

Sur quelques modules d'Iwasawa semi-simples*

Jean-François JAULENT & Jonathan W. SANDS

Résumé. Nous introduisons la notion de \mathbb{Z}_ℓ -extension cyclotomiquement ramifiée sur un corps de nombres K pour obtenir des conditions arithmétiques générales de semi-simplicité algébrique du module d'Iwasawa standard \mathcal{C}_{K_∞} associé à une telle extension.

Revenant ensuite sur les exemples déjà étudiés par Jaulent ou Carroll et Kisilevsky, nous montrons que cette nouvelle approche permet de retrouver des résultats connus mais aussi de rendre compte naturellement de la plupart des cas de non semi-simplicité.

Les preuves reposent essentiellement sur la théorie ℓ -adique du corps de classes.

Abstract. We define the notion of a cyclotomically ramified \mathbb{Z}_ℓ -extension of number fields K_∞/K , and relate it to the semisimplicity of the corresponding standard unramified Iwasawa module \mathcal{C}_{K_∞} .

Returning to the setting in which semisimplicity was originally studied by Jaulent and Carroll-Kisilevsky, we find that our approach leads to some more precise results.

An essential tool is the ℓ -adic class-field theory, which we review.

Introduction

Soient K un corps de nombres, ℓ un nombre premier, $K_\infty = \cup_{n \in \mathbb{N}} K_n$ une \mathbb{Z}_ℓ -extension de K , puis γ un générateur topologique du groupe procyclique $\Gamma = \text{Gal}(K_\infty/K)$, et $\Lambda = \mathbb{Z}_\ell[[\gamma-1]]$ l'algèbre d'Iwasawa associée. Il est bien connu que le groupe de Galois \mathcal{C}_{K_∞} de la pro- ℓ -extension abélienne non ramifiée maximale C_∞ de K_∞ est un Λ -module noethérien et de torsion pseudo-isomorphe¹ comme tel à une unique somme directe finie de Λ -modules élémentaires de la forme :

$$\mathcal{C}_{K_\infty} \sim \bigoplus_P \left(\bigoplus_{i=1}^{n_P} \Lambda / P^{\nu_{P_i}} \Lambda \right),$$

où P parcourt le système de représentants des éléments irréductibles de l'anneau factoriel Λ formé du nombre premier ℓ et des polynômes irréductibles et distingués de l'anneau $\mathbb{Z}_\ell[\gamma-1]$, la quantité n_P mesure le nombre de P -facteurs de \mathcal{C}_{K_∞} , et les ν_{P_i} forment pour chaque P une suite décroissante d'entiers naturels non nuls. Le produit fini des dénominateurs

$$\chi_{\mathcal{C}_{K_\infty}} = \prod_{n_P \neq 0} \prod_{i=1}^{n_P} P^{\nu_{P_i}}$$

est ainsi le polynôme caractéristique du Λ -module \mathcal{C}_{K_∞} , et le sous-produit

$$P_{\mathcal{C}_{K_\infty}} = \prod_{n_P \neq 0} P^{\nu_{P_1}},$$

*Compositio Math. **99** (1995), 325–341.

¹ Un pseudo-isomorphisme est un morphisme à noyau et conoyau finis.

est, lui, le polynôme minimal de ce même module ². On dit alors que \mathcal{C}_{K_∞} est semi-simple (resp. semi-simple en un premier P) lorsque $P_{\mathcal{C}_{K_\infty}}$ est sans facteur carré (resp. lorsque P^2 ne divise pas $P_{\mathcal{C}_{K_\infty}}$ ou, ce qui revient au même, lorsque ν_{P^1} vaut 1 pour $n_P > 0$).

Le cas arithmétiquement le plus intéressant est celui où le polynôme premier P considéré est cyclotomique, i.e. de la forme $\omega_0 = \gamma - 1$ ou encore

$$\omega_n = (\gamma^{\ell^n} - 1)/(\gamma^{\ell^{n-1}} - 1) = \gamma^{\ell^{n-1}(\ell-1)} + \dots + \gamma^{\ell^{n-1}} + 1$$

pour $n > 0$, puisque dans ce cas le quotient $\mathcal{C}_{K_\infty}/\mathcal{C}_{K_\infty}^{\omega_n}$ s'interprète à l'aide de la théorie des genres : Plus précisément, si K_n est le sous-corps de K_∞ fixé par γ^{ℓ^n} , le quotient $\mathcal{C}_{K_\infty}/\mathcal{C}_{K_\infty}^{\gamma^{\ell^n}-1}$ n'est autre que le groupe de Galois de la sous-extension maximale de \mathcal{C}_∞ qui est abélienne sur K_n et son calcul relève donc de la théorie du corps de classes dans le corps K_n .

Dans ce contexte bien précis, le premier résultat de semi-simplicité est celui obtenu par R. Greenberg, à l'aide des théorèmes d'indépendance de logarithmes de Baker-Brumer, (cf. [Gr]), pour les \mathbb{Z}_ℓ -extensions cyclotomiques des corps abéliens (réels ou imaginaires), résultat qui fut généralisé ensuite par L.J. Federer et B. H. Gross (cf. [FG]) au cas où le corps de base K sans être nécessairement abélien est cependant équipé d'une conjugaison complexe (c'est-à-dire qu'il se présente comme extension quadratique totalement imaginaire d'un sous-corps K^+ totalement réel) et satisfait une condition d'indépendance ℓ -adique conjecturée par B. H. Gross.

Inversement, quelques exemples de non semi-simplicité pour certaines \mathbb{Z}_ℓ -extensions non cyclotomiques de corps abéliens imaginaires ont été produits par J.-F. Jaulent, via la théorie des genres (cf. [J₁]), puis indépendamment mais de façon plus systématique par H. Kisilevsky (cf. [Ki]), à partir d'une idée voisine.

Le but de cet article est d'expliciter des conditions arithmétiques non triviales de ramification qui entraînent la semi-simplicité algébrique du groupe \mathcal{C}_{K_∞} . Nous proposons ainsi d'appeler cyclotomiquement ramifiées les \mathbb{Z}_ℓ -extensions qui vérifient ces conditions de ramification, et nous montrons dans plusieurs situations qu'elles sont bien en général semi-simples sous les conjectures ℓ -adiques standard.

C'est ainsi que, revenant sur le cas métabélien déjà étudié par J.-F. Jaulent (cf. [J₁], [J₂], [J₃]) ou J. Carroll et H. Kisilevsky (cf. [CK₁], [CK₂], [K]), nous prouvons par exemple que pour les corps de nombres à groupe de Galois sur \mathbb{Q} abélien et d'exposant divisant $(\ell - 1)$, les \mathbb{Z}_ℓ -extensions absolument galoisiennes pour lesquelles le Λ -module \mathcal{C}_{K_∞} est semi-simple en $\omega_0 = \gamma - 1$ sont celles cyclotomiquement ramifiées et celles-là seulement dès lors que le caractère ω qui définit la décomposition semi-directe du groupe métaprocyclique $\text{Gal}(K/\mathbb{Q})$ n'est pas d'ordre 2 ; et nous les déterminons explicitement.

²C'est le plus petit polynôme Q de l'anneau factoriel $\mathbb{Z}_\ell[\gamma - 1]$ pour lequel le module $\mathcal{C}_{K_\infty}^Q$ (en notation multiplicative) est pseudo-nul (i.e. fini).

Notre outil essentiel dans ce travail est la théorie ℓ -adique du corps de classes élaborée dans [J₃], dont nous commençons par rappeler brièvement quelques résultats.

1.- Le formalisme ℓ -adique du corps de classes.

Nous supposons fixés dans tout ce qui suit un corps de nombres K et un nombre premier ℓ .

Pour chaque place \mathfrak{p} de K , nous écrivons $K_{\mathfrak{p}}$ le complété de K en \mathfrak{p} , puis $\mathcal{R}_{\mathfrak{p}}$ la ℓ -partie du complété profini du groupe multiplicatif $K_{\mathfrak{p}}^{\times}$, c'est-à-dire la limite projective

$$\mathcal{R}_{\mathfrak{p}} = \varprojlim K_{\mathfrak{p}}^{\times} / K_{\mathfrak{p}}^{\times \ell^n}$$

que l'isomorphisme d'Artin local $\omega_{\mathfrak{p}}$ identifie au groupe de Galois $\text{Gal}(K_{\mathfrak{p}}^{ab} / K_{\mathfrak{p}})$ de la pro- ℓ -extension abélienne maximale de $K_{\mathfrak{p}}$. Le groupe compact ainsi obtenu est donc trivial lorsque \mathfrak{p} est complexe, d'ordre 1 ou 2 lorsque \mathfrak{p} est réelle, et s'écrit dans le cas ultramétrique

$$\mathcal{R}_{\mathfrak{p}} \simeq \mathcal{U}_{\mathfrak{p}} \pi_{\mathfrak{p}}^{\mathbb{Z}_{\ell}},$$

si l'on note $\pi_{\mathfrak{p}}$ l'image dans $\mathcal{R}_{\mathfrak{p}}$ d'une uniformisante arbitraire de $K_{\mathfrak{p}}$, le sous-groupe unité $\mathcal{U}_{\mathfrak{p}}$ étant

- soit le ℓ -groupe $\mu_{\mathfrak{p}}$ des racines de l'unité dans $K_{\mathfrak{p}}$, lorsque \mathfrak{p} est modérée (i.e. étrangère à ℓ),
- soit le \mathbb{Z}_{ℓ} -module $U_{\mathfrak{p}}^1 = 1 + \mathfrak{p}$ des unités principales, lorsque \mathfrak{p} est sauvage (i.e. divisant ℓ).

Deux sous-groupes fermés de $\mathcal{R}_{\mathfrak{p}}$ nous intéressent particulièrement ici :

- d'une part le sous-groupe unité $\mathcal{U}_{\mathfrak{p}}$, déjà défini, qui est associé dans la correspondance galoisienne du corps de classes local à la \mathbb{Z}_{ℓ} -extension non ramifiée $K_{\mathfrak{p}}^{nr}$ de $K_{\mathfrak{p}}$;

- d'autre part le sous-groupe $\tilde{\mathcal{U}}_{\mathfrak{p}}$ des normes cyclotomiques, qui correspond, lui, à la \mathbb{Z}_{ℓ} -extension cyclotomique $K_{\mathfrak{p}}^c$ de $K_{\mathfrak{p}}$, et peut être défini comme le noyau dans $\mathcal{R}_{\mathfrak{p}}$ de la valeur absolue ℓ -adique principale $|\cdot|_{\mathfrak{p}}$ qui prend ses valeurs dans $1 + 2\ell\mathbb{Z}_{\ell}$ (cf. [J₃]).

Ces deux groupes sont toujours isomorphes (non canoniquement) mais ne coïncident en fait que lorsque la place \mathfrak{p} est modérée i.e. ici étrangère à ℓ : ce sont des \mathbb{Z}_{ℓ} -modules noethériens de rang $d_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_{\mathfrak{p}}]$ et de même sous-module fini $\mu_{\mathfrak{p}}$.

Introduisons maintenant le ℓ -groupe des idèles de K , c'est-à-dire le produit restreint

$$\mathcal{I} = \prod_{\mathfrak{p}}^{res} \mathcal{R}_{\mathfrak{p}} = \{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} \mathcal{R}_{\mathfrak{p}} \mid x_{\mathfrak{p}} \in \mathcal{U}_{\mathfrak{p}} \text{ pour presque tout } \mathfrak{p}\},$$

étendu aux places (non complexes) \mathfrak{p} de K , et équipé de sa topologie naturelle de limite inductive des sous-modules compacts

$$\mathcal{J}^S = \prod_{\mathfrak{p} \in S} \mathcal{R}_{\mathfrak{p}} \prod_{\mathfrak{p} \notin S} \mathcal{U}_{\mathfrak{p}}$$

pour S parcourant l'ensemble des sous-familles finies de places de K .

La théorie ℓ -adique du corps de classes global établit un isomorphisme (algébrique et topologique) entre le quotient $\mathcal{C} = \mathcal{J}/\mathcal{R}$ de \mathcal{J} par son sous-groupe principal $\mathcal{R} = \mathbb{Z}_{\ell} \otimes_{\mathbb{Z}} K^{\times}$, et le groupe de Galois $\text{Gal}(K^{ab}/K)$ de la pro- ℓ -extension abélienne maximale de K , lequel met en bijection les sous-extensions de K^{ab} et les sous-groupes fermés de \mathcal{J} qui contiennent \mathcal{R} . Un certain nombre de pro- ℓ -extensions *abéliennes* de K nous intéressant plus particulièrement, donnons en la liste, en indiquant pour chacune sa définition ainsi que le ℓ -groupe d'idèles associé :

<i>Extension</i>	<i>Définition</i>	<i>Groupe d'idèles associé</i>
K	corps de base	\mathcal{J}
K^{nr}	abélienne non ramifiée maximale	$\mathcal{UR} = (\prod_{\mathfrak{p}} \mathcal{U}_{\mathfrak{p}})\mathcal{R}$
K^c	\mathbb{Z}_{ℓ} -extension cyclotomique	$\tilde{\mathcal{J}} = \{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \mathcal{J} \mid \prod_{\mathfrak{p}} x _{\mathfrak{p}} = 1\}$
K^{lc}	localement cyclotomique	$\tilde{\mathcal{UR}} = (\prod_{\mathfrak{p}} \tilde{\mathcal{U}}_{\mathfrak{p}})\mathcal{R}$
$K^{\ell r}$	abélienne ℓ -ramifiée maximale	$(\prod_{\mathfrak{p} \nmid \ell} \mathcal{U}_{\mathfrak{p}})\mathcal{R} = (\prod_{\mathfrak{p} \nmid \ell} \mu_{\mathfrak{p}})\mathcal{R}$
K^{ab}	abélienne maximale	\mathcal{R}

Remarques.

(i) Le corps K^{nr} qui est la ℓ -extension abélienne non ramifiée (aux places finies) maximale de K est ce qu'il est convenu d'appeler le ℓ -corps des classes de Hilbert (au sens restreint) de K : c'est une extension de degré fini, de groupe de galois $\text{Gal}(K^{nr}/K) \simeq \mathcal{J}/\mathcal{UR} \simeq \mathcal{Cl}$ isomorphe au ℓ -groupe des classes de diviseurs de K .

(ii) Le corps K^{lc} est la pro- ℓ -extension abélienne maximale de K qui est localement cyclotomique c'est-à-dire complètement décomposé en chaque place au-dessus de K^c . Comme la montée dans la \mathbb{Z}_{ℓ} -extension cyclotomique K^c/K a épuisé toute possibilité d'inertie aux places ultramétriques modérées, on voit que la condition de complète décomposition signifie simplement que K^{lc}/K^c est non ramifiée (aux places modérés) et complètement décomposée en celles réelles ou sauvages.

(iii) Le groupe de Galois $\text{Gal}(K^{lc}/K^c) \simeq \tilde{\mathcal{J}}/\tilde{\mathcal{UR}} \simeq \tilde{\mathcal{Cl}}$ est, par définition, le ℓ -groupe des classes logarithmiques du corps K . Sa finitude constitue précisément la conjecture de Gross généralisée, pour le corps K et le nombre premier ℓ (cf. [J₃]). Lorsque celle-ci est vérifiée, le corps K^{lc} contient alors une unique \mathbb{Z}_{ℓ} -extension de K , à savoir la cyclotomique K^c .

(iv) L'isomorphisme $\text{Gal}(K^{\ell r}/K^{nr}) \simeq \mathcal{UR}/\prod_{\mathfrak{p} \nmid \ell} \mathcal{U}_{\mathfrak{p}} \mathcal{R}$ identifie le groupe de Galois $\text{Gal}(K^{\ell r}/K^{nr})$ au quotient $\mathcal{U}_{\ell}/s_{\ell}(\mathcal{E})$ du groupe des unités principales

semi-locales $\mathcal{U}_\ell = \prod_{\mathfrak{p}|\ell} \mathcal{U}_{\mathfrak{p}}$ par l'image $\mathcal{E}_\ell = s_\ell(\mathcal{E})$ du tensorisé $\mathcal{E} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E$ du groupe des unités (totalement positives) de K . La conjecture de Leopoldt (pour le corps K et le premier ℓ) postule que \mathcal{E} s'injecte dans \mathcal{U}_ℓ , autrement dit que le quotient $\mathcal{U}_\ell/s_\ell(\mathcal{E})$ est de rang $(r+2c) - (r+c-1) = c+1$ (r étant le nombre de places réelles et c le nombre de places complexes du corps K), i.e. que K admet $c+1$ \mathbb{Z}_ℓ -extensions linéairement indépendantes (seulement).

2.- Extensions cyclotomiquement ramifiées.

Définition 1. *Nous disons qu'une pro- ℓ -extension L de K est cyclotomiquement ramifiée lorsqu'elle vérifie les deux conditions suivantes :*

- (i) *Toutes les places de K au-dessus de ℓ se ramifient (infiniment) dans L/K .*
- (ii) *L'extension induite LK^c/K^c au-dessus de la tour cyclotomique K^c est non ramifiée.*

Avant de dégager l'intérêt de cette définition pour le problème qui nous préoccupe, commençons par dénombrer les \mathbb{Z}_ℓ -extensions linéairement indépendantes qui sont cyclotomiquement ramifiées. Remarquons d'abord que toutes sont contenues dans la pro- ℓ -extension abélienne maximale K^{cr} de K qui est non ramifiée sur K^c (i.e. le corps des genres attaché à l'extension cyclotomique K^c/K). Or nous avons :

Théorème 2. *Le ℓ -groupes d'idèles qui est associé par la théorie du corps de classes à la pro- ℓ -extension abélienne cyclotomiquement ramifiée maximale K^{cr} de K est le produit $\widehat{\mathcal{U}}\mathcal{R}$ du ℓ -groupe $\widehat{\mathcal{U}} = \mathcal{U} \cap \widehat{\mathcal{U}}$ des idèles unités qui sont des normes cyclotomiques par le sous-groupe principal \mathcal{R} .*

En particulier, il vient donc :

$$\text{Gal}(K^{cr}/K^{lc}) \simeq \widetilde{\mathcal{U}}\mathcal{R}/\widehat{\mathcal{U}}\mathcal{R} \simeq \widetilde{\mathcal{U}}_\ell/\widehat{\mathcal{U}}_\ell\mathcal{E}_\ell ,$$

où $\widetilde{\mathcal{U}}_\ell$ (resp. $\widehat{\mathcal{U}}_\ell$) est le noyau des valeurs absolues ℓ -adiques dans $\mathcal{R}_\ell = \prod_{\mathfrak{t}|\ell} \mathcal{R}_{\mathfrak{t}}$ (resp. dans $\mathcal{U}_\ell = \prod_{\mathfrak{t}|\ell} \mathcal{U}_{\mathfrak{t}}$) et $\mathcal{E}_\ell = s_\ell(\mathcal{E})$ la projection dans \mathcal{R}_ℓ du groupe $\widetilde{\mathcal{E}} = \widetilde{\mathcal{U}} \cap \mathcal{R}$ des normes cyclotomiques globales.

Preuve. La composée K^{cr} des pro- ℓ -extensions abéliennes cyclotomiquement ramifiées de K étant trivialement la pro- ℓ -extension abélienne maximale de K qui est non ramifiée sur K^c , elle contient en particulier K^{lc} (qui est, elle, la pro- ℓ -extension abélienne maximale qui est complètement décomposée sur K^c) ; et d'un autre côté, elle est ℓ -ramifiée (i.e. non ramifiée en dehors des places divisant ℓ) c'est-à-dire qu'elle est contenue dans $K^{\ell r}$.

Considérons un instant l'extension abélienne K^{ab}/K : Pour chaque \mathfrak{p} de K , le sous-groupe de décomposition correspondant $D_{\mathfrak{p}}(K^{ab}/K)$ dans $\text{Gal}(K^{ab}/K) \simeq \mathcal{J}/\mathcal{R}$ étant l'image du facteur local $\mathcal{R}_{\mathfrak{p}}$ dans le quotient \mathcal{J}/\mathcal{R} , sa trace dans le sous-groupe $\text{Gal}(K^{ab}/K^c) \simeq \widetilde{\mathcal{J}}/\mathcal{R}$ est donnée par l'intersection $(\mathcal{R}_{\mathfrak{p}}\mathcal{R} \cap \widetilde{\mathcal{J}})/\mathcal{R}$. Et comme $\widetilde{\mathcal{J}}$ est précisément le noyau dans \mathcal{J} de la formule du produit pour les

valeurs absolues, les éléments du numérateur sont exactement ceux de $\tilde{\mathcal{U}}_{\mathfrak{p}}\mathcal{R}$, où $\tilde{\mathcal{U}}_{\mathfrak{p}}$ est le noyau de $|\cdot|_{\mathfrak{p}}$ dans $\mathcal{R}_{\mathfrak{p}}$. Il vient donc :

$$D_{\mathfrak{p}}(K^{ab}/K^c) \simeq \tilde{\mathcal{U}}_{\mathfrak{p}}\mathcal{R}/\mathcal{R},$$

et, par un calcul tout à fait semblable :

$$I_{\mathfrak{p}}(K^{ab}/K^c) \simeq \widehat{\mathcal{U}}_{\mathfrak{p}}\mathcal{R}/\mathcal{R},$$

puisque le sous-groupe d'inertie $I_{\mathfrak{p}}$ provient, lui, du sous-groupe unité $\mathcal{U}_{\mathfrak{p}}$ de $\mathcal{R}_{\mathfrak{p}}$.

Ainsi, le sous-groupe engendré par les groupes de décomposition $D_{\mathfrak{p}}(K^{ab}/K^c)$ est $\text{Gal}(K^{lc}/K^c) \simeq \tilde{\mathcal{U}}\mathcal{R}/\mathcal{R}$, et celui engendré par les sous-groupes d'inertie $I_{\mathfrak{p}}(K^{ab}/K^c)$ est $\text{Gal}(K^{cr}/K^c) \simeq \widehat{\mathcal{U}}\mathcal{R}/\mathcal{R}$; d'où les résultats annoncés.

Remarque. Nous avons vu que K^{cr} est intermédiaire entre l'extension localement cyclotomique K^{lc} et celle ℓ -ramifiée K^{lr} . Or les rangs ℓ -adiques de ces dernières extensions (i.e. le nombre de \mathbb{Z}_{ℓ} -extensions linéairement indépendantes qu'elles contiennent) sont indépendants du nombre premier ℓ (du moins sous les conjectures standard), puisqu'on a $\text{rg Gal}(K^{lr}/K) = c + 1$ (sous la conjecture de Leopoldt) et $\text{rg Gal}(K^{lc}/K) = 1$ (sous celle de Gross). Mais il n'en va pas de même pour l'extension K^{cr} qui dépend effectivement de façon non triviale de la nature des places de K au-dessus de ℓ .

Ce dernier point apparaît clairement sur les deux exemples limites suivants :

Proposition 3. (i) *Supposons que K admette une unique place \mathfrak{l} au dessus de ℓ (autrement dit que ℓ ne se décompose pas dans l'extension K/\mathbb{Q}). Alors l'extension cyclotomiquement ramifiée maximale K^{cr} est de degré fini sur l'extension localement cyclotomique maximale K^{lc} . En particulier, si K vérifie la conjecture de Gross, le rang ℓ -adique du groupe de Galois $\text{Gal}(K^{cr}/K)$ est égal à 1.*

(ii) *Supposons au contraire que ℓ soit complètement décomposé dans l'extension K/\mathbb{Q} . Alors l'extension ℓ -ramifiée maximale K^{lr} est de degré fini sur l'extension cyclotomiquement ramifiée maximale K^{cr} . En particulier, si K vérifie la conjecture de Leopoldt, le rang ℓ -adique du groupe de Galois $\text{Gal}(K^{cr}/K)$ est égal à $1 + c$.*

Preuve. (i) Lorsque K admet une unique place \mathfrak{l} au-dessus de ℓ , le \mathbb{Z}_{ℓ} -module $\mathcal{U}_{\ell}\ell^{\mathbb{Z}_{\ell}}$ engendré par le sous-groupe unité $\mathcal{U}_{\ell} = \mathcal{U}_{\mathfrak{l}}$ et l'image du nombre ℓ est d'indice fini dans $\mathcal{R}_{\ell} = \mathcal{R}_{\mathfrak{l}}$. Et comme ℓ est une norme cyclotomique, il en résulte que $\tilde{\mathcal{U}}_{\ell}$ contient $\tilde{\mathcal{U}}_{\ell}\ell^{\mathbb{Z}_{\ell}}$ avec un indice fini.

(ii) Inversement, lorsque ℓ est complètement décomposé dans K/\mathbb{Q} , chaque complété $K_{\mathfrak{l}}$ au dessus de ℓ est égal à \mathbb{Q}_{ℓ} , et il suit : $\tilde{\mathcal{U}}_{\ell} = \prod_{\mathfrak{l}|\ell} \tilde{\mathcal{U}}_{\mathfrak{l}} = \prod_{\mathfrak{l}|\ell} \mu_{\mathfrak{l}}\ell_{\mathfrak{l}}^{\mathbb{Z}_{\ell}}$, où $\mu_{\mathfrak{l}}$ est le ℓ -groupe des racines de l'unité dans $K_{\mathfrak{l}} = \mathbb{Q}_{\ell}$ et $\ell_{\mathfrak{l}}$ l'image dans $\mathcal{R}_{\mathfrak{l}}$ du nombre premier ℓ . Il vient ainsi : $\widehat{\mathcal{U}}_{\mathfrak{l}} = \mu_{\mathfrak{l}}$, pour $\mathfrak{l}|\ell$; puis $\widehat{\mathcal{U}}\mathcal{R} = (\prod_{\mathfrak{p}|\ell} \mu_{\mathfrak{p}})\mathcal{R}$, et ce dernier groupe contient bien $(\prod_{\mathfrak{p}|\ell} \mu_{\mathfrak{p}})\mathcal{R}$ avec un indice fini.

Bien entendu, sous les conjectures d'indépendance ℓ -adique standard, il est possible de préciser ces résultats. Ainsi :

Proposition 4. *Lorsque K est une extension quadratique totalement imaginaire d'un sous-corps totalement réel K_+ qui vérifie la conjecture de Leopoldt (pour le nombre premier ℓ), le rang ℓ -adique du groupe de Galois $\text{Gal}(K^{cr}/K)$ est égal à $1 + s^-$, où s^- est le nombre de places sauvages de K_+ (i.e. de places au-dessus de ℓ) qui se décomposent dans K/K_+ .*

Preuve. Comparons K^{cr} au ℓ -corps des classes de Hilbert (au sens restreint) K^{nr} . Nous obtenons immédiatement :

$$\text{Gal}(K^{cr}/K^{nr}) \simeq \mathcal{UR}/\widehat{\mathcal{UR}} \simeq \mathcal{U}_\ell/\widehat{\mathcal{U}}_\ell \mathcal{E}_\ell,$$

si $\mathcal{E}_\ell = s_\ell(\mathcal{E})$ désigne l'image du ℓ -adifié $\mathcal{E} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E$ du groupe des unités globales dans celui $\mathcal{U}_\ell = \prod_{\ell|l} \mathcal{U}_l$ des unités semi-locales. Or, puisque nous ne sommes intéressés que par le rang ℓ -adique, nous pouvons raisonner à un fini près et écrire en particulier $\mathcal{U}_\ell \sim \mathcal{U}_\ell^+ \oplus \mathcal{U}_\ell^-$, en faisant apparaître les composantes propres de \mathcal{U}_ℓ pour l'action de la conjugaison complexe. Et nous avons ainsi :

- d'un côté $(\mathcal{U}_\ell/\widehat{\mathcal{U}}_\ell s_\ell(\mathcal{E}))^+ \sim \mathbb{Z}_\ell$, en vertu de la conjecture de Leopoldt ;
- de l'autre $(\mathcal{U}_\ell/\widehat{\mathcal{U}}_\ell s_\ell(\mathcal{E}))^- \sim (\mathcal{U}_\ell/\widehat{\mathcal{U}}_\ell)^- \simeq \mathbb{Z}_\ell^{s^-}$, en l'absence d'unités imaginaires ; d'où le résultat annoncé.

Corollaire 5. *Sous la conjecture de Leopoldt, le rang ℓ -adique du groupe de Galois $\text{Gal}(K^{cr}/K)$ est au plus 2 dans chacun des deux cas particuliers suivants :*

- (i) *Lorsque K est une extension quadratique totalement imaginaire d'un sous-corps totalement réel K_+ dont au plus une place au-dessus de ℓ est décomposée par la conjugaison complexe.*
- (ii) *Lorsque K possède au plus une place complexe.*

Preuve. C'est clair.

Remarque. Plusieurs familles infinies de corps qui satisfont l'hypothèse (ii) du corollaire sont connues pour vérifier également la conjecture de Leopoldt. Ainsi :

- (i) Tous les corps quadratiques.
- (ii) Tous les corps cubiques qui ne sont pas totalement réels, en particulier les corps cubiques purs $\mathbb{Q}[\sqrt[3]{m}]$, pour lesquels le nombre de Dirichlet $r+c-1$ vaut 1.
- (iii) Certaines familles de corps quintiques qui admettent S_5 pour groupe de Galois de leur clôture galoisienne (cf. [BS]).

3.- Critère arithmétique de semi-simplicité.

Considérons un instant une \mathbb{Z}_ℓ -extension arbitraire $K_\infty = \cup_{n \in \mathbb{N}} K_n$ d'un corps de nombres K . Pour chaque entier naturel n , notons $\mathcal{C}\ell_{K_n}$ le ℓ -groupe des classes de diviseurs du corps K_n (i.e. le ℓ -sous-groupe de Sylow de son groupe de classes d'idéaux pris au sens restreint), et écrivons

$$\mathcal{C}_{K_\infty} = \varprojlim \mathcal{C}\ell_{K_n}$$

leur limite pour le système projectif des applications normes, qui s'identifie, via l'isomorphisme du corps de classes, au groupe de Galois $\text{Gal}(K_\infty^{nr}/K_\infty)$ de la pro- ℓ -extension abélienne non ramifiée (aux places finies) maximale de K_∞ . Si γ désigne un générateur topologique du groupe procyclique $\Gamma = \text{Gal}(K_\infty/K)$, et $\Lambda = \mathbb{Z}_\ell[[\gamma - 1]]$ l'algèbre d'Iwasawa associée à Γ , le groupe obtenu \mathcal{C}_{K_∞} est un Λ -module noethérien et de torsion, et nous nous proposons d'étudier s'il est semi-simple en $\gamma - 1$ (autrement dit si $\omega_0 = \gamma - 1$ n'est pas un facteur carré de son polynôme minimal) ; et, plus généralement, s'il est semi-simple en $\omega_n = (\gamma^{\ell^n} - 1)/(\gamma^{\ell^{n-1}} - 1)$ pour $n \geq 1$ (autrement dit s'il est encore semi-simple en $\gamma^{\ell^n} - 1$ lorsqu'on l'étudie comme $\mathbb{Z}_\ell[[\gamma^{\ell^n} - 1]]$ -module).

Disons tout de suite que presque tous les résultats de semi-simplicité connus à ce jour reposent *in fine* sur le critère explicite ou implicite suivant :

Proposition 6. *Soit $K_\infty = \cup_{n \in \mathbb{N}} K_n$ une \mathbb{Z}_ℓ -extension d'un corps de nombres K , de groupe de Galois $\Gamma = \gamma^{\mathbb{Z}_\ell}$. Si les deux conditions suivantes sont vérifiées :*

- i) Les places au-dessus de ℓ sont finiment décomposées dans l'extension procyclique K_∞/K ;*
- (ii) La pro- ℓ -extension abélienne maximale de K (resp. de K_n) qui est complètement décomposée sur K_∞ aux places qui divisent ℓ et non ramifiée partout, est de degré fini sur K_∞ ;*

Alors le Λ -module $\mathcal{C}_{K_\infty} = \varprojlim \mathcal{C}_{K_n}$ est semi-simple en $\gamma - 1$ (resp. en $\gamma^{\ell^n} - 1$).

Remarques. (i) Lorsque K_∞ est la \mathbb{Z}_ℓ -extension cyclotomique de K , la condition (ii) ci-dessus est l'une des formulations équivalente de la conjecture de Gross généralisée (cf. par exemple, [J₃] IV.2.3 §b) pour le corps K (resp. K_n). Elle est donc en particulier satisfaite lorsque K est abélien sur \mathbb{Q} . Comme expliqué plus loin elle peut être cependant en défaut pour certaines \mathbb{Z}_ℓ -extensions non cyclotomiques lors même que K est abélien sur \mathbb{Q} .

(ii) La condition (ii) est toujours vérifiée, en revanche, lorsqu'il n'existe qu'une seule place de K qui se ramifie dans K_∞ : Dans ce dernier cas, en effet, la formule des genres appliquée à l'extension procyclique K_∞/K (cf. [J₃], III.2.2 §b) montre directement que le groupe $\mathcal{C}_{K_\infty}/\mathcal{C}_{K_\infty}^{\gamma-1}$ est pseudo-nul.

Preuve. Pour chaque $n \geq 0$, notons \mathcal{S}_{K_n} le sous-groupe de \mathcal{C}_{K_n} engendré par les classes des diviseurs construits sur les places au-dessus de ℓ , et $\mathcal{C}'_{K_n} = \mathcal{C}_{K_n}/\mathcal{S}_{K_n}$ le quotient correspondant. Par passage à la limite projective, nous obtenons la suite exacte courte de Λ -modules (cf. [J₃], prop. IV.2.5) :

$$1 \longrightarrow \mathcal{S}_{K_\infty} = \varprojlim \mathcal{S}_{K_n} \longrightarrow \mathcal{C}_{K_\infty} = \varprojlim \mathcal{C}_{K_n} \longrightarrow \mathcal{C}'_{K_\infty} = \varprojlim \mathcal{C}'_{K_n} \longrightarrow 1$$

qui nous montre que le polynôme caractéristique du Λ -module \mathcal{C}_{K_∞} est le produit de ceux associés aux Λ -modules \mathcal{S}_{K_∞} et \mathcal{C}'_{K_∞} . Or, écrivons γ_n pour γ^{ℓ^n} :

- d'un côté, l'hypothèse (i) nous assure que le terme de gauche \mathcal{S}_{K_∞} est annulé par $\gamma_n - 1$ dès que n est assez grand, et que de ce fait il est semi-simple en $\gamma_n - 1$, quel que soit n .

- de l'autre, le quotient $\mathcal{C}'_{K_\infty}/\mathcal{C}'_{K_\infty}{}^{\gamma_n-1}$ s'interprète par la théorie des genres comme le groupe de Galois $\text{Gal}(K_\infty^{cd} \cap K_n^{ab}/K_\infty)$ attaché à la pro- ℓ -extension abélienne maximale de K_n qui est non ramifié partout et complètement décomposée aux places sauvages sur K_∞ ; et l'hypothèse (ii) revient à affirmer que le polynôme caractéristique du terme de droite \mathcal{C}'_{K_∞} est étranger à $\gamma - 1$ (resp. $\gamma_n - 1$).

Ce résultat nous conduit ainsi à la définition suivante :

Définition 7. *Nous disons qu'une \mathbb{Z}_ℓ -extension K_∞ d'un corps de nombres est arithmétiquement semi-simple lorsqu'elle satisfait les deux conditions de la proposition 6.*

Cela posé nous avons :

Théorème 8. *Si K_∞ est une \mathbb{Z}_ℓ -extension cyclotomiquement ramifiée d'un corps de nombres K , la pro- ℓ -extension abélienne cyclotomiquement ramifiée maximale K^{cr} de K est exactement la pro- ℓ -extension abélienne maximale de K qui est non ramifiée sur K_∞ .*

En particulier, si $\text{Gal}(K^{cr}/K)$ est de rang ≤ 2 (autrement dit si K admet au plus deux \mathbb{Z}_ℓ -extensions cyclotomiquement ramifiées qui soient linéairement indépendantes), les \mathbb{Z}_ℓ -extensions cyclotomiquement ramifiées de K sont arithmétiquement semi-simples si et seulement si K vérifie la conjecture de Gross (pour le nombre premier ℓ).

Preuve. Lorsque $\text{Gal}(K^{cr}/K)$ est de rang 1, le corps K admet une unique \mathbb{Z}_ℓ -extension cyclotomiquement ramifiée, à savoir la cyclotomique K^c , et celle-ci vérifie alors trivialement la conjecture de Gross, puisque la pro- ℓ -extension abélienne maximale K^{lc} de K qui est complètement décomposée sur K^c est contenue dans K^{cr} , donc de degré fini sur K^c .

En dehors de ce cas particulier, K admet des \mathbb{Z}_ℓ -extensions cyclotomiquement ramifiées K_∞ distinctes de la cyclotomique K^c . Celles-ci sont infiniment ramifiées aux places sauvages et contenues dans K^{cr} . Par suite, pour chaque place \mathfrak{l} de K au-dessus de ℓ , le groupe d'inertie $I_{\mathfrak{l}}(K^{cr}/K)$, qui est procyclique, rencontre trivialement $\text{Gal}(K^{cr}/K_\infty)$, ce qui signifie que K^{cr} est non ramifié en \mathfrak{l} (et donc partout) sur K_∞ , et elle est évidemment maximale sous ces conditions (sans quoi nous pourrions la grossir en une extension N abélienne sur K et non ramifiée sur K^{cr} , donc finalement sur K^c).

Ainsi, lorsque $\text{Gal}(K^{cr}/K)$ est de rang 2, la conjecture de Gross (pour le corps K et le nombre premier ℓ), qui affirme que la sous-extension maximale K^{lc} de K^{cr} qui est complètement décomposée sur K^c est de degré fini sur K^c , revient à postuler qu'il existe au moins une place \mathfrak{l} de K au dessus de ℓ qui n'est pas infiniment décomposée dans K^{cr}/K^c , autrement dit dont le groupe de décomposition $D_{\mathfrak{l}}(K^{cr}/K)$ est d'indice fini dans $\text{Gal}(K^{cr}/K)$. Pour chaque \mathbb{Z}_ℓ -sous-extension K_∞ de K^{cr} , la place \mathfrak{l} est donc finiment décomposée dans K^{cr}/K_∞ , et la sous-extension maximale de K^{cr} qui est complètement décomposée sur K_∞ est en particulier de degré fini sur K_∞ , comme annoncé.

Remarques. (i) Sous la conjecture de Leopoldt, la proposition 4 montre que la condition $\text{rg Gal}(K^{cr}/K) = 2$ a lieu, pour K extension quadratique totalement imaginaire d'un sous-corps K_+ totalement réel, lorsqu'il existe exactement une place de K_+ au-dessus de ℓ qui se décompose dans K/K_+ (cf. Cor. 5).

(ii) Si $\text{rg Gal}(K^{cr}/K)$ est strictement plus grand que 2, la condition de semi-simplicité pour une \mathbb{Z}_ℓ -extension cyclotomiquement ramifiée K_∞ de K revient à affirmer que les restrictions à $\text{Gal}(K^{cr}/K_\infty)$ des sous-groupes de décomposition $D_l(K^{cr}/K)$ attachés aux places sauvages engendrent un sous-module d'indice fini de $\text{Gal}(K^{cr}/K_\infty)$. La conjecture de Gross postule que c'est vrai pour $K_\infty = K^c$, mais ne permet pas de conclure en dehors de ce cas, sans hypothèse supplémentaire.

Bien entendu, le résultat ci-dessus paraît trop restrictif pour permettre d'avancer une conjecture suffisamment générale, puisque l'hypothèse faite ($\text{rg Gal}(K^{cr}/K) \leq 2$) implique des contraintes sévères sur l'arithmétique des extensions étudiées.

Aussi n'est-il pas inutile d'examiner avec une attention particulière le cas abélien, pour lequel les conjectures ℓ -adiques standard (Leopoldt & Gross) se trouvent satisfaites en vertu du théorème de Baker-Brumer (cf. [Br]).

4.- Etude du cas absolument abélien.

Dans ces dernières sections, K désigne désormais un corps de nombres imaginaire absolument abélien, K_+ son sous-corps réel maximal, et $\Delta = \text{Gal}(K/\mathbb{Q})$ son groupe de Galois.

Pour des raisons de commodité technique, nous supposons que le degré $d = [K : \mathbb{Q}]$ de K est étranger à ℓ et, plus précisément, que l'exposant du groupe abélien Δ divise $\ell - 1$, autrement dit que l'algèbre ℓ -adique du groupe Δ est produit direct de d exemplaires de \mathbb{Z}_ℓ :

$$\mathbb{Z}_\ell[\Delta] \simeq \bigoplus_{\varphi \in \Delta^*} \mathbb{Z}_\ell e_\varphi,$$

les idempotents primitifs attachés à cette décomposition étant indexés par le groupe Δ^* des caractères ℓ -adiques irréductibles du groupe Δ et donnés par la formule :

$$e_\varphi = \frac{1}{d} \sum_{\tau \in \Delta} \varphi(\tau^{-1})\tau.$$

Pour chaque place p de \mathbb{Q} , désignons par Δ_p le sous-groupe de décomposition associé, notons $\Delta_p^\perp = \{\varphi \in \Delta^* \mid (\varphi(\Delta_p) = 1)\}$ son orthogonal dans Δ^* , et écrivons :

$$\chi_p = \text{Ind}_{\Delta_p}^\Delta 1_{\Delta_p} = \sum_{\varphi \in \Delta_p^\perp} \varphi$$

l'induit à Δ du caractère de la représentation unité du sous-groupe Δ_p . En particulier, lorsque p est la place à l'infini, il est commode de dire réels les caractères

irréductibles représentés dans χ_∞ , qui prennent la valeur $+1$ la conjugaison complexe, et imaginaires les autres (i.e. ceux représentés dans $\chi_{\text{rég}} - \chi_\infty$), qui prennent la valeur -1 sur la conjugaison complexe.

Le résultat suivant est alors essentiellement bien connu (cf. [J₁] ou [CK₁]) :

Proposition 9. *Avec les notations ci-dessus, le groupe de Galois $\text{Gal}(Z/K)$ de la composée Z des \mathbb{Z}_ℓ -extensions de K est un $\mathbb{Z}_\ell[\Delta]$ -module projectif de caractère $\chi_{\text{rég}} - \chi_\infty + 1$.*

En d'autres termes, le corps K possède exactement $\frac{d}{2} + 1$ \mathbb{Z}_ℓ -extensions qui sont absolument galoisiennes, à savoir :

- (i) *La cyclotomique K^c , qui correspond au caractère unité, et dont le groupe de Galois*

$$\text{Gal}(K^c/\mathbb{Q}) \simeq \Gamma \times \Delta$$

est abélien, produit direct du groupe procyclique $\Gamma = \gamma^{\mathbb{Z}_\ell}$ isomorphe à \mathbb{Z}_ℓ par un exemplaire de Δ .

- (ii) *Les $\frac{d}{2}$ \mathbb{Z}_ℓ -extensions K_ω , indexées par les caractères ℓ -adiques irréductibles imaginaires de Δ , et dont les groupes de Galois*

$$\text{Gal}(K_\omega/\mathbb{Q}) \simeq \Gamma_\omega \times_\omega \Delta$$

sont métaprocycliques, produits semi-directs d'un groupe procyclique $\Gamma_\omega = \gamma_\omega^{\mathbb{Z}_\ell}$ isomorphe à \mathbb{Z}_ℓ par un exemplaire de Δ avec les relations :

$$\tau \gamma_\omega \tau^{-1} = \gamma_\omega^{\omega(\tau)}, \quad \forall \tau \in \Delta.$$

Preuve (d'après [J₁]). Comme nous ne sommes intéressés que par les caractères des $\mathbb{Z}_\ell[\Delta]$ -modules étudiés, nous pouvons raisonner à un fini près en remplaçant Z par la pro- ℓ -extension abélienne ℓ -ramifiée maximale $K^{\ell r}$ et K par la sous-extension non ramifiée K^{nr} de $K^{\ell r}$, i.e. $\text{Gal}(Z/K)$ par $\text{Gal}(K^{\ell r}/K^{nr}) \simeq \mathcal{U}_\ell/\mathcal{E}_\ell$ (cf. §1, rem. (iv)). Cela étant, le caractère du groupe des unités semi-locales³ \mathcal{U}_ℓ est le caractère régulier $\chi_{\text{rég}}$; et celui de l'image $\mathcal{E}_\ell = s_\ell(\mathcal{E})$ du tensorisé $\mathcal{E} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} E$ du groupe des unités globales est $\chi_\infty - 1$ en vertu du théorème de représentation de Herbrand et du fait que la conjecture de Leopoldt est ici vérifiée. D'où le résultat annoncé.

Considérons maintenant les $\frac{d}{2} + 1$ \mathbb{Z}_ℓ -extensions ainsi obtenues, et comparons celles qui sont cyclotomiquement ramifiées (au sens de la définition 1) et celles qui sont semi-simples (au sens de la définition 7). Hormis le cas spécial où le sous-corps réel K_+ n'admet qu'une seule place sauvage, la répartition des extensions K_ω est en fait extrêmement simple, puisque les résultats de [J₂] et de [Ki] peuvent être complétés comme suit :

³Par caractère d'un $\mathbb{Z}_\ell[\Delta]$ -module noethérien M , nous entendons le caractère du $\mathbb{Q}_\ell[\Delta]$ -module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} M$. Deux $\mathbb{Z}_\ell[\Delta]$ -modules noethériens sont ainsi pseudo-isomorphes si et seulement s'ils définissent le même caractère.

Théorème 10. *Soit K un corps abélien imaginaire d'exposant divisant $\ell - 1$, dont le sous-corps réel maximal K_+ possède au moins deux places sauvages (autrement dit tel que la place ℓ admette effectivement de la décomposition dans K_+/\mathbb{Q}). Alors pour chaque caractère ℓ -adique imaginaire irréductible ω du groupe $\Delta = \text{Gal}(K/\mathbb{Q})$, la nature de la \mathbb{Z}_ℓ -extension absolument galoisienne associée K_ω est gouvernée par l'alternative suivante :*

- (i) *ou bien ω divise χ_ℓ , et l'extension K_ω est cyclotomiquement ramifiée et arithmétiquement semi-simple ;*
- (ii) *ou bien ω ne divise pas χ_ℓ , et K_ω n'est ni cyclotomiquement ramifiée ni arithmétiquement semi-simple.*

Remarques. (i) Le degré du caractère de décomposition χ_ℓ est le nombre $s = s^+ + s^-$ de places sauvages dans K ; la quantité $s^+ = \deg \chi_\ell^+$ mesure le nombre de places sauvages dans K_+ , et la quantité $s^- = \deg \chi_\ell^-$ le nombre de places sauvages de K_+ qui sont décomposées par la conjugaison complexe. Dans le cas spécial $s^+ = 1$, on a $s^- \leq 1$ et K possède donc au plus une \mathbb{Z}_ℓ -extension absolument galoisienne cyclotomiquement ramifiée en sus de la cyclotomique K^c . Elle est arithmétiquement semi-simple en vertu du théorème 8.

(ii) la \mathbb{Z}_ℓ -extension cyclotomique K^c , qui correspond elle au caractère unité, est évidemment cyclotomiquement ramifiée. Elle est également semi-simple en vertu du résultat de Greenberg (cf. [Gr]).

5.- Démonstration du théorème énoncé.

Déterminons d'abord le caractère du groupe de galois $\text{Gal}(K^{cr}/K)$ de la pro- ℓ -extension abélienne cyclotomiquement ramifiée K^{cr} de K . Introduisons pour cela la sous-extension non ramifiée maximale K^{nr} de K^{cr} . D'après le théorème 2, la théorie ℓ -adique du corps de classes nous donne l'isomorphisme

$$\text{Gal}(K^{cr}/K^{nr}) \simeq \mathcal{U}\mathcal{R}/\widehat{\mathcal{U}}\mathcal{R} \simeq \mathcal{U}_\ell/\widehat{\mathcal{U}}_\ell \mathcal{E}_\ell,$$

où $\mathcal{U}_\ell = \prod_{\mathfrak{l}|\ell} \mathcal{U}_\mathfrak{l}$ est le groupe des unités semi-locales, $\widehat{\mathcal{U}}_\ell = \prod_{\mathfrak{l}|\ell} \widehat{\mathcal{U}}_\mathfrak{l}$ le sous-groupe des normes cyclotomiques dans \mathcal{U}_ℓ , et \mathcal{E}_ℓ l'image semi-locale du tensorisé $\mathcal{E} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E$ du groupe des unités globales. L'expression explicite des valeurs absolues ℓ -adiques montre alors que $\widehat{\mathcal{U}}_\ell$ est le noyau dans \mathcal{U}_ℓ de la norme locale $N_\ell = \sum_{\tau \in \Delta_\ell} \tau = |\Delta_\ell| \sum_{\varphi \in \Delta_\ell^\perp} e_\varphi$, autrement dit que le quotient $\mathcal{U}_\ell/\widehat{\mathcal{U}}_\ell$ est un $\mathbb{Z}_\ell[\Delta]$ -module projectif de caractère χ_ℓ .

Les \mathbb{Z}_ℓ -extensions de K qui sont absolument galoisiennes et cyclotomiquement ramifiées sur K sont ainsi exactement celles attachées aux caractères ℓ -adiques irréductibles ω de Δ qui sont représentés dans χ_ℓ mais non dans $\chi_\infty - 1$, c'est-à-dire en fin de compte :

- la cyclotomique K^c , qui correspond au caractère unité,
- et celles métaprocycliques K_ω qui sont associées aux diviseurs imaginaires du caractère χ_ℓ .

Reste alors à voir que celles-ci sont semi-simples, et que les autres ne le sont pas! Introduisons pour cela quelques notations : Faisons choix dans le sous-corps de décomposition K^{Δ_ℓ} de ℓ dans K d'un générateur ε d'une puissance principale non nulle de l'un des idéaux \mathfrak{l}_\circ au-dessus de ℓ , et notons $V = \varepsilon^{\mathbb{Z}[\Delta]}$ le $\mathbb{Z}[\Delta]$ -module multiplicatif engendré par ε , puis $\mathcal{V} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} V$ son tensorisé ℓ -adique, et \mathcal{V}_ℓ l'image de \mathcal{V} dans $\mathcal{R}_\ell = \prod_{\mathfrak{l}|\ell} \mathcal{R}_\mathfrak{l}$, qui est donc un sous-module projectif de caractère χ_ℓ . En particulier, \mathcal{R}_ℓ contient $\mathcal{U}_\ell \mathcal{V}_\ell$ comme sous-module d'indice fini.

Cela posé, pour chaque caractère ℓ -adique irréductible ω de Δ , unité ou imaginaire, et pour chaque place \mathfrak{l} de K au-dessus de ℓ , désignons par $\mathcal{R}_\mathfrak{l}^\omega$ le sous-module fermé de $\mathcal{R}_\mathfrak{l}$ formé des normes locales en \mathfrak{l} dans l'extension procyclique K_ω/K ; notons $\mathcal{U}_\mathfrak{l}^\omega = \mathcal{R}_\mathfrak{l}^\omega \cap \mathcal{U}_\mathfrak{l}$ son sous-groupe unité ; et formons les groupes semi-locaux $\mathcal{R}_\ell^\omega = \prod_{\mathfrak{l}|\ell} \mathcal{R}_\mathfrak{l}^\omega$ et $\mathcal{U}_\ell^\omega = \prod_{\mathfrak{l}|\ell} \mathcal{U}_\mathfrak{l}^\omega$. Distinguons alors deux cas suivant ω divise χ_ℓ ou non :

Lemme 11. *Supposons $\omega|\chi_\ell$ (i.e. $K_\omega \subset K^{cr}$). Dans ce cas le sous-module $\mathcal{V}_\ell \mathcal{R}_\ell^\omega$ est un pseudo-hyperplan⁴ du \mathbb{Z}_ℓ -module \mathcal{R}_ℓ . En particulier, les groupes de décomposition $D_\mathfrak{l}(K^{cr}/K_\omega)$ attachés aux places au-dessus de ℓ dans l'extension K^{cr}/K_ω engendrent un sous-groupe d'indice fini de $\text{Gal}(K^{cr}/K_\omega)$; de sorte que la \mathbb{Z}_ℓ -extension K_ω/K est bien semi-simple au sens de la définition 7.*

Preuve. Puisque \mathcal{R}_ℓ contient $\mathcal{U}_\ell \mathcal{V}_\ell$ comme sous-module d'indice fini, la première assertion du lemme revient à affirmer que $\mathcal{V}_\ell \mathcal{R}_\ell^\omega \cap \mathcal{U}_\ell$ est un pseudo-hyperplan de \mathcal{U}_ℓ . Or l'hypothèse $K_\omega \subset K^{cr}$, transportée par le corps de classes, nous donne $\widehat{\mathcal{U}}_\ell \subset \mathcal{R}_\ell^\omega$ donc $\widehat{\mathcal{U}}_\ell \subset (\mathcal{V}_\ell \mathcal{R}_\ell^\omega \cap \mathcal{U}_\ell)$. Ainsi, comme \mathcal{U}_ℓ est un $\mathbb{Z}_\ell[\Delta]$ -module de caractère régulier, et $\widehat{\mathcal{U}}_\ell$ son sous-module annulé par $N_\ell = |\Delta_\ell| \sum_{\varphi \in \Delta^\perp} e_\varphi$, tout revient à vérifier que $\mathcal{V}_\ell \mathcal{R}_\ell^\omega \cap \mathcal{U}_\ell$ ne peut être simultanément annulé par deux idempotents distincts e_φ et e_ψ associés à deux caractères de Δ_ℓ^\perp . Observons pour cela que la \mathbb{Z}_ℓ -extension K_ω/K étant presque totalement ramifiée, nous pouvons trouver un élément π_ω de $\mathcal{R}_{\mathfrak{l}_\circ}^\omega$ qui n'est pas dans $\mathcal{U}_{\mathfrak{l}_\circ}$, disons de valuation $v_0 > 0$, de sorte que la quantité :

$$\eta = \varepsilon^{v_0} \pi_\omega^{-v_{\mathfrak{l}_\circ}(\varepsilon)} \quad \text{est dans} \quad \mathcal{U}_\ell \cap \mathcal{V}_\ell \mathcal{R}_\ell^\omega.$$

Si donc nous avons $\eta^{e_\varphi} = \eta^{e_\psi} = 1$, et, par suite, $\eta^{e_\varphi - e_\psi} = 1$, pour deux caractères distincts φ et ψ de Δ_ℓ^\perp , nous obtiendrons, en prenant les \mathfrak{l}_\circ -composantes puis les logarithmes \mathfrak{l}_\circ -adiques :

$$0 = \sum_{\tau \in \Delta_\ell} (\varphi(\tau^{-1}) - \psi(\tau^{-1})) \text{Log}_{\mathfrak{l}_\circ} \eta^\tau = \sum_{\tau \in \Delta_\ell \setminus \{1\}} (\varphi(\tau^{-1}) - \psi(\tau^{-1})) \text{Log}_{\mathfrak{l}_\circ} \varepsilon^\tau,$$

une combinaison linéaire à coefficients algébriques de logarithmes \mathfrak{l}_\circ -adiques d'unités \mathfrak{l}_\circ -adiques algébriques et \mathbb{Z} -multiplicativement indépendantes, contrairement au théorème de Baker-Brumer ; ce qui établit la première assertion.

⁴Par pseudo-hyperplan d'un \mathbb{Z}_ℓ -module M nous entendons tout sous-module N tel que le quotient M/N soit pseudo-isomorphe à \mathbb{Z}_ℓ .

La seconde en résulte aussitôt, puisque dans le pseudo-isomorphisme donné par le corps de classes :

$$\text{Gal}(K^{cr}/K) \sim \mathcal{U}_\ell/\tilde{\mathcal{U}}_\ell \mathcal{E}_\ell \sim \mathcal{R}_\ell/\tilde{\mathcal{U}}_\ell \mathcal{V}_\ell \mathcal{E}_\ell ,$$

le sous-module engendré par les sous-groupes de décomposition $D_\ell(K^{cr}/K_\omega)$ correspond à l'image $\mathcal{R}_\ell^\omega(\tilde{\mathcal{U}}_\ell \mathcal{V}_\ell \mathcal{E}_\ell)/\tilde{\mathcal{U}}_\ell \mathcal{V}_\ell \mathcal{E}_\ell$ du sous-groupe \mathcal{R}_ℓ^ω de \mathcal{R}_ℓ .

Lemme 12. *Supposons $\omega \nmid \chi_\ell$ (i.e. $K_\omega \not\subset K^{cr}$). Dans ce cas, le sous-module $\mathcal{V}_\ell \mathcal{U}_\ell^\omega$ est d'indice fini dans le groupe $\mathcal{V}_\ell \mathcal{R}_\ell^\omega$. En particulier la pro- ℓ -extension abélienne maximale K_ω^{nr} de K_ω qui est non ramifiée est de degré fini sur celle K_ω^{cd} qui est non-ramifiée et ℓ -décomposée ; de sorte que la condition de semi-simplicité $[K_\omega^{cd} : K_\omega] < \infty$ est alors vérifiée si et seulement si on a $\chi_\ell \wedge \chi_\infty = 1$, c'est à dire lorsqu'il n'existe qu'une seule place au-dessus de ℓ dans le sous-corps réel maximal K_+ de K .*

Preuve. Partons du pseudo-isomorphisme $\text{Gal}(Z/K) \sim \mathcal{U}_\ell/\mathcal{E}_\ell$ donné par le corps de classes. Puisque l'hyperplan $\text{Gal}(Z/K_\omega)$ de $\text{Gal}(Z/K)$ qui fixe K_ω est le noyau de l'idempotent e_ω , et que ω n'est pas représenté dans \mathcal{E}_ω , le sous-groupe \mathcal{U}_ℓ^ω des unités locales de \mathcal{U}_ℓ qui sont normes dans l'extension procyclique K_ω/K est encore le noyau dans \mathcal{U}_ℓ cet idempotent. En particulier, le groupe semi-local $\mathcal{U}_\ell^\omega = \prod_{\mathfrak{l}|\ell} \mathcal{U}_\ell^\omega$ est donc le sous-module pur de \mathcal{U}_ℓ de caractère :

$$\omega(\chi_{\text{rég}} - \chi_\ell) = \chi_{\text{rég}} - \omega\chi_\ell .$$

Définissons alors η comme précédemment. Puisque χ_ℓ et $\omega\chi_\ell$ sont étrangers par hypothèse, il suit que \mathcal{U}_ℓ^ω contient nécessairement le sous-module $\eta^{\mathbb{Z}_\ell[\Delta]}$ engendré par η . Et le \mathbb{Z}_ℓ -module $\mathcal{U}_{\mathfrak{l}_\circ}^\omega \cdot \pi_\omega^{v_{\mathfrak{l}_\circ}(\varepsilon)}$, qui est d'indice fini dans $\mathcal{R}_{\mathfrak{l}_\circ}$, est ainsi contenu dans $\mathcal{V}_\ell \mathcal{U}_\ell^\omega$. Transportée par le corps de classes, cette inclusion nous dit alors que le sous-groupe de décomposition de la place \mathfrak{l}_\circ dans l'extension non ramifiée K_ω^{nr}/K_ω est fini, autrement dit que K_ω^{nr} est de degré fini sur K_ω^{cd} .

Cela étant, comme le groupe de Galois $\text{Gal}(K_\omega^{nr}/K) \sim \mathcal{U}_\ell/\mathcal{U}_\ell^\omega \mathcal{E}_\ell$ a pour caractère $\omega\chi_\ell \wedge (1 + \omega\chi_\infty) = \omega(\chi_\ell \wedge \chi_\infty)$, la condition de semi-simplicité $[K_\omega^{cd} : K_\omega] < \infty$, qui s'écrit ici $[K_\omega^{nr} : K_\omega] < \infty$, se lit en termes de caractère : $\omega = \omega(\chi_\ell \wedge \chi_\infty)$, i.e. $\chi_\ell \wedge \chi_\infty = 1$, et exprime simplement que Δ_ℓ et Δ_∞ engendrent conjointement Δ ou, si l'on préfère, qu'il n'existe qu'une seule place au-dessus de ℓ dans le sous-corps réel maximal K_+ de K .

6.- Semi-simplicité algébrique et semi-simplicité arithmétique.

Il est naturel de se demander si le critère suffisant de semi-simplicité donné dans la section 3 est également nécessaire, autrement dit si toute \mathbb{Z}_ℓ -extension K_∞ d'un corps de nombres qui est algébriquement semi-simple (au sens de l'introduction) l'est encore arithmétiquement (i.e. au sens de la définition 7). Pour aborder cette question, il est alors essentiel de disposer d'un procédé permettant de construire des \mathbb{Z}_ℓ -extensions qui ne soient pas algébriquement semi-simples, ce que donne précisément la théorie des genres :

Supposons toujours K_∞ métapro-cyclique sur \mathbb{Q} ; conservons les notations de la section 4 et notons en particulier ω le caractère ℓ -adique qui définit l'action de

$\Delta = \text{Gal}(K/\mathbb{Q})$ sur $\Gamma = \text{Gal}(K_\infty/K)$. Observons maintenant que si le groupe de Galois \mathcal{C}_{K_∞} est semi-simple en $\gamma-1$, son quotient des genres ${}^\Gamma\mathcal{C}_{K_\infty} = \mathcal{C}_{K_\infty}/\mathcal{C}_{K_\infty}^{\gamma-1}$ et son sous-groupe ambige $\mathcal{C}_{K_\infty}^\Gamma$ sont alors pseudo-isomorphes comme $\mathbb{Z}_\ell[\Delta]$ -modules donc définissent le même caractère. Or celui-ci est bien connu : D'après [J₃] (cf. th.III.2.21), le caractère du quotient des genres est le p.g.c.d.

$$\beta = \omega(\chi_\ell - 1) \wedge \omega\chi_\infty ,$$

tandis que celui du sous-groupe ambige est donné, par une extension convenable de la classique formule de Chevalley (cf. [J₃], th.III.1.20), comme somme de deux caractères entiers, par la formule

$$\alpha = (\chi_\ell - \chi_1\omega^{-1}) + (\chi_2\omega^{-1} - ((\chi_\ell - 1) \wedge \chi_\infty)\omega^{-1}) ,$$

où χ_1 et χ_2 sont les caractères respectifs des groupes de cohomologie $H^1(\Gamma, \mathcal{E}_{K_\infty})$ et $H^2(\Gamma, \mathcal{E}_{K_\infty})$ construits sur le tensorisé ℓ -adique du groupe des unités de K_∞ . Et comme le caractère unité n'est pas représenté dans χ_2 , l'inégalité résultante

$$\alpha \leq \chi_\ell + \chi_2 \omega^{-1} ,$$

montre que l'inverse ω^{-1} du caractère ω n'est pas représenté dans α , dès qu'il ne l'est pas dans χ_ℓ , en d'autres termes que l'on a :

$$\langle \alpha, \omega^{-1} \rangle = 0, \quad \text{pour } \omega \nmid \chi_\ell ;$$

tandis que l'expression de β donnée ci-dessus conduit à l'égalité :

$$\langle \beta, \omega^{-1} \rangle = 1, \quad \text{pour } \omega^2 \mid (\chi_\ell - 1) ,$$

puisque la condition $\omega^2 \mid \chi_\infty$ est toujours vérifiée.

Telle est la clef des premiers contre-exemples produits dans [J₂] et repris sous une forme générale sensiblement différente par Kisilevsky dans [Ki]. En résumé, le théorème principal énoncé dans la section 4 peut donc être précisé comme suit :

Scolie 13. *Sous les hypothèses du théorème 10, la \mathbb{Z}_ℓ -extension métaprocyclique K_ω attachée au caractère ℓ -adique imaginaire irréductible ω n'est pas algébriquement semi-simple dès lors que ω vérifie les deux conditions :*

(i) $\omega \nmid \chi_\ell$, autrement dit K_ω n'est pas arithmétiquement semi-simple ;

(ii) $\omega^2 \mid (\chi_\ell - 1)$.

Remarque. La théorie des genres ne permet pas de conclure si l'hypothèse (ii) est en défaut. Par exemple, lorsque l'ordre du sous-groupe de décomposition Δ_ℓ est impair, on a $\omega \mid_{\Delta_\ell} \neq 1 \Leftrightarrow \omega^2 \mid_{\Delta_\ell} \neq 1$ i.e. $\omega \nmid \chi_\ell \Leftrightarrow \omega^2 \nmid \chi_\ell$, et les conditions (i) et (ii) sont incompatibles.

Lorsque Δ_ℓ est pair, en revanche, les conditions (i) et (ii) expriment que ω doit être un caractère de Δ qui n'est pas d'ordre 2 (c'est-à-dire que l'extension K_ω/\mathbb{Q} ne provient pas, par composition avec une extension absolument abélienne, d'une extension prodiédrale de \mathbb{Q}), mais dont la restriction au sous-groupe Δ_ℓ est d'ordre 2.

RÉFÉRENCES

- [Br] A. BRUMER, *On the units of algebraic number fields*, *Mathematica* **14** (1967), 121–124.
- [BS] J. BUCHMANN & J. SANDS, *Leopoldt's conjecture in parametrized families*, *Proc. Amer. Math. Soc.* **104** (1988), 43–49.
- [CK₁] J. CARROLL & H. KISILEVSKY, *On Iwasawa's λ invariant for certain \mathbb{Z}_p -extensions*, *Acta Arith.* **40** (1981), 1–8.
- [CK₂] J. CARROLL & H. KISILEVSKY, *On the Iwasawa invariants of certain \mathbb{Z}_p -extensions*, *Compositio Math.* **49** (1983), 217–229.
- [FG] L.J. FEDERER & B.H. GROSS, (with an appendix by W. Sinnott) *Regulators and Iwasawa modules*, *Invent. Math.* **62** (1981), 443–457.
- [Gr] R. GREENBERG, *On a certain ℓ -adic representation*, *Invent. Math.* **21** (1973), 117–124.
- [Iw] K. IWASAWA, *On \mathbb{Z}_ℓ -extensions of algebraic number fields*, *Ann. of Math.* **98** (1973), 243–326.
- [J₁] J.-F. JAULENT, *Théorie d'Iwasawa des tours métabéliennes*, *Sém. Th. Nombres Bordeaux* (1980/81), exp. n°21.
- [J₂] J.-F. JAULENT, *Sur la théorie des genres dans les tours métabéliennes*, *Sém. Th. Nombres Bordeaux* (1981/82), exp. n°24.
- [J₃] J.-F. JAULENT, *L'arithmétique des ℓ -extensions (Thèse d'Etat)*, *Pub. Math. Fac. Sci. Besançon Théor. Nombres* 1984-85 & 1985/86, fasc. 1 (1986), 1–349.
- [Ki] H. KISILEVSKY, *Some non-semi-simple Iwasawa modules*, *Compositio Math.* **49** (1983), 399–404.

Jean-François JAULENT
 Université Bordeaux 1
 Institut de Mathématiques
 351, cours de la Libération
 F-33405 TALENCE Cedex
 jaulent@math.u-bordeaux.fr

Jonathan W. SANDS
 Department of Mathematics
 and Statistics
 University of Vermont
 16 Colchester Avenue
 BURLINGTON 05405, USA