THEORIE DES NOMBRES
BESANCON

Années 1984/85-1985/86
Fascicule 2

ETUDE DES DECOMPOSITIONS DES GROUPES DES p-CLASSES D'IDEAUX DANS LA $\mathbb{Z}_p$-EXTENSION CYCLOTOMIQUE D'UNE EXTENSION ABELIENNE DE $\mathbb{Q}$

Marc GRANDET

Etude des décompositions des groupes des p-classes d'idéaux dans la $\mathbb{Z}_p$-extension cyclotomique d'une extension abélienne de $\mathbb{Q}$.

par Marc GRANDET

Résumé .

Soient p un nombre premier et $K_\infty = \bigcup_{n\geq 0} K_n$ la $\mathbb{Z}_p$-extension cyclotomique attachée à une extension abélienne finie K de $\mathbb{Q}$ de degré d étranger à p. Nous montrons que notre résultat sur la capitulation des p-groupes de classes d'idéaux des corps K_n vaut encore pour les φ-composantes de ces groupes regardés comme $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$ -modules, lorsque φ parcourt les caractères p-adiques irréductibles de Gal(K/$\mathbb{Q}$) ; puis nous relions les décompositions élémentaires que nous obtenons aux théorèmes de structures classiques pour les classes imaginaires dans le cas monogène.

Abstract

Let p be a prime number and $K_\infty = \bigcup_{n\geq 0} K_n$ the cyclotomic $\mathbb{Z}_p$-extension attached to a finite abelian extension K of $\mathbb{Q}$, of degree d prime to p. We show that our result about capitulation of p-groups of ideal class of K_n fields is still valid for φ-componants of theese groups viewed as $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-modules when φ is an irreducible p-adic character of Gal(K/$\mathbb{Q}$). Then we connect elementary decompositions which we obtain to classical structure theorems for imaginary class in monogenious case.

1. Introduction.

Soient p un nombre premier et K une extension abélienne de $\mathbb{Q}$ de degré fini d étranger à p. Notons $\mathbb{Q}_\infty = \bigcup_{n\geq 0} \mathbb{Q}_n$ la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$ et $K_\infty = \bigcup_{n\geq 0} K_n$ celle de $K = K_0$ qui est défini par $K_n = K\,\mathbb{Q}_n$. Le groupe de Galois $\Delta = \mathrm{Gal}(K/\mathbb{Q})$

s'identifie avec son relèvement canonique $Gal(K_\infty/\mathbb{Q}_\infty)$ ce qui permet d'écrire pour tout n : $\Delta \simeq Gal(K_n/\mathbb{Q}_n) \simeq Gal(K_\infty/\mathbb{Q}_\infty)$.

Désignons par C_n la p-composante du groupe des classes d'idéaux de K_n et par γ un générateur topologique de $Gal(K_\infty/K)$ de sorte que si nous posons $T=\gamma-1$ et $\Lambda=\mathbb{Z}_p[[T]]$, le système projectif des groupes C_n pour les applications normes détermine un $\Lambda[\Delta]$-module $C=\varprojlim C_n$ qui est de type fini et de torsion. Si nous désignons par X l'ensemble des caractères irréductibles de Δ sur $\mathbb{Q}_p$ et par $(e_\varphi)_{\varphi\in X}$ celui des idempotents primitifs de l'algèbre $\mathbb{Q}_p[\Delta]$, nous avons $\mathbb{Q}_p[\Delta] \simeq \prod_{\varphi\in X} \mathbb{Q}_\varphi$ où $\mathbb{Q}_\varphi \simeq \mathbb{Q}_p[\Delta]\, e_\varphi$ est l'extension non ramifiée de $\mathbb{Q}_p$ de degré f_φ qui correspond à φ. Les groupes C_n se décomposent ainsi comme sommes de leur φ-composantes :

$$C_n = \bigoplus_{\varphi\in X} C_{n,\varphi}$$

avec $C_{n,\varphi} = e_\varphi C_n$. Soit alors $\mathbb{Z}_\varphi$ l'anneau des entiers de $\mathbb{Q}_\varphi$ et $\Lambda_\varphi = \mathbb{Z}_\varphi[[T]]$; d'après les théorèmes de structure établis par J.-P. Serre (cf. [5], Théorèmes 7 et 8) il existe un quasi-isomorphisme de $C_\varphi = \varprojlim C_{n,\varphi}$ dans un Λ_φ-module de la forme :

$$\bigoplus_{i=1}^{r} \Lambda_\varphi/p^{\mu_i}\Lambda_\varphi \bigoplus_{j=1}^{s} \Lambda_\varphi/g_{\varphi,j}\Lambda_\varphi$$

où chaque $g_{\varphi,j}$ est un polynôme distingué de l'anneau $\mathbb{Z}_\varphi[T]$. Comme K est une extension abélienne de $\mathbb{Q}$ on a d'après un théorème de Ferrero et Washington : $\mu = \Sigma\mu_i=0$ (cf. [6], th. 7.15, p. 130) de sorte que les C_φ sont des $\mathbb{Z}_\varphi$-modules de type fini.

Nous visons avec cette note un double but. Tout d'abord dans une première partie, nous généralisons le théorème établi dans [2]. En effet nous montrons, c'est le point essentiel, que le sous-groupe de $C_{n,\varphi}$ qui correspond aux classes qui capitulent dans K_∞ est, dès que n est assez grand, facteur direct de $C_{n,\varphi}$.

Nous utilisons cependant pour établir ce résultat une méthode différente de celle de [2] ; celle-ci est résumée dans les deux lemmes énoncés dans cette première partie.

Ensuite, dans une deuxième partie, après avoir fait des hypothèses justifiées par des "évidences" numériques (cf [3]) nous étudions le cas monogène.

Nous montrons comment la décomposition des groupes $C_{n,\varphi}$ pour les caractères imaginaires établie dans la première partie, est canonique, c'est-à-dire comment elle est liée à la structure de Λ_φ-module de $C_{n,\varphi}$ (rappelée ci-dessus) de façon naturelle. Nous indiquons brièvement la méthode utilisée par deux lemmes qui suivent l'énoncé du théorème 2.

2. Structure de la capitulation dans une $\mathbb{Z}_p$ -extension cyclotomique.

Soit K l'extension abélienne définie plus haut et $K_\infty = \bigsqcup_{n>o} K_n$ son extension cyclotomique. Désignons par $j_{n,m}$ l'homomorphisme de Λ_φ-module de $C_{n,\varphi}$ dans $C_{m,\varphi}$, pour m>n, induit par l'extension des idéaux et par $N_{n,m}$ l'homomorphisme de $C_{m,\varphi}$ dans $C_{n,\varphi}$ induit par la norme arithmétique. Définissons le sous-groupe $\Theta_{n,\varphi}$ des classes qui capitulent par :

$$\Theta_{n,\varphi} = \{x_n / x_n \in C_{n,\varphi} \text{ , il existe } m>n \text{ tel que } j_{n,m}(x_n)=1\}.$$

La condition $\mu = 0$ est équivalente à $rg_{\mathbb{Z}_\varphi} C_{n,\varphi} = \nu_\varphi$ pour n assez grand, où $rg_{\mathbb{Z}_\varphi}$ désigne le $\mathbb{Z}_\varphi$-rang de $C_{n,\varphi}$; c'est encore la dimension sur le corps des restes $\mathbb{F}_\varphi = \mathbb{Z}_\varphi / \ p\ \mathbb{Z}_\varphi$(extension de degré f_φ de $\mathbb{F}_p$) du quotient $C_{n,\varphi}/pC_{n,\varphi}$ (cf. [6], lemme 13.20, p. 282).

Nous savons que pour n assez grand si x_{n+1} est un relèvement dans $C_{n+1,\varphi}$ de $x_n \in C_{n,\varphi}$ (i.e. si l'on a $N_{n+1,n}(x_{n+1})=x_n$) il existe un élément inversible u de Λ_φ, indépendant de n et tel que $j_{n,n+1}(x_n) = pu\ x_{n+1}$. Nous sommes maintenant en mesure d'énoncer notre résultat :

Théorème 1.

Soit $K_\infty = \bigcup\limits_{n>o} K_n$ la $\mathbb{Z}_p$-extension cyclotomique d'une extension abélienne de $\mathbb{Q}$ de degré étranger à p.

i) Il existe un entier n_o tel que les trois conditions suivantes soient réalisées pour tout $n \geqslant n_o$:

a) $rg_{\mathbb{Z}_\varphi} C_{n,\varphi} = \nu_\varphi$ où ν_φ est une constante.

b) $j_{n+1,n}(x_n) = pu\, x_{n+1}$ pour un élément inversible u de Λ_φ.

c) Les idéaux premiers de K_n au-dessus de p sont totalement ramifiés dans K_∞.

Sous ces conditions les p-groupes de classes $C_{n,\varphi}$ se décomposent comme sommes de deux sous-modules :

$$C_{n,\varphi} = S_{n,\varphi} \oplus T_{n,\varphi}$$

où les sous-modules $T_{n,\varphi}$ sont deux à deux isomorphes via les homomorphismes $N_{n+1,n}$:

$$N_{n+1,n} : T_{n+1,\varphi} \xrightarrow{\sim} T_{n,\varphi}$$

et ont pour limite projective le sous-module de $\mathbb{Z}_\varphi$-torsion de C_φ. Celà implique en particulier $T_{n,\varphi} \subset \Theta_{n,\varphi}$.

ii) Il existe de plus un rang $n_1 \geqslant n_o$, des constantes λ et ρ ainsi que des entiers relatifs $\alpha_{i,\varphi}$ $(i=1,\dots \lambda)$ et des entiers positifs $\gamma_{i,\varphi}$ $(i=1\dots\rho)$ tels que pour $n \geqslant n_1$, on ait exactement $T_{n,\varphi} = \Theta_{n,\varphi}$ et :

$$C_{n,\varphi} = S_{n,\varphi} \oplus \Theta_{n,\varphi}$$

avec $$\begin{cases} S_{n,\varphi} = \bigoplus\limits_{i=1}^{\lambda} \mathbb{Z}_\varphi / p^{\alpha_{i,\varphi}+n}\, \mathbb{Z}_\varphi \\ \Theta_{n,\varphi} = \bigoplus\limits_{i=1}^{\rho} \mathbb{Z}_\varphi / p^{\gamma_{i,\varphi}}\, \mathbb{Z}_\varphi \end{cases}$$

iii) Toute pseudo-base de $C_{n,\varphi}$ se relève via la surjection naturelle $N_{n+1,n}$ de C_{n+1} sur C_n en une pseudo-base de $C_{n+1,\varphi}$.

iv) La limite projective des groupes $C_{n,\varphi}$ est isomorphe en tant que $\mathbb{Z}_\varphi$-module à la somme directe :

$$\mathbb{Z}_\varphi^\lambda \oplus \theta_\varphi$$

où $\theta_\varphi \simeq \theta_{n,\varphi}$ quel que soit $n \geq n_1$.

Nous nous appuyons pour démontrer ce résultat sur les deux lemmes qui suivent :

<u>Lemme 1</u>. Il existe pour n assez grand une pseudo-base de $C_{n,\varphi}$: $(x_{n,i})$ et une pseudo-base de $C_{n+1,\varphi}$: $(x_{n+1,i})$ pour $i=1,\ldots,\nu_\varphi$ telles que pour tout i : $N_{n+1,n}(x_{n+1,i}) = x_{n,i}$.
Ces pseudo-bases correspondent aux décompositions élémentaires suivantes :

$$C_{n,\varphi} = \bigoplus_{i=1}^{\nu_\varphi} \mathbb{Z}_\varphi/p^{\beta_i}\,\mathbb{Z}_\varphi \quad \text{et} \quad C_{n+1,\varphi} = \bigoplus_{i=1}^{\nu_\varphi} \mathbb{Z}_\varphi/p^{\beta'_i}\,\mathbb{Z}_\varphi$$

avec $\beta'_i = \beta_i$ ou $\beta'_i = \beta_i+1$ pour tout i.

D'après ce lemme nous pouvons écrire :

$$C_{n,\varphi} = \bigoplus_{i=1}^{\lambda_n} \mathbb{Z}_\varphi/p^{\alpha_i}\,\mathbb{Z}_\varphi \bigoplus_{i=1}^{\rho_n} \mathbb{Z}_\varphi/p^{\gamma_i}\,\mathbb{Z}_\varphi$$

et

$$C_{n+1,\varphi} = \bigoplus_{i=1}^{\lambda_n} \mathbb{Z}_\varphi/p^{\alpha_i+1}\,\mathbb{Z}_\varphi \bigoplus_{i=1}^{\rho_n} \mathbb{Z}_\varphi/p^{\gamma_i}\,\mathbb{Z}_\varphi$$

avec : $\lambda_n + \rho_n = \nu_\varphi$.

Nous obtenons à partir de là le second lemme :

<u>Lemme 2</u>.

Pour n assez grand, les groupes $C_{n,\varphi}$ et $C_{n+1,\varphi}$ ayant des décompositions comme ci-dessus, il existe une pseudo-base

$(x_{n+2,i})$ de $C_{n+2,\varphi}$ pour $i=1,\ldots,\nu_\varphi$ telle que :

$$C_{n+2,\varphi} = \bigoplus_{i=1}^{\lambda_{n+1}} \mathbb{Z}_\varphi/p^{\alpha_i+2}\,\mathbb{Z}_\varphi \bigoplus_{i=1}^{\rho_{n+1}} \mathbb{Z}_\varphi/p^{\gamma_i}\,\mathbb{Z}_\varphi$$

avec $\lambda_{n+1} \leqslant \lambda_n$ et $\rho_{n+1} \geqslant \rho_n$. Les $x_{n+1,i} = N_{n+2,n+1}(x_{n+2,i})$ forment une pseudo-base de $C_{n+1,\varphi}$. De plus si $\lambda_{n+1} = \lambda_n$ les $x_{n,i} = N_{n+1,n}\,(x_{n+1,i})$ forment également une pseudo-base de $C_{n,\varphi}$.

Ainsi à partir d'un certain rang n_1 : $\lambda = \inf \lambda_n$, $\rho = \sup \rho_n$ sont constants : le théorème 1 découle alors facilement des décompositions précédentes.

3. Décomposition des groupes $C_{n,\varphi}$ dans le cas monogène.

Nous supposons dans cette partie que p est un nombre premier impair. Nous supposons également que K contient le groupe μ_p des racines p-ièmes de l'unité et nous notons ω le caractère de l'action de $\mathrm{Gal}(K/\mathbb{Q})$ qui lui correspond. Comme la conjugaison complexe J a une action naturelle sur C_n indépendante du plongement de K dans $\mathbb{C}$ choisi (puisque K est une extension quadratique totalement imaginaire de son sous-corps totalement réel K^+) les groupes C_n se décomposent comme sommes directes de leurs composantes réelles et imaginaires :

$$C_n = C_n^+ \oplus C_n^+ = (1+J)C_n,\ C_n^- = (1-J)\ C_n\ .$$

Les groupes C_n^- se décomposent à leur tour à l'aide des idempotents orthogonaux e_φ qui correspondent aux caractères impairs de X, c'est-à-dire ceux pour lesquels on a : $Je_\varphi = -e_\varphi$. On obtient alors :

$$C_n^- = \bigoplus_{\varphi \in \bar{X}} C_{n,\varphi}$$

$\bar{X}$ désignant le sous-ensemble des caractères impairs de X.

Supposons maintenant que C_0^- soit monogène en tant que Λ-module, ce qui est le cas si par exemple la conjecture de Vandiver est vérifiée pour K^+. On obtient alors, pour les φ-

-composantes des groupes de classe $C_{n,\varphi}$ qui correspondent aux caractères impairs autres que le caractère cyclotomique ω, les isomorphismes de Λ_φ-modules :

$$C_{n,\varphi} \overset{\sim}{\to} C_\varphi/\omega_n C_\varphi \overset{\sim}{\to} \Lambda\varphi/(g_\varphi,\omega_n)\Lambda\varphi$$

pour un certain polynôme distingué g_φ de $\mathbb{Z}_\varphi[T]$. (cf. [1], § 2.4, p. 516....) et $\omega_n = (1+T)^{p^n}-1$.

Enonçons notre résultat :

Théorème 2. Soient p un nombre premier impair et K une extension abélienne de $\mathbb{Q}$ de degré étranger à p, contenant le groupe μ_p des racines p-ièmes de l'unité.

i) Pour tout caractère imaginaire φ de $\bar{X}$ il existe un entier α_φ positif ou nul tel que

$$C_\varphi \simeq \mathbb{Z}_\varphi^{\alpha_\varphi};$$

en particulier pour chaque valeur de n on a $\Theta_{n,\varphi}=1$.

ii) Supposons, en outre, que les conditions suivantes soient réalisées :

a) Il n'existe dans K qu'un seul idéal premier $\mathfrak{P}\,|p$ lequel est totalement ramifié dans K_∞.

b) Le sous-groupe C_0^- de C_0 est engendré sur $\mathbb{Z}_p$ [Gal(K/$\mathbb{Q}$)] par un unique générateur σ_0.

c) Les caractères considérés sont ceux de $\bar{X}$ distincts du caractère cyclotomique ω.

Il existe alors un rang r tel que pour n>r on ait un isomorphisme $\psi_{n,\varphi}$ de Λ_φ-module :

$$\Psi_{n,\varphi} : \qquad \mathbb{Z}_\varphi/p^{\tau_\varphi+n}\,\mathbb{Z}_\varphi \oplus \mathbb{Z}_\varphi/p^n\,\mathbb{Z}_\varphi^{\alpha_\varphi-1} \overset{\sim}{\to} C_{n,\varphi}$$

où α_φ est le degré de g_φ et τ_φ est la valuation p-adique de $g_\varphi(0)$.

Nous nous bornerons à quelques indications à propos de ce théorème. Pour la partie i) le sous-groupe de $\mathbb{Z}_\varphi$ torsion de C_φ, soit Θ_φ, est isomorphe à $\Theta_{n,\varphi}$ (cf. théorème 1, iv) or pour $\varphi\in X$ et $\varphi\neq\omega$ on a d'après la formule des classes ambiges $\Theta_{n,\varphi}=1$.

Pour $\varphi=\omega$ comme on a :

$$\Theta_{n,\varphi} \hookrightarrow H^1(\mathrm{Gal}(K_\infty/K_n),\ \mathbb{Z}_p \otimes_{\mathbb{Z}} E_{K_\infty})^{e_\varphi}$$

et comme les racines de l'unité sont cohomologiquement triviales c'est-à-dire :

$$H^1(\mathrm{Gal}(K_\infty/K_n),\ \mathbb{Z}_p \otimes {}_{\mathbb{Z}}E_{K_\infty})^{e_\varphi} = H^1(\mathrm{Gal}(K_\infty/K_n),\ \mu_{K_\infty})=1,$$

on a bien dans tous les cas $\Theta_\varphi=1$ (voir à ce sujet [4] chapitre III). Quant à la partie ii), considérons :

$$(\lambda_1,\dots,\lambda_{\alpha_\varphi}) \in \mathbb{Z}_\varphi/p^{\tau_\varphi+n}\ \mathbb{Z}_\varphi \oplus \mathbb{Z}_\varphi/p^n\ \mathbb{Z}_\varphi^{\alpha_\varphi-1} \qquad (1)$$

soit $\sigma_{n,\varphi}$ un relèvement de $\sigma_{o,\varphi}$ dans $C_{n,\varphi}$ alors $\psi_{n,\varphi}$ opère de la façon suivante :

$$\psi_{n,\varphi}(\lambda_1,\dots,\lambda_{\alpha_\varphi}) = \Big(\sum_{i=1}^{\alpha_\varphi} \lambda_i\ T^{i-1}\Big)\sigma_{n,\varphi}$$

Cette relation permet de définir sur la somme directe (1) une structure de Λ_φ-module. Remarquons que :

$$T^{\alpha_\varphi} = -\sum_{i=1}^{\alpha_\varphi-1} a_i\ T^{\alpha_\varphi-i} \quad \text{où} \quad g_\varphi = T^{\alpha_\varphi} + \sum_{i=1}^{\alpha_\varphi-1} a_i\ T^{\alpha_\varphi-i-1}$$

La décomposition des groupes $C_{n,\varphi}$ s'obtient en utilisant les deux lemmes suivants :

<u>Lemme 3</u>. Soit $\alpha_\varphi = d^o g_\varphi$, posons $\Lambda_{n,\varphi} = \Lambda_\varphi/(g_\varphi,\ \omega_n)\Lambda_\varphi$.
Alors tout élément $P \in \Lambda_{n,\varphi}$ admet une unique représentation sous la forme :

$$P = \sum_{j=o}^{n} P_{n-j}\ \frac{\omega_n}{\omega_{n-j}}$$

avec $P_{n-j} = \sum_{i=o}^{\alpha_\varphi-1} a_{ij}\ T^j$, les a_{ij} étant des représentants dans $\mathbb{Z}_\varphi$ du corps résiduel $\mathbb{F}_\varphi$ et $P_o \in \mathbb{Z}_\varphi/g_\varphi(0)\mathbb{Z}_\varphi$.

Ce lemme permet d'exprimer, dès que n est assez grand, p^i pour $i \leqslant n$ de la façon suivante :

$$p^i = \sum_{j=o}^{n-i} \frac{\omega_n}{\omega_{n-i-j}} B_{n-i-j,i}$$

où $B_{n-i-j,i} \in \mathbb{Z}_\varphi[T]$, $d^o B_{n-i-j,i} \leqslant \alpha_\varphi - 1$. Nous déduisons de là :

<u>Lemme 4</u>. Dans $\Lambda_{n,\varphi}$ les relations suivantes sont vérifiées :

$$\frac{\omega_n}{\omega_{n-i}} = \sum_{j=o}^{n-i} p^{i+j} \quad \omega_{n-i-j,i} \quad \text{pour } i=1,\dots,n.$$

avec $\omega_{j,i} = \sum_{k=o}^{\alpha_\varphi - 1} a_{k,i,j} T^k$, $a_{k,i,j} \in \mathbb{F}_\varphi$.

Il est aisé à partir de là de montrer que la suite :

$$0 \to N_\varphi \to \mathbb{Z}_\varphi / p^{\tau_\varphi + n} \quad \mathbb{Z}_\varphi^{\alpha_\varphi} \to \Lambda_{n,\varphi} \to 0$$

est exacte et que le noyau N_φ est égal à ce qu'on attend. Nous obtenons alors l'expression des $\psi_{n,\varphi}$.

BIBLIOGRAPHIE

[1] J. COATES, S. LICHTENBAUM. On ℓ-adic zeta functions, Ann. of Math., 98 (1973), p. 498-550.

[2] M. GRANDET et J.-F. JAULENT. Sur la capitulation dans une $\mathbb{Z}_\ell$-extension, J. reine angew. Math., 362 (1985), p. 213-217.

[3] K. IWASAWA and C.C. SIMS. Computations of invariant of cyclotomic fields, J. Math. Soc. JAPAN, Vol. 18 n°1 (1966), p. 86-96.

[4] J.-F. JAULENT. L'arithmétique des ℓ-extensions. Thèse d'Etat (1986). Public. Math. Fac. Sci. Besançon (Théorie des nombres) Années 1984-1985. 1985-1986, fasc. 1.

[5] J.-P. SERRE. Classes des corps cyclotomiques (d'après IWASAWA), Séminaire Bourbaki, exp. 174 (1958).

[6] L.C. WASHINGTON. Introduction to cyclotomic fields, Springer-Verlag (1982).

Université Paul Sabatier
U.F.R. de Mathématiques et Gestion
118, route de Narbonne
31062 TOULOUSE Cédex