UNIVERSITÉ DE LIMOGES
ÉCOLE DOCTORALE Science – Technologie – Santé
FACULTÉ des Sciences et Techniques

XLIM - **D**épartement de **M**athématiques et **I**nformétique

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Mathématiques

présentée et soutenue par

Mohsen ASGHARI-LARIMI

le 7 juillet 2006

Bornes Pour La Capitulation des groupes de K-théorie étale

Thèse dirigée par : Abbas MOVAHHEDI

Jury

Rapporteurs :	Jilali ASSIM
	Professeur à l'université de Meknès (Maroc)
	Manfred KOLSTER
	Professeur à McMaster University (Canada, Hamilton)
Examinateurs :	François LAUBIE
	Professeur à l'université de Limoges
	Abbas MOVAHHEDI
	Professeur à l'université de Limoges
	Alain SALINIER
	Maître de conférences HDR à l'université de Limoges

.

Remerciements

Je voudrais, en premier lieu, remercier mon directeur de thèse Abbas MOVAHHEDI, dont les idées et les conseils m'ont été extrêmement précieux.

Je remercie également Manfred KOLSTER d'avoir accepté d'être rapporteur de la thèse et qui me fait l'honneur de présider le jury.

Je tiens également à remercier Jilali ASSIM pour les discussions que nous avons pu avoir lors de la préparation de cette thèse et d'avoir rapporté sur ce travail.

Mes remerciements vont ensuite à François LAUBIE et Alain SALINIER qui me font l'amabilité de prendre part à ce jury.

Je remercie les membres du département DMI de XLIM et toutes les personnes qui m'ont aidé à la réalisation matérielle de ce travail ; en particulier, Sylvie LAVAL, Patricia VAREILLE et Yolande VIECELI. Mes remerciements vont également à Guilhem, Pierre-Louis, Mikaël, Ahmed pour leurs soutiens mathématiques et linguistiques.

Je voudrais également remercier Reza AMERI et Kouroush SEDIGHI de l'université de Mazandaran en Iran qui ont suivi mon avancement et qui sont à l'initiative de mon déplacement en France.

Enfin, un grand merci à ma famille, Nasrin, Afshin et Amin qui m'ont toujours aidé.

Table des matières

Introduction

Soit p un nombre premier impair et F un corps de nombres, contenant μ_p. Pour tout ensemble S de places de F contenant les places divisant p et les places archimédiennes de F, soit o_F^S l'anneau des S-entiers de F. Il est bien connu que les groupes de K-théorie étale de o_F^S reflétent les propriétés arithmétiques du corps F par rapport au nombre premier p (voir e.g. [Dw-Fr 85,So 79,Ta 76],...). Si E est une extension galoisienne de F, non-ramifiée en dehors de S, de groupe de Galois G, nous avons un homomorphisme canonique $f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow (K_{2i-2}^{\text{ét}}(o_E^S))^G$, dont le noyau et le conoyau sont :

$$0 \to H^1(G, K_{2i-1}^{\text{ét}}E) \to K_{2i-2}^{\text{ét}}(o_F^S) \to (K_{2i-2}^{\text{ét}}(o_E^S))^G \to H^2(G, K_{2i-1}^{\text{ét}}E) \to 0.$$

Utilisant les résultats de Borel sur la structure de groupe abélien des K-groupes impairs, il n'est pas difficile de donner une majoration de l'ordre de $\ker(f_i)$ et $\text{coker}(f_i)$ (voir [Ka 93-1, section 4]), faisant intervenir le nombre de plongements réels et complexes de F. À l'inverse, trouver une minoration de l'ordre de $\ker(f_i)$ et $\text{coker}(f_i)$ s'avère difficile.

Notons $\mu_{p^\infty} := \cup_{n\geq 1}\mu_{p^n}$ le groupe de toutes les racines de l'unité d'ordre une puissance de p et $F_\infty := F(\mu_{p^\infty})$ la $\mathbb{Z}_p$-extension cyclotomique de F avec $\Gamma = \text{Gal}(F_\infty/F)$. Soit $\mathcal{X}$ le module d'Iwasawa p-ramifié relatif à F_∞ qui est un Λ-module de rang r_2 et X le quotient sans-torsion, où r_2 est le nombre de places complexes de F. Notons comme d'habitude $H_F := \Lambda^{r_2}/X$ le module quotient qui est fini.

Supposons que l'extension E/F est cyclique de degré p de groupe de Galois G et soit p^e l'exposant de H_F. Supposons que F vérifie la conjecture de Leopoldt au nombre premier p, et que $\mu_{p^{e+1}} \subset F$. Alors, Jilali ASSIM et

Abbas MOVAHHEDI démontrent dans [As-Mo 04, Theorem 3.8] que pour tout $i \geq 2$,

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| \geq p^t,$$

où t est le nombre maximal de non-p-places contenues dans un ensemble primitif contenu dans l'ensemble des places de F ramifiées dans E ou divisant p.

Dans cette thèse nous allons généraliser ce théorème au cas où E/F est une extension cyclique de corps de nombres de degré p^n pour tout entier $n \geq 2$ contenant μ_{p^n}. Soit $\{v_1, v_2, ..., v_t\}$ un ensemble maximal de non-p-places contenues dans un ensemble primitif contenu dans $S = Ram(E/F) \cup S_p$, l'ensemble des places de F ramifiées dans E ou divisant p. Soit p^e l'exposant du groupe fini H_F. Prenons $i \geq 2$ et soit $r \leq n + e$ un entier tel que p^r divise i. Si $\mu_{p^{n+e-r}} \subset F$, alors

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| \geq p^{e_1+...+e_t},$$

où $p^{e_1}, p^{e_2}, ..., p^{e_t} \geq p$ sont les indices de ramification de $v_1, v_2, ..., v_t$ dans E/F (Théorème 4.2.5).

Pour finir, nous établissons pour chaque nombre entier non négatif $t \leq 1+r_2$, l'existence d'une infinité d'extensions cycliques E de F de degré p^n, où pour chaque puissance $p^m \leq p^{n(1+r_2)}$ de p, nous avons $|\ker(f_i)| = |\mathrm{coker}(f_i)| = p^m$.

Dans les trois premiers chapitres préliminaires, nous exposons les propriétés des $\mathbb{Z}_p$-extensions des corps de nombres, les K-groupes étales et leurs relations avec les modules d'Iwasawa standard.

Notations générales

$\mathbb{Z}$	l'anneau des entiers relatifs ;
p	un nombre premier ;
$\mathbb{Z}_p$	l'anneau des entiers p-adiques ;
$\mathbb{Q}$	le corps des nombres rationnels ;
$\mathbb{Q}_p$	le corps des nombres p-adiques ;
n	un entier naturel ;
μ_n	le groupe des racines n-ièmes de l'unité ;
μ_{p^∞}	le groupe de toutes les racines p^n-ièmes de l'unité,
	i.e., $\mu_{p^\infty} := \cup_{n\geq 1}\mu_{p^n}$;

F	un corps de nombres ;
F^*	le groupe multiplicatif des éléments du corps F privé de 0 ;
r_1 (resp.r_2)	le nombre de places réelles (resp. complexes) du corps F ;
F_∞	la $\mathbb{Z}_p$-extension cyclotomique de F ;
F_n	le n-ième étage de F_∞ ;
$\tilde{F}$	le composé des $\mathbb{Z}_p$-extensions de F ;
$\tilde{F}_n$	le composé des n-ièmes étages des $\mathbb{Z}_p$-extensions de F,
	pour tout $n \geq 1$;
S_p	l'ensemble des places divisant le nombre premier p ;
S	un ensemble de places de F contenant S_p et
	les places archimédiennes de F ;
$[E : F]$	le degré de l'extension finie E/F ;
$\mathrm{Gal}(E/F)$	le groupe de Galois de l'extension galoisienne E/F ;
$\mathrm{N}_{E/F}$	l'application norme de l'extension galoisienne E/F ;
$Ram(E/F)$	l'ensemble des places de F qui se ramifient dans l'extension E/F ;
o_F	l'anneau des entiers de F ;
o_F^S	l'anneau des S-entiers de F ;

G	un groupe fini ;
$\mid G \mid$	le cardinal (G) ;
${}_nG$	le noyau de la multiplication du groupe abélien G par n ;
M^G	l'ensemble des G-invariants d'un G-module M,
	i.e., $M^G = \{x \in M \mid \forall \sigma \in G, \sigma x = \sigma\}$;
$I_G M$	le sous-module de M engendré par les éléments de
	la forme $\sigma x - x$, où $x \in M$ et $\sigma \in G$;
M_G	l'ensemble des G-coinvariants de M, *i.e.*, $M_G = M/I_G M$;
[x ,y]	le commutateur $xyx^{-1}y^{-1}$ pour des éléments $x,\ y$ de G ;
[G ,G]	le groupe dérivé de G,
	i.e., le sous-groupe de G engendré par les commutateurs ;
$\mathrm{Div}(G)$	le sous-groupe divisible maximal de G ;

R	un anneau ;
R^*	le groupe des éléments inversibles de R ;
$spec(R)$	le spectre de l'anneau commutatif R ;
M	un R-module ;
$\mathrm{Tor}_R(M)$	le sous-module de M formé des éléments de R-torsion ;
$\mathrm{Fr}_R(M)$	$M/\mathrm{Tor}_R(M)$.

Chapitre 1

Groupes de K-théorie et K-groupes étales

Dans ce chapitre, nous donnons sans démonstration les principales définitions et propriétés de la construction des premiers groupes de K-théorie K_0, K_1 et K_2 d'un anneau unitaire et des groupes de K-théorie supérieurs introduits par Milnor et Quillen. Puis, nous donnons les principales définitions et propriétés des K-groupes supérieurs étales relatifs à un nombre premier p. Notre principale référence pour ce chapitre est [Ko 02] ainsi que [Mi 71] et [Ro 94].

1.1 Le groupe K_0

Soit R un anneau unitaire. Soit P un R-module à gauche, on note $[P]$ sa classe d'isomorphisme (c'est-à-dire l'ensemble des R-modules isomorphes à P). Le *groupe de Grothendieck* $K_0(R)$ est par définition le groupe abélien libre engendré par les classes d'isomorphismes $[P]$ des R-modules à gauche projectifs de type fini P, quotienté par le sous-groupe engendré par la relation

$$[P] + [Q] - [P \oplus Q].$$

Deux classes d'isomophismes $[P]$ et $[Q]$ sont égales dans $K_0(R)$ si et seulement si P et Q sont stablement isomorphes, c'est-à-dire, $P \oplus R^n \cong Q \oplus R^n$ pour un certain n.

Corollaire 1.1.1 **[Ro 94]** *Soit R un anneau local ou principal, alors*

$$K_0(R) \cong \mathbb{Z},$$

engendré par la classe du R-module libre de rang 1 (i.e., par [R]), C'est donc vrai, si R est un corps.

Un exemple important est le cas des anneaux de Dedekind, puisque $K_0(R)$ est, à un facteur de $\mathbb{Z}$ près, le groupe de classes de R :

Théorème 1.1.2 **[Mi 71]** *Soit R un anneau de Dedekind (par exemple les anneaux d'entiers d'un corps de nombres), alors il y a un isomorphisme canonique*

$$K_0(R) \cong \mathbb{Z} \oplus Cl(R),$$

où $Cl(R)$ est le groupe de classes d'idéaux de l'anneau R.

On en déduit immédiatement le résultat suivant pour des anneaux de Dedekind bien particuliers :

Corollaire 1.1.3 *Soit F un corps de nombres, alors*

$$K_0(o_F) \cong \mathbb{Z} \oplus Cl(F),$$

où o_F est l'anneau d'entiers de F et $Cl(F) := Cl(o_F)$.

1.2 Le groupe K_1

Soit R un anneau unitaire et n un entier ≥ 1. Nous noterons $GL_n(R)$ le groupe des matrices carrées $n \times n$, inversibles à coefficients dans R. Par la correspondance $A \mapsto \begin{pmatrix} A & o \\ o & o \end{pmatrix}$, le groupe $GL_n(R)$ s'injecte dans $GL_{n+1}(R)$. Donc, on peut considérer la limite directe

$$GL(R) := \varinjlim GL_n(R) = \cup_{n \geq 1} GL_n(R),$$

que l'on appelle le groupe linéaire général infini.

Le *groupe de Whitehead* $K_1(R)$ est défini comme l'abélianisé du groupe linéaire infini $GL(R) = \cup_{n\geq 1} GL_n(R)$, nous avons donc

$$K_1(R) := GL(R)/[GL(R), GL(R)],$$

où $[\ ,\ ]$ est le sous-groupe des commutateurs.

Soit $E_n(R)$ le sous-groupe de $GL_n(R)$ engendré par les matrices élémentaires

$$E_{ij}(a) = I_n + ae_{ij}, \qquad 1 \leq i \neq j \leq n, \qquad a \in R,$$

où I_n est la matrice identité de taille n, les e_{ij} sont les matrices unités standard. Les générateurs de $E_{ij}(a)$ vérifient les relations suivantes :

$$\begin{aligned} E_{ij}(a)E_{ij}(b) &= E_{ij}(a+b), \\ [E_{ij}(a), E_{jk}(b)] &= E_{ik}(ab) \qquad \text{si } i \neq k, \\ [E_{ij}(a), E_{lk}(b)] &= 1 \qquad\qquad\ \ \text{si } i \neq k, j \neq l. \end{aligned}$$

Notons

$$E(R) := \varinjlim E_n(R) = \cup_{n\geq 1} E_n(R),$$

que l'on appelle le groupe des matrices élémentaires sur R.

La seconde relation montre que $E_n(R)$ est un groupe parfait (un groupe est dit parfait s'il est égal à son sous-groupe des commutateurs) pour $n \geq 3$. On a :

Lemme 1.2.1 (Whitehead) *Le groupe dérivé de $GL(R)$, c'est-à-dire le sous-groupe de $GL(R)$ engendré par les commutateurs, est le groupe $E(R)$:*

$$E(R) = [GL(R), GL(R)].$$

Par conséquent, $E(R)$ est un sous-groupe distingué de $GL(R)$. Nous avons donc

$$K_1(R) := GL(R)/E(R),$$

qui est un groupe abélien, compte tenu du lemme de Whitehead.

Proposition 1.2.2 *Soit R un anneau, alors*

$$K_1(R) \cong H_1(GL(R), \mathbb{Z}).$$

Si R est un anneau commutatif. On peut définir $SL_n(R)$, le sous-groupe de $GL_n(R)$ formé des matrices de déterminant $+1$, et

$$SL(R) := \lim_{\rightarrow} SL_n(R) = \cup_{n \geq 1} SL_n(R),$$

que l'on appelle le groupe spécial linéaire infini. Soit R^* les unités de R, nous avons donc une suite exacte

$$1 \longrightarrow SL(R) \longrightarrow GL(R) \xrightarrow{det} R^* \longrightarrow 1.$$

Comme $E(R) \subset SL(R)$, on obtient la suite exacte :

$$1 \longrightarrow SL(R)/E(R) \longrightarrow GL(R)/E(R) \xrightarrow{det} R^* \longrightarrow 1.$$

Puisque la composée

$$R^* \cong GL_1(R) \cong GL_1(R)/E_1(R) \subset GL(R)/E(R) = K_1(R) \xrightarrow{det} R^*,$$

est l'identité.

Proposition 1.2.3 [Ro 94] *Supposons que R est commutatif, alors*

$$K_1(R) \cong R^* \oplus SK_1(R),$$

où $SK_1(R) := SL(R)/E(R)$ et R^* est son groupe des unités.

Pour le cas qui nous intéresse en arithmétique, nous avons le résultat non-trivial suivant, qui découle de la solution au problème du sous-groupe de congruence ([Ba-Mi-Se 73]).

Théorème 1.2.4 *Soit R un anneau commutatif local ou l'anneau des entiers d'un corps de nombres, alors $SK_1(R)$ est trivial, donc*

$$K_1(R) \cong R^*.$$

En particulier, si F est un corps de nombres, alors

$$K_1(F) \cong F^* \text{ et } K_1(o_F) \cong U_F,$$

où o_F est l'anneau d'entiers de F et $U_F := o_F^*$ est le groupe des unités de F.

Exemple 1.2.5 *On a l'isomorphisme de groupes*

$$K_1(\mathbb{Z}) \cong \{+1, -1\} \cong \mathbb{Z}/2\mathbb{Z},$$

$$K_1(\mathbb{Z}[i]) \cong \{+1, -1, +i, -i\} \cong \mathbb{Z}/4\mathbb{Z}.$$

1.3 Le groupe K_2

Soit R un anneau unitaire. Soit n un entier ≥ 3. Le *groupe de Steinberg* $St_n(R)$ est, par définition, le groupe abélien libre de générateurs $x_{ij}(a)$, pour $1 \leq i, j \leq n$, $i \neq j$, et $a \in R$, modulo les relations universelles suivantes :

$$x_{ij}(a)x_{ij}(b) = x_{ij}(a+b),$$

$$[x_{ij}(a), x_{jk}(b)] = x_{ik}(ab) \qquad \text{si } i \neq k,$$

$$[x_{ij}(a), x_{lk}(b)] = 1 \qquad \text{si } i \neq k, j \neq l.$$

On peut naturellement considérer le morphisme de groupes de $St_n(R)$ dans $St_{n+1}(R)$ qui, à l'élément $x_{ij}(a) \in St_n(R)$, associe l'élément correspondant $x_{ij}(a) \in St_{n+1}(R)$.
Ainsi, on peut définir la limite directe

$$St(R) := \varinjlim St_n(R),$$

que l'on appelle le groupe de Steinberg.

En posant $\phi_n(x_{ij}(a)) = E_{ij}(a)$, on peut définir un morphisme canonique de groupes :

$$\phi_n : St_n(R) \to GL_n(R),$$

dont l'image est $\phi_n(St_n(R)) = E_n(R)$. En particulier, en passant à la limite directe, on obtient un morphisme de groupes

$$\phi : St(R) \to GL(R),$$

tel que $\phi(St(R)) = E(R)$.

Pour l'anneau unitaire R, Milnor (cf. [Mi 71]) définit ensuite le groupe $K_2(R)$ comme le noyau de la surjection naturelle de $St(R) \longrightarrow E(R)$. Nous avons donc la suite exacte :

$$1 \longrightarrow K_2(R) \longrightarrow St(R) \longrightarrow GL(R) \longrightarrow K_1(R) \longrightarrow 1.$$

Théorème 1.3.1 *Soit R un anneau, alors le groupe $K_2(R)$ est le centre du groupe de Steinberg $St(R)$. En particulier, $K_2(R)$ est un groupe abélien.*

Proposition 1.3.2 *Le groupe de Steinberg $St(R)$ associé au morphisme naturel ϕ est l'extension centrale universelle du groupe parfait $E(R)$. De plus, la théorie des extensions centrales universelles nous fournit l'isomorphisme*

$$K_2(R) \cong H_2(E(R), \mathbb{Z}).$$

Soit F un corps. Alors Matsumoto a démontré [Mi 71] que :

$$K_2(F) = F^* \otimes F^* / < u \otimes 1 - u,\ u \neq 0, 1 > .$$

En d'autres termes, $K_2(F)$ est défini par les générateurs $\{u, v\}$, $u, v \in F^*$, et les relations :

$$\begin{aligned} \{uv, w\} &= \{u, w\}\{v, w\}, \\ \{u, vw\} &= \{u, v\}\{u, w\}, \\ \{u, 1-u\} &= 1. \end{aligned}$$

Comme

$$-u = (1-u)(1-u^{-1})^{-1},$$

on a

$$\{u, -u\} = \{u, 1-u\}\{u, 1-u^{-1}\}^{-1} = \{u^{-1}, 1-u^{-1}\} = 1$$

et

$$1 = \{uv, -uv\} = \{u, -u\}\{u, v\}\{v, u\}\{v, -v\} = \{u, v\}\{v, u\}$$

donc

$$\{u, v\}^{-1} = \{v, u\}.$$

Exemple 1.3.3 (Milnor [Mi 71]) 1. *Soit F est un corps fini, alors le groupe $K_2(F)$ est trivial.*

2. $K_2(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

1.4 Les K-groupes supérieurs

Soit F un corps. Suite au théorème de Matsumoto, Milnor a introduit les K-groupes supérieurs $K_n^M(F)$ du corps F (voir [Mi 71]) - appelés *K-groupes de Milnor*-définis comme le quotient du n-ième produit tensoriel $F^* \otimes ... \otimes F^*$ par le sous-groupe de générateurs avec $< u_1 \otimes ... \otimes u_n >$, tel que $u_i + u_j = 1$ pour un certain $i \neq j$, avec la notation,

$$K_n^M(F) = (F^*)^{\otimes n} / < u_1 \otimes ... \otimes u_n;\ \exists i \neq j,\ u_i + u_j = 1 >,$$

où l'on a noté $(F^*)^{\otimes n} = \underbrace{F^* \otimes ... \otimes F^*}_{\text{n fois}}$.

Nous avons un théorème établissant la structure, pour un corps de nombres, des groupes $K_n^M(F)$ pour $n \geq 3$.

Théorème 1.4.1 (Bass, Tate [Ba-Ta 67]) *Soit F un corps de nombres, alors pour tout $n \geq 3$, on a*

$$K_n^M(F) \cong (\mathbb{Z}/2\mathbb{Z})^{r_1},$$

où r_1 est le nombre de places réelles de F .

Soit m un entier premier à la caractéristique de F. Alors le cup-produit induit un morphisme

$$g_{n,m} : K_n^M(F)/m \longrightarrow H^n(F, \mu_m^{\otimes n}),$$

que l'on appelle le *symbole galoisien*. Milnor a conjecturé que pour $m = 2$ les flèches $g_{n,2}$ sont des isomorphismes pour tout n. Bloch et Kato ont étendu cette conjecture à toutes les valeurs de m. Merkuriev et Suslin ont prouvé les conjectures de Bloch-Kato pour $n = 2$ et un corps quelconque F, *i.e.*, ils ont prouvé que le morphisme

$$g_{2,m} : K_2(F)/m \longrightarrow H^2(F, \mu_m \otimes \mu_m),$$

est un isomorphisme pour tout m (cf. [Me-Su 83]).

Passons maintenant à la définition qu'a donnée Quillen des groupes de K-théorie supérieurs. On a vu que les groupes K_1 et K_2 sont étroitement liés à l'homologie entière du groupe général linéaire infini :

$$K_1(R) \cong H_1(GL(R), \mathbb{Z}),$$

$$K_2(R) \cong H_2(E(R), \mathbb{Z}).$$

Ainsi, $K_1(R)$ et $K_2(R)$ sont intimement liés à l'homologie entière de $GL(R)$. C'est en partant de ce constat que Quillen s'est mis an quête d'un espace topologique dont l'homologie entière en tant qu'espace est proche de celle de $GL(R)$, pour ensuite définir les K-groupes supérieurs comme étant les groupes d'homotopie de cet espace. Dans une première étape, considérons l'espace classifiant $BGL(R)$ de $GL(R)$([Ro 94], chapitre 5). À équivalence d'homotopie près, cet espace est caractérisé par le fait qu'il est connexe et que ses groupes d'homotopie sont

$$\pi_1(BGL(R)) \cong GL(R),$$
$$\pi_i(BGL(R)) = 0,$$

pour $i \geq 2$. De plus :

$$H_n(BGL(R), \mathbb{Z}) \cong H_n(GL(R), \mathbb{Z}),$$

pour tout $n \geq 2$.
La construction " $+$ " de Quillen sur $BGL(R)$ est prise relativement au sous-groupe parfait $E(R)$ de $GL(R)$, noté $BGL(R)^+$, et possède la même homologie entière que $BGL(R)$ et l'inclusion $BGL(R) \longrightarrow BGL(R)^+$ induit l'application quotient

$$\pi_1(BGL(R)) \cong GL(R) \longrightarrow \pi_1(BGL(R)^+) \cong GL(R)/E(R).$$

Pour tout anneau R et tout entier $n \geq 1$, les groupes de K-théorie supérieurs $K_n(R)$ sont donc définis par

$$K_n(R) := \pi_n(BGL(R)^+).$$

On a donc un homomorphisme

$$K_n(R) = \pi_n(BGL(R)^+) \longrightarrow H_n(BGL(R)^+, \mathbb{Z})$$
$$= H_n(BGL(R), \mathbb{Z}) = H_n(GL(R), \mathbb{Z}),$$

appelé *morphisme d'Hurewicz*. En particulier, pour $n = 1$, on obtient

$$K_1(R) = H_1(GL(R), \mathbb{Z}) = GL(R)/E(R).$$

Pour le cas $n = 2$, puisque $BE(R)^+$ est le revêtement universel de $BGL(R)^+$ et que $\pi_1(BE(R)^+)$ est trivial, il vient

$$K_2(R) = \pi_2(BGL(R)^+) = \pi_2(BE(R)^+) = H_2(BE(R)^+, \mathbb{Z}) = H_2(E(R), \mathbb{Z}),$$

donc la définition de Quillen de $K_2(R)$ coïncide avec celle de Milnor.

Théorème 1.4.2 (Quillen [Qu 72]) *Soit $F = \mathbb{F}_q$ un corps fini avec q éléments, alors pour tout $n \geq 1$, on a*

$$K_{2n}(\mathbb{F}_q) = 0,$$

$$K_{2n-1}(\mathbb{F}_q) \cong \mathbb{Z}/(q^n - 1)\mathbb{Z}.$$

Soit o_F l'anneau des entiers d'un corps global. On a l'important théorème suivant :

Théorème 1.4.3 [Qu 72] *Soit o_F l'anneau des entiers d'un corps global. Pour tout $n \geq 0$, les groupes de K-théorie $K_n(o_F)$ sont de type fini.*

Les rangs de ces groupes ont été déterminés par Borel (cf. [Bo 77]) :

Théorème 1.4.4 *Pour $n \geq 1$, les groupes de K-théorie $K_{2n}(o_F)$ sont finis et*

$$rg_{\mathbb{Z}}(K_{2n-1}(o_F)) = \begin{cases} r_1 + r_2 & \text{si } n \text{ est impair} \geq 3 \\ r_2 & \text{si } n \text{ est pair,} \end{cases}$$

où r_1 est le nombre de places réelles de F et r_2 est le nombre de places complexes de F.

Théorème 1.4.5 (Soulé [So 84]) *Soit o_F l'anneau des entiers d'un corps global, alors*

$$K_{2n-1}(o_F) \cong K_{2n-1}(F),$$

pour tout $n \geq 2$.

1.5 Module tordu à la Tate

Soient F un corps et F^S une clôture algébrique séparable de F, et G_F le groupe de Galois de F^S sur F. Pour tout $m \geq 1$ premier avec la caractéristique de F, on note μ_m le groupe des racines m-ièmes de l'unité dans

F^S.
Soit p un nombre premier distinct de la caractéristique de F. Pour tout entier $i \geq 0$ on a un diagramme commutatif de G_F-modules discrets

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_{p^{i+1}} & \longrightarrow & F^{S*} & \xrightarrow{p^{i+1}} & F^{S*} & \longrightarrow & 0 \\ & & p\downarrow & & p\downarrow & & \mathrm{id}\downarrow & & \\ 0 & \longrightarrow & \mu_{p^i} & \longrightarrow & F^{S*} & \xrightarrow{p^i} & F^{S*} & \longrightarrow & 0 \end{array}$$

dont les lignes sont exactes. Puisque les flèches $\mu_{p^{i+1}} \longrightarrow \mu_{p^i}$ sont surjectives, la limite inverse de cette suite exacte de systèmes inverses est une suite exacte

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \varprojlim F^{S*} \longrightarrow F^{S*} \longrightarrow 0,$$

où l'on a posé $\mathbb{Z}_p(1) = \varprojlim \mu_{p^i}$, qui est un $\mathbb{Z}_p$-module libre de rang 1. Pour tout entier $m \in \mathbb{Z}$, on définit les G_F-modules $\mathbb{Z}_p(m)$ par :

$$\begin{cases} \mathbb{Z}_p(m+1) = \mathbb{Z}_p(m) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1) & \text{pour } m \geq 0 \\ \mathbb{Z}_p(0) = \mathbb{Z}_p & \\ \mathbb{Z}_p(m-1) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1), \mathbb{Z}_p(m)) & \text{pour } m \leq 0. \end{cases}$$

Et pour tout $(\mathbb{Z}_p, G_F)$-module M, on définit le m-ième *tordu à la Tate* de M par

$$M(m) = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(m),$$

avec les propiétés suivantes :

1. pour tout $n, m \in \mathbb{Z}$, $M(n)(m) \cong M(n+m)$;

2. pour tous $(\mathbb{Z}_p, G_F)$-modules M, N on a

$$\mathrm{Hom}_{\mathbb{Z}_p}(M, N(n)) \cong \mathrm{Hom}_{\mathbb{Z}_p}(M, N)(n) \cong \mathrm{Hom}_{\mathbb{Z}_p}(M(-n), N).$$

1.6 Les K-groupes étales

Dans cette section, nous avons les principales définitions et propriétés de la construction des groupes de K-théorie étale pour un corps de nombres F. Soit S un ensemble de places de F contenant l'ensemble S_p des places divisant

p et les places archimédiennes de F. Soit o_F^S l'anneau des S-entiers de F. Fixons un premier p.

Soit G_F^S le groupe de Galois de l'extension algébrique maximale de F non-ramifiée en dehors des places de S. Les groupes de cohomologie étale $H^*_{ét}(\text{spec } o_F[1/p], \mu_{p^m}^{\otimes n})$ du schéma spec $o_F[1/p]$ à valeurs dans le faisceau étale $\mu_{p^m}^{\otimes n}$ s'identifient aux groupes de cohomologie galoisienne $H^*(G_F^S, \mu_{p^m}^{\otimes n})$.
Le groupe de Galois G_F^S agit diagonalement sur le n-ième produit tensoriel $\mu_{p^m}^{\otimes n}$: $\sigma.(\zeta_1 \otimes ... \otimes \zeta_n) = \sigma(\zeta_1) \otimes ... \otimes \sigma(\zeta_n)$. Par simplicité, nous noterons $H^*_{ét}(o_F^S, \mathbb{Z}/p^m(n))$ au lieu de $H^*_{ét}(\text{spec } o_F[1/p], \mu_{p^m}^{\otimes n})$.
On note :

$$H^*_{ét}(o_F^S, \mathbb{Z}_p(n)) = \varprojlim H^*_{ét}(o_F^S, \mathbb{Z}/p^m(n)),$$

pour les groupes de cohomologie étale p-adiques et

$$H^*_{ét}(o_F^S, \mathbb{Q}_p/\mathbb{Z}_p(n)) = \varinjlim H^*_{ét}(o_F^S, \mathbb{Z}/p^m(n)).$$

Pour tout $n \in \mathbb{Z}$ la suite exacte

$$0 \longrightarrow \mathbb{Z}_p(n) \longrightarrow \mathbb{Q}_p(n) \longrightarrow \mathbb{Q}_p(n)/\mathbb{Z}_p(n) \longrightarrow 0,$$

donne par cohomologie étale des morphismes suivants :

$$\delta_i : H^{i-1}_{ét}(o_F^S, \mathbb{Q}_p/\mathbb{Z}_p(n)) \longrightarrow H^i_{ét}(o_F^S, \mathbb{Z}_p(n)).$$

Pour tout entier $i \geq 1$, alors pour les noyaux et les conoyaux de δ_i, nous avons ([Ta 76])

$$\text{Ker}(\delta_i) = \text{Div } H^{i-1}_{ét}(o_F^S, \mathbb{Q}_p/\mathbb{Z}_p(n)),$$

où $\text{Div}(G)$ est le sous-groupe divisible maximal de G, et

$$\text{Im}(\delta_i) = \text{Tor}_{\mathbb{Z}_p} H^i_{ét}(o_F^S, \mathbb{Z}_p(n)),$$

où $\text{Tor}_R(M)$ le sous-module de M formé des éléments de R-torsion.

Pour tout entier $i \geq 1$, nous obtenons ainsi l'isomorphisme suivant :

$$H^{i-1}_{ét}(o_F^S, \mathbb{Q}_p/\mathbb{Z}_p(n))/\text{Div} \cong \text{Tor}_{\mathbb{Z}_p} H^i_{ét}(o_F^S, \mathbb{Z}_p(n)).$$

En particulier, pour $i = 1$, puisque Div est trivial, on obtient que le sous-groupe de torsion de $H^1_{ét}(o_F^S, \mathbb{Z}_p(n))$ est isomorphe à $H^0_{ét}(o_F^S, \mathbb{Q}_p/\mathbb{Z}_p(n))$.

Les Théorèmes suivants concernent les groupes de cohomologie étale p-adiques des anneaux d'entiers de corps globaux.

Théorème 1.6.1 [So 79] 1. *Pour $n \neq 0$, $H^0_{ét}(o_F^S, \mathbb{Z}_p(n)) = 0$.*

2. *Pour $k \geq 3$, $H^k_{ét}(o_F^S, \mathbb{Z}_p(n)) = 0$ si p est impair.*

3. *Pour $k \geq 3$, $H^k_{ét}(o_F^S, \mathbb{Z}_2(n)) \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^{r_1(F)} & \text{si } k+n \text{ est pair} \\ 0 & \text{sinon.} \end{cases}$*

En général, la conjecture de Quillen-Lichtenbaum prédit :

Théorème 1.6.2 (Quillen-Lichtenbaum) *Soit F un corps global. Les caractères de Chern étales*

$$ch^{(p)}_{i,n} : K_{2n-i}(o_F) \otimes \mathbb{Z}_p \to H^i_{ét}(o_F^S, \mathbb{Z}_p(n)),$$

sont des isomorphismes pour $n \geq 2$, $i = 1, 2$ et p impair.

Pour $n = i = 1$, il existe également un caractère de Chern

$$ch^{(p)}_{1,1} : K_1(o_F) \otimes \mathbb{Z}_p \to H^1_{ét}(o_F^S, \mathbb{Z}_p(1)).$$

Les groupes de cohomologie étale $H^1_{ét}(o_F^S, \mu_{p^n})$ apparaissent dans la suite exacte

$$0 \longrightarrow (o_F^S)^*/p^n \longrightarrow H^1_{ét}(o_F^S, \mu_{p^n}) \longrightarrow_{p^n} Cl(o_F^S) \longrightarrow 0,$$

où ${}_{p^n}Cl(o_F^S)$ désigne les éléments de $Cl(o_F^S)$ tués par p^n, si bien qu'en prenant la limite projective il vient

$$H^1_{ét}(o_F^S, \mathbb{Z}_p(1)) \cong (o_F^S)^* \otimes \mathbb{Z}_p,$$

et le caractère de Chern $ch^{(p)}_{1,1}$ n'est autre que le déterminant.

Dwyer et Friedlander ont introduit les groupes de K-théorie étale supérieure $K^{ét}_{2n-i}(o_F^S)$ et montré que pour tout entier $n \geq 2, i = 1, 2$, on a un morphisme surjectif à noyau fini

$$K_{2n-i}(o_F^S) \otimes \mathbb{Z}_p \to K^{ét}_{2n-i}(o_F^S),$$

et un isomorphisme

$$K^{ét}_{2n-i}(o^S_F) \cong H^i_{ét}(o^S_F, \mathbb{Z}_p(n)).$$

En particulier, on a

$$K^{ét}_{2n-1}F = K^{ét}_{2n-1}(o_F).$$

Tate et Soulé ont montré que pour $n = i = 2$, ces surjections sont en fait des isomorphismes :

$$K^{ét}_2(o^S_F) := K_2(o^S_F)\{p\} \cong H^2_{ét}(o^S_F, \mathbb{Z}_p(2)).$$

Pour le K_3, Levine [Le 89] et Merkurjev-Suslin [Me-Su 90] ont montré que le noyau de la surjection $K_3(F) \otimes \mathbb{Z}_2 \to H^1_{ét}(o^S_F, \mathbb{Z}_2(2))$ est isomorphe à $K^M_3(F) \cong (\mathbb{Z}/2\mathbb{Z})^{r_1(F)}$. Nous avons donc la suite exacte suivante :

$$0 \to (\mathbb{Z}/2\mathbb{Z})^{r_1(F)} \to K_3(F) \otimes \mathbb{Z}_2 \to H^1_{ét}(o^S_F, \mathbb{Z}_2(2)) \to 0.$$

Pour tout corps F, le quotient $K_3(F)/K^M_3(F)$ s'appelle le K_3 indécomposable, on le note $K^{ind}_3(F)$.

Des Théorèmes 1.4.4 et 1.6.2, on déduit la structure des groupes de cohomologie étale $H^i_{ét}(o^S_F, \mathbb{Z}_p(n))$ pour $i = 1, 2$ et $n \geq 2$.

Corollaire 1.6.3 *Pour $n \geq 2$, le groupe $H^2_{ét}(o^S_F, \mathbb{Z}_p(n))$ est fini et même trivial pour presque tous premiers p, et*

$$rg_{\mathbb{Z}} H^1_{ét}(o^S_F, \mathbb{Z}_p(n)) = \begin{cases} r_1 + r_2 & \text{si } n \text{ est impair} \geq 1 \\ r_2 & \text{si } n \text{ est pair} \end{cases}$$

Notons pour conclure que

$$H^2_{ét}(o^S_F, \mathbb{Q}_p/\mathbb{Z}_p(n)) = H^2_{ét}(F, \mathbb{Q}_p/\mathbb{Z}_p(n)) = 0,$$

pour $n \geq 2$ et p impair (c'est une conséquence de la finitude des groupes $K_{2n-2}(o_F)$: Soulé-Tate).

Le résultat suivant est du à B. Kahn ([Ka 93-1, Théorème 2.1, Proposition 6.1]) :

Théorème 1.6.4 *Soit E/F une extension galoisienne de corps de nombres de groupe de Galois G et S un ensemble de places de F contenant des places qui sont ramifiées dans E. Alors, Il existe une suite exacte*

$$0 \to H^1(G, K_3^{ind}(E)) \to K_2(o_F^S) \to K_2(o_F^S)^G \to H^2(G, K_3^{ind}(E)) \to 0.$$

L'analogue pour les K-groupes étales supérieurs est bien connu (voir [As 94], [Br 93], [Ko-Mo 00]) :

Théorème 1.6.5 *Soit E/F une p-extension galoisienne de corps de nombres de groupe de Galois G et S un ensemble de places de F contenant les places divisant p et celles qui sont ramifiées dans E, alors pour $i \geq 2$ et p impair il existe une suite exacte*

$$0 \to H^1(G, K_{2i-1}^{\acute{e}t}E) \to K_{2i-2}^{\acute{e}t}(o_F^S) \to (K_{2i-2}^{\acute{e}t}(o_E^S))^G \to H^2(G, K_{2i-1}^{\acute{e}t}E) \to 0.$$

D'autre part, nous avons la co-descente pour les K-groupes pairs $K_{2i-2}^{\text{ét}}(o_F^S)$:

Proposition 1.6.6 *Soit E/F une p-extension galoisienne de corps de nombres de groupe de Galois G et S un ensemble de places de F contenant les places divisant p et les places qui sont ramifiées dans E, alors pour $i \geq 2$ et p impair*

$$(K_{2i-2}^{\acute{e}t}(o_E^S))_G \cong K_{2i-2}^{\acute{e}t}(o_F^S).$$

Maintenant $K_{2i-2}^{\text{ét}}(o_E^S)$ est fini, et par conséquent cette proposition et le Théorème 1.6.5 nous donnent :

Proposition 1.6.7 *Soit E/F une p-extension galoisienne cyclique de corps de nombres de groupe de Galois G et S un ensemble de places de F contenant les places divisant p et les places qui sont ramifiées dans E, alors pour $i \geq 2$ et p impair le quotient*

$$\frac{H^2(G, K_{2i-1}^{\acute{e}t}E)}{H^1(G, K_{2i-1}^{\acute{e}t}E)}$$

est trivial.

Pour finir, rappelons la définition des noyaux sauvages étales supérieurs (voir [Ba 93], [Ko 93], [Ng 92]) :

$$WK^{\text{ét}}_{2i-2}(F) := \ \ker(H^2_{\text{ét}}(o_F^S, \mathbb{Z}_p(i)) \to \oplus_{v\in S} H^2(F_v, \mathbb{Z}_p(i))).$$

La définition est indépendante du choix de l'ensemble fini S contenant S_p, et la dualité de Poitou-Tate entraîne la suite exact

$$0 \to WK^{\text{ét}}_{2i-2}(F) \to K^{\text{ét}}_{2i-2}(o_F^S) \to \oplus_{v\in S} H^2(F_v, \mathbb{Z}_p(i))) \to H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(1-i))^* \to 0.$$

où $*$ indique le dual de Pontryagin.

Chapitre 2

Théorie d'Iwasawa

Dans ce chapitre, nous exposons quelques résultats sur les $\mathbb{Z}_p$-extensions des corps de nombres, où p est un nombre premier impair. On insiste en particulier sur les modules d'Iwasawa standard dont on se sert abondamment aux chapitres suivants.

2.1 $\mathbb{Z}_p$-extensions

Dans cette section, nous exposons quelques résultats sur les $\mathbb{Z}_p$-extensions des corps de nombres. On fixe un nombre premier p supposé impair. Une $\mathbb{Z}_p$-*extension* d'un corps de nombres F est une extension galoisienne F_∞/F de groupe de Galois isomorphe à l'anneau des entiers p-adiques $\mathbb{Z}_p$:

$$Gal(F_\infty/F) \cong \mathbb{Z}_p.$$

Comme les sous-groupes fermés de $\mathbb{Z}_p$ sont (0) et $p^n\mathbb{Z}_p$, $n \geq 0$, par correspondance galoisienne pour tout n, il existe un unique corps intermédiaire F_n de F_∞/F :

$$F = F_o \subset F_1 \subset F_2 \subset ... \subset F_\infty = \bigcup_{n\geq 0} F_n,$$

avec $[F_n : F] = p^n$ et

$$Gal(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Le corps de nombres F possède toujours au moins une $\mathbb{Z}_p$-extension, la $\mathbb{Z}_p$-*extensions cyclotomique*, construite comme suit :
Soit $\mu_{p^{n+1}}$ le groupe des racines p^{n+1}-ièmes de l'unité. Comme le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q})$ est cyclique de degré $(p-1)p^n$, il existe un unique sous-corps $\mathbb{Q}_n$ de $\mathbb{Q}(\mu_{p^{n+1}})$ tel que $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. Soit $\mathbb{Q}_\infty$ l'union sur n des corps $\mathbb{Q}_n$. Alors $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$. Il suffit ensuite de prendre $F_\infty := F.\mathbb{Q}_\infty$. Soit $\mathbb{Q}_e := F \cap \mathbb{Q}_\infty$, alors

$$Gal(F_\infty/F) \cong \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_e) \cong \mathbb{Z}_p.$$

Dans la $\mathbb{Z}_p$-extension cyclotomique, toutes les p-places se ramifient, puisque, la $\mathbb{Z}_p$-extension cyclotomique $\mathbb{Q}_\infty$ de $\mathbb{Q}$ est totalement ramifiée en p.

La ramification dans les $\mathbb{Z}_p$-extensions d'un corps de nombres est décrite par la Proposition suivante :

Proposition 2.1.1 *Soit F un corps de nombres et F_∞/F une $\mathbb{Z}_p$-extension. Alors*

(i) *F_∞/F est non-ramifiée en dehors des places de F divisant p (on dit que les $\mathbb{Z}_p$-extensions sont p-ramifiées).*

(ii) *Il existe au mois une place v au-dessus de p ramifiée dans F_∞/F et il existe un entier $n \geq 0$ tel que toute place de F qui se ramifie dans F_∞/F se ramifie totalement dans F_∞/F_n.*

Preuve. Soit v une non-p-place de F et $I_v \subseteq Gal(F_\infty/F) \cong \mathbb{Z}_p$ son groupe d'inertie. Puisque le groupe I_v est fermé, $I_v = 0$ ou $I_v = p^n\mathbb{Z}_p$ pour un certain n. Si $I_v = 0$ alors v est non ramifiée dans F_∞/F. Supposons $I_v = p^n\mathbb{Z}_p$. Puisque I_v est infini et doit être de degré 1 ou 2 pour les places infinies, on peut supposer que v est une place finie. Pour tout n, soit v_n une place de F_n divisant v_{n-1} avec $v_0 = v$. On appelle $F_{n,v}$ le complété en la place v_n et on pose $F_{\infty,v} = \cup F_{n,v}$. Alors

$$I_v \subseteq Gal(F_{\infty,v}/F_v).$$

Soit U le groupe des unités de $F_v = F_{0,v}$. La théorie du corps de classes local fournit un homomorphisme surjectif

$$U \longrightarrow I_v \cong p^n\mathbb{Z}_p.$$

Mais, le logarithme l-adique, induit un isomorphisme

$$U \cong (\text{groupe fini}) \times \mathbb{Z}_l^r, \quad r \in \mathbb{Z},$$

où l est la place rationnelle que divise v. On aurait alors un morphisme surjectif $\mathbb{Z}_l^r \longrightarrow p^n\mathbb{Z}_p \longrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$. Puisque $\mathbb{Z}_l^r$ n'a pas de sous-groupe fermé d'indice p, ceci est impossible, donc $I_v = 0$, et (i) est démontré.

Par la théorie du corps de classes, on sait que l'extension abélienne non-ramifiée maximale de F a un groupe de Galois isomorphe au groupe des classes de F, qui est fini , puisque F est un corps de nombres. Or, F_∞/F est un extension infinie, donc un premier doit se ramifier dans F_∞/F.
D'aprés (i), seul un nombre fini de places de F se ramifie dans F_∞/F. On note $I_1, ..., I_s$ les groupes d'inertie correspondants aux places qui se ramifient dans l'extension. Alors

$$\bigcap_{i=1}^{s} I_i = p^n\mathbb{Z}_p,$$

pour un certain n. Le corps fixe par $p^n\mathbb{Z}_p$ est F_n et $Gal(F_\infty/F_n)$ est contenu dans tous les I_i. Donc tous les premiers qui se ramifient dans $Gal(F_\infty/F)$ se ramifient totalement dans $Gal(F_\infty/F_n)$, et (ii) est démontré. □

Dans la suite, on note n_0 le plus petit entier n tel que l'extension F_∞/F_n est totalement ramifiée au-dessus de p. Lorsque F_∞/F est la $\mathbb{Z}_p$-extension cyclotomique et $[F : \mathbb{Q}]$ premier à p ou p ne se ramifie pas dans $F/\mathbb{Q}$, alors $n_0 = 0$.

Notons U_F le groupe des unités de F, F_v le complété de F en la place v et U_v le groupe des unités locales de F_v. Soit D_F le *noyau de Leopoldt*, c'est-à-dire, le noyau du morphisme suivant :

$$U_F \otimes \mathbb{Z}_p \longrightarrow \prod_{v|p} U_v \otimes \mathbb{Z}_p,$$

où $U_F \otimes \mathbb{Z}_p$ est le pro-p- complété de U_F et $U_v \otimes \mathbb{Z}_p$ est le pro-p- complété de U_v. Alors D_F est un $\mathbb{Z}_p$-module libre, de rang δ_F, appelé *défaut de Leopoldt*. Une des formulations de la *conjecture de Leopoldt* s'énonce comme suit :

Conjecture (de Leopoldt) Pour tout corps de nombre F, $\delta_F = 0$.

Notons S_p l'ensemble des places de F divisant p et M_F (resp. L_F) la pro-p-extension (resp. p-extension) abélienne maximale S_p-ramifiée (resp. non-ramifiée) de F. Par la théorie du corps de classes global on a :

$$0 \to D_F \to U_F \otimes \mathbb{Z}_p \to \prod_{v|p} U_v \otimes \mathbb{Z}_p \xrightarrow{A} G(M_F/F) \to G(L_F/F) \to 0,$$

où A envoie chaque facteur $U_v \otimes \mathbb{Z}_p$ sur le groupe d'inertie en v.

Théorème 2.1.2 ([Wa 97], Théorème 13.4) *Soit $\tilde{F}$ la composée de toutes les $\mathbb{Z}_p$-extensions de F et δ_F le défaut de Leopoldt, Alors*

$$Gal(\tilde{F}/F) \cong \mathbb{Z}_p^{1+r_2+\delta_F},$$

où $2r_2$ est le nombre de plongements complexes de F.

Ainsi, modulo la conjecture de Leopoldt, le nombre de $\mathbb{Z}_p$-extensions indépendantes de F est égal à $1 + r_2$.

2.2 Modules d'Iwasawa

Soit Γ un groupe topologique multiplicatif isomorphe au groupe additif $\mathbb{Z}_p$. On fixe un générateur topologique γ de Γ. Par exemple, on peut choisir pour γ l'élément correspondant à $1 \in \mathbb{Z}_p$. Puisque les sous-groupes fermés de $\mathbb{Z}_p$ sont de la forme $p^n\mathbb{Z}_p$, les sous-groupes fermés de Γ sont de la forme Γ^{p^n}. Pour $n \geq 0$, soit $\Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$.

Considérons l'algèbre de groupe $\mathbb{Z}_p[\Gamma]$. Pour $n \geq m \geq 0$, on a un morphisme naturel $\phi_n^m : \mathbb{Z}_p[\Gamma_n] \longrightarrow \mathbb{Z}_p[\Gamma_m]$ induit par $\Gamma_n \longrightarrow \Gamma_m$. Il est clair que $\mathbb{Z}_p[\Gamma] \subseteq \mathbb{Z}_p[[\Gamma]]$, car un élément $\alpha \in \mathbb{Z}_p[\Gamma]$ donne une suite d'éléments $\alpha_m \in \mathbb{Z}_p[\Gamma_m]$ tel que $\phi_n^m(\alpha_n) = \alpha_m$.

Soit $w_n = (1+T)^{p^n} - 1$, alors $w_{n+1} = (w_n + 1)^p - 1$, en particulier $w_n | w_{n+1}$. On a donc l'isomorphisme

$$\mathbb{Z}_p[\Gamma_n] \longrightarrow \mathbb{Z}_p[T]/(w_n)$$

$$\gamma \bmod \Gamma^{p^n} \to 1+T \bmod (w_n),$$

Par définition, la limite inverse des algèbres de groupe $\mathbb{Z}_p[\Gamma_n]$ par rapport aux morphismes ϕ_n^m, notée $\Lambda = \mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma_n]$ est appelée l'*algèbre d'Iwasawa*. Nous avons donc :

$$\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \varprojlim \mathbb{Z}_p[T]/(w_n).$$

Un polynôme $P(T) \in \mathbb{Z}_p[T]$ est dit *distingué* si $P(T) = T^n + a_{n-1}T^{n-1} + ... + a_0$ avec $p|a_i$ pour $0 \leq i \leq n-1$.

Soit $f(T) = \sum a_i T^i \in \mathbb{Z}_p[[T]]$, tel que $p|a_i$ pour $0 \leq i \leq n-1$ et $p \not| a_n$. Alors, le théorème de *préparation de Weierstrass* : il existe un entier $\mu \geq 0$ tel que $f(T)$ peut s'écrire de façon unique $f(T) = p^\mu P(T).U(T)$, où $P(T) \in \mathbb{Z}_p[T]$ est distingué de degré n et $U(T) \in \mathbb{Z}_p[[T]]^*$.

Théorème 2.2.1 *L'application $\gamma \longrightarrow 1+T$ induit un isomorphisme*

$$\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]].$$

Preuve. Il suffit de montrer que $\mathbb{Z}_p[[T]] \cong \varprojlim \mathbb{Z}_p[T]/(w_n)$, où w_n est un polynôme distingué. C'est clair que $w_0 \in (p,T)$. Car

$$w_{n+1}/w_n = (1+T)^{p^n(p-1)} + (1+T)^{p^n(p-2)} + ... + (1+T)^{p^n} + 1 \in (p,T),$$

(c'est-à-dire p divise le terme fixe), on a donc $w_n \in (p,T)^{n+1}$. Par l'Algorithme d'Euclide, on a une application naturelle $\mathbb{Z}_p[[T]] \to \mathbb{Z}_p[T]$ $(mod\ w_n)$ pour tout n. On note, $f(T) \to f_n(T)$, où $f(T) = q_n(T)w_n + f_n(T)$, $deg\ f_n \leq p^n - 1$. Si $f_n = 0$ pour tout n, alors w_n divise f pour tout n, et $f \in \cap_{n=0}^{\infty}(p,T)^{n+1} = 0$, donc cette application est injective.

Pour montrer la surjectivité, soit $(f_0, f_1, ...) \in \varprojlim \mathbb{Z}_p[T]/(w_n)$. Pour $m \geq n \geq 0$, $f_m \equiv f_n (mod\ w_n)$ donc aussi $mod\ (p,T)^{n+1}$. Comme $\mathbb{Z}_p[[T]]$ est complet, il s'ensuit que $f = lim f_n$ existe dans $\mathbb{Z}_p[[T]]$. On vérifie alors que $f\ mod\ w_n = f_n$ pour tout n et f est bien un antécédent de $(f_0, f_1, ...)$. $\square$

Proposition 2.2.2 *Les idéaux premiers de Λ sont (0), (p,T), (p) et les $(P(T))$, où $P(T)$ est un polynôme distingué et irréductible. L'idéal (p,T) est l'unique idéal maximal de Λ.*

Preuve. Tous les idéaux mentionnés sont évidemment premiers. Soit $\mathcal{P} \neq 0$ un idéal premier et $h \in \mathcal{P}$ de degré minimum. Alors, $h = p^{\mu}P(T)$ avec $P(T) = 1$ ou $P(T)$ distingué. On a donc $p \in \mathcal{P}$ ou $P(T) \in \mathcal{P}$. Si $P(T) \in \mathcal{P}$ est distingué, alors par minimalité $P(T)$ est irréductible. Donc $f = p$ ou f est irréductible et distingué.
Si $(f) \neq \mathcal{P}$, alors il existe $g \in \mathcal{P}$ tel que $f \not| g$. Comme f est irréductible, on a $(f, g) = 1$, alors $\Lambda/\mathcal{P}$ est fini. Il existe donc un entier n tel que $p^n \in \mathcal{P}$, donc $p \in \mathcal{P}$. Il existe aussi deux entiers $i \leq j$ tels que $T^i = T^j \pmod{\mathcal{P}}$, comme $(1 - T^{i-j}) \in \Lambda^*$, alors $T^i = 0 \pmod{\mathcal{P}}$ et donc $T \in \mathcal{P}$. De sorte que $(p, T) \subseteq \mathcal{P}$. Mais $\Lambda/(p, T) \cong \mathbb{Z}/p\mathbb{Z}$, donc (p, T) est un idéal maximal et $\mathcal{P} = (p, T)$. Ainsi, (p, T) est le seul idéal maximal. □

On dit que le Λ-module M est $pseudo - isomorphe$ au Λ-module M' avec notation $M \sim M'$, s'il existe un morphisme $f : M \longrightarrow M'$ avec le noyau et le conoyau finis. On a une pseudo-décomposition, analogue au théorème de structure des modules de type fini sur un anneau principal.

Théorème 2.2.3 ([Wa 97] Théorème 13.12) *Soit M un Λ-module de type fini. Alors*

$$M \sim \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}),$$

où $r,\ s,\ t,\ n_i,\ m_j$, sont des entiers et les f_j sont des polynômes distingués irréductibles.

Nous introduisons quelques notations utiles pour la suite, $r := rg_{\Lambda}M$ le $\Lambda - rang$ de M et $\lambda(M) := \sum_{i=1}^{m} m_i \deg f_i$ l'invariant λ de M.

Pour un Λ-module M, Notons M^{Γ} le sous-module de M des éléments invariants par Γ et $M_{\Gamma} = M/(\gamma - 1)M$ le module des co-invariants. nous avons les deux résultats classiques suivants (voir [Wa 97], chapitre 13) :

Proposition 2.2.4 *([co 77]) Soit M un Λ-module de type fini et de torsion. Soit $f(T)$ le polynôme caractéristique de M. Les propriétés suivantes sont*

équivalentes :
(i) M^Γ *est fini*
(ii) M_Γ *est fini*
(iii) $f(0) \neq 0$.
Si l'une des propositions est vérifiée, on a

$$\frac{|M^\Gamma|}{|M_\Gamma|} = |f(0)|_p = p^{-v_p(f(0))}.$$

Preuve. De la suite exacte

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

de Λ-modules de torsion, on déduit du lemme du serpent la suite exacte

$$0 \longrightarrow A^\Gamma \longrightarrow B^\Gamma \longrightarrow C^\Gamma \longrightarrow A_\Gamma \longrightarrow B_\Gamma \longrightarrow C_\Gamma \longrightarrow 0.$$

Ceci montre qu'il suffit de prouver la proposition pour le Λ-module élémentaire M dans le théorème de structure. En décomposant M en somme directe, il reste alors deux cas à traiter : $M = \Lambda/p^i\Lambda$ et $M = \Lambda/(f(T))$ où $f(T)$ est un polynôme distingué. Comme $M^\Gamma = ker(M \stackrel{\times T}{\to} M)$ et $M_\Gamma = coker(M \stackrel{\times T}{\to} M)$, il vient dans le premier cas $M^\Gamma = 0$ et $M_\Gamma = \mathbb{Z}/p^i\mathbb{Z}$, d'où la proposition dans ce cas.
Soit $M = \Lambda/(f(T))$. Puisque M est $\mathbb{Z}_p$-libre, M^Γ est fini si et seulment s'il est nul. Or $M^\Gamma = 0$ équivaut à $f(0) \neq 0$, ce que est équivalent à la finitude de $M_\Gamma = M/TM$. Si M^Γ ou M_Γ est fini, on a $M_\Gamma \cong \mathbb{Z}/f(0)\mathbb{Z}$. Cette dernière propriété implique les propriétés habituelles du quotient de Herbrand. □

Proposition 2.2.5 *Soit* M *un* Λ*-module de type fini, on a :*

$$rg_\Lambda M = rg_{\mathbb{Z}_p} M_\Gamma - rg_{\mathbb{Z}_p} M^\Gamma.$$

Preuve. Soit $M = \Lambda^a$, alors $M^\Gamma = 0$ et $M_\Gamma \cong {\mathbb{Z}_p}^a$. Soit $M = \Lambda/(p^n)$, alors $M^\Gamma = 0$ et M_Γ est fini. Soit $M = \Lambda/(f)$, alors M est $\mathbb{Z}_p$-libre, donc $rg_{\mathbb{Z}_p} M_\Gamma = rg_{\mathbb{Z}_p} M^\Gamma$. □

2.3 Modules d'Iwasawa standard

Nous adoptons les notations suivantes :
p un nombre premier impair ;
$\Gamma := \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$;
$\Gamma^{p^n} := \mathrm{Gal}(F_\infty/F_n)$;
$\Lambda = \mathbb{Z}_p[[\Gamma]]$ l'algèbra d'Iwasawa ;
M_∞ la pro-p-extension abélienne maximale S-ramifiée de F_∞ ;
Ω_S la pro-p-extension maximale S-ramifiée de F ;
M_n l'extension abélienne maximale de F_n contenue dans M_∞ ;
$\mathcal{X}_\infty := \mathrm{Gal}(M_\infty/F_\infty)$ le *module d'Iwasawa standard* (p-ramifiée) ;
$G_{S,\infty} := \mathrm{Gal}(\Omega_S/F_\infty)$;
$G_\infty := Gal(M_\infty/F)$;
$G_S := Gal(\Omega_S/F)$.

On a la suite exacte de $\mathbb{Z}_p$-modules

$$0 \longrightarrow \mathcal{X}_\infty \longrightarrow G_\infty \longrightarrow \Gamma \longrightarrow 0.$$

Puisque $\mathcal{X}_\infty$ est abélien, Γ agit sur $\mathcal{X}_\infty$ par

$$x^\gamma = \tilde{\gamma} x \tilde{\gamma}^{-1},$$

où $x \in \mathcal{X}_\infty$ et $\tilde{\gamma}$ est un relèvement de $\gamma \in \Gamma$ à G_∞. Cette action fait de $\mathcal{X}_\infty$ un Λ-module compact. Soit $\mathcal{X}$ un Λ-module compact, alors par le *lemme de Nakayama* on a

$$\mathcal{X} \text{ est un } \Lambda - \text{module de type fini} \Longleftrightarrow \mathcal{X}/\mathfrak{m}\mathcal{X} \text{ est fini.}$$

où $\mathfrak{m}$ est l'unique idéal maximal de Λ.

Soit F_n, $n \geq 0$, les corps intermédiaires de la $\mathbb{Z}_p$-extension F_∞/F :

$$F = F_0 \subset F_1 \subset ... \subset F_n \subset ... \subset F_\infty = \bigcup_{n \geq 0} F_n.$$

où $[F_n : F] = p^n$. On a donc

$$M = M_0 \subset M_1 \subset ... \subset M_n \subset ... \subset M_\infty = \bigcup_{n \geq 0} M_n.$$

Lemme 2.3.1 *Pour tout $n \geq 1$, on a*

$$w_n\mathcal{X}_\infty = Gal(M_\infty/M_n) \quad \text{et} \quad \mathcal{X}_\infty/w_n\mathcal{X}_\infty = Gal(M_n/F_\infty),$$

où $w_n = \gamma^{p^n} - 1$.

Preuve. On a la suite exacte :

$$0 \longrightarrow \mathcal{X}_\infty/Gal(M_\infty/M_n) \longrightarrow Gal(M_n/F_n) \longrightarrow Gal(F_\infty/F_n) = \Gamma^{p^n} \longrightarrow 0.$$

Comme $Gal(M_n/F_n)$ est abélien, Γ^{p^n} agit trivialement sur $\mathcal{X}_\infty/Gal(M_\infty/M_n)$. Donc $w_n\mathcal{X}_\infty \subseteq Gal(M_\infty/M_n)$, puisque Γ^{p^n} est le plus grand quotient qui agit trivialement sur $\mathcal{X}_\infty/Gal(M_\infty/M_n)$.

Soit $L \subseteq M_\infty$ tel que $\mathcal{X}_\infty/w_n\mathcal{X}_\infty = Gal(L/F_n)$. Comme Γ^{p^n} agit trivialement sur $\mathcal{X}_\infty/w_n\mathcal{X}_\infty$, alors $Gal(L/F_n)$ est abélien donc $L \subseteq M_n$ et $Gal(M_\infty/M_n) \subseteq w_n\mathcal{X}_\infty$. □

Puisque $M_\infty = \bigcup_{n\geq 0} M_n$, on a $\mathcal{X}_\infty = \varprojlim \mathcal{X}_\infty/w_n\mathcal{X}_\infty$, où la limite projective est prise pour les applications restrictions.

Corollaire 2.3.2 *$\mathcal{X}_\infty$ est noetherien sur Λ si et seulement si $\mathrm{Gal}(M_0/F)$ est de $\mathbb{Z}_p$-rang fini.*

Preuve. Soit $\mathfrak{m}$ l'unique idéal maximal de Λ, alors $\mathcal{X}_\infty$ est noetherien si et seulement si $\mathcal{X}_\infty/\mathfrak{m}\mathcal{X}_\infty$ est fini. Soit

$$Y = \mathcal{X}_\infty/w_0\mathcal{X}_\infty = \mathrm{Gal}(M_0/F_\infty).$$

Alors $\mathcal{X}_\infty/\mathfrak{m}\mathcal{X}_\infty = Y/pY$, donc $\mathcal{X}_\infty/\mathfrak{m}\mathcal{X}_\infty$ est fini si et seulement si Y est fini si et seulement si $\mathrm{Gal}(M_0/F)$ est de $\mathbb{Z}_p$-rang fini. □

Corollaire 2.3.3 *$\mathcal{X}_\infty$ est un Λ-module noetherien.*

Preuve. Puisque M_0 est l'extension abélienne maximale p-ramifiée de F, par le théorème 2.1.2, $\mathrm{Gal}(M_0/F)$ est de $\mathbb{Z}_p$-rang fini. Par le corollaire 2.3.2, on a donc $\mathcal{X}_\infty$ est fini. □

Puisque M_n est l'extension abélienne maximale p-ramifiée de F_n, on a $F_\infty \subseteq M_n$. Par le théorème 2.1.2,

$$rk_{\mathbb{Z}_p}\mathrm{Gal}(M_0/F) = 1 + r_2(F) + \delta,$$

où $\delta = \delta_F$ est le défaut de Leopoldt de F. De plus,

$$rk_{\mathbb{Z}_p}\mathcal{X}_\infty/w_0\mathcal{X}_\infty = r_2(F) + \delta.$$

Pour tout $n \geq 0$, nous avons donc

$$rk_{\mathbb{Z}_p}\mathcal{X}_\infty/w_n\mathcal{X}_\infty = r_2(F)p^n + \delta_n,$$

où $\delta_n = \delta_{F_n}$ est le défaut de Leopoldt de F_n.

Soit $rk_\Lambda\mathcal{X}_\infty = \alpha$, on a un pseudo-isomorphisme

$$\mathcal{X}_\infty \sim \Lambda^\alpha \oplus \mathrm{Tor}_\Lambda\mathcal{X}_\infty,$$

pour un certain $\alpha \geq 0$. Par le théorème de structure, $rk_{\mathbb{Z}_p}(\mathrm{Tor}_\Lambda\mathcal{X}_\infty/w_n\mathrm{Tor}_\Lambda\mathcal{X}_\infty)$ est borné par $\lambda = \lambda(\mathcal{X}_\infty)$ (l'invariant λ de $\mathcal{X}_\infty$) et comme $rk_{\mathbb{Z}_p}\Lambda^\alpha/w_n\Lambda^\alpha = \alpha p^n$, on obtient

$$\alpha p^n \leq rk_{\mathbb{Z}_p}\mathcal{X}_\infty/w_n\mathcal{X}_\infty \leq \alpha p^n + \lambda,$$

On a donc la proposition suivante :

Proposition 2.3.4 *Soit $\delta_\infty = rk_\Lambda\mathcal{X}_\infty - r_2(F)$, on a $\delta_\infty \geq 0$ et $\delta_\infty = 0$ si et seulement si les défauts de Leopoldt δ_n de F_n sont bornés indépendamment de n.*

On dit que F_∞/F satisfait la conjecture faible de Leopoldt si $\delta_\infty = 0$. Puisque $rk_\Lambda\mathcal{X}_\infty \leq rk_{\mathbb{Z}_p}\mathcal{X}_\infty/w_0\mathcal{X}_\infty$, donc $0 \leq \delta_\infty \leq \delta_F$. Ainsi

Théorème 2.3.5 *Si F satisfait à la conjecture de Leopoldt, alors $\delta_\infty = 0$. C'est-à-dire*

$$\mathcal{X}_\infty \sim \Lambda^{r_2(F)} \oplus \mathrm{Tor}_\Lambda\mathcal{X}_\infty.$$

De plus, par la proposition 2.2.5, puisque $rg_\Lambda \mathcal{X}_\infty = rg_{\mathbb{Z}_p}(\mathcal{X}_\infty)_\Gamma - rg_{\mathbb{Z}_p}\mathcal{X}_\infty^\Gamma$, alors $\delta_\infty = \delta_F - rg_{\mathbb{Z}_p}\mathcal{X}_\infty^\Gamma$.

Soit Ω_S la pro-p-extension maximale S-ramifiée de F, $G_{S,\infty} := \mathrm{Gal}(\Omega_S/F_\infty)$ et $G_S := \mathrm{Gal}(\Omega_S/F)$. La suite spectrale de Hochschild-Serre en basse dimension [Ne-Sc-Wi 00] plus le fait que la p-dimension cohomologique de Γ est 1 donne la suite exacte :

$$0 \to H^1(\Gamma, H^1(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)) \to H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma \to 0.$$

Puisque $\mathbb{Q}_p/\mathbb{Z}_p$ est un $G_{S,\infty}$-module trivial et comme $\mathcal{X}_\infty$ est l'abélianisé de $G_{S,\infty}$, on a

$$H^1(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p) = Hom_{\mathbb{Z}_p}(\mathcal{X}_\infty, \mathbb{Q}_p/\mathbb{Z}_p) = \mathcal{X}_\infty^*,$$

où $\mathcal{X}_\infty^*$ est le dual de Pontryagin de $\mathcal{X}_\infty$.

Par dualité de Poitou-Tate, on a

$$(\mathcal{X}_\infty^\Gamma)^* \cong (\mathcal{X}_\infty^*)_\Gamma \cong H^1(\Gamma, H^1(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)) \text{ et } (D_F)^* \cong H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p),$$

où D_F est le noyau de Leopoldt. En dualisant la suite exacte précédente, il vient

$$0 \to (H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma)^* \to D_F \to \mathcal{X}_\infty^\Gamma \to 0.$$

Corollaire 2.3.6 *$\delta_\infty = 0$ si et seulement si $H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$.*

Preuve. On a $H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ si et seulement si $H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma = 0$. Comme D_F est $\mathbb{Z}_p$-libre, alors le module $(H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma)^*$ est $\mathbb{Z}_p$-libre et

$$rg_{\mathbb{Z}_p}(H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma)^* = rg_{\mathbb{Z}_p} D_F - rg_{\mathbb{Z}_p}\mathcal{X}_\infty^\Gamma = \delta_\infty.$$

□

Proposition 2.3.7 *La $\mathbb{Z}_p$-extension cyclotomique satisfait la conjecture faible de Leopoldt.*

Preuve. La conjecture faible de Leopoldt satisfait la descente donc on peut supposer que F contient μ_p. La p-dimension cohomologique de $G_{S,\infty}$ est 1 [Se 97]. On conclut avec le corollaire précédent, puisque $H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. □

Théorème 2.3.8 *Si F satisfait à la conjecture de Leopoldt, alors le module $\mathcal{X}_\infty$ n'a pas de sous-Λ-module fini non-nul, on a donc l'injection suivante :*

$$\mathcal{X}_\infty/\mathrm{Tor}_\Lambda \mathcal{X}_\infty \hookrightarrow \Lambda^{r_2(F)},$$

avec le conoyau fini.

Preuve. Par le théorème 2.3.5 et le corollaire 2.3.6, $H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, alors pour tout n, on a donc $H^2(G_{S,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma^{p^n}} = 0$. Par conséquent, pour tout n, $D_{F_n} \cong \mathcal{X}_\infty^{\Gamma^{p^n}}$. Soit $\mathcal{X}_\infty^o$ le sous-Λ-module fini maximal de $\mathcal{X}_\infty$. Pour n assez grand, $\mathcal{X}_\infty^o$ est invariant par Γ^{p^n}, donc s'identifie à un sous-groupe de D_{F_n}. Or, puisque D_{F_n} est sans torsion on a $\mathcal{X}_\infty^o = 0$. □

Le conoyau de l'injection ci-dessus $\mathcal{X}_\infty/\mathrm{Tor}_\Lambda \mathcal{X}_\infty \hookrightarrow \Lambda^{r_2(F)}$, est isomorphe à un certain noyau de capitulation H_F auquel on fera appel au chapitre 4.

Chapitre 3

Relations entre K-groupes et $\mathbb{Z}_p$-extensions

Dans ce chapitre d'abord nous présentons une définition du K_2 à l'aide des symboles sur un corps commutatif dans un groupe abélien. On expose ensuite le résultat de Greenberg sur la relation entre le radical de Kummer A_F du composé des premiers étages des $\mathbb{Z}_p$-extensions de F et le groupe discret $\mathcal{K} := F_\infty^* \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p)$:

$$A_F = \{a \in F^* \mid a \otimes (p^{-1} \, mod \, \mathbb{Z}_p) \in \ \mathrm{Div}(\mathcal{K}(-1)^\Gamma)\},$$

où $\Gamma := \mathrm{Gal}(F_\infty/F)$ et où $\mathrm{Div}\,\mathcal{K}(-1)$ est le sous-groupe divisible maximal de $\mathcal{K}$ tordu -1 fois à la Tate. On termine le chapitre par les relations entre K_2 et la cohomolgie galoisienne et le noyau de Tate classique

$$D_F^{(2,1)} = \{a \in F^*; \{a, \zeta_p\} = 0\},$$

qui sera généralisé au chapitre suivant.

3.1 Symboles sur un corps commutatif

3.1.1 Propriétés élémentaires des symboles

Soit F un corps commutatif et G un groupe abélien. Un *symbole* sur F dans G est une application :

$$\langle\ ,\ \rangle\ :\ F^* \times F^* \longrightarrow G$$

qui est bilinéaire et prend la valeur 1 sur tous les couples (a, b) qui vérifient $a + b = 1$; ce qui peut se résumer par les trois conditions :

$$\begin{array}{lccll} (i) & \langle aa', b\rangle & = & \langle a, b\rangle\langle a', b\rangle & , \quad \forall (a, a', b) \in F^* \times F^* \times F^*; \\ (ii) & \langle a, bb'\rangle & = & \langle a, b\rangle\langle a, b'\rangle & , \quad \forall (a, b, b') \in F^* \times F^* \times F^*; \\ (iii) & \langle a, 1-a\rangle & = & 1 & , \quad \forall a \in F^* - \{0, 1\}. \end{array}$$

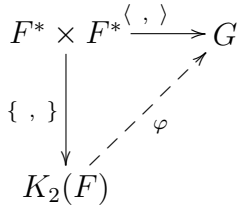
Proposition 3.1.1 *Soit F un corps commutatif, on a :*

$$\begin{array}{lccll} (iv) & \langle a, -a\rangle & = & 1 & , \quad \forall a \in F^*; \\ (v) & \langle a, a\rangle & = & \langle a, -1\rangle & , \quad \forall a \in F^*; \\ (vi) & \langle a, b\rangle\langle b, a\rangle & = & 1 & , \quad \forall (a, b) \in F^* \times F^*. \end{array}$$

La propriété (v) s'obtient à partir des égalités $\langle a, a\rangle^2 = \langle a, 1\rangle = 1$.

Le groupe $K_2(F)$ est caractérisé par la propriété universelle suivante :

Proposition 3.1.2 *Soit F un corps commutatif et G un groupe abélien. Pour chaque symbole $\langle\ ,\ \rangle$ sur F dans G, il existe un unique morphisme de groupe φ de $K_2(F)$ dans G, tel qu'on a le diagramme commutatif suivant :*



L'application canonique de $F^* \times F^*$ dans $K_2(F)$, qui au couple (x, y) associe la classe dans $K_2(F)$ du produit tensoriel $x \otimes y$, est un symbole sur F, appelé *symbole universel* sur le corps F.

3.1.2 Les homomorphismes d'extension et de transfert

Soit L/F une extension finie de corps. L'application canonique

$$i_{L/F} \ : \ K_2(F) \ \longrightarrow \ K_2(L),$$

induite par l'injection $F \hookrightarrow L$ est appelée *homomorphisme d'extension.*

Il existe également l'homomorphisme dual naturel (le transfert) qui est aux symboles ce que la norme est aux idéaux :

$$Tr_{L/F} \ : \ K_2(L) \longrightarrow K_2(F),$$

avec les propriétés suivantes :

$$Tr_{L/F} \ * \ i_{L/F} = [L : F].$$

Si l'extension L/K est galoisienne, on a :

$$i_{L/F} \ * \ Tr_{L/F} = \Sigma_{\sigma \in G(L/F)} \sigma,$$

où $\{a, b\}^\sigma = \{\sigma(a), \sigma(b)\}$ tel que $\sigma \in G(L/F)$. On a aussi :

$$Tr_{L/F}(\{a, l\}_L) = \{a, N_{L/F}(l)\}_F \quad , \quad \forall (a, l) \in F^* \times L^*.$$

Si $a \in F^*$ est une puissance n-ième dans L, disons $a = A^n$, on a

$$\{a, N_{L/F}(l)\}_F = (Tr_{L/F}\{A, l\}_L)^n,$$

où $\{a, N_{L/F}(l)\}_F$ est une puissance n-ième dans $K_2(F)$, pour tout $l \in L^*$.

De plus, si $F \subseteq L \subseteq M$, alors l'homomorphisme d'extension et le transfert ont les propriétés fonctorielles :

$$i_{M/F} = i_{M/L} * i_{L/F} \ \text{ et } \ Tr_{M/F} = Tr_{L/F} * Tr_{M/L},$$

et qu'ils sont naturellement compatibles avec l'action des automorphismes de Galois (relatifs à une clôture algébrique donnée)

$$(i_{L/F}(x_F))^\sigma = i_{\sigma(L)/\sigma(F)}(x_F^\sigma) \ \text{ et } \ (Tr_{L/F}(x_F))^\sigma = Tr_{\sigma(L)/\sigma(F)}(x_F^\sigma).$$

3.2 Les symboles classiques sur un corps de nombres

3.2.1 Les symboles modérés

Nous adoptons les notations suivantes :
$\mathfrak{p}$ une place finie de F ;
$F_\mathfrak{p}$ le complété de F en $\mathfrak{p}$;
$\mathcal{O}_\mathfrak{p} := \{x \in F_\mathfrak{p} / \ v(x) \geq 0\}$ l'anneau de valuation associé à $F_\mathfrak{p}$;
$\mathfrak{M}_\mathfrak{p} := \{x \in F_\mathfrak{p} / \ v(x) > 0\}$ l'idéal maximal de $\mathcal{O}_\mathfrak{p}$;
$k_\mathfrak{p} := \mathcal{O}_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$ le corps résiduel de $F_\mathfrak{p}$;
$\nu_\mathfrak{p}$ la valuation associée.

On définit, pour $a, b \in F^*$, l'application de $F^* \times F^*$ dans le groupe multiplicatif $k_\mathfrak{p}^*$ par :

$$[a,b]_\mathfrak{p} = (-1)^{\nu_\mathfrak{p}(a)\nu_\mathfrak{p}(b)} \frac{a^{\nu_\mathfrak{p}(b)}}{b^{\nu_\mathfrak{p}(a)}} \pmod{\mathfrak{M}_\mathfrak{p}}.$$

C'est un symbole sur F, appelé *symbole modéré* associé à la place $\mathfrak{p}$.

Pour vérifier (iii), si a et $(1-a)$ sont tous deux des $\mathfrak{p}$-unités, nous avons trivialement $[a, 1-a]_\mathfrak{p} = 1$. Sinon l'un d'eux, par exemple a, est une unité principale, et il vient encore

$$(-1)^{\nu_\mathfrak{p}(a)\nu_\mathfrak{p}(1-a)} \frac{a^{\nu_\mathfrak{p}(1-a)}}{(1-a)^{\nu_\mathfrak{p}(a)}} = a^{\nu_\mathfrak{p}(1-a)} \equiv 1 \pmod{\mathfrak{M}_\mathfrak{p}}.$$

Supposons maintenant $\mathfrak{p}$ une place à linfini. Notons $F_\mathfrak{p}$ le complété de F en $\mathfrak{p}$, puis $k_\mathfrak{p}^*$ le groupe résiduel $F_\mathfrak{p}^*/F_\mathfrak{p}^{*2}$. La valuation $\nu_\mathfrak{p}$ de F^* dans $\{0,1\}$ définie par :

$$\begin{cases} \nu_\mathfrak{p}(x) = 0, \text{ si } x \text{ est un carré dans } F_\mathfrak{p}^*, \\ \nu_\mathfrak{p}(x) = 1, \text{ sinon.} \end{cases}$$

Si $\mathfrak{p}$ est une place infinie, le symbole modéré $[a,b]_\mathfrak{p} \in k_\mathfrak{p}^* = F_\mathfrak{p}^*/F_\mathfrak{p}^{*2}$ définie comme ci-dessus. Du plus, le symbole $[\ ,\ ]_\mathfrak{p}$ est trivial lorsque $\mathfrak{p}$ est complexe et si $\mathfrak{p}$ est une place réelle, la quantité $[a,b]_\mathfrak{p}$ n'est pas 1 si et seulement si les images de a et de b dans le complété $F_\mathfrak{p}$ sont toutes deux négatives.

La condition (iii), lorsque $\mathfrak{p}$ est réelle. Si a (ou b) est positif dans $F_{\mathfrak{p}}$, alors

$$(-1)^{\nu_{\mathfrak{p}}(a)\nu_{\mathfrak{p}}(b)}\frac{a^{\nu_{\mathfrak{p}}(b)}}{b^{\nu_{\mathfrak{p}}(a)}} = a^{\nu_{\mathfrak{p}}(b)} \equiv 1 \pmod{\mathfrak{M}_{\mathfrak{p}}}.$$

Au contraire si a et b sont tous deux négatifs, il en est de même de $(-1)^{\nu_{\mathfrak{p}}(a)\nu_{\mathfrak{p}}(b)}\frac{a^{\nu_{\mathfrak{p}}(b)}}{b^{\nu_{\mathfrak{p}}(a)}}$, mais ce cas est exclu si $a+b=1$.

3.2.2 Les symboles de Hilbert

Pour chaque place non complexe $\mathfrak{p}$ de F, désignons par $F_{\mathfrak{p}}$ le complété de F en $\mathfrak{p}$, notons $m_{\mathfrak{p}}$ l'ordre du sous-groupe $\mu(F_{\mathfrak{p}})$ des racines de l'unité dans $F_{\mathfrak{p}}^*$ et considérons l'application d'Artin $w_{\mathfrak{p}}$ relative à une clôture abélienne $\bar{F}_{\mathfrak{p}}^{ab}$ de $F_{\mathfrak{p}}$.

Pour chaque place non complexe $\mathfrak{p}$ de F, l'application

$$\begin{aligned}(\ , \ )_{\mathfrak{p}} \ : \ F_{\mathfrak{p}}^* \times F_{\mathfrak{p}}^* &\longrightarrow \mu(F_{\mathfrak{p}}) \\ (a,b) &\longmapsto (a,b)_{\mathfrak{p}} = \sqrt[m_{\mathfrak{p}}]{a}^{(w_{\mathfrak{p}}(b)-1)},\end{aligned}$$

définit un symbole sur $F_{\mathfrak{p}}$, à valeurs dans le groupe $\mu(F_{\mathfrak{p}})$. Sa restriction à $F^* \times F^*$ est un symbole sur F, appelé *symbole de Hilbert* attaché à la place $\mathfrak{p}$.

Il s'agit de montrer la bilinéarité, ainsi que l'identité $(a,b)_{\mathfrak{p}} = 1$ pour $a+b=1$.

(i) La multiplicativité en a est évidente (tout comme le fait que la définition du symbole est indépendante du choix de la racine $m_{\mathfrak{p}}$-ième de a dans $\bar{F}_{\mathfrak{p}}^{ab}$).

$$(aa', b)_{\mathfrak{p}} = (a,b)_{\mathfrak{p}}(a',b)_{\mathfrak{p}}.$$

(ii) Pour établir la multiplicativité en b, remarquons que si b et b' sont dans $F_{\mathfrak{p}}^*$, nous avons la relation : $\sqrt[m_{\mathfrak{p}}]{a}^{(w_{\mathfrak{p}}(b)-1)(w_{\mathfrak{p}}(b')-1)} = 1$, puisque le groupe $Gal(\bar{F}_{\mathfrak{p}}^{ab}/F_{\mathfrak{p}})$ opère trivialement sur $\mu(F_{\mathfrak{p}})$; puis, en développant :

$$(a, bb')_{\mathfrak{p}} = (a,b)_{\mathfrak{p}}(a,b')_{\mathfrak{p}}.$$

(iii) Pour tout $a \neq \{0,1\}$ dans $F_{\mathfrak{p}}$, $(1-a) = \prod_{\zeta \in \mu(F_{\mathfrak{p}})} (1-\zeta\ \sqrt[m_{\mathfrak{p}}]{a})$ est norme dans l'extension cyclique $F_{\mathfrak{p}}(\sqrt[m_{\mathfrak{p}}]{a})/F_{\mathfrak{p}}$, donc contenu dans le noyau de la restriction à $F_{\mathfrak{p}}(\sqrt[m_{\mathfrak{p}}]{a})$ de l'application d'Artin.

$$(a, 1-a)_{\mathfrak{p}} = 1 \quad \forall a \in F_{\mathfrak{p}}^* - \{0,1\}.$$

On notera que, quand la place $\mathfrak{p}$ est complexe, le complété $F_{\mathfrak{p}}$ est algébriquement clos, et le corps de classes local ne permet de définir d'autre symbole en $\mathfrak{p}$ que le symbole trivial. Par des propriétés normiques de l'application d'Artin, on a [Ne 86] :

Proposition 3.2.1

(i) $(a,b)_{\mathfrak{p}} = 1$ *si et seulement si* b *est norme dans l'extension locale* $F_{\mathfrak{p}}(\sqrt[m_{\mathfrak{p}}]{a})/F_{\mathfrak{p}}$;

(ii) $(a,b)_{\mathfrak{p}} = (b,a)_{\mathfrak{p}}^{-1}$;

(iii) $(a,-a)_{\mathfrak{p}} = 1$ *;*

(iv) Si $(a,b)_{\mathfrak{p}} = 1$ *pour tout* $a \in F_{\mathfrak{p}}^*$, *alors* $b \in F_{\mathfrak{p}}^{*m_{\mathfrak{p}}}$;

(v) Si K/F *est une extension finie et* $\mathcal{P}$ *une place finie de* K *contenant* $\mathfrak{p}$, *alors, pour* $a \in F_{\mathfrak{p}}^*$ *et* $b \in K_{\mathcal{P}}^*$,

$$(a,b)_{\mathcal{P}} = (a, N_{K/F}(b))_{\mathfrak{p}}.$$

Théorème 3.2.2 *Les symboles de Hilbert vérifient la formule du produit :*

$$\prod_{\mathfrak{p}} (a,b)_{\mathfrak{p}}^{m_{\mathfrak{p}}/m} = 1.$$

Preuve. Deux éléments a et b de F^* étant donnés, l'extension abélienne $F(\sqrt[m]{a})/F$ est non-ramifiée en dehors d'un nombre fini de places. Comme b est norme locale en toute place non-ramifiée qui ne le divise pas, les symboles $(a,b)_{\mathfrak{p}}^{m_{\mathfrak{p}}/m}$ sont presque tous égaux à 1, et la formule du produit a bien un sens. Plus précisément, nous obtenons :

$$\prod_{\mathfrak{p}} (a,b)_{\mathfrak{p}}^{m_{\mathfrak{p}}/m} = \sqrt[m]{a}^{\sum_{\mathfrak{p}} (w_{\mathfrak{p}}(b)-1)} = \sqrt[m]{a}^{(\prod_{\mathfrak{p}} w_{\mathfrak{p}}(b)-1)} = \sqrt[m]{a}^{(w(b)-1)} = 1,$$

puisque l'application d'Artin globale w (définie sur le groupe des idèles de F) est triviale sur l'image diagonale de F^*. □

3.3 K_2 et $\mathbb{Z}_p$-extensions

Rappelons les notations :
p un nombre premier impair ;
v une place finie de F ;
F_v le complété de F en v ;
$\Gamma := \mathrm{Gal}(F_\infty/F)$;
γ_o un générateur topologique pour Γ ;
$\Lambda = \mathbb{Z}_p[[T]]$ l'algébra d'Iwasawa ;
K_o la pro-p-extension abélienne maximale de F ;
K_∞ la pro-p-extension abélienne maximale de F_∞ ;
M_∞ la pro-p-extension abélienne maximale S-ramifiée de F_∞ ;
$\mathcal{X}_\infty := \mathrm{Gal}(M_\infty/F_\infty)$ le Module d'Iwasawa standard (S-ramifiée) ;
N_∞ le sous-corps de M_∞ fixé par $\mathrm{Tor}_\Lambda(\mathcal{X}_\infty)$.

Nous avons [Wa 97] :

$$Gal(\tilde{F}/F) \cong \mathbb{Z}_p^d\ , \quad 1 + r_2 \leq d \leq [F : \mathbb{Q}],$$

La conjecteure de Leopoldt équivaut au fait que le nombre de $\mathbb{Z}_p$-extensions indépendantes de F est égal à $1 + r_2$. Ce qui est le cas lorsque F est une extension abélienne de $\mathbb{Q}$ (voir A. Brumer [Bru 67]).

Par définition A_F est le radical de Kummer du composé des premiers étages des $\mathbb{Z}_p$-extensions de F, c'est-à-dire :

$$A_F := \{a \in F^* \mid F(\sqrt[p]{a}) \subset \tilde{F}\}.$$

Il est clair que A_F est un sous-groupe de F^* contenant $(F^*)^p$ et que si $a \in A_F$ mais $\notin (F^*)^p$, alors $F(\sqrt[p]{a})$ est le premier étage d'une $\mathbb{Z}_p$-extension de F. Ainsi, on a

$$A_F/(F^*)^p \cong (\mathbb{Z}/p\mathbb{Z})^d.$$

Notons $\mathcal{K}$ le groupe discret $F_\infty^* \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p)$, sur lequel $\Gamma = \mathrm{Gal}(F_\infty/F)$ opère à travers le premier facteur et K_∞ la pro-p-extension abélienne maximale de F_∞. Par la théorie de Kummer, nous avons un accouplement parfait (voir [Iw 73, section 7]).

$$\begin{array}{ccc} \mathrm{Gal}(K_\infty/F_\infty) \times \mathcal{K} & \longrightarrow & \mu_{p^\infty} \\ (\sigma, a \otimes (p^{-n} \mathrm{mod}\ \mathbb{Z}_p)) & \longmapsto & \sigma(\sqrt[p^n]{a})/\sqrt[p^n]{a}, \end{array} \tag{3.1}$$

où n est un entier positif et $\sqrt[p^n]{a}$ est une racine p^n-ième de a dans K_∞ (c'est-à-dire $F_\infty(\sqrt[p^n]{a}) \subset K_\infty$).

Si N_∞ est un corps tel que $F_\infty \subseteq N_\infty \subseteq K_\infty$, alors le sous-groupe de $\mathcal{K}$ correspondant à N_∞ est

$$\begin{aligned}\mathrm{Gal}(K_\infty/N_\infty)^\perp &= \{\alpha \in \mathcal{K} \mid \alpha = a \otimes (p^{-n} \ mod \ \mathbb{Z}_p),\ F_\infty(\sqrt[p^n]{a}) \subseteq N_\infty\},\\ &= \{\alpha \in \mathcal{K} \mid (\sigma, \alpha) = 1 \text{ pour tout } \sigma \in \mathrm{Gal}(K_\infty/N_\infty)\},\\ &= \{\alpha = a \otimes (p^{-n} \ mod \ \mathbb{Z}_p) \in \mathcal{K} \mid \sigma(\sqrt[p^n]{a}) = \sqrt[p^n]{a}\}.\end{aligned}$$

Si $\gamma \in \Gamma$, alors γ agit naturellement sur $\mathcal{K}$ et μ_{p^∞} :

$$\gamma((\sigma, \alpha)) = (\gamma(\sigma), \gamma(\alpha)),$$

pour tout $\sigma \in \mathrm{Gal}(K_\infty/F_\infty),\ \alpha \in \mathcal{K}$.

$\gamma \in \Gamma$ agit aussi sur le groupe abélien $\mathrm{Gal}(K_\infty/F_\infty)$. Soit $\tilde{\gamma} \in \mathrm{Gal}(K_\infty/F)$ un relèvement de γ, alors pour tout n

$$\begin{aligned}(\sigma^\gamma, (a \otimes (p^{-1} \ mod \ \mathbb{Z}_p))^\gamma) &= (\tilde{\gamma}\sigma\tilde{\gamma}^{-1})(\sqrt[p^n]{a}^\gamma)/\sqrt[p^n]{a}^\gamma\\ &= (\tilde{\gamma}\sigma\tilde{\gamma}^{-1}\tilde{\gamma})(\sqrt[p^n]{a})/\tilde{\gamma}(\sqrt[p^n]{a})\\ &= \tilde{\gamma}(\sigma(\sqrt[p^n]{a})/\sqrt[p^n]{a})\\ &= (\sigma, a)^\gamma.\end{aligned}$$

Donc $(\ ,\ )$ est un accouplement de Γ-modules.

Soit K_o la pro-p-extension abélienne maximale de F et soit γ_o un générateur topologique pour Γ, alors :

$$\mathrm{Gal}(K/K_o) = (\gamma_o - 1)\mathrm{Gal}(K/F_\infty).$$

Soit $\gamma_o(\zeta) = \zeta^{\kappa_o}$ pour tout $\zeta \in \mu_{p^\infty}$, où κ_o est l'unité p-adique donnant l'action de γ sur μ_{p^∞}. Alors le sous-groupe de $\mathcal{K}$ correspondant à K_o est

$$\mathrm{Gal}(K/K_o)^\perp = \{\alpha \in \mathcal{K} \mid \gamma_0(\alpha) = \alpha^{\kappa_o}\}. \tag{3.2}$$

Maintenant $F_\infty \subseteq \tilde{F} \subseteq K_0$ et $\mathrm{Gal}(\tilde{F}/F_\infty) \cong \mathbb{Z}_p^{d-1}$. Puisque $\mathbb{Q}_p/\mathbb{Z}_p$ est le dual de Pontryagin de $\mathbb{Z}_p$, alors $\tilde{F}$ correspond au sous-groupe de

$$\{\alpha \in \mathcal{K} \mid \gamma_0(\alpha) = \alpha^{\kappa_o}\}$$

qui est isomorphe à $(\mathbb{Q}_p/\mathbb{Z}_p)^{d-1}$. Donc, il est clair qu'un sous-groupe de (3.2) qui est isomorphe à $\mathbb{Q}_p/\mathbb{Z}_p$, doit correspondre à un sous-groupe de $\tilde{F}$. On a donc le sous-groupe de $\mathcal{K}$ correspondant à $\tilde{F}$ est le sous-groupe divisible maximal de (3.2). On a

$$\begin{aligned} A_F &= \{a \in F^* \mid \sqrt[p]{a} \in \tilde{F}\} \\ &= \{a \in F^* \mid g(\sqrt[p]{a}) = \sqrt[p]{a} \text{ pour tout } g \in \mathrm{Gal}(K/\tilde{F})\} \\ &= \{a \in F^* \mid (g,\ a \otimes p^{-1}\ mod\ \mathbb{Z}_p) = 1 \text{ pour tout } g \in \mathrm{Gal}(K/\tilde{F})\} \\ &= \{a \in F^* \mid a \otimes p^{-1}\ mod\ \mathbb{Z}_p\ \in \text{ sous} - \text{groupe correspondant à } \tilde{F}\}. \end{aligned}$$

Ainsi

$$A_F = \{a \in F^* \mid a \otimes (p^{-1}\ mod\ \mathbb{Z}_p) \in \mathrm{Div}\{\alpha \in \mathcal{K} \mid \gamma_0(\alpha) = \alpha^{\kappa_o}\}\},$$

où Div est le sous-groupe divisible maximal.

Soit M_∞ la pro-p-extension abélienne maximale de F_∞ non ramifiée en dehors de S. Alors $\mathcal{X}_\infty = \mathrm{Gal}(M_\infty/F_\infty)$ est un module sur l'algèbre $\Lambda = \mathbb{Z}_p[[T]]$, où $T = \gamma_o - 1$.

Soit N_∞ le sous-corps de M_∞ fixé par $\mathrm{Tor}_\Lambda(\mathcal{X}_\infty)$, donc $X := \mathrm{Gal}(N_\infty/F_\infty) = \mathrm{Fr}_\Lambda\mathcal{X}_\infty$(voir [Gr 76]) et aussi X est un sous-module d'indice fini de Λ^{r_2} et le module quotient $H_F := \Lambda^{r_2}/X$ est isomorphe (en tant que groupe abélien) au noyau de l'homomorphisme naturel $K_2F_n \longrightarrow K_2F_\infty$, pour n assez grand [Co 72].

Puisque F_∞ contient toutes les racines p-primaires de l'unité, le groupe de Galois Γ opère sur μ_{p^∞}. Si $\gamma \in \Gamma$, par définition du caractère cyclotomique, $\kappa(\gamma)$ est donné par l'équation :

$$\gamma(\zeta) = \zeta^{\kappa(\gamma)},$$

pour tout $\zeta \in \mu_{p^\infty}$. Donc nous avons un homomorphisme $\kappa : \Gamma \longrightarrow \mathbb{Z}_p^*$. Si $\mathcal{U}$ est un Γ-module et aussi un $\mathbb{Z}_p$-module, alors pour tout $i \geq 1$ nous considèrons un nouveau Γ-module $\mathcal{U}(i)$ avec une nouvelle action de Γ :

$$\gamma.u = \kappa(\gamma)^i\gamma(u),$$

pour tout $\gamma \in \Gamma$, $u \in \mathcal{U}(i)$, où $\gamma(u)$ est l'action de Γ sur $\mathcal{U}$. C'est le module tordu à la Tate introduit au 1.5. On a alors le corollaire suivant :

Corollaire 3.3.1 $A_F = \{a \in F^* \mid a \otimes (p^{-1} \, mod \, \mathbb{Z}_p) \in \text{ Div}(\mathcal{K}(-1)^\Gamma)\}$.

Preuve. Par définition, on a $\mathcal{K}(-1)^\Gamma = \{\alpha \in \mathcal{K}(-1) \mid \gamma_o.\alpha = \alpha \ , \ \forall \alpha \in \Gamma\}$, alors

$$\begin{aligned}\mathcal{K}(-1)^\Gamma &= \{\alpha \in \mathcal{K}(-1) \mid \kappa(\gamma_o)^{-1}.\gamma_o(\alpha) = \alpha \ , \ \forall \alpha \in \Gamma\} \\ &= \{\alpha \in \mathcal{K} \mid \gamma_o(\alpha) = \alpha^{\kappa_o} \ , \ \forall \alpha \in \Gamma\}.\end{aligned}$$

□

Maintenant, le corps F_∞ contient μ_{p^∞}, on peut tordre (3.1) pour obtenir un accouplement parfait :

$$\text{Gal}(K_\infty/F_\infty)(i) \times \mathcal{K}(1-i) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

avec la propriété

$$(\gamma.\sigma, \alpha) = (\sigma, \gamma^{-1}.\alpha),$$

pour tout $i \in \mathbb{Z}$, $\sigma \in \text{Gal}(K_\infty/F_\infty)(i)$ et $\gamma \in \Gamma$.

Notons $\mathcal{N}$ le sous-groupe de $\mathcal{K}$ correspondant au N_∞. Nous pouvons voir du paragraphe précédent que pour chaque nombre entier i nous avons un accouplement parfait

$$X(i) \times \mathcal{N}(1-i) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

$$X(i)_\Gamma \times \mathcal{N}(1-i)^\Gamma \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

où $\mathcal{N}(1-i)^\Gamma$ est le dual de Pontryagin de $X(i)_\Gamma = X(i)/TX(i)$. Puisque $X(i)$ est isomorphe à un sous-module d'indice fini de Λ^{r_2}, alors $X(i)_\Gamma$ est isomorphe à $\mathbb{Z}_p^{r_2} \times$(groupe fini). Donc, pour tout $i \neq 0$, le sous-groupe divisible maximale de $\mathcal{N}(i)^\Gamma$ est isomorphe à $(\mathbb{Q}_p/\mathbb{Z}_p)^{r_2}$. Pour tout i, on conjecture que le sous-groupe divisible maximale de $\mathcal{K}(i)^\Gamma$ est isomorphisme à $(\mathbb{Q}_p/\mathbb{Z}_p)^{r_2}$, c'est-à-dire

$$\text{Div}\, \mathcal{N}(i)^\Gamma \cong \text{Div}\, \mathcal{K}(i)^\Gamma.$$

3.4 Relations entre les K-groupes et la Cohomologie galoisienne

Les premières relations entre les K-groupes et la cohomologie galoisienne ont été données par Tate [Ta 76]. Il a montré l'existence d'un isomorphisme, pour un corps global F, entre K_2F et le quotient du groupe de cohomologie galoisienne $H^1(F, (\mathbb{Q}/\mathbb{Z})(2))$ par son sous-groupe divisible maximal.

Nous rappelons les notations suivantes :
p un nombre premier impair ;
F_S une clôture algébrique séparable de F ;
μ_{p^n} le groupe de racine p^n-ième de l'unité dans F_S ;
$\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$;
$E = F(\mu_{p^n})$;
$G = \mathrm{Gal}(E/F)$.

Puisque les flèches $\mu_{p^{i+1}} \longrightarrow \mu_{p^i}$ sont surjectives, la limite projective de cette suite exacte de systèmes inverses donne une suite exacte

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \varprojlim F_s^* \longrightarrow F_s^* \longrightarrow 0.$$

Puisque F_S^* est discret, on a un homomorphisme

$$d_F : F^* = H^0(F, F_S^*) \longrightarrow H^1(F, \mathbb{Z}_p(1)).$$

Théorème 3.4.1 *Nous avons un unique homomorphisme*

$$h : K_2F \longrightarrow H^2(F, \mathbb{Z}_p(2))$$

$$\{a, b\} \longmapsto h(\{a, b\}) = d_F a \cup d_F b,$$

pour tous les éléments $a, b \in F^*$.

Soit $n = 1$, c'est-à-dire $E = F(\mu_p)$, Nous avons le diagramme suivant :

$$\begin{array}{ccccccccc}
(\mu_p \otimes E^*)^G & \xrightarrow{\gamma} & K_2F & \xrightarrow{p} & K_2F & \to & K_2F/pK_2F & \to & 0 \\
id \downarrow & & h \downarrow & & h \downarrow & & \mathrm{h}_1 \downarrow & & \\
H^1(F, \mathbb{Z}/p\mathbb{Z}(2)) & \xrightarrow{\delta} & H^2(F, \mathbb{Z}_p(2)) & \xrightarrow{p} & H^2(F, \mathbb{Z}_p(2)) & \to & H^2(F, \mathbb{Z}/p\mathbb{Z}(2)) & &
\end{array}$$

La ligne inférieure est obtenue en prenant la suite exacte longue de cohomologie à partir de la suite courte exacte

$$0 \to \mathbb{Z}_p(2) \xrightarrow{p} \mathbb{Z}_p(2) \to \mathbb{Z}/p\mathbb{Z}(2) \to 0.$$

Nous définissons l'homomorphisme γ et l'isomorphisme id dans le cas $E = F$, c'est-à-dire, le groupe des racines p^n-ièmes de l'unité sont dans F. Dans ce cas, γ est l'homomorphisme défini par

$$\gamma(\zeta_p \otimes a) = \{\zeta_p, a\}$$

où ζ_p est une racine primitive p-ième de 1 et $a \in F^*$, et aussi id est défini par

$$id(\zeta_p \otimes a) = \zeta_p \cup d_1 a,$$

où $d_1 : F^* \longrightarrow H^1(F, \mu_p)$ est l'homomorphisme de liaison obtenu à partir de la suite exacte

$$0 \longrightarrow \mu_{p^n} \longrightarrow F_S^* \xrightarrow{p^n} F_S^* \longrightarrow 0,$$

en passant à la cohomologie.

Supposons que G est cyclique d'ordre p^n et que F contient le groupe μ_{p^n} des racines p^n-ièmes de l'unité. Alors, on a la suite exacte

$$0 \longrightarrow H^0(F, \mu_{p^n}) \longrightarrow H^0(F, F_S^*) \xrightarrow{p^n} H^0(F, F_S^*) \xrightarrow{d_1} H^1(F, \mu_{p^n}) \longrightarrow H^1(F, F_S^*).$$

Par le Théorème 90 de Hilbert $H^1(F, F_S^*) = 0$, on a donc

$$H^1(F, \mu_{p^n}) \cong F^*/F^{*p^n} \cong F^* \otimes \mathbb{Z}/p^n\mathbb{Z}$$

Pour chaque entier $i \geq 2$, la suite exacte

$$0 \to \mathbb{Z}_p(i) \xrightarrow{p^n} \mathbb{Z}_p(i) \to \mathbb{Z}/p^n\mathbb{Z}(i) \to 0,$$

induit par cohomologie une injection :

$$K_{2i-1}^{\text{ét}} F/p^n \cong H^1(F, \mathbb{Z}_p(i))/p^n \hookrightarrow H^1(F, \mathbb{Z}/p^n\mathbb{Z}(i)) = H^1(F, \mu_{p^n})(i-1).$$

Il existe donc un sous-module $D_F^{(i,n)}$ de F^* contenant F^{*p^n}, tel que

$$K_{2i-1}^{\text{ét}} F/p^n \cong (D_F^{(i,n)}/F^{*p^n})(i-1).$$

Pour le cas classique $i = 2$ et $n = 1$, la suite exacte

$$0 \to \mathbb{Z}_p(2) \xrightarrow{p} \mathbb{Z}_p(2) \to \mathbb{Z}/p\mathbb{Z}(2) \to 0,$$

donne par cohomologie

$$0 \to D_F^{(2,1)}/F^{*p}(1) = H^1(F, \mathbb{Z}_p(2))/p \to H^1(F, \mathbb{Z}/p\mathbb{Z}(2)) \to_p H^2(F, \mathbb{Z}_p(2)) \to 0,$$

et donc un diagramme commutatif (Théorème 3.4.1)

$$\begin{array}{ccccccc} 0 & \to & D_F^{(2,1)}/F^{*p}(1) & \to & H^1(F, \mathbb{Z}/p\mathbb{Z}(2)) & \to & {}_pH^2(F, \mathbb{Z}_p(2)) \\ & & & & \downarrow \wr & & \downarrow \wr \\ & & & & F^*/F^{*p} \otimes \mu_p & \to & {}_pK_2(F) \\ & & & & a \otimes \zeta_p & \longmapsto & \{a, \zeta_p\}. \end{array}$$

donc :

$$D_F^{(2,1)} = \{a \in F^* ;\ \{a, \zeta_p\} = 0\},$$

est le noyau de Tate classique tel qu'il a été difini dans [Ta 76].

Théorème 3.4.2 ([Ta 76] Théorème (6.3)) *Soit $\epsilon = 1$ si $[F(\mu_p) : F] \leq 2$, et soit $\epsilon = 0$ sinon. Alors* $\ker(\gamma)$ *est un groupe abélien élémentaire d'ordre $p^{r_2+\epsilon}$. En particulier, si le corps de nombres F contient μ_p, alors*

$$[D_F^{(2,1)} : F^{*p}] = p^{r_2+1}.$$

Chapitre 4

Bornes Pour La Capitulation des groupes de K-théorie étale

Dans ce chapitre, nous obtenons les résultats nouveaux de la thèse en généralisant les minorations obtenues dans [As-Mo 04] aux cas des extensions cycliques de degré une puissance quelconque de p dès lors qu'il y a "suffisamment" de racines p-primaires de l'unité contenues dans le corps de base F.

4.1 Noyaux de Tate et $\mathbb{Z}_p$-extensions

Soit $\mu_{p^\infty} := \cup_{n\geq 1}\mu_{p^n}$ le groupe de toutes les racines p-primaires de l'unité et $F_\infty := F(\mu_{p^\infty})$ la $\mathbb{Z}_p$-extension cyclotomique de F. Sopposons $F_n = F(\mu_{p^n})$ et $\Gamma = \mathrm{Gal}(F_\infty/F)$.

Soit $\mathcal{K} := F_\infty^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ et K_∞ la pro-p-extension abélienne maximale de F_∞. Par la théorie de Kummer, nous avons un accouplement parfait (voir [Iw 73, section 7]).

$$\begin{array}{ccc} \mathrm{Gal}(K_\infty/F_\infty) \times \mathcal{K} & \longrightarrow & \mu_{p^\infty} \\ (\sigma, a \otimes (p^{-n} \bmod \mathbb{Z}_p)) & \longmapsto & \sigma(\sqrt[p^n]{a})/\sqrt[p^n]{a}, \end{array} \tag{4.1}$$

où $\sqrt[p^n]{a}$ est la racine p^n-ième de a dans K_∞.

Puisque F_∞ contient toutes les racines p-primaires de l'unité, le groupe de Galois Γ opère sur μ_{p^∞}.

Soit $\tilde{F}$ le composé des $\mathbb{Z}_p$-extensions de F et $\mu_{p^n} \subset F$. Soit $A_F^{(n)}$ le radical de Kummer du composé des n-ièmes étages des $\mathbb{Z}_p$-extensions de F, i.e. :

$$A_F^{(n)} := \{a \in F^* \mid F(\sqrt[p^n]{a}) \subset \tilde{F}\}.$$

Nous avons $F^{*p^n} \subseteq A_F^{(n)} \subseteq F^*$ et le lemme suivant donne une description de $A_F^{(n)}$:

Soit $\gamma_o(\zeta) = \zeta^{\kappa_o}$ pour tout $\zeta \in \mu_{p^\infty}$, où κ_o est l'unité p-adique donnant l'action γ_0 sur μ_{p^∞}

Lemme 4.1.1 *Soit $\mathcal{K}$ le groupe discret $F_\infty^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Alors*

$$A_F^{(n)} = \{a \in F^* \mid a \otimes (p^{-n} \ mod \ \mathbb{Z}_p) \in \ {}_{p^n}\mathrm{Div}(\mathcal{K}(-1)^\Gamma)\}.$$

Preuve. On se fixe dorénavant un générateur topologique γ_0 de Γ. Alors par le section 3.3, le sous-groupe de $\mathcal{K}$ correspondant à $\tilde{F}$, c'est-à-dire

$$\{\alpha = a \otimes (p^{-n} \ mod \ \mathbb{Z}_p) \in \mathcal{K} \mid F_\infty(\sqrt[p^n]{a}) \subseteq \tilde{F}\},$$

est le sous-groupe divisible maximal de $\{\alpha \in \mathcal{K} \mid \gamma_0(\alpha) = \alpha^{\kappa_o}\}$.

ou de façon équivalente :

$$\{\alpha \in \mathcal{K} \mid (g, \alpha) = 1 \text{ pour tout } g \in \mathrm{Gal}(K_\infty/\tilde{F})\}.$$

Soit $a \in A_F^{(n)}$, alors $\sqrt[p^n]{a} \in \tilde{F}$. Pour tout $g \in \mathrm{Gal}(K_\infty/\tilde{F})$, nous avons $g(\sqrt[p^n]{a}) = \sqrt[p^n]{a}$, soit $(g, a \otimes (p^{-n} \ mod \ \mathbb{Z}_p)) = 1$ pour tout $g \in \mathrm{Gal}(K_\infty/\tilde{F})$, *i.e.*

$$A_F^{(n)} = \{a \in F^* \mid (g, a \otimes (p^{-n} \ mod \ \mathbb{Z}_p)) = 1 \text{ pour tout } g \in \mathrm{Gal}(K_\infty/\tilde{F})\}.$$

Soit

$$A_F^{(n)} = \{a \in F^* \mid a \otimes (p^{-n} \ mod \ \mathbb{Z}_p) \in \mathcal{K} \ , \ F(\sqrt[p^n]{a}) \subseteq F_\infty(\sqrt[p^n]{a}) \subseteq \tilde{F}\}.$$

Finalement, nous avons

$$A_F^{(n)} = \{a \in F^* \mid a \otimes (p^{-n} \; mod \; \mathbb{Z}_p) \in \mathrm{Div}\,\{\alpha \in \mathcal{K} \mid \gamma_0(\alpha) = \alpha^{\kappa_o}\}\}.$$

□

Supposons que G est cyclique d'ordre p^n et F contient le groupe μ_{p^n} des racines p^n-ièmes de l'unité. Alors, on sait que [As-Mo 04]

$$\mathrm{coker}(f_i) \cong (K^{\text{ét}}_{2i-1}F/p^n)/N_{E/F}(K^{\text{ét}}_{2i-1}E/p^n) \text{ et } |\mathrm{coker(f_i)}| = |\ker(\mathrm{f_i})|.$$

Soit E/F une extension cyclique de corps de nombres, contenant μ_{p^n}, de degré p^n. Alors,

$$K^{\text{ét}}_{2i-1}F/p^n \hookrightarrow F^*/F^{*p^n}(i-1),$$

où la notation $M(i)$ pour un G_F-module M est le i-ième tordu à la Tate.

En effet, la suite exacte

$$0 \longrightarrow \mu_{p^n} \longrightarrow F^* \xrightarrow{p^n} F^* \longrightarrow H^1(F, \mu_{p^n}) \longrightarrow 0$$

donne

$$H^1(F, \mu_{p^n}) \cong F^*/F^{*p^n} \cong F^* \otimes \mathbb{Z}/p^n\mathbb{Z}.$$

Pour chaque entier $i \geq 2$, la suite exacte

$$0 \to \mathbb{Z}_p(i) \xrightarrow{p^n} \mathbb{Z}_p(i) \to \mathbb{Z}/p^n\mathbb{Z}(i) \to 0,$$

donne :

$$K^{\text{ét}}_{2i-1}F/p^n \cong H^1(F, \mathbb{Z}_p(i))/p^n \hookrightarrow H^1(F, \mathbb{Z}/p^n\mathbb{Z}(i)) = H^1(F, \mu_{p^n})(i-1).$$

Ce qui conduit à la définition suivante :

Définition 4.1.2 *Il existe un sous-module $D_F^{(i,n)}$ de F^* contenant F^{*p^n}, tel que*

$$K^{\acute{e}t}_{2i-1}F/p^n \cong (D_F^{(i,n)}/F^{*p^n})(i-1).$$

Pour chaque entier $i \geq 2$, on a [As-Mo 04]

$$\begin{aligned}\mathcal{K}(i-1)^{\Gamma}/\mathrm{Div} &\cong H^1(F, \mathbb{Q}_p/\mathbb{Z}_p(i))/\mathrm{Div} \\ &\cong \mathrm{Tor}_{\mathbb{Z}_p}(H^2(F, \mathbb{Z}_p(i))).\end{aligned}$$

Donc, on a le diagramme commutatif

$$\begin{array}{ccccc} 0 \to K_{2i-1}^{\acute{e}t}F/p^n & \to & H^1(F, \mathbb{Z}/p^n\mathbb{Z}(i)) & \to & H^2(F, \mathbb{Z}_p(i)) \\ & & \wr\downarrow & & \wr\downarrow \\ & & F^* \otimes \mathbb{Z}/p^n\mathbb{Z}(i-1)) & \to & (F_\infty^* \otimes \mathbb{Q}_p/\mathbb{Z}_p(i-1))^{\Gamma}/\mathrm{Div}, \end{array}$$

dans lequel la suite du haut est exacte. Par définition de $D_F^{(i,n)}$, le groupe quotient $D_F^{(i,n)}/F^{*p^n}$ est le noyau de l'homomorphisme du bas. Par conséquent, pour $i \geq 2$,

$$D_F^{(i,n)} = \{a \in F^* \mid a \otimes (p^{-n} \; mod \; \mathbb{Z}_p) \in \; {}_{p^n}\mathrm{Div}(\mathcal{K}(\mathrm{i}-1)^{\Gamma})\}.$$

Soit M_∞ la pro-p-extension abélienne maximale de F_∞ non ramifiée en dehors de S, et soit $\mathcal{M}$ le sous-groupe de $\mathcal{K}$ correspondant au corps M_∞ par l'accouplement d'Iwasawa ci-dessus. Nous avons un accouplement non dégénéré :

$$\mathcal{X}_\infty \times \mathcal{M} \longrightarrow \mu_{p^\infty}, \tag{4.2}$$

où $\mathcal{X}_\infty = \mathrm{Gal}(\mathrm{M}_\infty/\mathrm{F}_\infty)$.

Soit N_∞ le sous-corps de M_∞ fixé par $\mathrm{Tor}_\Lambda(\mathcal{X}_\infty)$ et soit $\mathcal{N}$ le sous-groupe de $\mathcal{M}$ correspondant au corps N_∞. Notons $X := \mathrm{Fr}_\Lambda\mathcal{X}_\infty = \mathrm{Gal}(N_\infty/F_\infty)$. Pour tout nombre entier i, nous avous donc un accouplement parfait :

$$X(-i) \times \mathcal{N}(i-1) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p,$$

$$X(-i)_\Gamma \times \mathcal{N}(i-1)^{\Gamma} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p,$$

Où $\mathcal{N}(i-1)^{\Gamma}$ est le dual de Pontryagin de $X(-i)_\Gamma = X(-i)/TX(-i)$. Nous avous donc un accouplement parfait :

$$\mathrm{Fr}_{\mathbb{Z}_p}(X(-i)_\Gamma)/p^n \; \times \; {}_{p^n}\mathrm{Div}(\mathcal{N}(i-1)^{\Gamma}) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

Il est bien connu que X est un sous-module d'indice fini de Λ^{r_2}. Le module quotient $H_F := \Lambda^{r_2}/X$ est isomorphe (en tant que groupe abélien) au noyau de l'homomorphisme naturel $K_2F_n \longrightarrow K_2F_\infty$, pour n assez grand [Co 72].

Lemme 4.1.3 *On a*

$$\mathrm{Fr}_{\mathbb{Z}_p}(X(i)_\Gamma)/p^n \cong X(i)/(X(i) \cap T(\Lambda^{r_2}(i)) + p^n X(i))$$

pour tout $i \in \mathbb{Z}$.

Preuve. Puisque $\Lambda^{r_2}(i)/T(\Lambda^{r_2}(i)) \cong (\Lambda/T\Lambda)^{r_2} \cong \mathbb{Z}_p^{r_2}$. Alors, $\Lambda^{r_2}(i)_\Gamma$ est $\mathbb{Z}_p$-libre. La suite exacte :

$$0 \longrightarrow X \longrightarrow \Lambda^{r_2} \longrightarrow H_F \longrightarrow 0$$

donne alors la suite exacte :

$$0 \longrightarrow \ker(H_F(i) \xrightarrow{T} H_F(i)) \xrightarrow{f} X(i)_\Gamma \xrightarrow{g} \Lambda^{r_2}(i)_\Gamma = \Lambda^{r_2}(i)/T(\Lambda^{r_2}(i)).$$

On a donc

$$\mathrm{Ker}(g) = \mathrm{Im}(f) = X(i) \cap T(\Lambda^{r_2}(i))/TX(i).$$

Puisque $\Lambda^{r_2}(i)_\Gamma$ est un $\mathbb{Z}_p$-module libre, $\mathrm{Tor}_{\mathbb{Z}_p}(X(i)_\Gamma)$ est le noyau de l'homomorphisme naturel $X(i)_\Gamma \xrightarrow{g} \Lambda^{r_2}(i)_\Gamma$.

Ainsi

$$\mathrm{Fr}_{\mathbb{Z}_p}(X(i)_\Gamma) := \frac{X(i)_\Gamma}{\mathrm{Tor}_{\mathbb{Z}_p}(X(i)_\Gamma)} \cong X(i)/(X(i) \cap T(\Lambda^{r_2}(i))).$$

Donc

$$\mathrm{Fr}_{\mathbb{Z}_p}(X(i)_\Gamma)/p^n \cong X(i)/(X(i) \cap T(\Lambda^{r_2}(i)) + p^n X(i)).$$

□

On suppose désormais que $\mu_p \subset F$. Soit $r \in \mathbb{Z}$ et $r \geq 0$. Le lemme suivant montre que ces modules sont indépendants du twist lorsque $j \equiv i \pmod{\mathrm{p^r}}$ pour des entiers r convenables :

Lemme 4.1.4 *Soit E/F une extension cyclique de corps de nombres de degré p^n et p^e l'exposant du groupe fini H_F. Soit $j \equiv i \pmod{\mathrm{p^r}}$ pour un entier $r \leq n + e$. Si $\mu_{p^{n+e-r}} \subset F$, alors*

$$X(i) \cap T(\Lambda^{r_2}(i)) + p^n X(i) \cong (X(j) \cap T(\Lambda^{r_2}(j)) + p^n X(j))(i - j).$$

Preuve. Soit $Y_i := X(i) \cap T(\Lambda^{r_2}(i)) + p^n X(i)$. On doit montrer que

$$Y_i = Y_j \text{ lorsque } j \equiv i \pmod{p^r}.$$

Puisque

$$X(j)/Y_j \cong \mathrm{Fr}_{\mathbb{Z}_p}(X(j)_\Gamma)/p^n \cong (\mathbb{Z}/p^n\mathbb{Z})^{r_2}.$$

Alors $X(j)/Y_j$ est d'exposant p^n. Donc l'exposant de $\Lambda^{r_2}(j)/Y_j$ est inférieur ou égal à p^{e+n} :

$$p^{e+n}\Lambda^{r_2}(j) \subset Y_j.$$

Un élément $y \in Y_i$ s'écrit $y = T^{(i)}\lambda + p^n x$, avec $\lambda \in \Lambda^{r_2}$ et $x \in X$. Ici $T^{(i)}$ est l'action de T sur $\Lambda^{r_2}(i)$, avec $\lambda \in \Lambda^{r_2}$, $T^{(i)}\lambda \in X$ et $x \in X$. On se fixe dorénavant un générateur topologique γ_0 de Γ. Par hypothèse, $\kappa(\gamma_o) \equiv 1 \pmod{p^{n+e-r}}$, comme de plus p^r divise $i - j$, alors

$$\kappa(\gamma_o)^{i-j} \equiv 1 \pmod{p^{n+e}}.$$

Ainsi

$$\gamma_0{}^{(i)}\lambda = \kappa(\gamma_0)^{i-j}\gamma_0{}^{(j)}\lambda = \gamma_0{}^{(j)}\lambda + (\kappa(\gamma_0)^{i-j} - 1)\gamma_0{}^{(j)}\lambda = \gamma_0{}^{(j)}\lambda + y_1$$

où $\gamma_0{}^{(i)}\lambda$ est l'action de T sur $\Lambda^{r_2}(i)$. Alors $T^{(i)}\lambda = T^{(j)}\lambda + y_1$ et $y = T^{(j)}\lambda + p^n x + y_1$, où $y_1 \in p^{n+e}\Lambda^{r_2}(j) \subset Y_j$. Puisque les éléments y, y_1 et $p^n x$ sont dans X, d'élément $T^{(j)}\lambda$ de $T(\Lambda^{r_2}(j))$ est ainsi dans X. Donc $y \in Y_j$. $\square$

D'après les lemmes 4.1.3 et 4.1.4, on obtient :

Proposition 4.1.5 *Soit E/F une extension cyclique de corps de nombres de degré p^n et p^e l'exposant du groupe fini H_F. Soit $j \equiv i \pmod{\mathrm{p^r}}$ pour un entier $r \leq n + e$ si $\mu_{p^{n+e-r}} \subset F$, alors*

$$\mathrm{Fr}_{\mathbb{Z}_p}(X(i)_\Gamma)/p^n \cong (\mathrm{Fr}_{\mathbb{Z}_p}(X(j)_\Gamma)/p^n)(i - j).$$

On conjecture que $\mathrm{Div}\mathcal{K}(i-1)^\Gamma = \mathrm{Div}\mathcal{N}(i-1)^\Gamma$, pour tout entier $i \neq 1$ (Greenberg, Schneider,...). Pour tout nombre entier $i \geq 2$, Soulé a montré dans [So 79] que $\mathrm{Div}\,\mathcal{K}(i-1)^\Gamma = \mathrm{Div}\,\mathcal{N}(i-1)^\Gamma$. L'egalité $\mathrm{Div}\,\mathcal{K}(-1)^\Gamma = \mathrm{Div}\,\mathcal{N}(-1)^\Gamma$ est équivalente à la conjecture de Leopoldt pour F au nombre

premier p. Dans la suite, on suppose que ces conjectures sont vérifiées, ce qui est le cas pour $i \geq 2$.

Donc $A_F^{(n)} = D_F^{(0,n)}$ et $D_F^{(i,1)} = D_F^{(i)}$, comme dans [As-Mo 04]. Nous allons comparer les noyaux de Tate $D_F^{(i,n)}$ pour $i \neq 1$, au radical de Kummer :

$$A_F^{(n)} := \{a \in F^* \mid F(\sqrt[p^n]{a}) \subset \tilde{F}\},$$

où $\tilde{F}$ est le composé des $\mathbb{Z}_p$-extensions de F.

Puisque ${}_{p^n}\mathrm{Div}(\mathcal{N}(i-1)^\Gamma)$ est le dual de $\mathrm{Fr}_{\mathbb{Z}_p}(X(-i)_\Gamma)/p^n$. On en déduit les Corollaires suivants :

Corollaire 4.1.6 *Supposons E/F une extension cyclique de corps de nombres de degré p^n et p^e l'exposant du groupe fini H_F. Soient $i, j \geq 2$, $j \equiv i \pmod{p^r}$ pour un entier $r \leq n+e$. Si $\mu_{p^{n+e-r}} \subset F$, alors*

$$D_F^{(i,n)} = D_F^{(j,n)}(i-j).$$

Supposons E/F une extension cyclique de corps de nombres de degré p^n et F vérifiant la conjecture de Leopoldt au nombre premier p. Soit p^e l'exposant de H_F. Prenons $i \geq 2$ et soit $r \leq n+e$ un entier tel que p^r divise i. Prenons $j = 0$. Si $\mu_{p^{n+e-r}} \subset F$. Par le Proposition 4.1.5 on a

$$\begin{array}{ccc} \mathrm{Hom}(\mathrm{Fr}_{\mathbb{Z}_p}(X(-i)_\Gamma)/p^n, \mathbb{Q}_p/\mathbb{Z}_p) & = & \mathrm{Hom}((\mathrm{Fr}_{\mathbb{Z}_p}(X(0)_\Gamma)/p^n)(-i), \mathbb{Q}_p/\mathbb{Z}_p) \\ \wr\downarrow & & \wr\downarrow \\ {}_{p^n}\mathrm{Div}(\mathcal{N}(i-1)^\Gamma) & & {}_{p^n}\mathrm{Div}(\mathcal{N}(-1)^\Gamma)(i) \\ \| i \geq 2 & & \| \text{Leopoldt} \\ {}_{p^n}\mathrm{Div}(\mathcal{K}(i-1)^\Gamma) & & {}_{p^n}\mathrm{Div}(\mathcal{K}(-1)^\Gamma)(i) \end{array}$$

Nous obtenons le corollaire suivant :

Corollaire 4.1.7 *Supposons E/F une extension cyclique de corps de nombres de degré p^n et F vérifiant la conjecture de Leopoldt au nombre premier p. Soit p^e l'exposant de H_F. Prenons $i \geq 2$ et soit $r \leq n+e$ un entier tel que p^r divise i. Si $\mu_{p^{n+e-r}} \subset F$, alors*

$$D_F^{(i,n)} = A_F^{(n)}(i).$$

Puisque $\mu_p \subset F$, pour m assez grand, les m-ièmes étages F_m de la $\mathbb{Z}_p$-extension cyclotomique de F satisfait au corollaire suivant :

Corollaire 4.1.8 *Soit E/F une extension cyclique de corps de nombres de degré p^n et telle que la conjecture de Leopoldt soit satisfaite pour tous les étages F_m au nombre premier p. Soit p^e l'exposant de H_F. Prenons $i \geq 2$ et soit $r \leq n+e$ un entier tel que p^r divise i. Si $\mu_{p^{n+e-r}} \subset F$, alors*

$$D_{F_m}^{(i,n)} = A_{F_m}^{(n)}(i),$$

pour m assez grand.

Corollaire 4.1.9 *Supposons E/F une extension cyclique de corps de nombres de degré p^n et F vérifiant la conjecture de Leopoldt au nombre premier p. Supposons p^e l'exposant de H_F et $i = p^e m$, $p \nmid m$ et $\mu_{p^n} \subset F$. Alors, pour tout entier $i \geq 2$,*

$$D_F^{(i,n)} = A_F^{(n)}(i).$$

Ce dernier Corollaire généralise le Corollaire 2.4 de [As-Mo 04], où $n = 1$ et $r = 0$. Nous avons le corollaire suivant :

Corollaire 4.1.10 *Supposons E/F une extension cyclique de corps de nombres de degré p^n et F vérifiant la conjecture de Leopoldt au nombre premier p et que $H_F = 0$. Prenons $i \geq 2$ et soit $r \leq n$ un entier tel que p^r divise i. Si $\mu_{p^{n-r}} \subset F$, alors*

$$D_F^{(i,n)} = A_F^{(n)}(i).$$

4.2 Bornes pour le noyau de capitulation

Rappelons les notations des sections précédentes : p un nombre premier impair, F un corps de nombres et E/F une extension cyclique de corps de nombres de degré p^n et contenant μ_{p^n}, de groupe de Galois G et S est un ensemble fini de places de F contenant les places divisant p et les places archimédiennes de F. Soit o_F^S l'anneau des S-entiers de F. Soit $\tilde{F}$ le composé des $\mathbb{Z}_p$-extensions de F et pour tout $n \geq 1$, $\tilde{F}_n$ désigne le composé des n-ièmes étages des $\mathbb{Z}_p$-extensions de F. Fixons un entier $n \geq 1$.

Proposition 4.2.1 *Soit E/F une extension cyclique de corps de nombres de degré p^n et contenant μ_{p^n}. Alors,*

$$|\mathrm{coker}(f_i)| = |\ker(f_i)| \geq [D_F^{(i,n)} : D_F^{(i,n)} \cap N_{E/F}(E^*)].$$

Preuve. Puisque (voir [As-Mo 04])

$$\mathrm{coker}(f_i) \cong (K_{2i-1}^{\text{ét}} F/p^n)/N_{E/F}(K_{2i-1}^{\text{ét}} E/p^n),\ |\mathrm{coker}(f_i)| = |\ker(f_i)|$$

et $K_{2i-1}^{\text{ét}} F/p^n \cong (D_F^{(i,n)}/F^{*p^n})(i-1)$, alors

$$\mathrm{coker}(f_i) \cong (D_F^{(i,n)}/F^{*p^n} N_{E/F}(D_E^{(i,n)}))(i-1).$$

D'où le résultat puisque $F^{*p} N_{E/F}(D_E^{(i,n)}) \subset D_F^{(i,n)} \cap N_{E/F}(E^*)$. □

Rappelons la définition d'ensemble de places primitif [Mo-Ng 90], [Gr-Ja 89], [Mo 88], [Mo 90] :

Définition 4.2.2 *Un ensemble S de places de F contenant S_p est dit primitif pour (F,p) s'il vérifie l'une des conditions équivalentes suivantes :*

(i) les Frobenius $\sigma_v(\tilde{F}/F)$ attachés aux places $v \in S - S_p$ engendrent un $\mathbb{Z}_p$-facteur direct de $\mathrm{Gal}(\tilde{F}/F)$ de dimension $|S - S_p|$.

(ii) le $\mathbb{Z}/p^n\mathbb{Z}$-module $< \sigma_v(\tilde{F}_n/F),\ v \in S - S_p >$ est un facteur direct de $\mathrm{Gal}(\tilde{F}_n/F)$ de dimension $|S - S_p|$.

La condition (ii) entraîne que $< \sigma_v(\tilde{F}_n/F),\ v \in S - S_p >$ est isomorphe (en tant que groupe abélian) à $(\mathbb{Z}/p^n\mathbb{Z})^{|S-S_p|}$. Notons que l'équivalence entre (i) et (ii) est une conséquence du lemme de Nakayama pour les pro-p-groupes.

Remarque

(a) L'ensemble S_p est, par définition, primitif pour tout couple (F, p).

(b)La condition (i) est utilisée par Gras dans [Gra 83] et la condition (ii) est utilisée par Movahhedi ([Mo 88], §3). Par G. Gras [Gra 86], une extension E/F corps de nombres est primitivement ramifiée si l'ensemble des p-places de F ainsi que celles qui se ramifient dans E forme un ensemble de places primitif pour (F, p).

(c) Le théorème de densité de Čebotarev̆ garantit l'existence d'une infinité d'ensembles primitifs ne rencontrant pas un ensemble fini donné de places et que tout ensemble primitif non maximal peut être complété en un ensemble primitif maximal d'une infinité de façons.

(d) Soit E/F une extension de corps de nombres de degré p et soit S l'ensemble des places ramifiées dans l'extension E/F. Si S est primitif, alors on a $|S - S_p| \leq 1 + r_2 + \delta_F$ où δ_F est le défaut de la conjecture de Leopoldt pour F au nombre premier p.

On suppose à partir de maintenant que F contient le groupe μ_{p^n} des racines p^n-ièmes de l'unité, $n \geq 1$ fixé. Soit

$$A_F^{(n)} := \{a \in F^*/F(\sqrt[p^n]{a}) \subset \tilde{F}\}.$$

On a un accouplement parfait :

$$\begin{array}{ccccc} \mathrm{Gal}(\tilde{F}_n/F) & \times & A_F^{(n)}/F^{*p^n} & \longrightarrow & \mu_{p^n} \\ (\sigma, a) & & & \longmapsto & \sigma(\sqrt[p^n]{a})/\sqrt[p^n]{a}. \end{array} \tag{4.3}$$

Soit maintenant E/F une extension cyclique de corps de nombres contenant μ_{p^n}, de degré p^n et soit S l'ensemble des p-places de F et des places ramifiées dans l'extension E/F.

Soit $\{v_1, v_2, .., v_t\}$ un sous-ensemble de $S - S_p = \{v_1, v_2, .., v_t, ..., v_s\}$ tel que $T := \{v_1, v_2, .., v_t\} \cup S_p$ est un ensemble primitif pour (F, p). Pour tout i,

$1 \leq i \leq s$, notons $\sigma_i = \sigma_{v_i}(\tilde{F}_n/F)$ le Frobenius attaché à la place $v_i \in S - S_p$ dans l'extension $\tilde{F}_n/F$. Par définition de la primitivité, l'ensemble $\{\sigma_1, \sigma_2, ..., \sigma_t\}$ est $\mathbb{Z}/p^n\mathbb{Z}$-libre et peut alors être complété en une $\mathbb{Z}/p^n\mathbb{Z}$-base $\{\sigma_1, ..., \sigma_t, \sigma_{t+1}, ..., \sigma_{1+r_2+\delta_F}\}$ de $Gal(\tilde{F}_n/F)$, où δ_F est le défaut de la conjecture de Leopoldt pour F au nombre premier p.

Soit $\{a_1, ..., a_t, a_{t+1}, ..., a_{1+r_2+\delta_F}\}$ la base duale de $\{\sigma_1, ..., \sigma_t, \sigma_{t+1}, ..., \sigma_{1+r_2+\delta_F}\}$ relativement à l'accouplement (4.3) :

$$\begin{cases} \sigma_i(\sqrt[p^n]{a_i}) = \zeta_{p^n}\sqrt[p^n]{a_i} & \text{pour tout } i = 1, 2, ..., 1 + r_2 + \delta_F \\ \sigma_i(\sqrt[p^n]{a_j}) = \sqrt[p^n]{a_j} & \text{si} \qquad j \neq i. \end{cases}$$

où ζ_{p^n} est une racine primitive p^n-ième de l'unité fixée. En particulier, pour tout i, la place v_i reste inerte dans $F(\sqrt[p^n]{a_i})/F$ et ainsi v_i est totalement décomposée dans $F(\sqrt[p^n]{a_1}, ..., \sqrt[p^n]{a_{i-1}}, \sqrt[p^n]{a_{i+1}}, ..., \sqrt[p^n]{a_{1+r_2+\delta_F}})$.

Soit v une place de $\{v_1, v_2, .., v_t\}$. Soit w une place de E au-dessus de v. Soit F_v et E_w les complétés de F et E pour v et w respectivement. Donc

$$A_F^{(n)} \hookrightarrow F^* \hookrightarrow F_v^*$$

induit l'injection suivante

$$A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^*) \hookrightarrow F_v^*/N_{E_w/F_v}(E_w^*) \cong Gal(E_w/F_v)$$

qui montre que $A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^*)$ est cyclique. Le lemme suivant donne l'ordre de ce groupe cyclique et sera la clé de la preuve du théorème principal ci-dessous :

Lemme 4.2.3 *Soit E/F une extension cyclique de degré p^n contenant μ_{p^n} et soit w une place de E au-dessus de v. Pour une non-p-place $v := v_i$ de $\{v_1, v_2, .., v_t\}$, on a*

$$[A_F^{(n)} : A_F^{(n)} \cap N_{E_w/F_v}(E_w^*)] = p^e,$$

où w est une place de E au-dessus de v et $p^e \geq p$ est l'indice de ramification de v dans E/F.

Preuve. Par construction, puisque $\sqrt[p^n]{a_j} \in F_v$, on a $a_j \in N_{E_w/F_v}(E_w^*)$ pour tout $j \in \{1, 2, ..., 1+r_2\}, j \neq i$, donc pour tout $v_i = v$, $A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^*)$

est engendré par la classe de $a = a_j$. On doit donc montrer que :

$$\begin{cases} a^{p^{e-1}} \notin N_{E_w/F_v}(E_w^*) \\ a^{p^e} \in N_{E_w/F_v}(E_w^*). \end{cases}$$

Soit $b \in F^*$ tel que $E = F(\sqrt[p^n]{b})$. Pour montrer $a^{p^\alpha} \notin N_{E_w/F_v}(E_w^*)$ pour un entier α entre 1 et $e-1$, il suffit de montrer que $(a^{p^\alpha}, b)_v \neq 1$, où $(\ ,\ )_v$ est le symbole de Hilbert dans F_v, à valeurs dans μ_{p^n}. Soit $v(.)$ la valuation $\mathcal{L}$-adique ($\mathcal{L}$ est l'idéal premier associé à la place v). Alors :

$$\begin{aligned} (a^{p^\alpha}, b)_v = (a, b^{p^\alpha})_v = 1 &\Longleftrightarrow b^{p^\alpha} \in N_{F_v(\sqrt[p^n]{a})/F_v}(F_v(\sqrt[p^n]{a})) \\ &\Longleftrightarrow p^n \mid v(b^{p^\alpha}) = p^\alpha v(b) \\ &\Longleftrightarrow p^{n-\alpha} \mid v(b). \end{aligned}$$

Ce qui signifie que $F_v(\sqrt[p^{n-\alpha}]{b})/F_v$ est non-ramifiée.

Maintenant, par définition de e, $F_v(\sqrt[p^{n-e}]{b})$ étant l'extension non-ramifiée maximale de F_v contenue dans $E_w = F_v(\sqrt[p^n]{b})$, on conclut que l'ordre de la classe de a dans $A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^*)$ est exactement p^e. □

Corollaire 4.2.4 *Soit E/F une extension cyclique de corps de nombres de degré p^n et contenant μ_{p^n}. Soit $\{v_1, v_2, ..., v_t\}$ un ensemble maximal de non-p-places contenues dans un ensemble primitif contenu dans $S = Ram(E/F) \cup S_p$, l'ensemble des places de F ramifiées dans E ou divisant p. Alors*

$$[A_F^{(n)} : A_F^{(n)} \cap N_{E/F}(E^*)] \geq p^{e_1+...+e_t},$$

où $p^{e_1}, p^{e_2}, ..., p^{e_t} \geq p$ sont les indices de ramification respectifs de $v_1, v_2, ..., v_t$ dans E/F.

Preuve. Soit le diagramme suivant :

$$\begin{array}{ccc} A_F^{(n)}/A_F^{(n)} \bigcap_{v\in T-S_p} N_{E_w/F_v}(E_w^*) & \xrightarrow{\varphi} & \prod_{v\in T-S_p} A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^*) \\ \uparrow \psi & \nearrow & \\ A_F^{(n)}/A_F^{(n)} \cap N_{E/F}(E^*) & & \end{array}$$

C'est clair que φ est injective. D'autre part, pour tout $i = 1, ...t$, par la construction de la base duale a_i, nous avons

$$\begin{cases} \varphi(\overline{a}_1) = (\overline{a}_1, 0, ..., 0) \\ \varphi(\overline{a}_2) = (0, \overline{a}_2, 0, ..., 0) \\ \quad ... \\ \varphi(\overline{a}_t) = (0, ..., 0, \overline{a}_t). \end{cases}$$

Ainsi φ est un isomorphisme et donc ψ est surjectif. D'où le résultat. □

Combinant ce corollaire avec les résultats de la section précédente nous obtenons la borne suivante pour le noyau ou le conoyau de l'homomorphisme canonique $f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow (K_{2i-2}^{\text{ét}}(o_E^S))^G$, $i \geq 2$:

Théorème 4.2.5 *Supposons E/F une extension cyclique de corps de nombres de degré p^n contenant μ_{p^n} et F vérifiant la conjecture de Leopoldt au nombre premier p. Soit $\{v_1, v_2, ..., v_t\}$ un ensemble maximal de non-p-places contenues dans un ensemble primitif contenu dans $S = Ram(E/F) \cup S_p$. Soit p^e l'exposant du groupe fini H_F. Prenons $i \geq 2$ et soit $r \leq n + e$ un entier tel que p^r divise i. Si $\mu_{p^{n+e-r}} \subset F$. Alors*

$$|\ker(f_i)| = |\text{coker}(f_i)| \geq p^{e_1+...+e_t},$$

où $p^{e_1}, p^{e_2}, ..., p^{e_t} \geq p$ sont les indices de ramification respectifs de $v_1, v_2, ..., v_t$ dans E/F.

Preuve. Par le Corollaire 4.2.4, $[A_F^{(n)} : A_F^{(n)} \cap N_{E/F}(E^*)] \geq p^{e_1+...+e_t}$. Puisque par le Corollaire 4.1.7, nous avons $D_F^{(i,n)} = A_F^{(n)}(i)$, alors

$$\begin{aligned} |\ker(f_i)| = |\text{coker}(f_i)| &\geq [D_F^{(i,n)} : D_F^{(i,n)} \cap N_{E/F}(E^*)] \\ &= [A_F^{(n)}(i) : A_F^{(n)}(i) \cap N_{(E/F)}(E^*)] \\ &= [A_F^{(n)} : A_F^{(n)} \cap N_{(E/F)}(E^*)] \\ &\geq p^{e_1+...+e_t}. \end{aligned}$$

□

Dans le cas classique de $i = 2$, nous avons nécessairement $r = 0$ et pour le noyau et le conoyau de $f_2 : K_2(o_F^S) \longrightarrow (K_2(o_E^S))^G$ on a :

Corollaire 4.2.6 *Soit E/F une extension cyclique de corps de nombres de degré p^n et contenant μ_{p^n}. Soit F vérifiant la conjecture de Leopoldt au nombre premier p. Soit $\{v_1, v_2, ..., v_t\}$ un ensemble maximal de non-p-places contenues dans un ensemble primitif contenu dans $S = Ram(E/F) \cup S_p$. Supposons p^e l'exposant de H_F et $\mu_{p^{n+e}} \subset F$. Alors, nous avons la minoration suivante*

$$|\ker(f_2)| = |\mathrm{coker}(f_2)| \geq p^{e_1+...+e_t},$$

où $p^{e_1}, p^{e_2}, ..., p^{e_t} \geq p$ sont les indices de ramification respectifs de $v_1, v_2, ..., v_t$ dans E/F.

Quand le groupe H_F est trivial, on a donc le corollaire suivant :

Corollaire 4.2.7 *Soit E/F une extension cyclique de corps de nombres de degré p^n et F vérifiant la conjecture de Leopoldt au nombre premier p. Soit $\{v_1, v_2, ..., v_t\}$ un ensemble maximal de non-p-places contenues dans un ensemble primitif contenu dans $S = Ram(E/F) \cup S_p$. Supposons $H_F = 0$ et $\mu_{p^n} \subset F$. Alors, pour $i \geq 2$*

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| \geq p^{e_1+...+e_t},$$

où $p^{e_1}, p^{e_2}, ..., p^{e_t} \geq p$ sont les indices de ramification respectifs de $v_1, v_2, ..., v_t$ dans E/F.

En ce qui concerne la majoration de l'ordre du noyau ou du conoyau de f_i, nous avons :

Proposition 4.2.8 *Soit E/F une extension cyclique de corps de nombres de degré p^n et contenant μ_{p^n}. Alors, pour $i \geq 2$*

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| \leq p^{n(1+r_2)}$$

où r_2 est le nombre de places complexes de F.

Preuve. Puisque, grâce aux résultats de Borel, les K-groupes étales $K^{\text{ét}}_{2i-1}F$ sont de rang r_2, on a

$$K^{\text{ét}}_{2i-1}F \cong \mathbb{Z}_p^{r_2} \oplus \mathrm{Tor}(K^{\text{ét}}_{2i-1}o_F^S).$$

Puisque $\mathrm{Tor}(K^{\text{ét}}_{2i-1}F) \cong H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(i))$ est cyclic d'ordre $\geq p^n$, il vient

$$\mathrm{Tor}(K^{\text{ét}}_{2i-1}F)/p^n \cong \mathbb{Z}/p^n\mathbb{Z}$$

et donc

$$K^{\text{ét}}_{2i-1}F/p^n \cong (\mathbb{Z}/p^n\mathbb{Z})^{r_2} \oplus (\mathbb{Z}/p^n\mathbb{Z}) \cong (\mathbb{Z}/p^n\mathbb{Z})^{1+r_2}.$$

Comme $K^{\text{ét}}_{2i-1}F/p^n$ se surjecte sur le conoyau de f_i, on obtient bien :

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| \leq |K^{\text{ét}}_{2i-1}F/p^n| = p^{n(1+r_2)}.$$

□

Supposons E/F une extension cyclique de corps de nombres de degré p^n contenant μ_{p^n} et F vérifiant la conjecture de Leopoldt au nombre premier p. Soit $\{v_1, v_2, ..., v_t\}$ un ensemble maximal de non-p-places contenues dans un ensemble primitif contenu dans $S = Ram(E/F) \cup S_p$. Par le Théorème 4.2.5 et le Proposition 4.2.8, nous avons les bornes suivantes pour $|\ker(f_i)| = |\mathrm{coker}(f_i)|$:

Corollaire 4.2.9 *Supposons E/F une extension cyclique de corps de nombres de degré p^n contenant μ_{p^n} et F vérifiant la conjecture de Leopoldt au nombre premier p. Soit $\{v_1, v_2, ..., v_t\}$ un ensemble maximal de non-p-places contenues dans un ensemble primitif contenu dans $S = Ram(E/F) \cup S_p$. Soit p^e l'exposant du groupe fini H_F. Prenons $i \geq 2$ et soit $r \leq n + e$ un entier tel que p^r divise i. Si $\mu_{p^{n+e-r}} \subset F$. Alors*

$$p^{e_1+...+e_t} \leq |\ker(f_i)| = |\mathrm{coker}(f_i)| \leq p^{n(1+r_2)},$$

où r_2 est le nombre de places complexes de F et où $p^{e_1}, p^{e_2}, ..., p^{e_t} \geq p$ sont les indices de ramification respectifs de $v_1, v_2, ..., v_t$ dans E/F.

Soit $S = Ram(E/F) \cup S_p$. Un ensemble $T \subset S$ de places de F contenant S_p primitif pour $(F,\ p)$ est maximal si $T - S_p$ est de cardinal maximal, c'est-à-dire, $|T - S_p| = 1 + r_2 + \delta_F$, où δ_F est le défaut de la conjecture de Leopoldt pour F au nombre premier p. Si on dégage un ensemble primitif maximal $T \subset S$ et pour tout $v \in T - S_p$, $p^{e_v} = p^n$ (c'est-à-dire, v est totalement ramifiée dans E), alors on a :

Proposition 4.2.10 *Supposons E/F une extension cyclique de corps de nombres de degré p^n contenant μ_{p^n} et F vérifiant la conjecture de Leopoldt au nombre premier p. Soit $T \subset S$ un ensemble primitif maximal tel que toute place $v \in T - S_p$ est totalement ramifiée dans E. Soit p^e l'exposant du groupe fini H_F. Prenons $i \geq 2$ et soit $r \leq n + e$ un entier tel que p^r divise i. Si $\mu_{p^{n+e-r}} \subset F$, alors*

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| = p^{n(1+r_2)},$$

où r_2 est le nombre de places complexes de F.

Pour finir, nous établissons pour chaque nombre entier non négatif $t \leq 1+r_2$, l'existence d'une infinité d'extensions cycliques E de F de degré p^n, où pour chaque puissance $p^m \leq p^{n(1+r_2)}$ de p, nous avons $|\ker(f_i)| = |\mathrm{coker}(f_i)| = p^m$.

Soit E/F une extension cyclique de degré p^n et soit $G = Gal(E/F)$. Supposons F_∞ la $\mathbb{Z}_p$-extension cyclotomique de F, $E^o = E \cap F_\infty$ tel que $e^o = [E : E^o]$ et $f^o = [E^o : F]$. Le morphisme suivant

$$H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(1-i)) \longrightarrow H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(1-i))$$

a été étudié par Griffiths :

Lemme 4.2.11 ([Gri 05, Lemme 4.2.1]) *Soit $H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(1-i)) \neq 0$ et $i \neq 1$. Alors*

(i) le morphisme

$$H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(1-i)) \longrightarrow H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(1-i))$$

est injectif avec le conoyau cyclique de l'ordre $f^o = [E^o : F]$.

(ii) le morphisme canonique

$$H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(1-i))_G \longrightarrow H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(1-i))$$

induit par la norme a le noyau et le conoyau d'ordre $|H^0(F, \mathbb{Z}/e^o\mathbb{Z}(1-i))|$.

Commençons par la suite exacte canonique suivante

$$0 \to K_{2i-2}^{\text{ét}}(o_F) \to K_{2i-2}^{\text{ét}}(o_F^S) \to \oplus_{v\in S-S_p} H^2(F_v, \mathbb{Z}_p(i))) \to 0.$$

Nous allons maintenant étudier plus en détail le cas particulier où le corps de base F est p-régulier, c'est-à-dire $K_2^{\text{ét}}(o_F) = 0$. Puisqu'on suppose que F contient μ_{p^n}, donc $K_{2i-2}^{\text{ét}}(o_F) = 0$ pour tout entier $i \geq 2$. Par exemple, si p est un premier régulier, les corps cyclotomiques $\mathbb{Q}(\mu_{p^n})$ sont p-réguliers. En outre, nous supposons que l'ensemble S est primitif pour (F, p) de sorte que le corps de nombres E est également p-régulier et soit w une place de E au-dessus de v de F. De cette façon, nous obtenons le diagramme commutatif suivant

$$\begin{array}{ccc} K_{2i-2}^{\text{ét}}(o_E^S)^G & \xrightarrow{\sim} & (\oplus_{v\in S-S_p}, (\oplus_{w|v} H^2(E_w, \mathbb{Z}_p(i))))^G \\ f_i \uparrow & & \oplus_{v\in S-S_p} f_v \uparrow \\ K_{2i-2}^{\text{ét}}(o_F^S) & \xrightarrow{\sim} & \oplus_{v\in S-S_p} H^2(F_v, \mathbb{Z}_p(i)) \end{array}$$

et tout ce que nous devons faire maintenant est d'estimer l'ordre du noyau du morphisme vertical de droite. Pour chacun place v, par la dualité locale, le noyau de f_v a le même ordre que le conoyau du morphisme canonique

$$(\oplus_{w|v} H^0(E_w, \mathbb{Q}_p/\mathbb{Z}_p(1-i)))_G \longrightarrow H^0(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1-i))$$

induit par la norme (puisque, $H^2(F_w, \mathbb{Z}_p(i)) = \text{Dual } H^0(F_w, \mathbb{Q}_p/\mathbb{Z}_p(1-i))$). Soit E'_w le corps d'inertie dans l'extension E_w/F_v. Alors E'_w est obtenu en adjoignant les racines p-primaires de l'unité à F_v (c'est en fait un étage de la $\mathbb{Z}_p$-extension cyclotomique de F_v. Précisement, $E'_w = F_{v,\infty} \cap E_w$).

Ainsi le morphisme :

$$(\oplus_{w|v} H^0(E'_w, \mathbb{Q}_p/\mathbb{Z}_p(1-i))) \longrightarrow H^0(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1-i))$$

est en fait surjectif dans l'extension totalement ramifiée E_w/E'_w, alors que le conoyau du morphisme suivante

$$(\oplus_{w|v} H^0(E_w, \mathbb{Q}_p/\mathbb{Z}_p(1-i))) \longrightarrow H^0(E'_w, \mathbb{Q}_p/\mathbb{Z}_p(1-i))$$

est d'ordre $p^{e_v} = [E_w : E'_w]$, l'indice de ramification de v dans E/F [Lemme 4.2.11] (puisque F_v contient $\mu_{p^{e_v}}$, on a donc une action triviale $H^0(F_v, \mathbb{Z}_p/p^{e_v}\mathbb{Z}_p(1-i)) = H^0(F_v, \mu_{p^{e_v}})(2-i)$).

Nous avons donc montré la

Proposition 4.2.12 *Soit F un corps de nombres p-régulier contenant μ_{p^n} et soit E/F une extension cyclique primitivement ramifiée de degré p^n. Alors*

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| = p^{\sum_{v \in S - S_p} e_v},$$

où S est l'ensemble des p-places de F et des places ramifiées dans l'extension E/F.

Pour chaque corps de nombres p-régulier F avec r_2 places complexes et pour chaque nombre entier non négatif $t \leq 1 + r_2$, nous pouvons trouver, par le théorème de la densité de Čebotarev̆, une infinité d'extensions cycliques E de F de degré p^n, telle que l'ensemble S des p-places de F et les places ramifiées dans l'extension E/F est primitif pour (F, p) et pour chaque $v \in S - S_p$ l'indice de ramification p^{e_v} dans E/F est donné à l'avance. Ainsi, selon la proposition précédente, pour chaque puissance de p (donnée à l'avance) $p^m \leq p^{n(1+r_2)}$, nous avons donc $|\ker(f_i)| = |\mathrm{coker}(f_i)| = p^m$.

Bibliographie

[As 94] **J. Assim**, Sur la p-nullité de certains noyaux de la K-théorie, Thèse, Université de Franche-Comté (1994).

[As 95] **J. Assim**, *Codescente en K-théorie étale et corps de nombres.* Manuscripta Math. **86** (1995) 499-518.

[As-Mo 04] **J. Assim, and A. Movahhedi**, *Bounds For Étale Capitulation Kernels K-theory*, **33** (2004), 199-213.

[Ba 93] **G. Banaszak**, Generalization of the Moore exact sequence and the wild kernel for higher K-groups, Compositio Math. **86** (1993), 281-305.

[Ba-Mi-Se 73] **H. Bass, J. Milnor, et J.-P. Serre** , *Solution of the congruence subgroup problem for $SL_n(n \geq 3)$ and $Sp_{2n}(n \geq 2)$*, Publ. Math. I.H.E.S. **33** (1973).

[Ba-Ta 67] **H. Bass, J. Tate**, *The Milnor ring of a global field (with an appendix on euclidean quadratic imaginary fields, by Tate J.)*, Lecture Notes in Math. vol. **342**, Springer Verlag (1967), 349-446.

[Bo 77] **A. Borel**, *Stable real cohomology of arithmetic groups*, Ann. Sci. École Norm. Sup.**7** (1977), 613-636.

[Br 93] **B. Brauckmann**, Étale K-theory and Iwasawa-theory of number fields, Thesis McMaster University (1993).

[Bru 67] **A. Brumer**, " extensions of algebraic number fields " Math. **14** (1967), 121-124.

[Ca 74] **A. Candiotti** Computations of Iwasawa invariants and K_2. Compositio Math. **29** (1974), 89-111.

[Co 72] **J. Coates**, *On K_2 and some classical conjectures in algebraic number theory.* Ann. of Math. **95** (2) (1972), 99-116.

[Co 77] **J. Coates**, *p-adic L-functions and Iwasawa's theory.* Algebr. Number Fields (ed. A. Fröhlich), Proc. Symp. London math. Soc., Univ. Durham 1975, 269-353 (1977)

[Co-Li 73] **J. Coates, S. Lichtenbaum,** *On l-adic zeta functions.* Ann. of Math. **98** (1973), 498-550.

[Dw-Fr 85] **W. Dwyer, and E. Friedlander**, *Algebraic and étale K-theory*, Trans. Amer. Math. soc. **247** (1) (1985), 247-280.

[Gr 76] **R. Greenberg**, *On the Iwasawa invariants of totally real fields*, Amer. J. Math. **98**, (1976), 263-284.

[Gr 78] **R. Greenberg**, *A note on K_2 and the theory of $\mathbb{Z}_p$-extensions,* Amer. J. Math. **100** (6) (1978), 1235–1245.

[Gra 83] **G. Gras**, *Logarithme p-adique et groupe de Galois,* J. für reine und angew. Math. **343** (1983), 64-80.

[Gra 86] **G. Gras**, *Remarks on K_2 of number fields*, J. Number Th. **23** (1986), 322-335.

[Gri 05] **R. GRIFFITHS**, *A genus formula for étale Hilbert kernels in a cyclic p-power extension,* Thesis, McMaster university (2005).

[Hu 05] **K. Hutchinson**, *Tate kernels, étale K-theory and the Gross kernel.* Preprint (2005).

[Gr-Ja 89] **G. Gras, et J.-F. Jaulent**, *Sur les corps de nombres réguliers.* Math. Z. **202** (3) (1989), 343–365.

[Iw 73] **K. Iwasawa**, *On $\mathbb{Z}_l$-extensions of algebraic number fields,* Ann. Math. (1973).

[Ka 93] **B. Kahn**, *Descente galoisienne et K_2 des corps de nombres*, K-Theory **7** (1) (1993), 55-100.

[Ko 93] **M. Kolster**, *Remarks on étale K-theory and Leopold's Conjecture* Séminaire de Théorie des Nombres, Paris, 1991-1992, Progress in Mathematics 116, Birkhäuser (1993), 37-62.

[Ko 02] **M. Kolster**, *K-theory and arithmetic,* Contemporary developments in algebraic K-theory. Proceedings of the school and conference on algebraic K-theory and its applications, ICTP, Trieste, Italy, July 8-19, 2002. Dedicated to H. Bass on the occasion of his 70th birthday. Trieste : ICTP - The Abdus Salam International Centre for Theoretical Physics. ICTP Lecture Notes 15, 195-258 (2003).

[Ko 3] **M. Kolster**, *Iwasawa Theory*, Chapter 1, monographe.

[Ko-Mo 00] **M. Kolster, and A.Movahhedi**, *Galois co-descent for étale wild kernels and capitulation*, Annales de l'Institut Fourier **50** (1) (2000), 35-65.

[Ko-Mo 00] **M. Kolster, and A.Movahhedi**, *Bi-quadratic number fields with trivial 2-primary Hilbert kernels*, Proc. London Math. Soc. (3) **87** (2003), no. 1, 109–136.

[Le 89] **M. Levine**, *The indecomposable K_3 of a field*, Ann. Sci. École Norm. Sup. **22** (1989), 255-344.

[Li 72] **S. Lichtenbaum,** *On the values zeta and L-functions,* Ann. of Math. **96** (1972), 338-360.

[Li 73] **S. Lichtenbaum,** *Values of zeta-functions, étale cohomology, and algebraic K-theory,* Algebraic K-theory II. Lecteure Notes in Math. **342**, 489-501. Berlin-Heidelberg-New York : Springer (1973)

[Me-Su 83] **A. S. Merkurjev, and A. A. Suslin**, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Math. USSR **21** (1983), 307-340.

[Me-Su 90] **A. S. Merkurjev, and A. A. Suslin**, *The K_3 of a field*, Math. USSR **36** (1990), 541-565.

[Mi 71] **J. Milnor**, *Introduction to algebraic K-theory,* Annals of Mathematical Studies, vol. **72**, Princeton University Press, New Jersey (1971).

[Mo 88] **A. Movahhedi**, *Sur les p-extensions des corps p-rationnels*, Thèse Paris **7** (1988).

[Mo 90] **A. Movahhedi**, *Sur les p-extensions des corps p-rationnels*, Math. Nachr. **149** (1990), 163–176.

[Mo-Ng 90] **A. Movahhedi, et T. Nguyen Quang Do**, *Sur l'arithmétique des corps de nombres p-rationnels, Séminaire de Théorie des nombres, Paris 1987-88*, 155–200, Progr. Math., **81**, Birkhäuser (1990).

[Ne 86] **J. Neukirch**, *Class Field Theory*, Springer-Verlag Berlin Heidelberg (1986).

[Ne-Sc-Wi 00] **J. Neukirch, A. Schmidt, et K. Wingberg**, *Cohomology of number fields,* Grundlehren, Springer (2000).

[Ng 86] **T. Nguyen Quang Do**, *Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens*, Ann. Inst. Fourier, 36-2 (1986), 27-46.

[Ng 92] **T. Nguyen Quang Do**, *Analogues supérieurs du noyau sauvage Séminaire de Théorie des nombres,* Bordeaux, **4** (1992), 263-271.

[Qu 72] **D. Quillen**, *On the cohomology and K-theory of the general linear group over a finite field,* Annals of Math. **96** (1972), 552-586.

[Ro 94] **J. Rosenberg**, *Algebraic K-thoery and Its Applications*, Springer-Verlag (1994).

[Sc 79] **P. Schneider**, *Über gewisse Galoiskohomologiegruppen*, Math. Z. **168** (1979), 181-205

[Se 64] **J.-P. Serre**, *Cohomologie galoisienne*, Lecture Notes in Math., **5**, Springer (1964).

[Se 97] **J.-P. Serre**, *Cohomologie galoisienne*, Lecture Notes in Math., **5**, Springer-Verlag, Berlin, 5^e édition (1997).

[So 79] **C. Soulé**, *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Inv. math **55** (1979), 251-295.

[So 84] **C. Soulé**, *Groupes de Chow et K-théorie de variétés sur un corps fini*, Math. Ann. **268** (1984), 317-345.

[Ta 76] **J. Tate**, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257-274.

[Va 05] **D. Vauclair**, *Capitulation, Cup-produit et sous-modules finis dans les $\mathbb{Z}_p$-extensions d'un corps de nombres*, Preprint, Besançon (2005).

[Wa 97] **L. C. Washington**, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, seconde edition (1997).

BORNES POUR LA CAPITULATION DES K-THÉORIE ÉTALE

Résumé : Cette thèse porte sur l'arithmétique.
Soit p un nombre premier impair et F un corps de nombres contenant le groupe des racines p-ièmes de l'unité. Pour tout ensemble S de places de F contenant les places divisant p et les places archimédiennes de F, soit o_F^S l'anneau des S-entiers de F. Si E est une extension galoisienne de F, non-ramifiée en dehors de S, de groupe de Galois G, nous avons un morphisme canonique d'extension $f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow (K_{2i-2}^{\text{ét}}(o_E^S))^G$. On connait une bonne majoration de l'ordre du noyau et du conoyau de ce morphisme d'extension. Le travail du doctorant a consisté à trouver des minorations pour le noyau ou conoyau de ce morphisme lorsque E/F est une extension cyclique de corps de nombres de degré une puissance de p. Ce travail généralise les travaux précédents dans le domaine.

Mots-clés : théorie d'Iwasawa des **Z**-p-extensions, K-théorie étale, capitulation, noyaux de Tate.

BOUNDS FOR ETALE CAPITULATION KERNELS IN K-THÉORY

Abstract : This thesis concerns arithmetic.
Let p be an odd prime number and let F be an algebraic number field containing the group of the p-th roots of unity. For a finite set S of primes of F containing the primes above p and the infinite primes of F, let o_F^S denote the ring of S-integers of F. If E is a Galois p-extensions of F with Galois group G which is unramified outside S, we have the natural map $f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow (K_{2i-2}^{\text{ét}}(o_E^S))^G$. We know an upper bound for the kernel and of the cokernel of this map. The work of this PhD. thesis consisted in finding lower bounds for the kernel or the cokernel of this map when E/F is a cyclic extensions of an algebraic number fields of degree a power of p. This work generalizes preceding work in the field.

Keywords : theory of Iwasawa the **Z**-p-extensions, etale K-theory, capitulation, kernel of Tate.

XLIM - **D**épartement de **M**athématiques et **I**nformétiques, 123, avenue Albert Thomas, 87060 Limoges Cedex.