}_{M_\chi}$ et de la même façon, $h \circ \widetilde{h} = \mathrm{id}_{\widetilde{M_\chi}}$, donc M_χ et $\widetilde{M_\chi}$ sont isomorphes.

Montrons maintenant que $M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]}$ et $\varphi : m \mapsto m \otimes 1$ vérifient cette propriété universelle.
Soit N un $\mathbb{Z}_p[\chi][G]$-module χ-isotypique et $f : M \to N$ une application $\mathbb{Z}_p[G]$-linéaire. Alors on peut définir une application $\mathbb{Z}_p[G]$-bilinéaire $f_0 : M \times \underline{\mathbb{Z}_p[\chi]} \to N$ en posant $f_0(m, a) = af(m)$. D'après la propriété universelle du produit tensoriel, en notant $\psi : M \times \underline{\mathbb{Z}_p[\chi]} \to M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]}$, il existe une unique application $\mathbb{Z}_p[G]$-linéaire $h : M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]} \to N$ vérifiant $h \circ \psi = f_0$.
En notant $i_1 : M \to M \times \underline{\mathbb{Z}_p[\chi]}$, définie par $i_1(m) = (m, 1)$, on a $\varphi = \psi \circ i_1$, donc

$$h \circ \varphi = h \circ \psi \circ i_1 = f_0 \circ i_1 = f_0 \circ i_1 = f.$$

Réciproquement, si h' vérifie $h' \circ \varphi = f_0 \circ i_1 = f$, elle vérifie également $h' \circ \psi = f_0$, donc par unicité d'une telle fonction, $h' = h$.
Il existe donc une unique application $\mathbb{Z}_p[G]$-linéaire $h : M_\chi \to N$ telle que $h \circ \varphi = f$.
Enfin h est une application $\mathbb{Z}_p[G]$-linéaire entre deux $\mathbb{Z}_p[\chi][G]$-modules χ-isotypiques, donc elle est $\mathbb{Z}_p[\chi]$-linéaire. □

Remarque. On remarque que φ_χ^M est une surjection de M sur M_χ. En effet pour tout $m \in M$ et tout $g \in G$, on a $m \otimes \chi(g) = gm \otimes 1$, donc par linéarité tout élément de $M \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]}$ s'écrit $m \otimes 1 = \varphi_\chi^M(m)$ pour un $m \in M$ (non unique en général).

Exemple. Si $M = \mathbb{Z}/p\mathbb{Z}$ est $\mathbb{Z}_p[G]$-module tel que $pM = 0$ sur lequel $G = \mathbb{Z}/p\mathbb{Z}$ agit trivialement, alors pour tout caractère irréductible χ non trivial, on a $M_\chi \simeq M$. En effet, si on fixe $g \in G \setminus \{1_G\}$, on peut définir une application $\mathbb{Z}_p[G]$-bilinéaire

$$l : \begin{cases} M \times \overline{\mathbb{Z}_p[\chi]} \to M \\ \Big(m, \sum_{i=0}^{p-1} \lambda_i \chi(g)^i\Big) \mapsto \sum_{i=0}^{p-1} \lambda_i m \end{cases}.$$

Si $\sum_{i=0}^{p-1} \lambda_i \chi(g)^i = 0$, comme le polynôme minimal de $\chi(g)$ est $\sum_{i=0}^{p-1} X^i$, nécessairement il divise $\sum_{i=0}^{p-1} \lambda_i X^i$, et comme ces deux polynômes sont de même degré, on en conclut que pour tout $i \in [\![0, p-1]\!]$, on a $\lambda_i = \lambda_0$ et ainsi,

$$\sum_{i=0}^{p-1} \lambda_i m = \lambda_0 pm = 0.$$

L'application l est donc bien définie, de plus elle est $\mathbb{Z}_p[G]$-bilinéaire car G agit trivialement sur M. On a donc une application $\mathbb{Z}_p[G]$-linéaire $f_l : M_\chi \to M$ telle que $f_l\Big(m \otimes \sum_{i=0}^{p-1} \lambda_i \chi(g)^i\Big) = \sum_{i=0}^{p-1} \lambda_i m$. On a alors

$$f_l \circ \varphi_\chi^M = \mathrm{id}_M,$$

donc φ_χ^M est injective et réalise un isomorphisme entre M et M_χ.

Si $f : M \to N$ est un morphisme de $\mathbb{Z}_p[G]$-modules, comme $\varphi_\chi^N \circ f : M \to N_\chi$ est $\mathbb{Z}_p[G]$-linéaire comme N_χ est χ-isotypique, par définition de M_χ, il existe une unique application $\mathbb{Z}_p[\chi]$-linéaire $f_\chi : M_\chi \to N_\chi$ telle que $f_\chi \circ \varphi_\chi^M = \varphi_\chi^N \circ f$. Elle est donnée par $f_\chi(m \otimes 1) = f(m) \otimes 1$.

Proposition-Définition 2.2.4. *On définit le foncteur covariant $\mathcal{F}_\chi$ de la catégorie des $\mathbb{Z}_p[G]$-modules vers la catégorie des $\mathbb{Z}_p[\chi][G]$-modules χ-isotypiques en posant $\mathcal{F}_\chi(M) = M_\chi$ pour tout $\mathbb{Z}_p[G]$-module M et $\mathcal{F}_\chi(f) = f_\chi$ pour tout $\mathbb{Z}_p[G]$-morphisme f.*

Démonstration. Si $f : M \to N$ et $g : N \to P$ sont des $\mathbb{Z}_p[G]$-morphismes, comme

$$g_\chi \circ f_\chi \circ \varphi_\chi^M = g_\chi \circ \varphi_\chi^N \circ f = \varphi_\chi^P \circ g \circ f,$$

on a bien

$$\mathcal{F}_\chi(g \circ f) = g_\chi \circ f_\chi = \mathcal{F}_\chi(g) \circ \mathcal{F}_\chi(f).$$

Et comme

$$\mathrm{id}_{M_\chi} \circ \varphi_\chi^M = \varphi_\chi^M \circ \mathrm{id}_M,$$

on a bien

$$\mathcal{F}_\chi(\mathrm{id}_M) = \mathrm{id}_{M_\chi},$$

donc $\mathcal{F}_\chi$ est un foncteur covariant. □

Proposition 2.2.5. *Le foncteur $\mathcal{F}_\chi$ est exact à droite.*

Démonstration. Soit

$$0 \to M \to N \to P \to 0$$

une suite exacte de $\mathbb{Z}_p\,[G]$-modules. La suite de $\mathbb{Z}_p[\chi]\,[G]$-modules

$$M_\chi \to N_\chi \to P_\chi \to 0$$

est exacte comme suite de $\mathbb{Z}_p\,[G]$-modules par exactitude à droite de $- \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p\,[\chi]}$, donc elle est exacte comme suite de $\mathbb{Z}_p[\chi]\,[G]$-modules. □

Proposition 2.2.6. *Si χ et χ' sont conjugués, le χ-quotient et le χ'-quotient sont naturellement isomorphes comme $\mathbb{Z}_p\,[G]$-modules.*

Démonstration. Soit $\sigma \in G_\chi$ tel que $\chi' = \sigma\chi$. Comme σ induit un isomorphisme de $\mathbb{Z}_p$-modules entre $\underline{\mathbb{Z}_p\,[\chi]}$ et $\underline{\mathbb{Z}_p[\chi']}$, et comme pour tout $g \in G$ et tout $x \in \underline{\mathbb{Z}_p\,[\chi]}$, on a

$$\sigma(gx) = \sigma(\chi(g)x) = \chi'(g)\sigma(x) = g\sigma(x),$$

on en déduit que σ induit un isomorphisme de $\mathbb{Z}_p\,[G]$-modules

$$\underline{\mathbb{Z}_p\,[\chi]} \simeq \underline{\mathbb{Z}_p[\chi']}.$$

Ainsi, pour tout $\mathbb{Z}_p\,[G]$-module M on a un isomorphisme de $\mathbb{Z}_p\,[G]$-modules

$$\sigma_M : \begin{cases} M_\chi \to M_{\chi'} \\ m \otimes \chi(g) \mapsto m \otimes \chi'(g) \end{cases}.$$

Si $f : M \to N$ est un morphisme de $\mathbb{Z}_p\,[G]$-modules, pour tout $m \otimes 1 \in M_\chi$, on a

$$\sigma_N(f_\chi(m \otimes 1)) = \sigma_N(f(m) \otimes 1) = f(m) \otimes 1 = f_{\chi'}(m \otimes 1) = f_{\chi'}(\sigma_M(m \otimes 1)).$$

On a donc le diagramme commutatif suivant

$$\begin{array}{ccc} M_\chi & \xrightarrow{f_\chi} & N_\chi \\ \downarrow{\scriptstyle \sigma_M} & & \downarrow{\scriptstyle \sigma_N} \\ M_{\chi'} & \xrightarrow{f_{\chi'}} & N_{\chi'} \end{array}$$

donc les σ_M fournissent un isomorphisme naturel entre les foncteurs $O_\chi \circ \mathcal{F}_\chi$ et $O_{\chi'} \circ \mathcal{F}_{\chi'}$, où O_χ désigne toujours le foncteur d'oubli de la catégorie des $\mathbb{Z}_p[\chi][G]$-modules χ-isotypiques vers la catégorie des $\mathbb{Z}_p[G]$-modules, et $O_{\chi'}$ celui de la catégorie des $\mathbb{Z}_p[\chi'][G]$-modules χ'-isotypiques vers la catégorie des $\mathbb{Z}_p[G]$-modules. □

Théorème 2.2.7. *Soit M un $\mathbb{Z}_p[G]$-module et χ un caractère p-adique irréductible de G.*
Le $\mathbb{Z}_p[\chi]$-module

$$\left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right) / I_\chi \left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right)$$

et le morphisme

$$\varphi : \begin{cases} M \to \left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right) / I_\chi \left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right) \\ m \mapsto (m \otimes 1) + I_\chi \left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right) \end{cases}$$

satisfont la propriété universelle du χ-quotient, ce module est donc naturellement isomorphe à M_χ.

Démonstration. Notons $\hat{M} = \left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right) / I_\chi \left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right)$ et π la projection de $M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]$ sur $\hat{M}$. Par construction $I_\chi \hat{M} = 0$ donc $\hat{M}$ est un $\mathbb{Z}_p[\chi][G]$-module χ-isotypique.
On définit les applications $\mathbb{Z}_p[G]$-linéaires

$$\widetilde{\varphi} : \begin{cases} M \to M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi] \\ m \mapsto m \otimes 1 \end{cases},$$

et

$$\varphi_M = \varphi = \pi \circ \widetilde{\varphi} : M \to \hat{M} \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi].$$

Pour tout $m \in M$ et tout $g \in G$, comme $\hat{M}$ est isotypique, on a

$$\pi(m \otimes \chi(g)) = \pi(gm \otimes 1) = \varphi(gm),$$

donc φ est surjective.
Soit N un $\mathbb{Z}_p[\chi][G]$-module χ-isotypique et $f : M \to N$ une application $\mathbb{Z}_p[G]$-linéaire. Alors l'application $\mathbb{Z}_p$-bilinéaire

$$f_0 : \begin{cases} M \times \mathbb{Z}_p[\chi] \to N \\ (m, a) \mapsto a f(m) \end{cases}$$

fournit une application $\mathbb{Z}_p$-linéaire

$$\widetilde{h} : \begin{cases} M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi] \to N \\ m \otimes a \mapsto af(m) \end{cases}.$$

Pour tout $g \in G$, on a

$$\widetilde{h}(g(m \otimes a)) = af(gm) = gaf(m) = \chi(g)af(m) = \widetilde{h}(\chi(g)(m \otimes a))$$

donc $\widetilde{h}$ est $\mathbb{Z}_p[G]$-linéaire et contient $I_\chi\left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right)$ dans son noyau. Donc on peut passer au quotient et obtenir une application

$$h : \hat{M} \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi] \to N$$

qui est $\mathbb{Z}_p[G]$-linéaire entre deux modules χ-isotypiques, donc $\mathbb{Z}_p[\chi]$-linéaire. On a alors

$$h \circ \varphi = h \circ \pi \circ \widetilde{\varphi} = \widetilde{h} \circ \widetilde{\varphi} = f$$

et comme φ est surjective, une telle application h est unique.

Pour tout $\mathbb{Z}_p[G]$-module M, on note alors $h_M : M_\chi \to \hat{M}$ l'unique isomorphisme de $\mathbb{Z}_p[\chi]$-modules tel que $h_M \circ \varphi_\chi^M = \varphi_M$ et pour tout morphisme de $\mathbb{Z}_p[G]$-modules $f : M \to N$, on note $\hat{f} : \hat{M} \to \hat{N}$ tel que $\hat{f} \circ \varphi_M = \varphi_N \circ f$.

Les diagrammes $\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \varphi_\chi^M} & & \downarrow{\scriptstyle \varphi_\chi^N} \\ M_\chi & \xrightarrow{f_\chi} & N_\chi \end{array}$ et $\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \varphi_M} & & \downarrow{\scriptstyle \varphi_N} \\ \hat{M} & \xrightarrow{\hat{f}} & \hat{N} \end{array}$ commutent.

Donc $h_N \circ f_\chi \circ \varphi_\chi^M = h_N \circ \varphi_\chi^N \circ f = \varphi_N \circ f = \hat{f} \circ \varphi_M = f \circ h_M \circ \varphi_\chi^M$, et comme φ_χ^M est surjective, on en déduit que $\begin{array}{ccc} M_\chi & \xrightarrow{f_\chi} & N_\chi \\ \downarrow{\scriptstyle h_M} & & \downarrow{\scriptstyle h_N} \\ \hat{M} & \xrightarrow{\hat{f}} & \hat{N} \end{array}$ commute.

Ainsi, le foncteur $\mathcal{F} : (M, f) \mapsto (\hat{M}, \hat{f})$ est naturellement isomorphe à $\mathcal{F}_\chi$ et donc le $\mathbb{Z}_p[\chi]$-module $\left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right) / I_\chi\left(M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]\right)$ est naturellement isomorphe à M_χ. □

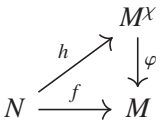
On en déduit une nouvelle caractérisation du χ-quotient.

Proposition 2.2.8. *Soit M un $\mathbb{Z}_p[G]$-module et χ un caractère p-adique irréductible de G.*
Le χ-quotient de M est isomorphe au plus grand quotient de $\mathbb{Z}_p[\chi][G]$-modules de $M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]$ sur lequel G agit via χ.

2.2.2 χ-partie

Nous allons maintenant définir une deuxième χ-composante, duale de la première.

Théorème-Définition 2.2.9. *Soit M un $\mathbb{Z}_p[G]$-module.*
Il existe un $\mathbb{Z}_p[\chi]$-module M^χ et une application $\mathbb{Z}_p[G]$-linéaire $\varphi : M^\chi \to M$ vérifiant la propriété universelle suivante :
pour tout $\mathbb{Z}_p[\chi][G]$-module χ-isotypique N et pour toute application $\mathbb{Z}_p[G]$-linéaire $f : N \to M$, il existe une unique application $\mathbb{Z}_p[\chi]$-linéaire $h : N \to M^\chi$ telle que $\varphi \circ h = f$.



Ce $\mathbb{Z}_p[\chi]$-module M^χ est unique à isomorphisme près, il s'agit de $\mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\underline{\mathbb{Z}_p[\chi]}, M\right)$ et l'application $\varphi = \varphi_M^\chi : M^\chi \to M$ est donnée par $\varphi(l) = l(1)$. La structure de $\mathbb{Z}_p[\chi]$-module est donnée par la multiplication au départ :

$$\forall \lambda \in \mathbb{Z}_p[\chi],\ (\lambda l)(a) = l(\lambda a).$$

On appelle $M^\chi = \mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\underline{\mathbb{Z}_p[\chi]}, M\right)$ la χ-partie de M.

On remarque que la structure de $\mathbb{Z}_p[\chi]$-module de M^χ est bien compatible avec sa structure de $\mathbb{Z}_p[G]$-module :

$$\forall g \in G, \forall l \in M^\chi, \forall a \in \underline{\mathbb{Z}_p[\chi]} \text{ on a } (\chi(g)l)(a) = l(\chi(g)a) = l(ga) = gl(a) = (gl)(a),$$

donc $\chi(g)l = gl$. M^χ est donc un $\mathbb{Z}_p[\chi][G]$-module χ-isotypique.

Démonstration. Montrons d'abord l'unicité à isomorphisme de $\mathbb{Z}_p[\chi]$-modules près.
Soit $\widetilde{M^\chi}$ un $\mathbb{Z}_p[\chi][G]$-module et $\widetilde{\varphi} : \widetilde{M^\chi} \to M$ vérifiant également la propriété universelle. D'après la propriété universelle de M^χ, il existe $h : \widetilde{M^\chi} \to M^\chi$ telle que $\varphi \circ h = \widetilde{\varphi}$. D'après celle de $\widetilde{M^\chi}$ il existe $\widetilde{h} : M^\chi \to \widetilde{M^\chi}$ telle que $\widetilde{\varphi} \circ \widetilde{h} = \varphi$, donc $\varphi \circ h \circ \widetilde{h} = \varphi$. Or d'après la propriété universelle de M^χ, il y a une unique application

$\mathbb{Z}_p[\chi]$-linéaire $\psi : M^\chi \to M^\chi$ telle que $\varphi \circ \psi = \varphi$, c'est id_{M^χ}, donc $h \circ \widetilde{h} = \mathrm{id}_{M^\chi}$ et de la même façon, $\widetilde{h} \circ h = \mathrm{id}_{\widetilde{M^\chi}}$, donc M^χ et $\widetilde{M^\chi}$ sont isomorphes.

Montrons maintenant que $\mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi]}, M\big)$ et $\varphi : l \mapsto l(1)$ vérifient cette propriété universelle.
Soit N un $\mathbb{Z}_p[\chi][G]$-module χ-isotypique et $f : N \to M$ une application $\mathbb{Z}_p[G]$-linéaire. Alors on peut définir une application $\mathbb{Z}_p[G]$-linéaire

$$h : \begin{cases} N \to \mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi]}, M\big) \\ m \mapsto (a \mapsto f(am)) \end{cases} .$$

On a bien $\varphi \circ h = f$.
Comme h est une application $\mathbb{Z}_p[G]$-linéaire entre N et $\mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi]}, M\big)$ qui sont des $\mathbb{Z}_p[\chi][G]$-modules χ-isotypiques, elle est également $\mathbb{Z}_p[\chi]$-linéaire. De plus cette application est unique : pour tout $m \in N$, on a

$$h(m)(1) = f(m)$$

car $\varphi \circ h = f$ et pour $a \in \underline{\mathbb{Z}_p[\chi]}$, la structure de $\mathbb{Z}_p[\chi]$-module de $\mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi]}, M\big)$ et la $\mathbb{Z}_p[\chi]$-linéarité de h impliquent

$$h(m)(a) = (ah(m))(1) = h(am)(1) = f(am).$$

□

Remarque. L'application φ_M^χ est une injection de M^χ dans M. En effet si $\alpha \in \ker(\varphi_M^\chi)$, on a $\alpha(1) = 0$, or pour tout $x \in \underline{\mathbb{Z}_p[\chi]}$ il existe $\lambda \in \mathbb{Z}_p[G]$ tel que $x = \lambda 1$, donc $\alpha(x) = \alpha(\lambda 1) = \lambda\alpha(1) = 0$, et $\alpha = 0$.

Exemple. Si M est un $\mathbb{Z}_p[G]$-module sur lequel G agit trivialement, alors pour tout caractère irréductible χ non trivial, $M^\chi = 0$. En effet, si $f \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi]}, M\big)$, en fixant $g \in G$ tel que $\chi(g) \neq 1$, pour tout $m \in M$ on a

$$f(m) = f(gm) = \chi(g)f(m)$$

et comme $\mathbb{Z}_p[\chi]$ est intègre, on en déduit $f(m) = 0$, donc $f = 0$.

Si $f : M \to N$ est un morphisme de $\mathbb{Z}_p[G]$-modules, comme $f \circ \varphi_M^\chi : M^\chi \to N$ est $\mathbb{Z}_p[G]$-linéaire et comme M^χ est χ-isotypique, par définition de N^χ il existe une unique application $\mathbb{Z}_p[\chi]$-linéaire $f^\chi : M^\chi \to N^\chi$ telle que $\varphi_N^\chi \circ f^\chi = f \circ \varphi_M^\chi$. Elle est donnée par $f^\chi(\alpha) = (x \mapsto f(\alpha(x)))$.

Proposition-Définition 2.2.10. *On définit un foncteur $\mathcal{F}^\chi$ de la catégorie des $\mathbb{Z}_p[G]$-modules vers la catégorie des $\mathbb{Z}_p[\chi][G]$-modules χ-isotypiques en posant $\mathcal{F}_\chi(M) = M^\chi$ pour tout $\mathbb{Z}_p[G]$-module M et $\mathcal{F}_\chi(f) = f^\chi$ pour tout $\mathbb{Z}_p[G]$-morphisme f.*

Démonstration. Si $f : M \to N$ et $g : N \to P$ sont des $\mathbb{Z}_p[G]$-morphismes, comme

$$\varphi_P^\chi \circ g^\chi \circ f^\chi = g \circ \varphi_N^\chi \circ f^\chi = g \circ f \circ \varphi_M^\chi,$$

on a bien

$$\mathcal{F}^\chi(g \circ f) = g^\chi \circ f^\chi = \mathcal{F}^\chi(g) \circ \mathcal{F}^\chi(f).$$

Et comme

$$\varphi_M^\chi \circ \mathrm{id}_{M^\chi} = \mathrm{id}_M \circ \varphi_M^\chi,$$

on a bien

$$\mathcal{F}^\chi(\mathrm{id}_M) = \mathrm{id}_{M^\chi},$$

donc $\mathcal{F}^\chi$ est un foncteur covariant. □

Proposition 2.2.11. *Le foncteur $\mathcal{F}^\chi$ est exact à gauche.*

Démonstration. Soit

$$0 \to M \to N \to P \to 0$$

une suite exacte de $\mathbb{Z}_p[G]$-modules. La suite de $\mathbb{Z}_p[\chi][G]$-modules

$$0 \to M^\chi \to N^\chi \to P^\chi$$

est exacte comme suite de $\mathbb{Z}_p[G]$-modules par exactitude à gauche du foncteur $\mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi]}, -\big)$, donc elle est exacte comme suite de $\mathbb{Z}_p[\chi][G]$-modules. □

Proposition 2.2.12. *Si χ et χ' sont conjugués, la χ-partie et le χ'-partie sont naturellement isomorphes comme $\mathbb{Z}_p[G]$-modules.*

Démonstration. Soit $\sigma \in G_\chi$ tel que $\chi' = \sigma\chi$, on sait que σ induit un isomorphisme de $\mathbb{Z}_p[G]$-modules entre $\underline{\mathbb{Z}_p[\chi]}$ et $\underline{\mathbb{Z}_p[\chi']}$. Ainsi, pour tout $\mathbb{Z}_p[G]$-module M on a un isomorphisme de $\mathbb{Z}_p[G]$-modules entre $M^{\chi'}$ et M^χ donné par $\sigma_M(\alpha) = \alpha \circ \sigma$ pour tout $\alpha \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi']}, M\big)$.
Si $f : M \to N$ est un morphisme de $\mathbb{Z}_p[G]$-modules, et si $\alpha \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\big(\underline{\mathbb{Z}_p[\chi']}, M\big)$, on a

$$\sigma_N(f^{\chi'}(\alpha)) = f^{\chi'}(\alpha) \circ \sigma = f^\chi(\alpha\sigma) = f^\chi \circ \sigma_M(\alpha).$$

On a donc le diagramme commutatif suivant

$$\begin{array}{ccc} M^{\chi'} & \xrightarrow{f^{\chi'}} & N^{\chi'} \\ \downarrow{\scriptstyle \sigma_M} & & \downarrow{\scriptstyle \sigma_N} \\ M^{\chi} & \xrightarrow{f^{\chi}} & N^{\chi} \end{array}$$

donc les σ_M fournissent un isomorphisme naturel entre les foncteurs $O_{\chi'} \circ \mathcal{F}^{\chi'}$ et $O_\chi \circ \mathcal{F}^{\chi}$, où O_χ est le foncteur d'oubli de la catégorie des $\mathbb{Z}_p[\chi]\,[G]$-modules χ-isotypiques vers la catégorie des $\mathbb{Z}_p\,[G]$-modules, et $O_{\chi'}$ celui de la catégorie des $\mathbb{Z}_p[\chi]\,[G]$-modules χ'-isotypiques vers la catégorie des $\mathbb{Z}_p\,[G]$-modules. □

Théorème 2.2.13. *Soit M un $\mathbb{Z}_p\,[G]$-module.*
Le $\mathbb{Z}_p\,[\chi]$-module $\{x \in M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p\,[\chi]$ tel que pour tout $g \in G$ on a $\chi(g)x = gx\}$ composé des éléments de $M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p\,[\chi]$ annulés par I_χ est naturellement isomorphe à M^χ.

Notation. Pour tout $x \in \mathbb{Q}_p$, $v_p(x)$ désigne la valuation p-adique de x et $\alpha_\chi = \min\limits_{x \in \mathbb{Z}_p[\chi]} v_p\left(\mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p}(x)\right)$. On note $\mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p} : \mathbb{Q}_p\,[\chi] \to \mathbb{Q}_p$ la trace de l'extension $\mathbb{Q}_p\,[\chi]\,/\mathbb{Q}_p$ et on en définit une renormalisation sur $\mathbb{Z}_p\,[\chi]$:

$$\mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}} : \begin{cases} \mathbb{Z}_p\,[\chi] \to \mathbb{Z}_p \\ x \mapsto \frac{\mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p}(x)}{p^{\alpha_\chi}} \end{cases} .$$

Lemme 2.2.14. *Les $\mathbb{Z}_p\,[\chi]$-modules $\mathbb{Z}_p\,[\chi]$ et $\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p\,[\chi]\,, \mathbb{Z}_p\right)$ sont isomorphes via le morphisme qui envoie x sur l'application $\mathbb{Z}_p$-linéaire $l_x : y \mapsto \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(xy)$.*

Démonstration. On pose $l : x \mapsto (l_x : y \to \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(xy))$.

Comme $\mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p}$ est $\mathbb{Z}_p$-linéaire, l_x appartient bien $\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p\,[\chi]\,, \mathbb{Z}_p\right)$ et l'application l est bien $\mathbb{Z}_p$-linéaire.
Considérons l'extension de l à $\mathbb{Q}_p\,[\chi]$:

$$\begin{array}{rccc} \widetilde{l}: & \mathbb{Q}_p\,[\chi] & \to & \mathrm{Hom}_{\mathbb{Q}_p}\left(\mathbb{Q}_p\,[\chi]\,, \mathbb{Q}_p\right) \\ & x & \mapsto & \left(\widetilde{l_x} : y \to \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(xy)\right) \end{array}$$

Soit $x \in \mathbb{Q}_p\,[\chi]$. Si pour tout $y \in \mathbb{Q}_p\,[\chi]$ on a $\mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(xy) = 0$, alors $\mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p}(xy) = 0$. Or l'extension $\mathbb{Q}_p\,[\chi]\,/\mathbb{Q}_p$ est séparable donc la forme trace est non dégénérée et donc $x = 0$. L'application $\widetilde{l}$ est donc injective et donc sa restriction l aussi.

De plus $\widetilde{l}$ est une application linéaire entre deux $\mathbb{Q}_p$-espaces vectoriels de même dimension $\left[\mathbb{Q}_p[\chi] : \mathbb{Q}_p\right]$, donc $\widetilde{l}$ est un isomorphisme.
Pour tout $\lambda \in \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], \mathbb{Z}_p\right) \subset \mathrm{Hom}_{\mathbb{Q}_p}\left(\mathbb{Q}_p[\chi], \mathbb{Q}_p\right)$, il existe $x \in \mathbb{Q}_p[\chi]$ tel que $\lambda = \widetilde{l}(x) : y \to \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(xy)$. Pour montrer que l est surjective, il suffit donc de montrer que $x \in \mathbb{Z}_p[\chi]$. Notons $\beta = \upsilon_p(x)$, et $x' = \frac{x}{p^\beta} \in \mathbb{Z}_p[\chi]^\times$, soit $z \in \mathbb{Z}_p[\chi]$ tel que $\upsilon_p\left(\mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p}(z)\right) = \alpha$. On a alors

$$\lambda(zx'^{-1}) = \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(p^\beta z) = p^\beta \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(z),$$

or $\upsilon_p(\mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(z)) = 1$, donc $\upsilon_p(\lambda(zx'^{-1})) = \beta$, et comme $zx'^{-1} \in \mathbb{Z}_p[\chi]$, on a $\lambda(zx'^{-1}) \in \mathbb{Z}_p$ et nécessairement $\beta \geq 0$. Ainsi $x = p^\beta x' \in \mathbb{Z}_p[\chi]$ et l est surjective. □

Lemme 2.2.15. *Les $\mathbb{Z}_p[\chi][G]$-modules $M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]$ et $\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], M\right)$ sont isomorphes via le morphisme qui envoie $x = m \otimes a$ sur l'application $\mathbb{Z}_p$-linéaire $l_x : y \mapsto \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(ay)m$.*

Démonstration. Comme $\mathbb{Z}_p[\chi]$ est un $\mathbb{Z}_p$-module libre, la proposition 1.3.2 implique que les $\mathbb{Z}_p$-modules $M \otimes \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], \mathbb{Z}_p\right)$ et $\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], M\right)$ sont isomorphes, l'isomorphisme étant donné par $m \otimes f \mapsto (f_m : \alpha \mapsto f(\alpha)m)$. Or, d'après le lemme précédent, les $\mathbb{Z}_p$-modules $M \otimes \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], \mathbb{Z}_p\right)$ et $M \otimes \mathbb{Z}_p[\chi]$ sont isomorphes, donc en combinant les deux isomorphismes, on obtient un isomorphisme l de $\mathbb{Z}_p$-modules entre $M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]$ et $\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], M\right)$ qui envoie $x = m \otimes a$ sur l'application $\mathbb{Z}_p$-linéaire $l_x : y \mapsto \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(xy)m$.
Montrons maintenant que cet isomorphisme est $\mathbb{Z}_p[\chi][G]$-linéaire.
Soit $g \in G$. On a alors

$$l(g(m \otimes a)) = l(gm \otimes a) = \left(y \mapsto \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(ay)gm\right) = (gl)(m \otimes a).$$

On a aussi

$$l(\chi(g)(m \otimes a)) = l(m \otimes a\chi(g)) = \left(y \mapsto \mathrm{tr}^*_{\mathbb{Z}_p[\chi]/\mathbb{Z}}(a\chi(g)y)m\right) = (\chi(g)l)(m \otimes a).$$

□

Démonstration du théorème. Pour tout $\mathbb{Z}_p[G]$-module M, on note

$$\check{M} = \{x \in M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi] \text{ tel que pour tout } g \in G \text{ on a } \chi(g)x = gx\}.$$

Soit $\lambda \in \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], M\right)$ et $g \in G$. On a $\chi(g)\lambda = g\lambda$ si et seulement si pour tout $x \in \mathbb{Z}_p[\chi]$, $\lambda(\chi(g)x) = g\lambda(x)$, or $\lambda(\chi(g)x) = \lambda(gx)$, donc $\lambda \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\underline{\mathbb{Z}_p[\chi]}, M\right)$ si et seulement si, pour tout $g \in G$, $\chi(g)\lambda = g\lambda$.
D'après le lemme précédent, les $\mathbb{Z}_p[\chi][G]$-modules $M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]$ et $\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[\chi], M\right)$ sont isomorphes, donc leurs deux sous-$\mathbb{Z}_p[\chi][G]$-modules χ-isotypiques maximaux $\check{M}$ et $\mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\underline{\mathbb{Z}_p[\chi]}, M\right)$ sont isomorphes, on note h_M cet isomorphisme entre $\check{M}$ et M^χ.

Pour tout $\mathbb{Z}_p[G]$-morphisme $f : M \to N$, on définit

$$\check{f} : \begin{cases} \check{M} \to \check{N} \\ \sum\limits_i m_i \otimes \chi(g)^i \mapsto \sum\limits_i f(m_i) \otimes \chi(g)^i \end{cases} .$$

On a alors

$$\begin{aligned} h_N \circ \check{f}\Big(\sum_i m_i \otimes \chi(g)^i\Big) &= h_N\Big(\sum_i f(m_i) \otimes \chi(g)^i\Big) = \Big(x \mapsto f\Big(\sum_i \mathrm{tr}^*(\chi(g)^i x) m_i\Big)\Big) \\ &= f^\chi \circ h_M\Big(\sum_i m_i \otimes \chi(g)^i\Big). \end{aligned}$$

Donc le diagramme $\begin{array}{ccc} \check{M} & \xrightarrow{\check{f}} & \check{N} \\ \downarrow{\scriptstyle h_M} & & \downarrow{\scriptstyle h_N} \\ M^\chi & \xrightarrow{f^\chi} & N^\chi \end{array}$ commute.
Ainsi, le foncteur $\mathcal{F} : (M, f) \mapsto (\check{M}, \check{f})$ est naturellement isomorphe à $\mathcal{F}_\chi$ et donc le $\mathbb{Z}_p[\chi]$-module $\check{M}$ est naturellement isomorphe à M^χ. □

On en déduit une nouvelle caractérisation de la χ-partie.

Proposition 2.2.16. *Soit M un $\mathbb{Z}_p[G]$-module et χ un caractère p-adique irréductible de G.*
La χ-partie de M est isomorphe au plus grand sous-$\mathbb{Z}_p[\chi][G]$-module χ-isotypique de $M \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[\chi]$.

Théorème 2.2.17. *Il existe une transformation naturelle η de la χ-partie vers le χ-quotient donnée pour tout $\mathbb{Z}_p[G]$-module M par $\eta_M = \varphi_\chi^M \circ \varphi_M^\chi : M^\chi \to M_\chi$.*

Pour tout $\mathbb{Z}_p[G]$-module et tout $\alpha \in M^\chi$, on a donc $\eta_M(\alpha) = \alpha(1) \otimes 1 \in M_\chi$.

Démonstration. Comme les diagrammes $\begin{array}{ccc} M^\chi & \xrightarrow{f^\chi} & N^\chi \\ \downarrow{\scriptstyle \varphi_M^\chi} & & \downarrow{\scriptstyle \varphi_N^\chi} \\ M & \xrightarrow{f} & N \end{array}$ et $\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \varphi_\chi^M} & & \downarrow{\scriptstyle \varphi_\chi^N} \\ M_\chi & \xrightarrow{f_\chi} & N_\chi \end{array}$ commutent, on en déduit que le diagramme $\begin{array}{ccc} M^\chi & \xrightarrow{f^\chi} & N^\chi \\ \downarrow{\scriptstyle \eta_M} & & \downarrow{\scriptstyle \eta_N} \\ M_\chi & \xrightarrow{f_\chi} & N_\chi \end{array}$ commute et donc η est bien une transformation naturelle de $\mathcal{F}^\chi$ vers $\mathcal{F}_\chi$. □

En général, cette transformation naturelle n'est pas un isomorphisme naturel. Par exemple, si M est un $\mathbb{Z}_p[G]$-module tel que $pM = 0$ sur lequel $G = \mathbb{Z}/p\mathbb{Z}$ agit trivialement, et si χ est un caractère non trivial, on a vu que $M_\chi \simeq M$ alors que $M^\chi = 0$.

2.2.3 Troisième χ-composante

Définition 2.2.18. *Si p ne divise pas l'ordre de G, on peut définir une troisième χ-composante : le $\mathbb{Z}_p[G]$-module $e_{\psi_\chi}M$.*
C'est un sous-$\mathbb{Z}_p[G]$-module de M.

Dans cette section, on supposera donc que p ne divise pas $\mathrm{card}(G)$.

Proposition 2.2.19. *On peut étendre la structure de $\mathbb{Z}_p[G]$-module de $e_{\psi_\chi}M$ en une structure de $\mathbb{Z}_p[\chi][G]$-module χ-isotypique de manière unique.*

$$\forall \lambda = \sum_{g\in G} \lambda_g \chi(g) \in \mathbb{Z}_p[\chi], \forall m \in e_{\psi_\chi}M \text{ on pose } \lambda m = \sum_{g\in G} \lambda_g gm.$$

Lemme 2.2.20. *Soit χ' un caractère irréductible, on a*

$$g e_{\chi'} = \chi'(g) e_{\chi'}.$$

Démonstration. Soit $g \in G$.
On a

$$g e_{\chi'} = \frac{1}{\mathrm{card}(G)} \sum_{h\in G} \chi'(h^{-1}) gh = \frac{1}{\mathrm{card}(G)} \sum_{h'\in G} \chi'(h'^{-1} g) h' = \chi'(g) e_{\chi'}.$$

□

Démonstration de la proposition. Notons $\widetilde{\chi} : \mathbb{Z}_p[G] \to \mathbb{Z}_p[\chi]$ le $\mathbb{Z}_p$-morphisme défini par

$$\widetilde{\chi}\Big(\sum_{g\in G} \lambda_g g\Big) = \sum_{g\in G} \lambda_g \chi(g).$$

Comme χ est un caractère linéaire, $\widetilde{\chi}$ est un morphisme d'anneau.
Définition : Soit $\lambda \in \mathbb{Z}_p[\chi][G]$ et $x, y \in \mathbb{Z}_p[G]$ tels que $\widetilde{\chi}(x) = \widetilde{\chi}(y) = \lambda$.
On note $x = \sum_{g\in G} \lambda_g g$ et $y = \sum_{g\in G} \lambda'_g g$.
Soit $\chi' \in C_\chi$, et $\sigma \in \mathrm{Gal}(\mathbb{Q}_p[\chi]/\mathbb{Q}_p)$ tel que $\chi' = \sigma(\chi)$, on a alors

$$\sum_{g\in G} \lambda_g \chi'(g) = \sigma\Big(\sum_{g\in G} \lambda_g \chi(g)\Big) = \sigma\Big(\sum_{g\in G} \lambda'_g \chi(g)\Big) = \sum_{g\in G} \lambda'_g \chi'(g) e_{\chi'}$$

donc

$$x e_{\chi'} = \sum_{g\in G} \lambda_g g e_{\chi'} = \sum_{g\in G} \lambda_g \chi'(g) e_{\chi'} = \sum_{g\in G} \lambda'_g \chi'(g) e_{\chi'} = \sum_{g\in G} \lambda'_g g e_{\chi'} = y e_{\chi'}$$

et

$$x e_{\psi_\chi} = \sum_{\chi'\in C_\chi} x e_{\chi'} = \sum_{\chi'\in C_\chi} y e_{\chi'} = y e_{\psi_\chi}.$$

Pour tout $m \in e_{\psi_\chi} M$ il existe $n \in M$ tel que $m = e_{\psi_\chi} n$, donc on a

$$xm = x e_{\psi_\chi} n = y e_{\psi_\chi} n = ym.$$

Donc λm est bien défini.

$\mathbb{Z}_p[\chi]$-module : Soit $m, m' \in e_{\psi_\chi} M$, $\lambda, \lambda' \in \mathbb{Z}_p[\chi]$ et $x, x' \in \mathbb{Z}_p[G]$ tels que $\widetilde{\chi}(x) = \lambda$ et $\widetilde{\chi'}(x) = \lambda'$. Comme $e_{\psi_\chi} M$ est un $\mathbb{Z}_p[G]$-module, on a les relations suivantes

$$\lambda(m + m') = x(m + m') = xm + xm' = \lambda m + \lambda m',$$

$$(\lambda + \lambda')m = (x + x')m = xm + x'm = \lambda m + \lambda' m,$$

$$1m = m,$$

et comme $\widetilde{\chi}$ est un morphisme d'anneau, $\lambda\lambda' = \widetilde{\chi}(x)\widetilde{\chi}(x') = \widetilde{\chi}(xx')$, donc on a également

$$(\lambda\lambda')m = (xx')m = x(x'm).$$

Donc $e_{\psi_\chi} M$ est bien un $\mathbb{Z}_p[\chi]$-module.

$\mathbb{Z}_p[\chi]\,[G]$-module χ-isotypique : Comme l'action de $g \in G$ sur $e_{\psi_\chi} M$ est donnée par la multiplication par $\chi(g) \in \mathbb{Z}_p\,[\chi]$, elle est $\mathbb{Z}_p\,[\chi]$-linéaire, donc $e_{\psi_\chi} M$ est bien un $\mathbb{Z}_p[\chi]\,[G]$-module. Il est χ-isotypique par définition.

Unicité : Pour que la structure de $\mathbb{Z}_p[\chi]\,[G]$-module de $e_{\psi_\chi} M$ soit χ-isotypique, il est nécessaire d'imposer $\chi(g)m = gm$ pour tout $g \in G$ et $m \in e_{\psi_\chi} M$, et donc d'imposer $\widetilde{\chi}(x)m = xm$ pour tout $x \in \mathbb{Z}_p\,[G]$ et $m \in e_{\psi_\chi} M$ par $\mathbb{Z}_p$-linéarité. □

Proposition 2.2.21. *Soit M un $\mathbb{Z}_p[\chi]\,[G]$-module χ-isotypique.*
Alors pour tout $m \in M$, on a

$$e_{\psi_\chi} m = e_\chi m = m,$$

et en particulier

$$e_{\psi_\chi} M = M.$$

Démonstration. Soit $m \in M$, comme G agit via χ, pour tout $g \in G$, on a

$$\chi(g^{-1})gm = m$$

et donc

$$e_\chi m = \frac{1}{\mathrm{card}(G)} \sum_g \chi(g^{-1})gm = m.$$

On a alors

$$e_{\psi_\chi} m = e_{\psi_\chi}(e_\chi m) = (e_{\psi_\chi} e_\chi)m = e_\chi m = m.$$

□

Théorème 2.2.22. *Le $\mathbb{Z}_p[\chi]\,[G]$-module $e_{\psi_\chi} M$ satisfait les propriétés universelles de la χ-partie et du χ-quotient de M.*
Les trois χ-composantes sont naturellement isomorphes en tant que $\mathbb{Z}_p[\chi]\,[G]$-modules

$$M^\chi \simeq e_{\psi_\chi} M \simeq M_\chi.$$

Démonstration. Notons $i_M : e_{\psi_\chi} M \to M$ l'injection définie par $i_M(m) = m$ et $s_M : M \to e_{\psi_\chi} M$ la surjection définie par $s_M(m) = e_{\psi_\chi} m$. On a $s_M \circ i_M = \mathrm{id}_{e_{\psi_\chi} M}$ et si $\varphi : N \to M$ est un morphisme de $\mathbb{Z}_p\,[G]$-modules tel que $\mathrm{Im}(\varphi) \subset e_{\psi_\chi} M$, alors $i_M \circ s_M \circ \varphi = \varphi$.

Montrons que le $\mathbb{Z}_p\,[\chi]$-module $e_{\psi_\chi} M$ et l'injection i_M satisfont la propriété universelle de la χ-partie.

Soit N un $\mathbb{Z}_p[\chi]\,[G]$-module χ-isotypique et $f : N \to M$ une application $\mathbb{Z}_p\,[G]$-linéaire.
Pour tout $n \in N$, $n = e_{\psi_\chi} n$, or $e_{\psi_\chi} \in \mathbb{Z}_p\,[G]$ et f est $\mathbb{Z}_p\,[G]$-linéaire, donc

$$f(n) = f(e_{\psi_\chi} n) = e_{\psi_\chi} f(n) \in e_{\psi_\chi} M.$$

Donc on définit une application $\mathbb{Z}_p\,[G]$-linéaire

$$h : \begin{cases} N \to e_{\psi_\chi} M \\ n \mapsto f(n) \end{cases}.$$

Comme N et $e_{\psi_\chi} M$ sont χ-isotypiques, elle est $\mathbb{Z}_p\,[\chi]$-linéaire. On a bien $i_M \circ h = f$, et un tel $\mathbb{Z}_p\,[\chi]$-morphisme h est unique par injectivité de i_M.
Ainsi la corestriction de $\varphi_M^\chi : M^\chi \to M$ à $e_{\psi_\chi} M$ réalise un isomorphisme de $\mathbb{Z}_p[\chi]\,[G]$-modules $s_M \circ \varphi_M^\chi : M^\chi \to e_{\psi_\chi} M$.

Montrons maintenant que le $\mathbb{Z}_p\,[\chi]$-module $e_{\psi_\chi} M$ et la surjection s_M satisfont la propriété universelle du χ-quotient.
Soit N un $\mathbb{Z}_p[\chi]\,[G]$-module χ-isotypique et $f : M \to N$ une application $\mathbb{Z}_p\,[G]$-linéaire.
On définit une application $\mathbb{Z}_p\,[G]$-linéaire

$$h : \begin{cases} e_{\psi_\chi} M \to N \\ e_{\psi_\chi} m \mapsto f(e_{\psi_\chi} m) \end{cases}.$$

Comme $e_{\psi_\chi} M$ et N sont χ-isotypiques, elle est $\mathbb{Z}_p\,[\chi]$-linéaire. De plus, pour tout $m \in M$, comme N est χ-isotypique et f est $\mathbb{Z}_p\,[G]$-linéaire, on a

$$f(m) = e_{\psi_\chi} f(m) = f(e_{\psi_\chi} m) = h(s_M(m)),$$

donc $h \circ s_M = f$ et un tel h est unique par surjectivité de s_M. Ainsi la restriction de $\varphi_\chi^M : M \to M_\chi$ réalise un isomorphisme de $\mathbb{Z}_p[\chi]\,[G]$-modules $\varphi_\chi^M \circ i_M : e_{\psi_\chi} M \to M_\chi$.

On définit le foncteur $\mathcal{E}_{\psi\chi}$ de la catégorie des $\mathbb{Z}_p\,[G]$-modules vers la catégorie des $\mathbb{Z}_p[\chi]\,[G]$-modules χ-isotypiques de la façon suivante : pour tout $\mathbb{Z}_p\,[G]$-module M, $\mathcal{E}_{\psi\chi}(M) = e_{\psi_\chi} M$ et pour tout $\mathbb{Z}_p\,[G]$-morphisme $f : M \to N$, $\mathcal{E}_{\psi\chi}(f) = f\big|_{e_{\psi_\chi} M}^{e_{\psi_\chi} N}$ est la fonction obtenue à partir de f par restriction à $e_{\psi_\chi} M$ et corestriction à $e_{\psi_\chi} N$. Si $f : M \to N$ et $g : N \to P$ sont deux $\mathbb{Z}_p\,[G]$-morphismes, on a bien

$$(g \circ f)\big|_{e_{\psi_\chi} M}^{e_{\psi_\chi} P} = g\big|_{e_{\psi_\chi} N}^{e_{\psi_\chi} P} \circ f\big|_{e_{\psi_\chi} M}^{e_{\psi_\chi} N}$$

et

$$\mathrm{id}_M\big|_{e_{\psi_\chi} M}^{e_{\psi_\chi} M} = \mathrm{id}_{e_{\psi_\chi} M},$$

donc $\mathcal{E}_{\psi\chi}$ est bien un foncteur covariant.

Soit $f : M \to N$ un $\mathbb{Z}_p[G]$-morphisme. Comme f est $\mathbb{Z}_p[G]$-linéaire et comme $e_{\psi_\chi} \in \mathbb{Z}_p[G]$, les diagrammes

$$\begin{array}{ccc} e_{\psi_\chi} M & \xrightarrow{\mathcal{E}_{\psi\chi}(f)} & e_{\psi_\chi} N \\ \downarrow{\scriptstyle i_M} & & \downarrow{\scriptstyle i_N} \\ M & \xrightarrow{f} & N \end{array} \quad \text{et} \quad \begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle s_M} & & \downarrow{\scriptstyle s_N} \\ e_{\psi_\chi} M & \xrightarrow{\mathcal{E}_{\psi\chi}(f)} & e_{\psi_\chi} N \end{array}$$

commutent.
Or

$$\begin{array}{ccc} M^\chi & \xrightarrow{f^\chi} & N^\chi \\ \downarrow{\scriptstyle \varphi_M^\chi} & & \downarrow{\scriptstyle \varphi_N^\chi} \\ M & \xrightarrow{f} & N \end{array} \quad \text{et} \quad \begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \varphi_\chi^M} & & \downarrow{\scriptstyle \varphi_\chi^N} \\ M_\chi & \xrightarrow{f_\chi} & N_\chi \end{array}$$

commutent également, donc

$$\begin{array}{ccc} e_{\psi_\chi} M & \xrightarrow{\mathcal{E}_{\psi\chi}(f)} & e_{\psi_\chi} N \\ \downarrow{\scriptstyle \varphi_\chi^M \circ i_M} & & \downarrow{\scriptstyle \varphi_\chi^N \circ i_N} \\ M_\chi & \xrightarrow{f_\chi} & N_\chi \end{array}, \quad \begin{array}{ccc} M^\chi & \xrightarrow{f^\chi} & N^\chi \\ \downarrow{\scriptstyle s_M \circ \varphi_M^\chi} & & \downarrow{\scriptstyle s_N \circ \varphi_N^\chi} \\ e_{\psi_\chi} M & \xrightarrow{\mathcal{E}_{\psi\chi}(f)} & e_{\psi_\chi} N \end{array} \text{ et } \begin{array}{ccc} M^\chi & \xrightarrow{f^\chi} & N^\chi \\ \downarrow{\scriptstyle \varphi_\chi^M \circ \varphi_M^\chi} & & \downarrow{\scriptstyle \varphi_\chi^N \circ \varphi_N^\chi} \\ M_\chi & \xrightarrow{f_\chi} & N_\chi \end{array}$$

commutent.
Ainsi les foncteurs $\mathcal{E}_{\psi\chi}$, $\mathcal{F}_\chi$ et $\mathcal{F}^\chi$ sont naturellement isomorphes, et donc pour tout $\mathbb{Z}_p[G]$-module M les $\mathbb{Z}_p[\chi][G]$-modules $e_{\psi_\chi} M$, M_χ et M^χ sont naturellement isomorphes. □

L'application naturelle entre χ-quotient et χ-partie établie à la partie précédente est donc un isomorphisme naturel dans le cas semi-simple.

Proposition 2.2.23. *Soit M un $\mathbb{Z}_p[G]$-module.*
Alors $M = \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi M$.

Démonstration. Les $e_\psi M$ sont des sous-$\mathbb{Z}_p[G]$-modules de M, donc

$$\sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi M \subset M.$$

Soit $m \in M$, comme $\sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi = 1$, on a $m = \sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi m$. Donc

$$M = \sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi M.$$

Supposons $\sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi m_\psi = 0$. Comme les e_ψ forment un système fondamental d'idempotents orthogonaux, pour tout $\psi \in X_{\mathrm{irr},\mathbb{Q}_p}$ on a

$$e_\psi m_\psi = e_\psi 0 = 0,$$

donc la somme des $e_\psi M$ est directe. □

Remarque. Ce résultat n'est pas généralisable en utilisant le χ-quotient ou la χ-partie dans le cas non semi-simple.

Considérons le cas du groupe $G = \mathbb{Z}/3\mathbb{Z} = \{1_G, g, g^2\}$, du nombre premier $p = 3$ et prenons comme module $M = \mathbb{Z}_3[G]$ lui-même sur lequel G agit par multiplication. Les deux représentants des caractères $\overline{\mathbb{Q}_3}$-irréductibles de G sont $\chi_0 : g \mapsto 1$ et $\chi_1 : g \mapsto \zeta = \zeta_3$.
Concernant les χ-parties on a alors

$$\varphi_M^{\chi_0}(M^{\chi_0}) = \mathrm{Vect}_{\mathbb{Z}_3}(1_G + g + g^2),$$

$$\varphi_M^{\chi_1}(M^{\chi_1}) = \mathrm{Vect}_{\mathbb{Z}_3}(g - 1_G, g^2 - 1_G)$$

or $1_G \notin \mathrm{Vect}_{\mathbb{Z}_3}(1_G + g + g^2, g - 1_G, g^2 - 1_G)$, donc

$$M \neq \varphi_M^{\chi_0}(M^{\chi_0}) \oplus \varphi_M^{\chi_1}(M^{\chi_1}).$$

En ce qui concerne les χ-quotients, on a les isomorphismes suivants

$$M_{\chi_0} = \mathbb{Z}_3[G] \underset{\mathbb{Z}_3[G]}{\otimes} \underline{\mathbb{Z}_3} \simeq \underline{\mathbb{Z}_3},$$

$$M_{\chi_1} = \mathbb{Z}_3[G] \underset{\mathbb{Z}_3[G]}{\otimes} \underline{\mathbb{Z}_3[\zeta]} \simeq \underline{\mathbb{Z}_3[\zeta]}.$$

En notant ψ_χ^M les surjections φ_χ^M composées avec ces isomorphismes, on a alors

$$\psi_{\chi_0}^M(\alpha_0 1_G + \alpha_1 g + \alpha_2 g^2) = \alpha_0 + \alpha_1 + \alpha_2,$$

$$\psi_{\chi_1}^M(\alpha_0 1_G + \alpha_1 g + \alpha_2 g^2) = (\alpha_0 - \alpha_2) + (\alpha_1 - \alpha_2)\zeta.$$

Alors le morphisme $\psi_{\chi_0}^M \oplus \psi_{\chi_1}^M : M \to \underline{\mathbb{Z}_3} \oplus \underline{\mathbb{Z}_3[\zeta]}$ est injectif mais pas surjectif car $(1, 0)$ n'a pas d'antécédent. Ainsi, le morphisme $\varphi_{\chi_0}^M \oplus \varphi_{\chi_1}^M : M \to M^{\chi_0} \oplus M^{\chi_1}$ n'est pas surjectif.

Proposition 2.2.24. *On a l'isomorphisme d'anneaux*

$$\mathbb{Z}_p[G] \simeq \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} \underline{\mathbb{Z}_p\left[\chi_\psi\right]}.$$

Chaque choix d'une famille de $\chi_\psi \in C_\psi$ fournit un tel isomorphisme.

Démonstration. En appliquant la proposition précédente on obtient

$$\mathbb{Z}_p[G] = \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi \mathbb{Z}_p[G].$$

Et pour tout $\chi_\psi \in C_\psi$ on a

$$e_\psi \mathbb{Z}_p[G] \simeq \mathbb{Z}_p[G]_{\chi_\psi} = \mathbb{Z}_p[G] \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p\left[\chi_\psi\right]} \simeq \underline{\mathbb{Z}_p\left[\chi_\psi\right]}.$$

L'isomorphisme de $\mathbb{Z}_p[G]$-modules $f : e_\psi \mathbb{Z}_p[G] \to \underline{\mathbb{Z}_p\left[\chi_\psi\right]}$ est donné par

$$f\Big(\sum_{g \in G} \alpha_g g\Big) = \sum_{g \in G} \alpha_g \chi(g).$$

Pour tout $a, b \in e_\psi \mathbb{Z}_p[G]$, on a bien

$$f(ab) = f(a)f(b)$$

et

$$f(1_G) = \chi(1_G) = 1$$

donc il s'agit d'un isomorphisme d'anneaux.
On obtient alors l'isomorphisme d'anneaux

$$\mathbb{Z}_p[G] = \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi \mathbb{Z}_p[G] \simeq \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} \underline{\mathbb{Z}_p\left[\chi_\psi\right]}.$$

□

Corollaire 2.2.25. *Pour tout caractère $\overline{\mathbb{Q}}_p$-irréductible χ le $\mathbb{Z}_p[G]$-module $\underline{\mathbb{Z}_p[\chi]}$ est projectif.*

On rappelle que p ne divise par le cardinal de G.

Proposition 2.2.26. *Alors $\mathbb{Z}_p[G]$ est quasi-principal (tous ses idéaux sont principaux mais il n'est pas nécessairement intègre).*

Démonstration. Soit I un idéal de $\mathbb{Z}_p[G]$. On a

$$I = \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi I.$$

Pour tout $\psi \in X_{\mathrm{irr},\mathbb{Q}_p}$, $e_\psi I$ est un idéal de $e_\psi \mathbb{Z}_p[G] \simeq \mathbb{Z}_p[\chi_\psi]$ qui est un anneau principal, donc $e_\psi I = e_\psi a_\psi \mathbb{Z}_p[G]$.
Ainsi

$$I = \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi a_\psi \mathbb{Z}_p[G] = \Big(\sum_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi a_\psi \Big) \mathbb{Z}_p[G]$$

car les e_ψ sont orthogonaux. □

Théorème 2.2.27 (décomposition du Fitting en χ-composantes)**.** *Soit M et N deux $\mathbb{Z}_p[G]$-modules de type fini.*
Alors on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}(N)$$

si et seulement si pour tout $\chi \in X_{\mathrm{irr}}$ on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(M_\chi) = \mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(N_\chi).$$

Démonstration. Soit $\chi \in X_{\mathrm{irr}}$. On note

$$f_\chi : \underline{\mathbb{Z}_p[\chi]} \to \mathbb{Z}_p[G]_\chi,$$

$$g_\chi : \mathbb{Z}_p[G]_\chi \to e_{\psi_\chi} \mathbb{Z}_p[G]$$

et

$$h_\chi = g_\chi \circ f_\chi : \underline{\mathbb{Z}_p[\chi]} \to e_{\psi_\chi} \mathbb{Z}_p[G]$$

les isomorphismes de $\mathbb{Z}_p[G]$-modules. Pour tout $\lambda = \sum_g \lambda_g \chi(g) \in \underline{\mathbb{Z}_p[\chi]}$, on a

$$h_\chi\Big(\lambda\Big) = g_\chi\Big(1_G \otimes \sum_g \lambda_g \chi(g)\Big) = g_\chi\Big(\sum_g \lambda_g g \otimes 1\Big) = e_{\psi_\chi} \sum_g \lambda_g g.$$

Pour tout $\mathbb{Z}_p[G]$-module P on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(P_\chi) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}(P) \underline{\mathbb{Z}_p[\chi]}$$

d'après la proposition 1.6.10 sur l'extension des scalaires vis-à-vis du Fitting.
On a alors

$$f_\chi\Big(\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(P_\chi)\Big) = f_\chi\Big(\mathrm{Fitt}_{\mathbb{Z}_p[G]}(P) \underline{\mathbb{Z}_p[\chi]}\Big) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}(P) \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p[\chi]},$$

donc

$$h_\chi\Big(\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(P_\chi)\Big) = g_\chi\Big(\mathrm{Fitt}_{\mathbb{Z}_p[G]}(P) \underset{\mathbb{Z}_p[G]}{\otimes} \underline{\mathbb{Z}_p\,[\chi]}\Big) = e_{\psi_\chi}\mathrm{Fitt}_{\mathbb{Z}_p[G]}(P).$$

Et comme h_χ est un isomorphisme de $\mathbb{Z}_p\,[G]$-modules, on en déduit que

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(M_\chi) = \mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(N_\chi) \Leftrightarrow e_{\psi_\chi}\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = e_{\psi_\chi}\mathrm{Fitt}_{\mathbb{Z}_p[G]}(N).$$

Donc si $\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}(N)$, pour tout $\chi \in X_{\mathrm{irr}}$ on a

$$e_{\psi_\chi}\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = e_{\psi_\chi}\mathrm{Fitt}_{\mathbb{Z}_p[G]}(N)$$

et par conséquent

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(M_\chi) = \mathrm{Fitt}_{\mathbb{Z}_p[\chi]}(N_\chi).$$

Réciproquement, si pour tout $\chi \in X_{\mathrm{irr}}$ on a

$$e_{\psi_\chi}\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = e_{\psi_\chi}\mathrm{Fitt}_{\mathbb{Z}_p[G]}(N),$$

on a alors

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = \bigoplus_{\psi\in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = \bigoplus_{\psi\in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi\mathrm{Fitt}_{\mathbb{Z}_p[G]}(N) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}(N).$$

□

2.2.4 Interaction avec la partie moins

On suppose maintenant que G possède un élément d'ordre 2 fixé que l'on note τ. Comme dans la section précédente, on se place dans le cas où p ne divise pas l'ordre du groupe G.

Définition 2.2.28. *Soit χ un $\overline{\mathbb{Q}}_p$-caractère irréductible de G.*
On dit que χ est impair si $\chi(\tau) = -1$ et pair si $\chi(\tau) = 1$. On note X^-_{irr} l'ensemble des $\overline{\mathbb{Q}}_p$-caractères irréductibles impairs et X^+_{irr} celui des $\overline{\mathbb{Q}}_p$-caractères irréductibles pairs.

On remarque que deux caractères conjugués ont même parité, on peut donc étendre la notion aux caractères sur $\mathbb{Q}_p$.

Définition 2.2.29. *Soit ψ un $\mathbb{Q}_p$-caractère irréductible.*
On dit que ψ est impair (respectivement pair) si pour tout $\chi \in C_\psi$, χ est impair (respectivement pair). On note $X^-_{\mathrm{irr},\mathbb{Q}_p}$ l'ensemble des $\mathbb{Q}_p$-caractères irréductibles impairs et $X^+_{\mathrm{irr},\mathbb{Q}_p}$ celui des $\mathbb{Q}_p$-caractères irréductibles pairs.

On remarque que si ψ est impair, on a $\psi(\tau) = -\psi(1_G) = -\text{card}(C_\psi)$ et si ψ est pair, on a $\psi(\tau) = \psi(1_G) = \text{card}(C_\psi)$.

La parité de ψ se lit également sur son idempotent.

Proposition 2.2.30. *Soit ψ un $\mathbb{Q}_p$-caractère irréductible.*
Alors on a

$$e^- e_\psi = \begin{cases} e_\psi \ \ si \ \ \psi \in X^-_{\text{irr},\mathbb{Q}_p}, \\ 0 \ \ si \ \ \psi \in X^+_{\text{irr},\mathbb{Q}_p}. \end{cases}$$

Démonstration. Soit $\chi \in C_\psi$. On a

$$\tau e_\chi = \frac{1}{\text{card}(G)} \sum_{g\in G} \chi(g^{-1})\tau g = \frac{1}{\text{card}(G)} \sum_{g\in G} \chi(g^{-1}\tau) g = \chi(\tau) e_\chi.$$

Si χ est impair, $\tau e_\chi = -e_\chi$ et $e^- e_\chi = \frac{1-\tau}{2} e_\chi = e_\chi$.
Si χ est pair, $\tau e_\chi = e_\chi$ et $e^- e_\chi = \frac{1-\tau}{2} e_\chi = 0$.
Ainsi,

$$e^- e_\psi = \sum_{\chi\in C_\psi} e^- e_\chi = \begin{cases} e_\psi \ \text{ si } \ \psi \in X^-_{\text{irr},\mathbb{Q}_p}, \\ 0 \ \text{ si } \ \psi \in X^+_{\text{irr},\mathbb{Q}_p}. \end{cases}$$

□

Proposition 2.2.31. *On a l'isomorphisme d'anneaux* $\mathbb{Z}_p[G]^- \simeq \bigoplus_{\psi\in X^-_{\text{irr},\mathbb{Q}_p}} \underline{\mathbb{Z}_p\left[\chi_\psi\right]}$.

Démonstration. D'après la proposition 2.2.23, on a $\mathbb{Z}_p[G] = \bigoplus_{\psi\in X_{\text{irr},\mathbb{Q}_p}} e_\psi \mathbb{Z}_p[G]$, donc d'après la proposition précédente,

$$\mathbb{Z}_p[G]^- = e^- \mathbb{Z}_p[G] = \bigoplus_{\psi\in X_{\text{irr},\mathbb{Q}_p}} e^- e_\psi \mathbb{Z}_p[G] = \bigoplus_{\psi\in X^-_{\text{irr},\mathbb{Q}_p}} e_\psi \mathbb{Z}_p[G].$$

De plus, on a vu dans la proposition 2.2.24 que les anneaux $e_\psi \mathbb{Z}_p[G]$ et $\underline{\mathbb{Z}_p\left[\chi_\psi\right]}$ sont isomorphes, donc on a bien

$$\mathbb{Z}_p[G]^- \simeq \bigoplus_{\psi\in X^-_{\text{irr},\mathbb{Q}_p}} \underline{\mathbb{Z}_p\left[\chi_\psi\right]}.$$

□

Proposition 2.2.32. *Soit M un $\mathbb{Z}_p[G]$-module.*
Alors

$$M^- = \bigoplus_{\psi\in X^-_{\text{irr},\mathbb{Q}_p}} e_\psi M.$$

Démonstration. D'après la proposition 2.2.23, on a

$$M = \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e_\psi M.$$

Donc d'après la proposition 2.2.30, on a

$$M^- = e^- M = \bigoplus_{\psi \in X_{\mathrm{irr},\mathbb{Q}_p}} e^- e_\psi M = \bigoplus_{\psi \in X^-_{\mathrm{irr},\mathbb{Q}_p}} e_\psi M.$$

□

Chapitre 3

Conjectures de Stark

Dans ce chapitre, nous introduisons les conjectures énoncées par Harold Stark dans une série de quatre articles [Sta71], [Sta75], [Sta76] et [Sta80] publiés entre 1971 et 1980.

3.1 Formule analytique du nombre de classes

3.1.1 Version originale

La motivation des conjectures de Stark étant une généralisation de la formule analytique du nombre des classes établie par Dirichlet, nous commencerons par nous y intéresser. Dans cette formule, Dirichlet établit une relation entre des caractéristiques arithmétiques d'un corps de nombres quadratique et une valeur spéciale de la fonction L de Dirichlet associée.

Définition 3.1.1 (Fonction L de Dirichlet)**.** 1. *Soit $n \in \mathbb{N}^*$.*
Un caractère de Dirichlet modulo d est un morphisme $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}^*$. On étend sa définition à $\mathbb{N}^*$ en posant $\chi(n) = \chi(m + d\mathbb{Z})$ si n est premier à d et $\chi(n) = 0$ sinon. Le plus petit $d \in \mathbb{N}^*$ tel que le caractère soit défini modulo d s'appelle son conducteur.

2. *La fonction L de Dirichlet associée au caractère χ est définie, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, par la série de Gauss*

$$L(\chi, s) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

On prolonge ensuite analytiquement la fonction L de Dirichlet à tout le plan complexe.

Le caractère de Dirichlet constant égal à 1 sur $(\mathbb{Z}/d\mathbb{Z})^\times$ s'appelle caractère principal modulo d, pour $d = 1$ on obtient le caractère trivial 1.
Si χ est le caractère trivial 1, la fonction L de Dirichlet associée à χ a un pôle d'ordre 1 en $s = 1$, sinon, elle est holomorphe sur $\mathbb{C}$. Dirichlet s'intéressa plus précisément au comportement de ces fonctions en $s = 1$ pour établir le théorème de la progression arithmétique.

Théorème 3.1.2 (Formule du nombre de classes de Dirichlet)**.** *Soit $k = \mathbb{Q}\left(\sqrt{d}\right)$ un corps de nombres quadratique et χ le caractère défini pour tout $n \in \mathbb{N}$ par le symbole de Jacobi $\chi(n) = \left(\frac{d}{n}\right)$.*
Alors si $d < 0$, on a

$$L(\chi, 1) = \frac{2\pi h_k}{\omega_k \sqrt{-d}}$$

et si $d > 0$, on a

$$L(\chi, 1) = \frac{2h_k \log(\varepsilon_k)}{\sqrt{d}},$$

où h_k est le nombre de classes de k, ω_k le nombre de racines de l'unité de k et quand $d > 0$, ε_k est une unité fondamentale de k.

Définition 3.1.3 (Fonction ζ de Dedekind)**.** *Soit k un corps de nombres. La fonction ζ de Dedekind de k est définie, pour tout $s \in \mathbb{C}$ tel que* $\mathrm{Re}(s) > 1$ *par*

$$\zeta_k(s) = \sum_{I \subset O_k} \frac{1}{N_{k/\mathbb{Q}}(I)^s} = \prod_{\mathfrak{p}\ premier} \frac{1}{1 - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}},$$

où la somme porte sur tous les idéaux non nuls de O_k et le produit eulérien sur ses idéaux premiers.
On prolonge ensuite analytiquement la fonction ζ de Dedekind en une fonction méromorphe sur tout le plan complexe, elle a un unique pôle simple en $s = 1$.

Exemple. Pour $k = \mathbb{Q}$, on retrouve la fonction ζ de Riemann.

Si k est une extension abélienne de $\mathbb{Q}$, sa fonction ζ de Dedekind peut s'écrire comme produit de fonctions L de Dirichlet. En particulier, si $k = \mathbb{Q}\left(\sqrt{d}\right)$, on a pour tout $s \in \mathbb{C}$,

$$\zeta_k(s) = \zeta_{\mathbb{Q}}(s) L(\chi, s),$$

où χ est le caractère donné par le symbole de Jacobi $\chi(n) = \left(\frac{d}{n}\right)$.

La fonction ζ de Dedekind permet donc une reformulation de la formule du nombre de classes de Dirichlet. Celle-ci se généralise à tous les corps de nombres.

Théorème 3.1.4 (Formule analytique du nombre de classes en $s = 1$)**.** *Soit k un corps de nombres. On note (r_1, r_2) sa signature, h_k son nombre de classes, R_k son régulateur, Δ_k son discriminant absolu et ω_k le nombre de racines de l'unité de k. Alors le résidu en $s = 1$ de sa fonction ζ de Dedekind est donné par*

$$\lim_{s\to 1}(s-1)\zeta_k(s) = \frac{2^{r_1+r_2}\pi^{r_2}h_kR_k}{\omega_k\sqrt{|\Delta_k|}}.$$

Grâce à l'équation fonctionnelle reliant les valeurs de ζ_k en s et $1-s$, on peut énoncer une version de la formule analytique des classes qui donne le comportement de la fonction ζ de Dedekind en $s = 0$.

Théorème 3.1.5 (Formule analytique du nombre de classes en $s = 0$)**.** *Soit k un corps de nombres. On note (r_1, r_2) sa signature, h_k son nombre de classes, R_k son régulateur et ω_k le nombre de racines de l'unité de k.*
Alors le terme dominant du développement limité de sa fonction ζ de Dedekind en $s = 0$ est donné par

$$\lim_{s\to 0} s^{-r_1-r_2+1}\zeta_k(s) = \frac{-h_kR_k}{\omega_k}.$$

3.1.2 Version $\mathcal{S}$

Dans cette section, k désigne un corps de nombres et $\mathcal{S}$ désigne un ensemble fini de places de k contenant ses places infinies. Nous allons donner ici une généralisation de la formule analytique des classes relative à l'ensemble de places $\mathcal{S}$.

Commençons par définir les différents $\mathcal{S}$-invariants algébriques de k.

Définition 3.1.6. *L'anneau des $\mathcal{S}$-entiers de k est défini ainsi*

$$O_{k,\mathcal{S}} = \{x \in k \text{ tel que } \forall v \notin \mathcal{S},\ |x|_v \geq 1\}.$$

L'ensemble des éléments inversibles de cet anneau forme le groupe des $\mathcal{S}$-unités de k

$$\mathcal{U}_{k,\mathcal{S}} = O_{k,\mathcal{S}}^{\times} = \{x \in k \text{ tel que } \forall v \notin \mathcal{S},\ |x|_v = 1\}.$$

On note $Cl_{k,\mathcal{S}}$ et on appelle $\mathcal{S}$-groupe de classes de k le quotient du groupe des idéaux fractionnaires de $O_{k,\mathcal{S}}$ par le sous-groupe de ses idéaux fractionnaires principaux. Son cardinal est noté $h_{k,\mathcal{S}}$ et appelé $\mathcal{S}$-nombre de classes.

En choisissant $\mathcal{S} = \mathcal{S}_\infty(k)$ l'ensemble des places infinies de k, on retrouve l'anneau des entiers O_k, le groupe des unités $\mathcal{U}_k$, le groupe de classes Cl_k et le nombre de classes h_k usuels.

Notation. Soit A un anneau commutatif.
On note

$$A[\mathcal{S}] = \left\{ \sum_{v \in \mathcal{S}} a_v v \right\}$$

le A-module libre engendré par $\mathcal{S}$, et $\varepsilon_{\mathcal{S}} : A[\mathcal{S}] \to A$ son morphisme d'augmentation défini par

$$\varepsilon_{\mathcal{S}} \left(\sum_{v \in \mathcal{S}} a_v v \right) = \sum_{v \in \mathcal{S}} a_v.$$

On note $A[\mathcal{S}]_0$ le noyau du morphisme d'augmentation.

Afin de définir le $\mathcal{S}$-régulateur, nous allons nous intéresser au morphisme de groupes

$$\mathrm{Log}_{k,\mathcal{S}} : \begin{cases} \mathcal{U}_{k,\mathcal{S}} \to \mathbb{R}[\mathcal{S}]_0 \\ x \mapsto \sum\limits_{v \in \mathcal{S}} \log |x|_v \, v \end{cases}.$$

En montrant que son noyau est μ_k (le groupe des racines de l'unité de k) et son image un réseau de $\mathbb{R}[\mathcal{S}]_0$, on obtient une généralisation du théorème des unités de Dirichlet.

Théorème 3.1.7 (Théorème des $\mathcal{S}$-unités de Dirichlet)**.** *On a l'isomorphisme de groupes suivant*

$$\mathcal{U}_{k,\mathcal{S}} \simeq \mu_k \times \mathbb{Z}^{\mathrm{card}(\mathcal{S})-1}.$$

On retrouve le théorème des unités de Dirichlet classique en choisissant $\mathcal{S} = \mathcal{S}_\infty(k)$. Le covolume du réseau $\mathrm{Log}_{k,\mathcal{S}}(\mathcal{U}_{k,\mathcal{S}})$ est également un $\mathcal{S}$-invariant important.

Proposition-Définition 3.1.8. *On définit le $\mathcal{S}$-régulateur $R_{k,\mathcal{S}}$ de k de la façon suivante*

$$R_{k,\mathcal{S}} = \frac{\mathrm{vol}\left(\mathrm{Log}_{k,\mathcal{S}}(\mathcal{U}_{k,\mathcal{S}})\right)}{\sqrt{\mathrm{card}(\mathcal{S})}}.$$

Si $(u_i)_{i \in [\![1, \mathrm{card}(S)-1]\!]}$ est un système de $\mathcal{S}$-unités fondamentales (c'est-à-dire si les u_i engendrent $\mathcal{U}_{k,\mathcal{S}}/\mu_k$) et si $v_0 \in \mathcal{S}$, on peut obtenir le $\mathcal{S}$-régulateur ainsi

$$R_{k,\mathcal{S}} = \left| \det \left((\log |u_i|_v)_{\substack{v \in \mathcal{S} \setminus \{v_0\} \\ i \in [\![1, \mathrm{card}(S)-1]\!]}} \right) \right|.$$

Une fois encore, en choisissant $\mathcal{S} = \mathcal{S}_\infty(k)$, on retrouve la définition du régulateur usuel R_k.

Définition 3.1.9 (Fonction de Dedekind associée à $\mathcal{S}$)**.** *La fonction $\zeta_{k,\mathcal{S}}$ de Dedekind de k associée à $\mathcal{S}$ est définie, pour tout $s \in \mathbb{C}$ tel que* $\mathrm{Re}(s) > 1$ *par*

$$\zeta_{k,\mathcal{S}}(s) = \prod_{\mathfrak{p} \notin \mathcal{S}} \frac{1}{1 - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}}.$$

On prolonge ensuite analytiquement $\zeta_{k,\mathcal{S}}$ en une fonction méromorphe sur tout le plan complexe, elle a un unique pôle simple en $s = 1$.

Avec cette généralisation de la fonction ζ de Dedekind, on peut alors étendre la formule analytique des classes.

Théorème 3.1.10 (Version $\mathcal{S}$ de la formule analytique du nombre de classes en $s = 0$)**.** *Le terme dominant du développement limité de sa fonction $\zeta_{k,\mathcal{S}}$ de Dedekind en $s = 0$ est donné par*

$$\lim_{s \to 0} s^{-\mathrm{card}(\mathcal{S})+1} \zeta_{k,\mathcal{S}}(s) = \frac{-h_{k,\mathcal{S}} R_{k,\mathcal{S}}}{\omega_k}.$$

3.2 Conjecture principale de Stark

Nous allons maintenant nous intéresser à la conjecture principale que Stark formula dans [Sta75]. Pour les preuves des résultats, on pourra se référer aux chapitres 1 et 2 des notes de cours publiées de John Tate sur "Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$" [Tat84].

Dans cette partie, K/k est une extension galoisienne de corps et G son groupe Galois.

3.2.1 Fonctions L d'Artin

Dans la section précédente, nous avons vu que l'on peut associer aux extensions quadratiques de $\mathbb{Q}$ les fonctions L de Dirichlet. Nous allons maintenant nous intéresser à une classe plus large de fonctions L que l'on peut associer à toutes les extensions galoisiennes de corps de nombres : les fonctions L d'Artin.

Notation. Soit $\mathfrak{p}$ est un idéal premier de O_k et $\mathcal{P}$ un idéal premier de O_K au-dessus de $\mathfrak{p}$.
On note

$$\mathcal{D}_{\mathcal{P}/\mathfrak{p}} = \{\sigma \in G \text{ tel que } \sigma(\mathcal{P}) = \mathcal{P}\}$$

le sous-groupe de décomposition de $\mathcal{P}$,

$$\mathcal{I}_{\mathcal{P}/\mathfrak{p}} = \{\sigma \in G \text{ tel que } \forall x \in \mathcal{O}_K, \sigma(x) - x \in \mathcal{P}\}$$

le sous-groupe d'inertie de $\mathcal{P}$,

$$\sigma_{\mathcal{P}/\mathfrak{p}} \in \mathcal{D}_{\mathcal{P}/\mathfrak{p}} \text{ tel que } \forall x \in \mathcal{O}_K, \sigma_{\mathcal{P}/\mathfrak{p}}(x) - x^{N_{k/\mathbb{Q}}(\mathfrak{p})} \in \mathcal{P}$$

le Frobenius de $\mathcal{P}$,

$$e_{\mathcal{P}/\mathfrak{p}} = \upsilon_{\mathcal{P}}(\mathfrak{p}\mathcal{O}_K) = \text{card}(\mathcal{I}_{\mathcal{P}/\mathfrak{p}})$$

l'indice de ramification de $\mathcal{P}$ et

$$f_{\mathcal{P}/\mathfrak{p}} = [\mathcal{O}_K/\mathcal{P} : \mathcal{O}_k/\mathfrak{p}] = \frac{\text{card}(\mathcal{D}_{\mathcal{P}/\mathfrak{p}})}{\text{card}(\mathcal{I}_{\mathcal{P}/\mathfrak{p}})}$$

le degré d'inertie de $\mathcal{P}$.

Le Frobenius de $\mathcal{P}$ est unique à multiplication près par les éléments de $\mathcal{I}_{\mathcal{P}/\mathfrak{p}}$. Ainsi, il n'est totalement défini que lorsque l'idéal $\mathcal{P}$ est non ramifié. En revanche, la classe $\overline{\sigma_{\mathcal{P}/\mathfrak{p}}}$ de $\sigma_{\mathcal{P}/\mathfrak{p}}$ dans $\mathcal{D}_{\mathcal{P}/\mathfrak{p}}/\mathcal{I}_{\mathcal{P}/\mathfrak{p}}$ est toujours bien définie et elle engendre $\mathcal{D}_{\mathcal{P}/\mathfrak{p}}/\mathcal{I}_{\mathcal{P}/\mathfrak{p}}$.

Proposition 3.2.1. *Soit $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_k$ et $\mathcal{P}$ et $\mathcal{P}' = \sigma(\mathcal{P})$ deux idéaux premiers de $\mathcal{O}_K$ au-dessus de $\mathfrak{p}$.*
Alors on a

$$\mathcal{D}_{\mathcal{P}'/\mathfrak{p}} = \sigma\mathcal{D}_{\mathcal{P}/\mathfrak{p}}\sigma^{-1},$$

$$\mathcal{I}_{\mathcal{P}'/\mathfrak{p}} = \sigma\mathcal{I}_{\mathcal{P}/\mathfrak{p}}\sigma^{-1},$$

$$\sigma_{\mathcal{P}'/\mathfrak{p}} = \sigma\sigma_{\mathcal{P}/\mathfrak{p}}\sigma^{-1}.$$

Notation. Si l'extension K/k est abélienne, le sous-groupe de décomposition, le sous-groupe d'inertie, le Frobenius, l'indice de ramification et le degré d'inertie ne dépendant pas du choix de l'idéal $\mathcal{P}$ au-dessus de $\mathfrak{p}$, on pourra donc les noter $\mathcal{D}_{\mathfrak{p}}$, $\mathcal{I}_{\mathfrak{p}}$, $\sigma_{\mathfrak{p}}$, $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$.

On considère une représentation complexe (ρ, V) de G dont le caractère est noté χ. On peut étendre $\rho : G \to \text{GL}_{\mathbb{C}}(V)$ à l'anneau de groupe de G, on notera également $\rho : \mathbb{Z}[G] \to \text{End}_{\mathbb{C}}(V)$ le morphisme d'anneaux défini par

$$\rho\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \rho(g).$$

Notation. Pour tout sous-groupe H de G on note V^H l'ensemble des éléments de V invariants par l'action de H :

$$V^H = \{v \in V \text{ tel que } \forall h \in H,\ \rho(h)(v) = v\}.$$

Comme V muni de l'action de G donnée par ρ est un $\mathbb{C}[G]$-module, V est en particulier un G-module. Cette notation coïncide avec la définition des invariants d'un G-module.

Notation. Pour tout sous-groupe F de G on note (ρ_F, V) la représentation de F définie par

$$\rho_F : \begin{cases} F \to \mathrm{GL}_{\mathbb{C}}(V) \\ g \mapsto \rho(g) \end{cases}.$$

Proposition-Définition 3.2.2. *Soit F un sous-groupe de G et H un sous-groupe distingué de F.*
Alors (ρ, V) induit une représentation $(\rho_{F/H}, V^H)$ de F/H définie par

$$\rho_{F/H} : \begin{cases} F/H \to \mathrm{GL}_{\mathbb{C}}(V^H) \\ gH \mapsto \rho(g)\big|_{V^H}^{V^H} \end{cases},$$

où $\rho(g)\big|_{V^H}^{V^H}$ désigne la restriction et corestriction de $\rho(g)$ à V^H.

Démonstration. Commençons par montrer que $\rho_{F/H} : F/H \to \mathrm{GL}_{\mathbb{C}}(V^H)$ est bien définie.
Soit $g \in F$ et $h \in H$, alors pour tout $v \in V^H$, on a

$$\rho(gh)(v) = \rho(g)(\rho(h)(v)) = \rho(g)(v),$$

donc l'image de la classe gH ne dépend pas du choix du représentant.
Soit $v \in V^H$, montrons que pour tout $g \in F$, on a bien $\rho(g)(v) \in V^H$. Soit $h \in H$, on a

$$\rho(h)(\rho(g)(v)) = \rho(hg)(v) = \rho(gg^{-1}hg)(v) = \rho(g)(\rho(g^{-1}hg)(v)) = \rho(g)(v)$$

car H est distingué et donc $g^{-1}hg \in H$, et donc $\rho_{F/H}$ est bien définie. De plus, pour tout $gH, g'H \in F/H$, on a

$$\rho_{F/H}(gg'H) = \rho(gg')|_{V^H}^{V^H} = \rho(g)|_{V^H}^{V^H} \circ \rho(g')|_{V^H}^{V^H} = \rho_{F/H}(gH) \circ \rho_{F/H}(g'H)$$

donc $(\rho_{F/H}, V^H)$ est bien une représentation de F/H. □

Notation. Pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_k$ et tout idéal premier $\mathcal{P}$ de $\mathcal{O}_K$ au-dessus de $\mathfrak{p}$, comme $\mathcal{I}_{\mathcal{P}/\mathfrak{p}}$ est distingué dans $\mathcal{D}_{\mathcal{P}/\mathfrak{p}}$ on peut considérer la représentation de $\mathcal{D}_{\mathcal{P}/\mathfrak{p}}/\mathcal{I}_{\mathcal{P}/\mathfrak{p}}$ donnée par $(\rho_{\mathcal{D}_{\mathcal{P}/\mathfrak{p}}/\mathcal{I}_{\mathcal{P}/\mathfrak{p}}}, V^{\mathcal{I}_{\mathcal{P}/\mathfrak{p}}})$, on la note $(\rho_{\mathcal{P}/\mathfrak{p}}, V^{\mathcal{I}_{\mathcal{P}/\mathfrak{p}}})$.

On montre alors facilement le résultat suivant.

Proposition 3.2.3. *Soit $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_k$ et $\mathcal{P}$ et $\mathcal{P}' = \sigma(\mathcal{P})$ deux idéaux premiers de $\mathcal{O}_K$ au-dessus de $\mathfrak{p}$.*
Alors on a

$$V^{\mathcal{I}_{\mathcal{P}'/\mathfrak{p}}} = \rho(\sigma)\left(V^{\mathcal{I}_{\mathcal{P}/\mathfrak{p}}}\right),$$

$$\mathrm{id}_{V^{\mathcal{I}_{\mathcal{P}'/\mathfrak{p}}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho_{\mathcal{P}'/p}(\overline{\sigma_{\mathcal{P}'/\mathfrak{p}}}) = \rho(\sigma)\left(\mathrm{id}_{V^{\mathcal{I}_{\mathcal{P}/\mathfrak{p}}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho_{\mathcal{P}/p}(\overline{\sigma_{\mathcal{P}/\mathfrak{p}}})\right)\rho(\sigma)^{-1}.$$

En particulier, $\det\left(\mathrm{id}_{V^{\mathcal{I}_{\mathcal{P}/\mathfrak{p}}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho_{\mathcal{P}/\mathfrak{p}}(\overline{\sigma_{\mathcal{P}/\mathfrak{p}}})\right)$ ne dépend pas du choix de l'idéal $\mathcal{P}$ au dessus de $\mathfrak{p}$, on peut donc le noter $\det\left(\mathrm{id}_{V^{I_\mathfrak{p}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho_\mathfrak{p}(\overline{\sigma_\mathfrak{p}})\right)$.

Proposition 3.2.4. *Soit $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_k$ et $\mathcal{P}$ un idéal premier de $\mathcal{O}_K$ au-dessus de $\mathfrak{p}$.*
Alors $\mathrm{id}_{V^{\mathcal{I}_{\mathcal{P}/\mathfrak{p}}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho_{\mathcal{P}/\mathfrak{p}}(\overline{\sigma_{\mathcal{P}/\mathfrak{p}}})$ est inversible.

Démonstration. On vérifie par le calcul que

$$\left(\mathrm{id}_{V^{\mathcal{I}_{\mathcal{P}'/\mathfrak{p}}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-sf_{\mathcal{P}/\mathfrak{p}}}\right)\sum_{j=0}^{f_{\mathcal{P}/\mathfrak{p}}-1}\rho_{\mathcal{P}/\mathfrak{p}}(\overline{\sigma_{\mathcal{P}/\mathfrak{p}}})^j N_{k/\mathbb{Q}}(\mathfrak{p})^{-sj}$$

est l'inverse de $\mathrm{id}_{V^{\mathcal{I}_{\mathcal{P}/\mathfrak{p}}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho_{\mathcal{P}/\mathfrak{p}}(\overline{\sigma_{\mathcal{P}/\mathfrak{p}}})$. □

Ceci nous permet alors de définir les fonctions L d'Artin.

Définition 3.2.5 (Fonction L d'Artin)**.** *On appelle fonction L d'Artin associée au caractère χ la fonction définie pour tout $s \in \mathbb{C}$,* $\mathrm{Re}(s) > 1$ *par*

$$L_{K/k}(\chi, s) = \prod_{\mathfrak{p}\subset\mathcal{O}_k}\frac{1}{\det\left(\mathrm{id}_{V^{I_\mathfrak{p}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho_\mathfrak{p}(\overline{\sigma_\mathfrak{p}})\right)}$$

où le produit eulérien est pris sur les idéaux premiers de $\mathcal{O}_k$.
On prolonge ensuite analytiquement cette fonction sur $\mathbb{C}$.

Exemple. Si $(\rho, V) = (1, \mathbb{C})$ est la représentation triviale de $G = \mathrm{Gal}(K/k)$, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, on a $L_{K/k}(1, s) = \zeta_k(s)$.

Soit $\mathcal{S}$ un ensemble fini de places de k contenant ses places infinies. On peut alors définir une généralisation relative à $\mathcal{S}$ de la fonction L d'Artin.

Définition 3.2.6 (Fonction L d'Artin généralisée)**.** *On appelle fonction L d'Artin associée au caractère χ et relative à l'ensemble de places $\mathcal{S}$ la fonction définie pour tout $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$ par le produit eulérien*

$$L_{K/k,\mathcal{S}}(\chi, s) = \prod_{\mathfrak{p} \notin \mathcal{S}} \frac{1}{\det\left(\mathrm{id}_{V^{I_\mathfrak{p}}} - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s} \rho_\mathfrak{p}(\overline{\sigma_\mathfrak{p}})\right)}.$$

On prolonge ensuite analytiquement cette fonction sur $\mathbb{C}$.

Exemple. Si $(\rho, V) = (1, \mathbb{C})$ est la représentation triviale de $G = \mathrm{Gal}(K/k)$, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, on a $L_{K/k,\mathcal{S}}(1, s) = \zeta_{k,\mathcal{S}}(s)$.

Notation. On note $r_{K/k,\mathcal{S}}(\chi)$ le rang d'annulation de $L_{K/k,\mathcal{S}}(\chi, .)$ en $s = 0$ et $c_{K/k,\mathcal{S}}(\chi)$ le coefficient dominant de son développement en série entière.

3.2.2 Régulateur de Stark

Pour pouvoir généraliser la formule analytique des classes aux fonctions L d'Artin, nous avons besoin de définir un analogue du $\mathcal{S}$-régulateur.
Soit $\mathcal{S}$ un ensemble fini de places de k contenant ses places infinies.

Notation. Pour toute extension de corps de nombres L/k, on note $\mathcal{S}_L$ l'ensemble des places de L au-dessus des places k qui sont dans $\mathcal{S}$.

Pour tout anneau commutatif A, on munit alors $A[\mathcal{S}_K]$ et $A[\mathcal{S}_K]_0$ d'une structure de $A[G]$-module en faisant agir G sur $\mathcal{S}_K$ de la façon suivante :

$$\forall w \in \mathcal{S}_K,\ \forall \sigma \in G,\ \forall x \in K,\ |x|_{\sigma w} = \left|\sigma^{-1}(x)\right|_w.$$

Comme pour tout $\sigma \in G$ et tout $x \in \mathcal{U}_{K,\mathcal{S}_K}$ on a $\sigma(x) \in \mathcal{U}_{K,\mathcal{S}_K}$, le groupe des $\mathcal{S}_K$-unités de K est également un G-module.

Comme pour le $\mathcal{S}$-régulateur, nous allons commencer par nous intéresser au morphisme de $\mathbb{Z}$-modules

$$\mathrm{Log}_{K,\mathcal{S}_K} : \begin{cases} \mathcal{U}_{K,\mathcal{S}_K} \to \mathbb{R}[\mathcal{S}_K]_0 \\ x \mapsto \sum\limits_{w \in \mathcal{S}_K} \log|x|_w \, w \end{cases}.$$

On remarque que pour tout $\sigma \in G$, comme σ permute les places de $\mathcal{S}_K$, on a

$$\begin{aligned} \mathrm{Log}_{K,\mathcal{S}_K}(\sigma(x)) &= \sum_{w \in \mathcal{S}_K} \log|\sigma(x)|_w \, w = \sum_{w \in \mathcal{S}_K} \log|x|_{\sigma^{-1}w} \, w = \sum_{w' \in \mathcal{S}_K} \log|x|_{w'} \, \sigma w' \\ &= \sigma \mathrm{Log}_{K,\mathcal{S}_K}(x), \end{aligned}$$

donc $\mathrm{Log}_{K,\mathcal{S}_K} : \mathcal{U}_{K,\mathcal{S}_K} \to \mathbb{R}[\mathcal{S}_K]_0$ est un morphisme de G-modules.
D'après le théorème 3.1.7 des $\mathcal{S}$-unités de Dirichlet, on a l'isomorphisme de $\mathbb{R}[G]$-module

$$\mathrm{Log}^{\mathbb{R}}_{K,\mathcal{S}_K} : \begin{cases} \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{R} \to \mathbb{R}[\mathcal{S}_K]_0 \\ x \otimes a \mapsto a \sum\limits_{w \in \mathcal{S}_K} \log |x|_w \, w \end{cases} .$$

On en déduit alors l'isomorphisme de $\mathbb{C}[G]$-modules

$$\mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K} : \begin{cases} \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{C} \to \mathbb{C}[\mathcal{S}_K]_0 \\ x \otimes a \mapsto a \sum\limits_{w \in \mathcal{S}_K} \log |x|_w \, w \end{cases} .$$

Cela signifie que les représentations $\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{C}$ et $\mathbb{C}[\mathcal{S}_K]_0$ de G sur $\mathbb{C}$ ont même caractère $\chi_0 : G \to \mathbb{C}$. Or on a les isomorphismes de $\mathbb{C}[G]$-modules suivants

$$\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{C} \simeq (\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}) \otimes \mathbb{C},$$

$$\mathbb{C}[\mathcal{S}_K]_0 \simeq \mathbb{Q}[\mathcal{S}_K]_0 \otimes \mathbb{C}.$$

On en déduit que le caractère de $\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}$ est la corestriction de χ_0 à $\mathbb{Q}$, et celui de $\mathbb{Q}[\mathcal{S}_K]_0$ également. Ainsi, les représentations $\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}$ et $\mathbb{Q}[\mathcal{S}_K]_0$ de G sur $\mathbb{Q}$ ont même caractère donc sont isomorphes en tant que $\mathbb{Q}[G]$-modules.
Soit

$$f : \mathbb{Q}[\mathcal{S}_K]_0 \to \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}$$

un tel isomorphisme de $\mathbb{Q}[G]$-modules. On l'étend naturellement en un isomorphisme de $\mathbb{C}[G]$-modules

$$f^{\mathbb{C}} : \mathbb{C}[\mathcal{S}_K]_0 \to \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{C}.$$

Notation. Pour tout $\mathbb{C}[G]$-module V, on note $V^* = \mathrm{Hom}_{\mathbb{C}[G]}(V, \mathbb{C}[G])$ le $\mathbb{C}[G]$-module dual de V.

Soit (ρ, V) une représentation complexe de G de caractère χ.

Comme $\mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K} \circ f^{\mathbb{C}}$ est un automorphisme de $\mathbb{C}[G]$-module de $\mathbb{C}[\mathcal{S}_K]_0$ et $\mathrm{Hom}_{\mathbb{C}[G]}(V^*, -)$ un foncteur covariant exact à gauche, le morphisme

$$\left(\mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K} \circ f^{\mathbb{C}}\right)_V : \begin{cases} \mathrm{Hom}_{\mathbb{C}[G]}(V^*, \mathbb{C}[\mathcal{S}_K]_0) \to \mathrm{Hom}_{\mathbb{C}[G]}(V^*, \mathbb{C}[\mathcal{S}_K]_0) \\ h \mapsto \mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K} \circ f^{\mathbb{C}} \circ h \end{cases}$$

est un automorphisme de $\mathbb{C}$-module.

Proposition-Définition 3.2.7. *Soit $f : \mathbb{Q}[\mathcal{S}_K]_0 \to \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}$ un isomorphisme de $\mathbb{Q}[G]$-modules.*
Le régulateur de Stark du caractère χ associé à f et relatif à $\mathcal{S}$ est défini par

$$R_{K/k,\mathcal{S}_K}(\chi, f) = \det\left(\left(\mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K} \circ f^{\mathbb{C}}\right)_V\right) \in \mathbb{C}.$$

Ce déterminant ne dépend que du caractère χ de G et non de sa réalisation V.

Proposition 3.2.8. *Supposons que $K = k$ et que $(\rho, V) = (1, \mathbb{C})$ est la représentation triviale de $G = \{1_G\}$. Soit $f : \mathbb{Q}[\mathcal{S}]_0 \to \mathcal{U}_{k,\mathcal{S}_k} \otimes \mathbb{Q}$ un isomorphisme de $\mathbb{Q}$-espaces vectoriels.*
Alors

$$R_{k/k,\mathcal{S}}(1, f) = \det\left(\mathrm{Log}^{\mathbb{C}}_{k,\mathcal{S}} \circ f^{\mathbb{C}}\right) = \pm\, R_{k,S}\, \frac{[U_{k,S} : f(\mathbb{Z}[\mathcal{S}]_0)]}{\omega_k}.$$

3.2.3 Énoncé de la conjecture

À l'aide de la proposition 3.2.8, on peut reformuler la formule analytique des classes en $s = 0$.

Théorème 3.2.9. *Soit $f : \mathbb{Q}[\mathcal{S}]_0 \to \mathcal{U}_{k,\mathcal{S}_k} \otimes \mathbb{Q}$ un isomorphisme de $\mathbb{Q}$-espaces vectoriels.*
Alors on a l'égalité suivante

$$\frac{R_{k/k,\mathcal{S}}(1, f)}{c_{k/k,\mathcal{S}}(1)} = \pm\, \frac{[U_{k,S} : f(\mathbb{Z}[\mathcal{S}]_0)]}{h_{k,\mathcal{S}}}.$$

En particulier la formule analytique des classes implique que le quotient du régulateur de Stark par le coefficient dominant du développement limité de la fonction $\zeta_{k,\mathcal{S}}$ en $s = 0$ est un nombre rationnel. C'est ce résultat que cherche à généraliser la conjecture principale de Stark.

Conjecture 3.2.10 (Conjecture principale de Stark)**.** *Soit χ le caractère d'une représentation complexe de G, $\mathcal{S}$ un ensemble fini de places de k contenant ses places infinies et $f : \mathbb{Q}[\mathcal{S}_K]_0 \to \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}$ un isomorphisme de $\mathbb{Q}[G]$-modules.*
On note

$$A_{K/k,\mathcal{S}}(\chi, f) = \frac{R_{K/k,\mathcal{S}}(\chi, f)}{c_{K/k,\mathcal{S}}(\chi)} \in \mathbb{C}.$$

Alors pour tout automorphisme de corps α de $\mathbb{C}$ on a

$$A_{K/k,\mathcal{S}}(\alpha \circ \chi, f) = \alpha\left(A_{K/k,\mathcal{S}}(\chi, f)\right).$$

Ou de manière équivalente,

$$\begin{cases} A_{K/k,\mathcal{S}}(\chi, f) \in \mathbb{Q}[\chi] \\ A_{K/k,\mathcal{S}}(\sigma\chi, f) = \sigma\left(A_{K/k,\mathcal{S}}(\chi, f)\right) \text{ pour tout } \sigma \in \mathrm{Gal}(\mathbb{Q}[\chi]/\mathbb{Q}) \end{cases}.$$

Théorème 3.2.11. *La véracité de la conjecture principale de Stark ne dépend ni du choix du morphisme $f : \mathbb{Q}[\mathcal{S}_K]_0 \to \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}$, ni du choix de l'ensemble $\mathcal{S}$ de places de k.*

La reformulation de la formule analytique des classes nous permet d'énoncer un premier cas dans lequel cette conjecture est vérifiée.

Théorème 3.2.12. *On suppose que $K = k$ et que $\chi = 1$ est le caractère trivial. Alors la conjecture principale de Stark est vraie pour χ.*

Cette conjecture est toujours un problème ouvert, mais il existe un certain nombre de cas dans lesquels elle a été démontrée.

Théorème 3.2.13. *Soit χ un caractère à valeurs rationnelles.*
La conjecture principale de Stark est vraie pour χ.

Théorème 3.2.14. *Soit χ un caractère tel que $r_{k/k,\mathcal{S}}(\chi) = 0$.*
La conjecture principale de Stark est vraie pour χ.

Il existe aussi des familles de cas auxquelles on peut se ramener pour déduire le cas général.

Théorème 3.2.15. *Si la conjecture principale de Stark est vraie pour toutes les extensions galoisiennes $K/\mathbb{Q}$, alors elle est vraie dans le cas général.*
Si la conjecture principale de Stark est vraie pour toutes les extensions abéliennes K/k, alors elle est vraie dans le cas général.

3.3 Conjecture abélienne de Stark de rang 1

Dans son quatrième article [Sta80], Stark s'intéressa plus particulièrement au cas des extensions abéliennes. Pour les preuves des résultats énoncés dans cette partie, on pourra se référer aux chapitres 3 et 4 de [Tat84].

3.3.1 Conjecture principale de rang 1 et unités de Stark

Soit K/k est une extension galoisienne de corps de nombres, G son groupe de Galois, χ un caractère complexe irréductible de G et $\mathcal{S}$ un ensemble fini de places de k

contenant ses places infinies.
D'après la proposition 2.1.7, $\psi_\chi = \mathrm{tr}_{\mathbb{Q}_p[\chi]/\mathbb{Q}_p}(\chi)$ est un caractère irréductible sur $\mathbb{Q}$. On peut montrer que le $\mathbb{Q}[G]$-module $\mathbb{Q}[\mathcal{S}_K]$ admet une unique sous-représentation de G de caractère ψ_χ. Comme le $\mathbb{Q}[G]$-module $\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}$ lui est isomorphe, il admet également un unique sous-$\mathbb{Q}[G]$-module de caractère ψ_χ, on note $\mathcal{U}_{\psi_\chi}$ ce sous-module.
Comme sur $\overline{\mathbb{Q}}_p$, la notion d'idempotent associé à un χ va nous être utile.

Définition 3.3.1. *On définit ainsi l'idempotent de χ :*

$$e_\chi = \frac{\chi(1)}{\mathrm{card}(G)} \sum_{g\in G} \chi(g^{-1})g = \frac{\chi(1)}{\mathrm{card}(G)} \sum_{g\in G} \overline{\chi(g)}g \in \mathbb{Q}[\chi][G] \subset \mathbb{C}[G].$$

Si $r_{K/k,\mathcal{S}}(\chi) = 0$, on peut montrer que $e_\chi \mathbb{Q}[\mathcal{S}_K] = 0$.

Comme sur $\mathbb{Q}_p$, on note $G_\chi = \mathrm{Gal}(\mathbb{Q}[\chi]/\mathbb{Q})$ et $C_\chi = \left\{g\chi \text{ avec } g \in G_\chi\right\}$.

Définition 3.3.2. *Soit $a \in \mathbb{Q}[\chi]$. On définit*

$$\pi_{K/k,\mathcal{S}}(\chi, a) = \sum_{g\in G_\chi} ga\, L'_{K/k,\mathcal{S}}(g\chi, 0)e_{\overline{g\chi}} \in \mathbb{C}[G].$$

Si $r_{K/k,\mathcal{S}}(\chi) > 1$, on a $\pi_{K/k,\mathcal{S}}(\chi, a) = 0$. On en déduit que si $r_{K/k,\mathcal{S}}(\chi) \neq 1$, on a $\pi_{K/k,\mathcal{S}}(\chi, a)\mathbb{Q}[\mathcal{S}_K] = 0$. La reformulation de Tate de la conjecture de Stark s'intéresse au comportement de $\pi_{K/k,\mathcal{S}}(\chi, a)\mathbb{Q}[\mathcal{S}_K]$ quand $\pi_{K/k,\mathcal{S}}(\chi, a)\mathbb{Q}[\mathcal{S}_K]$.

Proposition 3.3.3. *Soit $a \in \mathbb{Q}[\chi]^*$. On suppose que $r_{K/k,\mathcal{S}}(\chi) = 1$.*
Les assertions suivantes sont équivalentes

1. $\pi_{K/k,\mathcal{S}}(\chi, a)\mathbb{Q}[\mathcal{S}_K]_0 \cap \mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K}(\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Q}) \neq \{0\}$;
2. $\pi_{K/k,\mathcal{S}}(\chi, a)\mathbb{Q}[\mathcal{S}_K]_0 = \mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K}\left(\mathcal{U}_{\psi_\chi}\right)$;
3. *la conjecture principale de Stark est vraie pour χ.*

Soit X un ensemble de caractères irréductibles non triviaux de G vérifiant $C_\chi \subset X$ pour tout $\chi \in X$. On considère une famille $(a_\chi)_{\chi\in X}$ de nombres complexes tels que $\alpha(a_\chi) = \chi_{\alpha\chi}$ pour tout $\chi \in X$. On a alors

$$\pi_{K/k,\mathcal{S}}(\chi, a_\chi) = \sum_{\chi'\in C_\chi} a_{\chi'}\, L'_{K/k,\mathcal{S}}(\chi', 0)e_{\overline{\chi'}}.$$

Donc en notant Rep_X un système de représentants des classes C_χ de X, on obtient

$$\sum_{\chi\in X} a_\chi\, L'_{K/k,\mathcal{S}}(\chi, 0)e_{\overline{\chi}} = \sum_{\chi\in \mathrm{Rep}_X} \pi_{K/k,\mathcal{S}}(\chi, a_\chi).$$

Supposons la conjecture de Stark vérifiée pour tous les $\chi \in X$, la proposition 3.3.3 et la remarque 3.3.1 permettent d'obtenir le résultat suivant

$$\sum_{\chi\in X} a_\chi \, L'_{K/k,\mathcal{S}}(\chi,0)e_{\bar{\chi}}\mathbb{Z}[\mathcal{S}_K]_0 \subset \mathrm{Log}^{\mathbb{C}}_{K,\mathcal{S}_K}(\mathcal{U}_{K/k,\mathcal{S}}\otimes\mathbb{Q}) = \mathbb{Q}\mathrm{Log}_{K,\mathcal{S}_K}(\mathcal{U}_{K/k,\mathcal{S}}).$$

Et comme tous les caractères de X sont orthogonaux au caractère trivial 1, on a même

$$\sum_{\chi\in X} a_\chi \, L'_{K/k,\mathcal{S}}(\chi,0)e_{\bar{\chi}}\mathbb{Z}[\mathcal{S}_K] \subset \mathbb{Q}\mathrm{Log}_{K,\mathcal{S}_K}(\mathcal{U}_{K/k,\mathcal{S}}).$$

Définition 3.3.4 (Unités de Stark)**.** *Soit v une place de $\mathcal{S}$ et $w \in \mathcal{S}_K$ une place au-dessus de v.*
Si la conjecture principale de Stark est vérifiée pour tous les $\chi \in X$, alors il existe un entier $m \in \mathbb{Z}$ et une $\mathcal{S}$-unité $u \in \mathcal{U}_{K/k,\mathcal{S}}$ tels quel

$$m\sum_{\chi\in X} a_\chi \, L'_{K/k,\mathcal{S}}(\chi,0)e_{\bar{\chi}}w = \mathrm{Log}_{K,\mathcal{S}_K}(u),$$

ou de manière équivalente

$$\begin{cases} \log|u|_{\sigma w} = \frac{m\,\chi(1)}{\mathrm{card}(G)} \sum\limits_{\chi\in X} a_\chi \, L'_{K/k,\mathcal{S}}(\chi,0) \sum\limits_{\tau\in\mathcal{D}_{w/v}} \chi(\sigma\tau), \ si\ \sigma\in G \\ |u|_{w'} = 1, \ si\ w' \nmid v \end{cases}.$$

On dit que u est une unité de Stark.

Grâce au théorème des $\mathcal{S}$-unités de Dirichlet, on remarque qu'à m fixé, l'unité de Stark est unique à multiplication par les racines de l'unité près.

3.3.2 Fonctions L de Hecke

On se place dorénavant dans le cas d'une extension abélienne de corps de nombres K/k. On note $G = \mathrm{Gal}(K/k)$ son groupe de Galois et $\hat{G}$ l'ensemble des caractères irréductibles de G.

Notation. Pour tout corps de nombres L on note $\mathcal{S}_\infty(k)$ l'ensemble de ses places infinies, et si L'/L est une extension de corps de nombres on note $\mathcal{S}_{ram}(L'/L)$ l'ensemble des places de L qui sont ramifiées dans L'.

Soit $\mathcal{S}$ un ensemble fini de places de k contenant $\mathcal{S}_\infty(k)$ et $\mathcal{S}_{ram}(K/k)$ et soit $\chi \in \hat{G}$. Comme G est abélien, le caractère χ est de dimension 1.

Proposition 3.3.5. *Pour tout $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$ on a*

$$L_{K/k,\mathcal{S}}(\chi, s) = \prod_{\mathfrak{p}\notin\mathcal{S}} \frac{1}{1 - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\chi(\sigma_{\mathfrak{p}})}.$$

Ces fonctions L ont été définies dans le cas abélien par Erich Hecke pour généraliser les fonctions L de Dirichlet, avant qu'elles ne soient à leur tour généralisées au cas non abélien par Emil Artin. On les appelle donc fonctions L de Hecke.

Définition 3.3.6 (Fonction ζ partielle)**.** *Soit $\sigma \in G$.*
On appelle fonction ζ partielle associée σ et relative à $\mathcal{S}$ la fonction définie pour tout $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$ par la série de Dirichlet

$$\zeta_{K/k,\mathcal{S}}(\sigma, s) = \sum_{\substack{(\mathfrak{a},\mathcal{S})=1 \\ \sigma_{\mathfrak{a}}=\sigma}} N_{k/\mathbb{Q}}(\mathfrak{a})^{-s}$$

où $\mathfrak{a} = \prod_{\mathfrak{p}\notin\mathcal{S}} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$ parcourt les idéaux entiers de k non divisibles par les idéaux contenus dans $\mathcal{S}$ et dont le symbole d'Artin $\sigma_{\mathfrak{a}} = \prod_{\mathfrak{p}\notin\mathcal{S}} \sigma_{\mathfrak{p}}^{\alpha_{\mathfrak{p}}}$ vaut σ.
On prolonge ensuite analytiquement cette fonction sur $\mathbb{C}$.

Les fonctions ζ partielles sont très liées aux fonction L de Hecke.

Proposition 3.3.7. *Pour tout $\sigma \in G$ et pour tout $s \in \mathbb{C}$, on a*

$$\zeta_{K/k,\mathcal{S}}(\sigma, s) = \frac{1}{[K/k]} \sum_{\chi\in\hat{G}} L_{K/k,\mathcal{S}}(\chi, s)\bar{\chi}(\sigma).$$

Pour tout $\chi \in \hat{G}$ et pour tout $s \in \mathbb{C}$, on a

$$L_{K/k,\mathcal{S}}(\chi, s) = \sum_{\sigma\in G} \zeta_{K/k,\mathcal{S}}(\sigma, s)\chi(\sigma).$$

Définition 3.3.8. *Soit v une place infinie de k. On définit de manière analogue aux places finies son groupe de décomposition*

$$\mathcal{D}_v = \{\sigma \in G \text{ tel que } \sigma w = w\}$$

où w est une place infinie de K au dessus de v.
On dit que v est totalement décomposée (ou encore non ramifiée) dans K/k si $\mathrm{card}\,(\mathcal{D}_v) = 1$.

Proposition 3.3.9. *Soit v une place infinie de k.*
– *Si v est complexe, alors v est totalement décomposée dans K/k.*
– *Si v est réelle et si toutes les places au-dessus de v dans K sont réelles, alors v est totalement décomposée dans K/k.*
– *Si v est réelle et s'il existe une place complexe de K au dessus de v, alors v est ramifiée dans K/k.*

On a alors le résultat suivant sur le rang d'annulation des fonctions L de Hecke en $s = 0$.

Proposition 3.3.10. *Le rang d'annulation de $L_{K/k,\mathcal{S}}(\chi, .)$ en $s = 0$ vaut*

$$r_{K/k,\mathcal{S}}(\chi) = \begin{cases} \text{card}(\mathcal{S}) - 1 \ \ si\ \chi = 1 \\ \text{card}\left(\{v \in \mathcal{S} \ tel\ que\ \chi(\mathcal{D}_v) = 1\}\right) \ \ sinon. \end{cases}$$

3.3.3 Conjecture abélienne

Dans son quatrième article [Sta80], Stark proposa une version plus fine de sa conjecture dans le cas des extensions abéliennes, qui précise notamment la valeur de l'entier m présent dans la définition précédente des unités de Stark.
On rappelle que K/k désigne une extension abélienne de corps de nombres.

Notation. On note toujours $\mathcal{S}_\infty(k)$ l'ensemble des places infinies de k et $\mathcal{S}_{ram}(K/k)$ l'ensemble des places finies de k qui sont ramifiées dans K/k. De plus, on note $\mathcal{S}_{tdec}(K/k)$ l'ensemble des places de k qui sont totalement décomposées dans K/k.

Soit $\mathcal{S}$ un ensemble fini de places de k vérifiant les conditions suivantes

(C1) $\mathcal{S}_\infty(k) \cup \mathcal{S}_{ram}(K/k) \subset \mathcal{S}$,

(C2) $\mathcal{S}_{tdec}(K/k) \cap \mathcal{S} \neq \emptyset$,

(C3) $\text{card}(\mathcal{S}) \geq 2$.

Comme précédemment, on note $\mathcal{S}_K$ l'ensemble des places de K au-dessus de places appartenant à $\mathcal{S}$.
Fixons $v \in \mathcal{S}_{tdec}(K/k) \cap \mathcal{S}$, et $w \in \mathcal{S}_K$ une place au-dessus de v.

Notation. On note

$$\mathcal{U}_{K/k,v} = \begin{cases} \{u \in \mathcal{U}_{K,\mathcal{S}_K} \text{ tel que } |u|_{w'} = 1 \text{ pour tout } w' \nmid v\} & \text{si card}(S) \geq 3 \\ \{u \in \mathcal{U}_{K,\mathcal{S}_K} \text{ tel que } |u|_{w'} = |u|_{w''} \text{ pour tout } w', w'' \nmid v\} & \text{si card}(S) = 2 \end{cases}.$$

Conjecture 3.3.11 (Conjecture abélienne de rang 1 de Stark)**.** *Il existe une $\mathcal{S}$-unité $\varepsilon_{K/k,\mathcal{S},w} \in \mathcal{U}_{K/k,v}$ telle que*

1. *pour tout caractère irréductible χ de G on a*

$$L'_{K/k,\mathcal{S}_K}(\chi,0) = -\frac{1}{\omega_K}\sum_{\sigma\in G}\chi(\sigma)\log\left|\sigma(\varepsilon_{K/k,\mathcal{S},w})\right|_w$$

2. *et l'extension $K\left(\varepsilon_{K/k,\mathcal{S},w}^{1/\omega_K}\right)/k$ est abélienne.*

Une telle unité s'appelle unité de Stark associée à l'extension K/k, l'ensemble de places $\mathcal{S}$ et la place w.

On remarque que la véracité de la conjecture est indépendante du choix de la place $w \in \mathcal{S}_K$ au-dessus v et si $w' = \sigma w$ avec $\sigma \in G$, alors $\varepsilon_{K/k,\mathcal{S},w'} = \sigma(\varepsilon_{K/k,\mathcal{S},w})$.

Proposition 3.3.12. *La condition 1. est équivalente à la condition suivante :*

1.' *pour tout $\sigma \in G$, on a*

$$\log\left|\sigma(\varepsilon_{K/k,\mathcal{S},w})\right|_w = -\omega_K\zeta'_{K/k,\mathcal{S}}(\sigma,0).$$

Comme la conjecture fixe les valuations de l'unité de Stark selon toutes les places de K, cette dernière est unique à multiplication près par une racine de l'unité de K. Tout comme pour la conjecture principale de Stark, il existe un certain nombre de cas dans lesquels la conjecture est vérifiée.

Proposition 3.3.13. *On suppose que $\mathcal{S}$ contient au moins deux places totalement décomposées.*
Alors la conjecture abélienne de rang 1 *de Stark est vraie.*

On en déduit que la véracité de la conjecture ne dépend que de l'extension K/k et de l'ensemble de places $\mathcal{S}$ et non du choix de v, puisque lorsqu'il y a un choix possible la conjecture est démontrée. On notera donc $\mathrm{St}(K/k,\mathcal{S})$ la conjecture abélienne de Stark de rang 1. Lorsqu'il y une unique place totalement décomposée, on note $\varepsilon_{K/k,\mathcal{S}}$ l'unité de Stark associée (définie à multiplication par une racine de l'unité et à conjugaison galoisienne près).

Corollaire 3.3.14. – *Si $K = k$, alors* $\mathrm{St}(k/k,\mathcal{S})$ *est vraie.*
– *Si k a au moins deux plongements complexes, alors* $\mathrm{St}(K/k,\mathcal{S})$ *est vraie.*
– *Si k a un plongement complexe et si $\mathcal{S}$ contient une place finie totalement décomposée, alors* $\mathrm{St}(K/k,\mathcal{S})$ *est vraie.*

La véracité de la conjecture dans certains cas entraîne sa véracité dans d'autres cas.

Proposition 3.3.15. *Soit $\mathcal{S}'$ un ensemble fini de places de k vérifiant $\mathcal{S} \subset \mathcal{S}'$.*
Alors $\mathrm{St}(K/k,\mathcal{S})$ *implique* $\mathrm{St}(K/k,\mathcal{S}')$.

Proposition 3.3.16. *Soit F/k une sous-extension de K/k.*
Alors $\mathrm{St}(K/k, \mathcal{S})$ *implique* $\mathrm{St}(F/k, \mathcal{S})$.

Lorsqu'il énonça sa conjecture dans [Sta80], Stark la démontra dans deux cas.

Théorème 3.3.17 (Stark)**.** *On suppose que $k = \mathbb{Q}$ ou que k est un corps quadratique imaginaire.*
Alors $\mathrm{St}(K/k, \mathcal{S})$ *est vraie.*

La théorie du corps de classes permet de démontrer le résultat suivant.

Lemme 3.3.18. *On suppose que k a au moins* $\mathrm{card}(\mathcal{S}_\infty(k)) - 1$ *places totalement décomposée dans K/k et que $\mathcal{S}_{ram}(K/k) = \emptyset$.*
Alors, toutes les places infinies de k sont totalement décomposée dans K/k.

On peut donc déduire du théorème précédent le corollaire suivant.

Corollaire 3.3.19. *Si* $\mathrm{card}(\mathcal{S}) = 2$*, alors* $\mathrm{St}(K/k, \mathcal{S})$ *est vraie.*

D'après la proposition 3.3.13, comme les places complexes sont toujours totalement décomposées, on peut décomposer les cas à étudier en trois grandes familles.

$\mathbf{TR}_\infty$: v est une place réelle. Le corps k est *totalement réel* : toutes ses places infinies sont réelles. Les places infinies de K au-dessus de v sont réelles, les autres sont complexes. $\mathcal{S}$ n'a pas de nombre premier totalement décomposé.

$\mathbf{PTR}_\infty$: v est une place complexe. Le corps k est *presque totalement réel* : à part v toutes ses places sont réelles. Le corps K est totalement complexe : toutes ses places infinies sont complexes. $\mathcal{S}$ n'a pas de nombre premier totalement décomposé.

$\mathbf{TR}_\mathbf{p}$: v est une place finie. Le corps k est *totalement réel*. Le corps K est totalement complexe : toutes ses places infinies sont complexes. $\mathcal{S}$ n'a pas d'autre nombre premier totalement décomposé.

Le cas **$\mathbf{TR}_\mathbf{p}$** est à l'origine de la conjecture de Brummer-Stark dont on ne traitera pas ici.

3.3.4 Formules d'indice

Dans le reste de cette thèse, on s'intéresse au cas $\mathbf{TR}_\infty$. On a vu que si $k = \mathbb{Q}$ la conjecture est vraie, on peut donc supposer que $k \neq \mathbb{Q}$.

On a alors $\mathrm{card}(\mathcal{S}_\infty(k)) \geq 2$ et de plus k a une unique place infinie totalement décomposée, donc on déduit du lemme 3.3.3 que $\mathrm{card}(\mathcal{S}) \geq 3$. Comme $v \in \mathcal{S}_\infty(k)$, on a

$$\mathcal{U}_{K/k,v} = \{u \in \mathcal{U}_K \text{ tel que } |u|_{w'} = 1 \text{ pour tout } w' \nmid v\} \subset \mathcal{U}_K.$$

On en déduit également que K admet des plongements réels, et donc $\omega_K = 2$.

La conjecture abélienne de Stark se reformule alors ainsi.

Conjecture 3.3.20 (Conjecture abélienne de rang 1 de Stark)**.** *Il existe une unité $\varepsilon_{K/k,\mathcal{S}} \in \mathcal{U}_K$ telle que*

0. pour toute place infinie w' de K ne divisant pas v, on a

$$|u|_{w'} = 1,$$

1. pour tout caractère irréductible χ de G on a

$$L'_{K/k,\mathcal{S}_K}(\chi, 0) = -\frac{1}{2}\sum_{\sigma\in G}\chi(\sigma)\log\left|\sigma(\varepsilon_{K/k,\mathcal{S}})\right|_w$$

2. et l'extension $K\left(\sqrt{\varepsilon_{K/k,\mathcal{S}}}\right)/k$ est abélienne.

On peut reformuler la deuxième condition à l'aide de la proposition 1.2 du chapitre IV de [Tat84].

Proposition 3.3.21. *La condition 2. est équivalente à la condition suivante :*

2.' pour tout $\sigma \in G$, on a

$$\varepsilon_{K_M/k,\mathcal{S}}^{\sigma-1_G} \in \mathcal{U}_K^2.$$


On suppose dorénavant la conjecture de Stark vraie dans le cas $\mathbf{TR}_\infty$.

On a vu que l'unité de Stark est unique à multiplication par une racine de l'unité et à conjugaison galoisienne près. Il est donc naturel de s'intéresser au sous-groupe du groupe des unités engendré par ± 1 et les conjugués galoisiens de l'unité de Stark. Dans cette thèse, nous nous intéressons plus particulièrement au quotient de la partie moins du groupe de classes par le sous-groupe engendré par les conjugués de l'unité de Stark. Pour que l'indice de ce sous-groupe dans le groupe des unités soit défini et fini, il est nécessaire de faire les hypothèses suivantes

(C4) K est une extension de degré 2 de son sous-corps totalement réel maximal K^+,

(C5) toutes les places finies dans $\mathcal{S}_{K^+}$ sont soit ramifiées, soit inertes dans K/K^+.

Ces deux conditions reviennent donc à demander l'existence d'une sous-extension L/k de K/k telle que $[K : L] = 2$ et telle que toute place dans $\mathcal{S}_L$ qui n'est pas au-dessus de v admette une unique place au-dessus d'elle dans K. On a alors $L = K^+$.

Définition 3.3.22. *On définit alors le sous-$\mathbb{Z}[G]$-module de $\mathcal{U}_K$ suivant*

$$\mathcal{U}_{\mathrm{Stark},K/k,\mathcal{S}} = \mathrm{Vect}_{\mathbb{Z}[G]}\left(\varepsilon_{K_\mathcal{M}/k,\mathcal{S}}; u \in \mathcal{U}_{K^+}\right).$$

Sous ces conditions, Xavier-François Roblot a établi dans [Rob13] une première formule d'indice.

Théorème 3.3.23. *L'indice de $\mathcal{U}_{\mathrm{Stark},K/k,\mathcal{S}}$ dans le groupe des unités de K vaut*

$$(\mathcal{U}_K : \mathcal{U}_{\mathrm{Stark},K/k,\mathcal{S}}) = 2^{[K^+:k]+t_\mathcal{S}-1}\frac{h_K}{h_{K^+}}$$

où $t_\mathcal{S}$ désigne le nombre de places finies de $\mathcal{S}_{K^+}$ qui sont inertes dans K/K^+.

Comme K et K^+ ont tous deux les mêmes racines de l'unité 1 et -1, cette formule d'indice reste vraie quand on considère les parties $\mathbb{Z}$-libres de ces deux groupes.

Notation. Pour tout corps de nombres L, on note

$$\overline{\mathcal{U}}_L = \mathcal{U}_L/\mu_L,$$

et pour tout $u \in \mathcal{U}_L$ on note $\bar{u}$ son image dans $\overline{\mathcal{U}}_L$.
Si de plus $\mathcal{S}$ est un ensemble fini de places de L contenant ses places infinies, on note

$$\overline{\mathcal{U}}_{L,\mathcal{S}} = \mathcal{U}_{L,\mathcal{S}}/\mu_L,$$

et pour tout $u \in \mathcal{U}_{L,\mathcal{S}}$ on note $\bar{u}_\mathcal{S}$ son image dans $\mathcal{U}_{L,\mathcal{S}}/\mu_L$.

Comme $[K : K^+] = 2$, $G^+ = \mathrm{Gal}(K/K^+)$ a un unique élément non trivial que l'on note τ. Comme τ est un élément d'ordre 2 fixé de $\mathrm{Gal}(K/k)$, on peut définir les parties moins Cl_K^- et $\overline{\mathcal{U}}_K^-$. D'après la théorie du corps de classes $\mathcal{N}_{G^+,Cl_K}(Cl_K) \simeq Cl_{K^+}$ donc $\mathrm{card}(Cl_K^-) = \frac{h_K}{h_{K^+}}$, et il existe $e \in \mathbb{N}$ tel que $\left(\overline{\mathcal{U}}_{K^+} : \mathcal{N}_{G^+,\overline{\mathcal{U}}_K}(\mathcal{U}_K)\right) = 2^e$.

Proposition 3.3.24. *On a $\bar{\varepsilon}_{K_\mathcal{M}/k,\mathcal{S}} \in \overline{\mathcal{U}}_K^-$.*

Démonstration. Si on fixe un plongement complexe de K, ce plongement est associé à une place $w' \nmid v$, donc $\left|\varepsilon_{K_\mathcal{M}/k,\mathcal{S}}\right|_{w'} = 1$. De plus, τ s'identifie alors à la conjugaison complexe sur K, et donc $(1_G + \tau)(\varepsilon_{K_\mathcal{M}/k,\mathcal{S}}) = \left|\varepsilon_{K_\mathcal{M}/k,\mathcal{S}}\right|_{w'}^2 = 1$. □

Ceci permet la reformulation de 3.3.23 en une deuxième formule d'indice.

Théorème 3.3.25. *L'indice du G-module engendré par $\bar{\varepsilon}_{K_\mathcal{M}/k,\mathcal{S}}$ dans $\overline{\mathcal{U}}_K^-$ vaut*

$$\left(\overline{\mathcal{U}}_K^- : \mathbb{Z}[G]\,\bar{\varepsilon}_{K_\mathcal{M}/k,\mathcal{S}}\right) = 2^{e+t_S}\mathrm{card}(Cl_K^-).$$

Corollaire 3.3.26. *Soit p un nombre premier impair.*
Alors

$$\mathrm{card}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}_{K_\mathcal{M}/k,\mathcal{S}} \otimes \mathbb{Z}_p\right) = \mathrm{card}(Cl_K^- \otimes \mathbb{Z}_p).$$

Afin d'obtenir plus d'informations sur les unités de Stark, il est intéressant de comparer les cardinaux des χ-composantes. En 1992, Karl Rubin montra dans [Rub92] des formules d'indices de χ-quotient pour un autre sous-groupe des unités liés aux unités de Stark valables sous certaines conditions. Pour nous placer dans le cadre d'application de ses résultats, il est nécessaire de faire la supposition suivante

(C5) K contient le corps de classes de Hilbert $k(1)$ de k.

Notation. Soit $\mathfrak{f} = \mathfrak{f}(K/k)$ le conducteur de l'extension K/k. Pour tout cycle $\mathcal{M}$ de k divisant $\mathfrak{f}$, on note $k(\mathcal{M})$ le corps de classes de rayon de $\mathcal{M}$, $K_\mathcal{M} = K \cap k(\mathcal{M})$ et $G_\mathcal{M} = \mathrm{Gal}(K_\mathcal{M}/k) \subset G$.

Comme v est totalement décomposée dans K/k, pour tout $\mathcal{M} \mid \mathfrak{f}$, v est également totalement décomposée dans $K_\mathcal{M}/k$, et comme $\mathcal{S}_{ram}(K_\mathcal{M}/k) \subset \mathcal{S}_{ram}(K/k) \subset \mathcal{S}$ on peut appliquer la conjecture de Stark à $K_\mathcal{M}/k$, $\mathcal{S}$ et v. On note $\varepsilon_\mathcal{M}$ l'unité de Stark obtenue. D'après la reformulation 2.', on a $\varepsilon_\mathcal{M}^{\sigma-1_G} \in \mathcal{U}_{K_\mathcal{M}}^2 \subset \mathcal{U}_K^2$. Et comme l'unité de Stark est définie à multiplication près par une racine de l'unité et à conjugaison galoisienne près, on peut définir le sous-groupe des unités de K suivant.

Définition 3.3.27. *On appelle groupe des unités de Stark le sous-$\mathbb{Z}[G]$-module de $\mathcal{U}_K$ défini ainsi*

$$C_{\mathrm{Stark},K/k,\mathcal{S}} = \mathrm{Vect}_{\mathbb{Z}[G]}\left(\pm 1;\ \sqrt{\varepsilon_{K_\mathcal{M}/k,\mathcal{S}}^{\sigma-1_G}}\ \textit{pour tout } \mathcal{M} \mid \mathfrak{f} \textit{ et tout } \sigma \in G_\mathcal{M}\right).$$

Les résultats de Rubin nous fournissent le théorème suivant.

Théorème 3.3.28. *Soit p un nombre premier ne divisant pas $[K : k]$ et χ un $\overline{\mathbb{Q}}_p$-caractère irréductible impair de G.*
Alors

$$\mathrm{card}\left(\left(\mathcal{U}_K/C_{\mathrm{Stark},K/k,\mathcal{S}} \otimes \mathbb{Z}_p\right)_\chi\right) = \mathrm{card}\left(\left(Cl_K^- \otimes \mathbb{Z}_p\right)_\chi\right).$$

De ce théorème, Roblot déduit des raffinements de sa formule d'indice globale.

Théorème 3.3.29. *Soit p un nombre premier ne divisant pas $[K : k]$ et χ un $\overline{\mathbb{Q}}_p$-caractère irréductible impair de G.*
Alors

$$\mathrm{card}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}_{K_M/k,S}\otimes\mathbb{Z}_p\right)_\chi\right)=\mathrm{card}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right.$$

Ces formules sont le point de départ du cas semi-simple traité dans le chapitre suivant.

Chapitre 4

Liens entre les idéaux de Fitting du groupe de classes et des unités

Commençons par rappeler le cadre dans lequel on se place. On considère une extension abélienne de corps de nombres K/k et un ensemble fini $\mathcal{S}$ de places de k qui satisfont les conditions suivantes :
– k est un corps de nombres totalement réel différent de $\mathbb{Q}$,
– $[K : K^+] = 2$, on note τ le générateur de $\mathrm{Gal}(K/K^+)$,
– il existe une unique place infinie v de k qui reste réelle dans K,
– $\mathcal{S}_\infty(k) \cup \mathcal{S}_{ram}(k) \subset \mathcal{S}$,
– tous les idéaux premiers dans $\mathcal{S}_{K^+}$ sont inertes ou ramifiés dans K/K^+.


On suppose la conjecture de Stark vérifiée dans ce cadre, on note $\varepsilon = \varepsilon_{K_\mathcal{M}/k,\mathcal{S}} \in \mathcal{U}_K$ l'unité de Stark obtenue et $\bar{\varepsilon}$ son image dans $\overline{\mathcal{U}}_K = \mathcal{U}_K/\{\pm 1\}$.

4.1 Conjectures sur l'égalité des idéaux de Fitting

D'après la proposition 3.3.24, on sait que $\bar{\varepsilon} \in \overline{\mathcal{U}}_K^-$ et donc que $\mathbb{Z}[G]\,\bar{\varepsilon}$ est un sous-G-module de $\overline{\mathcal{U}}_K^-$.

Dans ce cadre, on conjecture le lien suivant entre unité de Stark et groupe de classes.

Conjecture 4.1.1 (Conjecture globale faible)**.** *On a égalité entre les deux idéaux de Fitting suivants*

$$\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}[1/2]\right) = \mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^- \otimes \mathbb{Z}[1/2]\right).$$

Pour tout p premier impair, cette conjecture globale se traduit localement de la façon suivante.

Conjecture 4.1.2 (Conjecture locale faible)**.** *Soit p un nombre premier impair. On a égalité entre les deux idéaux de Fitting suivants*

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)=\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right).$$

Proposition 4.1.3. *La conjecture globale faible est vérifiée si et seulement si, pour tout nombre premier impair la conjecture locale faible l'est.*

Démonstration. Notons $I=\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}[1/2]\right)$.
Pour tout G-module M et pour tout $p\neq 2$ on a $\left(M\otimes\mathbb{Z}[1/2]\right)\otimes\mathbb{Z}_p\simeq M\otimes\mathbb{Z}_p$, donc

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(M\otimes\mathbb{Z}_p\right)=\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\left(M\otimes\mathbb{Z}[1/2]\right)\otimes\mathbb{Z}_p\right).$$

Donc d'après la proposition 1.6.13 de principe local-global des idéaux de Fitting, on a alors pour tout $p\neq 2$

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)=I\mathbb{Z}_p[G].$$

Puis d'après le principe local-global,

$$\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^-\otimes\mathbb{Z}[1/2]\right)=I$$

si et seulement si pour tout $p\neq 2$, on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right)=I\mathbb{Z}_p[G].$$

Autrement dit, on a

$$\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^-\otimes\mathbb{Z}[1/2]\right)=\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}[1/2]\right)$$

si et seulement si, pour tout $p\neq 2$, on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right)=\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right).$$

□

Dans certains cas, on peut espérer une propriété plus forte.

Conjecture 4.1.4 (Propriété globale forte)**.** *On a l'isomorphisme de $\mathbb{Z}[1/2][G]$-module suivant*

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}[1/2]\simeq\mathbb{Z}[1/2][G]/\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^-\otimes\mathbb{Z}[1/2]\right).$$

Pour que cette propriété ait des chances d'être vérifiée, il faut en particulier que $\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}[1/2]$ puisse être engendré par 2 générateurs en tant que $\mathbb{Z}[1/2][G]$-module.

Cette propriété admet également une version locale.

Conjecture 4.1.5 (Propriété locale forte)**.** *Soit p un nombre premier impair. On a l'isomorphisme de $\mathbb{Z}_p[G]$-modules suivant*

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[G]/\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right).$$

Proposition 4.1.6. *La propriété globale forte est satisfaite si et seulement si, pour tout nombre premier impair la propriété locale forte l'est.*

Démonstration. D'après la proposition 1.6.10, on a

$$\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^- \otimes \mathbb{Z}[1/2]\right) = \mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^- \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}[1/2][G]\right) = \mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right)\mathbb{Z}[1/2][G]$$

et pour tout p premier

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right) = \mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}_p[G]\right) = \mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right)\mathbb{Z}_p[G].$$

Donc la proposition 1.3.1 implique

$$\begin{aligned}\mathbb{Z}[1/2][G]/\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^- \otimes \mathbb{Z}[1/2]\right) &\simeq \mathbb{Z}[G]/\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right) \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}[1/2][G] \\ &\simeq \mathbb{Z}[G]/\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right) \otimes \mathbb{Z}[1/2]\end{aligned}$$

en tant que $\mathbb{Z}[1/2]$-modules, et pour tout p premier

$$\begin{aligned}\mathbb{Z}_p[G]/\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right) &\simeq \mathbb{Z}[G]/\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right) \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}_p[G] \\ &\simeq \mathbb{Z}[G]/\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right) \otimes \mathbb{Z}_p\end{aligned}$$

en tant que $\mathbb{Z}_p$-modules.
En utilisant le corollaire 1.4.4, on a alors les isomorphismes de $\mathbb{Z}[1/2]$-modules suivants

$$\begin{aligned}\mathbb{Z}[1/2][G]/\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^-\right) &\simeq \mathbb{Z}[G]/\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right) \otimes \mathbb{Z}[1/2] \\ &\simeq \bigoplus_{p\neq 2}\left(\mathbb{Z}_p[G]/\mathrm{Fitt}_{\mathbb{Z}_p[G]}(Cl_K^- \otimes \mathbb{Z}_p)\right),\end{aligned}$$

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}[1/2] \simeq \bigoplus_{p\neq 2}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}_p\right).$$

Ces isomorphismes commutant avec l'action de G, on en déduit que si pour tout $p \neq 2$ premier on a

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[G]/\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right)$$

en tant que $\mathbb{Z}_p[G]$-modules, alors

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}[1/2] \simeq \mathbb{Z}[1/2][G]/\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^- \otimes \mathbb{Z}[1/2]\right)$$

en tant que $\mathbb{Z}[1/2][G]$-modules.
Réciproquement, si

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}[1/2] \simeq \mathbb{Z}[1/2][G]/\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^- \otimes \mathbb{Z}[1/2]\right),$$

alors pour tout $p \neq 2$, on a

$$\begin{aligned}\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}_p &\simeq \mathbb{Z}[1/2][G]/\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^- \otimes \mathbb{Z}[1/2]\right) \otimes \mathbb{Z}_p \\ &\simeq \mathbb{Z}_p[G]/\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right).\end{aligned}$$

□

Ces nouvelles conjectures représentent des versions plus fortes des précédentes.

Proposition 4.1.7. *La propriété locale forte implique la conjecture locale faible.*

Démonstration. Soit p premier impair.
On suppose qu'on a l'isomorphisme de $\mathbb{Z}_p[G]$-modules suivant

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon} \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[G]/\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right).$$

Alors on a

$$\begin{aligned}\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}_p[G]\,\bar{\varepsilon} \otimes \mathbb{Z}_p\right) &= \mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\mathbb{Z}_p[G]/\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right)\right) \\ &= \mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^- \otimes \mathbb{Z}_p\right)\end{aligned}$$

d'après la proposition 1.6.6. □

Corollaire 4.1.8. *La propriété globale forte implique la conjecture globale faible.*

4.2 Le cas semi-simple

Dans cette section, nous nous intéressons au cas semi-simple, ce qui signifie que le nombre premier considéré ne divise pas le cardinal de G. Nous allons démontrer que ces nombres premiers vérifient la conjecture locale forte, en commençant par la démonstration de la conjecture locale faible. Pour être dans le cadre d'application de [Rub92], nous faisons l'hypothèse supplémentaire suivante :
– K contient le corps de classes de Hilbert de k.

4.2.1 Théorème semi-simple faible

Le but de cette section est d'établir la conjecture faible dans le cas semi-simple.

Théorème 4.2.1 (Théorème semi-simple faible)**.** *Soit p un nombre premier ne divisant pas* card(G).
Alors

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)=\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right).$$

Pour y parvenir, nous procédons d'abord χ-composante par χ-composante puis nous les recollerons.

Lemme 4.2.2. *Soit χ un $\overline{\mathbb{Q}}_p$-caractère irréductible de G.*
On a alors l'égalité suivante entre idéaux de Fitting

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)=\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right).$$

Démonstration. D'après la formule d'indice 3.3.29 démontrée dans [Rob13], on a

$$\mathrm{card}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)=\mathrm{card}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right).$$

L'anneau $\mathbb{Z}_p[\chi]$ est un anneau de valuation discrète, donc d'après la proposition 1.6.8 on a

$$\mathrm{card}\left(\mathbb{Z}_p[\chi]/\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)\right)=\mathrm{card}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)$$

et

$$\mathrm{card}\left(\mathbb{Z}_p[\chi]/\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right)\right)=\mathrm{card}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right),$$

donc

$$\mathrm{card}\left(\mathbb{Z}_p[\chi]/\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)\right)=\mathrm{card}\left(\mathbb{Z}_p[\chi]/\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right)\right).$$

Notons π l'uniformisante de $\mathbb{Z}_p[\chi]$ et m et n les valuations π-adiques des générateurs de $\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\right)\otimes\mathbb{Z}_p\right)_\chi\right)$ et de $\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right)$.
On a

$$\begin{aligned}\mathrm{card}\left(\mathbb{Z}_p[\chi]/\pi^m\mathbb{Z}_p[\chi]\right)&=\mathrm{card}\left(\mathbb{Z}_p[\chi]/\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)\right)\\&=\mathrm{card}\left(\mathbb{Z}_p[\chi]/\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right)\right)\\&=\mathrm{card}\left(\mathbb{Z}_p[\chi]/\pi^n\mathbb{Z}_p[\chi]\right)\end{aligned}$$

donc $m=n$ et

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)=\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right).$$

□

En recollant les χ-quotients, nous allons maintenant démontrer le théorème 4.2.1.

Démonstration. Comme les $\mathbb{Z}_p[G]$-modules $\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p$ et $Cl_K^-\otimes\mathbb{Z}_p$ sont finis, donc de type fini et que pour tout χ irréductible on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)_\chi\right)=\mathrm{Fitt}_{\mathbb{Z}_p[\chi]}\left(\left(Cl_K^-\otimes\mathbb{Z}_p\right)_\chi\right),$$

on déduit l'égalité

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)=\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right)$$

du théorème 2.2.27 de décomposition du Fitting en χ-composantes. □

4.2.2 Monogénéité de $\overline{\mathcal{U}}_K^-\otimes\mathbb{Z}_p$ comme $\mathbb{Z}_p[G]$-module

Dans cette section, nous allons identifier le G-module $\overline{\mathcal{U}}_K^-$ à un idéal $I_{\overline{\mathcal{U}}_K^-}$ de $\mathbb{Z}[G]$. Ceci fournira une identification de $\overline{\mathcal{U}}_K^-\otimes\mathbb{Z}_p$ avec un idéal de $\mathbb{Z}_p[G]$, ce qui permettra d'établir sa monogénéité.

Proposition 4.2.3. *Il existe $\bar{\alpha}\in\overline{\mathcal{U}}_K^-$ tel que*

$$\overline{\mathcal{U}}_K^-\otimes\mathbb{Q}=\mathbb{Q}[G]^-\,(\alpha\otimes 1)=\mathbb{Q}[G]\,(\alpha\otimes 1).$$

De plus $\mathrm{Ann}_{\mathbb{Q}[G]^-}(\bar{\alpha}\otimes 1)=0$ *et donc*

$$\overline{\mathcal{U}}_K^-\otimes\mathbb{Q}\simeq\mathbb{Q}[G]^-$$

en tant que $\mathbb{Q}[G]$-modules.

Démonstration. D'après la section 3.2.2 sur le régulateur de Stark,

$$\overline{\mathcal{U}}_K\otimes\mathbb{Q}=\mathcal{U}_{K,\mathcal{S}_\infty(K)}\otimes\mathbb{Q}\simeq\mathbb{Q}[\mathcal{S}_\infty(K)]_0$$

en tant que $\mathbb{Q}[G]$-modules, donc

$$\overline{\mathcal{U}}_K^-\otimes\mathbb{Q}\simeq\mathbb{Q}[\mathcal{S}_\infty(K)]_0^-$$

en tant que $\mathbb{Q}[G]$-modules. Nous allons donc étudier $\mathbb{Q}[\mathcal{S}_\infty(K)]_0^-$. Comme

$$\mathbb{Q}[\mathcal{S}_\infty(K)]=\bigoplus_{v'\in\mathcal{S}_\infty(k)}\mathbb{Q}[G]\,w'$$

où pour tout $v'\in\mathcal{S}_\infty(k)$, w' est une place de K au-dessus de v', on a

$$\mathbb{Q}[\mathcal{S}_\infty(K)]^-=\bigoplus_{v'\in\mathcal{S}_\infty(k)}\mathbb{Q}[G]^-\,w'.$$

Or si $v' \neq v$, on a $\tau w' = w'$, donc $\mathbb{Q}[G]^- w' = \mathbb{Q}[G](1_G - \tau)w' = 0$. Ainsi

$$\mathbb{Q}[\mathcal{S}_\infty(K)]^- = \mathbb{Q}[G]^- w$$

où w est une place de K au-dessus de v.
On a

$$\mathbb{Q}[\mathcal{S}_\infty(K)]_0^- = \mathbb{Q}[\mathcal{S}_\infty(K)]^- \cap \mathbb{Q}[\mathcal{S}_\infty(K)]_0,$$

mais pour tout $b = \sum_{\sigma\in G} \beta_\sigma \in \mathbb{Q}[G]^-$, on a $\beta_{\tau\sigma} = -\beta_\sigma$, donc $\sum_{\sigma\in G} \beta_\sigma = 0$ et donc

$$\mathbb{Q}[\mathcal{S}_\infty(K)]^- \subset \mathbb{Q}[\mathcal{S}_\infty(K)]_0.$$

Ainsi,

$$\mathbb{Q}[\mathcal{S}_\infty(K)]_0^- = \mathbb{Q}[\mathcal{S}_\infty(K)]^- = \mathbb{Q}[G](1_G - \tau)w.$$

Comme tout élément de $\overline{\mathcal{U}}_K^- \otimes \mathbb{Q}$ est de la forme $\bar{\gamma} \otimes \frac{1}{c}$, on peut donc noter $\bar{\alpha} \otimes \frac{1}{a}$ l'image de $(1_G - \tau)w$ dans $\overline{\mathcal{U}}_K^- \otimes \mathbb{Q}$. On a alors

$$\overline{\mathcal{U}}_K^- \otimes \mathbb{Q} = \mathbb{Q}[G]^- \left(\bar{\alpha} \otimes \frac{1}{a}\right) = \mathbb{Q}[G]^- (\bar{\alpha} \otimes 1) = \mathbb{Q}[G](\bar{\alpha} \otimes 1)$$

et

$$\mathrm{Ann}_{\mathbb{Q}[G]^-}(\bar{\alpha} \otimes 1) = \mathrm{Ann}_{\mathbb{Q}[G]^-}\left(\bar{\alpha} \otimes \frac{1}{a}\right) = \mathrm{Ann}_{\mathbb{Q}[G]^-}((1_G - \tau)w) = 0.$$

□

Proposition 4.2.4. *Le G-module engendré par $\bar{\alpha}$ est d'indice fini dans $\overline{\mathcal{U}}_K^-$.*
On note $a_{\bar{\alpha}} = \left(\overline{\mathcal{U}}_K^- : \mathbb{Z}[G]\bar{\alpha}\right)$.

Démonstration. Comme $\mathbb{Q}$ est un $\mathbb{Z}$-module plat,

$$\left(\overline{\mathcal{U}}_K^- / \mathbb{Z}[G]\bar{\alpha}\right) \otimes \mathbb{Q} \simeq \left(\overline{\mathcal{U}}_K^- \otimes \mathbb{Q}\right) / \left(\mathbb{Z}[G]\bar{\alpha} \otimes \mathbb{Q}\right) = \mathbb{Q}[G]^- (\alpha \otimes 1) / \mathbb{Q}[G](\alpha \otimes 1) = 0.$$

Donc pour tout $x \in \overline{\mathcal{U}}_K^-$ il existe $n_x \in \mathbb{N}$ tel que $n_x x \in \mathbb{Z}[G]\bar{\alpha}$, et comme $\overline{\mathcal{U}}_K^-$ est un $\mathbb{Z}$-module de type fini, il existe $a_{\bar{\alpha}} \in \mathbb{N}$ tel que pour tout $x \in \overline{\mathcal{U}}_K^-$ on a $a_{\bar{\alpha}} x \in \mathbb{Z}[G]\bar{\alpha}$. □

Nous allons maintenant construire une injection de $\overline{\mathcal{U}}_K^-$ dans $\mathbb{Z}[G]$ en trois temps.

Grâce à la proposition précédente, on peut définir le premier morphisme de G-modules suivant

$$f_1 : \begin{cases} \overline{\mathcal{U}}_K^- \to \mathbb{Z}[G]\bar{\alpha} \\ \bar{x} \mapsto a_{\bar{\alpha}} \bar{x} \end{cases}.$$

Comme $\overline{\mathcal{U}}_K^-$ est sans $\mathbb{Z}$-torsion, ce morphisme est injectif.

On construit ensuite le deuxième morphisme de G-modules

$$f_2 : \begin{cases} \mathbb{Z}[G]\,\bar{\alpha} \to \mathbb{Z}[G]^\sim \\ y\bar{\alpha} \mapsto e^- y \end{cases} .$$

Si $y\bar{\alpha} = 0$, on a alors $e^- y\bar{\alpha} = 0$ et $e^- y(\bar{\alpha} \otimes 1) = 0$, or $e^- y \in \mathbb{Q}[G]^-$ et $\mathrm{Ann}_{\mathbb{Q}[G]^-}(\bar{\alpha} \otimes 1) = 0$ donc $e^- y = 0$ et f_2 est bien défini. De plus, ce morphisme admet $y \mapsto y\bar{\alpha}$ comme réciproque, il s'agit donc d'un isomorphisme de G-modules.

Il ne reste alors plus qu'à injecter $\mathbb{Z}[G]^\sim$ dans $\mathbb{Z}[G]$ grâce à

$$f_3 : \begin{cases} \mathbb{Z}[G]^\sim \to \mathbb{Z}[G] \\ y \mapsto 2y \end{cases} .$$

Le morphisme composé

$$f = f_3 \circ f_2 \circ f_1 : \overline{\mathcal{U}}_K^- \to \mathbb{Z}[G]$$

est alors un morphisme de G-modules injectif.

Notation. Notons $I_{\overline{\mathcal{U}}_K^-} = f\left(\overline{\mathcal{U}}_K^-\right)$ l'idéal de $\mathbb{Z}[G]$.

Proposition 4.2.5. *Le G-module $\overline{\mathcal{U}}_K^-$ est isomorphe à l'idéal $I_{\overline{\mathcal{U}}_K^-}$ de $\mathbb{Z}[G]$.*
Plus précisément, on a

$$n_{\bar{\alpha}}\overline{\mathcal{U}}_K^- = I_{\overline{\mathcal{U}}_K^-}\bar{\alpha},$$

où $n_{\bar{\alpha}} = 2a_{\bar{\alpha}} \in \mathbb{N}$.

Ceci nous permet de démontrer le résultat suivant.

Théorème 4.2.6. *Soit p un nombre premier ne divisant pas* $\mathrm{card}(G)$.
Alors il existe $\beta \in \overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p$ tel que

$$\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p = \mathbb{Z}_p[G]\beta = \mathbb{Z}_p[G]^-\beta \simeq \mathbb{Z}_p[G]^- .$$

Démonstration. D'après la proposition 2.2.26, comme $p \nmid \mathrm{card}(G)$, l'anneau $\mathbb{Z}_p[G]$ est quasi-principal. L'anneau $\mathbb{Z}[G] \otimes \mathbb{Z}_p$ étant isomorphe à l'anneau $\mathbb{Z}_p[G]$, il est lui aussi quasi-principal.
Ainsi $I_{\overline{\mathcal{U}}_K^-} \otimes \mathbb{Z}_p$ est donc un idéal principal de $\mathbb{Z}[G] \otimes \mathbb{Z}_p$ et donc un $\mathbb{Z}_p[G]$-module monogène. Il existe donc $x \in I_{\overline{\mathcal{U}}_K^-} \otimes \mathbb{Z}_p$ tel que

$$I_{\overline{\mathcal{U}}_K^-} \otimes \mathbb{Z}_p = \mathbb{Z}_p[G]\,x.$$

On a donc

$$n_{\bar{\alpha}}\left(\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p\right) = \left(n_{\bar{\alpha}}\overline{\mathcal{U}}_K^-\right) \otimes \mathbb{Z}_p = I_{\overline{\mathcal{U}}_K^-}\bar{\alpha} \otimes \mathbb{Z}_p = \mathbb{Z}_p\left[G\right]\bar{\alpha}x.$$

Notons $\beta \in \overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p$ tel que $\bar{\alpha}x = n_{\bar{\alpha}}\beta$. On a donc

$$n_{\bar{\alpha}}\left(\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p\right) = n_{\bar{\alpha}}\mathbb{Z}_p\left[G\right]\beta.$$

Or $n_{\bar{\alpha}} \in \mathbb{Z}$ et $\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p$ n'a pas de $\mathbb{Z}$-torsion, on en déduit

$$\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p = \mathbb{Z}_p\left[G\right]\beta.$$

Par ailleurs, $\beta \in \overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p$, donc $e^-\beta = \beta$ et

$$\mathbb{Z}_p\left[G\right]\beta = \mathbb{Z}_p\left[G\right]^-\beta.$$

De plus

$$\begin{aligned}\mathbb{Q}_p\left[G\right]^-\beta \simeq \mathbb{Z}_p\left[G\right]^-\beta \otimes \mathbb{Q}_p &= \left(\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p\right) \otimes \mathbb{Q}_p \simeq \overline{\mathcal{U}}_K^- \otimes \mathbb{Q}_p \\ &\simeq \left(\overline{\mathcal{U}}_K^- \otimes \mathbb{Q}\right) \otimes \mathbb{Q}_p \simeq \mathbb{Q}\left[G\right]^- \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p\left[G\right]^-\end{aligned}$$

donc $\mathrm{Ann}_{\mathbb{Z}_p[G]^-}(\beta) \subset \mathrm{Ann}_{\mathbb{Q}_p[G]^-}(\beta) = 0$ et on a bien

$$\mathbb{Z}_p\left[G\right]^-\beta \simeq \mathbb{Z}_p\left[G\right]^-.$$

□

4.2.3 Théorème semi-simple fort

Nous pouvons maintenant démontrer que la conjecture locale forte est vérifiée pour les nombres premiers p ne divisant pas $\mathrm{card}(G)$.

Théorème 4.2.7 (Théorème semi-simple fort)**.** *Soit p un nombre premier ne divisant pas* $\mathrm{card}(G)$.
Alors on a l'isomorphisme de $\mathbb{Z}_p\left[G\right]$-modules suivant

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}\left[G\right]\bar{\varepsilon} \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p\left[G\right]^-/\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(Cl_K^- \otimes \mathbb{Z}_p\right).$$

D'après le théorème 4.2.6, il existe $\beta \in \overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p$ tel que

$$\overline{\mathcal{U}}_K^- \otimes \mathbb{Z}_p = \mathbb{Z}_p\left[G\right]\beta = \mathbb{Z}_p\left[G\right]^-\beta \simeq \mathbb{Z}_p\left[G\right]^-.$$

Comme $\bar{\varepsilon} \in \overline{\mathcal{U}}_K^-$, il existe $\lambda_{\bar{\varepsilon}} \in \mathbb{Z}_p\left[G\right]$ tel que

$$\bar{\varepsilon} \otimes 1 = \lambda_{\bar{\varepsilon}}\beta.$$

Proposition 4.2.8. *On a l'isomorphisme de $\mathbb{Z}_p[G]^-$-modules suivant*

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p \simeq \mathbb{Z}_p[G]^-/\lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]^-. \tag{4.1}$$

Démonstration. Comme $\mathbb{Z}_p$ est un $\mathbb{Z}$-module plat,

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p \simeq \left(\overline{\mathcal{U}}_K^-\otimes\mathbb{Z}_p\right)/\left(\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p\right).$$

Or on a

$$\overline{\mathcal{U}}_K^-\otimes\mathbb{Z}_p = \mathbb{Z}_p[G]^-\beta,$$

et

$$\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p = \mathbb{Z}_p[G](\bar{\varepsilon}\otimes 1) = \lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]\beta = \lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]^-\beta,$$

on a donc

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p \simeq \mathbb{Z}_p[G]^-\beta/\lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]^-\beta.$$

Or $\mathrm{Ann}_{\mathbb{Z}_p[G]^-}(\beta) = 0$, donc on a l'isomorphisme de $\mathbb{Z}_p[G]^-$-modules suivant

$$\mathbb{Z}_p[G]^-\beta/\lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]^-\beta \simeq \mathbb{Z}_p[G]^-/\lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]^-.$$

□

Démonstration du théorème semi-simple fort 4.2.7. D'après le corollaire 1.6.12,

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p\right) = e^-\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p\right)$$

et

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(Cl_K^-\otimes\mathbb{Z}_p\right) = e^-\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right),$$

donc le théorème semi-simple faible 4.2.1 implique

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(Cl_K^-\otimes\mathbb{Z}_p\right) = \mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p\right).$$

On déduit alors de la proposition 4.2.8,

$$\begin{aligned}\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(Cl_K^-\otimes\mathbb{Z}_p\right) &= \mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p\right)\\ &= \mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(\mathbb{Z}_p[G]^-/\lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]^-\right)\\ &= \lambda_{\bar{\varepsilon}}\mathbb{Z}_p[G]^-.\end{aligned}$$

L'isomorphisme de 4.2.8 se réécrit alors

$$\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\bar{\varepsilon}\otimes\mathbb{Z}_p \simeq \mathbb{Z}_p[G]^-/\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(Cl_K^-\otimes\mathbb{Z}_p\right).$$

□

4.3 Principalité simultanée des idéaux de Fitting

Dans cette partie, on démontre le résultat suivant à l'aide des suites de Tate.

Théorème 4.3.1. *Soit p un nombre premier impair.*
Alors les deux affirmations suivantes sont équivalentes

1. $\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)$ *est un idéal principal de* $\mathbb{Z}_p[G]$ *engendré par un élément non diviseur de* 0*,*
2. $\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right)$ *est un idéal principal de* $\mathbb{Z}_p[G]$ *engendré par un élément non diviseur de* 0*.*

Nous établirons d'abord une variante de ce théorème relative aux $\mathcal{S}$-unités et au $\mathcal{S}$-groupe de classes avant de montrer que les deux variantes sont identiques. On ne suppose plus ici que K contient le corps de classes de Hilbert de k.

4.3.1 Suites de Tate

Nous allons maintenant nous intéresser aux suites de Tate, un outil introduit par John Tate dans [Tat66] puis notamment développé par Theodore Chinburg dans [Chi83] pour étudier la structure galoisienne des unités. La version que nous donnons ici correspond au théorème 9 de [Wei96].

Théorème 4.3.2. *Il existe une suite exacte, appelée suite de Tate, de la forme*

$$0 \to \mathcal{U}_{K,\mathcal{S}_K} \to A \to B \to \nabla \to 0,$$

où A est un G-module cohomologiquement trivial, B un G-module projectif, et ∇ un G-module vérifiant les conditions suivantes :

1. *le sous-module* $\mathrm{Tor}_{\mathbb{Z}}(\nabla)$ *de $\mathbb{Z}$ torsion de ∇ est isomorphe à $Cl_{K,\mathcal{S}_K}$,*
2. *en notant* $\nabla = \nabla/\mathrm{Tor}_{\mathbb{Z}}(\nabla)$*, on a la suite exacte suivante*

$$0 \to \overline{\nabla} \to \mathbb{Z}[\mathcal{S}] \to \mathbb{Z} \to 0,$$

où $\mathbb{Z}[\mathcal{S}] \to \mathbb{Z}$ est le morphisme d'augmentation qui à un élément de $\mathbb{Z}[\mathcal{S}]$ associe la somme de ses coefficients. Autrement dit,

$$\nabla/\mathrm{Tor}_{\mathbb{Z}}(\nabla) \simeq \mathbb{Z}[\mathcal{S}]_0$$

en tant que G-modules.

Notation. Pour tout nombre premier p, on note G_p le p-Sylow de G.

Proposition 4.3.3. *Soit p un nombre premier impair.*
Alors pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) \simeq \hat{H}^{i+2}\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right).$$

Démonstration. **Implications du résultat de Weiss pour la partie moins :**
Soit A et B les G-modules fournis par le théorème 4.3.2.
On a les trois suites exactes de G-modules suivantes

1. $0 \to \mathcal{U}_{K,\mathcal{S}_K} \to A \to B \to \nabla \to 0$,
2. $0 \to Cl_{K,\mathcal{S}_K} \to \nabla \to \overline{\nabla} \to 0$,
3. $0 \to \overline{\nabla} \to \mathbb{Z}[\mathcal{S}] \to \mathbb{Z} \to 0$.

Comme $\mathbb{Z}_p$ est un $\mathbb{Z}$-module plat sur lequel G agit trivialement, on obtient l'exactitude des suites de $\mathbb{Z}_p[G]$-modules qui en sont issues

1. $0 \to \mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p \to A \otimes \mathbb{Z}_p \to B \otimes \mathbb{Z}_p \to \nabla \otimes \mathbb{Z}_p \to 0$,
2. $0 \to Cl_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p \to \nabla \otimes \mathbb{Z}_p \to \overline{\nabla} \otimes \mathbb{Z}_p \to 0$,
3. $0 \to \overline{\nabla} \otimes \mathbb{Z}_p \to \mathbb{Z}_p[\mathcal{S}] \to \mathbb{Z}_p \to 0$.

Et d'après la proposition 1.5.11, on obtient enfin l'exactitude des suites de $\mathbb{Z}_p[G]$-modules obtenues par passage à la partie moins (pour la suite à quatre termes, il suffit de la diviser en deux suites exactes courtes via l'image du deuxième morphisme)

1. $0 \to \left(\mathcal{U}_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right)^- \to \left(A \otimes \mathbb{Z}_p\right)^- \to \left(B \otimes \mathbb{Z}_p\right)^- \to \left(\nabla \otimes \mathbb{Z}_p\right)^- \to 0$,
2. $0 \to \left(Cl_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right)^- \to \left(\nabla \otimes \mathbb{Z}_p\right)^- \to \left(\overline{\nabla} \otimes \mathbb{Z}_p\right)^- \to 0$,
3. $0 \to \left(\overline{\nabla} \otimes \mathbb{Z}_p\right)^- \to \mathbb{Z}_p[\mathcal{S}]^- \to \mathbb{Z}_p^- \to 0$.

Or τ agit trivialement sur $\mathbb{Z}_p$, donc $\mathbb{Z}_p^- = 0$ et pour tout G-module M, G agit à gauche sur $M \otimes \mathbb{Z}_p$, donc $\left(M \otimes \mathbb{Z}_p\right)^- = M^- \otimes \mathbb{Z}_p$. Par ailleurs, τ agissant trivialement sur μ_K, on a $\overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \simeq \mathcal{U}^-_{K,\mathcal{S}_K}$ en tant que G-modules. On peut donc réécrire les suites exactes ainsi

1. $0 \to \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p \to A^- \otimes \mathbb{Z}_p \to B^- \otimes \mathbb{Z}_p \to \nabla^- \otimes \mathbb{Z}_p \to 0$,
2. $0 \to Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p \to \nabla^- \otimes \mathbb{Z}_p \to \overline{\nabla}^- \otimes \mathbb{Z}_p \to 0$,
3. $0 \to \overline{\nabla}^- \otimes \mathbb{Z}_p \to \mathbb{Z}_p[\mathcal{S}]^- \to 0$.

Calcul de $\mathbb{Z}_p[\mathcal{S}]^-$:
Par définition

$$\mathbb{Z}_p[\mathcal{S}] = \bigoplus_{v' \in \mathcal{S}} \mathbb{Z}_p[G]\, w',$$

où pour toute place $v' \in \mathcal{S}$, v' est une place de K au-dessus de v'. On a donc

$$\mathbb{Z}_p[\mathcal{S}]^- = \bigoplus_{v' \in \mathcal{S}} \mathbb{Z}_p[G]^-\, w'.$$

– Si $v' \neq v$, alors $\tau w' = w'$. En effet, les places infinies qui ne sont pas au-dessus de v sont ramifiées dans K/K^+ et on a supposé que toutes les places finies dans $\mathcal{S}$ sont soit inertes soit ramifiées dans K/K^+. On a alors

$$\mathbb{Z}_p[G]^- w' = \mathbb{Z}_p[G](1_G - \tau)w' = 0.$$

– Si $v' = v$, v est totalement décomposée dans K/k, donc

$$\mathbb{Z}_p[G]\, w \simeq \mathbb{Z}_p[G]$$

en tant que $\mathbb{Z}_p[G]$-modules et on en déduit l'isomorphisme de $\mathbb{Z}_p[G]$-modules suivant

$$\mathbb{Z}_p[G]^- w \simeq \mathbb{Z}_p[G]^-.$$

Ainsi,

$$\mathbb{Z}_p[\mathcal{S}]^- = \mathbb{Z}_p[G]^- w \simeq \mathbb{Z}_p[G]^-,$$

où w est une place de K au dessus de la place v totalement décomposée dans K/k.

Calculs de cohomologie :

D'après le théorème 4.3.2 et le corollaire 1.2.22 on sait que A et B sont des G-modules cohomologiquement triviaux, et comme G_p est un sous-groupe de G, pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, A\right) = \hat{H}^i\left(G_p, B\right) = 0.$$

On déduit alors de la proposition 1.5.14 que pour tout $i \in \mathbb{Z}$,

$$\hat{H}^i\left(G_p, A^- \otimes \mathbb{Z}_p\right) = \hat{H}^i\left(G_p, B^- \otimes \mathbb{Z}_p\right) = 0.$$

On découpe la première suite exacte en deux suites exactes courtes

$$0 \to \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p \to A^- \otimes \mathbb{Z}_p \to C \to 0$$

et

$$0 \to C \to B^- \otimes \mathbb{Z}_p \to \nabla^- \otimes \mathbb{Z}_p \to 0,$$

dont on déduit l'exactitude des deux suites infinies de cohomologie

$$... \to \hat{H}^i\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) \to 0 \to \hat{H}^i\left(G_p, C\right) \to \hat{H}^{i+1}\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) \to 0...$$

$$... \to \hat{H}^i\left(G_p, C\right) \to 0 \to \hat{H}^i\left(G_p, \nabla^- \otimes \mathbb{Z}_p\right) \to \hat{H}^{i+1}\left(G_p, C\right) \to 0...$$

Donc pour tout $i \in \mathbb{Z}$,

$$\hat{H}^i\left(G_p, C\right) = \hat{H}^{i+1}\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right)$$

et

$$\hat{H}^i\left(G_p, \nabla^- \otimes \mathbb{Z}_p\right) = \hat{H}^{i+1}\left(G_p, C\right).$$

Ainsi, pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, \nabla^- \otimes \mathbb{Z}_p\right) = \hat{H}^{i+2}\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right). \tag{4.2}$$

On a montré dans le paragraphe précédent que $\mathbb{Z}_p\left[\mathcal{S}\right]^- \simeq \mathbb{Z}_p\left[G\right]^-$ en tant que $\mathbb{Z}_p\left[G\right]$-modules, donc en tant que G-modules. Par ailleurs $\mathbb{Z}_p\left[G\right]^-$ est cohomologiquement trivial d'après la proposition 1.5.15 et G_p est un sous-groupe de G, donc pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, \mathbb{Z}_p\left[\mathcal{S}\right]^-\right) = \hat{H}^i\left(G_p, \mathbb{Z}_p\left[G\right]^-\right) = 0.$$

À l'aide de la troisième suite exacte, on obtient donc pour tout $i \in \mathbb{Z}$

$$\hat{H}^i\left(G_p, \overline{\nabla}^- \otimes \mathbb{Z}_p\right) = 0$$

La deuxième suite exacte fournit donc la suite exacte de cohomologie suivante

$$... \to 0 \to \hat{H}^i\left(G_p, Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) \to \hat{H}^i\left(G_p, \nabla^- \otimes \mathbb{Z}_p\right) \to 0 \to ...$$

Ainsi, pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) = \hat{H}^i\left(G_p, \nabla^- \otimes \mathbb{Z}_p\right). \tag{4.3}$$

Ainsi, en combinant les équations (4.2) et (4.3), on obtient finalement, pour tout $i \in \mathbb{Z}$,

$$\hat{H}^i\left(G_p, Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) = \hat{H}^{i+2}\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right).$$

□

4.3.2 Cohomologie d'un quotient du groupe des $\mathcal{S}$-unités

La connaissance de la cohomologie du groupe infini des $\mathcal{S}$-unités nous renseigne sur la cohomologie de certains quotients finis de ce même groupe.

Proposition 4.3.4. *Soit p un nombre premier impair, F un sous-groupe de G et $\bar{\alpha} \in \overline{\mathcal{U}}^-_{K,\mathcal{S}_K}$ tel que $\mathbb{Z}_p\left[G\right]^-\left(\bar{\alpha} \otimes 1\right) \simeq \mathbb{Z}_p\left[G\right]^-$ en tant que $\mathbb{Z}_p\left[G\right]$-modules.*
Alors, pour $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(F, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) = \hat{H}^i\left(F, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K}/\mathbb{Z}\left[G\right]^{\sim} \bar{\alpha} \otimes \mathbb{Z}_p\right).$$

Démonstration. On a la suite exacte de G-modules suivante

$$0 \to \mathbb{Z}_p[G]^-(\bar{\alpha}\otimes 1) \to \overline{\mathcal{U}}^-_{K,S_K}\otimes\mathbb{Z}_p \to \overline{\mathcal{U}}^-_{K,S_K}/\mathbb{Z}[G]^\sim\,\bar{\alpha}\otimes\mathbb{Z}_p \to 0.$$

Comme F est un sous-groupe de G, en déduit la suite infinie exacte de cohomologie

$$\begin{aligned}... \to \hat{H}^i\left(F,\mathbb{Z}_p[G]^-(\bar{\alpha}\otimes 1)\right) &\to \hat{H}^i\left(F,\overline{\mathcal{U}}^-_{K,S_K}\otimes\mathbb{Z}_p\right)\to\\ &\hat{H}^i\left(F,\overline{\mathcal{U}}^-_{K,S_K}/\mathbb{Z}[G]^\sim\,\bar{\alpha}\otimes\mathbb{Z}_p\right)\to \hat{H}^{i+1}\left(F,\mathbb{Z}_p[G]^-(\bar{\alpha}\otimes 1)\right)\to ...\end{aligned}$$

On a supposé $\mathbb{Z}_p[G]^-(\bar{\alpha}\otimes 1)\simeq\mathbb{Z}_p[G]^-$ en tant que $\mathbb{Z}_p[G]$-modules, donc en tant que G-modules. D'après la proposition 1.5.15 $\mathbb{Z}_p[G]^-(\bar{\alpha}\otimes 1)$ est donc un G-module cohomologiquement trivial et donc pour tout $i\in\mathbb{Z}$,

$$\hat{H}^i\left(F,\mathbb{Z}_p[G]^-(\bar{\alpha}\otimes 1)\right)=0.$$

On en déduit que pour tout $i\in\mathbb{Z}$

$$\hat{H}^i\left(F,\overline{\mathcal{U}}^-_{K,S_K}\otimes\mathbb{Z}_p\right)\simeq\hat{H}^i\left(F,\overline{\mathcal{U}}^-_{K,S_K}/\mathbb{Z}[G]^\sim\,\bar{\alpha}\otimes\mathbb{Z}_p\right).$$

□

4.3.3 Idéaux de Fitting

Soit p un nombre premier impair. On rappelle que G_p désigne le p-Sylow de G. Notons Δ_p un supplémentaire de G_p dans G. Le résultat de cette section découle de la proposition 4 de [CG98] reproduite ci-dessous.

Proposition 4.3.5. *Soit χ un caractère p-adique de Δ_p irréductible sur $\overline{\mathbb{Q}}_p$ et M un $\mathbb{Z}_p[\chi][G_p]$-module fini.*
Les affirmations suivantes sont équivalentes
– *$\hat{H}^i(G_p,M)=0$ pour tout $i\in\mathbb{Z}$,*
– *il existe $l\in\mathbb{N}$ tel que la suite*

$$0\to\mathbb{Z}_p[\chi][G_p]^l\to\mathbb{Z}_p[\chi][G_p]^l\to M\to 0$$

est une suite exacte de $\mathbb{Z}_p[\chi][G_p]$-modules,
– *$\mathrm{Fitt}_{\mathbb{Z}_p[\chi][G_p]}(M)$ est un idéal principal de $\mathbb{Z}_p[\chi][G_p]$ engendré par un élément non diviseur de 0.*

Proposition 4.3.6. *Soit M un $\mathbb{Z}_p[G]$-module fini.*
Les affirmations suivantes sont équivalentes
– *$\hat{H}^i(G_p,M^-)=0$ pour tout $i\in\mathbb{Z}$,*

– $\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}(M^-)$ *est un idéal principal de* $\mathbb{Z}_p[G]^-$ *engendré par un élément non diviseur de* 0.

Démonstration. Comme $p \nmid \mathrm{card}(\Delta_p)$, en notant $Y^-_{\mathrm{irr},\mathbb{Q}_p}$ l'ensemble des caractères $\mathbb{Q}_p$-irréductibles impairs de Δ_p, d'après la proposition 2.2.32 on a

$$M^- = \bigoplus_{\psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}} e_\psi M,$$

donc, d'après la proposition 1.2.18, pour tout $i \in \mathbb{Z}$,

$$\hat{H}^i\left(G_p, M^-\right) = \bigoplus_{\psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}} \hat{H}^i\left(G_p, e_\psi M\right).$$

Ainsi, pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, M^-\right) = 0$$

si et seulement si

$$\hat{H}^i\left(G_p, e_\psi M\right) = 0 \ \text{ pour tout } \psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}.$$

Pour tout $\psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}$, il existe un caractère $\overline{\mathbb{Q}}_p$-irréductible χ_ψ de Δ_p tel que $\psi = \psi_{\chi_\psi}$ et donc $e_\psi M \simeq M_{\chi_\psi}$ est un $\mathbb{Z}_p[\chi_\psi][\Delta_p]$-module χ_ψ-isotypique. Et comme $e_\psi M$ est un sous-$\mathbb{Z}_p[G]$-module de M, on en déduit que c'est un $\mathbb{Z}_p[\chi_\psi][G_p]$-module fini auquel on peut appliquer la proposition précédente.
Ainsi, on a

$$\hat{H}^i\left(G_p, M^-\right) = 0 \ \text{ pour tout } i \in \mathbb{Z}$$

si et seulement si

$$\begin{gathered}\mathrm{Fitt}_{\mathbb{Z}_p[\chi_\psi][G_p]}(e_\psi M) \ \text{ est un idéal principal de } \ \mathbb{Z}_p[\chi_\psi][G_p] \\ \text{engendré par un élément non diviseur de 0 pour tout } \psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}.\end{gathered}$$

Par ailleurs, d'après la démonstration de 2.2.24, pour tout $\psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}$ on a l'isomorphisme d'anneaux

$$\mathbb{Z}_p[\chi_\psi] \simeq e_\psi \mathbb{Z}_p[\Delta_p],$$

dont on déduit l'isomorphisme d'anneaux

$$\mathbb{Z}_p[\chi_\psi][G_p] \simeq e_\psi \mathbb{Z}_p[\Delta_p][G_p] = e_\psi \mathbb{Z}_p[G].$$

On a également l'isomorphisme de $\mathbb{Z}_p[\chi_\psi][G_p]$-modules

$$e_\psi M \simeq e_\psi M \underset{\mathbb{Z}_p[G]}{\otimes} \mathbb{Z}_p[G] = M \underset{\mathbb{Z}_p[G]}{\otimes} e_\psi \mathbb{Z}_p[G],$$

donc

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi_\psi][G_p]}(e_\psi M) = \mathrm{Fitt}_{\mathbb{Z}_p[\chi_\psi][G_p]}\left(M \underset{\mathbb{Z}_p[G]}{\otimes} e_\psi \mathbb{Z}_p\,[G]\right).$$

Ainsi l'isomorphisme d'anneaux $\mathbb{Z}_p[\chi_\psi][G_p] \simeq e_\psi \mathbb{Z}_p\,[G]$ envoie l'idéal $\mathrm{Fitt}_{\mathbb{Z}_p[\chi_\psi][G_p]}(e_\psi M)$ sur l'idéal $\mathrm{Fitt}_{e_\psi \mathbb{Z}_p[G]}\left(M \underset{\mathbb{Z}_p[G]}{\otimes} e_\psi \mathbb{Z}_p\,[G]\right)$. Or $e_\psi \mathbb{Z}_p\,[G]$ est une $\mathbb{Z}_p\,[G]$-algèbre associative, donc d'après la proposition 1.6.10, on a

$$\mathrm{Fitt}_{e_\psi \mathbb{Z}_p[G]}\left(M \underset{\mathbb{Z}_p[G]}{\otimes} e_\psi \mathbb{Z}_p\,[G]\right) = e_\psi \mathbb{Z}_p\,[G]\,\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = e_\psi \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M).$$

Ainsi, on pour tout $\psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}$ on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[\chi_\psi][G_p]}(e_\psi M) \text{ est un idéal principal de } \mathbb{Z}_p[\chi_\psi][G_p] \text{ engendré par un élément non diviseur de 0}$$

si et seulement si

$$e_\psi \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) \text{ est un idéal principal de } e_\psi \mathbb{Z}_p\,[G] \text{ engendré par un élément non diviseur de 0.}$$

Or d'après le corollaire 1.6.12 et la proposition 2.2.32, on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}(M^-) = e^- \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) = \bigoplus_{\psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}} e_\psi \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M).$$

Et comme les e_ψ sont orthogonaux, on a

$$e_\psi \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M) \text{ est un idéal principal de } e_\psi \mathbb{Z}_p\,[G] \text{ engendré par un élément non diviseur de 0 pour tout } \psi \in Y^-_{\mathrm{irr},\mathbb{Q}_p}$$

si et seulement si

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}(M^-) \text{ est un idéal principal de } \mathbb{Z}_p\,[G]^- \text{ engendré par un élément non diviseur de 0}$$

ce qui achève la démonstration. □

4.3.4 Théorème de simultanée principalité des idéaux de Fitting

Pour tout nombre premier p, on note toujours G_p le p-Sylow de G. On note $\bar{\varepsilon}_{\mathcal{S}}$ l'image de l'unité de Stark ε dans $\overline{\mathcal{U}}^-_{K,\mathcal{S}_K}$. On a alors le résultat suivant.

Théorème 4.3.7. *Soit p un nombre premier impair.*
Alors, ces deux affirmations sont équivalentes

1. $\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(\overline{\mathcal{U}}^-_{K,\mathcal{S}_K}/\mathbb{Z}[G]^\sim \bar{\varepsilon}_{\mathcal{S}} \otimes \mathbb{Z}_p\right)$ *est un idéal principal de $\mathbb{Z}_p[G]^-$ engendré par un élément non diviseur de* 0*,*
2. $\mathrm{Fitt}_{\mathbb{Z}_p[G]^-}\left(Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right)$ *est un idéal principal de $\mathbb{Z}_p[G]^-$ engendré par un élément non diviseur de* 0*.*

Démonstration. D'après la proposition 4.3.3, pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) = \hat{H}^{i+2}\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right).$$

D'après la formule d'indice 3.3.25, $\mathbb{Z}[G]\bar{\varepsilon}$ est d'indice fini dans $\overline{\mathcal{U}}^-_K$, donc pour tout $p \neq 2$, on a $\mathrm{Ann}_{\mathbb{Z}_p[G]^-(\bar{\varepsilon}\otimes 1)} = 0$, donc $\mathbb{Z}_p[G]^-(\bar{\alpha}\otimes 1) \simeq \mathbb{Z}_p[G]^-$ en tant que $\mathbb{Z}_p[G]$-modules. Grâce à la proposition 4.3.4, on en déduit que pour tout $i \in \mathbb{Z}$, on a

$$\hat{H}^i\left(G_p, Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) = \hat{H}^{i+2}\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K}/\mathbb{Z}[G]^\sim \bar{\varepsilon}_{\mathcal{S}} \otimes \mathbb{Z}_p\right).$$

En particulier,

$$\hat{H}^i\left(G_p, Cl_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p\right) = 0 \text{ pour tout } i \in \mathbb{N}$$

si et seulement si

$$\hat{H}^i\left(G_p, \overline{\mathcal{U}}^-_{K,\mathcal{S}_K}/\mathbb{Z}[G]^\sim \bar{\varepsilon}_{\mathcal{S}} \otimes \mathbb{Z}_p\right) = 0 \text{ pour tout } i \in \mathbb{Z}.$$

Et comme les $\mathbb{Z}_p[G]$-modules $Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p$ et $\overline{\mathcal{U}}^-_{K,\mathcal{S}_K}/\mathbb{Z}[G]^\sim \bar{\varepsilon}_{\mathcal{S}} \otimes \mathbb{Z}_p$ sont finis, on peut leur appliquer la proposition 4.3.6 pour conclure. □

Pour en déduire le théorème 4.3.1 énoncé en début de section nous allons recourir à la proposition ci-dessous.

Proposition 4.3.8. *On a*

$$\overline{\mathcal{U}}^-_{K,\mathcal{S}_K} = \overline{\mathcal{U}}^-_K$$

et pour tout nombre premier impair p on a

$$Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p \simeq Cl^-_K \otimes \mathbb{Z}_p$$

en tant que $\mathbb{Z}_p[G]$-modules.

Ceci implique en particulier $\bar{\varepsilon}_{\mathcal{S}} = \bar{\varepsilon}$.

Démonstration. – Comme les idéaux premier dans $\mathcal{S}$ sont inertes ou ramifiés dans K/K^+, tout idéal premier $\mathcal{P}$ dans $\mathcal{S}_K$ vérifie $\tau(\mathcal{P}) = \mathcal{P}$. Soit $x \in \mathcal{U}_{K,\mathcal{S}_K}$ tel que $\bar{x} \in \overline{\mathcal{U}}_{K,\mathcal{S}_K}$. Pour tout $\mathcal{P} \in \mathcal{S}_K \setminus \mathcal{S}_\infty(K)$, on a

$$|\tau(x)|_{\mathcal{P}} = |x|_{\tau(\mathcal{P})} = |x|_{\mathcal{P}}\,.$$

Or $(1_G + \tau)x \in \mu_K = \{\pm 1\}$, donc

$$|x|^2_{\mathcal{P}} = |\tau(x)|_{\mathcal{P}}\,|x|_{\mathcal{P}} = 1.$$

On en déduit que pour tout $\mathcal{P} \in \mathcal{S}_K \setminus \mathcal{S}_\infty(K)$, $|x|_{\mathcal{P}} = 1$, donc $\bar{x} \in \overline{\mathcal{U}}^-_K$.
On a donc bien

$$\overline{\mathcal{U}}^-_{K,\mathcal{S}_K} = \overline{\mathcal{U}}^-_K.$$

– Considérons le morphisme de G-modules

$$f : Cl_K \to Cl_{K,\mathcal{S}_K}.$$

C'est un morphisme surjectif de noyau $\langle\overline{\mathcal{P}}\rangle_{\mathcal{P}\in\mathcal{S}_K\setminus\mathcal{S}_\infty(K)}$, où $\overline{\mathcal{P}}$ désigne la classe de $\mathcal{P}$ dans Cl_K. Comme f et τ commutent, il induit un morphisme de G-modules surjectif de G-modules

$$f^- : Cl^-_K \to Cl^-_{K,\mathcal{S}_K}$$

dont le noyau vaut $\langle\overline{\mathcal{P}}\rangle^-_{\mathcal{P}\in\mathcal{S}_K\setminus\mathcal{S}_\infty(K)}$.
Comme $\mathbb{Z}_p$ est un $\mathbb{Z}$-module plat, on obtient alors le morphisme surjectif de $\mathbb{Z}_p\,[G]$-modules

$$f^-_p : Cl^-_K \otimes \mathbb{Z}_p \to Cl^-_{K,\mathcal{S}_K} \otimes \mathbb{Z}_p,$$

dont le noyau vaut $\langle\overline{\mathcal{P}}\rangle^-_{\mathcal{P}\in\mathcal{S}_K\setminus\mathcal{S}_\infty(K)} \otimes \mathbb{Z}_p = (1_G - \tau)\langle\overline{\mathcal{P}}\rangle_{\mathcal{P}\in\mathcal{S}_K\setminus\mathcal{S}_\infty(K)} \otimes \mathbb{Z}_p$ comme $p \neq 2$.
Soit $\mathcal{P} \in \mathcal{S}_K \setminus \mathcal{S}_\infty(K)$. Comme $\mathcal{P}$ est soit inerte soit ramifié dans K/K^+, on a $\tau\mathcal{P} = \mathcal{P}$ et $(1_G - \tau)\mathcal{P} = \mathcal{O}_K$.
Ainsi, $(1_G - \tau)\langle\overline{\mathcal{P}}\rangle_{\mathcal{P}\in\mathcal{S}_{ram}(K/k)} \otimes \mathbb{Z}_p = 0$ et f^-_p est un isomorphisme.

□

Nous allons donc pouvoir démontrer le résultat souhaité.

Théorème (4.3.1)**.** *Soit p un nombre premier impair.*
Alors les deux affirmations suivantes sont équivalentes

1. $\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}^-_K/\mathbb{Z}\,[G]\,\bar{\varepsilon} \otimes \mathbb{Z}_p\right)$ *est un idéal principal de* $\mathbb{Z}_p\,[G]$ *engendré par un élément non diviseur de* 0*,*
2. $\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl^-_K \otimes \mathbb{Z}_p\right)$ *est un idéal principal de* $\mathbb{Z}_p\,[G]$ *engendré par un élément non diviseur de* 0*.*

Démonstration. D'après la proposition précédente, pour tout p premier impair, on a

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)=\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(\overline{\mathcal{U}}_{K,\mathcal{S}_K}^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}_p\right)$$

et

$$\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_K^-\otimes\mathbb{Z}_p\right)=\mathrm{Fitt}_{\mathbb{Z}_p[G]}\left(Cl_{K,\mathcal{S}_K}^-\otimes\mathbb{Z}_p\right).$$

Et comme $\bar{\varepsilon}=\bar{\varepsilon}_{\mathcal{S}}$, le théorème 4.3.7 fournit directement le résultat souhaité. □

Chapitre 5

Exemples de vérification algorithmique de la conjecture faible

5.1 Représentation algorithmique des objets algébriques

Pour représenter algorithmiquement les objets algébriques dont nous avons besoin, nous avons utilisé les représentations algorithmiques des groupes abéliens présentées par Henri Cohen dans [Coh93] et implémentées dans PARI/GP [The18]. Nous avons également pris en compte la structure de modules galoisiens des modules considérés pour pouvoir calculer leurs idéaux de Fitting.

5.1.1 Représentation algorithmique des groupes abéliens de type fini

Dans ce paragraphe, G désigne un groupe abélien (noté multiplicativement) de type fini, ayant r générateurs. Algorithmiquement, un groupe abélien de type fini peut être représenté par un système de générateurs, et une matrice qui indique les relations algébriques entre ses générateurs.
On note $\mathrm{Gen}_{\mathbb{Z}}(G) = (gen_1, ..., gen_r)$ un ensemble de générateurs de G :

$$\forall g \in G,\ \exists X = (x_i) \in \mathcal{M}_{r,1}(\mathbb{Z}) \text{ tel que } g = \mathrm{Gen}_{\mathbb{Z}}(G)X = \prod_{i=1}^{r} gen_i^{x_i}.$$

On note $\mathrm{Rel}_{\mathbb{Z}}(G) \in \mathcal{M}_{r,r}(\mathbb{Z})$ sa matrice de relations sur $\mathbb{Z}$:

$$\forall X \in \mathcal{M}_{r,1}(\mathbb{Z}), \mathrm{Gen}_{\mathbb{Z}}(G)X = 1_G \text{ si et seulement si}$$
$$\exists Y \in \mathcal{M}_{r,1}(\mathbb{Z}) \text{ tel que } X = \mathrm{Rel}_{\mathbb{Z}}(G)Y.$$

5.1.2 Représentation algorithmique des groupes abéliens finis

Dorénavant, G est un groupe abélien (toujours multiplicatif) fini à t éléments. On lui associe toujours un système de générateurs et relations $(\mathrm{Gen}_{\mathbb{Z}}(G), \mathrm{Rel}_{\mathbb{Z}}(G))$, mais on peut également le représenter par la liste exhaustive de ses éléments que l'on donne par leur coefficients sur les générateurs du groupe. Plutôt que de stocker la loi de G en établissant sa table de Cayley globale, on peut se contenter de représenter la multiplication de chacun de ses générateurs par une matrice de permutation des éléments de G.
On note $\mathcal{G}$ le vecteur ligne constitué de ses éléments :

$$\mathcal{G} = (g_1, ..., g_t).$$

On note $\mathrm{Elt}_{\mathbb{Z}}(G)$ la liste des t vecteurs de longueur r des coefficients des éléments de G sur les générateurs $\mathrm{Gen}_{\mathbb{Z}}(G)$:

$$\mathrm{Elt}_{\mathbb{Z}}(G) = (X_1, ..., X_t) \in \mathcal{M}_{r,1}(\mathbb{Z})^t$$
$$\text{où } \forall i \in [\![1; t]\!],\ X_i \in \mathcal{M}_{r,1}(\mathbb{Z}) \text{ vérifie } g_i = \mathrm{Gen}_{\mathbb{Z}}(G) X_i.$$

Pour chaque générateur gen de G, la multiplication par gen fournit une matrice de permutation de $\mathrm{Elt}_{\mathbb{Z}}(G)$. On note $\mathrm{Multgen}(G)$ le vecteur constitué de ces matrices :

$$\mathrm{Multgen}(G) = (M_1, ..., M_r) \in \mathrm{GL}_t(\mathbb{Z})^r$$
$$\text{où } \forall k \in [\![1; r]\!],\ M_k = \left(m_{i,j}^{(k)}\right) \in \mathrm{GL}_t(\mathbb{Z}) \text{ est la matrice de permutation vérifiant}$$
$$m_{i,j}^{(k)} = 1 \text{ si et seulement si } g_i = g_j\, gen_k.$$

Les générateurs de G sont donc les vecteurs de $\mathrm{Elt}_{\mathbb{Z}}(G)$ dont une coordonnée vaut 1 et les autres 0. On garde en mémoire leurs positions dans $\mathrm{Elt}_{\mathbb{Z}}(G)$ au sein d'une liste $\mathrm{Index}_{\mathbb{Z}}(G)$:

$$\mathrm{Index}_{\mathbb{Z}}(G) = (n_1, ..., n_r) \in \mathbb{Z}^r$$
$$\text{où } \forall k \in [\![1; r]\!], n_k \in \mathbb{Z} \text{ vérifie } gen_k = g_{n_k}.$$

5.1.3 Représentation algorithmique des G-modules

On considère maintenant un G-module de type fini M. Ce G-module est aussi de type fini sur $\mathbb{Z}$, on lui associe un système de générateurs (dont on note s le cardinal) et relations sur $\mathbb{Z}$:

$$(\mathrm{Gen}_{\mathbb{Z}}(M), \mathrm{Rel}_{\mathbb{Z}}(M)).$$

Pour tout générateur m_k de M et tout générateur gen_l de G, on note $B_{k,l} \in \mathcal{M}_{s,1}(\mathbb{Z})$ l'action de gen_l sur m_k :

$$gen_l.m_k = \mathrm{Gen}_{\mathbb{Z}}(M) B_{l,k}.$$

On note $B_l \in \mathcal{M}_{s,s}(\mathbb{Z})$ la matrice dont la k-ième colonne est $B_{l,k}$, le vecteur de l'action de gen_l sur m_k. Cette matrice encode l'action de gen_l sur M :

$$\forall m = \mathrm{Gen}_{\mathbb{Z}}(M)Y_m \in M, \text{ on a } gen_l.m = \mathrm{Gen}_{\mathbb{Z}}(M)B_lY_m.$$

À partir de ces matrices, on peut retrouver l'action de tous les éléments de G sur M :

$$\forall m = \mathrm{Gen}_{\mathbb{Z}}(M)Y_m \in M, \forall g_i = \mathrm{Gen}_{\mathbb{Z}}(G)X_i = \mathrm{Gen}_{\mathbb{Z}}(G)\begin{pmatrix} x_1^{(i)} \\ ... \\ x_r^{(i)} \end{pmatrix} \in G,$$
$$\text{on a } g_i.m = \mathrm{Gen}_{\mathbb{Z}}(M)B_1^{x_1^{(i)}}...B_r^{x_r^{(i)}}Y_m.$$

Pour tout $i \in [\![1, t]\!]$, on note $\mathrm{Act}_i = B_1^{x_1^{(i)}}...B_r^{x_r^{(i)}}$ l'action galoisienne de $g_i \in G$ sur M :

$$\forall m = \mathrm{Gen}_{\mathbb{Z}}(M)Y_m \in M, \text{ on a } g_i.\mathrm{Gen}_{\mathbb{Z}}(M)Y_m = g_i.m = \mathrm{Gen}_{\mathbb{Z}}(M)\mathrm{Act}_iY_m.$$

5.1.4 Idéaux de Fitting

Les éléments du vecteur $\mathrm{Gen}_{\mathbb{Z}}(M) = (m_1, ..., m_s)$ étant des générateurs de M sur $\mathbb{Z}$, ce sont également des générateurs de M sur $\mathbb{Z}[G]$. Le morphisme de G-modules $\varphi : \mathbb{Z}[G]^s \to M$ défini par $\varphi(a_1, ..., a_s) = a_1m_1 + ... + a_sm_s$ est donc surjectif.
Pour tout $k \in [\![1, s]\!]$, on note $\mathrm{Act}'_k \in \mathcal{M}_{s,t}(\mathbb{Z})$ la matrice dont la j-ième colonne est la k-ième colonne de Act_j. Cette matrice représente l'action galoisienne des éléments de G sur m_k :

$$\forall a = \alpha_1g_1 + ... + \alpha_tg_t = \mathcal{G}A \in \mathbb{Z}[G]$$
$$\text{on a } \mathcal{G}A.m_k = a.m_k = \alpha_1g_1.m_k + ... + \alpha_tg_t.m_k = \mathrm{Gen}_{\mathbb{Z}}(M)\mathrm{Act}'_kA.$$

Soit $(a_1, ..., a_s) \in \mathbb{Z}[G]^s$, pour tout $l \in [\![1, s]\!]$, on note $A_i \in \mathcal{M}_{t,1}(\mathbb{Z})$ le vecteur colonne tel que $a_i = \mathcal{G}A_i$.
On a alors $\varphi(a_1, ..., a_s) = M\mathrm{Act}'_1A_1 + ... + M\mathrm{Act}'_sA_s = M\left(\mathrm{Act}'_1A_1 + ... + \mathrm{Act}'_sA_s\right)$.
Ainsi,

$$(a_1, ..., a_s) \in \mathrm{Ker}(\varphi) \text{ si et seulement si } \left(\mathrm{Act}'_1A_1 + ... + \mathrm{Act}'_sA_s\right) \in \mathrm{Rel}_{\mathbb{Z}}(M)\mathcal{M}_{s,1}(\mathbb{Z}).$$

On est donc en mesure de déterminer algorithmiquement une famille $\left\{v_1, ..., v_q\right\}$ génératrice sur $\mathbb{Z}$ du noyau du morphisme surjectif de G-modules $\varphi : \mathbb{Z}[G]^s \to M$.
Le déterminant sur $\mathbb{Z}[G]$ étant $\mathbb{Z}$-linéaire, l'idéal de Fitting $\mathrm{Fitt}_{\mathbb{Z}[G]}(M)$ est engendré sur $\mathbb{Z}$ par les $\det(v_{\alpha_1}, ..., v_{\alpha_s})$, où $(\alpha_i)_i$ parcourt les $\binom{s}{q}$ suites strictement croissantes de $[\![1; s]\!]$ dans $[\![1; q]\!]$. On peut ainsi obtenir sa structure de sous-groupe de $\mathbb{Z}[G]$.

5.2 Construction d'une base d'extensions satisfaisant les conditions souhaitées

5.2.1 Extensions souhaitées

Soit k un corps de nombres totalement réel et K/k une extension galoisienne abélienne. On note K^+ le sous-corps totalement réel maximal de K. On souhaite que les conditions suivantes soient satisfaites :

1. K^+ est d'indice 2 dans K, on note τ l'élément non trivial de $\mathrm{Gal}(K/K^+)$,
2. pour tout idéal premier $\mathfrak{p}$ de O_k ramifié dans K/k, les idéaux de O_{K^+} au-dessus de $\mathfrak{p}$ sont soit inertes soit ramifiés dans K/K^+,
3. il existe une place infinie v de k qui reste réelle dans K, toutes les autres deviennent complexes.

On note $\mathcal{S}_\infty(k)$ l'ensemble des places infinies de k et $\mathcal{S}_{ram}(K/k)$ l'ensemble des idéaux premiers de k qui sont ramifiés dans K/k.

5.2.2 Un peu de théorie du corps de classes

Cette section présente des résultats de théorie du corps de classes global utiles à la construction algorithmique d'extensions ayant les propriétés souhaitées. Pour plus de détail, on pourra consulter les chapitres 3 et 4 de [Coh00]. Le chapitre 3, dont la présente section est fortement inspirée, présente les résultats théoriques et le chapitre 4 présente des algorithmes explicites.

Soit k un corps de nombres.

Définition 5.2.1. *Un cycle arithmétique de k (aussi appelé cycle, modulus ou encore diviseur) est un couple* $(\mathfrak{M}_0, \mathfrak{M}_\infty)$*, où* $\mathfrak{M}_0$ *est un idéal entier de k et* $\mathfrak{M}_\infty = \prod_{v \in \mathcal{S}} v$ *est un produit formel de plongements réels de k.*
On écrit formellement $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$.

Définition 5.2.2. *Soit* $\mathfrak{M} = \mathfrak{M}_0 \prod_{v \in \mathcal{S}_\mathfrak{M}} v$ *et* $\mathfrak{N} = \mathfrak{N}_0 \prod_{v \in \mathcal{S}_\mathfrak{N}} v$ *deux cycles arithmétiques de k.*
On dit que $\mathfrak{M}$ *divise* $\mathfrak{N}$ *si* $\mathfrak{M}_0 \mid \mathfrak{N}_0$ *et* $\mathcal{S}_\mathfrak{M} \subset \mathcal{S}_\mathfrak{N}$.

À tout cycle arithmétique, on peut associer un analogue du groupe de classes appelé groupe de classes de rayon. Nous allons donc définir ce qui joue le rôle des idéaux fractionnaires et des idéaux fractionnaires principaux dans cet analogue.

Définition 5.2.3. *Soit $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$ un cycle arithmétique de k, $\mathfrak{a}$ un idéal fractionnaire de k et $\alpha \in k^*$.*
On dit que $\mathfrak{a}$ est premier à $\mathfrak{M}$ si $\mathfrak{a}$ est un quotient de deux idéaux entiers premiers à $\mathfrak{M}_0$.
On note $I_k(\mathfrak{M})$ l'ensemble des idéaux fractionnaires de k premiers à $\mathfrak{M}$.
On dit que α est premier à $\mathfrak{M}$ si l'idéal fractionnaire αO_k l'est.

La notion de primalité à un module ne dépend donc pas de sa partie infinie.

Définition 5.2.4. *Soit $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$ un cycle arithmétique de k et $\alpha \in k^*$. On note $\mathfrak{M}_0 = \prod_{\mathfrak{p}\in\mathcal{S}_0} \mathfrak{p}^{a_\mathfrak{p}}$ et $\mathfrak{M}_\infty = \prod_{v\in\mathcal{S}_\mathfrak{M}} v$.*
On écrit

$$\alpha \equiv 1 \pmod^* \mathfrak{M}$$

si $\upsilon_\mathfrak{p}(\alpha - 1) \geq a_\mathfrak{p}$ pour tout $\mathfrak{p} \in \mathcal{S}_0$ et $v(\alpha) > 0$ pour tout $v \in \mathcal{S}_\mathfrak{M}$.
On note $k^*_\mathfrak{M}$ l'ensemble des tels $\alpha \in k^*$ et $P_k(\mathfrak{M})$ l'ensemble des idéaux fractionnaires principaux de k engendrés par des $\alpha \in k^*_\mathfrak{M}$. On appelle $P_k(\mathfrak{M})$ le groupe de rayon de $\mathfrak{M}$.

Si $\alpha \in O_k^*$ et $\mathfrak{M} = \mathfrak{M}_0$, $\alpha \equiv 1 \pmod^* \mathfrak{M})$ est équivalent à $\alpha \equiv 1 \pmod{\mathfrak{M}_0}$.

Comme $P_k(\mathfrak{M})$ est un sous-groupe de $I_k(\mathfrak{M})$, on peut poser la définition suivante.

Définition 5.2.5. *Soit $\mathfrak{M}$ un cycle arithmétique de k.*
On définit le groupe de classes de rayons de $\mathfrak{M}$ et on note $Cl_K(\mathfrak{M})$ le quotient de $I_k(\mathfrak{M})$ par $P_k(\mathfrak{M})$.

Pour le cycle trivial $\mathfrak{M} = 1$ de k, on retrouve le groupe de classes usuels : $Cl_K(1) = Cl_K$.

Définition 5.2.6. *Soit $\mathfrak{M}$ un cycle arithmétique de k.*
Un sous-groupe de congruence de niveau $\mathfrak{M}$ est un groupe d'idéaux fractionnaires C de k tel que :

$$P_k(\mathfrak{M}) \subset C \subset I_k(\mathfrak{M}).$$

Pour expliciter le niveau $\mathfrak{M}$ du sous-groupe de congruence, on utilise la notation $(C, \mathfrak{M})$.

Soit K/k une extension abélienne de corps de nombres.

On rappelle que pour tout idéal premier $\mathfrak{p}$ de k non ramifié dans K/k, on note $\sigma_\mathfrak{p} \in \mathcal{D}_\mathfrak{p} \subset \mathrm{Gal}(K/k)$ le Frobenius de $\mathfrak{p}$. L'application d'Artin est la généralisation de la notion de Frobenius à tous les idéaux fractionnaires de k dont la décomposition en idéaux premiers ne contient que des premiers non ramifiés.

Définition 5.2.7 (Application de réciprocité d'Artin)**.** *Soit $\mathfrak{M}$ un cycle de k divisible par toutes les places ramifiées dans K/k.*
Pour tout $\mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \in I_k(\mathfrak{M})$, on pose

$$\mathrm{Art}_{K/k,\mathfrak{M}}(\mathfrak{a}) = \prod_{\mathfrak{p}|\mathfrak{a}} \sigma_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}.$$

On appelle application de réciprocité d'Artin le morphisme de groupes

$$\mathrm{Art}_{K/k,\mathfrak{M}} : I_k(\mathfrak{M}) \to \mathrm{Gal}(K/k).$$

Le théorème suivant énonce des résultats centraux dans la théorie du corps de classes global. On pourra par exemple se référer au chapitre 10 de [Lan94] pour une démonstration de ces résultats.

Théorème 5.2.8 (Réciprocité d'Artin)**.** *Soit $\mathfrak{M}$ un cycle de k divisible par toutes les places ramifiées dans K/k.*

1. *L'application $\mathrm{Art}_{K/k,\mathfrak{M}} : I_k(\mathfrak{M}) \to \mathrm{Gal}(K/k)$ est surjective.*
2. *Pour $\mathfrak{M}$ suffisamment grand au sens de la divisibilité, on a $P_k(\mathfrak{M}) \subset \ker(\mathrm{Art}_{K/k,\mathfrak{M}})$, autrement dit $\ker(\mathrm{Art}_{K/k,\mathfrak{M}})$ est un sous-groupe de congruence modulo $\mathfrak{M}$ qu'on appelle groupe d'Artin attaché à l'extension K/k et au cycle $\mathfrak{M}$. Un tel $\mathfrak{M}$ est dit admissible pour l'extension K/k. L'application de réciprocité d'Artin induit alors un morphisme surjectif $Cl_K(\mathfrak{M}) \to \mathrm{Gal}(K/k)$.*
3. *Si $\mathfrak{M}$ est admissible pour K/k,*

$$\ker(\mathrm{Art}_{K/k,\mathfrak{M}}) = P_k(\mathfrak{M}) N_{K/k}\left(I_K(\mathfrak{M}_0 O_K)\right).$$

   L'application de réciprocité d'Artin induit alors l'isomorphisme de groupes

$$I_k(\mathfrak{M})/P_k(\mathfrak{M}) N_{K/k}\left(I_K(\mathfrak{M}_0 O_K)\right) \simeq \mathrm{Gal}(K/k).$$

4. *Il existe un $\mathfrak{M}$ admissible minimal pour la divisibilité appellé conducteur de l'extension K/k et noté $\mathfrak{f}(K/k)$.*
5. *Le conducteur de K/k n'est divisible que par les places ramifiées dans K/k.*
6. *Un cycle est admissible pour K/k si et seulement s'il est divisible par le conducteur de K/k.*

Définition 5.2.9. *Deux sous-groupes de congruences de k $(C_1, \mathfrak{M}_1)$ et $(C_2, \mathfrak{M}_2)$ sont équivalents si*

$$C_1 \cap I_k(\mathfrak{M}_2) = C_2 \cap I_k(\mathfrak{M}_1).$$

On note alors $(C_1, \mathfrak{M}_1) \sim (C_2, \mathfrak{M}_2)$.

Proposition 5.2.10. *La relation $\sim$ est une relation d'équivalence.*

Proposition-Définition 5.2.11. *1. Soit C une classe d'équivalence de sous-groupes de congruence de k.*
Alors il existe un unique sous-groupe de congruence $(C_\mathfrak{f}, \mathfrak{f}) \in C$ tel que pour tout $(C, \mathfrak{M}) \in C$ $\mathfrak{M}$ est un multiple de $\mathfrak{f}$ et $C = C_\mathfrak{f} \cap I_k(\mathfrak{M})$.
On l'appelle conducteur de la classe C.

2. *Soit $(C, \mathfrak{M})$ un sous-groupe de congruence de k et $(C_\mathfrak{f}, \mathfrak{f})$ le conducteur de sa classe d'équivalence.*
On dit que le cycle arithmétique $\mathfrak{f}$ est le conducteur de $(C, \mathfrak{M})$.
3. *Un cycle arithmétique $\mathfrak{f}$ est un conducteur s'il existe un sous-groupe de congruence $(C, \mathfrak{M})$ de conducteur $\mathfrak{f}$.*

Cette nouvelle notion de conducteur est étroitement liée à la précédente.

Théorème 5.2.12. *L'ensemble des $(\mathfrak{M}, \ker(\mathrm{Art}_{K/k,\mathfrak{M}}))$ où $\mathfrak{M}$ parcourt l'ensemble des cycles admissibles pour K/k forme une classe d'équivalence de sous-groupes de congruences. Le conducteur de cette classe d'équivalence est $(\mathfrak{f}, \ker(\mathrm{Art}_{K/k,\mathfrak{f}}))$, où $\mathfrak{f} = \mathfrak{f}(K/k)$ est le conducteur de K/k.*

Ceci permet d'établir une correspondance entre les classes d'équivalence d'extension de k et les classes d'équivalence de sous-groupes de congruence.

Théorème 5.2.13 (Takagi)**.** *1. Soit K/k et K'/k deux extensions abéliennes de corps de nombres, $\mathfrak{M}$ un cycle admissible pour K/k et $\mathfrak{M}'$ un cycle admissible pour K'/k. On suppose que les sous-groupes de congruence $(\mathfrak{M}, (\mathrm{Art}_{K/k,\mathfrak{M}}))$ et $(\mathfrak{M}', (\mathrm{Art}_{K'/k,\mathfrak{M}'}))$ sont équivalents.*
Alors les corps de nombres K et K' sont k-isomorphes.

2. *Réciproquement, soit $(\mathfrak{M}, C)$ un sous-groupe de congruence de k.*
Alors il existe une extension abélienne K/k telle que $\mathfrak{M}$ soit un cycle admissible pour K/k et $C = \ker(\mathrm{Art}_{K/k,\mathfrak{M}})$. Cette extension est unique à k-isomorphisme près.

Définition 5.2.14. *Soit $(\mathfrak{M}, C)$ un sous-groupe de congruence de k. L'extension K/k correspondant à $(\mathfrak{M}, C)$ définie à k-isomorphisme près par le théorème de Takagi s'appelle le corps de classes de rayon de $(\mathfrak{M}, C)$. Si $C = \mathcal{P}_k(\mathfrak{M})$, on la note $k(\mathfrak{M})$.*
Si $\mathfrak{M} = 1$ est le cycle trivial, le corps de classes de rayon $k(1)$ s'appelle le corps de classes de Hilbert de k.

Proposition 5.2.15. *Soit $(\mathfrak{M}, C)$ un sous-groupe de congruence de k. Le corps de classes de rayon de $(\mathfrak{M}, C)$ est donné par $k(\mathfrak{M})^{\mathrm{Art}_{K/k,\mathfrak{M}}(C)}$.*

Proposition 5.2.16. *Le corps de classes de Hilbert $k(1)$ de k est l'extension abélienne non ramifiée maximale de k. L'application de réciprocité d'Artin induit l'isomorphisme* $\mathrm{Gal}(k(1)/k) \simeq Cl_K$.

Définition 5.2.17. *Soit $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$ un cycle arithmétique de k de partie finie $\mathfrak{M}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}}$ et $\mathfrak{p}$ un idéal premier de $\mathfrak{M}$.*
On appelle partie première à $\mathfrak{p}$ de $\mathfrak{M}$ et on note $\mathfrak{M}_\mathfrak{p}$ le cycle arithmétique $\mathfrak{M}_\mathfrak{p} = \prod_{\mathfrak{p}'\neq\mathfrak{p}} \mathfrak{p}'^{\alpha_{\mathfrak{p}'}}\mathfrak{M}_\infty$.

Proposition 5.2.18. *Pour tous cycles de k $\mathfrak{M}$ et $\mathfrak{N}$ tels que $\mathfrak{N} \mid \mathfrak{M}$, on a l'application surjective suivante :*

$$s_{\mathfrak{M},\mathfrak{N}} : Cl_k(\mathfrak{M}) \to Cl_k(\mathfrak{N}).$$

Soit K/k une extension abélienne de conducteur $\mathfrak{f} = \mathfrak{f}(K/k) = \mathfrak{f}_0\mathfrak{f}_\infty$ et K_0 une sous-extension de K/k.
Soit $\mathfrak{p}$ un idéal premier de k ramifié dans K/k (ou de manière équivalente dans $k(\mathfrak{f})/k$). On note $\mathcal{P}_0$ un idéal premier de K_0 au-dessus de $\mathfrak{p}$ et $\mathcal{P}$ un idéal premier de K au-dessus de P_0. On note $\mathcal{D}_\mathfrak{p}(k(\mathfrak{M})/k)$ le groupe de décomposition de $\mathfrak{p}$ dans $k(\mathfrak{M})/k$ et $k(\mathfrak{M})^{\mathcal{D}_\mathfrak{p}}$ le corps de décomposition de $\mathfrak{p}$ au dessus de k : $\mathfrak{p}$ y est totalement décomposé.
Le groupe de décomposition de $\mathcal{P}_0$ dans $k(\mathfrak{M})/K_0$ est alors $\mathcal{D}_{\mathcal{P}_0}(k(\mathfrak{M})/K_0) = \mathcal{D}_\mathfrak{p}(k(\mathfrak{M})/k) \cap \mathrm{Gal}(k(\mathfrak{M})/K_0)$

Proposition 5.2.19. *L'idéal premier $\mathcal{P}_0$ est totalement décomposé dans K/K_0 si et seulement si $\mathcal{D}_\mathfrak{p}(k(\mathfrak{M})/k) \cap \mathrm{Gal}(k(\mathfrak{M})/K_0) \subset \mathrm{Gal}(k(\mathfrak{M})/K)$.*

Démonstration. $k(\mathfrak{M})^{\mathcal{D}_{\mathcal{P}_0}}/K_0$ est la sous-extension de $k(\mathfrak{M})/K_0$ totalement décomposée en $\mathcal{P}_0$ maximale. Donc $\mathcal{P}_0$ est totalement décomposé dans K/K_0 si et seulement si $K \subset k(\mathfrak{M})^{\mathcal{D}_{\mathcal{P}_0}}$.
Or $K = k(\mathfrak{M})^{\mathrm{Gal}(k(\mathfrak{M})/K)}$, donc cela revient à avoir $\mathcal{D}_{\mathcal{P}_0}(k(\mathfrak{M})/K_0) = \mathcal{D}_\mathfrak{p}(k(\mathfrak{M})/k) \cap \mathrm{Gal}(k(\mathfrak{M})/K_0) \subset \mathrm{Gal}(k(\mathfrak{M})/k)$. □

5.2.3 Méthodologie pour le cas k quadratique réel et $\mathrm{Gal}(K/k) = \mathbb{Z}/2\ell\mathbb{Z}$

Dans cette partie, k est un corps quadratique réel de places infinies réelles ∞_1 et ∞_2, et ℓ est un nombre premier impair. On cherche à obtenir des extensions K/k cycliques de degré 2ℓ satisfaisant les conditions souhaitées.

Pour lister les extensions cycliques de degré 2ℓ de bon type, on parcourt les idéaux de k par norme croissante.
Pour tout idéal I de k, on construit le cycle $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$ de partie finie $\mathfrak{M}_0 = I$ et de

partie infinie $\mathfrak{M}_\infty = \infty_1$, et on vérifie qu'il est conducteur sur k (si ce n'est pas le cas, on peut l'éliminer car son conducteur a déjà été traité parmi les idéaux de plus petite norme).
On calcule alors les groupes de classes de rayon $Cl_k(\mathfrak{M})$ et $Cl_k(\mathfrak{M}_0)$, ainsi que l'application $s_{\mathfrak{M},\mathfrak{M}_0}$.
Pour tout idéal premier $\mathfrak{p}$ de k divisant $\mathfrak{M}_0$, on calcule la $\mathfrak{p}$-partie $\mathfrak{M}_\mathfrak{p}$ de $\mathfrak{M}$, son groupe de classes de rayon $Cl_k(\mathfrak{M}_\mathfrak{p})$ et l'application $s_{\mathfrak{M},\mathfrak{M}_\mathfrak{p}}$. En notant $C_\mathfrak{p}$ le sous-groupe de $Cl_k(\mathfrak{M}_\mathfrak{p})$ engendré par la classe de $\mathfrak{p}$ dans $Cl_k(\mathfrak{M}_\mathfrak{p})$, on obtient alors le groupe de décomposition $\mathcal{D}_\mathfrak{p}(k(\mathfrak{M})/k)$ de $\mathfrak{p}$ dans $k(\mathfrak{M})/k$ comme étant l'image inverse de $C_\mathfrak{p}$ par $s_{\mathfrak{M},\mathfrak{M}_\mathfrak{p}}$.

On parcourt alors les sous-groupes de $Cl_k(\mathfrak{M})$ de cardinal 2ℓ. L'extension $k(\mathfrak{M})^H/k$ sera alors de degré $2l$.
Si H est un tel sous-groupe, on commence par vérifier que $k(\mathfrak{M})/k$ et $k(\mathfrak{M})^H/k$ ont même conducteur (car sinon, l'extension a déjà été obtenue via un idéal de norme inférieure).
On calcule alors $H^+ = s_{\mathfrak{M},\mathfrak{M}_0}(H)$. En utilisant $\left[k(\mathfrak{M})^H : k(\mathfrak{M}_0)^{H^+}\right] = \frac{[Cl_k(\mathfrak{M}):H]}{[Cl_k(\mathfrak{M}_0):H^+]}$, on vérifie que $\left[k(\mathfrak{M})^H : k(\mathfrak{M}_0)^{H^+}\right] = 2$, ce qui assure que l'extension $k(\mathfrak{M})^H/k$ vérifie la première condition souhaitée.
On calcule le groupe de Galois de $k(\mathfrak{M}_0)^{H^+}/k$ en utilisant $\mathrm{Gal}(k(\mathfrak{M}_0)^{H^+}/k) \simeq Cl_k(\mathfrak{M}_0)/H^+ \simeq Cl_k(\mathfrak{M})/\langle H, \ker\left(s_{\mathfrak{M},\mathfrak{M}_0}\right)\rangle$.
Pour tout idéal premier $\mathfrak{p}$ de k divisant $\mathfrak{M}$ (c'est-à-dire ramifié dans $k(\mathfrak{M})^H/k$), on note $\mathcal{P}_0$ un idéal premier de $k(\mathfrak{M}_0)^{H^+}$ au-dessus de $\mathfrak{p}$ et on teste si $\mathcal{D}_\mathfrak{p}(k(\mathfrak{M})/k) \cap \mathrm{Gal}(k(\mathfrak{M})/K_0) \subset \mathrm{Gal}(k(\mathfrak{M})/k)$. D'après la proposition 2.3, c'est le cas si et seulement si $\mathcal{P}_0$ est totalement décomposée dans $k(\mathfrak{M})^H/k(\mathfrak{M}_0)^{H^+}$. Or cette extension est de degré 2, donc c'est le cas si et seulement si $\mathcal{P}_0$ est décomposée dans $k(\mathfrak{M})^H/k(\mathfrak{M}_0)^{H^+}$. Ainsi, si cette condition n'est vérifiée pour aucun idéal premier $\mathfrak{p}$ de k divisant $\mathfrak{M}$, cela garantit que $k(\mathfrak{M})^H/k$ vérifie la deuxième condition souhaitée.
Enfin, comme $\mathfrak{M}_\infty = \infty_1$, on a ∞_2 qui reste réelle dans $k(\mathfrak{M})^H$ et ∞_1 qui devient complexe, donc la troisième condition est satisfaite.

Comme le but sera ensuite de tester la conjecture en $p = \ell$, afin de ne pas être dans un cas trivial, on peut très tôt dans l'algorithme ignorer les cas dans lesquels $Cl_k(\mathfrak{M})$ n'est pas divisible par ℓ. De plus, deux groupes de cardinal $p = \ell$ étant nécessairement isomorphes, ont peut éliminer les extensions dont le groupe de classes n'est pas divisible par ℓ^2.

5.3 Vérification numérique de la conjecture faible

5.3.1 Méthode de vérification de la conjecture

Une fois une extension du bon type créée, on peut calculer les idéaux de Fitting $\mathrm{Fitt}_{\mathbb{Z}[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\right)$ et $\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right)$. Comme $\mathbb{Z}[1/2][G]$ est une $\mathbb{Z}[G]$-algèbre associative, pour tout $\mathbb{Z}[G]$-module M d'après la proposition 1.6.10 on a

$$\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}[1/2]\right)=\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(M\underset{\mathbb{Z}[G]}{\otimes}\mathbb{Z}[1/2][G]\right)=\mathbb{Z}[1/2][G]\mathrm{Fitt}_{\mathbb{Z}[G]}(M).$$

Ainsi

$$\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\otimes\mathbb{Z}[1/2]\right)=\mathrm{Fitt}_{\mathbb{Z}[1/2][G]}\left(Cl_K^-\otimes\mathbb{Z}[1/2]\right)$$

si et seulement si

$$\mathbb{Z}[1/2][G]\mathrm{Fitt}_{\mathbb{Z}[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\right)=\mathbb{Z}[1/2][G]\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right).$$

Pour vérifier que l'extension vérifie la conjecture global faible du chapitre précédent, il suffit alors de s'assurer qu'il existe deux entiers m et n tels que

$$2^m\mathrm{Fitt}_{\mathbb{Z}[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\right)\subset\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right)$$

et

$$2^n\mathrm{Fitt}_{\mathbb{Z}[G]}\left(Cl_K^-\right)\subset\mathrm{Fitt}_{\mathbb{Z}[G]}\left(\overline{\mathcal{U}}_K^-/\mathbb{Z}[G]\,\bar{\varepsilon}\right).$$

5.3.2 Résultats numériques

Nous avons vérifié numériquement à l'aide de PARI/GP la conjecture globale faible pour des extensions de groupe de Galois cyclique d'ordre 6. Pour tout corps de nombres quadratique réel k de discriminant Δ_k, la conjecture globale faible est donc vraie pour toutes les extensions abéliennes K/k de degré 6 dont le conducteur est inférieur à la borne B indiquée dans le tableau suivant.

Δ_k	5	8	12	13	17	21	24	28	29	33	37	40	41	44	53	56
B	26000															

57	60	61	65	69	73	76	77	85	88	89	92	93	97
24000	26000				18000	22000				20000			12000

101	104	105	109	113	120	124	129	133	136	137	140	141
16000							14000	16000	14000			

145	149	152	156	157	161	165	168	172	173	177	181	184
8000	10000									8000	10000	

185	188	193	197	201	204	205	209	213	217	220	221	229
10000		6000	8000	4000								

232	233	236	237	241	248	249	253	257	264	265	268	269	273	277
4000														

280	281	284	285	293	296	301	305	309	312	313	316	317	321	328
4000						2000								

329	332	337	341	344	345	348	349	353	357	364	365	373	376	377
2000														

380	381	385	389	393	397
2000					

Voici les structures rencontrées pour la 3-partie du groupe de classes des extensions K lorsque le nombre de classes est au moins divisible par 9.

$Cl_K \otimes \mathbb{Z}_3$	$\mathbb{Z}/9\mathbb{Z}$	$\mathbb{Z}/27\mathbb{Z}$	$\mathbb{Z}/81\mathbb{Z}$	$(\mathbb{Z}/3\mathbb{Z})^2$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$	$(\mathbb{Z}/9\mathbb{Z})^2$
occurrences	5133	147	6	7965	1195	45	18

$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$	$(\mathbb{Z}/3\mathbb{Z})^3$	$(\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z}$	$(\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/27\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/9\mathbb{Z})^2$	$(\mathbb{Z}/3\mathbb{Z})^4$
3	585	129	2	2	50

$(\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z}$	$(\mathbb{Z}/3\mathbb{Z})^5$
4	5

Bibliographie

[AW67] Michael Atiyah et Charles Wall : Cohomology of groups. *In Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 94–115. Thompson, Washington, D.C., 1967.

[CG98] Pietro Cornacchia et Cornelius Greither : Fitting ideals of class groups of real fields with prime power conductor. *Journal of Number Theory*, 73(2):459–471, 1998.

[Chi83] Theodore Chinburg : On the Galois structure of algebraic integers and S-units. *Invent. Math.*, 74(3):321–349, 1983.

[Coh93] Henri Cohen : *A course in computational algebraic number theory*, volume 138 de *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Coh00] Henri Cohen : *Advanced topics in computational number theory*, volume 193 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Lan94] Serge Lang : *Algebraic number theory*, volume 110 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1994.

[Mac67] Saunders MacLane : *Homology*. Springer-Verlag, Berlin-New York, first édition, 1967. Die Grundlehren der mathematischen Wissenschaften, Band 114.

[MW84] Barry Mazur et Andrew Wiles : Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[Nor76] Douglas Northcott : *Finite free resolutions*. Cambridge University Press, Cambridge-New York-Melbourne, 1976. Cambridge Tracts in Mathematics, No. 71.

[Rob13] Xavier-François Roblot : Index formulae for Stark units and their solutions. *Pacific J. Math.*, 266(2):391–422, 2013.

[Rub92] Karl Rubin : Stark units and Kolyvagin's "Euler systems". *J. Reine Angew. Math.*, 425:141–154, 1992.

[Sta71] Harold Stark : Values of L-functions at $s = 1$. I. L-functions for quadratic forms. *Advances in Math.*, 7:301–343 (1971), 1971.

[Sta75] Harold Stark : L-functions at $s = 1$. II. Artin L-functions with rational characters. *Advances in Math.*, 17(1):60–92, 1975.

[Sta76] Harold Stark : L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem. *Advances in Math.*, 22(1):64–84, 1976.

[Sta80] Harold Stark : L-functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. in Math.*, 35(3):197–235, 1980.

[Tat66] John Tate : The cohomology groups of tori in finite Galois extensions of number fields. *Nagoya Math. J.*, 27:709–719, 1966.

[Tat84] John Tate : *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, volume 47 de *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1984. Notes de cours rédigées par Dominique Bernardi et Norbert Schappacher.

[The18] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.9.5`, 2018. available from `http://pari.math.u-bordeaux.fr/`.

[Wei96] Alfred Weiss : *Multiplicative Galois module structure*, volume 5 de *Fields Institute Monographs*. American Mathematical Society, Providence, RI, 1996.