Tables des matières

0 Introduction

Cette thèse est consacrée à l'étude de la structure galoisienne du groupe des unités cyclotomiques. Les diverses définitions de ce sous-groupe des unités d'un corps abélien sont apparues au tout début avec les travaux de Kummer dans les corps cyclotomiques, suivis des résultats de Hasse et des définitions de Leopoldt qui généralisent ce groupe à des corps abéliens quelconques. On peut aussi mentionner le groupe des unités de Ramachandra qui est en général strictement contenu dans les unités cyclotomiques telles que définies ici.

Ce n'est que beaucoup plus récemment, au début des années 80, que Sinnott a défini son groupe des unités circulaires, dans les articles [Si 1] et [Si 2]. Aujourd'hui, celui-ci semble faire le consensus. Pour cette raison, on a choisi d'étudier cette version parmi tant d'autres des unités cyclotomiques.

La description effective de la structure galoisienne de ce groupe ne peut se faire que pour les cas des corps abéliens K, dont le conducteur est une puissance d'un seul nombre premier, ou dont le degré sur $\mathbb{Q}$ est premier. Dans ces cas, ce groupe est monogène sur l'anneau de groupe $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$, et donc, isomorphe au quotient de cet anneau par l'idéal engendré par la norme de K sur $\mathbb{Q}$. Pour des corps plus généraux, la quantité de générateurs nécessaire et le nombre de relations entre ces générateurs augmente considérablement. Cela rend les approches explicites beaucoup plus délicates, voire apparemment insolubles.

Dans le travail qui suit on s'est surtout intéressé à un problème légèrement plus simple. On a cherché à décrire la structure des unités cyclotomiques de certains corps relativement à l'action d'un sous-groupe très particulier du groupe de Galois. En effet, supposons que K soit un corps abélien réel, et soit p un nombre premier non ramifié dans K. On note K_∞ la $\mathbb{Z}_p$-extension cyclotomique de K, et K_n l'unique sous-corps de K_∞ qui soit de degré p^n sur K. On a étudié la structure des unités cyclotomiques de K_n, en tant que $\mathbb{Z}[\mathrm{Gal}(K_n/K)]$-module.

Le premier chapitre contient, en quelque sorte, un état de l'art des connaissances actuelles sur les unités cyclotomiques. On y décrit, sans aucune démonstration, certains résultats antérieurs à cette thèse. Ces résultats ont servi de point de départ à l'étude qui suit. On y expose notamment la définition de Sinnott ainsi que sa formule d'indice. Ensuite on passe à des résultats plus en rapport avec la structure galoisienne. On y rappelle la description des relations galoisiennes, entre les générateurs de Sinnott, due à Solomon. Ce chapitre se termine avec un exposé des résultats de Greither sur les "normes universelles" dans les $\mathbb{Z}_p$-extensions. Ces résultats ne s'appliquent pas, à proprement parler, aux normes universelles des unités ni à celles des unités cyclotomiques. Par contre, ils montrent que la structure galoisienne des normes universelles est très souvent simple. A partir de cette constatation, on est amené à définir puis à étudier un module $\mathcal{D}_n(K)$. Celui-ci ne contient que des normes universelles de $(p-)$unités, et son tensorisé avec $\mathbb{Z}_p$ contient le tensorisé avec $\mathbb{Z}_p$ des normes universelles des unités cyclotomiques.

La définition de ce module, ainsi que la description de son caractère est faite dans le chapitre II de cette thèse. Ce chapitre contient aussi quelques résultats élémentaires sur ce module, comme sa comparaison avec le module des unités cyclotomiques de Sinnott. On y démontre aussi que $\mathcal{D}_n(K) \otimes \mathbb{Z}_p$ contient le tensorisé avec $\mathbb{Z}_p$ des unités cyclotomiques.

Le chapitre III est consacré à l'étude des relations entre les générateurs de $\mathcal{D}_n(K)$. Le principal résultat de ce chapitre, le théorème 3.6, est dans le même style que le théorème 2.2 de [So 2]. Par contre la preuve présentée ici est complètement indépendante de celle de [So 2]. Elle ne s'appuie que de très loin sur le fait que $L(1,\chi) \neq 0$. En fait on n'utilise que la connaissance des rangs sur $\mathbb{Z}$ des unités cyclotomiques. On est aussi amené à distinguer deux types de relations galoisiennes. D'une part les relations appartenant au module noté $\mathcal{H}_n$, dites relations “horizontales” et qui sont d'une certaine manière indépendantes de l'étage n dans la $\mathbb{Z}_p$-extension considérée. Ces relations sont des ‘relevés’ des relations existant entre les générateurs des unités cyclotomiques du corps K, et l'action de $\mathrm{Gal}(K_n/K)$, n'intervient que très peu dans ces relations. La présence de relations d'une autre nature, dites ”verticales”, complique considérablement ce travail. Ces relations formées des éléments du module $\mathcal{V}_n$ concernent directement l'action de $\mathrm{Gal}(K_n/K)$. Elles se révèlent être l'obstruction majeure à la liberté du module $\mathcal{D}_n(K)$, comme cela se voit dans le chapitre IV.

Le chapitre IV contient le résultat central de cette thèse, à savoir le théorème 4.5. On y formule deux hypothèses, l'une de nature globale, l'hypothèse A, l'autre de nature locale, l'hypothèse B. Grâce à ces hypothèses, et en s'appuyant sur la présentation libre du chapitre précédent, on décrit complètement la structure globale, sous l'hypothèse A, locale sous l'hypothèse B, du module $\mathcal{D}_n(K)$. Comme on pouvait l'espérer, et même si $\mathcal{D}_n(K)$ n'est pas libre sur $\mathbb{Z}[\mathrm{Gal}(K_n/K)]$ ou $\mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$, sa structure reste très simple. En effet on montre que :

Si K vérifie H. A alors on a :

$$\mathcal{D}_n(K) \simeq (\mathbb{Z}[\mathrm{Gal}(K_n/K)])^r \oplus \left(\frac{\mathbb{Z}[\mathrm{Gal}(K_n/K)]}{I_n}\right)^t$$

Si (K,p) vérifie H. B alors on a :

$$\mathcal{D}_n(K) \otimes \mathbb{Z}_p \simeq (\mathbb{Z}_p[\mathrm{Gal}(K_n/K)])^r \oplus \left(\frac{\mathbb{Z}_p[\mathrm{Gal}(K_n/K)]}{I_n \otimes \mathbb{Z}_p}\right)^t$$

Où on note I_n l'idéal de $\mathbb{Z}[\mathrm{Gal}(K_n/K)]$ engendré par la norme de K_n sur K. Les entiers r et t dépendent de la décomposition en idéaux premiers de p dans K et se déduisent facilement du caractère calculé au chapitre II. On peut remarquer que la présence de facteurs du type $\mathbb{Z}[\mathrm{Gal}(K_n/K)]/I_n$ n'est due qu'aux éléments de $\mathcal{V}_n$ (les relations dites “verticales”).

Dans le chapitre V, on décrit, dans certains cas, la cohomologie des unités cyclotomiques par rapport à l'action des groupes de Galois relatifs d'une $\mathbb{Z}_p$-extension. On utilise deux techniques différentes qui permettent d'atteindre des cas assez dissemblables. La première est entièrement due à Kim et est extraite de l'article [K 1].

On applique simplement cette méthode à des cas un peu plus généraux que celui de l'article [K 1].

L'approche présentée en section V.3, s'appuie, elle, entièrement sur la version locale du théorème 4.5, et permet de traiter des corps K plus généraux car on n'y fait aucune hypothèse sur la divisibilité par p du degré de K sur $\mathbb{Q}$. Coïncidence (peut-être signifivative), la version locale de 4.5 entraîne ce que certains auteurs appellent la "descente galoisienne" pour les unités cyclotomiques dans la $\mathbb{Z}_p$-tour. Et cette propriété, qui n'est pas vérifiée en général, est l'ingrédient principal dans la démarche de Kim.

Dans le chapitre VI, on étudie plus en détail les hypothèses A et B du théorème 4.5. On commence par donner des conditions suffisantes à la validité de ces hypothèses. L'hypothèse B se trouve être vérifiée dans un grand nombres de cas, où la structure galoisienne des unités cyclotomiques semblait hors d'atteinte. En effet ces conditions suffisantes peuvent être réalisées, même sur des corps non cycliques dont le conducteur a un nombre quelconque de diviseurs premiers. De plus une de ces conditions suffisantes s'exprime en terme du groupe des classes de K. Ensuite on vérifie sur deux exemples que la conclusion locale de 4.5 n'est pas toujours vraie. Cela justifie l'utilisation des hypothèses A et B. Le dernier exemple dément en outre la propriété de descente galoisienne dans la $\mathbb{Z}_p$-tour.

Dans le dernier chapitre, on applique le formalisme des chapitres III et IV au $\mathbb{Z}_p$ module galoisien engendré par les p-unités cyclotomiques définies dans [So 1]. Sous l'hypothèse B, ce groupe se révèle être libre sur l'anneau $\mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$. Ici, les preuves se simplifient considérablement grâce à l'absence de relations comparables aux relations verticales. Cette absence explique aussi la liberté de ce module.

I Unités cyclotomiques

Dans ce chapitre on résume, sans démonstration, des résultats qui ont servi de point de départ à l'étude qui suit. Dans cette thèse, on a choisi la définition de Sinnott des unités cyclotomiques, même si de nombreuses variantes de ce type de sous-groupes des unités coëxistent encore (unités cyclotomiques formelles de Leopoldt [Le], de Greenberg [Gree 2], les groupes définis dans [Gi] et dans [Fr]).

I.1 La formule d'indice de Sinnott.

Soit K un corps de nombres abélien sur $\mathbb{Q}$. On notera G_K le groupe $\mathrm{Gal}(K/\mathbb{Q})$, et $\mathrm{cond}(K)$ le conducteur de K qui est un entier positif non congru à 2 modulo 4. $E(K)$ désignera le groupe des unités de K, et on notera $\mu(K)$ les racines de l'unité contenues dans K. Si l est un nombre premier qui ne se ramifie pas dans K, $\left(\frac{K}{l}\right) \in G_K$ désignera le Frobenius de l. Pour chaque entier n non nul on note ζ_n la racine primitive n^{ieme} de l'unité suivante :

$$\zeta_n = \exp\left(\frac{2i\pi}{n}\right)$$

On peut donc voir K comme un sous-corps de $\mathbb{Q}(\zeta_{\mathrm{cond}(K)})$.

On rappelle tout d'abord la définiton des unités cyclotomiques de Sinnott.

Définition I.1. *Soit $D(K)$ le groupe multiplicatif engendré dans K par les entiers de la forme :*

$$N_{K\cap\mathbb{Q}(\zeta_n)}^{\mathbb{Q}(\zeta_n)}(1-\zeta_n^a),$$

Où on fait parcourir à n l'ensemble des entiers supérieurs ou égaux à 3 et, pour chaque n, à a l' ensemble des entiers non divisibles par n. On appelle groupe des unités cyclotomiques (circulaires chez certains auteurs dont Sinnott lui-même) et on note $C(K)$ le groupe suivant :

$$C(K) = (\{\pm 1\}D(K)) \cap E(K)$$

$C(K)$ est évidemment un $\mathbb{Z}[G_K]$-module avec l'action naturelle de G_K. Une des propriétés les plus remarquables de ce groupe est qu'il est d'indice fini dans $E(K)$. Dans [Si 1] et [Si 2], Sinnott évalue cet indice sous la forme :

Théorème I.2. *Soit K^+ le sous-corps réel maximal de K et h^+ le nombre de classes de K^+. On a :*

$$(\dagger) \qquad [E(K):C(K)] \;=\; h^+ \; Q \; 2^a \frac{1}{[K:\mathbb{Q}]} \prod_{\substack{p^e \mid \operatorname{cond} K \\ p^{e+1} \nmid \operatorname{cond} K}} [\mathbb{Q}(\zeta_{p^e}) \cap K : \mathbb{Q}] \; c_K$$

Où $a = [K : \mathbb{Q}] - 1$ lorsque K est réel, a est un entier négatif sinon, p décrit l'ensemble des diviseurs premiers de $\operatorname{cond} K$, et $Q = [E(K) : \mu(K)E(K^+)]$, c'est-à-dire que $Q = 1$ lorsque K est réel, et vaut 1 ou 2 sinon.

Dans son article [Si 2], Sinnott donne un encadrement de a dans le cas où K est imaginaire et définit précisément la constante c_K comme l'indice dans $\mathbb{Z}[G_{K^+}]$ d'un réseau de $\mathbb{Q}[G_{K^+}]$. Il montre que cet indice, a priori un nombre rationnel, est un entier qui ne peut être divisible que par les (puissances des) nombres premiers divisant $[K : \mathbb{Q}]$. Cependant Sinnott n'explicite pas cette constante.

Néanmoins dans certains cas particuliers (qui d'ailleurs avaient été étudiés avant ce résultat) la formule (†) se simplifie considérablement. Par exemple, lorsque K est cyclotomique ou cyclique sur $\mathbb{Q}$, la constante c_K vaut 1. Et lorsque K est cyclique et totalement réel il est parfois préférable, d'un certain point de vue, de définir un groupe $C'(K)$ vérifiant $[E(K) : C'(K)] = h_K$. Cette construction est par exemple possible lorsque $\operatorname{cond} K$ n'est divisible que par les (puissances d') un seul nombre premier ou lorsque K est cyclique de degré premier sur $\mathbb{Q}$, voir [Ha]. Un autre résultat de [Si 2] est que les indices c_{K_n} ont le bon goût de rester bornés lorsque que $(K_n)_{n\in\mathbb{N}}$ décrit les étages de degré fini de la $\mathbb{Z}_p$-extension cyclotomique de K, pour $p \neq 2$.

I.2 Quelques informations sur la structure galoisienne.

Si l'on s'intéresse à la $\mathbb{Z}[G_K]$-structure des modules $C(K)$, une première approche est de décrire les relations entre les générateurs de $D(K)$ donnés dans la définition I.1. L'étude de ces relations remonte à l'article de Bass [Ba] corrigé par Ennola dans [E], où sont considérées les relations multiplicatives en voyant $C(K)$ comme un simple $\mathbb{Z}$-module et lorsque K est un corps cyclotomique. Ici on énonce des résultats extraits de [So 2].

Nous commençons par rappeler les relations de Bass entre les entiers suivants :

Lemme I.3. *Soit f un entier naturel non congru à 2 modulo 4 et p un nombre premier divisant f. Soit $f' = \frac{f}{p}$. Alors si $p \mid f'$ et si $f' \neq 2$ on a :*

$$N^{\mathbb{Q}(\zeta_f)}_{\mathbb{Q}(\zeta_{f'})}(1-\zeta_f) = 1 - \zeta_{f'}$$

si $p \nmid f'$ et si $f' \notin \{1,2\}$ on a :

$$N^{\mathbb{Q}(\zeta_f)}_{\mathbb{Q}(\zeta_{f'})}(1-\zeta_f) = (1-\zeta_{f'})^{\left(1-\left(\frac{\mathbb{Q}(\zeta_{f'})}{p}\right)^{-1}\right)}$$

si $f' \in \{1,2\}$ *on a (pour* $p \neq 2$*) :*

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(1-\zeta_p) = p$$

et pour $p = 2$ *:*

$$N_{\mathbb{Q}}^{\mathbb{Q}(i)}(1-i) = 2$$

Ces relations se combinent en divisant f par des puissances de plusieurs nombres premiers, et, par restriction des normes et des Frobenius elles donnent les relations de la formule (††) ci-dessous, entre les générateurs de $D(K)$. On reprend le formalisme de [So 2] pour expliquer en quoi ces relations sont (presque) les seules. A partir d'ici on suppose que K est totalement réel. Sous cette condition on voit que les générateurs de $D(K)$ sont totalement positifs et qu'ils engendrent un module sans $\mathbb{Z}$-torsion. Soient s le nombre de sous-corps de K distincts de $\mathbb{Q}$, et $\mathcal{P}$ l'ensemble des nombres premiers divisant $\operatorname{cond} K$. Soit Σ un ensemble de symbole de cardinal $s + \#\mathcal{P}$. On fixe une bijection $\sigma \mapsto [\sigma]$, partant de Σ et à valeur dans la réunion disjointe $\{F, F \text{ corps de nombres}, F \neq \mathbb{Q}, F \subset K\} \bigcup \mathcal{P}$. Soit $\sigma \in \Sigma$, on note $\mathcal{F}(\sigma) = [\sigma]$ lorsque $[\sigma]$ est un corps, et $\mathcal{F}([\sigma]) = \mathbb{Q}$ sinon. On note $G_\sigma = \operatorname{Gal}(\mathcal{F}(\sigma)/\mathbb{Q})$. Et on note de plus $\operatorname{cond}\sigma = \operatorname{cond}[\sigma]$ si $[\sigma]$ est un corps, $\operatorname{cond}\sigma = [\sigma]$ si $[\sigma]$ est un nombre premier impair et $\operatorname{cond}\sigma = 4$, si $[\sigma] = 2$. A chaque élément σ de Σ on associe l'entier algébrique :

$$\epsilon_\sigma = N_{\mathcal{F}(\sigma)}^{\mathbb{Q}(\zeta_{\operatorname{cond}\sigma})}(1-\zeta_{\operatorname{cond}\sigma})$$

Dans [So 2] Solomon utilise la relation d'ordre suivante sur Σ : $\sigma \prec \sigma'$ si et seulement si $\mathcal{F}(\sigma) \subset \mathcal{F}(\sigma')$ et $\operatorname{cond}\sigma \mid \operatorname{cond}\sigma'$. Pour $\sigma \prec \sigma'$ le lemme I.3 permet d'établir les relations :

$$(\dagger\dagger) \qquad N_{\mathcal{F}(\sigma)}^{\mathcal{F}(\sigma')}\epsilon_{\sigma'} = \epsilon_\sigma^{\prod_p \left(1-\left(\frac{\mathcal{F}(\sigma)}{p}\right)^{-1}\right)}$$

en faisant varier p parmi les diviseurs premiers de $\operatorname{cond}\sigma'$ qui ne divisent pas $\operatorname{cond}\sigma$.

Pour toute partie $\mathcal{T}$ de Σ, formons la somme directe :

$$W_{\mathcal{T}} = \bigoplus_{\sigma\in\mathcal{T}} \mathbb{Z}[G_\sigma]\sigma$$

On a évidemment un $\mathbb{Z}[G_K]$-homomorphisme $\alpha_{\mathcal{T}} : W_{\mathcal{T}} \longrightarrow D(K)$, défini par $\mathbb{Z}[G_K]$-linéarité avec $\alpha_{\mathcal{T}}(\sigma) = \epsilon_\sigma$. De plus, on a $\{\pm 1\}\operatorname{Im}(\alpha_\Sigma) \cap E(K) = C(K)$. En fait $\operatorname{Im}(\alpha_\Sigma)$ ne diffère de $D(K)$ que par le groupe libre engendré par les premiers ne divisant pas $\operatorname{cond} K$. L'étude des relations sur $D(K)$ consiste donc à décrire le noyau de α_Σ.

Définition I.4. *Soit $\mathcal{T}$ une partie de Σ. Appelons $U_{\mathcal{T}}$ le $\mathbb{Z}[G_K]$-sous-module de $W_{\mathcal{T}}$ engendré par les éléments de la formes :*

$$R_{\sigma}^{\sigma'} = N_{\mathcal{F}(\sigma)}^{\mathcal{F}(\sigma')} \ \sigma' - \prod_{\substack{p \mid \mathrm{cond}\,\sigma' \\ p \nmid \mathrm{cond}\,\sigma}} \left(1 - \left(\frac{\mathcal{F}(\sigma)}{p}\right)^{-1}\right) \sigma$$

En faisant varier $\{\sigma, \sigma'\}$ parmi tous les couples contenus dans $\mathcal{T}$ tels que $\sigma \prec \sigma'$

D'après ce qui précède on a $U_{\mathcal{T}} \subset \ker \alpha_{\mathcal{T}}$. Dans [So 2] les théorèmes suivants sont démontrés :

Théorème I.5. *Soit $\mathcal{G}$ le sous-ensemble de Σ formé des σ tels que $\mathcal{F}_\sigma$ soit cyclique sur $\mathbb{Q}$ (en particulier les σ tels que $[\sigma]$ soit un nombre premier), on a :* $\ker \alpha_{\mathcal{G}} = U_{\mathcal{G}}$

On peut remarquer que lorsque K est cyclique on a $\mathcal{G} = \Sigma$. De plus $\mathrm{Im}\,\alpha_{\mathcal{G}} \cap E(K)$ est toujours d'indice fini dans $E(K)$.

Théorème I.6. *Soit $\mathcal{T}$ une partie de Σ contenant $\mathcal{G}$. Alors $U_{\mathcal{T}}$ est d'indice fini dans* $\ker \alpha_{\mathcal{T}}$ *et cet indice n'est divisible que par les (puissances des) nombres premiers divisant* $[K : \mathbb{Q}]$.

Dans l'article [So2] la proposition suivante est démontrée. Soit L un sous-corps de K et $\alpha'_{\mathcal{T}}$ les homomorphismes du même type que ce qui précède en remplaçant K par L et soit $\mathcal{G}(L)$ la partie de Σ correspondant à la réunion des sous-corps cycliques de L et des premiers divisant $\mathrm{cond}\, L$. On a :

Proposition I.7.

$$\mathrm{Im}\,\alpha_{\mathcal{G}} \cap E(L) = \mathrm{Im}\,\alpha'_{\mathcal{G}(L)} \cap E(L) \ .$$

En particulier lorsque K est cyclique, on a $C(K) \cap L = C(L)$, ce qui avait déjà été démontré dans [Grei 1].

Pour les unités cyclotomiques de Sinnott ces propriétés d'intersection (improprement appelées parfois “descente galoisienne”) ont été étudiées dans les articles [Grei 1] et [G K]. L'article [Grei 1] contient un contre-exemple à cette propriété entre deux corps (l'un contenant l'autre, le premier n'étant pas cyclique sur $\mathbb{Q}$) dans lesquels tous les premiers ramifiés sont modérément ramifiés. Dans l'article [G K] Gold et Kim démontrent le théorème suivant :

Théorème I.8. *Soient a et b, deux entiers non congrus à 2 modulo 4 et tels que $a \mid b$. Alors, on a :*

$$C\left(\mathbb{Q}(\zeta_b)\right) \cap \mathbb{Q}(\zeta_a) = C\left(\mathbb{Q}(\zeta_a)\right)$$

I.3 $\mathbb{Z}_p$-extensions cyclotomiques.

Rappelons tout d'abord la construction des $\mathbb{Z}_p$-extensions de $\mathbb{Q}$. Soit p un nombre premier et soit $q = p$ si p est impair, $q = 4$ sinon. Soit $L = \bigcup_{n \in \mathbb{N}} \mathbb{Q}(\zeta_{qp^n})$. Alors L est un corps abélien sur $\mathbb{Q}$ et son groupe de Galois est naturellement isomorphe à $\mathbb{Z}_p^\times$ par l'application d'Artin (les Frobenius). Ainsi L contient un unique sous-corps $\mathbb{B}_\infty$ tel que :

$$\mathrm{Gal}(\mathbb{B}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p \simeq \frac{\mathbb{Z}_p^\times}{\mu\left(\mathbb{Q}_p\right)}$$

On appelle $\mathbb{B}_\infty$ la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$, et c'est sa seule $\mathbb{Z}_p$-extension. Pour tout $n \in \mathbb{N}$, le corps $\mathbb{B}_\infty$ contient un unique sous-corps cyclique de degré p^n sur $\mathbb{Q}$, que l'on note $\mathbb{B}_n$. ce dernier corps est totalement réel et son conducteur vaut qp^n (de telle sorte que p est totalement ramifié dans $\mathbb{B}_n$). Maintenant si K est un corps de nombres ne contenant pas $\mathbb{B}_\infty$, on appelle le composé $K_\infty = K\ \mathbb{B}_\infty$ la $\mathbb{Z}_p$-extension cyclotomique de K. Soit m l'entier tel que $\mathbb{B}_m = K \cap \mathbb{B}_\infty$, alors l'unique sous-corps de K_∞ de degré p^n sur K est le composé $K_n = K\ \mathbb{B}_{m+n}$. Dans cette thèse nous allons essayer de donner le plus d'informations possible sur la structure galoisienne des unités cyclotomiques dans la $\mathbb{Z}_p$-extension cyclotomique d'un corps abélien K, relativement à l'action des groupes de Galois $G_n^l = \mathrm{Gal}(K_l/K_n)$. A ma connaissance les seuls autres résultats dans cette direction sont de nature cohomologique et contenus dans [K 1] et [K 2]. On en donne ici un résumé. Soient p un nombre premier distinct de 2 et $K = \mathbb{Q}(\zeta_{pd})$ pour un entier d tel que $p \nmid d\ \varphi(d)$ (où φ est la fonction d'Euler, c'est-à-dire $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$). Ici la $\mathbb{Z}_p$-extension cyclotomique de K est la réunion des corps $\mathbb{Q}\left(\zeta_{p^{n+1}d}\right)$ pour $n \in \mathbb{N}$. En conséquence le théorème I.8 s'applique et Kim dans [K 1] en déduit le théorème suivant :

Théorème I.9. *Soient $m > n \geq 0$ deux entiers, soit r le $\mathbb{Z}$-rang des unités modulo leur $\mathbb{Z}$-torsion du corps de décomposition de p dans K. Notons $\widehat{H}^i$ les deux groupes de cohomologie modifiés à la Tate, on a :*

$$\widehat{H}^0(G_n^m, C(K_m)) \simeq \left(\frac{\mathbb{Z}}{p^{m-n}\ \mathbb{Z}}\right)^r$$

et

$$\widehat{H}^1(G_n^m, C(K_m)) \simeq \left(\frac{\mathbb{Z}}{p^{m-n}\ \mathbb{Z}}\right)^{r+1}$$

De plus Kim construit des générateurs explicites du $\widehat{H}^0$ dans [K 1] et du H^1 dans [K 2]. Les résultats des chapitres qui suivent ont aussi des applications cohomologiques, mais s'appuient sur une démarche différente, qui a été motivée en partie par les résultats de Greither dans [Grei 2] sur les normes universelles. On énonce ces résultats dans le paragraphe suivant (le dernier de ce chapitre de rappels).

I.4 Normes universelles.

Soit p un nombre premier et soit A un foncteur de la catégorie des corps de nombres avec les morphismes d'inclusions, dans celle des $\mathbb{Z}_p$-modules de type fini. Supposons que A vérifie les conditions suivantes :

P1). *Il existe un homorphisme de norme, $N_K^L : A(L) \longrightarrow A(K)$ pour toute extension L/K et lorsque L/K est galoisienne, de groupe de Galois G, l'homomorphisme composé :*

$$A(L) \longrightarrow A(K) \stackrel{A(K\subseteq L)}{\longrightarrow} A(L)$$

coïncide avec la multiplication par la norme $\sum_{g\in G} g$

P2). *A vérifie une propriété d'intersection semblable à celle de I.8, à savoir : pour toute extension L/K galoisienne de groupe de Galois G, l'application $A(K) \longrightarrow A(L)$ est injective d'image $A(L)^G$ (on peut la voir comme une inclusion).*

Etant donné une $\mathbb{Z}_p$-extension (pas nécessairement cyclotomique), $F_\infty = \bigcup_n F_n$ d'un corps de nombres $F = F_0$, avec $[F_n : F] = p^n$, en notant A_∞ la réunion $\bigcup_n A(F_n)$, on suppose en outre que :

P3). *Pour n assez grand, le $\mathbb{Z}_p$-rang de $A(F_n)$ peut s'écrire sous la forme $sp^n + t$ où les entiers positifs s et t sont indépendants de n.*

P4). *Les cardinaux des groupes de cohomologie continue $H^1(G_n^\infty, A_\infty)$ sont bornés, et les groupes de cohomologie $H^1(G_n^\infty, (A_\infty)_{\mathrm{tor}})$ sont réduits à zéro (en notant ici aussi $G_n^m = \mathrm{Gal}(F_m/F_n)$, pour $m > n$, $m \in \{\infty\} \cup \mathbb{N}$.*

Alors, on a :

Théorème I.10.
Les modules $\bigcap_{m\geq n} N_{F_n}^{F_m}\left(\frac{A(F_m)}{A(F_m)_{\mathrm{tor}}}\right) \subset \frac{A(F_n)}{A_(F_n)_{\mathrm{tor}}}$ (il s'agit des normes universelles associées à A/A_{tor}) sont libres de rang s sur l'anneau $\mathbb{Z}_p[G_0^n]$. En conséquence, leur limite projective (par rapport aux applications de norme) est libre de rang s sur l'algèbre d'Iwasawa $\Lambda = \varprojlim_n \mathbb{Z}_p[G_0^n]$.

Greither donne dans son article divers exemples de foncteurs A satisfaisant ses conditions, en particulier les p-unités tensorisées avec $\mathbb{Z}_p$ vérifient les propriétés 1) à

4). Malheureusement cette démarche ne s'applique pas aux unités tensorisées avec $\mathbb{Z}_p$ elles-mêmes. En fait les propriétés 2 et 3 ne sont pas vérifiées. Greither sauve une partie de son résultat sur les unités en s'appuyant sur la connaissance des p-unités. En supposant qu'aucune place de F divisant p ne se décompose totalement dans F_∞, on a la proposition :

Proposition I.11. *Soit g un générateur de G_0^∞. En posant $A(L) = E(L) \otimes \mathbb{Z}_p$, les modules $\cap_{m \geq n} N_{F_n}^{F_m}\left(\ker N_F^{F_m} \cap (A(F_m))\right)$ sont isomorphes à $(1-g)\left(\mathbb{Z}_p[G_0^n]\right)^s$, où s est la somme du nombre de places complexes de F avec le nombre de places réelles de F.*

Cela laisse supposer une G_0^n structure assez simple pour les normes universelles des unités. Le théorème 5.8 de [F K N] énonce que si on se place dans la $\mathbb{Z}_p$-extension cyclotomique d'un corps abélien sur $\mathbb{Q}$, sous la conjecture de Greenberg, énoncée dans [Gree 1], ces normes universelles coïncident, avec les normes universelles des unités cyclotomiques d'après le théorème 5.8 de [F K N]. L'idée directrice de cette thèse consiste à introduire un module galoisien (le module $\mathcal{D}_n(K)$ dans ce qui suit), qui correspondrait à une "globalisation" de ces normes universelles. Et d'étudier par une approche plus explicite que celle de [Grei 2], la G_0^n-structure de ce module.

II Définitions, premières propriétés

Dans ce chapitre on définit le module $\mathcal{D}_n(K)$, et on établit certaines des propriétés utiles de ce module. Plus précisément, on calcule son caractère (proposition 2.4) et on le compare avec le module des unités circulaires de Sinnott (proposition 2.6 et lemme 2.3).

II.1 Conventions et notations.

Dans toute la suite K est un corps abélien réel, et p un nombre premier rationnel fixé qui ne se ramifie pas dans K. On notera K_n le sous-corps de degré p^n sur K de la $\mathbb{Z}_p$-extension cyclotomique de K. Pour $m \geq n \geq 0$ on notera N_n^m la norme de K_m à K_n. Si G est un groupe et si M est un $\mathbb{Z}[G]$-module on notera χ_M^G son caractère (i.e. la trace de la représentation linéaire de G donnée par $M \otimes \mathbb{Q}$), et M^G le sous-module des G-invariants de M.

Définition 2.1. *A un couple (K, n) où K est un corps abélien réel de conducteur non divisible par p et n est un entier naturel, on associe le sous-module de $K_n^\times$, noté $\mathcal{D}_n(K)$ et engendré comme $\mathbb{Z}[G_{K_n}]$-module par les entiers algébriques :*

$$N^{\mathbb{Q}(\zeta_{qp^n m})}_{\mathbb{Q}(\zeta_{qp^n m})\cap K_n}(1-\zeta_{qp^n m}),\ m \in \mathbb{N},\ m \mid \mathrm{cond}(K),\ \textit{si } n \neq 0$$

$$\textit{et par } p \textit{ et } N^{\mathbb{Q}(\zeta_m)}_{\mathbb{Q}(\zeta_m)\cap K}(1-\zeta_m),\ m \in \mathbb{N}, m > 2,\ m \mid \mathrm{cond}(K),\ \textit{si } n = 0$$

Remarque 2.2. *Ces entiers sont des p-unités si $n \neq 0$, égaux à p ou à une* $\mathrm{cond}(K)$*-unité si $n = 0$.*

II.2 Propriétés élémentaires.

Une bonne façon de décrire ce module $\mathcal{D}_n(K)$, consiste, comme c'est fait dans le rapport de Gillard, à parler d'unités cyclotomiques nouvelles. En effet le Lemme 2.3 (3) ci-dessous montre que $\mathcal{D}_n(K)$ décrit les unités cyclotomiques de K_n qui ne sont pas dans $C(K)$.

Lemme 2.3. *Soit n un entier positif ou nul, on a :*

(1) *Tout élément de $\mathcal{D}_n(K)$ est totalement positif.*
(2) $C(K) = \{\pm 1\} \times (\mathcal{D}_0(K) \cap E(K))$
(3) *Si $n \neq 0$, alors $C(K_n) = C(K)\ (\mathcal{D}_n(K) \cap E(K_n))$.*
(4) *Si $n \neq 0$, alors $N_0^n(\mathcal{D}_n(K)) = p^{\mathbb{Z}} \times (\mathcal{D}_0(K))^{1-\left(\frac{K}{p}\right)}$*

(5) *Pour tout n, on a* $\mathcal{D}_n\,(K) \cap E(K_n) = \ker N_{\mathbb{Q}}^{K_n} \cap \mathcal{D}_n\,(K)$

Démonstration :
(1)
Comme K_n est totalement réel et que chaque générateur de $\mathcal{D}_n\,(K)$ est une norme depuis un corps totalement imaginaire vers un sous-corps de K_n, (1) est vrai pour un système générateur de $\mathcal{D}_n\,(K)$ donc pour chaque élément de $\mathcal{D}_n\,(K)$.

Dans (2) et (3) l'inclusion du groupe de droite dans le groupe de gauche provient directement des définitions. On vérifie les deux inclusions réciproques.
(2)
Un élément ϵ de $C(K)$ est une unité qui peut s'écrire:

$$\text{(i)} \qquad \epsilon = \pm \prod_{m} \prod_{m \nmid a} N_{\mathbb{Q}(\zeta_m)\cap K}^{\mathbb{Q}(\zeta_m)} (1-\zeta_m^a)^{x(m,a)}$$

où $m,\ a,\ x(m,a)$ sont des entiers, et où les $x(m,a)$ sont presque tous nuls.

Les identités du lemme I.3 et la transitivité de la norme donnent l'existence d'éléments y_m de $\mathbb{Z}[G_K]$ et d'entiers s_m divisant m qui vérifient :

$$N_{\mathbb{Q}(\zeta_m)\cap K}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m) = \begin{cases} N_{\mathbb{Q}(\zeta_d)\cap K}^{\mathbb{Q}(\zeta_d)}(1-\zeta_d)^{y_m} \text{ si } \operatorname{pgcd}(m, \operatorname{cond}(K)) = d \text{ et } d \neq 1 \\ s_m \text{ si } \operatorname{pgcd}(m, \operatorname{cond}(K)) = 1 \end{cases}$$

On constate donc que (i) se réécrit:

$$\epsilon = \pm \prod_{m|\operatorname{cond}(K)} N_{\mathbb{Q}(\zeta_m)\cap K}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^{x_m}\ s$$

où s est un nombre rationnel de valuation nulle en tout premier divisant $\operatorname{cond}(K)$, et où les x_m sont des éléments de $\mathbb{Z}[G_K]$. De plus si $\mathcal{L}$ est un idéal premier de K ne divisant pas $\operatorname{cond}(K)$, et si $v_{\mathcal{L}}$ désigne sa valuation sur K, on a (voir remarque 2.2):

$$0 = v_{\mathcal{L}}(\epsilon) - v_{\mathcal{L}}\left(\prod_{m|\operatorname{cond}(K)} N_{\mathbb{Q}(\zeta_m)\cap K}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^{x_m}\right) = v_{\mathcal{L}}(s)$$

ce qui donne $s \in \{\pm 1\}$ puis :

$$\pm\epsilon = \prod_{m|\operatorname{cond}(K)} N_{\mathbb{Q}(\zeta_m)\cap K}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^{x_m} \in \mathcal{D}_0\,(K) \cap E(K)$$

On peut aussi remarquer que le générateur p n'intervient pas ici. $\square$
(3)
Soit $\epsilon \in C(K_n)$. De même que dans la preuve de (2) ϵ peut s'écrire :

$$\text{(ii)} \qquad \epsilon = \pm \prod_{m|qp^n \operatorname{cond}(K)} N_{\mathbb{Q}(\zeta_m)\cap K_n}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^{x_m}$$

Pour des $x_m \in \mathbb{Z}[G_{K_n}]$. En séparant les indices m divisibles par p de ceux qui divisent $\operatorname{cond} K$ et en utilisant les identités (vraies pour $n \geq s \geq 0$ et pour tout $f \in \mathbb{N},\ f \neq 0$) :

$$N_{\mathbb{Q}(\zeta_{qp^s f})}^{\mathbb{Q}(\zeta_{qp^n f})}(1-\zeta_{qp^n f}) = (1-\zeta_{qp^s f})$$

on peut réécrire (ii) comme suit :

$$\epsilon = \pm \prod_{m|\operatorname{cond}(K)} N_{\mathbb{Q}(\zeta_m)\cap K_n}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^{x_m} \prod_{m|\operatorname{cond}(K)} N_{\mathbb{Q}(\zeta_{qp^n m})\cap K_n}^{\mathbb{Q}(\zeta_{qp^n m})}(1-\zeta_{qp^n m})^{y_m}$$

Or d'une part le premier produit est une $\operatorname{cond} K$-unités et d'autre part le second produit est une p-unité. Comme $p \nmid \operatorname{cond} K$ et comme ϵ est une unité, les deux produits sont deux unités. Donc le premier produit est un élément de $C(K)$, tandis que le second est un élément de $\mathcal{D}_n(K) \cap E(K)$, ce qui prouve (3). $\square$

(4) Pour $m \mid \operatorname{cond} K,\ m \neq 1$, on a :

$$\begin{aligned} N_0^n\left(N_{K_n\cap\mathbb{Q}(\zeta_{mqp^n})}^{\mathbb{Q}(\zeta_{mqp^n})}(1-\zeta_{mqp^n})\right) &= N_{K\cap\mathbb{Q}(\zeta_m)}^{\mathbb{Q}(\zeta_{mqp^n})}(1-\zeta_{mqp^n}) \\ &= N_{K\cap\mathbb{Q}(\zeta_m)}^{\mathbb{Q}(\zeta_m)}\left(N_{\mathbb{Q}(\zeta_m)}^{\mathbb{Q}(\zeta_{mqp^n})}(1-\zeta_{mqp^n})\right) \\ &= N_{K\cap\mathbb{Q}(\zeta_m)}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^{\left(1-\left(\frac{\mathbb{Q}(\zeta_m)}{p}\right)^{-1}\right)} \\ &= N_{K\cap\mathbb{Q}(\zeta_m)}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^{\left(1-\left(\frac{K}{p}\right)^{-1}\right)} \end{aligned}$$

D'autre part on a aussi :

$$N_0^n N_{K_n\cap\mathbb{Q}(\zeta_{qp^n})}^{\mathbb{Q}(\zeta_{qp^n})}(1-\zeta_{qp^n}) = N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{qp^n})}(1-\zeta_{qp^n}) = p$$

On constate donc qu'un système de générateurs de $\mathcal{D}_n(K)$ s'envoie par N_0^n sur un système de générateurs du module :

$$p^{\mathbb{Z}} \times (\mathcal{D}_0(K))^{\left(1-\left(\frac{K}{p}\right)^{-1}\right)} = p^{\mathbb{Z}} \times (\mathcal{D}_0(K))^{\left(1-\left(\frac{K}{p}\right)\right)}$$

Ce qui prouve (4). $\square$

(5)

L'inclusion du groupe de gauche dans celui de droite se déduit directement de (1) et l'inclusion réciproque vient de l'identité:

$$v(\epsilon^{\#G_{K_n}}) = v(N_{\mathbb{Q}}^{K_n}(\epsilon))$$

qui est vraie pour tout ϵ de $\mathcal{D}_n(K)$ et toute valuation non archimédienne de v de K_n. En effet si m est un entier naturel divisible par au moins deux premiers distincts, $1-\zeta_m$ est une unité. Si par contre $m = l^n$ avec l premier, $n \geq 1$ si $l \neq 2$ et $n > 1$ sinon, $1-\zeta_m$ est alors un générateur de l'unique idéal premier de $\mathbb{Q}(\zeta_m)$ divisant l (ce dernier étant totalement ramifié dans $\mathbb{Q}(\zeta_m)$). Dans tous les cas, et pour tout $g \in G_{K_n}$, $N_{\mathbb{Q}(\zeta_m)\cap K}^{\mathbb{Q}(\zeta_m)}(1-\zeta_m)^g$ vérifie notre identité. $\square$

On peut maintenant calculer le caractère de la représentation linéaire de G_{K_n} donnée par $\mathcal{D}_n(K) \otimes \mathbb{Q}$.

Proposition 2.4.
(1) *Soient n un entier naturel, $n \neq 0$, et $K_{\mathrm{dec}} = K^{\langle(\frac{K}{p})\rangle}$ le corps de décomposition de p dans K on a:*

$$\chi_{\mathcal{D}_n(K)}^{G_{K_n}} = \chi_{\mathbb{Z}[G_{K_n}]}^{G_{K_n}} - \chi_{\mathbb{Z}[G_{K_{\mathrm{dec}}}]}^{G_{K_n}} + \chi_{\mathbb{Z}}^{G_{K_n}}$$

(2) *Toujours pour $n \neq 0$ on a :*

$$\chi_{N_0^n(\mathcal{D}_n(K))}^{G_{K_n}} = \chi_{\mathbb{Z}[G_K]}^{G_{K_n}} - \chi_{\mathbb{Z}[G_{K\mathrm{dec}}]}^{G_{K_n}} + \chi_{\mathbb{Z}}^{G_{K_n}}$$

(3) *Soit $\mathcal{P}(K)$ l'ensemble des diviseurs premiers de $\mathrm{cond}(K)$ on a:*

$$\chi_{\mathcal{D}_0(K)}^{G_K} = \chi_{\mathbb{Z}[G_K]}^{G_K} + \#\mathcal{P}(K)\chi_{\mathbb{Z}}^{G_K}$$

Corollaire 2.5. *Soient $f = [K : K_{\mathrm{dec}}]$ et $g = [K_{\mathrm{dec}} : \mathbb{Q}]$. Si $n \neq 0$ on a:*

$$\dim_{\mathbb{Q}}(\mathcal{D}_n\,(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = \chi_{\mathcal{D}_n(K)}^{G_{K_n}}(1) = gfp^n - g + 1,$$

$$\dim_{\mathbb{Q}}(N_0^n(\mathcal{D}_n\,(K)) \otimes_{\mathbb{Z}} \mathbb{Q}) = \chi_{N_0^n(\mathcal{D}_n(K))}^{G_{K_n}}(1) = gf - g + 1$$

En outre on a:

$$\dim_{\mathbb{Q}}(\mathcal{D}_0\,(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = gf + \#\mathcal{P}(K)$$

Démonstration de 2.4 (1) : Le théorème de Dirichlet donne pour tout sous-corps F de K_n:

(ii)
$$\chi_{E(F)}^{G_{K_n}} = \chi_{\mathbb{Z}[G_F]}^{G_{K_n}} - \chi_{\mathbb{Z}}^{G_{K_n}}$$

Donc 2.4 (1) est une conséquence de l'exactitude des suites suivantes:

$$1 \to (\ker N_0^n \cap E(K_n)) \otimes \mathbb{Q} \longrightarrow \mathcal{D}_n\,(K) \otimes \mathbb{Q} \longrightarrow \left(p^{\mathbb{Z}} \times (\ker N_{K_{\mathrm{dec}}}^K \cap E(K))\right) \otimes \mathbb{Q} \longrightarrow 1$$

$$1 \longrightarrow (\ker N_0^n \cap E(K_n)) \otimes \mathbb{Q} \longrightarrow E(K_n) \otimes \mathbb{Q} \xrightarrow{N_0^n} E(K) \otimes \mathbb{Q} \longrightarrow 1$$

$$1 \longrightarrow \left(\ker N_{K_{\mathrm{dec}}}^K \cap E(K)\right) \otimes \mathbb{Q} \longrightarrow E(K) \otimes \mathbb{Q} \xrightarrow{N_{K_{\mathrm{dec}}}^K} E(K_{\mathrm{dec}}) \otimes \mathbb{Q} \longrightarrow 1$$

L'exactitude des deux dernières suites est immédiate. Pour obtenir la première suite exacte on part de :

$$1 \longrightarrow \ker N_0^n \cap \mathcal{D}_n\,(K) \longrightarrow \mathcal{D}_n\,(K) \longrightarrow N_0^n\,(\mathcal{D}_n\,(K)) \longrightarrow 1$$

Ensuite on utilise le fait que $C(K)$ est d'indice fini dans $E(K)$ dont on tire :

(*) Pour tout corps abélien F : $C(F) \otimes \mathbb{Q} = E(F) \otimes \mathbb{Q}$

Et par tensorisation avec $\mathbb{Q}$ on déduit notre suite exacte des identités qui suivent.

$$\Big(\ker N_K^{K_n} \cap E(K_n)\Big) \otimes \mathbb{Q} = \Big(\ker N_K^{K_n} \cap C(K_n)\Big) \otimes \mathbb{Q} \quad \text{d'après } (*)$$
$$= \Big(\ker N_K^{K_n} \cap (C(K)(\mathcal{D}_n(K) \cap E(K_n)))\Big) \otimes \mathbb{Q}$$

d'après 2.3 (3)

$$= \Big(\ker N_K^{K_n} \cap E(K_n) \cap \mathcal{D}_n(K)\Big) \otimes \mathbb{Q}$$

car $\forall x \in C(K)$ on a $N_K^{K_n}(x) = x^{p^n}$

$$= \Big(\ker N_K^{K_n} \cap \mathcal{D}_n(K)\Big) \otimes \mathbb{Q} \text{ d'après 2.3 (5)}$$

Ce qui donne l'exactitude à gauche de $\mathcal{D}_n(K)$. D'autre part on a :

$$N_K^{K_n}(\mathcal{D}_n(K)) \otimes \mathbb{Q} = \Big(p^{\mathbb{Z}} \times (\mathcal{D}_0(K))^{1-\left(\frac{K}{p}\right)}\Big) \otimes \mathbb{Q} \text{ d'après 2.2 (4)}$$
$$= \big(p^{\mathbb{Z}} \times (\ker N_{K_{\mathrm{dec}}}^{K} \cap \mathcal{D}_0(K))\big) \otimes \mathbb{Q}$$

car $H^1(\langle \left(\frac{K}{p}\right) \rangle, \mathcal{D}_0(K))$ est fini

$$= (p^{\mathbb{Z}} \times (\ker N_{K_{\mathrm{dec}}}^{K} \cap C(K))) \otimes \mathbb{Q}$$

d'après 2.3 (2) et (5)

$$= (p^{\mathbb{Z}} \times (\ker N_{K_{\mathrm{dec}}}^{K} \cap E(K))) \otimes \mathbb{Q} \text{ d'après } (*)$$

Ce qui donne l'exactitude à droite de $\mathcal{D}_n(K)$ et conclut cette preuve. $\square$
Démonstration de 2.4 (2) : C'est une conséquence évidente de (1) $\square$
Démonstration de 2.4 (3) : 2.3 (5), 2.3 (2), 1.3 et $(*)$ donnent la suite:

$$1 \longrightarrow E(K) \otimes \mathbb{Q} \longrightarrow \mathcal{D}_0(K) \otimes \mathbb{Q} \xrightarrow{N_{\mathbb{Q}}^{K}} \left(p^{\mathbb{Z}} \times \prod_{l \in \mathcal{P}(K)} l^{\mathbb{Z}}\right) \otimes \mathbb{Q} \longrightarrow 1$$

ce qui avec (ii) démontre 2.4 (3). $\square$

Proposition 2.6. *Le lemme I.3 donne, pour chaque couple d'entiers strictement positifs m et n, les inclusions :*

$$N_{K_n}^{K_{m+n}}(\mathcal{D}_{m+n}(K) \cap E(K_{m+n})) \subset \mathcal{D}_n(K) \cap E(K_n)$$

On désigne la limite projective relativement aux applications normiques des modules :

$(\mathcal{D}_n(K) \cap E(K_n)) \otimes \mathbb{Z}_p$ (resp. $C(K_n) \otimes \mathbb{Z}_p$) par $\varprojlim ((\mathcal{D}_n(K) \cap E(K_n)) \otimes \mathbb{Z}_p)$ (resp. $\varprojlim (C(K_n) \otimes \mathbb{Z}_p)$) On a :

$$\varprojlim ((\mathcal{D}_n(K) \cap E(K_n)) \otimes \mathbb{Z}_p) = \varprojlim (C(K_n) \otimes \mathbb{Z}_p)$$

Démonstration : Le lemme 2.3 (3) et l'exactitude à gauche de $\varprojlim$ donnent l'inclusion $\subset$. Pour vérifier l'inclusion réciproque on utilise quelques notations supplémentaires. On note $E^1(K_n)$ les éléments de $E(K_n)$ congrus à 1 modulo tout premier divisant p. Pour tout premier $\mathfrak{L}$ de K_n on note $U^1_{\mathfrak{L}}$ les unités principales du localisé de K_n en $\mathfrak{L}$. Soit $\wp_i$, $1 \leq i \leq g$ les premiers de K qui divisent p et pour tout n soit $\mathfrak{P}_{i,n}$ le premier de K_n qui divise $\wp_i$. On utilise ici la conjecture de Léopoldt (démontrée dans [Br] pour les corps abéliens) et on identifie $E(K_n) \otimes \mathbb{Z}_p = E^1(K_n) \otimes \mathbb{Z}_p$ avec un sous-$\mathbb{Z}_p[\mathrm{Gal}(K_n/K_{\mathrm{dec}})]$-module du produit $\prod_i U^1_{\mathfrak{P}_{i,n}}$. Soit maintenant $(\epsilon_n)_n$ une suite cohérente en norme avec $\epsilon_n \in C(K_n) \otimes \mathbb{Z}_p$, alors le lemme 2.3 (3) donne l'existence pour tout $n \in \mathbb{N}$ d'un $x_n \in C(K) \otimes \mathbb{Z}_p$ et d'un $x'_n \in (\mathcal{D}_n(K) \cap E(K_n)) \otimes \mathbb{Z}_p$ vérifiant : $\epsilon_n = x_n x'_n$. Ici la théorie du corps de classe locale donne pour tout n : $N^{K_n}_{K_{\mathrm{dec}}}(\epsilon_n) = 1 \otimes 1$. Il suit :

$$1 \otimes 1 = N^{K_n}_{K_{\mathrm{dec}}}(\epsilon_n) = N^{K_n}_{K_{\mathrm{dec}}}(x_n x'_n) = N^{K}_{K_{\mathrm{dec}}}(x_n^{p^n}) \text{ d'après 2.3 (4)}$$

Ainsi pour chaque $n \in \mathbb{N}$, comme $U^1_{\mathfrak{P}_{i,n}}$ ne contient pas de racines q^{ieme} de l'unité, on a $N^K_{K_{\mathrm{dec}}}(x_n) \in \{\pm 1 \otimes 1\}$.

En outre $C(K)^{1-\left(\frac{K}{p}\right)}$ est d'indice fini dans $\ker N^K_{K_{\mathrm{dec}}} \cap C(K)$, donc le lemme 2.3 (2) assure l'existence d'un entier m, indépendant de n, tel que :

$$x_n^{p^m} \in \mathcal{D}_0(K)^{1-\left(\frac{K}{p}\right)} \otimes \mathbb{Z}_p$$

Pour un n dorénavant fixé on a ici :

$$\epsilon_n = N^{K_{m+n}}_{K_n}(x_{m+n}x'_{m+n}) = x^{p^m}_{m+n} N^{K_{m+n}}_{K_n}(x'_{m+n}) \in (\mathcal{D}_n(K) \cap E(K_n)) \otimes \mathbb{Z}_p$$

En effet l'inclusion $\mathcal{D}_0(K)^{1-\left(\frac{K}{p}\right)} \subset \mathcal{D}_n(K)$ a déjà été prouvée en 2.3 (4) tandis que $\mathcal{D}_0(K)^{1-\left(\frac{K}{p}\right)} \subset E(K)$ est une conséquence de 2.3 (5). $\square$

III Une présentation galoisienne de $\mathcal{D}_n(K)$

III.1 Notations, énoncé du résultat principal.

A partir d'ici, on désigne par $\mathcal{P} = \mathcal{P}(K)$ l'ensemble des nombres premiers divisant cond(K) Pour $l \in \mathcal{P}$ on notera l^{e_l} l'exacte puissance de l qui divise cond(K).

Pour deux entiers naturels, $m \geq n$, on désigne par G_n^m le groupe $\mathrm{Gal}(\mathbb{B}_m/\mathbb{B}_n)$ qui s'identifie avec $\mathrm{Gal}(K_m/K_n)$. C'est un groupe cyclique d'ordre p^{m-n}. On notera $N_n^m \in \mathbb{Z}[G_n^m]$ l'élément : $N_n^m = \sum_{g \in G_n^m} g$.

Si G est un groupe abélien, on notera $\widehat{G}$ l'ensemble de ses caractères irréductibles sur $\mathbb{C}$, que l'on identifie avec le groupe des homomorphismes de G dans $\mathbb{C}^\times$. Si $n \in \mathbb{N}$ et si L est un sous-corps de K_n on identifiera $\widehat{G}_L$ avec le sous-groupe de $\widehat{G}_{K_n}$ constitué des $\chi \in \widehat{G}_{K_n}$ dont le noyau contient $\mathrm{Gal}(K_n/L)$. Si $\chi \in \widehat{G}$, on notera

$e_\chi = \frac{1}{\#G} \sum_{g \in G} \chi(g^{-1})g$, l'idempotent de $\mathbb{C}[G]$ associé à χ. Dans toute la suite on notera additivement la multiplication dans $\mathbb{C}^\times$.

Définition 3.1 (et notation). *A un couple (J, n) où $J \subset \mathcal{P}$ et $n \in \mathbb{N}$, on associe les objets :*

(1)
$$\begin{cases} d_J = \prod_{l \in J} l^{e_l}; \\ \xi_n(J) = \zeta_{qp^n d_J} \ \textit{si } n \neq 0; \\ \xi_0(J) = \zeta_{d_J} \end{cases}$$

(2)
$$\begin{cases} K_n(J) \overset{\text{def.}}{=} K_n \cap \mathbb{Q}(\xi_n(J)) = (K \cap \mathbb{Q}(\xi_0(J)))_n \\ K(J) \overset{\text{def.}}{=} K_0(J) \\ G(J) \overset{\text{def.}}{=} G_{K(J)} \\ K_{\mathrm{dec}}(J) \overset{\text{def.}}{=} K_{\mathrm{dec}} \cap K(J) = (K(J))_{\mathrm{dec}} \end{cases}$$

(3)
$$\begin{cases} \epsilon_n(J) = N_{K_n(J)}^{\mathbb{Q}(\xi_n(J))}(1 - \xi_n(J)) \ \textit{si } n \neq 0 \ \textit{ou } J \neq \emptyset \\ \epsilon_0(\emptyset) = p \end{cases}$$

Remarque 3.2. *Il est bien connu que pour I et J contenus dans $\mathcal{P}$ et tout $n \in \mathbb{N}$ on a :*

$$\mathbb{Q}(\xi_n(J)) \cap \mathbb{Q}(\xi_n(I)) = \mathbb{Q}(\xi_n(I \cap J))$$

Il suit directement :

$$K_n(J) \cap K_n(I) = K_n(I \cap J) \quad \textit{et} \quad K_{\mathrm{dec}}(J) \cap K_{\mathrm{dec}}(I) = K_{\mathrm{dec}}(I \cap J)$$

Remarque 3.3. *On voit immédiatement que* $\epsilon_n(J) \in \mathcal{D}_n(K(J)) + \mathbb{Q}^\times$ *. On montrera plus tard que* $\{\epsilon_n(I)\,; I \subset J\}$ *est un système* $\mathbb{Z}[G_{K_n}]$*-générateur de* $\mathcal{D}_n(K(J))$ *si* $n \neq 0$ *ou de*

$$\mathcal{D}_0(K(J)) \oplus \bigoplus_{\substack{l \in J \\ l \nmid \mathrm{cond}(K(J))}} \mathbb{Z}\, l \quad \textit{sinon} .$$

Pour la suite, on aura besoin d'une relation d'ordre sur l'ensemble des sous-ensembles de $\mathcal{P}$. Celle-ci doit être totale et prolonger l'inclusion. On choisit la relation d'ordre correspondant à l'ordre archimédien sur les d_J (qui est totale et prolonge la divisibilité).

Plus formellement on pose :

Définition 3.4. $I \prec J \iff d_I \leq d_J$

Jusqu'à la fin de ce chapitre, tous les homomorphismes utilisés seront des homomorphismes de $\mathbb{Z}[G_{K_n}]$-modules et on identifie ce dernier anneau avec $\mathbb{Z}[G_K] \otimes_{\mathbb{Z}} \mathbb{Z}[G_0^n]$. Si M est un $\mathbb{Z}[G_{K_n}]$-module et F une partie non vide de M, on notera $\langle F\rangle_M$ ou $\langle F\rangle$, s'il n'y a pas d'ambiguïté possible, le sous-module de M engendré sur $\mathbb{Z}[G_{K_n}]$ par les éléments de F. On définit maintenant les objets nécessaires à l'énoncé du résultat principal de ce chapitre.

Définition 3.5. *Soient* $J \subset \mathcal{P}$ *et* $n \in \mathbb{N}$
(1) *Soit* $l \in J$*, on notera* $N_l^J \in \mathbb{Z}[G(J)]$ *l'élément :*

$$N_l^J = \sum_{g \in \mathrm{Gal}(K(J)/K(J-\{l\}))} g$$

(2) *Soit* $(w_n(I))_{I \subset \mathcal{P}}$ *un ensemble de symboles en bijection avec les sous-ensembles de* $\mathcal{P}$*, on forme la somme :*

$$\mathcal{L}_n(J) = \bigoplus_{\substack{I \subset \mathcal{P} \\ I \prec J}} (\mathbb{Z}[G(I)] \otimes \mathbb{Z}[G_0^n]) w_n(I)$$

et pour $J' \prec J$ *on considère* $\mathcal{L}_n(J')$ *comme un sous-*$\mathbb{Z}[G_K] \otimes \mathbb{Z}[G_0^n]$*-module (facteur direct) de* $\mathcal{L}_n(J)$
(3) *Soit* $l \in J$ *on définit* $R_n(J,l) \in \mathcal{L}_n(J)$ *par :*

$$\begin{aligned} R_n(J,l) =& 0 \ \textit{si } n = 0 \quad \textit{et} \quad J = \{l\} \\ R_n(J,l) =& (N_l^J \otimes 1) w_n(J) - w_n(J - \{l\}) \\ & + \left(\left(\frac{K(J-\{l\})}{l} \right)^{-1} \otimes \left(\frac{\mathbb{B}_n}{l} \right)^{-1} \right) w_n(J - \{l\}) \\ & \textit{sinon} \end{aligned}$$

(4) *On définit* $v_n(J) \in \mathbb{Z}[G(J)] \otimes \mathbb{Z}[G_0^n]$ *par :*

$$v_0(J) = 0;\ v_n(\emptyset) = 0; v_n(J) = N_{K_{\mathrm{dec}}(J)}^{K(J)} \otimes N_0^n \ \textit{si}\ n \neq 0 \quad \textit{et} \quad J \neq \emptyset$$

(5) *On désignera par* $\mathcal{H}_n(J)$ *le sous-*$\mathbb{Z}[G_K] \otimes \mathbb{Z}[G_0^n]$*-module de* $\mathcal{L}_n(J)$ *engendré par les* $R_n(I, l)$ *suivants :*

$$\mathcal{H}_n(J) = \langle \{R_n(I, l) : I \subset \mathcal{P}, I \prec J, l \in I\} \rangle$$

(6) *On désignera par* $\mathcal{V}_n(J)$ *le sous-*$\mathbb{Z}[G_K] \otimes \mathbb{Z}[G_0^n]$*-module de* $\mathcal{L}_n(J)$ *engendré par les éléments suivants :*

$$\mathcal{V}_n(J) = \langle \{v_n(I)\, w_n(I) : I \subset \mathcal{P}, I \prec J\} \rangle$$

Le résultat principal de ce chapitre est :

Théorème 3.6. *Soit* $J \subset \mathcal{P}$*, soit* $n \in \mathbb{N}$ *et soit*

$$\alpha_n(J) \ : \ \mathcal{L}_n(J) \longrightarrow \mathcal{D}_n(K)$$

définie par $\mathbb{Z}[G_K] \otimes \mathbb{Z}[G_0^n]$*-linéarité avec*
$\forall I \prec J \quad w_n(I) \longmapsto \epsilon_n(I)$.
Pour tout $I \subset \mathcal{P}$*, l'action de* G_K *sur* $\epsilon_n(I)$ *se factorise par* $G(I)$*. Donc* $\alpha_n(J)$ *est bien défini, et on a :*

$$\mathcal{D}_n(K(J)) \subset \operatorname{Im} \alpha_n(J)\,, \textit{et}\ (\mathcal{H}_n(J) + \mathcal{V}_n(J)) \subset \ker \alpha_n(J)\,,$$

De plus il existe un entier non nul z_J *tel que :*

$$z_J \ \ker \alpha_n(J) \subset (\mathcal{H}_n(J) + \mathcal{V}_n(J))$$

Remarque 3.7. *Dans le chapitre V, on introduira l'hypothèse H.B portant sur* K *et un nombre premier. Pour* $n = 0$*, on peut choisir les* z_J *étrangers à tout premier satisfaisant cette hypothèse avec* K*. En particulier, il suivra de l'étude faite dans le chapitre VI, que l'on peut supposer que les* z_J *ne sont divisibles que par les (puissances des) nombres premiers divisant* $[K : \mathbb{Q}]$*, au moins pour* $n = 0$.

La vérification de cette dernière remarque se fera aussitôt après que l'on aura énoncé l'hypothèse B, en début du chapitre V.

Démonstration de 3.6 : On réduit ici la preuve de 3.6 à un calcul de rang que l'on fait en fin de chapitre. Les deux inclusions sont des conséquences des lemmes 3.9 et 3.10 qui suivent. On se préoccupe ici de trouver des z_J convenables. On utilise

$\prec$ pour faire une récurrence sur les sous-ensembles de $\mathcal{P}$. Si $J = \emptyset$ alors 3.6 suit directement des identités $\mathcal{H}_n(\emptyset) = \mathcal{V}_n(\emptyset) = \{0\}$ qui se traduisent par :

$$\frac{\mathcal{L}_n(\emptyset)}{\mathcal{H}_n(\emptyset) + \mathcal{V}_n(\emptyset)} = \mathbb{Z}[G_0^n] w_n(\emptyset)$$

Comme on a $\mathcal{D}_n(\mathbb{Q}) = \langle\{\epsilon_n(\emptyset)\}\rangle_{K_n^\times}$, La connaissance du caractère de $\mathcal{D}_n(\mathbb{Q})$ (proposition 2.4) donne que ce dernier est libre sur $\mathbb{Z}[G_0^n]$ engendré par $\epsilon_n(\emptyset)$. D'où l'isomorphisme :

$$\frac{\mathcal{L}_n(\emptyset)}{\mathcal{H}_n(\emptyset) + \mathcal{V}_n(\emptyset)} \simeq \mathcal{D}_n(\mathbb{Q})$$

Soit $I \subset \mathcal{P}$, avec $I \neq \emptyset$. On suppose que 3.6 est vrai pour $J = I'$, le précédent immédiat de I. On note M le module suivant :

$$M = \begin{cases} \dfrac{\mathbb{Z}[G(I)] \otimes \mathbb{Z}[G_0^n]}{N(I) \otimes \mathbb{Z}[G_0^n] + \langle\{v_n(I)\}\rangle} & \text{si } n \neq 0 \text{ ou } \#I > 1 \\ \mathbb{Z}[G(I)] \text{ si } n = 0 \quad \text{et} \quad \#I = 1 & \end{cases}$$

et on note $\beta_n(I)$ l'homomorphisme :

$$\begin{aligned} \beta_n(I) \;:\; M &\longrightarrow X_n(I) \\ x &\longmapsto x\epsilon_n(I) \end{aligned}$$

$\beta_n(I)$ est bien défini d'après 3.10 (2) et parce que $v_n(I)\epsilon_n(I) = 0$ en vertu de 1.3. De plus $\beta_n(I)$ est clairement surjectif. On note M_1 (resp M_2) le module $\langle\{\epsilon_n(I'') : I'' \subset \mathcal{P}, I'' \prec I'\}\rangle$ (resp. $\langle\{\epsilon_n(I'') : I'' \subset \mathcal{P}, I'' \prec I\}\rangle$) et soit $X_n(I)$ le quotient M_2/M_1, on considère le diagramme suivant :

$$\begin{tikzcd} & \dfrac{\mathcal{L}_n(I')}{\mathcal{H}_n(I') + \mathcal{V}_n(I')} \arrow[r] \arrow[d, "\bar{\alpha}_n(I')"'] & \dfrac{\mathcal{L}_n(I)}{\mathcal{H}_n(I) + \mathcal{V}_n(I)} \arrow[r, "\bar{\pi}_n(I)"] \arrow[d, "\bar{\alpha}_n(I)"'] & M \arrow[r] \arrow[d, "\beta_n(I)"'] & 1 \\ 1 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & X_n(I) \arrow[r] & 1 \end{tikzcd}$$

Les homomorphismes de la deuxième ligne sont évidemment bien définis et la suite est clairement exacte. Les applications verticales sont bien définies en factorisant les α_n. Soit $\pi_n(I) : \mathcal{L}_n(I) \longmapsto \mathbb{Z}[G(I)] \otimes \mathbb{Z}[G_0^n]$, la projection naturelle (de noyau $\mathcal{L}_n(I')$) qui envoie $\mathcal{H}_n(I) + \mathcal{V}_n(I)$ surjectivement dans $N(I) \otimes \mathbb{Z}[G_0^n] + v_n(I)$ si $n \neq 0$ ou $\#I \geq 2$ (resp. dans $\{0\}$ si $n = 0$ et $\#I = 1$). En passant aux quotients on obtient la première ligne (exacte), et le diagramme commute clairement. Le lemme du serpent donne la suite :

$$\frac{\ker \alpha_n(I')}{\mathcal{H}_n(I') + \mathcal{V}_n(I')} \longrightarrow \frac{\ker \alpha_n(I)}{\mathcal{H}_n(I) + \mathcal{V}_n(I)} \longrightarrow \ker \beta_n(I) \longrightarrow 1$$

dont le premier terme est fini par récurrence. Pour conclure cette preuve il suffit de montrer que les rangs sur $\mathbb{Z}$ de M et de $X_n(I)$ coïncident, ce qui entraîne la finitude de $\ker \beta_n(I)$ et donc de $\ker \bar{\alpha}_n(I)$. Pour vérifier cette égalité on est amené à introduire d'autres définitions.

III.2 Préparation.

Définition 3.8. *Soit* $J \subset \mathcal{P}$
(1) *On notera* g_J *l'entier :* $g_J = [K_{\text{dec}}(J) : \mathbb{Q}]$
(2) *On notera* f_J *l'entier :* $f_J = [K(J) : K_{\text{dec}}(J)]$
(3) *Si* $n \neq 0$ *on notera* $f_n(J)$ *l'entier :* $f_n(J) = g_J f_J p^n - g_J$
(4) *On appellera idéal normique associé à* J*, et on notera* $N(J)$*, le sous-module de* $\mathbb{Z}[G(J)]$ *engendré par tous les* N_l^J*, en faisant parcourir* J *à* l*.*
(5) *On désignera par* $X_n(J)$ *le module quotient :*

$$X_n(J) = \frac{\langle\{\epsilon_n(J)\}\rangle_{K_n^\times}}{\langle\{\epsilon_n(I) : I \subset \mathcal{P}, I \prec J, I \neq J\}\rangle_{K_n^\times} \cap \langle\{\epsilon_n(J)\}\rangle_{K_n^\times}}$$

(6) *Si* $I \subset J \subset \mathcal{P}$ *on désignera par* $X_n(I, J)$ *le module quotient :*

$$X_n(I,J) = \frac{\langle\{\epsilon_n(I)\}\rangle_{K_n^\times}}{\langle\{\epsilon_n(L) : L \subset J, L \prec I, L \neq I\}\rangle_{K_n^\times} \cap \langle\{\epsilon_n(I)\}\rangle_{K_n^\times}}$$

(7) *Si* A *est un anneau intègre de corps des fractions* $\mathrm{Fr}(A)$ *et si* M *est un* A*-module on abrègera* $\dim_{\mathrm{Fr}(A)}(M \otimes \mathrm{Fr}(A))$ *en* $\mathrm{rang}_A M$*, et lorsque* $A = \mathbb{Z}$ *on le notera plus simplement* $\mathrm{rang}\, M$

A partir d'ici et jusqu'à la fin de la preuve de 3.6 on fixe un $n \in \mathbb{N}$.

Lemme 3.9. *Soit* $J \subset \mathcal{P}$

(1) *Si* $n \neq 0$ *alors* $\{\epsilon_n(I) : I \subset J\}$ *est un système générateur de* $\mathcal{D}_n(K(J))$
(2) $\{\epsilon_0(I) : I \subset J\}$ *est un système générateur de :*

$$\mathcal{D}_0(K(J)) \oplus \bigoplus_{\substack{l \in J \\ l \nmid \mathrm{cond}(K(J))}} \mathbb{Z}\, l$$

Démonstration : Pour $I \subset J$, on voit facilement que $\epsilon_n(I) \in \mathcal{D}_n(K(J))$, dès que $K_n(I) \neq \mathbb{Q}$. On a aussi $l \in \mathcal{D}_0(K(J))$ dès que $l \mid \mathrm{cond}(K(J))$. Cela donne une inclusion. On vérifie l'inclusion réciproque de (1). Soit $m \mid \mathrm{cond}(K(J))$, il suffit de voir que :

$$N^{\mathbb{Q}(\zeta_{qp^n m})}_{\mathbb{Q}(\zeta_{qp^n m}) \cap K_n(J)}(1 - \zeta_{qp^n m}) \in \langle\{\epsilon_n(I) : I \subset J\}\rangle$$

Soit I l'ensemble des diviseurs premiers de m, on a clairement $I \subset J$ et aussi

$$\mathbb{Q}(\zeta_{qp^n m}) \subset \mathbb{Q}(\xi_n(I))$$

Ici le lemme I.3 donne :

$$\begin{aligned} N^{\mathbb{Q}(\zeta_{qp^n m})}_{\mathbb{Q}(\zeta_{qp^n m}) \cap K_n(J)}(1 - \zeta_{qp^n m}) &= N^{\mathbb{Q}(\xi_n(I))}_{\mathbb{Q}(\zeta_{qp^n m}) \cap K_n(J)}(1 - \xi_n(I)) \\ &= N^{K_n(I)}_{\mathbb{Q}(\zeta_{qp^n m}) \cap K_n(J)}(\epsilon_n(I)) \\ &\in \langle\{\epsilon_n(I) : I \subset J\}\rangle \end{aligned}$$

Ce qui prouve (1). Un raisonnement semblable donne (2). $\square$

Lemme 3.10. *Soient I et J deux sous-ensembles de $\mathcal{P}$, on a :*
(1) $(\mathcal{H}_n(J) + \mathcal{V}_n(J)) \subset \ker \alpha_n(J)$.
(2) *Si $n \neq 0$ ou $I \cap J \neq \emptyset$ alors $N_{K_n(I)}^{K_n}(\epsilon_n(J)) \in \langle \{\epsilon_n(I \cap J)\}\rangle$. Si de plus $I \subset J$, alors on a $N_{K_n(I)}^{K_n(J)}(\epsilon_n(J)) \in \langle \{\epsilon_n(I)\}\rangle$.*
(3) *Si $I \cap J = \emptyset$ alors $N_{K(I)}^{K}(\epsilon_0(J)) \in \langle J\rangle$.*

Démonstration : C'est une conséquence immédiate des formules du lemme I.3, de la transitivité de la norme, et de la remarque 3.2. $\square$

Lemme 3.11. *Soient I et J deux sous-ensembles de $\mathcal{P}$, avec $I \subset J$, on a*
$\operatorname{rang}(X_n(I,J)) = \operatorname{rang}(X_n(I))$

Démonstration : Comme on a :

$$(\langle \{\epsilon_n(I') : I' \subset J, I' \prec I, I' \neq I\}\rangle) \subset (\langle \{\epsilon_n(I') : I' \subset \mathcal{P}, I' \prec I, I' \neq I\}\rangle)$$

l'inégalité $\operatorname{rang}(X_n(I,J)) \geq \operatorname{rang}(X_n(I))$ est évidente. Réciproquement, on a :

$$\begin{aligned}
&(\langle \{\epsilon_n(I') : I' \subset \mathcal{P}, I' \prec I, I' \neq I\}\rangle \cap \langle \{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \\
&= [K_n : K_n(I)](\langle \{\epsilon_n(I') : I' \subset \mathcal{P}, I' \prec I, I' \neq I\}\rangle \cap \langle \{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \\
&= N_{K_n(I)}^{K_n}(\langle \{\epsilon_n(I') : I' \subset \mathcal{P}, I' \prec I, I' \neq I\}\rangle \cap \langle \{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \\
&\subset (\langle \{\epsilon_n(I') : I' \subset I, I' \neq I\}\rangle \cap \langle \{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \text{ d'après } 3.10\ (2) \\
&\subset (\langle \{\epsilon_n(I') : I' \subset J, I' \prec I, I' \neq I\}\rangle \cap \langle \{\epsilon_n(I)\}\rangle) \otimes \mathbb{C}
\end{aligned}$$

car $I \subset J$ et $\prec$ prolonge $\subset$.

$\square$

III.3 Les idéaux normiques.

Proposition 3.12. *Soit $J \subset \mathcal{P}$ tel que $J \neq \emptyset$. On a :*
(1) $\operatorname{rang} N(J) = \sum_{\substack{I \subset J \\ I \neq J}} (-1)^{\#J - \#I + 1} g_I f_I$
(2) *Si $n \neq 0$ alors :*

$$\forall J \subset \mathcal{P} \ : \ \operatorname{rang}\left(\frac{\mathbb{Z}[G(J)] \otimes \mathbb{Z}[G_0^n]}{(N(J) \otimes \mathbb{Z}[G_0^n]) + \langle \{v_n(J)\}\rangle}\right) = \sum_{I \subset J} (-1)^{\#J - \#I} f_n(I)$$

Démonstration de (1) : On laisse le soin au lecteur de vérifier la formule (principe d'inclusion-exclusion) :

$$(\dagger) \qquad \# \bigcup_{s=1}^{s=t} A_s = \sum_{\substack{M \subset \{1,\ldots,s\} \\ M \neq \emptyset}} (-1)^{\#M+1} \# \bigcap_{s \in M} A_s$$

qui est vraie pour toute famille $A_1, ..., A_t$ d'ensembles contenus dans un même ensemble fini (c'est un exercice sur les ensembles finis qui peut se faire par récurrence sur t). On a :

$$\begin{aligned}
\operatorname{rang} N(J) &= \#\{\chi \in \widehat{G}(J) : \exists l \in J \text{ avec } e_\chi N_l^J \neq 0\} \\
&= \#\{\chi \in \widehat{G}(J) : \exists l \in J \text{ avec } \operatorname{Gal}(K(J)/K(J-\{l\})) \subset \ker \chi\} \\
&= \# \bigcup_{l \in J} \widehat{G}(J - \{l\}) \\
&= \sum_{\substack{L \subset J \\ L \neq \emptyset}} (-1)^{\# L + 1} \# \widehat{G}(J - L)
\end{aligned}$$

en utilisant la remarque 3.2 et le principe d'inclusion-exclusion (†). En posant $I = J - L$ on en déduit :

$$\operatorname{rang} N(J) = \sum_{\substack{I \subset J \\ I \neq J}} (-1)^{\# J - \# I + 1} g_I f_I \text{ comme attendu.} \quad \square$$

Démonstration de (2) : On a naturellement :

$$\begin{aligned}
\operatorname{rang}\left((N(J) \otimes \mathbb{Z}[G_0^n]) + \langle\{v_n(J)\}\rangle\right) = {} & \operatorname{rang}(N(J) \otimes \mathbb{Z}[G_0^n]) + \operatorname{rang}\langle\{v_n(J)\}\rangle \\
& - \operatorname{rang}\left((N(J) \otimes \mathbb{Z}[G_0^n]) \cap \langle\{v_n(J)\}\rangle\right)
\end{aligned}$$

Or on a :

$$\begin{aligned}
& \operatorname{rang}\left((N(J) \otimes \mathbb{Z}[G_0^n]) \cap \langle\{v_n(J)\}\rangle\right) \\
&= \operatorname{rang}\left(\langle\{N_{K_{\mathrm{dec}}(J)}^{K(J)} N_l^J \otimes N_0^n : l \in J\}\rangle\right) \\
& \text{car } (v_n(J))^2 \in \mathbb{Q} v_n(J) \\
&= \#\{\chi \in \widehat{G}(J) : \exists l \in J \text{ avec } \operatorname{Gal}(K(J)/K_{\mathrm{dec}}(J - \{l\})) \subset \ker \chi\} \\
&= \# \bigcup_{l \in J} \widehat{G}_{K_{\mathrm{dec}}(J - \{l\})} \\
&= \sum_{\substack{I \subset J \\ I \neq J}} (-1)^{\# J - \# I + 1} g_I
\end{aligned}$$

en utilisant à nouveau le principe d'inclusion-exclusion (†) et 3.2

Et comme $\operatorname{rang}\langle\{v_n(J)\}\rangle = g_J$, cette dernière identité et (1) montrent (2). $\square$

III.4 Suites exactes récursives.

Proposition 3.13. *Soit $J \subset \mathcal{P}$, si $n \neq 0$ alors on a :*

$$(1) \qquad \operatorname{rang}\left(\langle\{\epsilon_n(I) : I \subset J, I \neq J\}\rangle\right) = \begin{cases} 0 \ \text{si } J = \emptyset \\ 1 + \sum\limits_{\substack{I \subset J \\ I \neq J}} (-1)^{\#J - \#I + 1} f_n(I) \ \text{sinon} \end{cases}$$

$$(2) \qquad \operatorname{rang}(X_n(J)) = \begin{cases} p^n \ \text{si } J = \emptyset \\ \sum\limits_{I \subset J} (-1)^{\#J - \#I} f_n(I) \ \text{sinon} \end{cases}$$

Proposition 3.14. *Soit $J \subset \mathcal{P}$, on a :*

$$(1) \qquad \operatorname{rang}\left(\langle\{\epsilon_0(I) : I \subset J, I \neq J\}\rangle\right) = \#J + \sum_{\substack{I \subset J \\ I \neq J}} (-1)^{\#J - \#I + 1} g_I f_I \ \text{si } \#J \geq 2$$

$$(2) \qquad \operatorname{rang}(X_0(J)) = \sum_{I \subset J} (-1)^{\#J - \#I} g_I f_I \ \text{si } \#J \geq 2$$

(3)
pour $\#J < 2$: $\operatorname{rang}(p^{\mathbb{Z}}) = 1$ *et* $\operatorname{rang}(X_0(J)) = g_J f_J = 1 + \sum\limits_{I \subset J} (-1)^{\#J - \#I} g_I f_I$

Démonstration de 3.13 : Le lemme 3.9 donne un isomorphisme :

$$X_n(J, J) \cong \frac{\mathcal{D}_n(K(J))}{\langle\{\epsilon_n(I) : I \subset J, I \neq J\}\rangle}$$

et avec le lemme 3.11 et le corollaire 2.5 qui se traduit ici par : $\operatorname{rang} \mathcal{D}_n(K(J)) = 1 + f_n(J)$, on en déduit l'équivalence entre (1) et (2). On vérifie (1) par récurrence sur $\#J$. Si $J = \emptyset$ alors (1) est évident. On suppose (1) (et donc (2)) vrai pour tout $J \subset \mathcal{P}$ tel que $\#J \leq s$ et soit $J_0 \subset \mathcal{P}$ de cardinal $s + 1$. On note l l'élément de J_0 tel que $\{l\}$ soit le plus petit élément des sous-ensembles de J_0 relativement à $\prec$. D'après la définition de $X_n(I, J)$ on peut associer à chaque sous-ensemble I non vide de J_0 (ou encore à chaque générateur de $\mathcal{D}_n(K(J_0))$ hormis $\epsilon_n(\emptyset)$) la suite exacte $S_n(I)$ suivante :

$$1 \to \langle\{\epsilon_n(L) : L \subset J_0, L \prec I, L \neq I\}\rangle \to \langle\{\epsilon_n(L) : L \subset J_0, L \prec I\}\rangle \to X_n(I, J_0) \to 1$$

On peut remarquer que $S_n(\{l\})$ se lit :

$$1 \longrightarrow \langle\{\epsilon_n(\emptyset)\}\rangle \longrightarrow \langle\{\epsilon_n(\{l\}), \epsilon_n(\emptyset)\}\rangle \longrightarrow X_n(\{l\}, J_0) \longrightarrow 1$$

Les suites ci-dessus nous donnent les identités (vraies pour tout I strictement supérieur à $\{l\}$ et strictement contenu dans J_0):

$$\begin{aligned}\operatorname{rang}\left(\langle\{\epsilon_n(L) : L\subset J_0,\ L\prec I\}\rangle\right) &= \operatorname{rang}\left(\langle\{\epsilon_n(L) : L\subset J_0,\ L\prec I,\ L\neq I\}\rangle\right)\\ &\quad + \operatorname{rang}\left(X_n(I,J_0)\right)\end{aligned}$$

Donc le lemme 3.11 nous donne les identités:

$$\begin{aligned}\operatorname{rang}\left(\langle\{\epsilon_n(L) : L\subset J_0,\ L\prec I\}\rangle\right) &= \operatorname{rang}\left(\langle\{\epsilon_n(L) : L\subset J_0,\ L\prec I,\ L\neq I\}\rangle\right)\\ &\quad + \operatorname{rang}\left(X_n(I)\right)\end{aligned}$$

En regroupant toutes ces égalités on obtient:

$$\begin{aligned}&\operatorname{rang}(\langle\{\epsilon_n(I) : I\subset J_0, I\neq J_0\}\rangle)\\
&= \operatorname{rang}\left(\langle\{\epsilon_n(\emptyset),\ \epsilon_n(\{l\})\}\rangle\right) + \sum_{\substack{I\subset J_0,\ I\neq\emptyset\\ I\neq J_0,\ I\neq\{l\}}} \operatorname{rang}\left(X_n(I)\right)\\
&= p^n + \operatorname{rang} X_n(\{l\}) + \sum_{\substack{I\subset J_0,\ I\neq\emptyset\\ I\neq J_0,\ I\neq\{l\}}} \operatorname{rang}\left(X_n(I)\right)\\
&= p^n + \sum_{\substack{I\subset J_0\\ I\neq J_0,\ I\neq\emptyset}} \operatorname{rang}(X_n(I))\\
&= 1 + f_n(\emptyset) + \sum_{\substack{I\subset J_0\\ I\neq J_0,\ I\neq\emptyset}} \sum_{L\subset I} (-1)^{\#I-\#L} f_n(L)\end{aligned}$$

par récurrence

$$\begin{aligned}&= 1 + \sum_{\substack{I\subset J_0\\ I\neq J_0}} \sum_{L\subset I} (-1)^{\#I-\#L} f_n(L)\\
&= 1 + \sum_{\substack{I\subset J_0\\ I\neq J_0}} (-1)^{\#J_0-\#I+1} f_n(I)\end{aligned}$$

La dernière égalité s'obtient avec le lemme 3.15 ci-dessous, et prouve (1) pour $J = J_0$. $\square$

Lemme 3.15. *Soit $s\in\mathbb{N}$ et soit $\mathbb{R}^{\mathbb{P}(\{1,\dots,s\})}$, l'ensemble de toutes les applications de $\mathbb{P}(\{1,\dots,s\})$ dans $\mathbb{R}$. On définit une application $\phi\mapsto T_\phi$ de $\mathbb{R}^{\mathbb{P}(\{1,\dots,s\})}$ dans lui-même par :*

$$T_\phi(J) = \sum_{\substack{I\subset J\\ I\neq J}} \sum_{L\subset I} (-1)^{\#I-\#L}\phi(L).\ \textit{Alors on a :}\ T_\phi(J) = \sum_{\substack{I\subset J\\ I\neq J}} (-1)^{\#J-\#I+1}\phi(I)$$

Démonstration de 3.15 : L'identité $\sum_{I'\subset I}(-1)^{\#I'} = 0$ est vraie pour tout ensemble I fini. En effet, ce dernier contient nécessairement autant de sous-ensembles de cardinaux pairs que de sous-ensembles de cardinaux impairs. On voit alors que l'on a :

$$(-1)^{\#I+1} = \sum_{\substack{I' \subset I \\ I' \neq I}} (-1)^{\#I'}$$

Et on en tire :

$$\begin{aligned} T_\phi(J) &= \sum_{\substack{I \subset J \\ I \neq J}} \phi(I) \sum_{\substack{I' \subset J \\ I' \neq J, I \subset I'}} (-1)^{\#I' - \#I} = \sum_{\substack{I \subset J \\ I \neq J}} \phi(I) \sum_{\substack{I' \subset (J-I) \\ I' \neq (J-I)}} (-1)^{\#I'} \\ &= \sum_{\substack{I \subset J \\ I \neq J}} (-1)^{\#J - \#I + 1} \phi(I) \end{aligned}$$

□

Démonstration de 3.14 : Ici aussi on a l'équivalence entre (1) et (2), grâce au lemme 3.11 et au corollaire 2.5 qui donne les égalités :

$$\operatorname{rang}(\langle\{\epsilon_0(I) : I \subset J\}\rangle) = \operatorname{rang} \mathcal{D}_0(K(J)) \oplus \bigoplus_{\substack{l \in J \\ l \nmid \operatorname{cond} K(J)}} \mathbb{Z}\, l = g_J f_J + \#J$$

De plus (3) est immédiat et cela nous permet de démarrer une récurrence pour démontrer (1) ou (2) à partir de $\#J \geq 2$. Comme dans la preuve de 3.13 on utilise $\prec$ pour démontrer (1) par récurrence. On suppose (1) (et donc (2)) vrai pour tout $J \subset \mathcal{P}$ tel que $\#J \leq s$ et soit $J_0 \subset \mathcal{P}$ de cardinal $s+1$. On note l l'élément de J_0 tel que $\{l\}$ soit le plus petit élément des sous-ensembles de J_0 relativement à $\prec$. D'après la définition de $X_o(I, J)$ on retrouve des suites $S_0(I)$ semblables à celle de 3.13 :

$$1 \to \langle\{\epsilon_0(L) : L \subset J_0, L \prec I, L \neq I\}\rangle \to \langle\{\epsilon_0(L) : L \subset J_0, L \prec I\}\rangle \to X_0(I, J_0) \to 1$$

Une différence avec le cas $n = 0$ vient du fait que $S_0(\{l\})$ se lit :

$$1 \longrightarrow \mathbb{Z}p \longrightarrow \langle\{\epsilon_n(\{l\})\}\rangle \oplus \mathbb{Z}\, p \longrightarrow X_n(\{l\}, J_0) \longrightarrow 1$$

tandis que $S_0(J_0)$ se lit :

$$1 \longrightarrow \langle\{\epsilon_n(I) : I \subset J_0, I \neq J_0\}\rangle \longrightarrow \mathcal{D}_n(K(J_0)) \longrightarrow X_n(J_0, J_0) \longrightarrow 1$$

Les suites ci-dessus nous donnent les identités (vraies pour tout I strictement supérieur à $\{l\}$ et strictement contenu dans J_0):

$$\begin{aligned} \operatorname{rang}(\langle\{\epsilon_0(L) : L \subset J_0,\ L \prec I\}\rangle) = \operatorname{rang}(\langle\{\epsilon_0(L) : L \subset J_0,\ L \prec I,\ L \neq I\}\rangle) \\ + \operatorname{rang}(X_n(I)) \end{aligned}$$

En remplaçant $\operatorname{rang}(X_n(I, J_0))$ par $\operatorname{rang}(X_n(I))$ grâce au lemme 3.11. En regroupant toutes ces égalités, on obtient:

$$
\begin{aligned}
&\operatorname{rang}\left(\left\langle\left\{\epsilon_0\left(I\right): I \subset J_0, I \neq J_0\right\}\right\rangle\right)\\
&= 1 + \sum_{r \in J_0} \operatorname{rang}\left(X_n\left(\{r\}\right)\right) + \sum_{\substack{I \subset J_0, \# I > 1\\ I \neq J_0}} \operatorname{rang}\left(X_n\left(I\right)\right)\\
&= 1 + \# J_0 + \sum_{r \in J_0} \sum_{L \subset \{r\}} (-1)^{\#\{r\} - \# L} g_L f_L + \sum_{\substack{I \subset J_0, \# I > 1\\ I \neq J_0}} \sum_{L \subset I} (-1)^{\# I - \# L} g_L f_L
\end{aligned}
$$

en utilisant (3) et l'hypothèse de récurrence

$$
\begin{aligned}
&= 1 + \# J_0 + \sum_{\substack{I \subset J_0\\ I \neq J_0,\ I \neq \emptyset}} \sum_{L \subset I} (-1)^{\# I - \# L} g_L f_L\\
&= \# J_0 + \sum_{\substack{I \subset J_0\\ I \neq J_0}} \sum_{L \subset I} (-1)^{\# I - \# L} g_L f_L\\
&= \# J_0 + \sum_{\substack{I \subset J_0\\ I \neq J_0}} (-1)^{\# J_0 - \# I + 1} g_I f_I
\end{aligned}
$$

La dernière égalité s'obtient aussi en utilisant le lemme 3.15. Cela prouve (1) pour $J = J_0$. □

Maintenant pour terminer la preuve de 3.6, il suffit de comparer les rangs calculés en 3.12, 3.13 et 3.14. Dans tous les cas les rangs de M et de $X_n\left(I\right)$ sont égaux. □

IV $\mathbb{Z}[G_0^n]$-structure de $\mathcal{D}_n(K)$, sous les hypothèses A et B.

Dans ce chapitre on conserve les notations et conventions du chapitre III, mais les modules sont ici des $\mathbb{Z}[G_0^n]$-modules et les homomorphismes des homomorphismes de $\mathbb{Z}[G_0^n]$-modules. (On "oublie" l'action de G_K). On travaille avec les hypothèses suivantes :

Hypothèse A : $\forall J \subset \mathcal{P} \ : \ \dfrac{\mathbb{Z}[G(J)]}{N(J)}$ est sans $\mathbb{Z}$-torsion

Hypothèse B : $\forall J \subset \mathcal{P} \ : \ \dfrac{\mathbb{Z}[G(J)]}{N(J)}$ est sans p-torsion

Remarque 4.1. *Dans le cas où $n = 0$, le module $\frac{\mathbb{Z}[G(J)]}{N(J)}$ coïncide avec celui noté M dans la preuve de 3.6. On en tire aisément la preuve de la remarque 3.7*

L'hypothèse A (resp. l'hypothèse B) entraîne que $\frac{\mathbb{Z}[G(J)]}{N(J)} \otimes \mathbb{Z}[G_0^n]$ (resp. $\frac{\mathbb{Z}[G(J)]}{N(J)} \otimes \mathbb{Z}_p[G_0^n]$) est $\mathbb{Z}[G_0^n]$-libre (resp. $\mathbb{Z}_p[G_0^n]$-libre) pour tout J.

Remarque 4.2. *On a l'équivalence entre :*

$$\forall\ l \text{ premier},\ (K,l) \text{ vérifie H.B}$$

et :

$$K \text{ vérifie H.A.}$$

Remarque 4.3. *Avant d'étudier H.A ou H.B, on donne l'exemple d'un couple (K,p) qui ne vérifie pas la seconde hypothèse.*

Si on pose $K = \mathbb{Q}(\sqrt{5\ .\ 17}, \sqrt{5\ .\ 13})$ et $p = 2$, alors on a le

Lemme 4.4.

$$\frac{\mathbb{Z}[G(\mathcal{P})]}{N(\mathcal{P})} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Démonstration : Chaque générateur de $N(\mathcal{P})$ est d'augmentation paire donc $1 \notin \mathcal{P}$. Par contre on a : $2 = N_5^{\mathcal{P}} + N_{17}^{\mathcal{P}} + N_{13}^{\mathcal{P}} - N_5^{\mathcal{P}} N_{13}^{\mathcal{P}} \in N(\mathcal{P})$ et pour tout $g \in G_K$ on a aussi $1 + g \in N(\mathcal{P})$. $\square$

Dans la suite de ce chapitre on établit la conséquence suivante des hypothèses A et B :

Théorème 4.5.

(1) Si (K,p) vérifie H.B., on a :

$$\forall n \in \mathbb{N}-\{0\} \ : \ \mathcal{D}_n(K)\otimes\mathbb{Z}_p \cong (\mathbb{Z}_p[G_0^n])^r \bigoplus \left(\frac{\mathbb{Z}_p[G_0^n]}{\langle N_0^n\rangle}\right)^t$$

(2) Si de plus K vérifie H.A. on a :

$$\forall n \in \mathbb{N}-\{0\} \ : \ \mathcal{D}_n(K) \cong (\mathbb{Z}[G_0^n])^r \bigoplus \left(\frac{\mathbb{Z}[G_0^n]}{\langle N_0^n\rangle}\right)^t$$

avec $r = g_{\mathcal{P}} f_{\mathcal{P}} - g_{\mathcal{P}} + 1$ et $t = g_{\mathcal{P}} - 1$

La preuve occupe le reste de ce chapitre. Dans toute la suite $\mathcal{L}_n$, $\mathcal{H}_n$, α_n etc. signifieront $\mathcal{L}_n(\mathcal{P})$, $\mathcal{H}_n(\mathcal{P})$, $\alpha_n(\mathcal{P})$ ... En outre $\mathcal{D}_n$ signifiera $\mathcal{D}_n(K)$. On fixe un $n\in\mathbb{N}$ non nul. On suppose dans la suite de ce chapitre que (K,p) vérifie H.B. On pose $\mathcal{R}=\mathbb{Z}$ si K vérifie H.A. et $\mathcal{R}=\mathbb{Z}_p$ sinon. La preuve repose essentiellement sur la $\mathcal{R}[G_0^n]$-liberté de $\frac{\mathcal{L}_n}{\mathcal{H}_n}\otimes\mathcal{R}$.

Pour obtenir cette liberté on construit une application surjective d'un module libre dans $\frac{\mathcal{L}_n}{\mathcal{H}_n}\otimes\mathcal{R}$ en section 4.1. On vérifie (en comparant les rangs) que cette application est injective en section 4.2, et la conclusion suivra en section 4.3.

IV.1 Retour sur $\frac{\mathcal{L}_n}{\mathcal{H}_n}$.

Proposition 4.6. *Pour tout $J\subset\mathcal{P}$ il existe une surjection de $\mathcal{R}[G_0^n]$-modules :*

$$\psi_n(J) \ : \ \bigoplus_{\substack{I\subset\mathcal{P}\\ I\prec J}} \frac{\mathbb{Z}[G(I)]}{N(I)}\otimes\mathcal{R}[G_0^n] \longrightarrow \frac{\mathcal{L}_n(J)}{\mathcal{H}_n(J)}\otimes\mathcal{R}\left(=\frac{\mathcal{L}_n(J)}{\mathcal{H}_n(J)} \text{ si } K \text{ vérifie H.A.}\right)$$

Démonstration : On utilise à nouveau $\prec$ pour faire une récurrence sur J.

Pour $J=\emptyset$ on définit $\psi_n(\emptyset)$ par $\mathcal{R}[G_0^n]$-linéarité avec $1\mapsto w_n(\emptyset)$.

Soit $I\subset\mathcal{P}$ et soit I' son précédent immédiat. On suppose l'existence d'une application $\psi_n(I')$ qui satisfaisait 4.6 pour $J=I'$. On considère le diagramme suivant :

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus\limits_{\substack{I''\subset\mathcal{P}\\ I''\prec I'}} \frac{\mathbb{Z}[G(I'')]}{N(I'')}\otimes\mathcal{R}[G_0^n] \arrow[r] \arrow[d, "\bar{\psi}_n(I')"'] \arrow[dr, dashed, "\psi"'] & \bigoplus\limits_{\substack{I''\subset\mathcal{P}\\ I''\prec I}} \frac{\mathbb{Z}[G(I'')]}{N(I'')}\otimes\mathcal{R}[G_0^n] \arrow[r] \arrow[d, dashed, "\psi_n(I)"'] & \frac{\mathbb{Z}[G(I)]}{N(I)}\otimes\mathcal{R}[G_0^n] \arrow[r] \arrow[d, "\bar{\beta}"'] \arrow[dl, dashed, "\tilde{\beta}"'] & 0 \\
0 \arrow[r] & \frac{\mathcal{L}_n(I')}{\mathcal{L}_n(I')\cap\mathcal{H}_n(I)}\otimes\mathcal{R} \arrow[r] & \frac{\mathcal{L}_n(I)}{\mathcal{H}_n(I)}\otimes\mathcal{R} \arrow[r] & \frac{\mathcal{L}_n(I)}{\mathcal{H}_n(I)+\mathcal{L}_n(I')}\otimes\mathcal{R} \arrow[r] & 0
\end{tikzcd}$$

Les lignes sont évidemment exactes (celle du dessus est même scindée). $\bar{\psi}_n(I')$ est la composée de $\psi_n(I')$ avec la surjection :

$$\frac{\mathcal{L}_n\,(I')}{\mathcal{H}_n\,(I')} \otimes \mathcal{R} \longrightarrow \frac{\mathcal{L}_n\,(I')}{\mathcal{L}_n\,(I') \cap \mathcal{H}_n\,(I)} \otimes \mathcal{R}$$

Donc $\bar{\psi}_n(I')$ est surjective. $\bar{\beta}$ provient par passage au quotient de la surjection $\beta \;:\; \mathbb{Z}[G(I)] \otimes \mathcal{R}[G_0^n] \longrightarrow \frac{\mathcal{L}_n(I)}{\mathcal{L}_n(I')} \otimes \mathcal{R}$ (en remarquant que $\beta(N(I) \otimes \mathcal{R}[G_0^n]) \subset (\mathcal{H}_n\,(I) + \mathcal{L}_n\,(I')) \otimes \mathcal{R}$) et $\bar{\beta}$ est donc surjectif. La $\mathcal{R}[G_0^n]$-liberté de $\frac{\mathbb{Z}[G(I)]}{N(I)} \otimes \mathcal{R}[G_0^n]$ (provenant de H.A. ou H.B.) garantit l'existence d'un $\tilde{\beta}$ relevant $\bar{\beta}$. En posant $\psi_n(I) = \psi \oplus \tilde{\beta}$ (ψ provenant de $\bar{\psi}_n(I')$) on obtient un diagramme commutatif aux lignes exactes. Les surjectivités de $\bar{\psi}_n(I')$ et de $\bar{\beta}$ entraînent (via le lemme du serpent) celle de $\psi_n(I)$. Cela montre 4.6 pour $J = I$. $\square$

Proposition 4.7. *ψ_n est un isomorphisme. En particulier :*

$$\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R} \textit{ est } \mathcal{R}[G_0^n]\textit{-libre}$$

Démonstration : Il reste à voir que ψ_n est injective, et pour ce, que son noyau est de $\mathcal{R}$-torsion. Maintenant 4.7 est une simple conséquence de la proposition 4.8 qui fait l'objet de la section suivante. $\square$

IV.2 Un autre calcul de rang.

Proposition 4.8. *On a :*

$$\mathrm{rang}_{\mathcal{R}}\,(\mathcal{H}_n \otimes \mathcal{R}) = \mathrm{rang}_{\mathcal{R}} \left(\bigoplus_{I \subset \mathcal{P}} N(I) \otimes \mathcal{R}[G_0^n] \right) = \mathrm{rang}_{\mathcal{R}}\,(\mathcal{L}_n \otimes \mathcal{R}) - g_{\mathcal{P}} f_{\mathcal{P}} p^n$$

Et comme $\mathrm{rang}_{\mathcal{R}}\,(\mathcal{L}_n \otimes \mathcal{R}) = \mathrm{rang}_{\mathcal{R}}\,(\bigoplus \mathbb{Z}[G(I)] \otimes \mathcal{R}[G_0^n]) = \sum_{I \subset \mathcal{P}} g_I f_I p^n$ *le rang du noyau de ψ_n est nul.*

Démonstration : On calcule indépendamment les rangs de

$$\mathcal{H}_n \otimes \mathcal{R} \quad \text{et} \quad \bigoplus_{I \subset \mathcal{P}} N(I) \otimes \mathcal{R}[G_0^n]$$

dans les lemmes qui suivent. $\square$

Lemme 4.9.

$$\mathrm{rang}_{\mathcal{R}} \bigoplus_{I\subset\mathcal{P}} N(I)\otimes\mathcal{R}[G_0^n] = \mathrm{rang}_{\mathcal{R}}\,\mathcal{L}_n\otimes\mathcal{R} - g_{\mathcal{P}} f_{\mathcal{P}} p^n$$

Démonstration : On a :

$$\begin{aligned}
\mathrm{rang}_{\mathcal{R}}(\bigoplus_{I\subset\mathcal{P}} N(I)\otimes\mathcal{R}[G_0^n]) &= \sum_{I\subset\mathcal{P}}\sum_{\substack{J\subset I\\ J\neq I}}(-1)^{\#I-\#J+1} g_J f_J p^n \text{ d'après 3.12 (1)}\\
&= -\sum_{\substack{I\subset\mathcal{P}\\ I\neq\mathcal{P}}}\sum_{J\subset I}(-1)^{\#I-\#J} g_J f_J p^n + \sum_{\substack{I\subset\mathcal{P}\\ I\neq\mathcal{P}}} g_I f_I p^n\\
&- \sum_{\substack{J\subset\mathcal{P}\\ J\neq\mathcal{P}}}(-1)^{\#\mathcal{P}-\#J} g_J f_J p^n\\
&= \sum_{\substack{I\subset\mathcal{P}\\ I\neq\mathcal{P}}} g_I f_I p^n \text{ d'après 3.15}\\
&= \mathrm{rang}_{\mathcal{R}}(\mathcal{L}_n\otimes\mathcal{R}) - g_{\mathcal{P}} f_{\mathcal{P}} p^n \text{ comme annoncé.}
\end{aligned}$$

□

Le rang de $\mathcal{H}_n$ est un petit peu plus difficile à calculer. On utilise le :

Lemme 4.10.

$$\mathrm{rang}(\mathcal{V}_n) = \sum_{I\subset\mathcal{P}, I\neq\emptyset} g_I, \qquad \mathrm{rang}(N_0^n\mathcal{H}_n) = \sum_{I\subset\mathcal{P}, I\neq\mathcal{P}} g_I f_I$$

Démonstration : La première identité est facile. Pour vérifier la seconde on considère l'homomorphisme surjectif $\delta\ :\ \mathcal{L}_n \longrightarrow \mathcal{L}_0$ défini par $\mathbb{Z}[G_0^n]$-linéarité avec

$$\forall I\ \forall g\in G(I)\ :\ g\otimes 1\ w_n(I)\mapsto g\ w_0(I)$$

Il est clair que la restriction de δ réalise un isomorphisme entre $N_0^n\mathcal{L}_n$ et $p^n\mathcal{L}_0$. De plus pour tout $J\subset\mathcal{P}$ de cardinal au moins 2 et tout $l\in J$ on a $\delta(N_0^n R_n(J,l)) = p^n R_0(J,l)$, tandis que pour $J=\{l\}$ on a $\delta(N_0^n R_n(J,l)) = p^n N_l^{\{l\}} w_0(\{l\})$. Ainsi on obtient l'isomorphisme suivant :

$$N_0^n\mathcal{H}_n \overset{\delta}{\cong} p^n\mathcal{H}_0 + \bigoplus_{l\in\mathcal{P}} p^n\mathbb{Z}N_l^{\{l\}}w_0(\{l\})$$

De plus, comme $\mathcal{H}_0\subset\ker\alpha_0$ et $\alpha_0(N_l^{\{l\}}w_0(\{l\})) = l$, on a $(\delta(N_0^n\mathcal{H}_n)\cap\ker\alpha_0) = p^n\mathcal{H}_0$. Donc la suite suivante est exacte :

$$0 \longrightarrow p^n\mathcal{H}_0 \longrightarrow \delta(N_0^n\mathcal{H}_n) \xrightarrow{\alpha_0} \bigoplus_{l\in\mathcal{P}} p^n\mathbb{Z}l \longrightarrow 0$$

Et cette suite donne :

$$\begin{aligned}\operatorname{rang}(N_0^n\mathcal{H}_n) = \operatorname{rang}(p^n\mathcal{H}_0) + \#\mathcal{P} &= \operatorname{rang}(\mathcal{L}_0) - \operatorname{rang}\mathcal{D}_0 + \#\mathcal{P}\\ &= \operatorname{rang}(\mathcal{L}_0) - g_{\mathcal{P}}f_{\mathcal{P}} - \#\mathcal{P} + \#\mathcal{P}\\ &\text{d'après le corollaire 2.5}\\ &= \sum_{\substack{I\subset\mathcal{P}\\ I\neq\mathcal{P}}} g_I f_I \text{ comme annoncé}\end{aligned}$$

□

Lemme 4.11.

$$\operatorname{rang}(\mathcal{H}_n) = \operatorname{rang}(\mathcal{L}_n) - g_{\mathcal{P}}f_{\mathcal{P}}p^n$$

Démonstration : En utilisant les résultats précédents la preuve se résume au calcul suivant :

$$\begin{aligned}\operatorname{rang}(\mathcal{H}_n) &= \operatorname{rang}(\mathcal{H}_n + \mathcal{V}_n) - \operatorname{rang}(\mathcal{V}_n) + \operatorname{rang}(\mathcal{H}_n \cap \mathcal{V}_n)\\ &= \operatorname{rang}(\mathcal{L}_n) - \operatorname{rang}(\mathcal{D}_n) - \operatorname{rang}(\mathcal{V}_n) + \operatorname{rang}(\mathcal{H}_n \cap \mathcal{V}_n)\\ &\text{d'après le théorème 3.6}\\ &= \operatorname{rang}(\mathcal{L}_n) - \operatorname{rang}(\mathcal{D}_n) - \operatorname{rang}(N_0^n\mathcal{V}_n) + \operatorname{rang}(N_0^n\mathcal{H}_n \cap N_0^n\mathcal{V}_n)\\ &\text{car } N_0^n \text{ agit comme } p^n \text{ sur } \mathcal{V}_n\\ &= \operatorname{rang}(\mathcal{L}_n) - \operatorname{rang}(\mathcal{D}_n) + \operatorname{rang}(N_0^n\mathcal{H}_n) - \operatorname{rang}(N_0^n\mathcal{H}_n + N_0^n\mathcal{V}_n)\end{aligned}$$

En constatant que $\operatorname{rang}(N_0^n\mathcal{L}_n \cap \ker\alpha_n) = \operatorname{rang}(N_0^n \ker\alpha_n)$, ce qui provient de l'inclusion du module p^n $(N_0^n\mathcal{L}_n \cap \ker\alpha_n)$ dans le module $N_0^n \ker\alpha_n$ on en déduit que:

$$\begin{aligned}\operatorname{rang}(\mathcal{H}_n) &= \operatorname{rang}(\mathcal{L}_n) - \operatorname{rang}(\mathcal{D}_n) + \operatorname{rang}(N_0^n\mathcal{H}_n) - \operatorname{rang}(N_0^n\mathcal{L}_n \cap \ker\alpha_n)\\ &= \operatorname{rang}(\mathcal{L}_n) - \operatorname{rang}(N_0^n\mathcal{L}_n) + \operatorname{rang}(N_0^n\mathcal{H}_n) - \operatorname{rang}(\mathcal{D}_n)\\ &+ \operatorname{rang}(N_0^n\alpha_n(\mathcal{L}_n))\end{aligned}$$

Pour conclure il suffit ici d'utilser les identités suivantes :

$$\operatorname{rang}(N_0^n\mathcal{L}_n) = \sum_{I\subset\mathcal{P}} g_I f_I (\text{évident}),\ \operatorname{rang}(N_0^n\mathcal{H}_n) = \sum_{I\subset\mathcal{P},\ I\neq\mathcal{P}} g_I f_I (\text{lemme 4.10}),$$

$$\operatorname{rang}(\mathcal{D}_n) = g_{\mathcal{P}}f_{\mathcal{P}}p^n - g_{\mathcal{P}} + 1 (\text{corollaire 2.5})$$

et

$$\operatorname{rang}(N_0^n(\alpha_n(\mathcal{L}_n))) = \operatorname{rang}(N_0^n\mathcal{D}_n) = g_{\mathcal{P}}f_{\mathcal{P}} - g_{\mathcal{P}} + 1 (\text{corollaire 2.5}).$$

Cela nous donne :

$$\begin{aligned}\operatorname{rang}(\mathcal{H}_n) &= \operatorname{rang}(\mathcal{L}_n) - g_{\mathcal{P}}f_{\mathcal{P}} - g_{\mathcal{P}}f_{\mathcal{P}}p^n + g_{\mathcal{P}} - 1 + g_{\mathcal{P}}f_{\mathcal{P}} - g_{\mathcal{P}} + 1\\ &= \operatorname{rang}(\mathcal{L}_n) - g_{\mathcal{P}}f_{\mathcal{P}}p^n \text{ comme annoncé.} \quad \square\end{aligned}$$

Avec la liberté de $\frac{\mathcal{L}_n}{\mathcal{H}_n}$, l'essentiel de la preuve du théorème 4.5 est achevé. Par exemple lorsque $g_{\mathcal{P}} = 1$ (i.e. p est inerte dans K), il est facile de voir que $\mathcal{V}_n \subset \mathcal{H}_n$, et, dans ce cas notre preuve est terminée. La section qui suit traite aussi les autres cas.

IV.3 Preuve du théorème 4.5.

A partir d'ici $\theta_n \ : \ \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R} \longrightarrow \mathcal{D}_n \otimes \mathcal{R}$ désignera l'homomorphisme surjectif qui factorise $\alpha_n \otimes 1$.

Lemme 4.12. $\ker \theta_n \subset \left(\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}\right)^{G_0^n} = N_0^n \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}$

Lemme 4.13. *Soit M un $\mathcal{R}[G_0^n]$-module libre, et soit $\{x_1, x_2, ..., x_s\}$ une $\mathcal{R}$-base de $N_0^n M$. Il existe une $\mathcal{R}[G_0^n]$-base de M, disons $\{\tilde{x}_1, \tilde{x}_2, ..., \tilde{x}_s\}$ qui vérifie :*

$$\forall i \ : \ N_0^n \tilde{x}_i = x_i$$

On admet momentanément les deux lemmes et on prouve 4.5. En vertu du lemme 4.12 l'application

$$\frac{N_0^n \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}}{\ker \theta_n} \overset{\theta_n}{\hookrightarrow} \mathcal{D}_n \otimes \mathcal{R} \text{ est une injection bien définie.}$$

Comme $(\mathcal{L}_n/\mathcal{H}_n) \otimes \mathcal{R}$ et $\mathcal{D}_n \otimes \mathcal{R}$ sont sans $\mathcal{R}$ torsion d'après la proposition 4.7 et le lemme 2.3 (1), les modules $\ker \theta_n$ et $\left(N_0^n \left(\mathcal{L}_n/\mathcal{H}_n \otimes \mathcal{R}\right)\right) / \ker \theta_n$ sont libres sur $\mathcal{R}$. Il existe donc une $\mathcal{R}$-base de $N_0^n \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}$ qui contient une $\mathcal{R}$-base de $\ker \theta_n$. En appliquant le lemme 4.13 à $M = \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}$ et à cette base, on obtient, en passant aux quotients, un isomorphisme entre $\mathcal{D}_n$ et un module de la forme voulue. Il reste à calculer les entiers r et t du théorème 4.5. Mais r est précisément la puissance du caractère trivial pour G_0^n intervenant dans la décomposition en caractère absolument irréductible de $\mathcal{D}_n$. Donc d'après la proposition 2.4 (1) on a $r = g_{\mathcal{P}} f_{\mathcal{P}} - g_{\mathcal{P}} + 1$. Et en utilisant l'identité : $p^n r + (p^n - 1)t = p^n g_{\mathcal{P}} f_{\mathcal{P}} - g_{\mathcal{P}} + 1$, on conclut que t est bien égal à $g_{\mathcal{P}} - 1$. $\square$

Démonstration de 4.12 : La dernière identité est un corollaire de la liberté de $\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}$. Pour l'inclusion, soit $x \in \ker \theta_n$ alors d'après le théorème 3.6 il existe un entier z non nul tel que l'on ait :

$$z\ x \in \left(\frac{\mathcal{V}_n}{\mathcal{V}_n \cap \mathcal{H}_n} \otimes \mathcal{R}\right) \subset \left(\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}\right)^{G_0^n} \text{ par définition de } \mathcal{V}_n$$

Soit $g \in G_0^n$, alors on a : $z(x - gx) = 0$ et comme $\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}$ est sans $\mathcal{R}$-torsion, on a bien $x = gx$. $\square$

Démonstration de 4.13 : Soit $\{y_1, y_2, ..., y_s\}$ une $\mathcal{R}[G_0^n]$-base de M, clairement $\{N_0^n y_1, N_0^n y_2, ..., N_0^n y_s\}$ est une $\mathcal{R}$-base de $N_0^n M$. Il existe donc une matrice $A = (a_{i,j})$ dans $\mathrm{Gl}_s(\mathcal{R})$ telle que (en notant $b_{i,j}$ les coefficients de A^{-1}) :

$$\forall i \ : \ \sum_{j=1}^{j=s} a_{i,j} N_0^n y_j = x_i; \ \forall j \ : \ \sum_{i=1}^{i=s} b_{i,j} x_i = N_0^n y_j$$

On pose $\tilde{x}_i = \sum_{j=1}^{j=s} a_{i,j} y_j$. Alors les $\tilde{x}_i$ vérifient clairement $N_0^n \tilde{x}_i = x_i$. Et quel que soit j, on a : $y_j = (\sum_{i=1}^{i=s} b_{i,j} \tilde{x}_i) \in (\sum \mathcal{R} \tilde{x}_i)$. Il suit donc :

$$M = \sum_i \mathcal{R}[G_0^n] \tilde{x}_i = \bigoplus_i \mathcal{R}[G_0^n] x_i$$

Pour la dernière égalité on utilise la $\mathcal{R}[G_0^n]$-liberté de M. $\square$

V Cohomologie des unités cyclotomiques

Dans ce chapitre on étudie les deux groupes de cohomologie modifiés à la Tate, des unités cyclotomiques. Plus précisément on va calculer les $\widehat{H}^i\left(G_n^m, C(F_m)\right)$, pour $i = 1$ ou 2, et pour certains corps abéliens F, en conservant les notations F_m et G_n^m des chapitres précédents. Cela peut se faire de deux façons différentes. Une méthode est due à Kim ([K 1]) et on la généralise quelque peu dans la première partie. Une autre méthode consiste à utiliser la version locale du théorème 4.5 (sous l'hypothèse B, donc).

V.1 Quelques rappels sur les groupes de cohomologie.

Définition 5.1. *Soit G un groupe cyclique fini, et soit g un générateur de G. Soit M un $\mathbb{Z}[G]$-module. On note T et S les homomorphismes :*

$$\begin{aligned} T\ &: M \to M \\ &x \mapsto \sum_{g \in G} gx \end{aligned}$$

$$\begin{aligned} S\ &: M \to M \\ &x \mapsto (g-1)x \end{aligned}$$

On appelle groupes de cohomologie modifiés les groupes :

$$\widehat{H}^0(G, M) = \frac{\ker S}{T(M)} \qquad et \qquad \widehat{H}^1(G, M) = \frac{\ker T}{S(M)}$$

On énonce, sans démonstration, quelques propriétés classiques de ces groupes. Toutes les preuves peuvent se trouver dans [La 1] ou [Se] ou [C F].

Proposition 5.2. *Soit G un groupe cyclique et soit A,B, et C trois $\mathbb{Z}[G]$-modules reliés par une suite exacte :*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

Alors, on a l'hexagone exact (où les flèches horizontales sont les homomorphismes évidents et où les flèches verticales s'obtiennent par deux applications du lemme du serpent) :

$$\begin{tikzcd} \widehat{H}^0(G,A) \arrow[r] & \widehat{H}^0(G,B) \arrow[r] & \widehat{H}^0(G,C) \arrow[d] \\ \widehat{H}^1(G,C) \arrow[u] & \widehat{H}^1(G,B) \arrow[l] & \widehat{H}^1(G,A) \arrow[l] \end{tikzcd}$$

Proposition 5.3. *Soient G un groupe cyclique, L un sous-groupe de G, et soit M un $\mathbb{Z}[G]$-module. Soit $\tilde{T}$ un relevé dans $\mathbb{Z}[G]$ de la somme $\sum_{g\in G/L} g$ et soit $H^1\left(G/L, M^L\right) \longrightarrow \widehat{H}^1(G,M)$ l'application obtenue par l'inclusion $M^L \subset M$. Alors on a la suite exacte (où la première application s'appelle l'inflation la seconde la restriction) :*

$$0 \longrightarrow \widehat{H}^1\left(G/L, M^L\right) \longrightarrow \widehat{H}^1(G,M) \xrightarrow{\tilde{T}} \widehat{H}^1(L,M)$$

Définition 5.4. *Soit G un groupe cyclique et M un $\mathbb{Z}[G]$-module, en supposant que $\widehat{H}^0(G,M)$ et $\widehat{H}^1(G,M)$ sont finis, ce qui est vrai lorsque M est de type fini, on appelle quotient de Herbrand de M pour l'action de G la constante :*

$$q_{G,M} = \frac{\#\widehat{H}^0(G,M)}{\#\widehat{H}^1(G,M)}$$

Proposition 5.5. *Soit G un groupe cyclique et soient $N \subset M$ deux $\mathbb{Z}[G]$-modules tels que M/N soit fini, alors on a :*

$$q_{G,M} = q_{G,N}$$

Proposition 5.6. *Soit F un corps de nombres et soit G un sous-groupe cyclique du groupe des automorphismes de F. Alors on a :*

$$q_{G,E(F)} = \frac{1}{\#G}$$

Démonstration : C'est une conséquence immédiate du corollaire 2 du paragraphe 5 chapitre IX de [La 1].

Corollaire 5.7. *avec les notations du début de ce chapitre on a :*

$$q_{G_n^m, C(F_m)} = \frac{1}{p^{m-n}}$$

Démonstration : Compte-tenu du fait que $C(K_m)$ est d'indice fini dans $E(K_m)$ cela suit des propositions 5.5 et 5.6.

V.2 La méthode de Kim.

Ici on reprend la démarche de [K 1], et on se donne un corps F abélien sur $\mathbb{Q}$, de degré fini sur $\mathbb{Q}$ et un nombre premier $p \neq 2$ au plus modérément ramifié dans F. Mais contrairement à [K 1] on ne suppose plus que $F = \mathbb{Q}(\zeta_{pd})$. On est cependant amené a faire les deux hypothèses qui suivent :

Soit Δ le groupe de ramification de p dans G_F, on admet que $p \nmid [F^\Delta : F_{dec}]$

On admet que pour tout $m \geq n \geq 0$ on a $C(F_m) \cap F_n = C(F_n)$.

Ces deux hypothèses sont par exemple vérifiées dans les corps considérés par Kim dans [K 1] ou bien par les corps F réels tels que (F, p) vérifie H.B. et $p \nmid [F^\Delta : F_{\rm dec}]$. On verra plus tard que d'une part H.B entraîne la deuxième hypothèse ci-dessus, et que d'autre part H.B est vraie lorsque $p \nmid [F : \mathbb{Q}]$. Dans cette section on applique exactement la technique de Kim [K 1], et on se permet de seulement esquisser certaines preuves, qui sont faites en détails dans [K 1], pour son cas particulier.

On a besoin tout d'abord de quelques notations supplémentaires. Soit $D'_n(F)$ le sous-module de $F_n^\times$, engendré sur $\mathbb{Z}[G_{F_n}]$ par les racines de l'unité dans F_n et par les entiers de la forme :

$$N_{F_n \cap \mathbb{Q}(\zeta_f)}^{\mathbb{Q}(\zeta_f)} (1 - \zeta_f)$$

avec $p \mid f$ et f non congru à 2 modulo 4.

Soit $C'_n = D'_n(F) \cap E(F_n)$. De la même manière que dans 2.3 (3) on peut vérifier que $C(F_n) = C(F^\Delta) C'_n$. Et on a aussi pour tout $m \geq n \geq 0$, $N_n^m (C'_m) = C'_n$. Pour simplifier on note N la norme de F^Δ à $F_{\rm dec}$. Soit ${}_N C(F^\Delta) = \{\xi \in C(F^\Delta) | N(\xi) = 1\}$ et soit $\overline{{}_N C(F^\Delta)} = \{\xi \in C(F^\Delta) | N(\xi) \in \mu(F_{\rm dec})\}$. On a :

Lemme 5.8. *Pour tout $m \geq 0$:*

$$\left(C\left(F^\Delta\right)\right)^{\left(\left(\frac{F^\Delta}{p}\right) - 1\right)} \subset C\left(F^\Delta\right) \cap C'_m \subset \overline{{}_N C(F^\Delta)}$$

Démonstration : On omet la preuve. Cela peut se faire en adaptant le raisonnement de 2.3 (4) à cette situation $\square$

Théorème 5.9. *Soit r le $\mathbb{Z}$-rang des unités de $F_{\rm dec}$. Pour tout $m > n \geq 0$ on a :*

$$\widehat{H}^0\left(G_n^m, C\left(F_m\right)\right) = \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^r$$

Démonstration : L'application naturelle obtenue en composant les deux homomorphismes :

$$C\left(F^\Delta\right) \longrightarrow C\left(F_n\right) \longrightarrow \frac{C\left(F_n\right)}{N_n^m\left(C\left(F_m\right)\right)}$$

est surjective, comme $C(F_n) = C\left(F^\Delta\right) C'_n$ et $N_n^m(C'_m) = C'_n$. Il s'agit de décrire son noyau, que l'on note ker. On a :

$$\begin{aligned}
\ker &= C\left(F^\Delta\right) \cap N_n^m\left(C\left(F_m\right)\right) \\
&= C\left(F^\Delta\right) \cap N_n^m\left(C\left(F^\Delta\right) C'_m\right) \\
&= C\left(F^\Delta\right) \cap \left(C\left(F^\Delta\right)\right)^{p^{m-n}} C'_n \\
&= C\left(F^\Delta\right)^{p^{m-n}} \left(C\left(F^\Delta\right) \cap C'_n\right)
\end{aligned}$$

Comme on suppose que $C(F_m)^{G_n^m} = C(F_n)$, on en tire :

$$\widehat{H}^0\left(G_n^m, C\left(F_m\right)\right) = \frac{C\left(F^\Delta\right)}{\left(C\left(F^\Delta\right)\right)^{p^{m-n}} \left(C\left(F^\Delta\right) \cap C'_n\right)}$$

De plus il est évident que $\overline{{}_N C\left(F^\Delta\right)}$ est un sous-groupe, facteur direct de $C\left(F^\Delta\right)$ et que le rang d'un supplémentaire est égal au rang de $N\left(E\left(F^\Delta\right)\right)$, c'est-à-dire r. D'après le lemme 5.8 on a les surjections :

$$\frac{C\left(F^\Delta\right)}{C\left(F^\Delta\right)^{p^{m-n}} C\left(F^\Delta\right)^{\left(\left(\frac{F^\Delta}{p}\right)-1\right)}} \longrightarrow \frac{C\left(F^\Delta\right)}{C\left(F^\Delta\right)^{p^{m-n}} \left(C\left(F^\Delta\right) \cap C'_n\right)}$$

et

$$\frac{C\left(F^\Delta\right)}{C\left(F^\Delta\right)^{p^{m-n}} \left(C\left(F^\Delta\right) \cap C'_n\right)} \longrightarrow \frac{C\left(F^\Delta\right)}{C\left(F^\Delta\right)^{p^{m-n}} \overline{{}_N C\left(F^\Delta\right)}}$$

Le théorème est donc une conséquence du lemme qui suit. $\square$

Lemme 5.10. *On a*

$$\frac{C\left(F^\Delta\right)}{C\left(F^\Delta\right)^{p^{m-n}} \overline{{}_N C\left(F^\Delta\right)}} = \frac{C\left(F^\Delta\right)}{C\left(F^\Delta\right)^{p^{m-n}} C\left(F^\Delta\right)^{\left(\left(\frac{F^\Delta}{p}\right)-1\right)}} \simeq \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^r$$

Démonstration : Partant d'une écriture de $C\left(F^\Delta\right)$ sous la forme :

$$C\left(F^\Delta\right) = \overline{{}_N C\left(F^\Delta\right)} \oplus \mathbb{Z}^r$$

on obtient :

$$\begin{aligned}
\frac{C\left(F^\Delta\right)}{\left(C\left(F^\Delta\right)^{p^{m-n}} \overline{{}_N C\left(F^\Delta\right)}\right.} &= \frac{\overline{{}_N C\left(F^\Delta\right)} \oplus \mathbb{Z}^r}{\overline{{}_N C\left(F^\Delta\right)} \oplus p^{m-n}\mathbb{Z}^r} \\
&= \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^r
\end{aligned}$$

Soient $f = [F^\Delta : F_{\mathrm{dec}}]$ et $w = \#\left(\mu\left(F^\Delta\right)\right)$. Alors $\overline{{}_N C\left(F^\Delta\right)} / \left(C\left(F^\Delta\right)\right)^{\left(\left(\frac{F^\Delta}{p}\right)-1\right)}$ est annulé par le produit wf car w annule $\overline{{}_N C\left(F^\Delta\right)} / {}_N C\left(F^\Delta\right)$ d'une part, et f

annule ${}_{N}C\left(F^{\Delta}\right)/\left(C\left(F^{\Delta}\right)\right)^{\left(\left(\frac{F^{\Delta}}{p}\right)-1\right)}$ qui coïncide avec $H^{1}\left(\left\langle\left(\frac{F^{\Delta}}{p}\right)\right\rangle, C\left(F^{\Delta}\right)\right)$. Comme p est différent de 2, il ne peut diviser w car il ne se ramifie pas dans F^{Δ}. Comme nous avons supposé de plus que p ne divise pas f, et que p^{m-n} annule $\overline{{}_{N}C\left(F^{\Delta}\right)}/\left(\overline{{}_{N}C\left(F^{\Delta}\right)}\right)^{p^{m-n}} C\left(F^{\Delta}\right)^{\left(\left(\frac{F^{\Delta}}{p}\right)-1\right)}$, ce dernier quotient est trivial. On en déduit donc que :

$$
\begin{aligned}
&\frac{C\left(F^{\Delta}\right)}{C\left(F^{\Delta}\right)^{p^{m-n}} C\left(F^{\Delta}\right)^{\left(\left(\frac{F^{\Delta}}{p}\right)-1\right)}} \\
&= \frac{\overline{{}_{N}C\left(F^{\Delta}\right)} \oplus (\mathbb{Z})^{r}}{\left(\overline{{}_{N}C\left(F^{\Delta}\right)}^{p^{m-n}} \oplus \left(p^{m-n}\mathbb{Z}\right)^{r}\right) C\left(F^{\Delta}\right)^{\left(\left(\frac{F^{\Delta}}{p}\right)-1\right)}} \\
&= \frac{\overline{{}_{N}C\left(F^{\Delta}\right)}}{\overline{{}_{N}C\left(F^{\Delta}\right)}^{p^{m-n}} C\left(F^{\Delta}\right)^{\left(\left(\frac{F^{\Delta}}{p}\right)-1\right)}} \oplus \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^{r} \\
&= \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^{r}
\end{aligned}
$$

□

Corollaire 5.11. *La preuve ci-dessus montre aussi que* $\overline{{}_{N}C\left(F^{\Delta}\right)}$ *est contenu dans* $N_{n}^{m}\left(C\left(F_{m}\right)\right)$.

On calcule maintenant $\widehat{H}^{1}\left(G_{n}^{m}, C\left(F_{m}\right)\right)$

Lemme 5.12. *Soit* $a > b > c$. *Si* $\delta \in C\left(F_{b}\right)$ *est tel que* $N_{c}^{b}(\delta) = 1$, *alors* $\delta \in N_{b}^{a}\left(C\left(F_{a}\right)\right)$.

Démonstration : Soit S un sous-groupe de $C\left(F^{\Delta}\right)$ supplémentaire de $\overline{{}_{N}C\left(F^{\Delta}\right)}$. Clairement on a $C\left(F_{m}\right) = S\overline{{}_{N}C\left(F^{\Delta}\right)}C_{m}'$. Ecrivons ici $\delta = \xi u v$, avec $\xi \in S$, $u \in \overline{{}_{N}C\left(F^{\Delta}\right)}$ et $v \in C_{m}'$. Alors, on a :

$$1 = N_{n}^{m}(\delta) = \xi^{p^{m-n}} u^{p^{m-n}} N_{n}^{m}(v)\ .$$

Or on a aussi $N_{n}^{m}v \in C_{n}'$ et donc on en déduit :

$$N_{n}^{m}v = \xi^{-p^{m-n}} u^{-p^{m-n}} \in C\left(F^{\Delta}\right) \cap C_{n}' \subset \overline{{}_{N}C\left(F^{\Delta}\right)}$$

Cela entraine $\xi^{-p^{m-n}} = N_{n}^{m}(v)u^{p^{m-n}} \in \overline{{}_{N}C\left(F^{\Delta}\right)}$ et donc $\xi^{-p^{m-n}} = 1$, puis $\xi = 1$. D'après la remarque qui précède on a donc $\delta \in \overline{{}_{N}C\left(F^{\Delta}\right)}C_{m}' \subset N_{m}^{s}\left(C\left(F_{s}\right)\right)$, comme attendu. □

Théorème 5.13. *Pour tout $m > n \geq 0$ on a :*

$$\widehat{H}^1\left(G_n^m, C\left(F_m\right)\right) \simeq \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^{r+1}$$

Démonstration : On fait une récurrence sur $m \geq n+1$. Si $m = n+1$, comme le quotient d'Herbrand pour $C\left(F_m\right)$ est le même que celui des unités de F_m, il vaut $1/\# G_n^{n+1} = 1/p$. Comme en outre on a $p\ \widehat{H}^1\left(G_n^{n+1}, C\left(F_{n+1}\right)\right) = 0$ on a bien $\widehat{H}^1\left(G_n^{n+1}, C\left(F_{n+1}\right)\right) \simeq \mathbb{F}_p^{r+1}$. Supposons le théorème vrai pour $m = s$, avec $s \geq n+1$, et vérifions le pour $m = s+1$. En utilisant l'injectivité de l'inflation et l'égalité

$$C\left(F_{s+1}\right)^{G_s^{s+1}} = C\left(F_s\right)$$

on obtient une injection :

$$1 \longrightarrow \widehat{H}^1\left(G_n^s, C\left(F_s\right)\right) \longrightarrow \widehat{H}^1\left(G_n^{s+1}, C\left(F_{s+1}\right)\right)$$

Le lemme 5.12 et le fait que pour tout $\delta \in \widehat{H}^1\left(G_n^{s+1}, C\left(F_{s+1}\right)\right)$ on a $N_s^{s+1}(\delta) = p\,\delta$, montre que l'image de $\widehat{H}^1\left(G_n^s, C\left(F_s\right)\right)$ est contenu dans $p\ \widehat{H}^1\left(G_n^{s+1}, C\left(F_{s+1}\right)\right)$. On connaît le cardinal de $\widehat{H}^1\left(G_n^{s+1}, C\left(F_{s+1}\right)\right)$ car on connaît le $\widehat{H}^0$ et le quotient de Herbrand correspondant. Comme $p^{s+1-n}\ \widehat{H}^1\left(G_n^{s+1}, C\left(F_{s+1}\right)\right) = 0$ on en déduit l'égalité entre l'image de $\widehat{H}^1\left(G_n^s, C\left(F_s\right)\right)$ et le sous-groupe $p\ \widehat{H}^1\left(G_n^{s+1}, C\left(F_{s+1}\right)\right)$. L'hypothèse de récurrence et l'identité

$$\#\left(\widehat{H}^1\left(G_n^{s+1}, C\left(F_{s+1}\right)\right)\right) = p^{s+1-n}\ \#\left(\widehat{H}^0\left(G_n^{s+1}, C\left(F_{s+1}\right)\right)\right)$$

prouvent donc le théorème pour $m = s+1$. □

V.2 Applications cohomologiques du théorème 4.5.

Dans cette section on calcule sous l'hypothèse B les deux groupes de cohomologie modifiés à la Tate, associés à l'action de G_n^m sur $C(K_m)$ (pour $m > n \geq 0$). On reprend les conventions et la notation K des chapitres II, III, et IV.

Une conséquence directe de 4.5 (1) est :

Corollaire 5.14. *Si (K,p) vérifie H.B, alors pour tout $m \geq n \geq 0$:*

$$\widehat{H}^0(G_n^m, \mathcal{D}_m\left(K\right)) = \{0\} \quad \textit{et} \quad \widehat{H}^1(G_n^m, \mathcal{D}_m\left(K\right)) \simeq \left(\frac{\mathbb{Z}}{p^{m-n}\ \mathbb{Z}}\right)^{g_{\mathcal{P}}-1}$$

On peut en déduire les deux propositions suivantes :

Proposition 5.15. *Si (K,p) vérifie H.B. alors on a pour tout $m \geq n \geq 0$:*

$$C(K_m) \cap K_n = C(K_n)$$

Proposition 5.16. $(\mathcal{D}_0\,(K))^{\left(\frac{K}{p}\right)-1}$ *est contenu dans $C(K)$ d'après 1.3 (5). Soit F le sous-$\mathbb{Z}$-module de torsion de $\frac{C(K)}{(\mathcal{D}_0(K))^{\left(\frac{K}{p}\right)-1}}$ et pour tout entier $r \in \mathbb{Z}$ soit $F_{p^r} = \ker\{F \xrightarrow{p^r} F\}$. Si (K,p) vérifie H.B. alors pour tout $m > n \geq 0$ on a :*

$$\widehat{H}^0(G_n^m, C(K_m)) \simeq \frac{F}{p^r F} \oplus \left(\frac{\mathbb{Z}}{p^{m-n}\ \mathbb{Z}}\right)^{g_{\mathcal{P}}-1}$$

et

$$\widehat{H}^1(G_n^m, C(K_m)) \simeq F_{p^{m-n}} \oplus \left(\frac{\mathbb{Z}}{p^{m-n}\ \mathbb{Z}}\right)^{g_{\mathcal{P}}}$$

Démonstration de 5.15 : Par la définition des deux modules, on a l'inclusion du module de droite dans le module de gauche. Réciproquement, soit $x \in C(K_m) \cap K_n$ alors d'après le lemme 2.3 (3) il existe $x_0 \in C(K)$ et $x' \in \mathcal{D}_m\,(K) \cap E(K_m)$ tels que $x = x_0 x'$. Comme x et x_0 sont fixés par G_n^m, x' l'est aussi. Le corollaire 5.14 donne donc $x' \in N_n^m(\mathcal{D}_m\,(K)) \subset \mathcal{D}_n\,(K)$. On en déduit $x' \in \mathcal{D}_n\,(K) \cap E(K_n)$ puis $x \in C(K_n)$ en utilisant à nouveau 2.3 (3) ou 2.3 (2). $\square$

Démonstration de 5.16 : On calcule d'abord la cohomologie de $\mathcal{D}_m\,(K) \cap E(K_m)$ à l'aide de la suite suivante dont l'exactitude est donnée par le lemme 2.3 (5) et par les identités $N_{\mathbb{Q}}^{K_m}(\epsilon_m\,(I)) = 1$ si $I \neq \emptyset$ et $N_{\mathbb{Q}}^{K_m}(\epsilon_m\,(\emptyset)) = p^{f_{\mathcal{P}} g_{\mathcal{P}}}$:

$$0 \longrightarrow \mathcal{D}_m\,(K) \cap E(K_m) \longrightarrow \mathcal{D}_m\,(K) \xrightarrow{N_{\mathbb{Q}}^{K_m}} \mathbb{Z}\ p^{f_{\mathcal{P}} g_{\mathcal{P}}} \longrightarrow 0$$

En utilisant l'hexagone exact de cohomologie et le corollaire 5.14, on obtient :

$$\widehat{H}^0(G_n^m, \mathcal{D}_m\,(K) \cap E(K_m)) = 0$$

Et on en déduit la suite exacte courte de $\mathbb{Z}/p^{m-n}\mathbb{Z}$-modules :

$$0 \longrightarrow \frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}} \longrightarrow \widehat{H}^1(G_n^m, \mathcal{D}_m\,(K) \cap E(K_m)) \longrightarrow \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^{g_{\mathcal{P}}-1} \longrightarrow 0$$

qui se scinde en $\widehat{H}^1(G_n^m, \mathcal{D}_m\,(K) \cap E(K_m)) \simeq (\mathbb{Z}/p^{m-n}\mathbb{Z})^{g_{\mathcal{P}}}$ puisque le dernier terme est libre. Cela étant, le corollaire 5.14 et le lemme 2.3 (4) donnent aussi :

$$C(K) \cap \mathcal{D}_m\,(K) \subset (\mathcal{D}_m\,(K))^{G_0^m} = N_0^m(\mathcal{D}_m\,(K)) = (\mathcal{D}_0\,(K))^{\left(\frac{K}{p}\right)-1} \oplus \mathbb{Z}\ p$$

On en déduit avec le lemme 2.3 (5) :

$$\begin{aligned} C(K) \cap \mathcal{D}_m\,(K) \ &\subset\ \left((\mathcal{D}_0\,(K))^{\left(\frac{K}{p}\right)-1} \oplus \mathbb{Z}\ p\right) \cap E(K) \ \subset\ (\mathcal{D}_0\,(K))^{\left(\frac{K}{p}\right)-1} \\ &\subset C(K) \cap \mathcal{D}_m\,(K) \end{aligned}$$

d'où l'égalité $C(K) \cap \mathcal{D}_m(K) = (\mathcal{D}_0(K))^{\left(\frac{K}{p}\right)-1}$ et avec le lemme 2.3 (3) on a l'exactitude de la suite :

$$0 \longrightarrow \mathcal{D}_m(K) \cap E(K_m) \longrightarrow C(K_m) \longrightarrow \frac{C(K)}{(\mathcal{D}_0(K))^{\left(\frac{K}{p}\right)-1}} \longrightarrow 0$$

Mais comme G_n^m agit trivialement sur $C(K)$ on a aussi :

$$\frac{C(K)}{(\mathcal{D}_0(K))^{\left(\frac{K}{p}\right)-1}} \simeq F \oplus \mathbb{Z}^{g_{\mathcal{P}}-1}$$

car $(\mathcal{D}_0(K))^{\left(\frac{K}{p}\right)-1}$ est d'indice fini dans $\ker N_{K_{\mathrm{dec}}}^K \cap C(K)$

Et l'hexagone exact de cohomologie donne :

$$\begin{tikzcd}
0 \arrow[r] & \widehat{H}^0(G_n^m, C(K_m)) \arrow[r] & \dfrac{F}{p^{m-n}F} \oplus \left(\dfrac{\mathbb{Z}}{p^{m-n}}\right)^{g_{\mathcal{P}}-1} \arrow[d] \\
F_{p^{m-n}} \arrow[u] & \widehat{H}^1(G_n^m, C(K_m)) \arrow[l] & \widehat{H}^1(G_n^m, \mathcal{D}_m(K) \cap E(K_m)) \arrow[l, "\phi"']
\end{tikzcd}$$

Mais d'après 2.3 (3), pour tout générateur γ de G_n^m, on a :

$C(K_m)^{\gamma-1} = (C(K)(\mathcal{D}_m(K) \cap E(K_m)))^{\gamma-1} = (\mathcal{D}_m(K) \cap E(K_m))^{\gamma-1}$ de telle sorte que ϕ est injective et que ce diagramme donne

$$\widehat{H}^0(G_n^m, C(K_m)) \cong \frac{F}{p^{m-n}F} \oplus \left(\frac{\mathbb{Z}}{p^{m-n}}\right)^{g_{\mathcal{P}}-1} \quad \text{et la suite :}$$

$$0 \longrightarrow \left(\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}}\right)^{g_{\mathcal{P}}} \longrightarrow \widehat{H}^1(G_n^m, C(K_m)) \longrightarrow F_{p^{m-n}} \longrightarrow 0$$

Mais comme $\mathbb{Z}/N\mathbb{Z}$ est injectif comme module sur lui-même la suite exacte ci-dessus est scindée et on a bien $\widehat{H}^1(G_n^m, C(K_m)) \simeq F_{p^{m-n}} \oplus (\frac{\mathbb{Z}}{p^{m-n}\mathbb{Z}})^{g_{\mathcal{P}}}$. □

Pour l'étude de la cohomologie, il n'est plus nécessaire de supposer que les corps sont réels. En effet on a le :

Corollaire 5.17. *Soit L un corps abélien imaginaire de sous-corps réel maximal K. Si $p \neq 2$ et si (K, p) vérifie H.B, alors pour tout $m > n \geq 0$ on a :*

$$\widehat{H}^0(G_n^m, C(L_m)) = \widehat{H}^0(G_n^m, C(K_m)) \simeq \frac{F}{p^{m-n}F} \oplus \left(\frac{\mathbb{Z}}{p^{m-n}\,\mathbb{Z}}\right)^{g_{\mathcal{P}}-1}$$

$$\text{\textit{et}} \quad \widehat{H}^0(G_n^m, C(L_m)) = \widehat{H}^0(G_n^m, C(K_m)) \simeq F_{p^{m-n}} \oplus \left(\frac{\mathbb{Z}}{p^{m-n}\,\mathbb{Z}}\right)^{g_{\mathcal{P}}}$$

Démonstration : Les deux égalités viennent de la suite exacte (en notant $\mu(L_m)$ le groupe des racines de l'unité contenues dans L_m).

$$0 \longrightarrow \mu(L_m) \longrightarrow C(L_m) \xrightarrow{N_K^L} C(K_m) \longrightarrow 0$$

Comme $p \neq 2$, $\mu(L_m)$ est cohomologiquement trivial. Cela donne les deux égalités. Et les deux isomorphismes sont ceux de la proposition 5.15. □

VI Etude des hypothèses A et B

Dans ce chapitre, on donne des conditions suffisantes pour qu'un couple (K,p) vérifie H.B. On en déduit des conditions suffisantes pour que K vérifie H.A : ce qui revient à dire que quelque soit p, le couple (K,p) vérifie H.B. Pour la commodité de l'exposé on laisse varier le nombre premier p, mais on conserve les autres conventions des chapitres II,III et IV. En deuxième section on détaillera l'exemple de deux couples (K,p) qui ne vérifient pas la conclusion locale (i.e. avec $\mathcal{R}=\mathbb{Z}_p$) de 4.5.

Si p est un nombre premier et G un groupe abélien, on notera G_p son (unique) p-sous-groupe de Sylow.

VI.1 Une liste de conditions suffisantes.

Proposition 6.1. *Soit p un nombre premier, on suppose que le p-sous-groupe de Sylow de G_K est cyclique, alors (K,p) vérifie H.B.*

Corollaire 6.2. *Si G_K est cyclique, alors K vérifie H.A.*

Démonstration de 6.2 : Cela vient de l'équivalence entre l'assertion K vérifie H.A et l'assertion pour tout p, (K,p) vérifie H.B. $\square$

Démonstration de 6.1 : On fixe $J\subset\mathcal{P}$. Comme $G(J)$ est un quotient de G_K, son p-sous-groupe de Sylow est cyclique. On écrit $G(J)=G'\times G_p$ où G_p est ce p-Sylow cyclique et où $p\nmid \#G'$. Soit h un générateur de G_p. On note $\mathcal{X}$ l'ensemble des caractères $\mathbb{Q}_p$-irréductibles de G', et pour chaque élément χ de $\mathcal{X}$, on note $\tilde{e}_\chi$ l'idempotent de $\mathbb{Z}_p[G']$ associé à χ. On a alors :

$$\frac{\mathbb{Z}[G(J)]}{N(J)}\otimes\mathbb{Z}_p\cong\bigoplus_{\chi\in\mathcal{X}}\tilde{e}_\chi\frac{\mathbb{Z}[G(J)]}{N(J)}\otimes\mathbb{Z}_p\cong\bigoplus_{\chi\in\mathcal{X}}\frac{\tilde{e}_\chi\mathbb{Z}_p[G(J)]}{\tilde{e}_\chi N(J)\otimes\mathbb{Z}_p}$$

Soit G'_l le plus grand sous-groupe de $\mathrm{Gal}(K(J)/K(J-\{l\}))$ qui vérifie $p\nmid\#G'_l$, alors pour chaque $l\in J$ il existe un couple d'entiers s_l et t_l avec $p^{s_l+t_l}=\#G_p$ et tel que : $N_l^J=\sum_{g\in G'_l}g\ \sum_{i=1}^{i=p^{t_l}}h^{is_l}$. Et on a de plus :

$$\tilde{e}_\chi N_l^J=\begin{cases}0 \text{ si } \exists\ g\in G'_l \text{ tel que } \chi(g)\neq\chi(1)\\ \#G'_l\ \tilde{e}_\chi\displaystyle\sum_{i=1}^{i=p^{t_l}}h^{is_l} \text{ sinon}\end{cases}$$

Soit s le maximum des s_l et t le minimum des t_l, alors comme $p \nmid \#G'$ on a :

$$\tilde{e}_\chi N(J) \otimes \mathbb{Z}_p = \tilde{e}_\chi \left(\sum_{i=1}^{i=p^t} h^{is} \right) \mathbb{Z}_p[G(J)]$$

Si on note A_χ l'anneau $A_\chi = \tilde{e}_\chi \mathbb{Z}_p[G']$ on a donc :

$$\frac{\tilde{e}_\chi \mathbb{Z}_p[G(J)]}{\tilde{e}_\chi N(J) \otimes \mathbb{Z}_p} \cong \frac{A_\chi[G_p]}{\left(\sum_{i=1}^{i=p^t} h^{it}\right) A_\chi[G_p]}$$

et comme pour tout χ ce dernier quotient est sans $\mathbb{Z}_p$-torsion, cela conclut notre preuve. $\square$

Proposition 6.3. *Soit p un nombre premier. Pour chaque sous-ensemble J de $\mathcal{P}$ et chaque élément l de J, on note $G_{l,p}^J$ le p-sous-groupe de Sylow du sous-groupe d'inertie en l de $G(J)$. On suppose que $G_{K,p}$ est le produit direct de tous ces sous-groupes : $G_{K,p} = \prod_{l \in \mathcal{P}} G_{l,p}^{\mathcal{P}}$.*

Alors pour tout $J \subset \mathcal{P}$, $G(J)_p$ est le produit direct : $G(J)_p = \prod_{l \in J} G_{l,p}^J$ et (K,p) vérifie H.B.

Corollaire 6.4. *Si K est un corps de genres au sens de [F], i.e. si G_K est le produit direct $G_K = \prod_{l \in \mathcal{P}} \mathrm{Gal}(K/K(\mathcal{P} - \{l\}))$, alors K vérifie H.A.*

Corollaire 6.5. *Soit p un nombre premier impair ne divisant pas le cardinal des G_K coinvariants du groupe des classes de K. Alors (K,p) vérifie H.B.*

Démonstration de 6.3 : Par restriction on a l'isomorphisme :

$$G(J)_p \cong \frac{\prod_{l \in \mathcal{P}} G_{l,p}^{\mathcal{P}}}{\prod_{l \notin J} G_{l,p}^{\mathcal{P}}}$$

Et cela donne la première affirmation avec la propriété de restriction des groupes d'inertie. Pour la deuxième, on fixe un $J \subset \mathcal{P}$, on écrit $G(J) = G' \times G_p$ comme dans la preuve de 6.1. et on reprend les notations $\tilde{e}_\chi$, A_χ et $\mathcal{X}$ de cette preuve. Ici aussi il s'agit de vérifier que pour tout χ, le quotient $\frac{A_\chi[G_p]}{\tilde{e}_\chi N(J) \otimes \mathbb{Z}_p}$ est sans $\mathbb{Z}_p$-torsion. On considère le diagramme commutatif suivant où les flèches diagonales représentent des applications A_χ-multilinéaires et les autres des homomorphismes de A_χ-algèbres unitaires.

$$\begin{tikzcd}
A_\chi[G_p] \arrow[r, "\psi"] \arrow[dd] & \underset{l\in J}{\otimes_{A_\chi}} A_\chi[G^J_{l,p}] \arrow[dd, dashed, "\pi"'] & \\
& & \prod_{l\in J} A_\chi[G^J_{l,p}] \arrow[ul] \arrow[dd, "s"] \\
\dfrac{A_\chi[G_p]}{\tilde e_\chi N(J)\otimes \mathbb{Z}_p} \arrow[r, dashed, "\phi"] & \underset{l\in J}{\otimes_{A_\chi}} \dfrac{A_\chi[G^J_{l,p}]}{\tilde e_\chi N^J_l A_\chi[G^J_{l,p}]} & \\
& & \prod_{l\in J} \dfrac{A_\chi[G^J_{l,p}]}{\tilde e_\chi N^J_l A_\chi[G^J_{l,p}]} \arrow[ul, "\mathrm{can}"'] \arrow[ull, "\omega"]
\end{tikzcd}$$

ψ est l'isomorphisme naturel donné par la première affirmation, et s est le produit des surjections naturelles. Comme $\mathrm{can}\circ s$ est A_χ-multilinéaire, π s'obtient avec la propriété universelle du produit tensoriel. ω est l'application A_χ-multilinéaire définie à l'aide des homomorphismes $\omega_l : \frac{A_\chi[G^J_l]}{\tilde e_\chi N^J_l A_\chi[G^J_l]} \longrightarrow \frac{A_\chi[G_p]}{\tilde e_\chi N(J)\otimes \mathbb{Z}_p}$ et de la multiplication dans le deuxième anneau. ϕ se définit par factorisation avec $\pi(\psi(\tilde e_\chi N^J_l)) = 0$. On peut vérifier que le diagramme commute. La propriété universelle du produit tensoriel donne donc , via ω, un homomorphisme réciproque à ϕ qui est un isomorphisme. On conclut la preuve en remarquant que chaque facteur de $\otimes_l \frac{A_\chi[G^J_{l,p}]}{\tilde e_\chi N^J_l A_\chi[G^J_{l,p}]}$ est un A_χ-module libre (de rang $\#G^J_{l,p}$ si $\tilde e_\chi N^J_l = 0$ et $\#G^J_{l,p} - 1$ sinon) ce qui montre que leur produit tensoriel est sans $\mathbb{Z}_p$-torsion. $\square$

Démonstration de 6.4 : Voir la preuve de 6.2. $\square$

Démonstration de 6.5 : Soit F_K le corps de genre abélien tel que $K \subset F_K \subset \mathbb{Q}(\zeta_{\mathrm{cond}(K)})$ et tel que $[F_K : K]$ est minimal. Alors l'extension F_K/K ne peut être ramifiée qu'aux places archimédiennes. F_K^+, le sous-corps réel maximal de K, est donc un sous-corps abélien sur $\mathbb{Q}$ du corps de classe de Hilbert de K. Donc $p \nmid [F_K^+ : K]$ et puisque $p \neq 2$, p ne divise pas $[F_K : K]$. Cela prouve que la restriction réalise un isomorphisme entre la p-partie du groupe de Galois de F_K sur $\mathbb{Q}$ et celle du groupe de Galois de K sur $\mathbb{Q}$. Les propriétés de restriction des sous-groupes d'inertie montrent que (K, p) vérifie l'hypothèse de 6.3 donc H.B. $\square$

Proposition 6.6. *Si $\#\mathcal{P}(K) \leq 2$, alors K vérifie H.A.*

Démonstration : Soit $J \subset \mathcal{P}$. Si $\#J \leq 1$, il est clair que $\frac{\mathbb{Z}[G(J)]}{N(J)}$ est sans $\mathbb{Z}$-torsion. On peut donc supposer que l'on a $J = \mathcal{P} = \{l_1, l_2\}$. On note ici $G_i = \mathrm{Gal}(K/K(\{l_i\}))$ (pour $i = 1$ ou 2). Soit $x \in \mathbb{Z}[G_K]$ dont l'image est de torsion. Il s'agit de montrer que $x \in N(\mathcal{P})$. Par hypothèse, il existe $s \in \mathbb{Z}$ tel que $sx \in N(J)$. Soit $H = G_1 \cap G_2$ et on désigne par $N_H = \sum_{h \in H} h$. On a évidemment $s\ x \in (\mathbb{Z}[G_K])^H = N_H\mathbb{Z}[G_K]$ et comme $\frac{\mathbb{Z}[G_K]}{N_H\mathbb{Z}[G_K]}$ est sans torsion on a aussi $x \in N_H\mathbb{Z}[G_K]$. Soit donc x' un élément de $\mathbb{Z}[G_K]$ tel que $x = N_H x'$. On fixe pour $i = 1$ ou 2 deux systèmes de représentants dans G_i, disons $\{g_{i,k}\}_{k=1}^{k=t_i}$ du quotient $\frac{G_i}{H}$. Par hypothèse, il existe deux éléments x_1 et x_2 de $\mathbb{Z}[G_K]$ qui vérifient :

$$sx = sN_H x' = N_{l_1}^{\mathcal{P}} x_1 + N_{l_2}^{\mathcal{P}} x_2 = N_H \left(\sum_{j=1}^{j=t_1} g_{1,j} x_1 + \sum_{j=1}^{j=t_2} g_{2,j} x_2 \right)$$

On utilise ici l'isomorphisme :

$$\begin{aligned} N_H\mathbb{Z}[G_K] &\xrightarrow{\psi} \mathbb{Z}[\frac{G_1}{H}] \otimes \mathbb{Z}[\frac{G_2}{H}] \\ N_H g &\mapsto g_{1,i}H \otimes g_{2,j}H \text{ avec } g_{1,i}g_{2,j}H = gH \end{aligned}$$

On voit alors qu'il existe deux éléments, disons $\bar{x}_1$ et $\bar{x}_2$ de $\mathbb{Z}[\frac{G_1}{H}] \otimes \mathbb{Z}[\frac{G_2}{H}]$ tels que :

$$s\ \psi(N_H x') = (\sum_{g \in \frac{G_1}{H}} g \otimes 1)\bar{x}_1 + (\sum_{g \in \frac{G_2}{H}} 1 \otimes g)\bar{x}_2$$

Comme d'autre part il est clair que :

$$\frac{\mathbb{Z}[\frac{G_1}{H}] \otimes \mathbb{Z}[\frac{G_2}{H}]}{\psi(N(J))} \cong \frac{\mathbb{Z}\ [\frac{G_1}{H}]}{(\sum_k g_{1,k})\ \mathbb{Z}\ [\frac{G_1}{H}]} \bigotimes \frac{\mathbb{Z}\ [\frac{G_2}{H}]}{(\sum_k g_{2,k})\ \mathbb{Z}\ [\frac{G_2}{H}]} \text{ est sans } \mathbb{Z}\text{-torsion,}$$

on a l'existence de deux éléments x_1' et x_2' tels que $\psi(N_H x') = (\sum_g g \otimes 1)x_1' + (\sum_g 1 \otimes g)x_2'$. En appliquant ψ^{-1} on trouve ici :

$$x = N_H x' = \sum_{i=1}^{i=t_1} g_{1,i}\psi^{-1}(x_1') + \sum_{i=1}^{i=t_2} g_{2,i}\psi^{-1}(x_2') \in N(\mathcal{P})$$

□

VI.2 Un contre-exemple avec $p = 2$.

Reprenons l'exemple $p = 2$ et $K = \mathbb{Q}(\sqrt{5 \times 17}, \sqrt{5 \times 13})$ de la remarque 4.3. C'est un corps bi-quadratique dont les sous-corps sont :

$$M_1 = \mathbb{Q}\left(\sqrt{5 \times 17}\right); \quad M_2 = \mathbb{Q}\left(\sqrt{13 \times 17}\right); \quad M_3 = \mathbb{Q}\left(\sqrt{5 \times 13}\right)$$

Pour $i \in \{1,2,3\}$ notons σ_i l'élément non trivial de $\mathrm{Gal}\,(M_i/\mathbb{Q})$, et ψ l'élément non trivial de $\mathrm{Gal}\,(\mathbb{B}_1/\mathbb{Q}) = \mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})\right)$. On remarque que pour $\#I = 1$ on a $K(I) = \mathbb{Q}$.

En utilisant le symbole de Legendre, on calcule les Frobenius suivants :

$$\left(\frac{M_1}{13}\right) = \left(\frac{M_1}{2}\right) = \sigma_1; \quad \left(\frac{M_2}{5}\right) = 1; \quad \left(\frac{M_2}{2}\right) = \sigma_2;$$

$$\left(\frac{M_3}{17}\right) = \sigma_3; \quad \left(\frac{M_3}{2}\right) = 1; \quad \left(\frac{\mathbb{B}_1}{5}\right) = \left(\frac{\mathbb{B}_1}{13}\right) = \psi; \quad \left(\frac{\mathbb{B}_1}{17}\right) = 1$$

Pour $l \in \{5,13,17\}$ on note $J_l = \mathcal{P} - \{l\}$. En partant de l'identité $2 = N_5^{\mathcal{P}} + N_{17}^{\mathcal{P}} + N_{13}^{\mathcal{P}} - N_5^{\mathcal{P}} N_{17}^{\mathcal{P}}$ et comme 17 est décomposé dans $\mathbb{B}_1$ et que $\epsilon_1(\{13\}) = \left(1 - \left(\frac{\mathbb{B}_1}{13}\right)\right)\epsilon_1(\emptyset)$ on obtient :

$$2\,\epsilon_1(\mathcal{P}) = (1-\psi)\epsilon_1(J_5) + (1-\sigma_3)\epsilon_1(J_{17}) + (1-\sigma_1\psi)\epsilon_1(J_{13}) \quad .$$

De plus comme on a

$$(1+\sigma_1)\epsilon_1(J_{13}) = \left(1 - \left(\frac{\mathbb{B}_1}{5}\right)\right)\left(1 - \left(\frac{\mathbb{B}_1}{17}\right)\right)\epsilon_1(\emptyset) = 0$$

et aussi

$$(1+\sigma_3)\epsilon_1(J_{17}) = 2(1-\psi)\epsilon_1(\emptyset)$$

on en déduit :

$$(\dagger) \qquad 2\,\epsilon_1(\mathcal{P}) = (1-\psi)\epsilon_1(J_5) + (1+\psi)\epsilon_1(J_{13}) + 2\,\epsilon_1(J_{17}) - 2\,(1-\psi)\epsilon_1(\emptyset)$$

Et en appliquant $(1-\psi)$ à $(\dagger)$ on trouve que :

$$2(1-\psi)(\epsilon_1(\mathcal{P}) - \epsilon_1(J_5) - \epsilon_1(J_{17}) + (1-\psi)\epsilon_1(\emptyset)) = 0$$

Comme $\mathcal{D}_1(K)$ est sans $\mathbb{Z}$-torsion on a :

$$(1-\psi)(\epsilon_1(\mathcal{P}) - \epsilon_1(J_5) - \epsilon_1(J_{17}) + (1-\psi)\epsilon_1(\emptyset)) = 0$$

Soit $u = (\epsilon_1(\mathcal{P}) - \epsilon_1(J_5) - \epsilon_1(J_{17}) + (1-\psi)\epsilon_1(\emptyset))$ on vient de montrer le :

Lemme 6.7.

$$u \in (\mathcal{D}_1(K))^{G_0^1}$$

$\square$

Il s'agit de montrer que $u \notin N_0^1 \mathcal{D}_1(K)$, auquel cas u sera un élément non trivial du $\widehat{H}^0\left(G_0^1, \mathcal{D}_1(K)\right)$, et cela montrera que la conclusion locale de 4.5 n'a pas lieu ici.

Pour ce faire nous utilisons la $\mathbb{Z}$-base de $N_0^1 \mathcal{D}_1(K)$ suivante :

Lemme 6.8. *Les entiers* $\{2; 2\ \epsilon_0\,(J_{13})\,; 2\ \epsilon_0\,(J_5)\}$ *forment une* $\mathbb{Z}$*-base de* $N_0^1\mathcal{D}_1\,(K)$

Démonstration : D'après la proposition 2.4 (2) et le lemme 2.3 (1) $N_0^1\mathcal{D}_1\,(K)$ est un $\mathbb{Z}$-module libre de rang 3, et il s'agit de vérifier que notre système est générateur.

Mais ici on a :

$$N_0^1\epsilon_1\,(\emptyset) = 2$$

$$N_0^1\epsilon_1\,(J_{17}) = 1$$

$$N_0^1\epsilon_1\,(J_{13}) = (1-\sigma_1)\epsilon_0\,(J_{13}) = 2\ \epsilon_0\,(J_{13})$$

$$N_0^1\epsilon_1\,(J_5) = (1-\sigma_2)\epsilon_0\,(J_5) = 2\ \epsilon_0\,(J_5)$$

et

$$N_0^1\epsilon_1\,(\mathcal{P}) = \left(1 - \left(\frac{K}{2}\right)\right)\epsilon_0\,(\mathcal{P})$$

Ici en utilisant $2 = N_5^{\mathcal{P}} + N_{17}^{\mathcal{P}} + N_{13}^{\mathcal{P}} - N_5^{\mathcal{P}}N_{17}^{\mathcal{P}}$ on peut vérifier que : $\epsilon_0\,(\mathcal{P}) = \epsilon_0\,(J_{13}) + \epsilon_0\,(J_{17})$ et cela nous donne :

$$N_0^1\epsilon_1\,(\mathcal{P}) = 2\ \epsilon_0\,(J_{13})$$

De plus pour $I \subset \mathcal{P}$ tel que $\#(I) = 1$, on a :

$$N_0^1\epsilon_1\,(I) = 1\ .$$

Ce qui prouve le lemme. $\square$

On peut maintenant, montrer la proposition suivante :

Proposition 6.9. $u \notin N_0^1\mathcal{D}_1\,(K)$

Démonstration : Il suffit de calculer dans la base de 6.8 les coefficients de $2u = N_0^1 u$ et de vérifier qu'ils ne sont pas divisibles par 2. Ce que l'on fait maintenant :

$$\begin{aligned} N_0^1 u &= N_0^1\epsilon_1\,(\mathcal{P}) - N_0^1\epsilon_1\,(J_5) - N_0^1\epsilon_1\,(J_{17}) + N_0^1(1-\psi)\epsilon_1\,(\emptyset) \\ &= 2\ \epsilon_0\,(J_{13}) - 2\ \epsilon_0\,(J_5) \notin 2\ N_0^1\mathcal{D}_1\,(K) \end{aligned}$$

$\square$

VI.3 Un contre-exemple avec $p = 3$.

Cet exemple avec $p = 3$, un peu plus difficile à décrire explicitement, est un peu plus significatif. Pour les problèmes survenant en 2 on pourra se rapporter à [Ku] où une amélioration explicite en 2 de $C(K)$ est construite. Les calculs nécessaires à l'élaboration de cet exemple ont été réalisés à l'aide du logiciel GP PARI. Soit $m = 7.181.673.3037$, on va travailler dans un sous-corps de $\mathbb{Q}(\zeta_m)$. Les premiers $l_i \in \{7, 181, 673, 3037\}$ ont été choisis pour vérifier :

(1) $$\forall i \ : \ l_i \equiv 1[3] \ \text{ et } \ \forall j \ : \ i \neq j \implies l_i \text{ est un cube modulo } l_j$$

Les propriétés arithmétiques d'un corps K de conducteur m qui servent notre démarche sont les suivantes :

(a-) $$G_K \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$$

(b-) Chacun des quatre sous-groupes cycliques non triviaux de G_K est le sous-groupe d'inertie de l'un des quatre éléments de $\mathcal{P}$ (ici cela revient à dire que dans chaque sous-corps cubique de K, exactement trois éléments de $\mathcal{P}$ sont ramifiés).

Plusieurs sous-corps bi-cubiques de $\mathbb{Q}(\zeta_m)$ vérifient la condition (b-). A titre d'exemple, on prend pour K le corps de rupture (et de décomposition) du polynôme qui suit :

$$\begin{aligned}
&X^9 - 3X^8 - 6335955X^7 + 2459856427X^6 + 9080370048953X^5\\
&- 4520985235480441X^4 - 1924917910115362484X^3\\
&+ 843128942882377125914X^2 + 1694606740972576814994 9X\\
&- 147058492763020663161837 77
\end{aligned}$$

Les quatre sous-corps cubiques de K (disons M_1, M_2, M_3, M_4) sont respectivement les corps de rupture des polynômes P_1, P_2, P_3, P_4 et respectivement les corps d'inertie dans K des premiers l_1, l_2, l_3, l_4 suivants :

$$\begin{aligned}
P_1 &= X^3 - X^2 - 123315360X + 296093881867; \quad l_1 = 7\\
P_2 &= X^3 - X^2 - 4769102X + 3507409816; \quad l_2 = 181\\
P_3 &= X^3 - X^2 - 1282626X - 442363571; \quad l_3 = 673\\
P_4 &= X^3 - X^2 - 284230X + 38592163; \quad l_4 = 3037
\end{aligned}$$

Enfin on a besoin de connaître le corps de décomposition de 3 dans K. Ici on a $K_{\text{dec}} = M_4$. On note $\{1, \psi, \psi^2\}$ les éléments de G_0^1 caractérisés par :

$$\psi = \left(\frac{\mathbb{B}_1}{7}\right)^{-1} = \left(\frac{\mathbb{B}_1}{673}\right)^{-1} \quad \text{et} \quad \psi^2 = \left(\frac{\mathbb{B}_1}{3037}\right)^{-1}$$

Pour $l \in \mathcal{P}$ on notera $J_l = \mathcal{P} - \{l\}$. En utilisant l'identité $3 = -N_7^{\mathcal{P}} N_{181}^{\mathcal{P}} + \sum_{l \in \mathcal{P}} N_l^{\mathcal{P}}$, le lemme 1.3 et le fait que 181 est décomposé dans $\mathbb{B}_1$ on constate qu'on a :

$$3\epsilon_1(\mathcal{P}) = \sum_{l \in \mathcal{P}} N_l^{\mathcal{P}} \epsilon_1(\mathcal{P}) - N_7^{\mathcal{P}} N_{181}^{\mathcal{P}} \epsilon_1(\mathcal{P}) = \sum_{l \in \mathcal{P}} \left(1 - \left(\frac{K(J_l)}{l} \right)^{-1} \left(\frac{\mathbb{B}_1}{l} \right)^{-1} \right) \epsilon_1(J_l)$$

Mais ici les l ont été choisis de telle sorte que $\left(\frac{K(J_l)}{l}\right) = 1$, et, notre équation se réécrit :

$$(\dagger) \quad 3\epsilon_1(\mathcal{P}) = (1-\psi)\epsilon_1(J_7) + (1-\psi)\epsilon_1(J_{673}) + (1-\psi^2)\epsilon_1(J_{3037})$$

En utilisant les identités formelles $(1-\psi)(2-\psi-\psi^2) = 3(1-\psi)$, $(1-\psi^2)(2-\psi-\psi^2) = 3(1-\psi)(1+\psi)$ et $(2-\psi-\psi^2) = (1-\psi)(1-\psi^2)$ on voit qu'en multipliant $(\dagger)$ par $2-\psi-\psi^2$ on obtient:

$$3(1-\psi)(1-\psi^2)\epsilon_1(\mathcal{P}) = 3(1-\psi)\left(\epsilon_1(J_7) + \epsilon_1(J_{673}) + (1+\psi)\epsilon_1(J_{3037})\right)$$

On note $u = (1-\psi^2)\epsilon_1(\mathcal{P}) - (\epsilon_1(J_7) + \epsilon_1(J_{673}) + (1+\psi)\epsilon_1(J_{3037}))$. Comme $\mathcal{D}_1(K)$ est sans $\mathbb{Z}$-torsion, cette dernière identité donne $(1-\psi)u = 0$ c'est-à-dire $u \in \mathcal{D}_1(K)^{G_0^1}$. Notre but dans cette section est de montrer :

Proposition 6.7. *$u \in \mathcal{D}_1(K)^{G_0^1}$ et $u \notin N_0^1 \mathcal{D}_1(K)$ de telle sorte que l'on a : $\hat{H}^0(G_0^1, \mathcal{D}_1(K)) \neq 0$ et que $\mathcal{D}_1(K) \otimes \mathbb{Z}_p \not\simeq \left(\mathbb{Z}_p[G_0^1]\right)^{g_{\mathcal{P}} f_{\mathcal{P}} - g_{\mathcal{P}} + 1} \oplus \left(\frac{\mathbb{Z}_p[G_0^1]}{N_0^1}\right)^{g_{\mathcal{P}}+1}$*

Démonstration : Compte tenu de ce qui précède, il reste à voir que $u \notin N_0^1 \mathcal{D}_1(K)$. En fait, on montre quelque chose d'un peu plus fort :

Lemme 6.8. *$u \notin \mathcal{D}_0(K)$.*

Remarque 6.9. *Cela donne de plus que $u \in C(K_1)^{G_0^1} - C(K)$, et montre que l'hypothèse B n'est pas superflue, par exemple vis à vis de la proposition 5.14*

Démonstration de 6.8 : On utilise une $\mathbb{Z}$-base de $\mathcal{D}_0(K)$. Dans ce cas celle-ci est facile à construire. En fait les relations du lemme 1.3 permettent de voir, comme $\mathcal{D}_0(K)$ est sans $\mathbb{Z}$-torsion et que tous les $l \in \mathcal{P}$ sont décomposés dans les $K(J_l)$, que $\epsilon_0(\mathcal{P}) = 1$. On en déduit, en considérant les rangs sur $\mathbb{Z}$, que $\mathcal{D}_0(K)$ coïncide avec la somme directe interne :

$$\mathcal{D}_0(K) = \mathbb{Z}\, 3 \oplus \bigoplus_{l \in \mathcal{P}} \frac{\mathbb{Z}[G(J_l)]}{N_{\mathbb{Q}}^{K(J_l)}}\, \epsilon_0(J_l) \oplus \bigoplus_{l \in \mathcal{P}} \mathbb{Z}\, l.$$

Pour conclure que $u \notin \mathcal{D}_0(K)$, il suffit de calculer les coefficients dans cette base de $3u = N_0^1 u$. Or comme $K_{\mathrm{dec}} = K(J_{3037})$ on a $N_0^1 \epsilon_1(J_{3037}) = 1$, et comme $N_0^1 \epsilon_1(\mathcal{P}) = 1$, on en déduit :

$$\begin{aligned} N_0^1 u &= -N_0^1 \epsilon_1(J_7) - N_0^1 \epsilon_1(J_{673}) \\ &= -\left(1 - \left(\frac{K(J_7)}{3}\right)^{-1}\right) \epsilon_0(J_7) - \left(1 - \left(\frac{K(J_{673})}{3}\right)^{-1}\right) \epsilon_0(J_{673}) \end{aligned}$$

Et comme 3 est inerte dans $K(J_7)$ et $K(J_{673})$, ces coefficients ne sont pas divisibles par 3. $\square$

VII Les p-unités cyclotomiques de Solomon

Dans ce chapitre nous appliquons les techniques qui précèdent aux modules des p-unités cyclotomiques définies dans [So 1]. Comme dans [So 1] on suppose que p est totalement décomposé dans K. On reprend tout d'abord la construction de [So 1]. Pour toute la suite on fixe un $\mathbb{Z}_p$-générateur γ de G_0^∞, et on notera $E_p(K_n)$ le groupe des p-unités de K_n, c'est-à-dire les éléments de K_n de valuations nulles en tout idéal de K_n ne divisant pas p.

VII.1 Construction des p-unités cyclotomiques.

Soit I tel que $\emptyset \neq I \subset \mathcal{P}$. Comme p est totalement décomposé dans K, pour tout $m \geq n$ on a $N_0^m \epsilon_m(I) = 1$, et le théorème de Hilbert 90, donne l'existence d'un unique $\beta_m(I) \in K_m(I)^\times / K(I)^\times$, tel que :

$$(\beta_m(I))^{\gamma-1} = \epsilon_m(I)$$

De plus comme pour tout $m \geq n > 0$, on a $N_n^m \epsilon_m(I) = \epsilon_n(I)$, on a évidemment aussi $N_n^m \beta_m(I) = \beta_n(I)$, en notant N_n^m l'application :

$$K_m(I)^\times / K(I)^\times \longrightarrow K_n(I)^\times / N_n^m K(I)^\times$$

On fixe un $n \in \mathbb{N}$, pour tout $m > n$, les éléments $N_n^m \beta_m(I)$ définissent, via la surjection $K_n(I)^\times / N_n^m(K(I)^\times) \longrightarrow K_n(I)^\times / \left(K_n(I)^\times\right)^{p^{m-n}}$ une suite d'éléments cohérents pour les applications de restrictions naturelles :

$$K_n(I)^\times / \left(K_n(I)^\times\right)^{p^{m-n}} \longrightarrow K_n(I)^\times / \left(K_n(I)^\times\right)^{p^{m-1-n}}$$

Dans [So 2] les suites définies ainsi ont été notées :

Définition 7.1.

$$\kappa_n(I,\gamma) = (N_n^{n+1}(\beta_{n+1}(I)), ..., N_n^m(\beta_m(I)), ...) \in \varprojlim_{m>n} \left(K_n(I)^\times / \left(K_n(I)^\times\right)^{p^{m-n}}\right)$$

Ici, pour simplifier les notations on les notera $\kappa_n(I)$, et on rapelle que γ est fixé une fois pour toute. Toujours dans [So 1] les valuations (à valeur dans $\mathbb{Z}_p$) de ces $\kappa_n(I)$ ont été calculées pour $n = 0$. En fait comme ces valuations sont nulles en tout idéal ne divisant pas p, et que les idéaux divisant p se ramifient totalement dans l'extension K_∞/K, les calculs de [So 1] valent pour $n > 0$.

Lemme 7.2. *Soit $\emptyset \neq I \subset \mathcal{P}$, et soit $\mathfrak{P}$ un idéal premier de $K_n(I)$, et $v_{\mathfrak{P}}$ la valuation à valeurs dans $\mathbb{Z}_p$ associée à $\mathfrak{P}$ de $\varprojlim_{m>n} K_n(I)^\times / (K_n(I)^\times)^{p^{m-n}}$. Cette valuation est l'application limite des valuations modulo p^{m-n} sur $K_n(I)^\times / (K_n(I)^\times)^{p^{m-n}}$. Alors on a :*
(1) Si $\mathfrak{P}$ ne divise pas p, alors $v_{\mathfrak{P}}(\kappa_n(I)) = 0$
(2) Si $\mathfrak{P}$ divise p, soient $\wp = \mathfrak{P} \cap K(I)$ et $\sigma_\wp$ le plongement de $K(I)$ dans $\mathbb{Q}_p$ correspondant à $\wp$. D'autre part G_0^∞ s'identifie naturellement avec un sous-groupe de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)_\infty / \mathbb{Q}\right)$ qui correspond via l'application du corps de classe au sous-groupe $(1+q\mathbb{Z}_p)$ de $\mathbb{Z}_p^\times$. On note $\tilde{\gamma}$ l'élément de $(1+q\mathbb{Z}_p)$ qui correspond à γ, et on note log_p le logarithme p-adique. On a :

$$v_{\mathfrak{P}}(\kappa_n(I)) = v_\wp(N_0^n(\kappa_n(I))) = v_\wp(\kappa_0(I)) = \frac{log_p\left(\sigma_\wp\left(\epsilon_0\left(I\right)\right)\right)}{log_p\left(\tilde{\gamma}\right)}$$

Démonstration : Pour (2) la dernière égalité est le théorème 2.1 de [So 1], la première vient de ce que $\wp$ se ramifie totalement dans $K_n(I)/K(I)$ et on déduit la deuxième de l'identité $N_n^m(\kappa_m(I)) = \kappa_n(I)$ qui s'obtient à partir de $N_n^m(\epsilon_m(I)) = \epsilon_n(I)$. □

Démonstration de (1) : On adapte au cas $n > 0$ la preuve de la proposition 2.2 de [So 1]. Il s'agit de vérifier que pour chaque $m > n$ on a $v_{\mathfrak{P}}\left(N_n^m\left(\beta_m(I)\right)\right) \equiv 0\ [p^{m-n}]$. Soit $\overline{\gamma_n}$ la restriction de γ^{p^n} à K_m et soit $D = \sum_{i=1}^{i=p^{m-n}-1} i\ \overline{\gamma_n}^i \in \mathbb{Z}[G_n^m]$, de telle sorte que l'on ait : $(\overline{\gamma_n} - 1)\,D = p^{m-n} - N_n^m$ Soit $b \in \beta_m(I) \subset K_m(I)$ et soit $k = N_n^m(b)$. Soit $\delta = \sum_{i=0}^{i=p^n-1} \gamma^i \in \mathbb{Z}[G_0^m]$, on a $(\overline{\gamma_n} - 1) = \delta(\gamma - 1)$. On note α la p-unité suivante $\alpha = (\epsilon_m(I))^\delta$.

Alors on a :

$$b^{\overline{\gamma_n}-1} = \alpha$$

et en appliquant D on trouve :

$$k = b^{p^{m-n}} / \alpha^D$$

Soit $\tilde{\mathfrak{P}}$ un premier de $K_m(I)$ divisant $\mathfrak{P}$. Comme $\mathfrak{P}$ ne divise pas p il ne se ramifie pas dans $K_m(I)$ et cela donne :

$$v_{\mathfrak{P}}\left(N_n^m\left(\beta_m(I)\right)\right) \equiv v_{\mathfrak{P}}(k) \equiv v_{\tilde{\mathfrak{P}}}(k) \equiv -v_{\tilde{\mathfrak{P}}}\left(\alpha^D\right) \equiv 0$$

comme attendu. □

Lemme 7.3. *Soit $I \subset \mathcal{P}$. Alors on a :*

$$\kappa_n(I) \in \varprojlim_{m>n} \left(E_p\left(K_n(I)\right) / \left(E_p\left(K_n(I)\right)^{p^{m-n}}\right)\right) \subset \varprojlim_{m>n} \left(K_n(I)^\times / \left(K_n(I)^\times\right)^{p^{m-n}}\right)$$

Démonstration : Il s'agit de montrer que $N_n^m\beta_m(I)\cap E_p(K_n(I))$ est non vide pour tout m. On note $\mathcal{I}'(K_n(I))$ le groupe des idéaux fractionnaires de $K_n(I)$ étranger à p. Soit θ l'homomorphisme qui envoie $a\in K_n(I)$ sur la projection naturelle dans $\mathcal{I}'(K_n(I))$ de l'idéal principal (a). Soit $P'(K_n(I))$ l'image de θ. Le quotient $\mathcal{I}'(K_n(I))/P'(K_n(I))$ est fini, car c'est un quotient du groupe des classes de $K_n(I)$. Soit p^s la puissance de p qui divise son annulateur d. Soit $k\in N_n^{m+s}(\beta_{m+s}(I))$. D'après le lemme 7.2 (1), on a $\theta(k)\in(p^{m+s-n}\mathcal{I}'(K_n(I)))\cap P'(K_n(I))$. Donc il existe $\mathfrak{a}\in\mathcal{I}'(K_n(I))$ tel que $p^{m+s-n}\mathfrak{a}=\theta(k)\in P'(K_n(I))$. Comme on a aussi $d\ \mathfrak{a}\in P'(K_n(I))$ et que p^s est le p.g.c.d. de d et p^{m+s-n}, on en déduit que $p^s\mathfrak{a}\in P'(K_n(I))$. Donc on a $\theta(k)\in p^{m-n}P'(K_n(I))=\theta\left(K_n(I)^{p^{m-n}}\right)$. C'est-à-dire qu'il existe un $x\in K_n(I)$ tel que $y=kx^{-p^{m-n}}\in\ker\theta=E_p(K_n(I))$. Comme $k\in N_n^m(\beta_m(I))$ on a $y\in N_n^m\beta_m(I)\cap E_p(K_n(I))$. $\square$

A partir d'ici on va travailler dans le module $\varprojlim_{m>n} E_p(K_n)/E_p(K_n)^{p^{m-n}}$ que l'on identifie avec $E_p(K_n)\otimes\mathbb{Z}_p$. Les p-unités qui précèdent ont été définies de telle sorte qu'elles vérifient :

Lemme 7.4. $\kappa_n(I)^{\gamma-1}=\epsilon_n(I)\otimes 1\in E_p(K_n)\otimes\mathbb{Z}_p$

$\square$

On va maintenant s'intéresser à la $\mathbb{Z}_p[G_{K_n}]$-structure du module engendré par ces $\kappa_n(I)$.

VII.2 Caractères et premières propriétés de ces p-unités.

A partir d'ici on note additivement l'action de $\mathbb{Z}_p[G_{K_n}]$ sur $E_p(K_n)\otimes\mathbb{Z}_p$.

Définition 7.5. *On note $\mathcal{K}_n(K)$ le $\mathbb{Z}_p[G_{K_n}]$-module engendré dans $E_p(K_n)\otimes\mathbb{Z}_p$ par :*

$$\mathcal{K}_n(K)=\langle\{\epsilon_n(\emptyset)\}\cup\{\kappa_n(I);\emptyset\neq I\subset\mathcal{P}\}\rangle$$

On commence par calculer le caractère (à valeurs dans $\mathbb{Q}_p$) de ce module. Soit χ_{reg} le caractère régulier pour G_{K_n} (i.e. le caractère de $\mathbb{Q}_p[G_{K_n}]$) et soit $\chi(\mathcal{K}_n(K))$ le caractère donné par le $\mathbb{Q}_p$-espace $\mathcal{K}_n(K)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$, alors on a :

Lemme 7.6.

$$\chi(\mathcal{K}_n(K))=\chi_{\mathrm{reg}}$$

Démonstration : Il suit de l'équation (23) de [So 2] que ce lemme est vrai pour $n=0$. Pour $n>0$, il suffit d'utiliser la suite exacte suivante :

$$1\longrightarrow\mathcal{K}_0(K)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\longrightarrow\mathcal{K}_n(K)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\xrightarrow{\gamma-1}(\mathcal{D}_n(K)\cap E(K_n))\otimes_{\mathbb{Z}}\mathbb{Q}_p\longrightarrow 1$$

L'exactitude à gauche provient des identités $N_n^m \kappa_n(I) = \kappa_0(I)$, et $N_n^m \epsilon_n(\emptyset) = p$. L'exactitude à droite est donnée par 7.4 et le fait que $\mathcal{D}_n(K) \cap E(K_n)$ est engendré par $(\gamma - 1)(\epsilon_n(\emptyset))$ et les autres $\epsilon_n(I)$. Enfin le caractère de $\mathcal{D}_n(K) \cap E(K)$ se déduit facilement du lemme 2.3 (5) de la proposition 2.4 (1) et du fait que $N_{\mathbb{Q}}^{K_n}(\mathcal{D}_n(K)) \simeq \mathbb{Z}$. $\square$

On va maintenant établir des relations de normes entre les $\kappa_n(I)$

Lemme 7.7. *Soit $I \subset \mathcal{P}$ et soit $l \in I$.*
(1) *Si $I - \{l\} \neq \emptyset$, alors on a :*

$$N_{K_n(I-\{l\})}^{K_n(I)}(\kappa_n(I)) = \left(1 - \left(\frac{K_n(I-\{l\})}{l}\right)^{-1}\right)(\kappa_n(I))$$

(2) *Si $I = \{l\}$, il existe un unique $y_l = y_l(n,\gamma) \in \mathbb{Z}_p[G_0^n]$ tel qu'on ait :*

$$N_{\mathbb{B}_n}^{K_n(I)}(\kappa_n(I)) = y_l \ \epsilon_n(\emptyset)$$

Démonstration de (1) : Soit $m \in \mathbb{N}$, $m > n$, et soit ψ l'application injective qui factorise la multiplication par $(\gamma - 1)$: $K_n^\times(I-\{l\})/K^\times(I-\{l\}) \longrightarrow K_n^\times(I-\{l\})$, on a :

$$\begin{aligned}
\psi\left(N_{K(I-\{l\})}^{K(I)}(\beta_m(I))\right) &= N_{K(I-\{l\})}^{K(I)}(\epsilon_m(I)) \\
&= \left(1 - \left(\frac{K_m(I-\{l\})}{l}\right)^{-1}\right)\epsilon_m(I-\{l\}) \\
&= \psi\left(\left(1 - \left(\frac{K_m(I-\{l\})}{l}\right)\right)\beta_m(I-\{l\})\right)
\end{aligned}$$

On en déduit l'identité $\left(\text{dans } K_n^\times(I-\{l\})/\left(K_n^\times(I-\{l\})\right)^{p^{m-n}}\right)$:

$$N_{K(I-\{l\})}^{K(I)} N_n^m \beta_m(I) = \left(1 - \left(\frac{K_m(I-\{l\})}{l}\right)^{-1}\right) N_n^m \beta_m(I)$$

Et en passant à la limite, cette identité donne (1). $\square$

Démonstration de (2) : En appliquant ce qui précède au cas $I = \{l\}$, on obtient l'identité (dans $E_p(\mathbb{B}_n) \otimes \mathbb{Z}_p$) :

$$(\gamma - 1) N_{\mathbb{B}_n}^{K_n(\{l\})} \kappa_n(\{l\}) = \left(1 - \left(\frac{\mathbb{B}_n}{l}\right)^{-1}\right)\epsilon_n(\emptyset)$$

Comme la restriction de γ à K_n engendre G_0^n, il existe un $z_l \in \mathbb{Z}_p[G_0^n]$ tel que $(\gamma - 1)\ z_l = \left(\frac{\mathbb{B}_n}{l}\right)^{-1}$. On voit donc que $N_{\mathbb{B}_n}^{K_n(\{l\})}(\kappa_n(\{l\})) - z_l \epsilon_n(\emptyset)$ appartient à $(E_p(K_n) \otimes \mathbb{Z}_p)^{G_{K_n}} = \mathbb{Z}_p\ (p \otimes 1)$.

Mais comme on a $p = N_0^n \epsilon_n(\emptyset)$ il existe un $t_l \in \mathbb{Z}_p[G_0^n]$ qui vérifie :

$$N_{\mathbb{B}_n}^{K_n(I)}(\kappa_n(I)) - z_l \epsilon_n(\emptyset) = t_l \epsilon_n(\emptyset)$$

Pour conclure à l'existence de y_l il suffit de poser $y_l = z_l + t_l$. D'autre part son unicité provient de ce que l'annulateur dans $\mathbb{Z}_p[G_0^n]$ de $\epsilon_n(\emptyset) \otimes 1$ est nul. $\square$

VII.3 $\mathbb{Z}_p[G_0^n]$-structure de $\mathcal{K}_n(K)$.

On va appliquer des techniques très semblables à celles des chapitres III et IV, pour étudier le module $\mathcal{K}_n(K)$. Par contre ici les preuves se simplifient considérablement car on n'a pas la gêne occasionnée par un équivalent de $\mathcal{V}_n$. On commence par quelques définitions.

Définition 7.8. *on reprend la notation $w_n(J)$ des chapitres III et IV, ainsi que la relation d'ordre $\prec$ de 3.4. Soient $n \in \mathbb{N}$ et $J \subset \mathcal{P}$.*
(1) *On forme la somme directe :*

$$\overline{\mathcal{L}_n(J)} = \bigoplus_{I \prec J} \mathbb{Z}_p[G(J)] \otimes \mathbb{Z}_p[G_0^n]\ w_n(I)$$

et de même qu'en 3.5, pour $I \prec J$ on considérera $\overline{\mathcal{L}_n(I)}$ comme un sous-module (facteur direct) de $\overline{\mathcal{L}_n(J)}$. $\overline{\mathcal{L}_n(J)}$ correspond à $\mathcal{L}_n(J)$ et on a $\overline{\mathcal{L}_n(J)} = \mathcal{L}_n(J) \otimes \mathbb{Z}_p$.
(2) *Soit $l \in J$, on définit $T_n(J,l) \in \overline{\mathcal{L}_n(J)}$ par :*

$$\begin{aligned} T_n(J,l) = {} & N_{K(J-\{l\})}^{K(J)} \otimes 1\ w_n(J) - w_n(J-\{l\}) \\ & + \left(\left(\frac{K(J-\{l\})}{l} \right)^{-1} \otimes \left(\frac{\mathbb{B}_n}{l} \right)^{-1} \right) w_n(J-\{l\}) \end{aligned}$$

lorsque $J \neq \{l\}$, auquel cas on a $T_n(J,l) = R_n(J,l) \otimes 1$ et par :

$$T_n(J,l) = \left(N_{\mathbb{Q}}^{K(J)} \otimes 1 \right)\ w_n(J) - (1 \otimes y_l)\ w_n(\emptyset)$$

lorsque $J = \{l\}$.
(3) *On désignera par $\mathcal{T}_n(J)$ le sous $\mathbb{Z}_p[G_K] \otimes \mathbb{Z}_p[G_0^n]$-module de $\overline{\mathcal{L}_n(J)}$ engendré par les $T_n(I,l)$ suivants :*

$$\mathcal{T}_n(J) = \langle \{ T_n(I,l) ; I \subset \mathcal{P} ; I \prec J ; l \in I \} \rangle$$

$\mathcal{T}_n(J)$ est l'analogue de $\mathcal{H}_n(J)$

(4) *On obtient évidemment une surjection de $\mathbb{Z}_p[G_K] \otimes \mathbb{Z}_p[G_0^n]$-modules $\overline{\mathcal{L}_n(\mathcal{P})} \longrightarrow \mathcal{K}_n(K)$, en envoyant les $w_n(I)$ sur $\kappa_n(I)$, pour $I \neq \emptyset$, et $w_n(\emptyset)$ sur $\epsilon_n(\emptyset)$. D'après le lemme 7.7 cet homomorphisme se factorise en :*

$$\eta_n\ :\ \frac{\overline{\mathcal{L}_n(\mathcal{P})}}{\mathcal{T}_n(\mathcal{P})} \longrightarrow \mathcal{K}_n(K)$$

Proposition 7.9. *On reprend les notations $G(I)$ et $N(I)$ du chapitre III. Posons $\mathcal{A} = \mathbb{Z}_p$ si (K,p) vérifie H.B., et $\mathcal{A} = \mathbb{Q}_p$ sinon. Pour tout $I \subset \mathcal{P}$, il existe une surjection de $\mathcal{A}[G_0^n]$-modules :*

$$\psi_n(I) \ : \ \bigoplus_{J \prec I} \frac{\mathbb{Z}_p[G(J)]}{N(J) \otimes \mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathcal{A}[G_0^n] \longrightarrow \frac{\overline{\mathcal{L}_n\,(I)}}{\mathcal{T}_n\,(I)} \otimes_{\mathbb{Z}_p} \mathcal{A}$$

Démonstration : La preuve est exactement calquée sur celle de la proposition 4.6. Ici $\mathcal{K}_n(K)$ joue le rôle de $\mathcal{D}_n\,(K)$, $\mathcal{T}_n\,(I)$ celui de $\mathcal{H}_n\,(I)$, $\mathcal{A}$ celui de $\mathcal{R}$. Les deux ingrédients importants sont ici aussi la $\mathcal{A}[G_0^n]$-liberté du module de départ de $\psi_n(I)$ et le fait que les relations sont des relations de normes. $\square$

On obtient ainsi les deux théorèmes suivants (analogues des théorèmes 4.5 et 3.6).

Théorème 7.10. *Supposons que (K,p) vérifie H.B., alors l'application composée $\eta_n \circ \psi_n(\mathcal{P})$ est un isomorphisme entre deux $\mathbb{Z}_p[G_0^n]$-modules libres de rang $g_{\mathcal{P}} f_{\mathcal{P}}$. En particulier η_n est un isomorphisme de $\mathbb{Z}_p[G_K] \otimes \mathbb{Z}_p[G_0^n]$-modules.*

Démonstration : Les lemmes 4.9 et 7.6 donnent les identités :

$$\mathrm{rang}_{\mathbb{Z}_p}\left(\bigoplus_{J \subset \mathcal{P}} \frac{\mathbb{Z}_p[G(J)]}{N(J) \otimes \mathbb{Z}_p} \bigotimes_{\mathbb{Z}_p} \mathbb{Z}_p[G_0^n] \right) = \mathrm{rang}_{\mathbb{Z}_p}(\mathcal{K}_n(K)) = g_{\mathcal{P}} f_{\mathcal{P}} p^n$$

Donc comme $\eta_n \circ \psi_n(\mathcal{P})$ est surjective et que $(\oplus_{J \subset \mathcal{P}} \mathbb{Z}_p[G(J)]/N(J) \otimes \mathbb{Z}_p) \otimes \mathbb{Z}_p[G_0^n]$ est sans $\mathbb{Z}_p$-torsion le noyau de cette composée est nul. $\square$

Théorème 7.11. *En toute généralité le noyau de η_n est fini.*

Démonstration : En appliquant le même raisonnement que pour 7.10 on constate que le noyau de l'application obtenue à partir de η_n par tensorisation avec $\mathbb{Q}_p$ est nul. Et cela entraine que le noyau de η_n est fini. $\square$

Remarque 7.12. *En utilisant la même démarche que dans [So 1], on peut voir que $\mathcal{K}_n(I)$ est sans $\mathbb{Z}_p$-torsion (cela ne pose de problèmes que lorsque $p = 2$). De cette manière on montre que $\ker \eta_n$ coïncide avec la $\mathbb{Z}_p$-torsion de $\overline{\mathcal{L}_n\,(\mathcal{P})}/\mathcal{T}_n(\mathcal{P})$.*

Bibliographie.

[Ba] H. Bass, *Generators and relations for cyclotomic units*, Nagoya Math. J. **27** 401–407 (1966)

[B B C O] C. Batut, D. Bernardi, H. Cohen, et M. Olivier, *User's guide to PARI-GP, version 1.39.03*, disponible sur ftp:megrez.math.u-bordeaux.fr (1995)

[Be] J.-R. Belliard, *Sur la structure galoisienne des unités circulaires dans les $\mathbb{Z}_p$-extensions*, à paraître dans J. Number Theory

[Br] A. Brumer, *On the units of algebraic number fields,* Mathematika **14** 121–124 (1967)

[C F] J. Cassels, A. Fröhlich (eds) Algebraic Number Theory, Academic Press, 1967

[E] V. Ennola, *On Relations between cyclotomic units*, J. Number Theory **4** 236–247 (1972)

[F K N] V. Fleckinger, M. Kolster, T. Nguyen Quang Do, *Twisted S-units, p-adic class number formulas, and the Lichtenbaum conjectures*, Duke Math. J. **84** 679–717 (1996)

[F] A. Fröhlich, *Units in real abelian fields*, J. Reine Angew. Math. **429** 191–217 (1992)

[Gi] R. Gillard, *Remarques sur les unités cyclotomiques et elliptiques*, J. of Number Theory **11** 21–48 (1979)

[G K] R. Gold, J. M. Kim, *Bases for cyclotomic units*, Compositio Math. **71** 13–28 (1989)

[Gree 1] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** 263–284 (1976)

[Gree 2] R. Greenberg, *On p-adic L-functions and cyclotomic fields II*, Nagoya Math. J. **67** 139–158 (1977)

[Grei 1] C. Greither, *Über relativ-invariante Kreiseinheiten und Stickelberger-Elemente*, Manuscripta Math. **80** 27–43 (1993)

[Grei 2] C. Greither, *Sur les normes universelles dans les $\mathbb{Z}_p$-extensions*, J. Th. Nombres de Bordeaux **6** 205–220 (1994)

[H] Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952

[Ki 1] J. M. Kim, *Cohomology groups of cyclotomic Units*, J. Algebra **152** 514–519 (1992)

[Ki 2] J. M. Kim, *Units and cyclotomic units in $\mathbb{Z}_p$-extensions*, Nagoya Math. J. **140** 101–116 (1995)

[K S] J. Kraft, R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Special issue in honour of Frans Oort, Compositio Math. **97** 135–155 (1995)

[Ku] R. Kučera, *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, J. Number Theory **56** 139–166 (1996)

[Ku N] R. Kučera, J. Nekovář, *Cyclotomic units in $\mathbb{Z}_p$-extensions*, J. Algebra **171** 457–472 (1995)

[La 1] S. Lang, *Algebraic Number Theory*, 2^e édition, GTM **110**, Springer-Verlag, New-York 1994

[La 2] S. Lang, *Introduction to Cyclotomic Fields I and II*, combined second edition, GTM **121**, Springer-Verlag, New-York 1990

[Le] Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. deutsch. Akad. Wiss., Berlin (1953)

[Se 1] J.-P. Serre, *Corps locaux*, Hermann, Paris 1968

[Se 2] J.-P. Serre, *Représentation linéaire des groupes finis*, Hermann, Paris 1967

[Si] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** 181–234 (1981)

[So 1] D. Solomon, *On a construction of $p-$units in abelian fields*, Invent. Math. **109** 329–350 (1992)

[So 2] D. Solomon, *Galois relations for cyclotomic numbers and p-units*, J. Number Theory **46** 158–178 (1994),

[W] L. Washington, *Introduction to Cyclotomic Fields*, 2^e édition, GTM **83**, Springer-Verlag 1982