SUR LA STRUCTURE GALOISIENNE DES UNITÉS CIRCULAIRES DANS LES $\mathbb{Z}_p$-EXTENSIONS

Jean-Robert Belliard

département de mathématiques pures
Université de Bordeaux I
351 Cours de la Libération
33405 Talence, France

Résumé : Le but de cet article est de décrire le comportement galoisien des unités circulaires dans la $\mathbb{Z}_p$-extension $K_\infty = \cup_n K_n$ d'un corps abélien réel $K = K_0$. Pour ce faire on introduit un sous-module de $K_n^\times$ qui est très proche de l'intersection des images des normes relatives (dans K_∞), appliquées à ces unités.

Sous des hypothèses assez faibles, on décrit la structure locale (éventuellement globale) de ce module, qui se révèle être la plus simple possible (compte-tenu de son caractère). On en déduit, par exemple, la cohomologie des unités circulaires. On construit également des exemples explicites de corps pour lesquels ni la cohomologie des unités circulaires, ni la structure de notre sous-module, ne sont aussi simples.

Introduction

L'objet de cet article est l'étude de la structure galoisienne relative des unités circulaires dans les $\mathbb{Z}_p$-extensions de corps abéliens sur $\mathbb{Q}$. Plus précisément, on définit un module D_n ( ), et on décrit sa structure locale ou globale comme une somme directe d'un module libre et du quotient d'un module libre par ses invariants (voir 3.4). Pour mieux appréhender les notions d'unités cyclotomiques, on peut regarder l'exemple suivant, le plus simple connu. Soit p un nombre premier fixé, on note $q = p$ si $p \neq 2$ et $q = 4$ sinon. on notera ζ_n la racine de l'unité:

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

Soit $M_n = \mathbb{Q}(\zeta_{qp^n} + \zeta_{qp^n}^{-1})$ et $\Gamma_n = \mathrm{Gal}(M_n/\mathbb{Q})$ et soit $\gamma_n \in \mathbb{Z}$ une racine primitive modulo qp^n. Soit ξ_n l'unité réelle suivante :

$$\xi_n = \sqrt{\frac{(1-\zeta_{qp^n}^{\gamma_n})(1-\zeta_{qp^n}^{-\gamma_n})}{(1-\zeta_{qp^n})(1-\zeta_{qp^n}^{-1})}} = \sqrt{\zeta_{qp^n}^{(1-\gamma_n)}}\,\frac{(1-\zeta_{qp^n}^{\gamma_n})}{(1-\zeta_{qp^n})}$$

Il est bien connu que le module galoisien engendré par ξ_n est isomorphe à l'idéal d'augmentation, et que l'indice de $\{\pm 1\} \times \xi_n^{\mathbb{Z}[\Gamma_n]}$ est égal au nombre de classe de M_n (voir [16]). Ce module s'appelle le module des unités cyclotomiques de M_n.

On trouve dans la littérature de nombreuses propositions pour un module qui généraliserait $\{\pm 1\} \times \xi_n^{\mathbb{Z}[\Gamma_n]}$ à un corps abélien K. Actuellement le consensus semble être fait sur le module des unités circulaires $C_S(K)$ défini dans [13]. Sinnott donne des générateurs explicites et calcule l'indice de ces unités, mais n'étudie pas leur structure galoisienne. Lorsque K n'est plus un sous-corps de M_n et que son degré sur $\mathbb{Q}$ n'est pas premier, on ne peut espérer que ce module galoisien soit isomorphe à l'idéal d'augmentation. En général, il n'est pas non plus monogène. On ne savait pratiquement rien sur sa structure galoisienne lorsque le conducteur de K est divisible par plus de deux nombres premiers.

Soit K un corps de nombres abélien réel, soit $K_\infty = \cup K_n$ la $\mathbb{Z}_p$-extension cyclotomique de $K = K_0$. On suppose que p ne se ramifie pas dans K. Pour $m \geq n \geq 0$, on note G_n^m le groupe $\mathrm{Gal}(K_m/K_n)$ et N_n^m la norme de K_m à K_n. La question précise étudiée ici a été motivée par l'article [8], où Greither étudie d'un point de vue général les "normes universelles dans une $\mathbb{Z}_p$-extension" d'un foncteur en $\mathbb{Z}_p$-modules partant de la catégorie des corps de nombres. Sous des hypothèses assez peu contraignantes, il montre que le module de ces normes universelles est libre par rapport à l'action des groupes de Galois relatifs de cette $\mathbb{Z}_p$-extension. Ces résultats laissent espérer une G_0^n-structure locale assez simple pour les modules $\cap_{m\geq n} N_n^m(C_S(K_m))$. Notamment, sous la conjecture de Greenberg les résultats de [8] montrent que le module $\ker N_0^n \cap (\cap_{m\geq n\geq 0} N_n^m(C_S(K_m) \otimes \mathbb{Z}_p))$ est libre sur l'anneau $\mathbb{Z}_p[G_0^n]/N_0^n$.

L'approche utilisée ici se différencie de celle de [8] par son côté effectif et élémentaire. Cela permet d'obtenir des résultats globaux mais impose une certaine perte en généralité. Dans le premier chapitre on définit un sous-module global $D_n(K)$ des p-unités de K_n ne contenant que des normes universelles et dont l'intersection avec les unités de K_n contient "l'essentiel" des normes universelles de $C_S(K_n)$ (voir proposition 1.6). Le résultat principal de cet article (théorème 3.4) est la description effective de la G_0^n-structure locale (éventuellement globale) de $D_n\,(K)$. Ce résultat est démontré sous des hypothèses fréquemment vérifiées par K ou p. Par exemple l'hypothèse locale est satisfaite lorsque p est impair et K est le sous-corps réel maximal d'un corps cyclotomique. Dans le chapitre II, on construit une présentation galoisienne de $D_n(K)$ (théorème 2.6). Cette présentation s'obtient à l'aide de relations de normes à la Bass, et constitue l'ingrédient principal de la preuve de 3.4. La littérature contient de nombreuses présentations similaires pour les unités cyclotomiques. Par exemple dans l'article [1] (avec une légère erreur corrigée dans [4]), Bass donne une présentation multiplicative des unités cyclotomiques. Puis Solomon a construit dans [15] une présentation galoisienne s'appliquant à de nombreux sous-modules d'indices finis de $C_S(K)$ (dont $C_S(K)$ lui-même pour $K/\mathbb{Q}$ cyclique). Mais celles-ci ne s'appliquent pas à $D_n(K)$ et ne semblent pas se simplifier aussi fréquemment que celle du théorème 2.6. Les preuves de 3.4 et 2.6 sont complètement explicites et peuvent par exemple conduire à un algorithme de recherche d'une $\mathbb{Z}[G_0^n]$-base de $D_n(K)$ lorsque ce dernier est libre. En application, lorsque la deuxième conclusion de 3.4 a lieu, on calcule la G_n^m-cohomologie de $C_S(K_m)$ (pour $m > n \geq 0$) et on vérifie l'égalité : $C_S(K_m) \cap K_n = C_S(K_n)$ (la "descente galoisienne" pour $C_S(K_n)$ entre deux étages de la $\mathbb{Z}_p$-tour). Cela complète les résultats de [6] et [9] qui concernaient les corps $K = \mathbb{Q}(\zeta_{pd})$ avec $p \neq 2$, $p \nmid d$ et $pd \not\equiv 2[4]$. Dans le dernier chapitre on donne des conditions suffisantes aux hypothèses de 3.4 et on donne deux exemples de corps K pour lesquels on construit une unité de $C_S(K_1) \cap K$ qui n'appartient pas à $C_S(K)$, avec $p = 2$ ou 3. Pour construire ces exemples on reprend des idées de [7] où la descente galoisienne pour les unités circulaires avait été démentie en général. Mais dans les corps étudiés dans [7], la ramification éventuelle était modérée, tandis que dans les exemples présentés ici l'absence de descente a lieu entre deux étages d'une $\mathbb{Z}_p$-extension cyclotomique. En constatant l'existence d'un tel défaut, il est naturel de se demander s'il reste borné dans la $\mathbb{Z}_p$-extension. Une réponse affirmative suit des résultats de [11] qui bornent l'indice des unités circulaires dans celles de Washington, et ces dernières vérifient la descente galoisienne (voir [6]).

I Définitions, premières propriétés

Dans ce chapitre on définit le module $D_n(K)$, et on établit certaines des propriétés utiles de ce module. Plus précisément, on calcule son caractère (proposition 1.4) et on le compare avec le module des unités circulaires de Sinnott (proposition 1.6 et lemme 1.3).

I.1 conventions et notations.

A chaque $n \in \mathbb{N}$, $n \neq 0$, on associe le corps $\mathbb{B}_n$ qui est le sous corps de $\mathbb{Q}(\zeta_{qp^n})$, fixé par le sous-groupe d'ordre $p-1$ de $\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q})$ si $p \neq 2$ (resp. par la conjugaison complexe sinon).

Si K est un corps abélien, on notera K_n le composé de K avec $\mathbb{B}_n$, G_K le groupe $\mathrm{Gal}(K/\mathbb{Q})$, $\mathrm{cond}(K)$ le conducteur de K qui est un entier positif non congru à 2 modulo 4, $E(K)$ le groupe des unités de K, $C_S(K)$ le groupe des unités circulaires défini dans [13], et, si l est un nombre premier qui ne se ramifie pas dans K, $\left(\frac{K}{l}\right)$ désignera le Frobenius de l.

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 1.1. *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 $D_n(K)$ et engendré comme $\mathbb{Z}[G_{K_n}]$-module par les entiers algébriques :*

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

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

Remarque 1.2. *Ces entiers sont des p-unités si $n \neq 0$,*
égaux à p ou à une $\mathrm{cond}(K)$*-unités si $n = 0$.*

I.2 propriétés élémentaires.

Dans toute la suite K est un corps abélien réel, et p un nombre premier rationnel fixé qui ne se ramifie pas dans K.

Lemme 1.3. *Soit n un entier positif ou nul, on a :*

(1) *Tout élément de $D_n(K)$ est totalement positif.*
(2) $C_S(K) = \{\pm 1\} \times (D_0(K) \cap E(K))$
(3) *Si $n \neq 0$ alors $C_S(K_n) = C_S(K)\ (D_n(K) \cap E(K_n))$.*
(4) *Si $n \neq 0$ alors $N_K^{K_n}(D_n(K)) = p^{\mathbb{Z}} \times (D_0(K))^{1-\left(\frac{K}{p}\right)}$*
(5) $D_n(K) \cap E(K_n) = \ker N_{\mathbb{Q}}^{K_n} \cap D_n(K)$

Démonstration :

(1)

Comme K_n est totalement réel et que chaque générateur de $D_n(K)$ est une norme depuis un corps totalement imaginaire vers un sous-corps de K_n, (1) est vrai pour un système générateur de $D_n(K)$ donc pour chaque élément de $D_n(K)$.

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 $C_S(K)$ est une unité qui peut s'écrire:

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

où $m,\ a,\ x(m,a)$ sont des entiers, et où les $x(m,a)$ sont presque tous nuls. Ici on a besoin d'utiliser les formules bien connues (voir par exemple [14]):

$$(*) \qquad N^{\mathbb{Q}(\zeta_m)}_{\mathbb{Q}(\zeta_r)}(1-\zeta_m) = (1-\zeta_r)^{\prod_l \left(1-\left(\frac{\mathbb{Q}(\zeta_r)}{l}\right)^{-1}\right)}$$

si $r \mid m$, $r \neq 1$ et en faisant parcourir à l les premiers divisant m et ne divisant pas r

et

$$(**) \qquad N^{\mathbb{Q}(\zeta_{l^m})}_{\mathbb{Q}}(1-\zeta_{l^m}) = l \text{ si } l \text{ est premier, } m \geq 1$$

Ces identités 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 :

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

On constate donc que (i) se réécrit:

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

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 1.2):

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

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

$$\pm\epsilon = \prod_{m \mid \operatorname{cond}(K)} N^{\mathbb{Q}(\zeta_m)}_{\mathbb{Q}(\zeta_m)\cap K}(1-\zeta_m)^{x_m} \in D_0\,(K) \cap E(K)$$

On peut aussi remarquer que le générateur p n'intervient pas ici.

(3)

En tenant compte de la remarque 2.2, les arguments précédents s'appliquent mutatis mutandis à l'inclusion réciproque de (3).

(4) se voit rapidement sur un système de générateurs des deux $\mathbb{Z}[G_K]$-modules en utilisant $(*)$ et $(**)$.

(5)

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

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

qui est vraie pour tout ϵ de $D_n\,(K)$ et toute valuation non archimédienne de v de K_n. En effet si m est un entier naturel divisible par au moins deux premier 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 $g \in G_{K_n}$, $N^{\mathbb{Q}(\zeta_m)}_{\mathbb{Q}(\zeta_m)\cap K}(1-\zeta_m)^g$ vérifie notre identité. $\square$

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

Proposition 1.4.

(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:*

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

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

$$\chi_{N_K^{K_n}(D_n(K))}^{G_{K_n}} = \chi_{\mathbb{Z}[G_K]}^{G_{K_n}} - \chi_{\mathbb{Z}[G_{K\mathrm{dec}}]}^{G_{K_n}} + \chi_{\mathbb{Z}}^{G_{K_n}}$$

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

$$\chi_{D_0(K)}^{G_K} = \chi_{\mathbb{Z}[G_K]}^{G_K} + \#\mathcal{P}(K)\chi_{\mathbb{Z}}^{G_K}$$

Corollaire 1.5. *Soient $f = [K : K_{\mathrm{dec}}]$ et $g = [K_{\mathrm{dec}} : \mathbb{Q}]$. Si $n \neq 0$ on a:*

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

$$\dim_{\mathbb{Q}}(N_K^{K_n}(D_n\,(K)) \otimes_{\mathbb{Z}} \mathbb{Q}) = \chi_{N_K^{K_n}(D_n(K))}^{G_{K_n}}(1) = gf - g + 1$$

En outre on a:

$$\dim_{\mathbb{Q}}(D_0\,(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = gf + \#\mathcal{P}(K)$$

Démonstration de 1.4 (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 1.4 (1) est une conséquence de l'exactitude des suites suivantes:

$$1 \longrightarrow \Big(\ker N_K^{K_n} \cap E(K_n)\Big) \otimes \mathbb{Q} \longrightarrow D_n\,(K) \otimes \mathbb{Q} \xrightarrow{N_K^{K_n}} \Big(p^{\mathbb{Z}} \times (\ker N_{K_{\mathrm{dec}}}^{K} \cap E(K))\Big) \otimes \mathbb{Q} \longrightarrow 1$$

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

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

L'exactitude des deux dernières suites est immédiate. Pour la première on utilise l'identité bien connue (voir [13]):

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

On en déduit :

$$\begin{aligned}
\Big(\ker N_K^{K_n} \cap E(K_n)\Big) \otimes \mathbb{Q} &= \Big(\ker N_K^{K_n} \cap C_S(K_n)\Big) \otimes \mathbb{Q} \quad \text{d'après } (***) \\
&= \Big(\ker N_K^{K_n} \cap (C_S(K)(D_n\,(K) \cap E(K_n)))\Big) \otimes \mathbb{Q} \quad \text{d'après 1.3 (3)} \\
&= \Big(\ker N_K^{K_n} \cap E(K_n) \cap D_n\,(K)\Big) \otimes \mathbb{Q} \\
&\quad\ \text{car } \forall x \in C_S(K) \text{ on a } N_K^{K_n}(x) = x^{p^n} \\
&= \Big(\ker N_K^{K_n} \cap D_n\,(K)\Big) \otimes \mathbb{Q} \text{ d'après 1.3 (5)}
\end{aligned}$$

Ce qui donne l'exactitude à gauche de $D_n\,(K)$. D'autre part on a :

$$\begin{aligned} N_K^{K_n}(D_n\,(K))\otimes\mathbb{Q} &= \left(p^{\mathbb{Z}}\times(D_0\,(K))^{1-\left(\frac{K}{p}\right)}\right)\otimes\mathbb{Q} \text{ d'après 1.2 (4)}\\ &= \left(p^{\mathbb{Z}}\times(\ker N_{K_{\mathrm{dec}}}^{K}\cap D_0\,(K))\right)\otimes\mathbb{Q} \text{ car } H^1(\langle\left(\frac{K}{p}\right)\rangle, D_0\,(K)) \text{ est fini}\\ &= (p^{\mathbb{Z}}\times(\ker N_{K_{\mathrm{dec}}}^{K}\cap C_S(K)))\otimes\mathbb{Q} \text{ d'après 1.3 (2) et (5)}\\ &= (p^{\mathbb{Z}}\times(\ker N_{K_{\mathrm{dec}}}^{K}\cap E(K)))\otimes\mathbb{Q} \text{ d'après } (***) \end{aligned}$$

Ce qui donne l'exactitude à droite de $D_n\,(K)$ et conclut cette preuve. □

Démonstration de 1.4 (2) : C'est une conséquence évidente de (1) □

Démonstration de 1.4 (3) : 1.3 (5), $(**)$ et $(***)$ donnent la suite:

$$1 \longrightarrow E(K)\otimes\mathbb{Q} \longrightarrow D_0\,(K)\otimes\mathbb{Q} \xrightarrow{N_{\mathbb{Q}}^{K}} \left(p^{\mathbb{Z}}\times\prod_{l\in\mathcal{P}(K)} l^{\mathbb{Z}}\right)\otimes\mathbb{Q} \longrightarrow 1$$

ce qui avec (ii) démontre 1.4 (3). □

Proposition 1.6. *Les identités* $(*)$ *et* $(**)$ *donnent, pour chaque couple d'entiers strictement positifs* m *et* n *les inclusions :*

$$N_{K_n}^{K_{m+n}}(D_{m+n}\,(K)\cap E(K_{m+n}))\subset D_n\,(K)\cap E(K_n)$$

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

$(D_n\,(K)\cap E(K_n))\otimes\mathbb{Z}_p$ *(resp.* $C_S(K_n)\otimes\mathbb{Z}_p$*) par* $\varprojlim\,((D_n\,(K)\cap E(K_n))\otimes\mathbb{Z}_p)$ *(resp.* $\varprojlim\,(C_S(K_n)\otimes\mathbb{Z}_p)$*) On a :*

$$\varprojlim\,((D_n\,(K)\cap E(K_n))\otimes\mathbb{Z}_p)=\varprojlim\,(C_S(K_n)\otimes\mathbb{Z}_p)$$

Démonstration : Le lemme 1.3 (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 [3] 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 $\epsilon_n\in C_S(K_n)\otimes\mathbb{Z}_p$, alors le lemme 1.3 (3) donne l'existence pour tout $n\in\mathbb{N}$ d'un $x_n\in C_S(K)\otimes\mathbb{Z}_p$ et d'un $x'_n\in(D_n\,(K)\cap E(K_n))\otimes\mathbb{Z}_p$ vérifiant : $\epsilon_n=x_nx'_n$. Ici la théorie du corps de classe locale donne pour tout n : $N_{K_{\mathrm{dec}}}^{K_n}(\epsilon_n)=1\otimes1$. Il suit :

$$1\otimes1=N_{K_{\mathrm{dec}}}^{K_n}(\epsilon_n)=N_{K_{\mathrm{dec}}}^{K_n}(x_nx'_n)=N_{K_{\mathrm{dec}}}^{K}(x_n^{p^n}) \text{ d'après 1.3 (4)}$$

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 $N_{K_{\mathrm{dec}}}^{K}(x_n)\in\{\pm1\otimes1\}$. En outre $C_S(K)^{1-\left(\frac{K}{p}\right)}$ est d'indice fini dans $\ker N_{K_{\mathrm{dec}}}^{K}\cap C_S(K)$, donc le lemme 1.3 (2) assure l'existence d'un entier m, indépendant de n, tel que :

$$x_n^{p^m}\in D_0\,(K)^{1-\left(\frac{K}{p}\right)}\otimes\mathbb{Z}_p$$

Pour un n dorénavant fixé on a ici :

$$\epsilon_n = N_{K_n}^{K_{m+n}}(x_{m+n}x'_{m+n}) = x_{m+n}^{p^m} N_{K_n}^{K_{m+n}}(x'_{m+n}) \in (D_n\,(K) \cap E(K_n)) \otimes \mathbb{Z}_p$$

En effet l'inclusion $D_0\,(K)^{1-\left(\frac{K}{p}\right)} \subset D_n\,(K)$ a déjà été prouvée en 1.3 (4) tandis que $D_0\,(K)^{1-\left(\frac{K}{p}\right)} \subset E(K)$ est une conséquence de 1.3 (5). $\square$

II Une présentation galoisienne de $D_n\,(K)$

II.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 Gal$(\mathbb{B}_m/\mathbb{B}_n)$. 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 $\mathbb{C}$-irréductibles, 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 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 2.1 (et notation). *A un couple (J, n) où $J \subset \mathcal{P}$ et $n \in \mathbb{N}$, on associe les objets :*

(1) $$d_J = \prod_{l\in J} l^{e_l};\quad \xi_n\,(J) = \zeta_{qp^n d_J}\ \text{si } n \neq 0;\quad \xi_0\,(J) = \zeta_{d_J}$$

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

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

Remarque 2.2. *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 :

$$K_n\,(J) \cap K_n\,(I) = K_n\,(I \cap J) \quad \text{et} \quad K_{\text{dec}}(J) \cap K_{\text{dec}}(I) = K_{\text{dec}}(I \cap J)$$

Remarque 2.3. *On voit immédiatement que* $\epsilon_n(J) \in D_n(K(J)) + \mathbb{Q}^\times$. *On montrera plus tard que* $\{\epsilon_n(J)\,; I \subset J\}$ *est un système* $\mathbb{Z}[G_{K_n}]$*-générateur de* $D_n(K(J))$ *si* $n \neq 0$ *ou de*

$$D_0(K(J)) \oplus \bigoplus_{\substack{l \in J \\ l \nmid \mathrm{cond}(K(J))}} \mathbb{Z}\, l \text{ sinon}.$$

On utilisera dans la suite de cet article une relation d'ordre (non stricte) sur les sous-ensemble de $\mathcal{P}$, notée $\prec$ et vérifiant les propriétés suivantes :

(i) $\prec$ est totale (i.e. : $\forall I \subset \mathcal{P}\ \forall J \subset \mathcal{P}$ on a $I \prec J$ ou $J \prec I$).

(ii) $\prec$ prolonge l'inclusion (i.e. : $I \subset J \implies I \prec J$).

Remarque 2.4. *L'existence de telles relations d'ordre est facile à vérifier. Par exemple l'ordre induit par l'ordre archimédien sur les* d_I *ou encore l'ordre lexicographique sur les sous ensembles de* $\mathcal{P}$ *conviennent.*

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 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 par les éléments de F. On définit maintenant les objets nécessaires à l'énoncé du résultat principal de ce chapitre.

Définition 2.5. *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 :*

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

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

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

(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 :*

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

(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 :*

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

Le résultat principal de ce chapitre est :

Théorème 2.6. *Soit $J \subset \mathcal{P}$, soit $n \in \mathbb{N}$ et soit $\alpha_n(J) : \mathcal{L}_n(J) \longrightarrow D_n(K)$ défini 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 clairement bien défini, et on a :*

$D_n(K(J)) \subset \operatorname{Im} \alpha_n(J)$, $(\mathcal{H}_n(J) + \mathcal{V}_n(J)) \subset \ker \alpha_n(J)$, de plus il existe un entier non nul z_J tel que :

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

La démonstration occupe le reste de ce chapitre. On conclut cette section avec quelques conventions supplémentaires.

Définition 2.7. *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 de fraction $\operatorname{Fr}(A)$ et si M est un A-module on abrègera $\dim_{\operatorname{Fr}(A)} M \otimes \operatorname{Fr}(A)$ en $\operatorname{rang}_A M$*

A partir d'ici et jusqu'à la fin de la preuve de 2.6 on fixe un $n \in \mathbb{N}$.

II.2 préparation.

Lemme 2.8. *Soit $J \subset \mathcal{P}$*

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

(2) *$\{\epsilon_0(I) : I \subset J\}$ est un système générateur de :*

$$D_0(K(J)) \oplus \bigoplus_{\substack{l \in J \\ l \nmid \operatorname{cond}(K(J))}} \mathbb{Z}\, l$$

Démonstration : Pour $I \subset J$, on voit facilement que $\epsilon_n(I) \in D_n(K(J))$, dès que $K_n(I) \neq \mathbb{Q}$. On a aussi $l \in D_0(K(J))$ dès que $l \mid \operatorname{cond}(K(J))$. Cela donne une inclusion. On vérifie l'inclusion réciproque de (1). Soit $m \mid \operatorname{cond}(K(J))$, 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 $\mathbb{Q}(\zeta_{qp^n m}) \subset \mathbb{Q}(\xi_n(I))$. Ici $(*)$ et $(**)$ donnent :

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

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

Lemme 2.9. *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 $N^{K_n}_{K_n(I)}(\epsilon_n(J)) \in \langle\{\epsilon_n(I \cap J)\}\rangle$. Si de plus $I \subset J$, alors on a $N^{K_n(J)}_{K_n(I)}(\epsilon_n(J)) \in \langle\{\epsilon_n(I)\}\rangle$.*
(3) *Si $I \cap J = \emptyset$ alors $N^{K}_{K(I)}(\epsilon_0(J)) \in \langle J\rangle$.*

Démonstration : C'est une conséquence immédiate des formules $(*)$ et $(**)$, de la transitivité de la norme, et de la remarque 2.2. $\square$

Lemme 2.10. *Soient I et J deux sous-ensembles de $\mathcal{P}$, avec $I \subset J$, on a*
$\mathrm{rang}_{\mathbb{Z}}(X_n(I,J)) = \mathrm{rang}_{\mathbb{Z}}(X_n(I))$

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 $\mathrm{rang}_{\mathbb{Z}}(X_n(I,J)) \geq \mathrm{rang}_{\mathbb{Z}}(X_n(I))$ est évidente. Réciproquement, on a :

$$\begin{aligned}
&(\langle\{\epsilon_n(I') : I' \subset \mathcal{P}, I' \prec I, I' \neq I\}\rangle \cap \langle\{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \\
&= [K_n : K_n(I)](\langle\{\epsilon_n(I') : I' \subset \mathcal{P}, I' \prec I, I' \neq I\}\rangle \cap \langle\{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \\
&= N^{K_n}_{K_n(I)}(\langle\{\epsilon_n(I') : I' \subset \mathcal{P}, I' \prec I, I' \neq I\}\rangle \cap \langle\{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \\
&\subset (\langle\{\epsilon_n(I') : I' \subset I, I' \neq I\}\rangle \cap \langle\{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \text{ d'après le lemme 2.9 (2)} \\
&\subset (\langle\{\epsilon_n(I') : I' \subset J, I' \prec I, I' \neq I\}\rangle \cap \langle\{\epsilon_n(I)\}\rangle) \otimes \mathbb{C} \text{ car } I \subset J \text{ et } \prec \text{ prolonge } \subset .
\end{aligned}$$

$\square$

II.3 Les idéaux normiques.

Proposition 2.11. *Soit $J \subset \mathcal{P}$ tel que $J \neq \emptyset$. On a :*
(1) $\mathrm{rang}_{\mathbb{Z}} N(J) = \sum_{\substack{I \subset J \\ I \neq J}} (-1)^{\#J - \#I + 1} g_I f_I$
(2) *Si $n \neq 0$ alors :*

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

Démonstration de (1) : On a :

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

En utilisant la remarque 2.2 et le principe d'inclusion-exclusion. En posant $I = J - L$ on en déduit :

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

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 :

$$\begin{aligned}& \operatorname{rang}\left((N(J) \otimes \mathbb{Z}[G_0^n]) \cap \langle\{v_n(J)\}\rangle\right) \\ = {} & \operatorname{rang}\left(\langle\{N_{K_{\mathrm{dec}}(J)}^{K(J)} N_l^J \otimes N_0^n : l \in J\}\rangle\right) \text{ car } (v_n(J))^2 = p^n [K(J) : K_{\mathrm{dec}}(J)] v_n(J) \\ = {} & \#\{\chi \in \widehat{G}(J) : \exists l \in J \text{ avec } \operatorname{Gal}(K(J)/K_{\mathrm{dec}}(J - \{l\})) \subset \ker \chi\} \\ = {} & \# \bigcup_{l \in J} \widehat{G}_{K_{\mathrm{dec}}(J - \{l\})} \\ = {} & \sum_{\substack{I \subset J \\ I \neq J}} (-1)^{\#J - \#I + 1} g_I \text{ en utilisant à nouveau le principe d'inclusion-exclusion et 2.2}\end{aligned}$$

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

II.4 Suites exactes récursives.

Proposition 2.12. *Soit $J \subset \mathcal{P}$, si $n \neq 0$ alors on a :*

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

$$\operatorname{rang}(X_n(J)) = \begin{cases} p^n \ \textit{si } J = \emptyset \\ \sum_{I \subset J} (-1)^{\#J - \#I} f_n(I) \ \textit{sinon} \end{cases} \tag{2}$$

Proposition 2.13. *Soit $J \subset \mathcal{P}$, on a :*

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

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

(3) *pour* $\#J\langle 2$: $\mathrm{rang}(p^{\mathbb{Z}}) = 1$ *et* $\mathrm{rang}(X_0\,(J)) = g_J f_J = 1 + \sum_{I\subset J} (-1)^{\#J-\#I} g_I f_I$

Démonstration de 2.12 : Le lemme 2.8 donne un isomorphisme :

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

et avec le lemme 2.10 et le corollaire 1.5 qui se traduit ici par : $\mathrm{rang}\, D_n\,(K(J)) = 1 + f_n(J)$, 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 $D_n\,(K(J_0))$ hormis $\epsilon_n\,(\emptyset)$) la suite exacte $S_n(I)$ suivante :

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

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):

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

Donc le lemme 2.10 nous donne les identités:

$$\mathrm{rang}\,(\langle\{\epsilon_n\,(L) : L\subset J_0,\ L\prec I\}\rangle) = \mathrm{rang}\,(\langle\{\epsilon_n\,(L) : L\subset J_0,\ L\prec I,\ L\neq I\}\rangle) + \mathrm{rang}\,(X_n\,(I))$$

En regroupant toutes ces égalités on obtient:

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

La dernière égalité s'obtient avec le lemme 2.14 ci-dessous, et prouve (1) pour $J = J_0$. $\square$

Lemme 2.14. *Soit $s \in \mathbb{N}$ et soit $\mathbb{R}^{\mathbb{P}(\{1,\dots,s\})}$, l'ensemble des applications de $\mathbb{P}(\{1,...,s\})$ 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 2.14 : c'est évident.

Démonstration de 2.13 : (3) est immédiat. Pour (1) et (2), avec les modifications mineures expliquées ci-dessous la preuve est semblable à celle de 2.12 en faisant jouer le rôle de $f_n(I)$ à $g_I f_I$. Ici il faut néanmoins commencer la récurrence à partir de $\#J_0 \geq 2$, et remarquer que :

• $S_0(J_0)$ se lit :

$$1 \longrightarrow \langle\{\epsilon_0\,(I) : I \subset J_0, I \neq J_0\}\rangle \longrightarrow D_0\,(K(J_0)) \oplus \bigoplus_{\substack{l\in J_0\\ l\nmid \mathrm{cond}(K(J_0))}} \mathbb{Z}\,l \longrightarrow X_0\,(J_0, J_0) \longrightarrow 1$$

• Le rang du terme du milieu vaut $g_{J_0} f_{J_0} + \#J_0$.

• La quantité $\#J_0$ est compensée par le terme $\sum_{l\in J_0} 1$, qui apparaît lorsqu'on somme les rangs des $X_0\,(\{l\})$ pour $l \in J_0$.

□

II.5 Preuve du théorème 2.6.

Les deux inclusions sont des conséquences des lemmes 2.8 et 2.9. Il ne reste plus qu'à trouver des z_J convenables. On utilise $\prec$ pour faire une récurrence sur les sous-ensembles de $\mathcal{P}$. Si $J = \emptyset$ alors 2.6 suit directement de $\mathcal{H}_n\,(\emptyset) = \mathcal{V}_n\,(\emptyset) = \{0\}$ qui se traduit par :

$$\frac{\mathcal{L}_n\,(\emptyset)}{\mathcal{H}_n\,(\emptyset) + \mathcal{V}_n\,(\emptyset)} = \mathbb{Z}[G_0^n]w_n\,(\emptyset) \simeq \langle\{\epsilon_n\,(\emptyset)\}\rangle_{K_n^\times}$$

Soit $I \subset \mathcal{P}$, avec $I \neq \emptyset$. On suppose que 2.6 est vrai pour $J = I'$, le précédent immédiat de I. On note M (resp. $\beta_n\,(I)$) le module (resp. l'homomorphisme) suivant :

$$M = \begin{cases} \mathbb{Z}[G(I)] \text{ si } n = 0 \ \text{ et } \ \#I = 1 \\ \dfrac{\mathbb{Z}[G\,(I)] \otimes \mathbb{Z}[G_0^n]}{N(I) \otimes \mathbb{Z}[G_0^n] + \langle\{v_n\,(I)\}\rangle} \text{ sinon} \end{cases} \qquad \text{resp.} \qquad \begin{aligned} \beta_n\,(I)\ :\ M &\longrightarrow X_n\,(I) \\ x &\longmapsto x\epsilon_n\,(I) \end{aligned}$$

$\beta_n\,(I)$ est bien défini d'après 2.10 (2) et parce que $v_n\,(I)\,\epsilon_n\,(I) = 0$ en vertu de $(*)$ et $(**)$. De plus $\beta_n\,(I)$ est clairement surjectif. En comparant les rang calculés en 2.11, 2.12 et 2.13, on constate que le noyau de $\beta_n\,(I)$ est fini. 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 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. Comme $\ker \beta_n(I)$ est aussi fini il en est de même pour le second, ce qui montre 2.6 pour $J = I$. $\square$

III $\mathbb{Z}[G_0^n]$-STRUCTURE DE $D_n(K)$

Dans ce chapitre on conserve les notations et conventions du chapitre II, 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 : $$\forall J \subset \mathcal{P} \ : \ \frac{\mathbb{Z}[G(J)]}{N(J)} \text{ est sans } \mathbb{Z}\text{-torsion}$$

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

Remarque 3.1. *L'hypothèse A (resp. l'hypothèse B) entraîne trivialement 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 3.2. *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 3.3.
$$\frac{\mathbb{Z}[G(\mathcal{P})]}{N(\mathcal{P})} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

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 3.4.
(1) Si (K, p) *vérifie H.B., on a :*

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

(2) Si de plus K *vérifie H.A. on a :*

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

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 D_n signifiera $D_n(K)$. 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 3.1. On vérifie (en comparant les rangs) que cette application est injective en section 3.2, et la conclusion suivra en section 3.3.

III.1 retour sur $\frac{\mathcal{L}_n}{\mathcal{H}_n}$.

Proposition 3.5. *Pour tout $J \subset \mathcal{P}$ il existe une surjection de $\mathcal{R}[G_0^n]$-modules :*

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

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 3.5 pour $J = I'$. On considère le diagramme suivant :

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

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 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 3.5 pour $J = I$. $\square$

Proposition 3.6. *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 3.6 est une simple conséquence de la proposition 3.7 qui fait l'objet de la section suivante. $\square$

III.2 Un autre calcul de rang.

Proposition 3.7. *On a :*

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

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

Démonstration : On calcule indépendamment les rangs de $\mathcal{H}_n \otimes \mathcal{R}$ et de $\bigoplus_{I \subset \mathcal{P}} N(I) \otimes \mathcal{R}[G_0^n]$ dans les lemmes qui suivent. □

Lemme 3.8.

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

Démonstration : On a :

$$\begin{aligned}
\mathrm{rang}_{\mathcal{R}}\Big(\bigoplus_{I \subset \mathcal{P}} N(I) \otimes \mathcal{R}[G_0^n]\Big) &= \sum_{I \subset \mathcal{P}} \sum_{\substack{J \subset I \\ J \neq I}} (-1)^{\#I - \#J + 1} g_J f_J p^n \text{ d'après 2.11 (1)} \\
&= -\sum_{\substack{I \subset \mathcal{P} \\ I \neq \mathcal{P}}} \sum_{J \subset I} (-1)^{\#I - \#J} g_J f_J p^n + \sum_{\substack{I \subset \mathcal{P} \\ I \neq \mathcal{P}}} g_I f_I p^n - \sum_{\substack{J \subset \mathcal{P} \\ J \neq \mathcal{P}}} (-1)^{\#\mathcal{P} - \#J} g_J f_J p^n \\
&= \sum_{\substack{I \subset \mathcal{P} \\ I \neq \mathcal{P}}} g_I f_I p^n \text{ d'après 2.14} \\
&= \mathrm{rang}_{\mathcal{R}}(\mathcal{L}_n \otimes \mathcal{R}) - g_{\mathcal{P}} f_{\mathcal{P}} p^n \text{ comme annoncé}
\end{aligned}$$

□

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

Lemme 3.9.

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

Démonstration : La première identité est facile, pour 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 :

$$\begin{aligned}\mathrm{rang}(N_0^n\mathcal{H}_n) = \mathrm{rang}(p^n\mathcal{H}_0) + \#\mathcal{P} &= \mathrm{rang}(\mathcal{L}_0) - \mathrm{rang}\,\mathcal{D}_0 + \#\mathcal{P} \\ &= \mathrm{rang}(\mathcal{L}_0) - g_\mathcal{P} f_\mathcal{P} - \#\mathcal{P} + \#\mathcal{P} \text{ d'après le corollaire 1.5} \\ &= \sum_{\substack{I\subset\mathcal{P}\\ I\neq\mathcal{P}}} g_I f_I \text{ comme annoncé}\end{aligned}$$

□

Lemme 3.10.

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

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

$$\begin{aligned}\mathrm{rang}(\mathcal{H}_n) &= \mathrm{rang}(\mathcal{H}_n + \mathcal{V}_n) - \mathrm{rang}(\mathcal{V}_n) + \mathrm{rang}(\mathcal{H}_n \cap \mathcal{V}_n) \\ &= \mathrm{rang}(\mathcal{L}_n) - \mathrm{rang}(D_n) - \mathrm{rang}(\mathcal{V}_n) + \mathrm{rang}(\mathcal{H}_n \cap \mathcal{V}_n) \text{ d'après le théorème 2.6} \\ &= \mathrm{rang}(\mathcal{L}_n) - \mathrm{rang}(D_n) - \mathrm{rang}(N_0^n\mathcal{V}_n) + \mathrm{rang}(N_0^n\mathcal{H}_n \cap N_0^n\mathcal{V}_n) \\ &\text{car } N_0^n \text{ agit comme } p^n \text{ sur } \mathcal{V}_n \\ &= \mathrm{rang}(\mathcal{L}_n) - \mathrm{rang}(D_n) + \mathrm{rang}(N_0^n\mathcal{H}_n) - \mathrm{rang}(N_0^n\mathcal{H}_n + N_0^n\mathcal{V}_n)\end{aligned}$$

En constatant que rang $(N_0^n\mathcal{L}_n \cap \ker\alpha_n) = $ 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:

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

Pour conclure il suffit ici d'utilser les identités suivantes : rang $(N_0^n\mathcal{L}_n) = \sum_{I\subset\mathcal{P}} g_I f_I$ (évident), rang $(N_0^n\mathcal{H}_n) = \sum_{I\subset\mathcal{P},\ I\neq\mathcal{P}} g_I f_I$ (lemme 3.9), rang $(D_n) = g_\mathcal{P} f_\mathcal{P} p^n - g_\mathcal{P} + 1$ (corollaire 1.5), et rang $(N_0^n(\alpha_n(\mathcal{L}_n))) = $ rang $(N_0^n D_n) = g_\mathcal{P} f_\mathcal{P} - g_\mathcal{P} + 1$ (corollaire 1.5). Cela nous donne :

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

Avec la liberté de $\frac{\mathcal{L}_n}{\mathcal{H}_n}$, l'essentiel de la preuve du théorème 3.4 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.

III.3 Preuve du théorème 3.4.

A partir d'ici κ_n : $\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R} \longrightarrow D_n \otimes \mathcal{R}$ désignera l'homomorphisme qui factorise $\alpha_n \otimes \mathbb{I}\mathrm{d}$.

Lemme 3.11. $\ker\kappa_n \subset \left(\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}\right)^{G_0^n} = N_0^n \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}$

Lemme 3.12. *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 3.4. Comme D_n est sans $\mathbb{Z}$-torsion (lemme 1.3 (1)), avec le lemme 3.11 on constate que :

$$\frac{N_0^n \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}}{\ker \kappa_n} \overset{\kappa_n}{\hookrightarrow} D_n \otimes \mathcal{R} \text{ et qu'on a donc la } \mathcal{R}\text{-liberté de } \frac{N_0^n \frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}}{\ker \kappa_n} \text{ et de } \ker \kappa_n$$

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 $\ker \kappa_n$. En appliquant le lemme 3.12 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 D_n et un module de la forme voulue. Il reste à calculer les entiers r et t du théorème 3.4. Or on a :

$$t = \mathrm{rang}_{\mathcal{R}}(\ker \kappa_n) = \mathrm{rang}_{\mathcal{R}} \left(\frac{\mathcal{V}_n}{\mathcal{V}_n \cap \mathcal{H}_n} \right) = g_{\mathcal{P}} - 1 \text{ d'après la preuve de 3.10}$$

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 r est bien égal à $g_{\mathcal{P}} f_{\mathcal{P}} - g_{\mathcal{P}} + 1$. $\square$

Démonstration de 3.11 : La dernière identité est un corollaire de la liberté de $\frac{\mathcal{L}_n}{\mathcal{H}_n} \otimes \mathcal{R}$. pour l'inclusion soit $x \in \ker \kappa_n$ alors d'après le théorème 2.6 il existe un entier z non nul tel qu'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 $x = gx$.

Démonstration de 3.12 : Soit $\{y_1, y_2, ..., y_s\}$ une $\mathcal{R}[G_0^n]$-base de M, alors $\{N_0^n y_1, N_0^n y_2, ..., N_0^n y_s\}$ 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 :

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

$\square$

III.4 Applications cohomologiques.

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 $C_S(K_m)$ (pour $m > n \geq 0$). On les notera $\widehat{H}^0(G_n^m, -)$ et $\widehat{H}^1(G_n^m, -)$. Une conséquence directe de 3.4 (1) est :

Corollaire 3.13. *Si (K,p) vérifie H.B, alors pour tout $m \geq n \geq 0$:*

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

On peut en déduire les deux propositions suivantes :

Proposition 3.14. *Si (K,p) vérifie H.B. alors on a pour tout $m \geq n \geq 0$:*

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

Proposition 3.15. $(D_0(K))^{\left(\frac{K}{p}\right)-1}$ *est contenu dans $C_S(K)$ d'après 1.3 (5). Soit F le sous-$\mathbb{Z}$-module de torsion de $\frac{C_S(K)}{(D_0(K))^{\left(\frac{K}{p}\right)-1}}$ 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 :*

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

Démonstration de 3.14 : Par la définition des deux modules, on a l'inclusion du module de droite dans le module de gauche. Réciproquement, soit $x \in C_S(K_m) \cap K_n$ alors d'après le lemme 1.3 (3) il existe $x_0 \in C_S(K)$ et $x' \in D_m(K) \cap E(K_m)$ tels que $x = x_0 x'$. Comme x et x_0 sont fixés par G_n^m, x' l'est aussi. Le corollaire 3.13 donne donc $x' \in N_n^m(D_m(K)) \subset D_n(K)$. On en déduit $x' \in D_n(K) \cap E(K_n)$ puis $x \in C_S(K_n)$ en utilisant à nouveau 1.3 (3) ou 1.3 (2). $\square$

Démonstration de 3.15 : On calcule d'abord la cohomologie de $D_m(K) \cap E(K_m)$ à l'aide de la suite suivante dont l'exactitude est donnée par le lemme 1.3 (5) et par les identités $N_{\mathbb{Q}}^{K_m}(\epsilon_m(I)) = 1$ si $I \neq \emptyset$ et $N_{\mathbb{Q}}^{K_m}(\epsilon_m(\emptyset)) = p^{f_{\mathcal{P}} g_{\mathcal{P}}}$:

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

En utilisant la suite longue de cohomologie qui ici se simplifie en un hexagone exact (voir [12] pour les groupes de cohomologie modifiés) et le corollaire 3.13, on obtient $\widehat{H}^0(G_n^m, D_m(K) \cap E(K_m)) = 0$ et la suite exacte courte de $\mathbb{Z}/p^{m-n}\mathbb{Z}$-modules :

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

qui se scinde en $\widehat{H}^1(G_n^m, D_m(K) \cap E(K_m)) \simeq (\mathbb{Z}/p^{m-n}\mathbb{Z})^{g_{\mathcal{P}}}$ puisque le dernier terme est libre. Cela étant, le corollaire 3.13 et le lemme 1.3 (4) donnent aussi :

$$C_S(K) \cap D_m(K) \subset (D_m(K))^{G_0^m} = N_0^m(D_m(K)) = (D_0(K))^{\left(\frac{K}{p}\right)-1} \oplus \mathbb{Z}\, p$$

On en déduit avec le lemme 1.3 (5) :

$$C_S(K) \cap D_m(K) \subset \left((D_0(K))^{\left(\frac{K}{p}\right)-1} \oplus \mathbb{Z}\, p\right) \cap E(K) \subset (D_0(K))^{\left(\frac{K}{p}\right)-1} \subset C_S(K) \cap D_m(K)$$

d'où l'égalité $C_S(K) \cap D_m(K) = (D_0(K))^{\left(\frac{K}{p}\right)-1}$ et avec le lemme 1.3 (3) l'exactitude de la suite :

$$0 \longrightarrow D_m(K) \cap E(K_m) \longrightarrow C_S(K_m) \longrightarrow \frac{C_S(K)}{(D_0(K))^{\left(\frac{K}{p}\right)-1}} \longrightarrow 0$$

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

$$\frac{C_S(K)}{(D_0\,(K))^{(\frac{K}{p})-1}} \simeq F \oplus \mathbb{Z}^{g_{\mathcal{P}}-1}, \text{ car } (D_0\,(K))^{(\frac{K}{p})-1} \text{ est d'indice fini dans } \ker N^K_{K_{\mathrm{dec}}} \cap C_S(K)$$

Et l'hexagone exact de cohomologie donne :

$$\begin{array}{ccccc} 0 & \longrightarrow & \widehat{H}^0(G_n^m, C_S(K_m)) & \longrightarrow & \dfrac{F}{p^{m-n}F} \oplus \left(\dfrac{\mathbb{Z}}{p^{m-n}}\right)^{g_{\mathcal{P}}-1} \\ \big\uparrow & & & & \big\downarrow \\ F_{p^{m-n}} & \longleftarrow & \widehat{H}^1(G_n^m, C_S(K_m)) & \xleftarrow{\ \phi\ } & \widehat{H}^1(G_n^m, D_m\,(K) \cap E(K_m)) \end{array}$$

Mais d'après 1.3 (3), pour tout générateur γ de G_n^m, on a $C_S(K_m)^{\gamma-1} = (C_S(K)(D_m\,(K) \cap E(K_m)))^{\gamma-1} = (D_m\,(K) \cap E(K_m))^{\gamma-1}$ de telle sorte que ϕ est injective et que ce diagramme donne

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

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

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

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

Corollaire 3.16. *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 :*

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

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

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).

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

Comme $p \neq 2$, $\mu(L_m)$ est cohomologiquement trivial. Cela donne les deux égalités. Et les deux isomorphismes sont ceux de la proposition 3.15. $\square$

IV Quelques exemples

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 du chapitre II. En deuxième section on détaillera l'exemple d'un couple (K, p) qui ne vérifie pas la conclusion locale (i.e. avec $\mathcal{R} = \mathbb{Z}_p$) de 3.4.

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

IV.1 les exemples positifs.

Proposition 4.1. *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 4.2. *Si G_K est cyclique, alors K vérifie H.A.*

Démonstration de 4.2 : 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 4.1 : 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 4.3. *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 des 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 4.4. *Si K est un corps de genre au sens de [5], 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 4.5. *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 4.3 : 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 4.1. 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.

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

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 4.4 : Voir la preuve de 4.2. $\square$

Démonstration de 4.5 : 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 4.3 donc H.B. $\square$

Proposition 4.6. *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 représentant 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 :

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

On utilise ici l'isomorphisme :

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

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 :

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

Comme d'autre part il est clair que :

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

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

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

$\square$

IV.2 Deux exemples négatifs.

Avec $p = 2$ et $K = \mathbb{Q}(\sqrt{5.17}, \sqrt{5.13})$ (voir remarque 3.2), on obtient avec les mêmes techniques que celles qui suivent un exemple de couple (K, p) pour lequel $\hat{H}^0(G_0^1, D_1(K)) \neq 0$. On choisit de présenter ici un exemple plus significatif, avec $p = 3$, mais un peu plus difficile à décrire explicitement. Pour les problèmes survenant en 2 on pourra se rapporter à [10] où une amélioration explicite en 2 de $C_S(K)$ 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 :

$$\begin{aligned}&X^9 - 3X^8 - 6335955X^7 + 2459856427X^6 + 9080370048953X^5 - 4520985235480441X^4\\&- 19249179101153624 84X^3 + 8431289428823771259 14X^2 +\\&16946067409725768149949X - 14705849276302066316183777\end{aligned}$$

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 $K_{\mathrm{dec}} = M_4$. 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 $3 = -N_7^{\mathcal{P}} N_{181}^{\mathcal{P}} + \sum_{l\in\mathcal{P}} N_l^{\mathcal{P}}$, $(*)$, $(**)$ 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 $D_1(K)$ est sans $\mathbb{Z}$-torsion, cette dernière identité donne $(1-\psi)u = 0$ c'est-à-dire $u \in D_1(K)^{G_0^1}$. Notre but dans cette section est de montrer :

Proposition 4.7. *$u \in D_1(K)^{G_0^1}$ et $u \notin N_0^1 D_1(K)$ de telle sorte que $\hat{H}^0(G_0^1, D_1(K)) \neq 0$ et que $D_1(K) \otimes \mathbb{Z}_p \not\simeq \left(\mathbb{Z}_p[G_0^1]\right)^{g_{\mathcal{P}} f_{\mathcal{P}} - g_{\mathcal{P}} + 1} \oplus \left(\frac{\mathbb{Z}_p[G_0^1]}{N_0^1}\right)^{g_{\mathcal{P}}+1}$*

Démonstration : Compte tenu de ce qui précède, il reste à voir que $u \notin N_0^1 D_1(K)$. En fait, on montre quelque chose d'un peu plus fort :

Lemme 4.8. $u \notin D_0\,(K)$.

Remarque 4.9. *Cela donne de plus que* $u \in C_S(K_1)^{G_0^1} - C_S(K)$, *et montre que l'hypothèse B n'est pas superflue, par exemple vis à vis de la proposition 3.14*

Démonstration de 4.8 : On utilise une $\mathbb{Z}$-base de $D_0\,(K)$. Dans ce cas celle-ci est facile à construire. En fait les relations $(*)$ et $(**)$ permettent de voir, comme $D_0\,(K)$ 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 $D_0\,(K)$ coïncide avec la somme directe interne :

$$D_0\,(K) = \mathbb{Z}\;3 \oplus \bigoplus_{l \in \mathcal{P}} \frac{\mathbb{Z}[G(J_l)]}{N_{\mathbb{Q}}^{K(J_l)}}\;\epsilon_0\,(J_l) \oplus \bigoplus_{l \in \mathcal{P}} \mathbb{Z}\;l.$$

Pour conclure que $u \notin D_0\,(K)$, il suffit de calculer les coefficients dans cette base de $3u = N_0^1 u$. Or comme $K_{\text{dec}} = K(J_{3037})$ on a $N_0^1 \epsilon_1\,(J_{3037}) = 1$, et comme $N_0^1 \epsilon_1\,(\mathcal{P}) = 1$, on en déduit :

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

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

Remerciements. Je tiens à exprimer ma reconnaissance envers C. Greither pour sa correspondance encourageante, X. F. Roblot pour sa précieuse connaissance du logiciel PARI et envers D. Solomon, qui m'a suggéré le problème et a eu la patience de lire la première version de ce travail.

Bibliographie.

[1] H. Bass, Generators and Relations for Cyclotomic Units, Nagoya Math. J. 27 (1966), 401-407

[2] 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)

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

[4] V. Ennola, On Relations between Cyclotomic Units, J. Number Theory 4 (1972), 236-247

[5] A. Fröhlich, Units in real Abelian Fields, J. Reine Angew. Math. 429 (1992), 191-217

[6] R. Gold, J. M. Kim, Bases for cyclotomic units, Compositio Math. 71 (1989), 13-28

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

[8] C. Greither, Sur les normes universelles dans les $\mathbb{Z}_p$-extensions, J. Théor. Nombres Bordeaux 6 (1994), 205-220

[9] J. M. Kim, Cohomology Groups of Cyclotomic Units, J. Algebra 152 (1992), 514-519

[10] R. Kučera, On the Stickelberger Ideal and Circular Units of a Compositum of Quadratic Fields, J. Number Theory 56 (1996), 139-166

[11] R. Kučera, J. Nekovář, Cyclotomic Units in $\mathbb{Z}_p$-Extensions, J. Algebra 171 (1995), 457-472

[12] J.-P. Serre, Corps locaux, Hermann (1968)

[13] W. Sinnott, On the Stickelberger Ideal and the Circular Units of an Abelian Field, Invent. Math. 62 (1981), 181-234

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

[15] D. Solomon, Galois Relations for Cyclotomic Numbers and p-units, J. Number Theory 46 (1994), 158-178,

[16] L. Washington, Introduction to Cyclotomic Fields, Springer verlag (1982)