Capitulation des classes logarithmiques et étude de certaines tours de corps de nombres

Christophe Brighi

Thèse présentée à l'UNIVERSITÉ Paul-Verlaine - METZ
pour l'obtention du
doctorat de l'Université de Metz
en Mathématiques
spécialité : Mathématiques pures

par **Christophe BRIGHI**

Titre de la thèse :

CAPITULATION DES CLASSES LOGARITHMIQUES ET ÉTUDE DE CERTAINES TOURS DE CORPS DE NOMBRES

Soutenue le 08 octobre 2007 devant le jury composé de :

E.-U. GEKELER, Professeur à l'Université des Saarlandes.
J.-F. JAULENT, Professeur à l'Université de Bordeaux I. Rapporteur.
C. MAIRE, Professeur à l'Université de Franche-Comté. Rapporteur.
C. MOVAHHEDI, Professeur à l'Université de Limoges.
F. SORIANO-GAFIUK, Professeure à l'IUFM de Lorraine.

Remerciements

Ma reconnaissance va en premier lieu à Florence Soriano-Gafiuk qui a dirigé ma thèse, pour avoir porté ce travail à bout de bras, pour avoir su me remotiver dans mes moments de découragement, pour sa gentillesse, sa patience et sa disponibilité.

A l'origine de ce travail, il y a les recherches de Jean-François Jaulent. Celui-ci a par ailleurs accepté d'être rapporteur et membre du jury. Je tiens à lui exprimer ici ma gratitude.

Je remercie Christian Maire, pour ses conseils avisés et pour avoir accepté d'être rapporteur et membre du jury.

Merci également à Ernst-Ulrich Gekeler et Abbas Movahhedi pour l'intérêt qu'ils ont porté à ce travail et pour avoir bien voulu participer au jury.

Je tiens à dire qu'il m'a été agréable de travailler au sein du LMAM et du département de Mathématiques de l'Université de Metz. Mes contacts avec certains membres de l'équipe de théorie des nombres, en particulier Isabelle Dubois et Georges Rhin, m'ont beaucoup appris. Je remercie Lucie Vogel et Sedat Yamaner qui m'ont si gentiment consacré du temps pour des tâches administratives concernant cette thèse. Merci également à Jean-Marc Sac-Epée, pour ses aides techniques précieuses et son soutien. Je n'oublie pas MM. Ludwig et Wurzbacher dont l'appui ne s'est jamais démenti lorsqu'il s'est agi de prendre en compte ma situation d'enseignant.

Je remercie enfin ma femme Édith pour la patience dont elle a fait preuve, son soutien constant et la relecture attentive du texte de cette thèse.

Table des matières

Introduction

Le cadre de ce travail est celui des ℓ-extensions abéliennes d'un corps de nombres K, où ℓ désigne un nombre premier fixé, et de leur groupe de Galois. La $\mathbb{Z}_\ell$-extension cyclotomique K^c de K y joue un rôle essentiel.
En 1994, dans [5], Jean-François Jaulent donne une formule explicite pour le calcul des ℓ-symboles de Hilbert construits sur les racines ℓ^r-ièmes de l'unité contenues dans K. Cette formule se présente sous la forme

$$\left(\frac{\zeta, x}{\mathfrak{p}}\right) = \zeta^{\tilde{v}_\mathfrak{p}(x)},$$

où l'exposant $\tilde{v}_\mathfrak{p}(x)$ est un élément de $\mathbb{Z}_\ell$ défini à l'aide du logarithme ℓ-adique de $|x|_\mathfrak{p}$. L'application $\tilde{v}_\mathfrak{p}$ ainsi obtenue est l'analogue d'une valuation et ouvre donc la voie à une théorie arithmétique, dite *des diviseurs logarithmiques* qui s'apparente à la théorie classique des diviseurs ou à celle des idéaux de K.
Les groupes de diviseurs et de classes provenant de cette arithmétique donnent accès au calcul numérique de certains groupes de la K-théorie des corps de nombres, et se présentent d'autre part, via la théorie ℓ-adique du corps de classe, comme des groupes de Galois de ℓ-extensions abéliennes de K ou de K^c.
Les définitions et propriétés de base des objets de l'arithmétique logarithmique sont détaillées dans une première partie.
On étudie ensuite des questions de *capitulation* des classes logarithmiques d'un corps K dans un surcorps L, le degré de L/K étant une puissance de ℓ. On établit notamment un théorème analogue au théorème 94 de Hilbert.
Ces questions conduisent naturellement à envisager une tour de ℓ-extensions de K, analogue de la tour de Hilbert de K. Bien qu'on ne dispose pas d'un *théorème de l'idéal principal* pour le groupe des classes logarithmiques, la *tour localement cyclotomique* construite par Jean-François Jaulent et Florence Soriano-Gafiuk, permet, comme la tour de Hilbert, de répondre à la question du plongement de K dans un corps *logarithmiquement principal*. On démontre, dans cette troisième partie, des conditions de finitude et surtout d'infinitude de cette tour. On obtient notamment un critère d'infinitude de la tour pour une extension L d'un corps K possédant lui une tour finie.

Il s'agit dans la dernière partie de construire une tour analogue à la tour localement cyclotomique, et ceci en imposant la décomposition complète pour les places de K appartenant à un ensemble fini donné. On donne une interprétation simple de la finitude ou de l'infinitude de cette tour.

Index des principales notations

Pour l'essentiel, on utilise les notations de [6] ainsi que de [7]. Elles sont définies dans le texte au fur et à mesure de leur apparition, mais ne sont en principe pas redéfinies dans chaque chapitre. On pourra se reporter à la liste qui suit.

On note :

- ℓ, p, q, des nombres premiers,
- K, L, des corps de nombres,
- $\mathfrak{p}$, une place de K,
- $\mathfrak{P}$, une place de L,
- $K_{\mathfrak{p}}$, le complété de K en $\mathfrak{p}$,
- P_K^0, l'ensemble des places finies de K,
- P_K^∞, l'ensemble des places infinies de K,
- $\tilde{v}_{\mathfrak{p}}$, la valuation logarithmique attachée à la place $\mathfrak{p}$,
- $\tilde{e}_{\mathfrak{p}}$, l'indice de ramification logarithmique de la place $\mathfrak{p}$ dans K,
- $\tilde{f}_{\mathfrak{p}}$, le degré résiduel logarithmique de la place $\mathfrak{p}$ dans K,
- $\tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$, l'indice de ramification logarithmique de la place $\mathfrak{p}$ dans l'extension L/K (avec $\mathfrak{P}|\mathfrak{p}$),
- $\tilde{f}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$, le degré résiduel logarithmique de la place $\mathfrak{p}$ dans l'extension L/K,
- $d_{\mathfrak{p}}(L/K)$, l'indice de ramification de la place infinie $\mathfrak{p}$ dans l'extension L/K,
- $R_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$, le compactifié ℓ-adique de $K^\times$,
- K^c, la $\mathbb{Z}_\ell$-extension cyclotomique de K,
- K^{lc}, la $\mathbb{Z}_\ell$-extension localement cyclotomique de K, i.e. l'extension abélienne de K totalement décomposée sur K^c, maximale,
- $K_{\mathfrak{p}}^c$, le compositum de $K_{\mathfrak{p}}$ et de K^c,
- $\widehat{K}_{\mathfrak{p}}^c$, le compositum de $K_{\mathfrak{p}}$ et de $\widehat{Q}_p^c$,
- $Dl_K = \bigoplus_{\mathfrak{p} \in P_K^0} \mathbb{Z}_\ell \ \mathfrak{p}$, le groupe des diviseurs logarithmiques de K,
- $\widetilde{div}_K$, le morphisme naturel de R_K dans Dl_K,
- Pl_K, le groupe des diviseurs logarithmiques principaux de K,
- $\deg(\mathfrak{a})$, le degré ℓ-adique du diviseur logarithmique $\mathfrak{a}$,
- $Cl_K = Dl_K/Pl_K$, le groupe des classes logarithmiques de K (non nécessairement

de degré nul),
- $\widetilde{Dl}_K, \widetilde{Pl}_K, \widetilde{Cl}_K$, les groupes correspondants formés des diviseurs, diviseurs principaux, et classes logarithmiques de degré nul ($\widetilde{Pl}_K = Pl_K$ et $\widetilde{Cl}_K = \widetilde{Dl}_K/\widetilde{Pl}_K$),
- $\tilde{E}_K$, le groupe des unités logarithmiques de K, i.e. le noyau de l'homomorphisme $R_K \to \widetilde{Pl}_K$,
- $i, \tilde{i}$ et $\tilde{j}$, les morphismes d'extension de Dl_K dans Dl_L, de $\widetilde{Dl}_K$ dans $\widetilde{Dl}_L$, et de $\widetilde{Cl}_K$ dans $\widetilde{Cl}_L$ respectivement,
- $\widetilde{cap}_{L/K}$, le ℓ-groupe de capitulation logarithmique de l'extension L/K,
- S, un ensemble fini de places non archimédiennes de K,
- K_S^{lc}, l'extension abélienne maximale de K qui est non logarithmiquement ramifiée et S-décomposée.

Chapitre 1

À propos des classes logarithmiques

Les aspects développés ci-dessous de la théorie des classes logarithmiques correspondent aux besoins des chapitres qui suivent. Pour davantage de détails et une présentation plus pédagogique, nous renvoyons le lecteur à [6].

1.1 Ramification logarithmique d'une place dans une extension

Dans cette section, on désigne par K un corps de nombres, p un nombre premier de $\mathbb{Q}$, et $\mathfrak{p}$ une place de K au dessus de p.

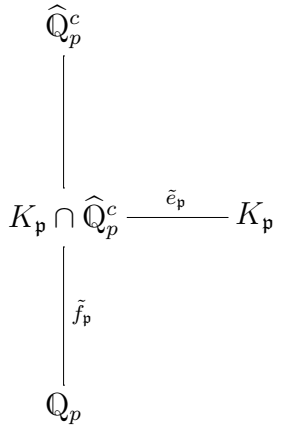
1.1.1 Définitions

Désignant par $\widehat{\mathbb{Q}}_p^c$ le compositum des $\mathbb{Z}_q$-extensions cyclotomiques de $\mathbb{Q}_p$ pour tous les nombres premiers q, on introduit les notions qui suivent.

Définition 1.1.1 *On appelle indice de ramification logarithmique (absolu) de la place* $\mathfrak{p}$ *le degré de l'extension* $K_\mathfrak{p}/K_\mathfrak{p} \cap \widehat{\mathbb{Q}}_p^c$.

L'indice de ramification logarithmique de $\mathfrak{p}$ mesure donc le « défaut de cyclotomicité » du complété $K_\mathfrak{p}$ de K.

Définition 1.1.2 *On appelle degré résiduel logarithmique (absolu) de la place* $\mathfrak{p}$ *le degré de l'extension* $K_\mathfrak{p} \cap \widehat{\mathbb{Q}}_p^c/\mathbb{Q}_p$.



La place $\mathfrak{p}$ est non logarithmiquement ramifiée dans K lorsque $\tilde{e}_\mathfrak{p} = 1$, ce qui équivaut à l'inclusion $K_\mathfrak{p} \subset \widehat{\mathbb{Q}}_p^c$.

1.1.2 Cas d'une ℓ-extension de $\mathbb{Q}$

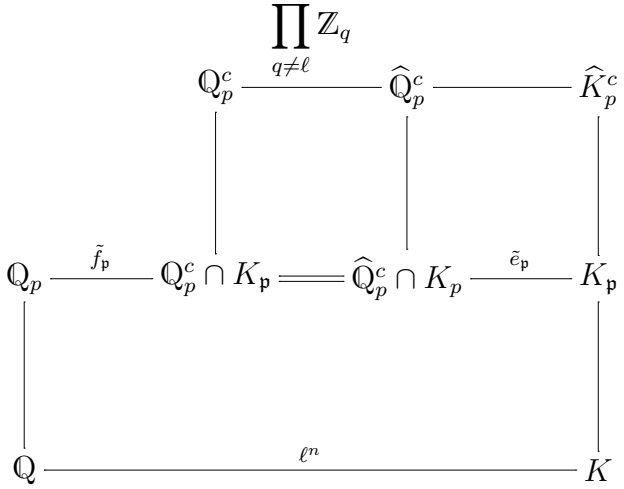
On suppose à présent que le corps de nombres K est une ℓ-extension de $\mathbb{Q}$, c'est-à-dire qu'il existe un entier $n > 0$ tel que $[L : \mathbb{Q}] = \ell^n$. L'extension $\widehat{\mathbb{Q}}_p^c/\mathbb{Q}_p^c$ ne contient que des sous-extensions dont le degré est étranger à ℓ. Par conséquent le degré $[\widehat{\mathbb{Q}}_p^c \cap K_\mathfrak{p} : \mathbb{Q}_p^c \cap K_\mathfrak{p}]$ est étranger à ℓ, et comme il divise ℓ^n, il est égal à 1. L'égalité $\widehat{\mathbb{Q}}_p^c \cap K_\mathfrak{p} = \mathbb{Q}_p^c \cap K_\mathfrak{p}$ qui en résulte entraîne la caractérisation suivante de la non-ramification logarithmique :

$$\tilde{e}_\mathfrak{p} = 1 \iff K_\mathfrak{p} \subset \mathbb{Q}_p^c.$$

De même

$$\tilde{f}_\mathfrak{p} = 1 \iff K_\mathfrak{p} \cap \mathbb{Q}_p^c = \mathbb{Q}_p.$$

L'extension $\mathbb{Q}_p^c/\mathbb{Q}_p$ étant galoisienne, la condition $K_\mathfrak{p} \cap \mathbb{Q}_p^c = \mathbb{Q}_p$ signifie que les extensions $K_\mathfrak{p}$ et $\mathbb{Q}_p^c$ sont linéairement disjointes sur $\mathbb{Q}_p$.

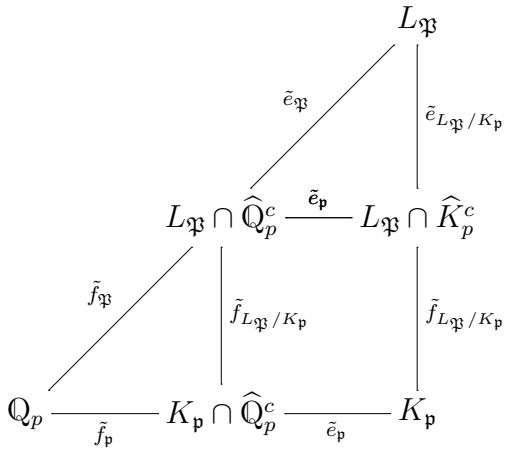


1.1.3 Cas d'une extension relative

Soit L une extension (de degré fini) de K. On note $\mathfrak{P}$ une place de L au dessus de $\mathfrak{p}$. On définit l'indice de ramification logarithmique relatif $\tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ et le degré résiduel logarithmique relatif $\tilde{f}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ (notés parfois $\tilde{e}_{\mathfrak{P}}(L/K)$ et $\tilde{f}_{\mathfrak{P}}(L/K)$) par les formules suivantes :

$$\tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = [L_{\mathfrak{P}} : L_{\mathfrak{P}} \cap \widehat{K}_{\mathfrak{p}}^c],$$
$$\tilde{f}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = [L_{\mathfrak{P}} \cap \widehat{K}_{\mathfrak{p}}^c : K_{\mathfrak{p}}],$$

où $\widehat{K}_{\mathfrak{p}}^c$ désigne le compositum des corps $K_{\mathfrak{p}}$ et $\widehat{\mathbb{Q}}_p^c$. On a donc le schéma suivant :



ainsi que les relations

$$\tilde{e}_{\mathfrak{P}} = \tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\tilde{e}_{\mathfrak{p}} \quad \text{et} \quad \tilde{f}_{\mathfrak{P}} = \tilde{f}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\tilde{f}_{\mathfrak{p}}.$$

Comme dans le cas absolu, on a les caractérisations :

$$\tilde{e}_{L\mathfrak{P}/K_\mathfrak{p}} = 1 \iff L\mathfrak{P} \subset \widehat{K}^c_\mathfrak{p},$$

$$\tilde{f}_{L\mathfrak{P}/K_\mathfrak{p}} = 1 \iff L\mathfrak{P} \cap \widehat{K}^c_\mathfrak{p} = K_\mathfrak{p},$$

où $\widehat{K}^c_p$ peut être remplacé par K^c_p lorsque le degré de L/K est une puissance du nombre premier ℓ.

1.1.4 Relation avec les indices au sens classique

On remarque que les définitions précédentes entraînent les égalités

$$\tilde{e}_\mathfrak{p}\tilde{f}_\mathfrak{p} = [K_\mathfrak{p} : \mathbb{Q}_p] = e_\mathfrak{p} f_\mathfrak{p},$$

$e_\mathfrak{p}$ et $f_\mathfrak{p}$ désignant l'indice de ramification et le degré résiduel de la place $\mathfrak{p}$ dans l'extension $K/\mathbb{Q}$, au sens habituel. Plus précisément, on montre que si p ne divise pas $[K_\mathfrak{p} : \mathbb{Q}_p]$, alors $e_\mathfrak{p} = \tilde{e}_\mathfrak{p}$ et $f_\mathfrak{p} = \tilde{f}_\mathfrak{p}$. Et ces propriétés s'étendent naturellement aux indices relatifs. Par conséquent, si L/K est une ℓ-extension, la ramification logarithmique ne diffère de la ramification classique que pour les places au-dessus de ℓ.

1.2 Diviseurs et classes logarithmiques

On fixe un nombre premier ℓ et un corps de nombres K.

1.2.1 Le ℓ-groupe des diviseurs logarithmiques d'un corps de nombres

Un diviseur logarithmique de K est une somme formelle

$$\sum_{\mathfrak{p} \in P^0_K} a_\mathfrak{p}\mathfrak{p},$$

indexée sur l'ensemble des places finies de K et où les coefficients $a_\mathfrak{p}$ sont des entiers ℓ-adiques. C'est donc un élément du $\mathbb{Z}_\ell$-module construit sur les places finies de K :

$$Dl_K = \bigoplus_{\mathfrak{p} \in P^0_K} \mathbb{Z}_\ell\, \mathfrak{p}.$$

1.2.2 Le degré d'un diviseur logarithmique

On définit sur P_K^0 l'application degré de la manière suivante :

$$\deg(\mathfrak{p}) = \tilde{f}_{\mathfrak{p}} \deg p,$$

le degré (ℓ-adique) du nombre premier p étant défini par
- si $p \neq \ell$, alors $\deg p = \mathrm{Log}_{Iw} p$,
- si $\ell \neq 2$, alors $\deg \ell = \ell$,
- $\deg 2 = 4$,

où Log_{Iw} est le logarithme d'Iwasawa défini sur $\mathbb{Z}_\ell^\times$. Cette fonction est donc à valeurs dans $\mathbb{Z}_\ell$. Elle induit naturellement, par linéarité, un morphisme degré sur Dl_K, encore noté deg :

$$\deg\left(\sum_{\mathfrak{p}\in P_K^0} a_{\mathfrak{p}}\mathfrak{p}\right) = \sum_{\mathfrak{p}\in P_K^0} a_{\mathfrak{p}} \deg(\mathfrak{p}).$$

En particulier si L/K est une extension de corps de nombres, $\mathfrak{p}$ une place de K et $\mathfrak{P}$ une place de L au dessus de $\mathfrak{p}$, on a

$$\deg \mathfrak{P} = \tilde{f}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} \deg \mathfrak{p}.$$

Le noyau de ce morphisme est un sous $\mathbb{Z}_\ell$-module de Dl_K qu'on note $\widetilde{Dl}_K$ et qu'on appelle le groupe des diviseurs logarithmiques de degré nul de K.

1.2.3 Diviseurs logarithmiques principaux

On note R_K le produit tensoriel du groupe multiplicatif de K par l'anneau des entiers ℓ-adiques :

$$R_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times.$$

De même qu'un élément du groupe $K^\times$ est de manière unique et à une unité près un produit (fini) $\prod_{\mathfrak{p}\in P_K^0} \mathfrak{p}^{x_{\mathfrak{p}}}$ où $x_{\mathfrak{p}} \in \mathbb{Z}$, on peut voir un élément de R_K comme un produit (fini) $\prod_{\mathfrak{p}\in P_K^0} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$ où les α_p sont dans $\mathbb{Z}_\ell$ (tous nuls sauf un nombre fini d'entre eux). Il en résulte un morphisme naturel

$$\begin{array}{rccc} \widetilde{div}_K : & R_K & \to & Dl_K \\ & x & \mapsto & \sum_{\mathfrak{p}\in P_K^0} \alpha_{\mathfrak{p}}\mathfrak{p}. \end{array}$$

L'image de ce morphisme est un sous $\mathbb{Z}_\ell$-module de Dl_K qu'on note $\widetilde{Pl}_K$ et qu'on appelle le groupe des diviseurs logarithmiques principaux de K. On montre que tout diviseur logarithmique principal est de degré nul. Autrement dit :

$$\widetilde{Pl}_K \subset \widetilde{Dl}_K.$$

On définit enfin la valuation logarithmique $\tilde{v}_\mathfrak{p} : Dl_K \to \mathbb{Z}_\ell$ par

$$\tilde{v}_p \left(\sum_{\mathfrak{p} \in P_K^0} a_\mathfrak{p} \mathfrak{p} \right) = a_\mathfrak{p}.$$

L'application induite par $\tilde{v}_\mathfrak{p}$, via l'application $\widetilde{div}_K$, de R_K dans $\mathbb{Z}_\ell$ sera encore notée $\tilde{v}_\mathfrak{p}$.

1.3 Le groupe des classes logarithmiques

Le quotient $\widetilde{Dl}_K/\widetilde{Pl}_K$ se note $\widetilde{Cl}_K$ et est appelé le groupe des classes logarithmiques de degré nul de K. On a donc la suite exacte

$$0 \to \widetilde{Pl}_K \to \widetilde{Dl}_K \to \widetilde{Cl}_K \to 0.$$

Selon la théorie ℓ-adique du corps de classe (voir [6]), ce groupe est isomorphe au groupe de Galois de l'extension K^{lc}/K^c, où K^c désigne la $\mathbb{Z}_\ell$-extension cyclotomique de K et K^{lc} la $\mathbb{Z}_\ell$-extension localement cyclotomique de K. La conjecture de Gross généralisée affirme que le groupe $\widetilde{Cl}_K$ est fini (voir [16]).

Chapitre 2

Capitulation des classes logarithmiques

Le problème de la capitulation des idéaux dans une extension L/K de corps de nombres est étudié depuis Hilbert. On dit d'un idéal I de l'anneau des entiers de K qu'il *capitule* dans L lorsqu'il engendre un idéal principal dans l'anneau des entiers de L. Le théorème 94 de Hilbert affirme que si l'extension L/K est cyclique et non ramifiée, il y a au moins un idéal non principal dans K qui « devient » principal dans L. Nous transposons ici le problème de la capitulation dans le cadre de l'arithmétique des classes logarithmiques. On établit notamment un résultat analogue au théorème 94. L'hypothèse de non-ramification est alors à prendre au sens logarithmique. Deux démonstrations différentes de ce théorème sont données. Son utilisation est testée dans le cas d'une extension totalement imaginaire d'un corps quadratique réel. Enfin, on donne un algorithme de calcul du groupe de capitulation logarithmique.

2.1 Le groupe $\widetilde{cap}_{L/K}$

Dans cette section, on considère une extension L/K de corps de nombres.

2.1.1 Extension des diviseurs et des classes logarithmiques

Soit a_K un diviseur logarithmique de K :

$$a_K = \sum_{\mathfrak{p}\in P_K^0} \tilde{v}_{\mathfrak{p}}(a_K)\,\mathfrak{p}.$$

À chaque place finie $\mathfrak{p}$ de K, on associe le diviseur logarithmique de L construit sur les places de L au dessus de $\mathfrak{p}$:

$$i(\mathfrak{p}) = \sum_{\mathfrak{P}|\mathfrak{p}} \tilde{e}_{\mathfrak{P}}\mathfrak{P},$$

où $\tilde{e}_{\mathfrak{P}}$ désigne, pour simplifier, l'indice de ramification logarithmique relatif de la place $\mathfrak{P}$ dans l'extension L/K. Il s'ensuit, par linéarité, une application naturelle de Dl_K dans Dl_L définie par

$$i(a_K) = \sum_{\mathfrak{p}\in P_K^0} \tilde{v}_{\mathfrak{p}}(a_K) \sum_{\mathfrak{P}|\mathfrak{p}} \tilde{e}_{\mathfrak{P}}\mathfrak{P},$$

si bien que

$$i(a_K) = \sum_{\mathfrak{P}\in P_L^0} \tilde{v}_{\mathfrak{p}}(a_K)\,\tilde{e}_{\mathfrak{P}}\mathfrak{P},$$

et finalement

$$\tilde{v}_{\mathfrak{P}}(i(a_K)) = \tilde{v}_{\mathfrak{p}}(a_K)\,\tilde{e}_{\mathfrak{P}}.$$

Il est clair que i est un homomorphisme de groupe. On l'appelle le *morphisme d'extension* de Dl_K à Dl_L.
Supposons que $\tilde{v}_{\mathfrak{P}}(i(a_K)) = 0$ pour toute place finie $\mathfrak{P}$ de L. Puisque les indices de ramifications logarithmiques sont des entiers strictement positifs, on a $\tilde{v}_{\mathfrak{p}}(a_K) = 0$ pour toute place finie $\mathfrak{p}$ de K. On voit ainsi que i est injectif. On note $\tilde{i}$ sa restriction au groupe $\widetilde{D\ell}_K$ des diviseurs logarithmiques de degré nul de K. Les égalités

$$\deg i(\mathfrak{p}) = \sum_{\mathfrak{P}|\mathfrak{p}} \tilde{e}_{\mathfrak{P}} \deg \mathfrak{P} = \sum_{\mathfrak{P}|\mathfrak{p}} \tilde{e}_{\mathfrak{P}}\tilde{f}_{\mathfrak{P}} \deg \mathfrak{p} = [L:K] \deg \mathfrak{p},$$

montrent que le degré de $i(a_K)$ est nul si et seulement si celui de a_K l'est. Nous pouvons résumer tout ceci par la proposition qui suit.

Proposition 2.1.1 *Le morphisme d'extension $i : Dl_K \to Dl_L$ est injectif. Sa restriction $\tilde{i}$ est un morphisme de $\widetilde{Dl}_K$ dans $\widetilde{Dl}_L$.*

Considérons à présent le cas particulier où a_K est logarithmiquement principal :

$$a_K = \widetilde{div}_K(x),\ x \in R_K.$$

On a alors

$$\tilde{i}(a_K) = \sum_{\mathfrak{P} \in P_L^0} \tilde{v}_{\mathfrak{P}}(a_K)\mathfrak{P} = \sum_{\mathfrak{P} \in P_L^0} \tilde{v}_{\mathfrak{P}}(x)\mathfrak{P}.$$

L'inclusion évidente de R_K dans R_L montre alors que $\tilde{i}\,(a_K)$ est principal. Puisque $\tilde{i}(\widetilde{Pl}_K) \subset \widetilde{Pl}_L$, le morphisme $\tilde{i}$ induit, par passage au quotient, un homomorphisme de groupes :

$$\tilde{j} : \widetilde{Cl}_K \to \widetilde{Cl}_L,$$

conformément au diagramme commutatif suivant :

$$\begin{array}{ccc} \widetilde{Dl}_K & \xrightarrow{\tilde{i}} & \widetilde{Dl}_L \\ \downarrow & & \downarrow \\ \widetilde{Cl}_K & \xrightarrow{\tilde{j}} & \widetilde{Cl}_L \end{array}$$

2.1.2 Capitulation des diviseurs et des classes logarithmiques

L'homomorphisme $\tilde{j}$, défini ci-dessus pour une extension L/K de corps de nombres, n'est pas nécessairement injectif. Son noyau se nomme *le groupe de capitulation logarithmique* de l'extension L/K. Il est noté :

$$Ker\tilde{j} = \widetilde{cap}_{L/K}.$$

On dit ainsi d'une classe logarithmique de K appartenant à $\widetilde{cap}_{L/K}$ qu'elle *capitule* dans L. On emploie le même vocabulaire pour un diviseur logarithmique appartenant à une telle classe (c'est-à-dire devenant principal dans L).

2.1.3 Exemple

Soit K un corps de nombres satisfaisant à la conjecture de Gross, et a_K un diviseur logarithmique de K. On va exhiber une extension L de K dans laquelle a_K capitule. Notons n l'ordre de la classe de a_K dans $\widetilde{Cl}_K$. Si x est un élément de R_K

tel que $na_K = \widetilde{div}_K(x)$, il existe des entiers ℓ-adiques u_i et des éléments t_i de $K^\times$ tels que

$$x = \prod_{i=1}^{n} u_i \otimes t_i.$$

On désigne alors par y_i une racine n-ième de t_i dans $\mathbb{C}$ (pour chaque entier i) et on pose : $L = K(y_1, \ldots, y_n)$. Il vient :

$$\begin{aligned}
na_K &= \widetilde{div}_K(x) \\
na_K &= \widetilde{div}_L(x) \\
na_K &= \widetilde{div}_L(\prod_{i=1}^{n} u_i \otimes t_i) \\
na_K &= \sum_{i=1}^{n} \widetilde{div}_L(u_i \otimes y_i^n) \\
na_K &= \sum_{i=1}^{n} \widetilde{div}_L(u_i \otimes y_i)^n \\
na_K &= n \sum_{i=1}^{n} \widetilde{div}_L(u_i \otimes y_i)
\end{aligned}$$

On a donc

$$a_K = \widetilde{div}_L(u \otimes y).$$

Donc a_K capitule dans L. Bien entendu, la problèmatique est en général inverse, c'est-à-dire qu'on a une extension L/K et qu'on veut connaître les diviseurs logarithmiques de K qui capitulent dans L.

2.1.4 Quelques résultats sur $\widetilde{cap}_{L/K}$

On considère une extension L/K de corps de nombres et on note n son degré.

Proposition 2.1.2 *Le groupe $\widetilde{cap}_{L/K}$ est un ℓ-groupe d'exposant un diviseur de n.*

Démonstration. Le fait que $\widetilde{cap}_{L/K}$ soit un ℓ-groupe est évident car c'est un sous-groupe du ℓ-groupe $\widetilde{Cl}_K$. Pour la deuxième assertion on utilise l'inclusion :

$$\ker \tilde{j} \subseteq \ker \tilde{N} \circ \tilde{j}.$$

Sachant que $\tilde{N} \circ \tilde{j}$ est le produit par n dans $\widetilde{Cl}_K$, $\widetilde{cap}_{L/K}$ est donc formé d'éléments dont l'ordre divise n. □

Corollaire 2.1.3 *Si l'ordre du groupe $\widetilde{Cl}_K$ est étranger à n, alors $\widetilde{cap}_{L/K} = 1$.*

DÉMONSTRATION. L'ordre d'un élément de $\widetilde{cap}_{L/K}$ est une puissance de ℓ et divise n, donc c'est 1. □

Corollaire 2.1.4 *Si $\widetilde{Cl}_K$ est cyclique et égal à $\widetilde{cap}_{L/K}$, alors $|\widetilde{Cl}_K|$ divise n (et donc $|\widetilde{Cl}_K| \leqslant n$).*

DÉMONSTRATION. Tout élément de $\widetilde{cap}_{L/K}$ est d'ordre diviseur de n, en particulier un générateur de $\widetilde{cap}_{L/K}$ qui est d'ordre $|\widetilde{Cl}_K|$. □

2.2 Une version logarithmique du théorème 94 de Hilbert

2.2.1 Diviseurs logarithmiques ambiges

On suppose que l'extension L/K est galoisienne et on note G son groupe de Galois. Un diviseur logarithmique a de L est dit *ambige* lorsque

$$\forall \sigma \in G, \sigma(a) = a.$$

Proposition 2.2.1 *Les éléments de* $\operatorname{Im} \tilde{i}$ *sont des diviseurs logarithmiques ambiges.*

Démonstration. Soit a_K un diviseur logarithmique ambige de K et σ un élément de G. On a :

$$\sigma\left(\tilde{i}\left(a_K\right)\right) = \sigma\left(\tilde{i}\left(\sum_{\mathfrak{p}\in P_K^0} \tilde{v}_{\mathfrak{p}}\left(a_K\right)\mathfrak{p}\right)\right) = \sum_{\mathfrak{p}\in Pl_K^0} \tilde{v}_{\mathfrak{p}}\left(a_K\right)\sigma\left(\tilde{i}\left(\mathfrak{p}\right)\right).$$

De plus

$$\sigma\left(\tilde{i}\left(\mathfrak{p}\right)\right) = \sum_{\mathfrak{P}|\mathfrak{p}} \tilde{e}_{\mathfrak{P}}\mathfrak{P}^{\sigma}.$$

Enfin, l'extension étant galoisienne, $\tilde{e}_{\mathfrak{P}}$ ne dépend que de $\mathfrak{p}$ et σ permute les places au dessus de $\mathfrak{p}$, de sorte que

$$\sigma\left(\tilde{i}\left(\mathfrak{p}\right)\right) = \tilde{i}\left(\mathfrak{p}\right).$$

Et ainsi

$$\sigma\left(\tilde{i}\left(a_K\right)\right) = \tilde{i}\left(a_K\right)$$

□

Proposition 2.2.2 *Si l'extension galoisienne L/K est non logarithmiquement ramifiée, alors* $\operatorname{Im} \tilde{i}$ *contient tous les diviseurs logarithmiques ambiges. Autrement dit,* $\operatorname{Im} \tilde{i} = \widetilde{Dl}_L^G$.

Démonstration. Soit a_L un diviseur logarithmique ambige de L. On a, pour tout élément σ de G :

$$a_L = \sigma\left(a_L\right),$$

ce que l'on peut écrire

$$\sum_{\mathfrak{P}\in P_L^0} \tilde{v}_{\mathfrak{P}}(a_L)\,\mathfrak{P} = \sum_{\mathfrak{P}\in P_L^0} \tilde{v}_{\mathfrak{P}}(a_L)\,\mathfrak{P}^{\sigma}.$$

Cette décomposition étant unique, on peut identifier les coefficients de $\mathfrak{P}^{\sigma}$ des deux membres :

$$\tilde{v}_{\mathfrak{P}^{\sigma}}(a_L) = \tilde{v}_{\mathfrak{P}}(a_L).$$

On note alors S un système maximal de diviseurs deux à deux non conjugués de a_L. Les termes de la somme ci-dessus peuvent se réorganiser comme suit :

$$a_L = \sum_{\mathfrak{P}\in S} \tilde{v}_{\mathfrak{P}}(a_L) \sum_{\tau\in G_{\mathfrak{P}}} \mathfrak{P}^{\tau}$$

où $G_{\mathfrak{P}}$ désigne un système de représentants des classes de G modulo le groupe de décomposition $D_{\mathfrak{P}}$ de la place $\mathfrak{P}$. L'extension étant logarithmiquement non ramifiée, on a :

$$\sum_{\tau\in G_{\mathfrak{P}}} \mathfrak{P}^{\tau} = \tilde{i}(\mathfrak{p}),$$

où $\mathfrak{p}$ est la place de K au dessous de $\mathfrak{P}$. Ce qui montre que

$$a_L \in \operatorname{Im}\tilde{i}.$$

□

2.2.2 Le théorème 94 "logarithmique"

On suppose ici que l'extension L/K est cyclique. On note G son groupe de Galois et σ un générateur de G. Soit a_K un diviseur logarithmique de K qui capitule dans L :

$$\tilde{i}(a_K) = \widetilde{div}_L(x),\ x \in R_L.$$

La proposition 2.2.1 nous donne

$$\sigma\left(\widetilde{div}_L(x)\right) = \widetilde{div}_L(x).$$

Mais il est clair que

$$\sigma\left(\widetilde{div}_L(x)\right) = \widetilde{div}_L\left(\sigma(x)\right),$$

de sorte que

$$\widetilde{div}_L(x) = \widetilde{div}_L\left(\sigma(x)\right).$$

Il en résulte que pour toute place finie $\mathfrak{P}$ de L,

$$\tilde{v}_{\mathfrak{P}}(x) = \tilde{v}_{\mathfrak{P}}\left(\sigma(x)\right).$$

L'élément $x^{1-\sigma}$ est donc une unité logarithmique de L. D'autre part, il est immédiat que $N_{L/K}\left(x^{1-\sigma}\right) = 1$. On a donc :

$$x^{1-\sigma} \in \widetilde{E}_L^*,$$

où $\widetilde{E}_L^*$ désigne le groupe des unités logarithmiques de norme 1 de L. Enfin, si $\widetilde{div}_L(x) = \widetilde{div}_L(y)$, on a pour toute place finie $\mathfrak{P}$ de L,

$$\tilde{v}_{\mathfrak{P}}(x) = \tilde{v}_{\mathfrak{P}}(y),$$

ou encore

$$\frac{y}{x} \in \widetilde{E}_L.$$

Par suite, en notant u cette unité logarithmique de L,

$$y^{1-\sigma} = u^{1-\sigma}x^{1-\sigma}.$$

On peut donc considérer l'homomorphisme de groupes

$$\varphi : [a_K] \mapsto x^{1-\sigma} \mod \tilde{E}_L^{1-\sigma},$$

de $\widetilde{cap}_{L/K}$ sur $\widetilde{E}_L^*/\tilde{E}_L^{1-\sigma}$. Ici, $[a_K]$ désigne la classe de a_K modulo $\widetilde{Pl}_K$. Vérifions que le morphisme φ est bien défini. L'égalité

$$[a_K] = [b_K]$$

entraîne

$$b_K = a_K + \widetilde{div}_K(z),\ z \in R_K,$$

de sorte que

$$i(b_K) = \widetilde{div}_L(x) + \widetilde{div}_L(z) = \widetilde{div}_L(xz).$$

Enfin, puisque $z \in R_K$, on a

$$(xz)^{1-\sigma} = (x)^{1-\sigma}.$$

Le fait que φ est un homomorphisme de groupes est immédiat. Le résultat suivant constitue un analogue logarithmique du théorème 94 de Hilbert.

Théorème 2.2.3 *Soit L/K une extension cyclique, non logarithmiquement ramifiée en les places finies. Le morphisme*

$$\varphi : [a_K] \mapsto x^{1-\sigma} \mod \widetilde{E}_L^{1-\sigma},$$

du groupe de capitulation logarithmique de L/K dans le quotient du groupe des unités logarithmiques de norme 1 de L par son sous-groupe des unités de la forme $\frac{t}{\sigma(t)}$, est un isomorphisme de groupes.

DÉMONSTRATION. On montre successivement l'injectivité et la surjectivité de φ. Seule cette dernière utilise l'hypothèse de non-ramification.

- Injectivité de φ :
  soit $[a_K]$ un élément de $ker\varphi$. On a

  $$\tilde{i}(a_K) = \widetilde{div}_L(x),\ x \in R_L$$

  et

  $$x^{1-\sigma} \in \widetilde{E}_L^{1-\sigma}.$$

  Il existe donc une unité logarithmique u de L telle que

  $$x^{1-\sigma} = u^{1-\sigma}.$$

  Posant $\frac{x}{u} = t$, on a donc $t \in R_K$. Si bien que

  $$\widetilde{div}_L(x) = \widetilde{div}_L(u) + \widetilde{div}_L(t),$$

  mais,

  $$\widetilde{div}_L(u) = 0,$$

  et, d'après [6] (point (i) de la preuve de la proposition 2.4),

  $$\widetilde{div}_L(t) = \widetilde{div}_K(t).$$

  Ainsi, a_K est un diviseur logarithmique principal de K et donc sa classe $[a_K]$ dans $\widetilde{Cl}_K$ est l'élément neutre de $ker\tilde{j}$.
- Surjectivité de φ :
  soit $u \in \widetilde{E}_L^*$. D'après le théorème 90 de Hilbert (L/K étant cyclique), il existe un élément x de R_L tel que $u = x^{1-\sigma}$. On considère alors le diviseur $\widetilde{div}_L(x)$:

  $$\widetilde{div}_L(x) = \widetilde{div}_L(x^\sigma u) = \widetilde{div}_L(x^\sigma) = \sigma\left(\widetilde{div}_L(x)\right).$$

  $\widetilde{div}_L(x)$ est donc un diviseur logarithmique ambige de L ; ce qui signifie, d'après la proposition 2.2.2 que $\widetilde{div}_L(x) = \widetilde{div}_K(x)$. La classe de $\widetilde{div}_K(x)$ dans $\widetilde{Cl}_K$ est donc un antécédent de $u \mod \widetilde{E}_L^{1-\sigma}$. □

Corollaire 2.2.4 *Lorsque la ℓ-extension L/K est cyclique et non logarithmiquement ramifiée en les places finies, alors*

$$|\widetilde{cap}_{L/K}| = \frac{\left[\widetilde{E}_K : N_{L/K}\left(\widetilde{E}_L\right)\right]}{\prod\limits_{\mathfrak{p}\in P_K^\infty} d_{\mathfrak{p}}(L/K)}.$$

Démonstration. En effet le quotient de Herbrand est défini par :

$$q(\widetilde{E}_L) = \frac{\left[\widetilde{E}_K : N_{L/K}\left(\widetilde{E}_L\right)\right]}{\left[\widetilde{E}_L^* : \widetilde{E}_L^{1-\sigma}\right]}.$$

D'autre part (voir [6], corollaire 3.7), il est connu que :

$$q(\widetilde{E}_L) = \prod_{\mathfrak{p}\in P_K^\infty} d_{\mathfrak{p}}(L/K).$$

Le théorème est alors une conséquence de l'isomorphisme obtenu au théorème précédent. □

Corollaire 2.2.5 *Si la ℓ-extension L/K est non logarithmiquement ramifiée en les places finies et infinies, alors :*

$$|\widetilde{cap}_{L/K}| = \left[\widetilde{E}_K : N_{L/K}\left(\widetilde{E}_L\right)\right].$$

Démonstration. On a en effet dans ce cas :

$$\prod_{\mathfrak{p}\in P_K^\infty} d_{\mathfrak{p}}(L/K) = 1.$$

□

L'importance du théorème 2.2.3 réside notamment dans le fait suivant. On peut considèrer que l'hypothèse de non-ramification pour une extension L/K est bien moins forte au sens logarithmique qu'au sens classique. En effet cette dernière notion signifie que L est inclus dans le corps de classe de Hilbert H_K, qui est une extension de degré fini de K. Alors que l'extension abélienne non logarithmiquement ramifiée maximale de K est de degré infini comme on le verra dans le théorème 3.1.5.

2.3 Démonstration cohomologique du théorème 94 "logarithmique"

On a tout d'abord, dans le cas d'une extension galoisienne logarithmiquement non ramifiée, une interprétation cohomologique du groupe de capitulation qui fait l'objet du théorème suivant.

Théorème 2.3.1 *Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G. Si L/K est non logarithmiquement ramifiée, alors*

$$\widetilde{cap}_{L/K} \simeq H^1\left(G, \widetilde{E}_L\right).$$

Démonstration. On part de la suite exacte de G-modules

$$1 \to \widetilde{E}_L \to R_L \to \widetilde{Pl}_L \to 1.$$

L'action de G nous fournit alors la suite exacte de cohomologie suivante :

$$1 \to \widetilde{E}_L^G \to R_L^G \to \widetilde{Pl}_L^G \to H^1\left(G, \widetilde{E}_L\right) \to H^1\left(G, R_L\right).$$

Mais d'après le théorème 90 de Hilbert,

$$H^1\left(G, R_L\right) = 1.$$

Compte tenu des égalités

$$\tilde{E}_L^G = \widetilde{E}_K, R_L^G = R_K,$$

on en déduit l'isomorphisme

$$H^1\left(G, \widetilde{E}_L\right) \simeq \widetilde{Pl}_L^G / \left(R_K/\widetilde{E}_K\right).$$

Cependant, on a l'isomorphisme

$$R_K/\widetilde{E}_K \simeq \widetilde{Pl}_K.$$

On en déduit

$$H^1\left(G, \widetilde{E}_L\right) \simeq \widetilde{Pl}_L^G/\widetilde{Pl}_K.$$

On considère à présent le diagramme commutatif suivant

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widetilde{Pl}_K & \longrightarrow & \widetilde{Dl}_K & \longrightarrow & \widetilde{Cl}_K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tilde{i}} & & \downarrow{\scriptstyle \tilde{i}} & & \downarrow{\scriptstyle \tilde{j}} & & \\
0 & \longrightarrow & \widetilde{Pl}_L^G & \longrightarrow & \widetilde{Dl}_L^G & \longrightarrow & \widetilde{Cl}_L^G & \longrightarrow & H^1\left(G, \widetilde{Pl}_L\right)
\end{array}$$

Tenant compte de l'injectivité de $\tilde{i}$ et de sa restriction à $\widetilde{Pl}_K$, le lemme du serpent nous donne la suite exacte

$$0 \to \ker \tilde{j} \to \widetilde{Pl}_L^G/\tilde{i}\left(\widetilde{Pl}_K\right) \to \widetilde{Dl}_L^G/\tilde{i}\left(\widetilde{Dl}_K\right).$$

Mais, puisque l'extension L/K est non logarithmiquement ramifiée, la proposition 2.2.2 nous donne

$$\tilde{i}\left(\widetilde{Dl}_K\right) = \widetilde{Dl}_L^G.$$

On a donc

$$\ker \tilde{j} \simeq \left(\widetilde{Pl}_L^G\right)/\tilde{i}\left(\widetilde{Pl}_K\right),$$

c'est-à-dire, d'après le raisonnement précédent,

$$\ker \tilde{j} \simeq H^1\left(G, \widetilde{E}_L\right),$$

ou encore

$$\widetilde{cap}_{L/K} \simeq H^1\left(G, \widetilde{E}_L\right).$$

□

On en déduit immédiatement le théorème 94 « logarithmique », puisque, lorsque G est cyclique,

$$H^1\left(G, \widetilde{E}_L\right) \simeq \widetilde{E}_L^*/\widetilde{E}_L^{1-\sigma}.$$

□

2.4 Étude d'une famille d'exemples

On va appliquer le théorème précédent pour étudier la capitulation logarithmique de certaines extensions L/K où $K = \mathbb{Q}\left(\sqrt{d}\right)$, d étant un entier supérieur ou égal à 2 sans facteur carré, et $L = K(i)$. On suppose donc que $\ell = 2$.

$$\begin{array}{ccc} \mathbb{Q}(i) & \text{———} & L \\ | & & | \\ \mathbb{Q} & \text{———} & K \end{array}$$

2.4.1 Ramification logarithmique dans L/K

L'extension de Kummer L/K est de degré 2, donc elle est non ramifiée en dehors des places qui divisent 2. Il en va de même pour la ramification logarithmique puisque $\ell = 2$ ([6] th.1.4). Il reste à examiner le cas des places paires. On considère une place $\mathfrak{p}$ de K au dessus de 2 et une place $\mathfrak{P}$ de L au dessus de $\mathfrak{p}$. On a donc :

$$\tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = \left[L_{\mathfrak{P}} : L_{\mathfrak{P}} \cap \widehat{\mathbb{Q}}_2^c K_{\mathfrak{p}}\right].$$

On s'intéresse au cas non logarithmiquement ramifiée pour pouvoir appliquer la version logarithmique du théorème 94 de Hilbert :

$$\tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = 1 \Leftrightarrow L_{\mathfrak{P}} \subseteq \widehat{\mathbb{Q}}_2^c K_{\mathfrak{p}}.$$

Et comme $L_{\mathfrak{P}} = K_{\mathfrak{p}}(i)$, on a l'équivalence

$$\tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = 1 \Leftrightarrow i \in \widehat{\mathbb{Q}}_2^c K_{\mathfrak{p}},$$

ou encore, puisque $\mathbb{Q}_2 \subseteq \widehat{\mathbb{Q}}_2^c K_{\mathfrak{p}}$:

$$\tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = 1 \Leftrightarrow \mathbb{Q}_2(i) \subseteq \widehat{\mathbb{Q}}_2^c K_{\mathfrak{p}}.$$

Le corps $\widehat{\mathbb{Q}}_2^c K_{\mathfrak{p}}$ est la composée de toutes les $\mathbb{Z}_q$-extensions cyclotomiques de $K_{\mathfrak{p}}$, où q décrit l'ensemble des nombres premiers. Elles sont linéairement disjointes sur $K_{\mathfrak{p}}$, de groupe de Galois $\mathbb{Z}_q$. Seul $\mathbb{Z}_2$ possède un quotient isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (qui est le groupe de Galois de $\mathbb{Q}_2(i)/\mathbb{Q}_2$), de sorte que la non-ramification (au sens logarithmique) en 2 se traduit plus simplement par

$$\mathbb{Q}_2(i) \subseteq \mathbb{Q}_2^c K_{\mathfrak{p}}.$$

L'extension $\mathbb{Q}_2^c/\mathbb{Q}_2$ étant cyclique, on peut même se limiter au premier étage de la tour définissant $\mathbb{Q}_2^c$, et la condition devient :

$$\mathbb{Q}_2(i) \subseteq \mathbb{Q}_2(\sqrt{2})K_{\mathfrak{p}}.$$

Ou encore, puisque $K_{\mathfrak{p}} = \mathbb{Q}_2(\sqrt{d})$:

$$\mathbb{Q}_2(i) \subseteq \mathbb{Q}_2(\sqrt{2})\mathbb{Q}_2(\sqrt{d}).$$

Le compositum $\mathbb{Q}_2(\sqrt{2})\mathbb{Q}_2(\sqrt{d})$ est une extension au plus biquadratique de $\mathbb{Q}_2$: elle contient au plus trois extensions quadratiques :

$$\mathbb{Q}_2(i), \mathbb{Q}_2(\sqrt{d}), \mathbb{Q}_2(\sqrt{2d}).$$

En général pour un corps M et deux éléments a, b de $M^\times$, nous avons

$$M(\sqrt{a}) = M(\sqrt{b}) \Leftrightarrow \frac{a}{b} \in M^{\times 2}.$$

On en déduit les équivalences suivantes

$$\begin{aligned}
\mathbb{Q}_2(i) = \mathbb{Q}_2(\sqrt{2}) &\Leftrightarrow -2 \in \mathbb{Q}_2^{\times 2}, \\
\mathbb{Q}_2(i) = \mathbb{Q}_2(\sqrt{d}) &\Leftrightarrow -d \in \mathbb{Q}_2^{\times 2}, \\
\mathbb{Q}_2(i) = \mathbb{Q}_2(\sqrt{2d}) &\Leftrightarrow -2d \in \mathbb{Q}_2^{\times 2}.
\end{aligned}$$

Il est connu (voir par exemple [18]) que les carrés de $\mathbb{Q}_2$ sont les $2^n u$, où u est une unité 2-adique congrue à 1 modulo 8, et n est un entier rationnel pair. Ainsi

$$\begin{aligned}
\mathbb{Q}_2(i) &\neq \mathbb{Q}_2(\sqrt{2}), \\
\mathbb{Q}_2(i) = \mathbb{Q}_2(\sqrt{d}) &\Leftrightarrow d \equiv -1 \mod 8, \\
\mathbb{Q}_2(i) = \mathbb{Q}_2(\sqrt{2d}) &\Leftrightarrow d \equiv -2 \mod 16.
\end{aligned}$$

En résumé, la version logarithmique du théorème 94 de Hilbert s'applique à l'extension L/K uniquement dans les cas suivants :

$$d \equiv -1 \mod 8, \quad d \equiv -2 \mod 16.$$

2.4.2 Le cas $d \equiv -1 \mod 8$

On a ici

$$\mathbb{Q}_2(i) = \mathbb{Q}_2(\sqrt{d}),$$

donc

$$\left[\mathbb{Q}_2(i, \sqrt{d}) : \mathbb{Q}_2\right] = 2,$$

c'est-à-dire

$$[L_{\mathfrak{P}} : \mathbb{Q}_2] = 2.$$

On en déduit le nombre g_2 de places de L au dessus de 2 :

$$2g_2 = [L : \mathbb{Q}],$$

$$g_2 = 2.$$

De même, puisque $[K_{\mathfrak{p}} : \mathbb{Q}_2] = [K : \mathbb{Q}]$, le corps K possède une seule place au dessus de 2.
On considère les groupes des unités logarithmiques de K :

$$\widetilde{E}_K = \mu_K \times < u_{\mathfrak{p}}, u_K >,$$

et de L :

$$\widetilde{E}_L = \mu_L \times < u_{\mathfrak{P}}, u_L >,$$

où u_K (resp. u_L) désigne l'unité fondamentale de K (resp. L), μ_K (resp. μ_L) le groupe des racines de l'unité de K (resp. L), et $u_{\mathfrak{p}}$, (resp. $u_{\mathfrak{P}}$) est une $\mathfrak{p}$-unité de K (resp. $\mathfrak{P}$-unité de L).
On a

$$\mu_K =< -1 >,\ \mu_L =< i >,$$

donc

$$N_{L/K}(\mu_L) =< 1 > .$$

On a aussi

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}.$$

D'autre part, d'aprés [1], les unités fondamentales u_L et u_K vérifient

$$u_L \in \{u_K, \sqrt{iu_K}\}.$$

Envisageons ces deux cas.

- Supposons que $u_L = u_K$. On a alors :

$$N_{L/K}(u_L) = u_L^2 = u_K^2,$$

et donc

$$\left[\widetilde{E}_K : N_{L/K}\left(\widetilde{E}_L\right)\right] = 4.$$

L/K étant une CM-extension, on a

$$\prod_{\mathfrak{p}\in P_K^\infty} d_{\mathfrak{p}}(L/K) = 4.$$

La version logarithmique du théorème 94 de Hibert nous donne alors

$$|\ \widetilde{cap}_{L/K}\ | = 1.$$

□

- Supposons que $u_L = \sqrt{iu_K}$. On a cette fois

$$N_{L/K}(u_L) = \sqrt{iu_K}\,\overline{\sqrt{iu_K}} = u_K,$$

ce qui nous donne

$$\left[\widetilde{E}_K : N_{L/K}\left(\widetilde{E}_L\right)\right] = 2.$$

C'est impossible puisque la ramification à l'infini conduit à un dénominateur égal à 4 dans la formule donnant $|\ \widetilde{cap}_{L/K}\ |$. □

2.4.3 Le cas $d \equiv -2 \mod 16$

La 2-valuation $v_2(d)$ est alors impaire, donc l'entier d n'est pas un carré de $\mathbb{Q}_2^\times$. Par conséquent :

$$\left[\mathbb{Q}_2\left(i, \sqrt{d}\right) : \mathbb{Q}_2\right] = 4,$$

c'est-à-dire

$$[L_{\mathfrak{P}} : \mathbb{Q}_2] = [L : \mathbb{Q}].$$

Cela entraîne que $\mathfrak{P}$ est la seule place de L au dessus de 2 (et donc $\mathfrak{p}$ est la seule place de K au dessus de 2). On a alors comme dans le cas précédent

$$\widetilde{E}_K = \mu_K \times < \mathfrak{p}, u_K >,\ \widetilde{E}_L = \mu_L \times < \mathfrak{P}, u_L > .$$

et toujours les deux cas :

- Si $u_L = u_K$. Alors

$$N_{L/K}(u_L) = u_L^2,$$
$$N_{L/K}(1+i) = 2,$$
$$N_{L/K}(\mu_L) =< 1 > .$$

D'où

$$\left[\widetilde{E}_K : N_{L/K}\left(\widetilde{E}_L\right)\right] = 4,$$

et là encore,

$$|\ \widetilde{cap}_{L/K}\ | = 1.$$

□

- Si $u_L = \sqrt{iu_K}$. Le seul changement est

$$N_{L/K}(u_L) = u_K.$$

D'où

$$\left[\widetilde{E}_K : N_{L/K}\left(\widetilde{E}_L\right)\right] = 2.$$

On aboutit encore à une impossibilité compte tenu de la complexification de L/K. □

2.4.4 Conclusion

On peut récapituler les résultat de cette étude dans le théorème qui suit.

Théorème 2.4.1 *Si d est un entier supérieur à 2, sans facteur carré, et congru à -1,7 ou -2 modulo 16, alors aucune classe logarithmique ne capitule dans* $\mathbb{Q}\left(i, \sqrt{d}\right)/\mathbb{Q}\left(\sqrt{d}\right)$.

Remarque 2.4.2
On voit que dans les deux cas étudiés, on a $u_L = u_K$. La preuve de ce résultat est ici indirecte.

2.4.5 Confrontation avec des résultats numériques connus

Dans [15], Florence Soriano donne la liste des extensions quadratiques 2-logarithmiquement principale (i.e. dont le 2-groupe des classes logarithmiques est trivial) de $\mathbb{Q}$. Lorsque le corps K appartient à cette liste, on a trivialement $\widetilde{cap}_{L/K} = 0$. C'est le cas pour certains des entiers d du théorème 2.4.1 (pour ceux-ci, ce résultat n'apporte rien), et il peut être intéressant de mettre en évidence le caractère non-trivial de ce théorème. Commençons par rappeler en substance les résultats de [15].

Théorème 2.4.3 *Les extensions quadratiques réelles 2-logarithmiquement principales de* $\mathbb{Q}$ *sont les extensions* $\mathbb{Q}(\sqrt{d})$ *où l'entier* d *vérifie l'une des conditions ci-dessous (les lettres* p, q, r *désignant des nombres premiers).*

- $d = 2$ *;*
- $d \in \{p, 2p\}$*, avec* $p \not\equiv 1 \mod 16$ *;*
- $d \in \{p, 2p\}$*, avec* $p \equiv 1 \mod 16$ *et -1 est la norme d'un élément* $\frac{u+\sqrt{d}}{v}$ *de* $\mathbb{Q}(\sqrt{d})$ *tel que l'entier* u *soit congru respectivement à* $\pm 7 \mod 16$, $\pm 1 \mod 16$, $\pm 3 \mod 8$ *selon que* d *est congru à 1,17 ou 2 modulo 32.*
- $d = pq$ *ou* $d = 2pq$*, avec* $(p \equiv -1 \mod 16,\ q \equiv -9 \mod 16)$ *ou* $(p \equiv \pm 3 \mod 8,\ q \not\equiv 1 \mod 8)$ *;*
- $d = pqr$ *ou* $d = 2pqr$*, avec* $p \equiv 1 \mod 8$, $q \equiv 5 \mod 8$, $r \equiv -1 \mod 8$.

On observe en particulier le fait suivant : si d est congru à -1,7 ou -2 modulo 16 et si de plus d est de l'une des formes $pq, 2pq, pqr, 2pqr$, où p, q et r sont des nombres premiers, alors $\widetilde{Cl}_K$ est non trivial cependant que $\widetilde{cap}_{L/K} = 0$ l'est.

2.5 Approche algorithmique

Le groupe $\widetilde{cap}_{L/K}$ est accessible au calcul numérique. L'algorithme qui suit utilise les fonctions suivantes :

- Calcul du groupe des classes logarithmiques d'un corps de nombres ;
- calcul de « l'étendu » $\sum_{\mathfrak{P}|\mathfrak{p}} \tilde{e}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\mathfrak{P}$ à $\widetilde{Cl}_L$ d'un diviseur logarithmique premier $\mathfrak{p}$ de K à l'aide de l'algorithme du logarithme discret ;
- calcul du noyau entier d'une matrice rectangulaire.

Les deux premières fonctions, implémentées notamment dans le logiciel Magma, ont été développées par F. Diaz y Diaz, J.F. Jaulent, S. Pauli, M. Pohst et F. Soriano-Gafiuk.

2.5.1 Le calcul des groupes de classes logarithmiques

Les auteurs de [2] ont développé un algorithme qui fournit, pour un corps de nombres K, une famille de générateurs $([a_i]_K)_{1\leqslant i\leqslant n}$ du groupe $\widetilde{Cl}_K$ (a_i désigne un diviseur logarithmique de degré nul de K et $[a_i]_K$ est sa classe modulo $\widetilde{Pl}_K$), ainsi que leur ordre ℓ^{n_i} (c'est une puissance de ℓ puisque $\widetilde{Cl}_K$ est un ℓ-groupe). On obtient donc la décomposition de $\widetilde{Cl}_K$ en somme directe de groupes cycliques :

$$\widetilde{Cl}_K \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/\ell^{n_i}\mathbb{Z}[a_i]_K.$$

Et on fait de même pour une extension finie L de K :

$$\widetilde{Cl}_L \simeq \bigoplus_{j=1}^{m} \mathbb{Z}/\ell^{m_j}\mathbb{Z}[b_j]_L.$$

2.5.2 Extension à L des générateurs de $\widetilde{Cl}_K$

Notant $\tilde{j}$ comme en 2.1.1, le morphisme d'extension de $\widetilde{Cl}_K$ dans $\widetilde{Cl}_L$, on écrit :

$$\tilde{j}\,([a_i]_K) = [a_i]_L.$$

Pour chaque entier i compris entre 1 et n, l'élément $[a_i]_L$ de $\widetilde{Cl}_L$ s'exprime alors à l'aide des générateurs de $\widetilde{Cl}_L$:

$$[a_i]_L = \sum_{j=1}^{m} a_{i,j}[b_j]_L,$$

où $a_{i,j}$ est un entier compris entre 0 et $\ell^{m_j} - 1$.

2.5.3 Condition d'appartenance à $\widetilde{cap}_{L/K}$

On considère la classe $[a]_K$ d'un diviseur logarithmique de degré nul de K. Exprimé en fonction des générateurs de $\widetilde{Cl}_K$, il s'écrit

$$[a]_K = \sum_{i=1}^{n} \alpha_i [a_i]_K.$$

On en tire l'expression de son étendu à L :

$$\begin{aligned}
[a]_L &= \sum_{i=1}^{n} \alpha_i \ [a_i]_L \\
[a]_L &= \sum_{i=1}^{n} \alpha_i \left(\sum_{j=1}^{m} a_{i,j} \ [b_j]_L \right) \\
[a]_L &= \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{i,j} \ \alpha_i \right) [b_j]_L.
\end{aligned}$$

Pour que $[a]_K$ appartienne à $\widetilde{cap}_{L/K}$, il faut et il suffit successivement que :

$$[a]_L = [0]_L,$$

$$\forall j \in \{1, \ldots, m\}, \ \sum_{i=1}^{n} a_{i,j} \ \alpha_i \equiv 0 \mod \ell^{m_j},$$

$$\forall j \in \{1, \ldots, m\}, \ \exists \lambda_j \in \mathbb{Z}, \ \sum_{i=1}^{n} a_{i,j} \ \alpha_i = \lambda_j \ell^{m_j},$$

$$\exists (\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m, \ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \\ -\lambda_1 \\ \vdots \\ -\lambda_m \end{pmatrix} \in \ker \begin{pmatrix} a_{1,1} & \ldots & a_{n,1} & & & \\ \vdots & & \vdots & & \ddots & \\ a_{1,m} & \ldots & a_{n,m} & & & \ell^{m_n} \end{pmatrix},$$

où le noyau considéré est le "noyau entier", c'est-à-dire l'intersection du noyau habituel avec $\mathbb{Z}^{m+n}$. On note A la matrice de terme général $a_{i,j}$, de sorte que la condition nécessaire et suffisante d'appartenance à $\widetilde{cap}_{L/K}$ est

$$\exists (\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m, \ {}^t(\alpha_1, \ldots, \alpha_n, -\lambda_1, \ldots, -\lambda_m) \in \left[{}^tA | \mathrm{diag}(\ell^{m_1}, \ldots, \ell^{m_n}) \right],$$

où $[{}^tA|\mathrm{diag}(\ell^{m_1}, \ldots, \ell^{m_n})]$ est la concaténation de la matrice A et de la matrice diagonale $\mathrm{diag}(\ell^{m_1}, \ldots, \ell^{m_n})$. En ne gardant que les n premières coordonnées de

chaque générateur du noyau ci-dessus, on obtient un système de générateurs de $\widetilde{cap}_{L/K}$ que l'on note $\{[g_1]_K, \ldots, [g_r]_K\}$, avec

$$\forall i \in \{1, \ldots r\},\ [g_i]_K = \sum_{j=1}^{n} g_{i,j}[a_j]_K.$$

Le calcul du groupe $\widetilde{cap}_{L/K}$ est ainsi achevé pour autant que les générateurs obtenus soient calculables. Le but cherché étant plutôt la détermination de $\widetilde{cap}_{L/K}$ en tant que groupe abstrait, il convient à présent de calculer un système complet de relations liant les générateurs. C'est l'objet du paragraphe qui suit.

2.5.4 Relations entre les $[g_i]_K$

On a donc $\widetilde{cap}_{L/K} =< [g_1]_K, \ldots, [g_r]_K >$ et si $\{x_1, \ldots, x_r\} \in \mathbb{Z}^r$, la relation $\sum_{i=1}^{r} x_i[g_i]_K = [0]_K$ équivaut successivement aux suivantes :

$$\sum_{i=1}^{r} x_i \sum_{j=1}^{n} g_{i,j}[a_j]_K = [0]_K,$$

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{r} x_i g_{i,j} \right) [a_j]_K = [0]_K,$$

$$\forall j \in \{1, \ldots, n\},\ \sum_{i=1}^{r} x_i g_{i,j} \equiv 0 \mod \ell^{n_j},$$

$$\forall j \in \{1, \ldots, n\},\ \exists \mu_j \in \mathbb{Z},\ \sum_{i=1}^{r} x_i g_{i,j} = \mu_j \ell^{n_j},$$

$$\exists (\mu_1, \ldots, \mu_n) \in \mathbb{Z}^m,\ \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ -\mu_1 \\ \vdots \\ -\mu_n \end{pmatrix} \in \ker \begin{pmatrix} g_{1,1} & \cdots & g_{r,1} & \ell^{n_1} & & \\ \vdots & & \vdots & & \ddots & \\ g_{1,n} & \cdots & g_{r,n} & & & \ell^{n_n} \end{pmatrix}.$$

Un système complet de relations entre les $[g_i]_K$ nous est donc fourni par le noyau (entier) de la matrice $[{}^tG|\mathrm{diag}(\ell^{n_1}, \ldots, \ell^{n_n})]$, où G est la matrice de terme général $g_{i,j}$.

Chapitre 3

Tours localement cyclotomiques

Les classes logarithmiques ont été introduites en 1994 dans [6] pour l'étude des ℓ-extensions abéliennes d'un corps de nombres en liaison avec la K-théorie. Jean-François Jaulent montre dans cet article, via la théorie ℓ-adique du corps de classes, que le groupe de Galois de la ℓ-extension K^{lc}/K^c s'identifie au groupe $\widetilde{Cl}_K$ des classes logarithmiques du corps de nombre K. Ce groupe est accessible au calcul numérique (cf. [2]), et la conjecture de Gross généralisée affirme qu'il est toujours fini (cf. [4]). Lorsqu'il est trivial, le corps K est dit *logarithmiquement principal*. Dans le cas contraire, la question du plongement d'un corps K dans une telle extension a été posée dans [8]. Pour les groupes de classes au sens usuel, le problème, classique, est celui de la finitude de la tour de Hilbert sur K (cf. [3] et [14]). Une transposition, dans le cadre de l'arithmétique des classes logarithmiques a permis à Jean-François Jaulent et Florence Soriano-Gafiuk de construire, canoniquement, une tour $(K_n)_{n\in\mathbb{N}}$ d'extensions de K. Si cette tour est finie, on dispose d'une extension K_∞ de K dont le groupe des classes logarithmiques est trivial.
La construction de la tour repose sur la notion de pro-ℓ-extension localement cyclotomique d'un corps de nombres, dont nous donnons une caractérisation. Les auteurs de [8] ont obtenu des conditions nécessaires et suffisantes de finitude de cette tour, ainsi qu'une condition suffisante d'infinitude. Dans cette partie, nous proposons une version *relative* de ces résultats dans le sens où nous nous attachons à préciser les conditions de finitude de la tour sur une extension L d'un corps K ayant lui une tour finie. Parce que le rôle de la ramification logarithmique dans L/K s'avère crucial dans la propagation de la finitude de K à L, nous sommes conduits à chercher les corps L ayant une tour infinie parmi les extensions notablement ramifiées (au sens logarithmique) de K. Un critère d'infinitude allant dans ce sens est obtenu dans la dernière partie. Son effectivité est testée sur plusieurs exemples.
Nous rappelons ci-dessous les notations plus particulièrement utilisées dans ce

chapitre.
Un nombre premier ℓ est fixé une fois pour toutes. Pour chaque corps de nombres K on note :

- P_K^0, l'ensemble des places finies de K,
- $R_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$, le compactifié ℓ-adique de $K^\times$,
- K^c, la $\mathbb{Z}_\ell$-extension cyclotomique de K,
- K^{lc}, la $\mathbb{Z}_\ell$-extension localement cyclotomique de K, i.e. l'extension abélienne de K totalement décomposée sur K^c, maximale,
- $Dl_K = \bigoplus_{\mathfrak{p} \in P_K^0} \mathbb{Z}_\ell \ \mathfrak{p}$, le groupe des diviseurs logarithmiques de K,
- Pl_K, le groupe des diviseurs logarithmiques principaux de K,
- $Cl_K = Dl_K/Pl_K$, le groupe des classes logarithmiques de K (non nécessairement de degré nul),
- $\widetilde{Dl}_K, \widetilde{Pl}_K, \widetilde{Cl}_K$, les groupes correspondants formés des diviseurs, diviseurs principaux, et classes logarithmiques de degré nul ($\widetilde{Pl}_K = Pl_K$ et $\widetilde{Cl}_K = \widetilde{Dl}_K/\widetilde{Pl}_K$),
- $\tilde{E}_K$, le groupe des unités logarithmiques de K, i.e. le noyau de l'homomorphisme $R_K \to \widetilde{Pl}_K$.

D'autre part, *on travaille sous la conjecture de Gross généralisée* ou, ce qui revient au même, on suppose que pour tous les corps de nombres considérés, le groupe des classes logarithmiques est fini.

3.1 La ℓ-extension localement cyclotomique d'un corps de nombres

On note K^c la $\mathbb{Z}_\ell$-extension cyclotomique de K. Il existe donc une suite croissante $(K_n)_{n\in\mathbb{N}}$ de corps de nombres telle que

$$K^c = \bigcup_{n\in\mathbb{N}} K_n.$$

Pour chaque entier n, désignons par K_n^{lc} l'extension abélienne maximale de K qui est totalement décomposée sur K_n. La suite $(K_n^{lc})_{n\in\mathbb{N}}$ est croissante et sa réunion est une ℓ-extension de degré infini de K, qu'on appelle la $\mathbb{Z}_\ell$-extension localement cyclotomique de K. On la note K^{lc}. Bien entendu, K^{lc} est une extension de K^c, et on dira simplement que K^{lc} est l'extension abélienne maximale de K qui est totalement décomposée sur K^c.
Considérons une place finie $\mathfrak{p}$ de K et notons encore, pour toute extension finie L de K, $L_\mathfrak{p}$ le complété de L en une place de L au dessus de $\mathfrak{p}$. Ce qui précède peut alors s'exprimer par l'égalité

$$(K_n^{lc})_\mathfrak{p} = (K_n^c)_\mathfrak{p},$$

valable pour tout entier n. Pour cette raison, on dira que K^{lc} est l'extension abélienne maximale de K dont la complétion en toute place $\mathfrak{p}$ coïncide avec la complétion correspondante de K^c :

$$K_\mathfrak{p}^{lc} = K_\mathfrak{p}^c.$$

Remarquons que $K_\mathfrak{p}^c$ est le compositum des extensions K^c et $K_\mathfrak{p}$ (on a ici suivi [11] pour les questions de décomposition dans une extension de degré infini).
On sait, via la théorie ℓ-adique du corps de classe ([6] ou [7]), que le groupe de Galois de l'extension K^{lc}/K^c est isomorphe au ℓ-groupe des classes logarithmiques $\widetilde{Cl}_K$ de K. Le résultat de croissance suivant nous sera utile.

Proposition 3.1.1 *Si L/K est une extension de corps de nombres, alors $K^{lc} \subset L^{lc}$.*

Démonstration. La démonstration utilise le lemme qui suit.

Lemme 3.1.2 *Soit A un corps, B une extension de A, C une extension finie de A, et $D = BC$. Si l'extension B/A est totalement décomposée, alors l'extension D/C est totalement décomposée.*

DÉMONSTRATION DU LEMME. C'est une conséquence immédiate de [11] (p.40, SC2), qui affirme que si $\mathfrak{p}$ est une place de A totalement décomposée dans B, alors une place $\mathfrak{P}$ de C au dessus de $\mathfrak{p}$ est totalement décomposée dans D. □

On applique le lemme au schéma suivant :

$$\begin{array}{ccc} L^{lc} & \text{——} & L^cK^{lc} \\ | & & | \\ K^c & \text{——} & K^{lc} \end{array}$$

L'extension K^{lc}/K^c est totalement décomposée et puisque $[L^c : K^c] \leqslant [L : K]$, L^c est de degré fini sur K^c. Il en résulte que l'extension L^cK^{lc}/L^c est totalement décomposée. (i)
D'autre part, le caractère abélien de l'extension K^{lc}/K se transmet à $K^{lc}L/KL$. Les égalités évidentes $KL = L$ et $K^{lc}L = K^{lc}L^c$ permettent de montrer que l'extension L^cK^{lc}/L est abélienne. (ii)
Le caractère maximal de L^{lc} pour les propriétés satisfaites par L^cK^{lc} en (i) et (ii) conduit alors à l'inclusion :

$$K^{lc}L^c \subset L^{lc}.$$

La proposition en découle immédiatement. □

Corollaire 3.1.3 *Pour deux corps de nombres K et L, on a*

$$K^{lc}L^{lc} \subset (KL)^{lc}.$$

DÉMONSTRATION. Il suffit d'appliquer la proposition avec les inclusions $K \subset KL$ et $L \subset KL$. □

Remarque 3.1.4
On peut remarquer que pour deux corps de nombres K et L, l'inclusion $K^c \subset L^c$ n'entraîne pas $K^{lc} \subset L^{lc}$. En effet, si tel était le cas, l'égalité $K^c = L^c$ des $\mathbb{Z}_\ell$-extensions cyclotomiques entraînerait celle, $K^{lc} = L^{lc}$, des $\mathbb{Z}_\ell$-extensions localement cyclotomiques correspondantes. En particulier les étages K_n de la tour cyclotomique K^c/K d'un corps de nombres auraient tous la même extension localement cyclotomique, et donc le même groupe des classes logarithmiques. Or on dispose d'exemples où l'ordre du groupe $\widetilde{Cl}_{K_n}$ tend vers l'infini avec n (voir [9], th.2.1 par exemple). Dans cet ordre d'idée, on dispose pour le groupe $\widetilde{Cl}_{K_n}$ d'un analogue du théorème d'Iwasawa : il existe des entiers positifs λ, μ, ν et un rang N à partir duquel l'ordre de $\widetilde{Cl}_{K_n}$ est $\ell^{\mu\ell^n+\lambda n+\nu}$.

Le théorème suivant caractérise l'extension K^{lc} en termes de ramification logarithmique.

Théorème 3.1.5 *Si K est un corps de nombres, K^{lc} est la ℓ-extension abélienne, non ramifiée logarithmiquement, maximale de K.*

Démonstration. La définition de K^{lc} entraîne, pour toute place $\mathfrak{p}$ de K :

$$K_{\mathfrak{p}}^{lc} = K_{\mathfrak{p}}^{c}.$$

Il s'ensuit que l'indice de ramification logarithmique $\left[K_{\mathfrak{p}}^{lc} : K_{\mathfrak{p}}^{lc} \cap K_{\mathfrak{p}}^{c}\right]$ est égal à 1. Inversement, soit L une ℓ-extension abélienne, non ramifiée logarithmiquement de K. On a donc pour toute place $\mathfrak{p}$ de K et toute place $\mathfrak{P}$ de L au dessus de $\mathfrak{p}$,

$$L_{\mathfrak{P}} \subset K_{\mathfrak{p}}^{c}.$$

Ainsi le compositum LK^{lc} vérifie :

$$\left(LK^{lc}\right)_{\mathfrak{p}} = L_{\mathfrak{p}} K_{\mathfrak{p}}^{lc} = K_{\mathfrak{p}}^{c}.$$

Autrement dit, l'extension LK^{lc}/K^{c} est totalement décomposée. Par ailleurs l'extension LK^{lc}/K est abélienne, comme composée de deux extensions abéliennes. Le caractère maximal de K^{lc} pour les deux propriétés précédentes nous donne alors l'inclusion :

$$LK^{lc} \subset K^{lc},$$

et par suite :

$$L \subset K^{lc}.$$

□

3.2 La ℓ-tour localement cyclotomique d'un corps de nombres

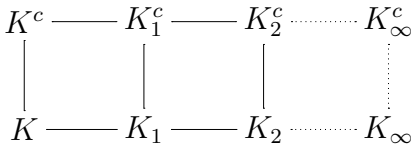
Dans [8], Florence Soriano-Gafiuk et Jean-François Jaulent ont construit canoniquement, pour un corps de nombre K, une tour $(K_n)_{n\in\mathbb{N}}$ d'extensions de K de façon qu'à chaque étage n, on ait :

$$K_n^{lc} = K_{n+1}^c.$$

L'extension K_{n+1}/K_n est abélienne, de groupe de Galois isomorphe au produit $\widetilde{Cl}_{K_n} \times \mathbb{Z}/e_n\mathbb{Z}$, où e_n est l'exposant du groupe $\widetilde{Cl}_{K_n}$. Sous l'hypothèse de Gross généralisée (relativement au premier ℓ), les corps K_n existent et sont des extensions finies du corps K. On pose alors :

$$K_\infty = \bigcup_{n\in\mathbb{N}} K_n.$$

On a donc le schéma suivant :



Il importe de préciser que les corps K_{n+1} et K_n^c ne sont, en général, pas linéairement disjoints sur K_n. En effet, K_{n+1} est le compositum de tous les corps F vérifiant

$$\begin{cases} F \cap K_n^c = K_n \\ FK_n^c = K_n^{lc} \end{cases}$$

Pour cette tour $(K_n)_{n\in\mathbb{N}}$, dite *tour localement cyclotomique de* K, deux cas peuvent se présenter :

- Soit $[K_\infty : K] < +\infty$. Dans ce cas, la suite $(K_n)_{n\in\mathbb{N}}$ est stationnaire :

  $$\exists n_0 \in \mathbb{N} \ / \ K_\infty = K_{n_0},$$

  avec

  $$K_{n_0}^{lc} = K_{n_0}^c.$$

  On dit alors que la tour localement cyclotomique sur K est finie et on note $T(K) < +\infty$.
- Soit $[K_\infty : K] = +\infty$. Dans ce cas, la tour localement cyclotomique sur K est infinie et on note $T(K) = +\infty$.

3.3 Finitude de la ℓ-tour localement cyclotomique

3.3.1 Quelques critères

Lorsque $T(K) < +\infty$, le corps K_∞ est une extension de K pour laquelle $K_\infty^{lc} = K_\infty^c$. Ce cas donne lieu à la définition qui suit.

Définition 3.3.1 *On dit d'un corps de nombre L qu'il est logarithmiquement principal lorsque $L^{lc} = L^c$ (i.e. lorsque $\widetilde{Cl}_L = 0$).*

Inversement, si K possède une extension L vérifiant $L^{lc} = L^c$, on peut montrer que $T(K) < +\infty$. C'est le critère de finitude donné dans [8] et qui fait l'objet du théorème suivant.

Théorème 3.3.2 *On a $T(K) < +\infty$ si et seulement s'il existe une extension finie L de K qui est logarithmiquement principale.*

En raison de cette caractérisation, la qualification de *quasi-logarithmiquement principal* a été proposée dans [8] pour un tel corps K.
Ce théorème entraîne immédiatement la conséquence suivante :

Corollaire 3.3.3 *Si $T(K) < +\infty$, et si k est une sous-extension de K, alors $T(k) < +\infty$.*

Démonstration. En effet $k \subset K \subset K_\infty$ et le corps K_∞ est logarithmiquement principal. □

Un second critère fait appel à la pro-ℓ-extension complètement décomposée maximale de K^c, que l'on notera $(K^c)^{cd}$.

Théorème 3.3.4 *L'extension K_∞/K est finie si et seulement si le groupe de Galois de $(K^c)^{cd}$ sur K^c est fini.*

3.3.2 Cas d'un compositum de deux corps

On peut se demander si la finitude de tour localement localement cyclotomique est une propriété stable par composition de corps. L'exemple qui suit montre que ce n'est pas le cas. On suppose que $\ell = 2$. D'une part, selon [8], le corps quadratique $\mathbb{Q}\left(\sqrt{255255}\right)$ possède une tour localement cyclotomique infinie. D'autre part, selon [15] (Théorème 6.1.2), les corps $\mathbb{Q}\left(\sqrt{d}\right)$ où $d \in \{3, 5, 11, 13, 119\}$ sont logarithmiquement principaux (dans les quatre premiers cas, d est un nombre premier congru à ± 3 modulo 8 ; et 119 est le produit de deux nombres premiers, l'un congru

à -1, l'autre à -9 modulo 16). Il s'ensuit que leur tour localement cyclotomique est triviale. On note Ω le compositum de ces cinq corps. Comme $\mathbb{Q}\left(\sqrt{255255}\right) \subset \Omega$, le corollaire 3.3.3 permet d'affirmer que $T(\Omega) = +\infty$. Considérons l'ensemble Σ formé des cinq corps $\mathbb{Q}\left(\sqrt{3}\right), \mathbb{Q}\left(\sqrt{5}\right), \mathbb{Q}\left(\sqrt{11}\right), \mathbb{Q}\left(\sqrt{13}\right), \mathbb{Q}\left(\sqrt{119}\right)$ et des composés d'au plus quatre de ces corps. Ce qui précède montre qu'il existe deux corps K et L appartenant à Σ tels que :

$$T(K) < +\infty, \quad T(L) < +\infty, \quad \text{et} \quad T(KL) = +\infty.$$

Pour ces deux corps, on a également le fait suivant :

$$K_\infty^{lc} L_\infty^{lc} = K_\infty^c L_\infty^c = (K_\infty L_\infty)^c \neq (K_\infty L_\infty)^{lc}.$$

Il existe donc deux corps de nombres M et N pour lesquels

$$M^{lc} N^{lc} \subsetneq (MN)^{lc}.$$

3.3.3 Relation avec la ramification logarithmique

Commençons par complèter les critères de finitude précédents.

Théorème 3.3.5 *Si K est un corps de nombres dont la tour localement cyclotomique est finie, alors quel que soit le corps de nombres L vérifiant $L \subseteq K_\infty^c$, la tour localement cyclotomique sur L est également finie.*

Démonstration. L'hypothèse $L \subseteq K_\infty^c$ montre que les corps K_∞ et LK_∞ sont *surcirculairement équivalents* :

$$(LK_\infty)^c = L^c K_\infty^c \subseteq K_\infty^c,$$

l'inclusion inverse étant évidente, on a bien :

$$(LK_\infty)^c = K_\infty^c.$$

Selon [8] (scolie 6), deux corps de nombres surcirculairement équivalents sont simultanément logarithmiquement principaux ou pas. Par hypothèse, K_∞ est logarithmiquement principal, si bien que LK_∞ l'est aussi. Le corps LK_∞ est une extension finie et logarithmiquement principale de L. On en déduit, avec 3.3.3, que L a une tour localement cyclotomique finie. □

Remarque 3.3.6
Avec la terminologie introduite précédemment, le théorème précédent peut encore se formuler ainsi :
les corps de nombres contenus dans un corps surcirculaire strictement ℓ-principal sont quasi-logarithmiquement principaux.

Dans le théorème précédent, on ne suppose pas que L est une extension de K. Cependant le cas de figure $K \subset L$ est susceptible de la réciproque qui suit.

Théorème 3.3.7 *Soit K un corps de nombres dont la tour localement cyclotomique est finie. Si L/K est une ℓ-extension finie, non ramifiée logarithmiquement, alors $L \subset K_\infty^c$.*

Démonstration. Une ℓ-extension étant résoluble, il existe une suite de groupes :

$$G_n = 1 \subset G_{n-1} \subset \ldots \subset G_0 = Gal(L/K),$$

telle que les quotients G_i/G_{i+1} soient abéliens. En conséquence, il existe une tour d'extensions de K :

$$K - K^{(1)} - K^{(2)} - \ldots - K^{(n)} = L,$$

telle que pour chaque indice i, l'extension $K^{(i+1)}/K^{(i)}$ soit abélienne.
Afin de montrer que chacun des étages de cette tour (et donc L) est inclus dans K_∞^{lc}, on raisonne par récurrence sur l'étage i de la tour. On suppose donc que :

$$K^{(i)} \subset K_\infty^c.$$

Puisque $K^{(i)}$ est de degré fini sur K, l'inclusion précédente permet d'affirmer que $K^{(i)}$ est inclus dans un étage K_∞^n de la tour cyclotomique sur K_∞. L'égalité évidente

$$(K_\infty^n)^c = K_\infty^c$$

signifie que K_∞^n et K_∞ sont surcirculairement équivalents ; ce qui, d'après [8], scolie 6, entraîne que K_∞^n est logarithmiquement principal :

$$(K_\infty^n)^c = (K_\infty^n)^{lc}.$$

Le théorème 3.1.5 appliqué à l'extension (abélienne non ramifiée logarithmiquement) $K^{(i+1)}/K^{(i)}$ nous donne alors l'inclusion

$$K^{(i+1)} \subset \left(K^{(i)}\right)^{lc}.$$

Ainsi, compte tenu de la proposition 3.1.1,

$$K^{(i+1)} \subset (K_\infty^n)^{lc} = (K_\infty^n)^c = (K_\infty)^c ;$$

ce qui achève la récurrence. □

Corollaire 3.3.8 *Si K est un corps de nombres tel que $T(K) < +\infty$, et si L est une ℓ-extension finie, non ramifiée logarithmiquement de K, alors $T(L) < +\infty$.*

Démonstration. C'est une conséquence immédiate du théorème précédent compte tenu de 3.3.5 □

3.3.4 Relation avec les groupes des classes logarithmiques des étages de K^c

Notons E_n, $n \in \mathbb{N}^*$ les étages de la $\mathbb{Z}_\ell$-extension cyclotomique K^c de K et, pour chaque n, $\widetilde{Cl}_n$ le groupe des classes logarithmiques de E_n. Les corps E_n ont la même $\mathbb{Z}_\ell$-extension cyclotomique K^c, alors que l'inclusion $E_n \subset E_{n+1}$ entraîne celle des extensions localement cyclotomiques correspondantes :

$$E_n^{lc} \subset E_{n+1}^{lc}.$$

Par conséquent $\widetilde{Cl}_n$ est un quotient de $\widetilde{Cl}_{n+1}$ et en particulier la suite des ordres $\left(|\widetilde{Cl}_n|\right)_{n\in\mathbb{N}^*}$ est croissante. Le résultat qui suit établit un lien avec le cas de finitude de la tour localement cyclotomique de K.

Proposition 3.3.9 *Si $T(K) < +\infty$, alors la suite $\left(|\widetilde{Cl}_n|\right)_{n\in\mathbb{N}^*}$ est stationnaire.*

Démonstration. Pour n fixé le corps E_n^{lc} est une extension abélienne et totalement décomposée de K^c, donc $E_n^{lc} \subset K_\infty^c$, mais K_∞^c/K est une extension finie, donc E_n^{lc}/K est finie également. □

En particulier l'hypothèse $T(K) < +\infty$ entraîne que les entiers λ_K et μ_K attachés au module d'Iwasawa $Gal(K_\infty^c/K)$ sont nuls.

3.4 Critères d'infinitude

On considère une ℓ-extension L/K de corps de nombres. Le théorème 11 de [8] énonce la condition suffisante ci-dessous pour que la ℓ-tour localement cyclotomique sur L soit infinie :

$$rg_\ell\, \widetilde{Cl}_L \geqslant 1 + 2\sqrt{r_L + c_L + \delta_L + 1} \implies T(L) = +\infty,$$

où r_L et $2c_L$ sont respectivement le nombre de places réelles et complexes du corps L, et où δ_L est égal à 1 ou 0 selon que L contient ou non les racines ℓ-ème de l'unité.
Par ailleurs, on a vu que si $T(K) = +\infty$, alors $T(L) = +\infty$. Par contre, si $T(K) < +\infty$ tout est possible pour $T(L)$ et on souhaite relier le cas d'infinitude de la tour sur L à des invariants liés à l'extension L/K. Dans cette direction, Jean-François Jaulent et Christian Maire ont obtenu le résultat qui fait l'objet du théorème 3.4.1 et dont nous détaillons la preuve. Nous démontrons ensuite un résultat un peu plus général.

3.4.1 Un théorème de Jaulent et Maire

Théorème 3.4.1 *Soit L/K une extension cyclique de degré ℓ. On note $\rho_{L/K}$ la somme du nombre de places réelles de K se complexifiant dans L et du nombre de places finies logarithmiquement ramifiées de K. Alors l'inégalité*

$$\rho_{L/K} \geqslant 2 + 2\sqrt{r_L + c_L + \delta_L + 1} + rg_\ell \tilde{E}_K$$

entraîne $T(L) = +\infty$.

Nous donnons ci-dessous la preuve de ce théorème. Elle utilise un résultat de théorie logarithmique des genres. Par ℓ-corps des genres logarithmiques attaché à l'extension L^{lc}/K, on entend la plus grande sous-extension M de L^{lc} qui est abélienne sur K. Le résultat en question, pour lequel nous renvoyons à [9], consiste en l'exactitude de la suite

$$1 \to \tilde{E}_K/(\tilde{E}_K \cap N_{L/K}^{loc}) \to \bigoplus_{\mathfrak{p}\in P_K^\infty} D_\mathfrak{p}(M/K) \bigoplus_{\mathfrak{p}\in P_K^0} \tilde{I}_\mathfrak{p}(M/K) \to Gal(M/K^{lc}) \to 1$$

où $D_\mathfrak{p}(M/K)$ est le groupe de décomposition de la place $\mathfrak{p}$ de K, $I_\mathfrak{p}(M/K)$ est son sous-groupe d'inertie logarithmique dans l'extension abélienne M/K et $\tilde{E}_K \cap N_{L/K}^{loc}$ est le groupe des unités logarithmiques de K qui sont normes locales partout dans L/K. D'autre part, on a besoin du lemme qui suit.

Lemme 3.4.2 *Étant donnée une suite exacte*

$$0 \longrightarrow A \xrightarrow{u} B \xrightarrow{v} C \longrightarrow 0$$

de $\mathbb{Z}_\ell$-modules, on a l'inégalité

$$rg_\ell\ B \leqslant rg_\ell\ A + rg_\ell\ C.$$

Démonstration du lemme. En tensorisant par μ_ℓ, la suite exacte de l'hypothèse donne lieu à la suite exacte de $\mathbb{F}_\ell$-espaces vectoriels :

$$\mu_\ell \otimes A \xrightarrow{\bar{u}} \mu_\ell \otimes B \xrightarrow{\bar{v}} \mu_\ell \otimes C \longrightarrow 0$$

(Voir [10], XVI, §2.6). Le théorème du rang nous donne :

$$\dim_{F_\ell} \mu_\ell \otimes B = \dim_{F_\ell} \mathrm{Im}\bar{v} + \dim_{F_\ell} \ker \bar{v}.$$

Mais $\ker \bar{v} = \mathrm{Im}\bar{u}$ et $\mathrm{Im}\bar{v} = \mu_\ell \otimes C$, donc

$$\dim_{F_\ell} \mu_\ell \otimes B = \dim_{F_\ell} \mathrm{Im}\bar{u} + \dim_{F_\ell} \mu_\ell \otimes C.$$

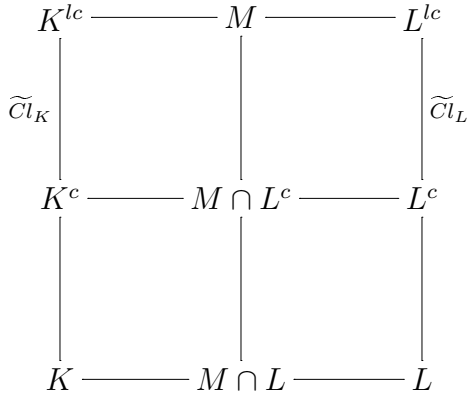
La majoration évidente $\dim_{F_\ell} \mathrm{Im}\bar{u} \leqslant \dim_{F_\ell} \mu_\ell \otimes A$ conduit alors à l'inégalité :

$$\dim_{F_\ell} \mu_\ell \otimes B \leqslant \dim_{F_\ell} \mu_\ell \otimes A + \dim_{F_\ell} \mu_\ell \otimes C.$$

C'est bien le lemme. □

Revenons à présent au théorème 3.4.1.

Démonstration. On considère le schéma suivant :



Le groupe de Galois de l'extension L^c/K^c est isomorphe à celui de l'extension $L/L \cap K^c$. L'inclusion $Gal(L/L \cap K^c) \subset Gal(L/K)$ nous donne alors l'inégalité

$$rg_\ell Gal(L/K) \geqslant rg_\ell Gal(L^c/K^c) \geqslant rg_\ell Gal(M \cap L^c/K^c).$$

D'autre part les isomorphismes

$$Gal(M/K^c) \simeq Gal(M/M \cap L^c) \times Gal(M \cap L^c/K^c) \simeq \widetilde{Cl}_L \times Gal(M \cap L^c/K^c)$$

imposent la seconde inégalité

$$rg_\ell Gal(M/K^c) \leqslant rg_\ell \widetilde{Cl}_L + rg_\ell Gal(M \cap L^c/K^c).$$

On en déduit

$$rg_\ell \widetilde{Cl}_L \geqslant rg_\ell Gal(M/K^c) - rg_\ell Gal(L/K).$$

Le lemme 3.4.2 appliqué à la suite exacte précédente montre que

$$rg_\ell Gal(M/K^c) + rg_\ell \tilde{E}_K/(\tilde{E}_K \cap N_{L/K}^{loc}) \geqslant rg_\ell \bigoplus_{\mathfrak{p} \in P_K^\infty} D_\mathfrak{p}(M/K) \bigoplus_{\mathfrak{p} \in P_K^0} \tilde{I}_\mathfrak{p}(M/K).$$

Le ℓ-rang du groupe $\bigoplus_{\mathfrak{p} \in P_K^\infty} D_\mathfrak{p}(M/K) \bigoplus_{\mathfrak{p} \in P_K^0} \tilde{I}_\mathfrak{p}(M/K)$ n'est autre que $\rho_{L/K}$, alors que celui du groupe $\tilde{E}_K/(\tilde{E}_K \cap N_{L/K}^{loc})$ est majoré par celui de $\tilde{E}_K$. Enfin, l'extension L/K étant cyclique, on a $rg_\ell Gal(L/K) = 1$. Finalement on obtient la minoration

$$rg_\ell \widetilde{Cl}_L \geqslant \rho_{L/K} - rg_\ell \tilde{E}_K - 1.$$

On peut alors conclure avec le critère du théorème 11 de [8] rappelé plus haut. □

3.4.2 Un autre critère d'infinitude "relatif"

Le théorème principal de cette partie donne, dans le cas où G est cyclique, une minoration du ℓ-rang de $\widetilde{Cl}_L$ en termes d'invariants liés à K et de ramification logarithmique dans L/K. Compte tenu du critère de [8] rappelé ci-dessus, on en déduira une nouvelle condition suffisante pour que $T(L) = +\infty$. C'est l'objet du corollaire 3.4.5. Les notations sont les mêmes que précédemment.

Théorème 3.4.3 *Soit L/K une ℓ-extension galoisienne de corps de nombres. On note G son groupe de Galois et t le nombre de places logarithmiquement ramifiées dans L/K. Alors :*

$$rg_\ell\ \widetilde{Cl}_L \geqslant t - 1 - rg_\ell\ H^1(G, \widetilde{E}_L).$$

DÉMONSTRATION. On applique le lemme 3.4.2 à la suite exacte

$$0 \longrightarrow \widetilde{Cl}_L \longrightarrow Cl_L \xrightarrow{Deg} \mathbb{Z}_\ell \longrightarrow 0,$$

où Cl_L est le groupe des diviseurs logarithmiques de L et $\widetilde{Cl}_L$ celui des diviseurs logarithmiques de degré nul, c'est-à-dire le noyau de l'application deg à valeur dans $\mathbb{Z}_\ell$. Il vient

$$rg_\ell\, Cl_L \leqslant rg_\ell\, \widetilde{Cl}_L + 1.$$

Tenant compte de l'inclusion $Cl_L^G \subset Cl_L$, nous obtenons

$$rg_\ell\, \widetilde{Cl}_L \geqslant rg_\ell\, Cl_L^G - 1. \tag{3.1}$$

On considère à présent la suite exacte déjà rencontrée :

$$0 \longrightarrow Pl_L \longrightarrow Dl_L \longrightarrow Cl_L \longrightarrow 0,$$

où $Pl_L = \widetilde{Pl}_L$ comme on l'a vu dans la partie 1.
L'action de G nous fournit alors la suite exacte de cohomologie suivante :

$$0 \longrightarrow Pl_L^G \longrightarrow Dl_L^G \longrightarrow Cl_L^G \longrightarrow H^1(G, Pl_L) \longrightarrow H^1(G, Dl_L),$$

le dernier terme étant nul d'après le théorème 90 de Hilbert. Cette suite, jointe à la suite exacte de K, conduit au diagramme commutatif suivant :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Pl_K & \longrightarrow & Dl_K & \longrightarrow & Cl_K & \longrightarrow & 0 \\
 & & i_1 \downarrow & & i_2 \downarrow & & i_3 \downarrow & & \\
0 & \longrightarrow & Pl_L^G & \xrightarrow{\psi} & Dl_L^G & \xrightarrow{\varphi} & Cl_L^G & \longrightarrow & H^1(G, Pl_L) \longrightarrow 0
\end{array}$$

C'est l'analogue de celui utilisé dans la partie 1, mais on ne se limite plus aux diviseurs logarithmiques de degré nul. Le lemme du serpent nous fournit la suite exacte suivante :

$$\begin{aligned}
0 \longrightarrow \ker i_1 \longrightarrow \ker i_2 \longrightarrow keri_3 \longrightarrow Pl_L^G/i_1(Pl_K) \longrightarrow Dl_L^G/i_2(Dl_K) \\
\longrightarrow Cl_L^G/i_3(Cl_K) \longrightarrow H^1(G, Pl_L) \longrightarrow 0
\end{aligned}$$

L'extension des diviseurs logarithmiques étant injective, la suite précédente devient :

$$0 \longrightarrow \mathrm{cap}_{L/K} \longrightarrow Pl_L^G/i_1(Pl_K) \xrightarrow{\bar{\psi}} Dl_L^G/i_2(Dl_K) \xrightarrow{\bar{\varphi}} Cl_L^G/i_3(Cl_K) \longrightarrow H^1(G, Pl_L) \longrightarrow 0$$

où les morphismes $\bar{\varphi}$ et $\bar{\psi}$ sont induits par φ et ψ respectivement. Compte tenu du diagramme commutatif

$$\begin{array}{ccc} Dl_L^G & \xrightarrow[\varphi]{} & Cl_L^G \\ \downarrow & & \downarrow \\ Dl_L^G/i_2(Dl_K) & \xrightarrow[\bar{\varphi}]{} & Cl_L^G/i_3(Cl_K) \end{array}$$

les générateurs de $\mathrm{Im}\bar{\varphi}$ sont les images des générateurs de $\mathrm{Im}\varphi$ par la surjection canonique $Cl_L^G \twoheadrightarrow Cl_L^G/i_3(Cl_L^K)$. Il s'ensuit la minoration

$$rg_\ell\ \mathrm{Im}\bar{\varphi} \leqslant rg_\ell\ \mathrm{Im}\varphi.$$

Et puisque $\mathrm{Im}\varphi \subset Cl_L^G$, on a finalement :

$$rg_\ell\ \mathrm{Im}\bar{\varphi} \leqslant rg_\ell\ Cl_L^G. \tag{3.2}$$

On achève la preuve du théorème en minorant $rg_\ell\ \mathrm{Im}\bar{\varphi}$. Dans ce but, on utilise à nouveau le lemme 3.4.2 avec la suite exacte suivante :

$$0 \longrightarrow \ker\bar{\varphi} \longrightarrow Dl_L^G/i_2(Dl_K) \xrightarrow{\bar{\varphi}} \mathrm{Im}\bar{\varphi} \longrightarrow 0.$$

Il vient :

$$rg_\ell\ \mathrm{Im}\bar{\varphi} \geqslant rg_\ell\ Dl_L^G/i_2(Dl_K) - rg_\ell\ \ker\bar{\varphi}.$$

On a vu au chapitre 2 que l'absence de ramification logarithmique dans L/K entraîne l'égalité des groupes Dl_L^G et $i_2(Dl_K)$. Plus généralement, en présence éventuelle de ramification logarithmique, le quotient $Dl_L^G/i_2(Dl_K)$ possède une interprétation simple qui fait l'objet du lemme qui suit.

Lemme 3.4.4 *Soit L/K une ℓ-extension galoisienne de corps de nombres, de groupe de Galois G. Le nombre t de places logarithmiquement ramifiées dans L/K est donné par :*

$$t = rg_\ell Dl_L^G/i_2(Dl_K).$$

Démonstration du lemme. Si $a = \sum_{\mathfrak{P}\in Pl_L^0} a_{\mathfrak{P}}\mathfrak{P}$ est un diviseur logarithmique ambige de L, on a pour tout élément σ de G :

$$\left(\sum_{\mathfrak{P}\in P_L^0} a_{\mathfrak{P}}\mathfrak{P}\right)^{\sigma} = \sum_{\mathfrak{P}\in P_L^0} a_{\mathfrak{P}}\mathfrak{P}^{\sigma} = \sum_{\mathfrak{P}\in P_L^0} a_{\mathfrak{P}^{\sigma^{-1}}}\mathfrak{P}.$$

Par conséquent, $a_{\mathfrak{P}^{\sigma^{-1}}} = a_{\mathfrak{P}}$ pour tout σ de G. L'action de G sur l'ensemble des places de L au dessus d'une place $\mathfrak{p}$ de K étant simplement transitive, il vient

$$a = \sum_{\mathfrak{p}\in P_K^0} a_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}.$$

Inversement, il est clair qu'un diviseur logarithmique de L de la forme précédente est G-invariant. On en déduit la description du groupe des diviseurs logarithmiques ambiges de L :

$$Dl_L^G = \bigoplus_{\mathfrak{p}\in Pl_K^0} \left(\sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}\right) \mathbb{Z}_\ell.$$

On dispose également de la décomposition suivante du $\mathbb{Z}_\ell$-module G-invariant Dl_K :

$$Dl_K = \bigoplus_{\mathfrak{p}\in P_K^0} \mathbb{Z}_\ell\mathfrak{p} = \bigoplus_{\mathfrak{p}\in P_K^0} \tilde{e}_{\mathfrak{p}}(L/K) \left(\sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}\right) \mathbb{Z}_\ell.$$

On en déduit la structure du quotient :

$$Dl_L^G/Dl_K = \bigoplus_{\mathfrak{p}\in P_K^0} \mathbb{Z}_\ell/\tilde{e}_{\mathfrak{p}}(L/K)\mathbb{Z}_\ell.$$

Le ℓ-rang du second membre est le nombre de quotients $\mathbb{Z}_\ell/\tilde{e}_{\mathfrak{p}}(L/K)\mathbb{Z}_\ell$ non triviaux. C'est bien le nombre de places logarithmiquement ramifiées dans l'extension L/K. □

Revenons à la preuve du théorème 3.4.3.
Notant t le nombre de places logarithmiquement ramifiées dans L/K, et revenant à la suite exacte (2), on voit que $\ker\bar{\varphi}$ n'est autre que $\mathrm{Im}\bar{\psi}$, lequel est inclus dans $Pl_L^G/i_2(Pl_K)$. Enfin l'isomorphisme

$$H^1(G, \tilde{E}_L) \simeq Pl_L^G/Pl_K$$

vu dans le paragraphe 2.3 donne finalement :

$$rg_\ell \ \mathrm{Im}\bar{\varphi} \geqslant t - rg_\ell \ H^1(G, \tilde{E}_L). \tag{3.3}$$

Le théorème 3.4.3 est alors une conséquence immédiate des inégalités 3.1, 3.2, et 3.3. □

Corollaire 3.4.5 *Si la ℓ-extension L/K est cyclique de degré ℓ^n et si le nombre t de places de K logarithmiquement ramifiées dans L/K vérifie :*

$$t \geqslant n(r_K + c_K + \delta_K) + 2 + 2\sqrt{r_L + c_L + \delta_L + 1},$$

alors $T(L) = +\infty$.

Démonstration. Il s'agit de majorer le ℓ-rang ρ du groupe $H^1(G, \widetilde{E}_L)$. Les facteurs directs de ce groupe sont d'ordre au moins ℓ de sorte que

$$\ell^\rho \leqslant |H^1(G, \widetilde{E}_L)|.$$

D'autre part, on sait que, lorsque G est cyclique, les ordres des deux premiers groupes de cohomologie de $\tilde{E}_L$ sont liés par la relation

$$\frac{|H^2(G, \widetilde{E}_L)|}{|H^1(G, \widetilde{E}_L)|} = q(\widetilde{E}_L),$$

où le quotient de Herbrand $q(\widetilde{E}_L)$ est tel que

$$q(\widetilde{E}_L) = \prod_{\mathfrak{p} \in P_K^\infty} d_\mathfrak{p}(L/K).$$

(voir [6], corollaire 3.7). Il découle de ceci que

$$\ell^\rho \leqslant |H^2(G, \widetilde{E}_L)|.$$

Par ailleurs l'égalité des groupes $H^2(G, \widetilde{E}_L)$ et $\widetilde{E}_K/N_{L/K}(\widetilde{E}_L)$ ainsi que l'inclusion de $(\widetilde{E}_K)^{\ell^n}$ dans $N_{L/K}(\widetilde{E}_L)$ nous donnent l'inégalité

$$|H^2(G, \widetilde{E}_L)| \leqslant [\widetilde{E}_K : (\widetilde{E}_K)^{\ell^n}].$$

Compte tenu de la structure du $\mathbb{Z}_\ell$-module $\widetilde{E}_K$, il vient

$$\ell^\rho \leqslant (\ell^n)^{r_K + c_K + \delta_K},$$

puis

$$\rho \leqslant n(r_K + c_K + \delta_K).$$

Le théorème 3.4.3 entraîne alors :

$$rg_\ell\, \widetilde{Cl}_L \geqslant t - 1 - n(r_K + c_K + \delta_K).$$

Le corollaire découle finalement de la condition suffisante de [8]. □

On dispose ainsi d'un critère simple pour que la ℓ-tour localement cyclotomique d'un corps L soit infinie. Ce critère est de même nature que celui du théorème 3.4.1, mais il est valable pour toute ℓ-extension cyclique L/K.

3.5 Étude de quelques exemples

Dans les trois premiers exemples, on prend $K = \mathbb{Q}$ et $n = 1$. La borne du corollaire 3.4.5 est alors $4 + 2\sqrt{r_L + c_L + 2}$.

3.5.1 Une extension quadratique réelle de $\mathbb{Q}$

Soit $L = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel, où d est un entier strictement supérieur à 1 et sans facteur carré. On choisit donc $\ell = 2$. La borne du corollaire 3.4.5 est ici donnée par :

$$4 + 2\sqrt{2 + 2} = 8.$$

Les nombres premiers impairs p_i, $1 \leqslant i \leqslant n$ qui divisent d sont ramifiés dans $L/\mathbb{Q}$. Puisque les p_i sont étrangers à ℓ, ils sont aussi logarithmiquement ramifiés. Dés que $n \geqslant 9$, la 2-tour localement cyclotomique sur L est infinie.

3.5.2 Une extension quadratique imaginaire de $\mathbb{Q}$

Soit $L = \mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire, où d est un entier supérieur à 1 et sans facteur carré. On choisit encore $\ell = 2$. La borne du corollaire 3.4.5 est ici $4 + 2\sqrt{3}$. Par conséquent, 8 diviseurs premiers impairs de d suffisent pour avoir $T(L) = +\infty$.

3.5.3 Un corps cubique

Soit t un entier. On note L le corps cubique cyclique $\mathbb{Q}(\theta)$, où θ est une racine du polynôme $X^3 - tX^2 - (t+3)X - 1$ (polynôme de Shanks). On se place ici dans le cas où $\ell = 3$. Soit p un nombre premier différent de 3. Il est connu (voir [19]) que p est ramifié dans $L/\mathbb{Q}$ si et seulement si $p | t^2 + 3t + 9$ et $p^3 \nmid t^2 + 3t + 9$. On pose $N = t^2 + 3t + 9$. Les plus petits nombre premiers qui peuvent diviser N sont, en dehors de 3, les entiers 7, 13, 19, 31, 37, 43, 61, 67, 73. Plus précisément, on

trouve :

$$\begin{aligned}
&7 \mid t^2+3t+9 \Leftrightarrow t \equiv 5,6 \quad \bmod 7,\\
&13 \mid t^2+3t+9 \Leftrightarrow t \equiv 1,9 \quad \bmod 13,\\
&19 \mid t^2+3t+9 \Leftrightarrow t \equiv 2,14 \quad \bmod 19,\\
&31 \mid t^2+3t+9 \Leftrightarrow t \equiv 13,15 \quad \bmod 31,\\
&37 \mid t^2+3t+9 \Leftrightarrow t \equiv 4,30 \quad \bmod 37,\\
&43 \mid t^2+3t+9 \Leftrightarrow t \equiv 18,22 \quad \bmod 43,\\
&61 \mid t^2+3t+9 \Leftrightarrow t \equiv 19,39 \quad \bmod 61,\\
&67 \mid t^2+3t+9 \Leftrightarrow t \equiv 20,44 \quad \bmod 67,\\
&73 \mid t^2+3t+9 \Leftrightarrow t \equiv 24,46 \quad \bmod 73.
\end{aligned}$$

On voit ainsi qu'à l'aide du théorème chinois, et en choisissant t convenablement, on peut rendre arbitrairement grand le nombre de diviseurs premiers de t^2+3t+9. Afin qu'ils soient non ramifiés dans $L/\mathbb{Q}$, il faut encore obtenir que les cubes de ces nombres premiers ne divisent pas t^2+3t+9. A l'aide du logiciel PARI, on obtient la valeur de t suivante : 25 285 696 305 728. L'entier N correspondant est tel que :

$$\begin{aligned}
&N = 639\ 366\ 437\ 665\ 582\ 483\ 934\ 527\ 177\\
&N = 7 \times 13 \times 19 \times 31 \times 37 \times 43 \times 61 \times 67 \times 73 \times 25\ 130\ 172\ 544\ 303.
\end{aligned}$$

L'entier N est donc le produit de 10 nombres premiers distincts. Ils sont ramifiés dans $L/\mathbb{Q}$ et puisqu'ils sont étrangers à ℓ, ils sont également logarithmiquement ramifiés. La borne du corollaire 3.4.5 est ici $4+2\sqrt{5}$ de sorte que 9 nombres premiers logarithmiquement ramifiés suffisent pour avoir $T(L) = +\infty$. C'est le cas pour l'entier t considéré.

3.5.4 Une extension de Kummer de $\mathbb{Q}$

Cet exemple généralise l'exemple 1. Soit $K = \mathbb{Q}(\mu_\ell)$, $p_1, p_2, ..., p_s$ des nombres premiers deux à deux distincts et distincts de ℓ, a leur produit, et L l'extension de Kummer $K(\sqrt[\ell]{a})$. On a ici $r_K = r_L = 0$, $c_K = \frac{\ell-1}{2}$, $c_L = \frac{\ell(\ell-1)}{2}$, de sorte que la borne du corollaire 3.4.5 ne dépend que de ℓ. D'autre part les p_i sont logarithmiquement ramifiés, et donc $T(L) = +\infty$ dés que $s \geqslant \frac{\ell-1}{2} + 3 + 2\sqrt{\frac{\ell(\ell-1)}{2}+2}$.

Chapitre 4

Tour non logarithmiquement ramifiée, S-décomposée

Dans ce qui suit, on désigne par K un corps de nombres et ℓ un nombre premier. Le théorème 3.1.5 du chapitre précédent donne une caractérisation de la ℓ-extension K^{lc} de K : c'est l'extension abélienne maximale de K qui est non logarithmiquement ramifiée. Le fait de considérer la ramification logarithmique au lieu de la ramification au sens classique, et bien que la différence entre les deux notions n'ait lieu que pour les places au dessus de ℓ, a pour conséquence de donner une extension de degré infini de K. Elle contient en effet la $\mathbb{Z}_\ell$-extension cyclotomique K^c de K. On fixe à présent un ensemble non vide S de places non archimédiennes de K et on note K_S^{lc} l'extension abélienne maximale de K qui est non logarithmiquement ramifiée et S-décomposée. C'est donc une sous-extension de K^{lc}. Nous allons établir que, sous la conjecture de Gross généralisée (relativement au nombre premier ℓ), il s'agit d'une extension *finie* de K, puis nous définirons et étudierons une tour de corps de nombres au dessus du corps K.

4.1 Étude de l'extension K_S^{lc}/K

4.1.1 Finitude de l'extension K_S^{lc}/K

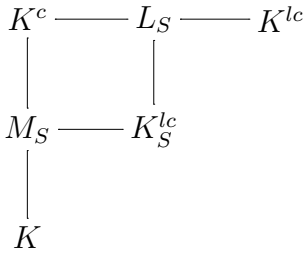
Introduisons les ℓ-extensions suivantes du corps K :

$$M_S = K_S^{lc} \cap K^c,$$
$$L_S = K_S^{lc} K^c.$$

L'extension L_S/K est abélienne et non logarithmiquement ramifiée en tant que composée de deux telles extensions, de sorte qu'on a l'inclusion

$$L_S \subset K^{lc}.$$

Le schéma de corps en jeu est donc le suivant :



On va en déduire le résultat qui suit.

Proposition 4.1.1 *Sous la conjecture de Gross généralisée, l'extension K_S^{lc}/K est de degré fini.*

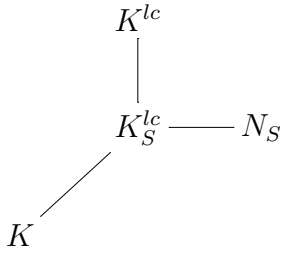
Démonstration. Il suffit de prouver que les extensions K_S^{lc}/M_S et M_S/K sont de degré fini.

- Le corps L_S est une sous-extension de K^{lc}/K^c qui est finie sous la conjecture de Gross, donc $[L_S : K^c] < +\infty$. Une conséquence immédiate de la définition des corps L_S et M_S (les extensions K_S^{lc} et K^c étant linéairement disjointes sur M_S) est alors l'égalité des degrés
$$[L_S : K^c] = [K_S^{lc} : M_S]$$
et en particulier la finitude de l'extension K_S^{lc}/M_S.
- Par ailleurs $M_S \subset K^c$ et le seul sous corps de K^c qui est de degré infini sur K est K^c lui-même. On ne peut avoir $M_S = K^c$ puisque au moins une place de K est totalement décomposée dans M_S (S est non vide) alors que, selon la théorie du corps de classe, aucune place n'est totalement décomposée dans K^c/K. Par suite, l'extension M_S/K est de degré fini. Ceci achève la preuve de la proposition.

□

4.1.2 Le groupe de Galois de l'extension K_S^{lc}/K

On considère la ℓ-extension maximale N_S de K, qui est abélienne et S-décomposée. La définition de K_S^{lc} signifie que $K_S^{lc} = K^{lc} \cap N_S$.



On va en déduire le résultat suivant.

Proposition 4.1.2 *Le groupe de Galois de l'extension K_S^{lc}/K s'identifie au quotient $Cl_K/Cl_K(S)$ du ℓ-groupe des classes logarithmiques de K par son sous-groupe engendré par les diviseurs logarithmiques construits sur les places de S.*

Démonstration. Notons $\mathfrak{X}_L$ le groupe des normes associé à une ℓ-extension abélienne L/K par la théorie ℓ-adique du corps de classe ([4], [7]). Nous avons d'une part

$$\mathfrak{X}_{N_S} = R_K \prod_{\mathfrak{p}\in S} \mathcal{R}_{\mathfrak{p}},$$

et d'autre part

$$\mathfrak{X}_{K^{lc}} = \mathcal{J}^* R_K.$$

Et puisque $K_S^{lc} = K^{lc} \cap N_S$, il vient

$$\mathfrak{X}_{K_S^{lc}} = \mathfrak{X}_{K^{lc}} \mathfrak{X}_{N_S},$$

c'est-à-dire

$$\mathfrak{X}_{K_S^{lc}} = \mathcal{J}^* \prod_{\mathfrak{p}\in S} \mathcal{R}_{\mathfrak{p}} R_K.$$

Le groupe de Galois de l'extension K_S^{lc}/K est donc donné par

$$Gal(K_S^{lc}/K) = \mathcal{J}/\mathcal{J}^* \prod_{\mathfrak{p}\in S} \mathcal{R}_{\mathfrak{p}} R_K.$$

Le quotient $\mathcal{J}/\mathcal{J}^* R_K$ n'est autre que le groupe Cl_K des diviseurs logarithmiques de K et si on note $Cl_K(S)$ le groupe des diviseurs logarithmiques construits sur les places au dessus de ℓ, on a

$$Cl_K(S) = \prod_{\mathfrak{p}\in S} \mathcal{R}_{\mathfrak{p}}/(\mathcal{J}^* R_K) \cap \prod_{\mathfrak{p}\in S} \mathcal{R}_{\mathfrak{p}},$$

de sorte que le quotient $Cl_K/Cl_K(S)$ s'identifie au groupe de Galois de l'extension K_S^{lc} comme annoncé. □

On note Cl_K^S le groupe quotient $Cl_K/Cl_K(S)$. On a donc

$$Gal(K_S^{lc}/K) = Cl_K^S = (Dl_K/Pl_K)\diagup(Dl_K(S)/Pl_K(S)) = Dl_K/Dl_K(S)Pl_K.$$

Il est intéressant de remarquer qu'on peut prouver directement la finitude du groupe Cl_K^S. C'est l'objet des deux lemmes qui suivent. Ceci nous fournit une autre preuve de la proposition 4.1.1. Introduisons un diviseur logarithmique *primitif* $\mathfrak{p}_0$ de K, c'est-à-dire tel que $\deg \mathfrak{p}_0$ engendre le sous-groupe $\deg(Dl_K)$ de $\mathbb{Z}_\ell$:

$$\deg(Dl_K) = \deg \mathfrak{p}_0 \mathbb{Z}_\ell.$$

On a d'une part le fait suivant.

Lemme 4.1.3 *Le ℓ-rang du groupe Cl_K vérifie*

$$rg_\ell Cl_K \leqslant 1 + rg_\ell \widetilde{Cl}_K.$$

Démonstration. Si $a_K \in Dl_K$, il existe un entier ℓ-adique α tel que $\deg a_K = \alpha \deg \mathfrak{p}_0$, de sorte que le diviseur $a_K - \alpha\mathfrak{p}_0$ est de degré nul. La classe $[a_K - \alpha\mathfrak{p}_0]$ de ce dernier modulo Pl_K est donc un élément de $\widetilde{Cl}_K$ qui est de type fini (et est même fini sous la conjecture de Gross). Par conséquent, notant $([a_1], \ldots, [a_s])$ un système minimal de générateurs de $\widetilde{Cl}_K$, on a

$$[a_K - \alpha\mathfrak{p}_0] = \sum_{i=1}^{s} \lambda_i [a_i],$$

ce qui montre que $[a_K]$ est combinaison $\mathbb{Z}_\ell$-linéaire d'au plus $s+1$ éléments fixés de Cl_K. □

Un second résultat, plus spécifique à Cl_K^S, permet de conclure.

Lemme 4.1.4 *Le diviseur logarithmique primitif $\mathfrak{p}_0$ est d'ordre fini dans Cl_K^S.*

Démonstration. Soit a_S un diviseur logarithmique de K construit sur les places de S :

$$a_S \in Dl_K(S).$$

On peut supposer que $\deg a_S \neq 0$. Il existe donc un entier ℓ-adique non nul γ tel que $\deg a_S = \gamma \deg \mathfrak{p}_0$, et donc

$$a_S - \gamma\mathfrak{p}_0 \in \widetilde{Dl}_K.$$

La classe $[a_S - \gamma\mathfrak{p}_0]$ de ce dernier modulo Pl_K (rappelons que $Pl_K = \widetilde{Pl}_K$) est donc un élément $[a_K]$ de $\widetilde{Cl}_K$. Il en résulte l'égalité des classes modulo $Dl_K(S)Pl_K$:

$$\{-\gamma\mathfrak{p}_0\} = \{a_K\}$$

où le second membre est d'ordre fini dans Cl_K^S puisque $[a_K]$ est d'ordre fini dans $\widetilde{Cl}_K$. Il en va de même pour $\mathfrak{p}_0$ puisque γ est non nul. □

On a prouvé que les générateurs de Cl_K^S sont en nombre fini et sont d'ordre fini. D'où le résultat.

4.2 La tour d'extensions S-décomposées et non logarithmiquement ramifiées de K

Le procédé de construction de l'extension K_S^{lc} d'un corps de nombres K, pour un nombre premier ℓ et un ensemble fini S de places non archimédiennes de K, est susceptible d'être itéré. On construit ainsi une suite $(K_S^n)_{n\in\mathbb{N}}$ de ℓ-extensions de K de la façon suivante :

$$\begin{aligned} &K_S^0 = K, \\ &\forall n \in \mathbb{N},\ K_S^{n+1} = (K_S^n)_{S_n}^{lc} \end{aligned}$$

où S_n désigne l'ensemble des places de K_S^n situées au-dessus de celles de S.
Il est immédiat que pour tout entier naturel n, l'extension K_S^n/K est non logarithmiquement ramifiée et S-décomposée. On a en outre le fait suivant :

Proposition 4.2.1 *Pour tout entier naturel n, l'extension K_S^n/K est galoisienne.*

Démonstration. On raisonne par récurrence sur l'entier n. Le résultat est clair pour $n = 1$ puisque K_S^1/K est abélienne. Considérons un entier $n \geqslant 1$ tel que l'extension K_S^n/K soit galoisienne. Soit alors σ un K-isomorphisme de K_S^{n+1} sur un sous-corps de $\mathbb{C}$. La restriction de σ à K_S^n est un K-isomorphisme de K_S^n sur un sous-corps de $\mathbb{C}$, donc, par hypothèse de récurrence, un K-automorphisme de K_S^n.

$$\begin{array}{ccc} K_S^{n+1} & \xrightarrow{\sigma} & \sigma(K_S^{n+1}) \\ | & & | \\ K_S^n & = & \sigma(K_S^n) \end{array}$$

Le corps $\sigma(K_S^{n+1})$ est une extension abélienne, non logarithmiquent ramifiée et S_n-décomposée de $\sigma(K_S^n)$, c'est-à-dire de K_S^n. Mais K_S^{n+1} est l'extension abélienne maximale de K_S^n qui est non logarithmiquent ramifiée et S_n-décomposée. Par conséquent, $\sigma(K_S^{n+1}) \subset K_S^{n+1}$, et donc, pour des raisons évidentes de degré, $\sigma(K_S^{n+1}) = K_S^{n+1}$. Ainsi, σ est un K-automorphisme de K_S^{n+1}, et donc l'extension K_S^{n+1}/K est galoisienne, ce qui achève la récurrence. □

Remarque 4.2.2
L'extension K_S^n/K n'est pas abélienne pour $n > 1$ en dehors du cas où la suite $(K_S^n)_{n\in\mathbb{N}}$ est constante à partir du rang 1.

4.3 La pro-ℓ-extension non logarithmiquement ramifiée, S-décomposée, maximale de K

On considère le corps défini par

$$K_S^\infty = \bigcup_{n\in\mathbb{N}} K_S^n.$$

Selon que K_S^∞ est une extension de degré fini de K ou non, on dira que la tour d'extensions S-décomposées et non logarithmiquement ramifiées de K est finie ou infinie. On va établir que K_S^∞ est la pro-ℓ-extension (galoisienne) non logarithmiquement ramifiée, S-décomposée, maximale de K. Le caractère galoisien de cette extension est acquis en raison de sa maximalité pour des propriétés stables par conjugaison (c'est le même argument que dans la preuve de 4.2.1).

Proposition 4.3.1 *Si L est une ℓ-extension galoisienne non logarithmiquement ramifiée, S-décomposée et de degré fini de K, alors $L \subset K_S^\infty$.*

Démonstration. Le groupe de Galois G de l'extension L/K est résoluble (en tant que ℓ-groupe) : il existe une suite de groupes

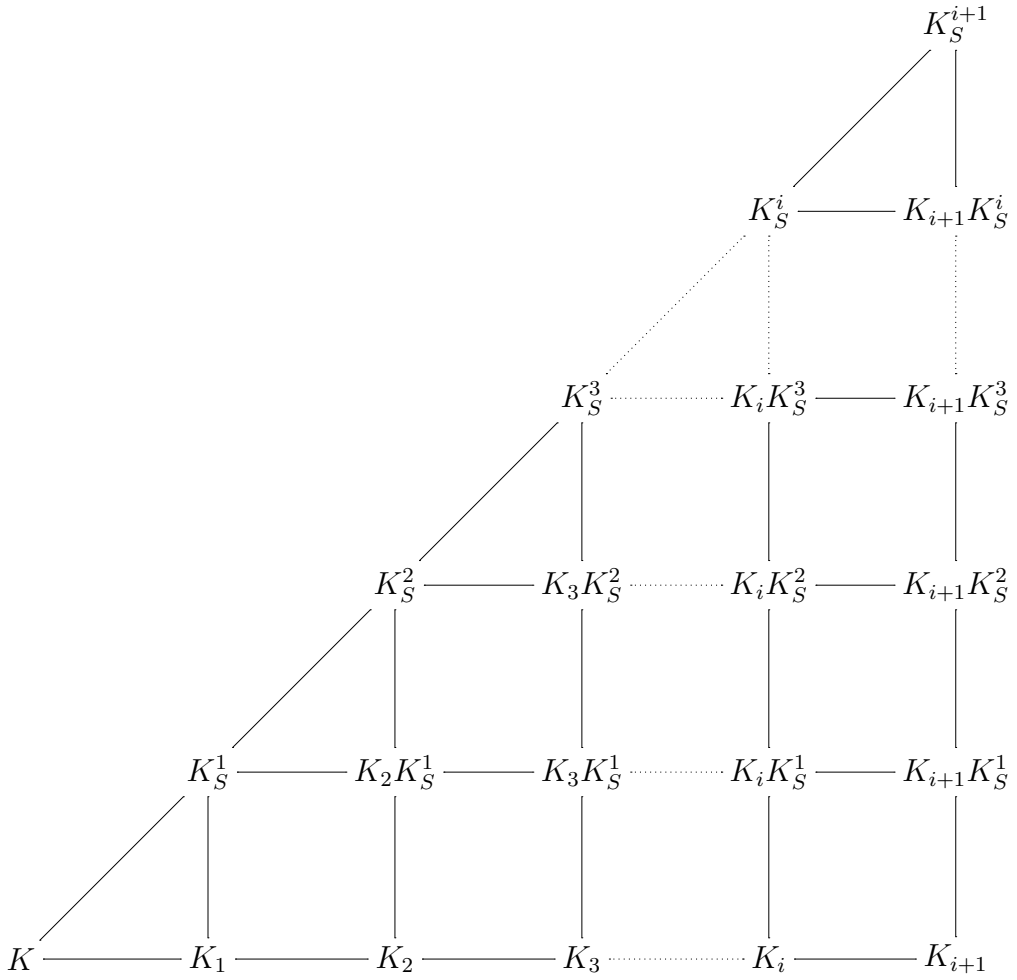
$$G_n = 1 \subset G_{n-1} \subset \ldots \subset G_0 = Gal(L/K),$$

telle que les quotients G_i/G_{i+1} soient abéliens. En conséquence, il existe une suite d'extensions intermédiaires entre K et L :

$$K - K_1 - K_2 - \ldots - K_n = L,$$

telle que pour chaque indice i, l'extension K_{i+1}/K_i soit abélienne.
On va montrer par récurrence sur l'entier i que pour $1 \leqslant i \leqslant n$, l'extension K_i est incluse dans l'étage K_S^i de la tour non logarithmiquement ramifiée et S-décomposée de K. Ce qui démontrera l'inclusion de L dans K_S^∞. La récurrence portera sur le résultat plus fort suivant :
«pour tout entier i compris entre 1 et n, $K_i \subset K_S^i$ et les étages de la tour K_i —— $K_iK_S^1$ —— $K_iK_S^2$ ····· $K_iK_S^i = K_S^i$ sont abéliens.»
Le résultat est clair pour $i = 1$ et on le suppose vrai à présent pour un entier i compris entre 1 et $n-1$. L'extension K_{i+1}/K_i est abélienne, ainsi que l'extension $K_iK_S^1/K_i$ (hypothèse de récurrence) ; donc leur compositum également : $K_{i+1}K_S^1/K_i$ est abélienne. Par suite l'extension $K_{i+1}K_S^1/K_{i+1}$ est abélienne comme recherché. C'est donc aussi le cas de l'extension $K_{i+1}K_S^1/K_iK_S^1$, ce qui permet d'itérer le raisonnement qui précède et d'obtenir de proche en proche le caractère

abélien des étages de la tour $K_{i+1} \text{——} K_{i+1}K_S^1 \text{——} K_{i+1}K_S^2 \cdots\cdots K_{i+1}K_S^i$ ainsi que de l'extension $K_{i+1}K_S^i/K_S^i$. Cette dernière est donc une sous-extension de l'extension K_S^{i+1}/K_S^i, ce qui achève la récurrence.



□

La caractérisation du corps K_S^∞ comme extension non logarithmiquement ramifiée, S-décomposée maximale de K, qui résulte de la proposition précédente, permet d'énoncer le critère suivant d'infinitude de la tour $(K_S^n)_{n\in\mathbb{N}}$.

Corollaire 4.3.2 *Pour que la tour $(K_S^n)_{n\in\mathbb{N}}$ soit infinie, il faut et il suffit que K possède une ℓ-extension non logarithmiquement ramifiée, S-décomposée, et de degré infini.*

Bibliographie

[1] A. Azizi, *Unités de certains corps de nombres imaginaires et abéliens sur* $\mathbb{Q}$, Ann. Sci. Math. Québec **23** 1999, 87-93.

[2] F. Diaz Y Diaz, J.F. Jaulent, S. Pauli, M. Pohst, F. Soriano-Gafiuk, *A New Algorithm for the Computation of Logarithmic ℓ-Class Groups of Number Fields*, Experimental Math. **14** 2005, 67-76.

[3] E.S. Golod, Shafarevitch, I.R., *Sur les tours de corps de classes* (en russe), Izv. Akad. Nauk S.S.S.R. **28** 1964, 261-272 (trad. anglaise : I.R. Shafarevitch, C.P. 317-328).

[4] J.F. Jaulent, *L'arithmétique des ℓ-extensions (thèse d'état)*, Publ. Math. Fac. Sci. Besançon, Théor. Nombres 1984/1985, 1985/1986 (1986), 1-348.

[5] J.F. Jaulent, *Sur le noyau sauvage des corps de nombres*, Acta Arithmetica **67** (1994), 335-348.

[6] J.F. Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1994), 303-327.

[7] J.F. Jaulent, *Théorie ℓ-adique globale du corps de classe*, J. Théor. Nombres Bordeaux **10** (2), 355-397.

[8] J.F. Jaulent, F. Soriano-Gafiuk, *Sur les tours localement cyclotomiques*, Archiv. Math, 132-140 (1999).

[9] J.F. Jaulent, C. Maire, *A propos de la tour localement cyclotomique d'un corps de nombres* Abh. Math. Sem. Hamburg **70** (2000), 239-250.

[10] S. Lang, *Algebra*, Addison-Wesley, Reading, MA 1993.

[11] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, MA 1970.

[12] S. Lang, *Cyclotomic fields*, Springer-Verlag, New-York, 1978.

[13] C. Maire, *Extensions T-ramifiées modérées, S-décomposées (thèse)*, Besançon, 1995.

[14] P. Roquette, *On class field towers*, in J.W.S. Cassels & A. Fröhlich, Algebraic number theory, Academic Press, London (1967), 231-249.

[15] F. Soriano, *Classes logarithmiques ambiges des corps quadratiques*, Acta Arithmetica LXXVIII. 3,201-219 (1997).

[16] F. Soriano, I. Dubois *Un nouveau régulateur de type Gross*, Abh. Math. Sem. Hamburg **74** (2004), 89-99.

[17] J.P. Serre, *Corps locaux*, Hermann, Paris, 1959.

[18] J.P. Serre, *Cours d'arithmétique*, PUF, Paris, 1970.

[19] D. Shanks, *The simplest cubic fields*, Math. Comp. **28**, 1137-1152 (1974)

[20] L. C. Washington, *Cyclotomic fields*, Springer-Verlag.