N° d'ordre : 4279

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Claire BOURBON**

pour obtenir le grade de

DOCTEUR

Spécialité : **Mathématiques Pures**

****

PROPAGATION DE LA 2-BIRATIONALITÉ

****

Soutenue le 30 juin 2011 à l'Institut de Mathématiques de Bordeaux, après avis de :

A. C. MOVAHHEDI	Professeur, Université de Limoges	**Rapporteur**
C. MAIRE	Professeur, Université de Franche-Comté	**Rapporteur**

et devant la commission d'examen composée de :

K. BELABAS	Professeur, Université Bordeaux I	
J.-F. JAULENT	Professeur, Université Bordeaux I	**Directeur**
C. MAIRE	Professeur, Université de Franche-Comté	**Rapporteur**
J. MARTINET	Professeur, Université Bordeaux I	**Président**
A. C. MOVAHHEDI	Professeur, Université de Limoges	**Rapporteur**
F. SORIANO-GAFIUK	Professeur, Université Paul-Verlaine-Metz	

- 2011 -

Remerciements

Je tiens à remercier en tout premier lieu Jean-François Jaulent qui a dirigé cette thèse. Tout au long de ces trois années, il s'est montré disponible pour m'aider, pour répondre à mes questions, il a su me guider dans mes recherches, m'épauler à certains moments difficiles. Pour tout cela, ainsi que pour la confiance qu'il m'a témoignée, je lui adresse ici toute ma gratitude et mon profond respect.

J'adresse mes plus sincères remerciements à Abbas Chazad Movahhedi et Christian Maire, d'avoir accepté d'être mes rapporteurs, ainsi que pour leur relecture attentive qui m'a permis d'améliorer mon travail, ainsi que pour l'intérêt qu'ils y ont porté. Je remercie aussi Florence Soriano-Gafiuk, d'avoir accepté de participer à ce jury ainsi que pour sa relecture. Enfin merci à Karim Belabas d'être présent dans mon jury. Un grand merci à Jacques Martinet, pour avoir accepté d'être membre de mon jury et pour le temps qu'il a consacré à répondre à mes interrogations.

Je tiens aussi à remercier chaleureusement Bill Allombert pour son aide précieuse pour les exemples numériques.

J'aimerais remercier Philippe Cassou Noguès, qui m'a donné l'envie de faire de la théorie des nombres en suivant ses cours de licence et de maitrise. Un grand merci aussi à Jean Fresnel et Michel Matignon, pour leur aide, pour leur soutien durant ces dernières années.

Je tiens bien sûr à remercier mes collègues doctorants pour ces trois années passées à leur côté qui n'auraient pas été pareilles sans eux... Donc un grand merci à Arthur (pour ces bons moments passés au bureau, pour les croissants..), Pierre et Nico (pour leurs conseils informatiques), Vincent (pour ton bon café), Guigui (pour ta bonne humeur et ton oreille attentive), Cédric (parce que Roland Garros ne sera plus pareil), Sofiane (pour m'avoir ouvert la voie) et enfin merci à Fred pour tous ces bons moments tout au long de ces sept dernières années... Je vous souhaite à tous bon courage et beaucoup de réussite.

Pour leur soutien tout au long de ces années, je remercie très sincèrement mes amis : Aurélie, Julie, Emilie, Christelle, Mathieu, Stéphanie avec un merci particulier à Justine et Matthias, pour leurs encouragements bien sûr et surtout pour leur relecture de cette thèse et j'imagine que ça a pu être pénible parfois... Un grand merci aussi à ma plus vieille amie Laure, qui même de l'autre bout du monde m'a encouragée et je sais qu'elle aimerait être ici aujourd'hui.

Je tiens également à remercier mes parents pour leur soutien, leur encouragement, pour m'avoir permis d'être là où j'en suis. Que seraient ces remerciements sans un mot sur ma petite soeur... Merci à toi pour tout, ton soutien, tes encouragements, ta confiance en moi, ta joie de vivre. Je te souhaite plein de bonheur.

Merci aussi à ma famille de m'avoir soutenue, aidée, soulagée parfois et surtout d'être venue aujourd'hui, cela me touche sincèrement. En ce jour qui marque la fin de mes études, je souhaite beaucoup de réussite et de courage à mes petits cousins Éva et Loïc qui les commencent ! ! Enfin, un grand merci à mes grands-parents, en particulier à ma grand-mère qui a tenu absolument à être là aujourd'hui et j'espère qu'elle ne sera pas déçue.

Pour terminer, merci au charmant Thibault, de m'avoir soutenue, encouragée et d'avoir cru en moi depuis deux ans et surtout de m'avoir supportée ces derniers mois....

Table des matières

Introduction

Pour un nombre premier ℓ fixé, la notion de corps ℓ-rationnel, déjà rencontrée implicitement chez divers auteurs, a été explicitement définie par A. Movahhedi et T. Nguyen quang Do (cf [11]) d'une part et G. Gras et J.-F. Jaulent d'autre part (cf [2]). Cette notion a ensuite été généralisée en celle de corps S-rationnel dans [9].

La question de la propagation de la S-rationalité dans une ℓ-extension L/K de corps de nombres a été complètement résolue dans [9] pour les ℓ premiers impairs. Pour $\ell = 2$ et L/K quadratique il peut arriver que le corps de base K soit $\mathfrak{l}$-rationnel en une place 2-adique décomposée dans l'extension L/K et que L soit $\mathfrak{l}$-rationnel pour chacune des deux places au-dessus de $\mathfrak{l}$; on dit alors que le corps L est birationnel. Le passage de la 2-rationalité à la 2-birationalité dans une extension L/K a été complètement traité dans [8] pour K un corps totalement réel. Rappelons ce résultat :

Soit L/K une extension quadratique totalement imaginaire d'un corps de nombres totalement réel. Les assertions suivantes sont équivalentes :

(i) Le corps L est 2-birationnel,

(ii) Le corps K est 2-rationnel, son unique place 2-adique est décomposée dans L/K et l'extension L/K est ramifiée modérement soit en une place semi-primitive $\mathfrak{p}$ soit en deux places primitives $\mathfrak{p}$ et $\mathfrak{q}$.

L'objet de cette thèse est de poursuivre dans cette voie en étudiant la propagation de la 2-birationalité dans des 2-extensions. Le problème est le suivant : On considère une extension quadratique à conjugaison complexe L d'un corps totalement réel K, et une 2-extension totalement réelle K' de K. On note ensuite $L' = K'L$ leur compositum. Le but de ce travail est d'étudier à quelles conditions sur les extensions L/K et K'/K la 2-birationalité de L est équivalente à celle de L'.

Notre étude se décompose en quatre parties. Dans un premier chapitre, nous rappelons quelques éléments de la théorie ℓ-adique du corps de classes, nous définissons les catégories de corps que nous allons étudier, à savoir les corps ℓ-rationnels et 2-birationnels et nous énonçons les principaux résultats déjà connus relatifs à ces objets.

Dans un deuxième chapitre, nous focalisons notre étude sur le cas quadratique. Nous considérons le cas particulier des corps multiquadratiques et nous listons les corps multiquadratiques 2-birationnels. Cette approche nous a permis de nous familiariser avec les objets avant d'aborder dans la suite du chapitre la question de la propagation de la 2-birationalité lorsque l'extension K'/K est quadratique. Cette simplification nous a permis de dégager les difficultés essentielles liées à notre question. Il s'avère en effet, que cette étude, qui ne fut pas sans écueils, nous a permis une fois résolue, d'éclaircir nos idées et nous a fourni en fin de compte toutes les pistes pour aborder le cas général.

Tout naturellement, le dernier chapitre traite enfin la question de la propagation de la 2-birationalité dans le cas d'une 2-extension totalement réelle quelconque et livre le résultat général. Pour terminer, nous donnons un florilège d'exemples numériques, illustrant notre propos, obtenus à l'aide du logiciel PARI développé à Bordeaux. Ces résultats expérimentaux nous ont amenés à étudier la construction de tours d'extensions 2-birationnelles qui fait l'objet du chapitre final.

Chapitre 1

Rappels et contexte

Ce chapitre est consacré aux rappels des différentes définitions et des principaux résultats nécessaires à la compréhension de notre travail. Nous commençons par un rappel de théorie ℓ-adique du corps de classes où ℓ est un nombre premier ; nous introduisons les principaux objets qui nous permettent d'énoncer le résultat principal à savoir l'isomorphisme du corps de classes ℓ-adique. Dans un second temps, nous définissons des corps particuliers, à savoir les corps ℓ-rationnels et les principaux théorèmes qui s'y rattachent. Puis, nous spécialisons ces objets pour $\ell = 2$ avec de nouvelles définitions dans ce cas particulier. Pour finir, nous introduisons les corps 2-birationnels qui sont l'objet principal de notre étude.

1.1 Index des principales notations

Fixons une fois pour toutes un nombre premier ℓ, on rappelle que les premiers ℓ-adique désignent les places au-dessus de ℓ, i.e. les places sauvages, par opposition aux places modérées objet principal de ce travail.

Notations attachées à un corps de nombres K :

- $\mathcal{P}l_r$, $\mathcal{P}l_c$, $\mathcal{P}l_l$: les ensembles des places réelles, complexes ou ℓ-adiques,
- r, c, l : les nombres de places réelles, complexes ou ℓ-adiques de K,
- S un sous-ensemble non vide des places sauvages (i.e. ℓ-adiques) de K,
- s le nombre de places dans S,
- X un ensemble de places finies modérées (i.e. étrangères à ℓ) de K,
- $\mathcal{J} = \prod_{\mathfrak{p}}^{res} \mathcal{R}_{\mathfrak{p}}$ le ℓ-adifié du groupe des idèles principaux,
- $\widetilde{\mathcal{J}}$: le noyau dans $\mathcal{J}$ de la formule du produit pour les valeurs absolues,
- $\mathcal{R} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$: le sous-groupe des idèles principaux,
- $\widetilde{\mathcal{U}} = \prod_{\mathfrak{p}} \widetilde{\mathcal{U}}_{\mathfrak{p}}$: le groupe des normes cyclotomiques dans $\mathcal{J}$,
- $\widetilde{\mathcal{D}\ell} = \widetilde{\mathcal{J}}/\widetilde{\mathcal{U}}$: le ℓ-groupe des diviseurs logarithmiques,
- $\widetilde{\mathcal{P}\ell} = \mathcal{R}\widetilde{\mathcal{U}}/\widetilde{\mathcal{U}}$: le sous-groupe des diviseurs logarithmiques principaux,
- $\widetilde{\mathcal{C}\ell} = \widetilde{\mathcal{J}}/\widetilde{\mathcal{U}}\mathcal{R} = \widetilde{\mathcal{D}\ell}/\widetilde{\mathcal{P}\ell}$: le ℓ-groupe des classes logarithmiques,
- $\mathcal{U}' = \prod_{\mathfrak{l}|l} \mathcal{R}_{\mathfrak{l}} \prod_{\mathfrak{p}\nmid l} \mathcal{U}_{\mathfrak{p}}$: le groupe de ℓ-unités,

- $\mathcal{C}\ell' = \mathcal{J}/\mathcal{U}'\mathcal{R}$: le ℓ-groupe des ℓ-classes de diviseurs au sens ordinaire,
- $\mathcal{E}' = \mathcal{R} \cap \mathcal{U}' \simeq \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E'_K$: le ℓ-groupe des ℓ-unités,
- $\widetilde{\mu} = \prod_{\mathfrak{p}} \mu_{\mathfrak{p}}$: le sous-groupe fermé des racines de l'unité dans $\mathcal{J}$,
- μ : le ℓ-groupe des racines de l'unité dans $\mathcal{R}$ ($= \widetilde{\mu} \cap \mathcal{R}$ sous Leopoldt).

Quelques pro-ℓ-extensions de K :

- K^c : la $\mathbb{Z}_\ell$-extension cyclotomique,
- K^{lc} : la pro-ℓ-extension abélienne localement cyclotomique maximale,
- M : la pro-ℓ-extension, ℓ-ramifiée, ∞-décomposée maximale de K et $\mathcal{G} = Gal(M/K)$ son groupe de Galois ,
- M^{ab} : la sous-extension maximale de M qui est abélienne sur K et $\mathcal{G}^{ab} = Gal(M^{ab}/K)$ son groupe de Galois,
- Z : la composée des $\mathbb{Z}_\ell$ extensions de K, de sorte que le groupe fini $\mathcal{T} = Gal(M^{ab}/Z)$ soit le sous-groupe de torsion de $\mathcal{G}$,
- K^Z : le compositum des $\mathbb{Z}_\ell$-extensions,

Plus généralement, étant donné un ensemble fini S de places étrangères à ℓ, nous notons :

- M_S : la pro-ℓ-extension, S modérément ramifiée, ∞-décomposée maximale de K (i.e. la composée des ℓ-extensions galoisiennes de K qui sont non ramifiées en dehors de S et de ℓ et complètement décomposées aux places à l'infini) et $\mathcal{G}_S = Gal(M_S/K)$ son groupe de Galois,
- M_S^{ab} : la sous-extension maximale de M_S qui est abélienne sur K, puis $\mathcal{G}_S^{ab} = Gal(M_S^{ab}/K)$ son groupe de Galois et $\mathcal{T}'_S = Gal(M_S^{ab}/Z)$ le sous-groupe de torsion de $\mathcal{G}_S^{ab}$,
- $\mathcal{C}\ell'_S$: le ℓ-groupe des $S\ell$-classes de diviseurs de K, i.e. le quotient de $\mathcal{C}\ell'$ par le sous-groupe engendré par les classes au sens restreint des idéaux construits sur les places de S.

Pour finir ces rappels de notations on introduit deux définitions qui précisent le vocabulaire employé par la suite :

Définition 1.1.1 *(a) On dit qu'une extension est ramifiée modérément lorsqu'il existe au moins une place modérée qui se ramifie dans cette extension.*

(b) On dit qu'une extension est modérément ramifiée, lorsqu'elle est ramifiée uniquement aux places modérées.

1.2 Quelques éléments de théorie ℓ-adique du corps de classes

Cette section est un rapide rappel de théorie ℓ-adique du corps de classes présentée dans [6] ; dans une première partie sont définis les objets nécessaires à l'énoncé des théorèmes exposés en deuxième partie.

1.2.1 Construction des $\mathbb{Z}_\ell$-modules fondamentaux

Le nombre premier ℓ étant fixé, on désigne par $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^k\mathbb{Z}$, l'anneau des entiers ℓ-adiques.

À chaque corps de nombres K, on associe deux $\mathbb{Z}_\ell$-modules : le premier $\mathcal{R}_K$ global, défini à partir du groupe multiplicatif $K^\times$ des éléments non nuls de K ; le second $\mathcal{J}_K$ semi-local, construit à partir des groupes multiplicatifs $K_\mathfrak{p}^\times$ des complétés non complexes de K.

Définition 1.2.1 *Étant donné un corps de nombres K, on appelle ℓ-groupe des idèles principaux de K et on note $\mathcal{R}_K$ le tensorisé ℓ-adique du groupe multiplicatif de ses éléments non nuls :*

$$\mathcal{R}_K = \mathbb{Z}_\ell \otimes_\mathbb{Z} K^\times.$$

Le groupe $\mathcal{R}_K$ est la réunion des ℓ-groupes de S-unités $\mathcal{E}_K^S = \mathbb{Z}_\ell \otimes_\mathbb{Z} E_K^S$, lorsque S parcourt les ensembles finis de places de K. Chacun des $\mathcal{E}_K^S$ est compact pour sa topologie naturelle de $\mathbb{Z}_\ell$-module noethérien et $\mathcal{R}_K$ est lui-même un $\mathbb{Z}_\ell$-module topologique pour la limite inductive des $\mathcal{E}_K^S$.

Définition et proposition 1.2.2 *Pour chaque place $\mathfrak{p}$ du corps de nombres K, on note*

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

le ℓ-adifié du groupe multiplicatif $K_\mathfrak{p}^\times$ du complété de K en $\mathfrak{p}$. Le groupe $\mathcal{R}_\mathfrak{p}$ est un $\mathbb{Z}_\ell$-module noethérien donc compact pour la topologie définie par ses sous-modules d'indice fini.

(i) Si $\mathfrak{p}$ est archimédienne, deux cas se présentent : si $\mathfrak{p}$ est réelle et ℓ égal à 2, $\mathcal{R}_\mathfrak{p}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$; il est nul dans tous les autres cas.

(ii) Si $\mathfrak{p}$ est ultramétrique, le choix d'une uniformisante $\pi_\mathfrak{p}$ permet d'écrire formellement $\mathcal{R}_\mathfrak{p} = \mathcal{U}_\mathfrak{p} \pi_\mathfrak{p}^{\mathbb{Z}_\ell}$ en notant encore $\pi_\mathfrak{p}$ l'image de $\pi_\mathfrak{p}$ dans $\mathcal{R}_\mathfrak{p}$ et en désignant par $\mathcal{U}_\mathfrak{p} = \varprojlim U_\mathfrak{p}/U_\mathfrak{p}^{\ell^k}$ la limite projective des quotients d'exposant ℓ-primaire du sous-groupe des unités du corps local $K_\mathfrak{p}$:

- lorsque $\mathfrak{p}$ divise ℓ, le groupe $\mathcal{U}_\mathfrak{p}$ n'est autre que le groupe des unités principales de $K_\mathfrak{p}$;

- *lorsque $\mathfrak{p}$ ne divise pas ℓ, il s'identifie au ℓ-sous-groupe de Sylow $\mu_{\mathfrak{p}}$ du groupe des racines de l'unité dans $K_{\mathfrak{p}}$.*

Dans les deux cas nous disons que $\mathcal{U}_{\mathfrak{p}}$ est le sous-groupe des unités de $\mathcal{R}_{\mathfrak{p}}$

Définition 1.2.3 *Par ℓ-groupe des idèles d'un corps de nombres K, on entend le produit*

$$\mathcal{J}_K = \prod_{\mathfrak{p}\in Pl_K}^{res} \mathcal{R}_{\mathfrak{p}}$$

des ℓ-adifiés des groupes multiplicatifs des complétés de K, restreint aux familles $(x_{\mathfrak{p}})_{\mathfrak{p}\in Pl_K}$ dont tous les éléments sont des unités à l'exception d'un nombre fini d'entre eux.

Le groupe $\mathcal{J}_K$ est la réunion des ℓ-groupes $\mathcal{J}_K^S = \prod_{\mathfrak{p}\in S}\mathcal{R}_{\mathfrak{p}}\prod_{\mathfrak{p}\notin S}\mathcal{U}_{\mathfrak{p}}$, lorsque S parcourt les ensembles finis de places de K. Chacun des $\mathcal{J}_K^S$ est compact pour sa topologie naturelle de $\mathbb{Z}_\ell$-module produit et $\mathcal{J}_K$ est lui-même un $\mathbb{Z}_\ell$-module topologique pour la limite inductive des topologies des $\mathcal{J}_K^S$.

Maintenant qu'on a construit ces $\mathbb{Z}_\ell$-modules on peut définir le ℓ-groupe des classes d'idèles.

Théorème et définition 1.2.4 *L'application naturelle du tensorisé ℓ-adique $\mathcal{R}_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$ du groupe multiplicatif du corps K dans le ℓ-adifié $\mathcal{J}_K$ du groupe des idèles de K, qui est induite par l'injection diagonale de K dans le produit de ses complétés $\prod_{\mathfrak{p}\in Pl_K} K_{\mathfrak{p}}$ est un morphisme continu. Le groupe topologique quotient :*

$$\mathcal{C}_K = \mathcal{J}_K/\mathcal{R}_K$$

est un $\mathbb{Z}_\ell$-module compact. On dit que c'est le ℓ-groupe des classes d'idèles du corps K.

1.2.2 Isomorphisme du corps de classes ℓ-adique

Nous rappelons sans démonstration dans ce paragraphe les résultats fondamentaux du corps de classes local et global pour les ℓ-extensions. (cf [5] Théorème 2.1 et Théorème 2.3)

Théorème 1.2.5 *(Corps de classes local). Étant donné un corps local $K_{\mathfrak{p}}$, l'application de réciprocité induit un isomorphisme de $\mathbb{Z}_\ell$-modules topologiques entre le compactifié profini $\mathcal{R}_{\mathfrak{p}} = \varprojlim K_{\mathfrak{p}}^\times/K_{\mathfrak{p}}^{\times\ell^k}$ et le groupe de Galois $\mathcal{D}_{\mathfrak{p}} = Gal(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}})$ de la ℓ-extension abélienne maximale du corps $K_{\mathfrak{p}}$. Dans cet isomorphisme le groupe d'inertie $I_{\mathfrak{p}} = In(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}})$ est l'image du sous-groupe $\mathcal{U}_{\mathfrak{p}}$, des unités de $\mathcal{R}_{\mathfrak{p}}$.*

- *Si $\mathfrak{p}$ ne divise pas ℓ, la ramification est modérée et le groupe $I_{\mathfrak{p}}$ est fini, isomorphe au ℓ-Sylow $\mu_{\mathfrak{p}}$ du groupe des racines de l'unité dans $K_{\mathfrak{p}}$.*
- *Si $\mathfrak{p}$ divise ℓ, la ramification est sauvage et le groupe $I_{\mathfrak{p}}$ est infini. Dans ce cas, la suite des sous-groupes supérieurs de ramification est l'image dans $\mathcal{D}_{\mathfrak{p}}$ de la filtration canonique $(U_{\mathfrak{p}}^i)_{i\geq 1} = (1+\mathfrak{p}^i)_{i\geq 1}$ du groupe $\mathcal{U}_{\mathfrak{p}}$.*

Théorème 1.2.6 *(Corps de classes global). Étant donné un corps de nombres K, l'application de réciprocité induit un isomorphisme continu du ℓ-groupe $\mathcal{J}_K$ des idèles de K sur le groupe de Galois $G_K^{ab} = Gal(K^{ab}/K)$ de la ℓ-extension abélienne maximale de K ; le noyau de ce morphisme est le sous-groupe $\mathcal{R}_K$ formé des idèles principaux. Dans la correspondance obtenue, le sous-groupe de décomposition $\mathcal{D}_\mathfrak{p}$ d'une place $\mathfrak{p}$ de K est l'image dans G_K^{ab} du sous-groupe $\mathcal{R}_\mathfrak{p}$ de $\mathcal{J}_K$ et son sous-groupe d'inertie $I_\mathfrak{p}$ est celle du sous-groupe $\mathcal{U}_\mathfrak{p}$ des unités de $\mathcal{R}_\mathfrak{p}$.*

Pour finir ce paragraphe de rappels on va introduire la notion de classes logarithmiques des corps de nombres.

1.2.3 Classes logarithmiques des corps de nombres

Avant de définir le groupe de classes logarithmiques d'un corps de nombres, il nous faut faire quelques définitions préalables. Nous commençons par introduire la valuation logarithmique sur un corps local, puis, les diviseurs logarithmiques et enfin le groupe des classes logarithmiques. Tous ces résultats et définitions sont présentés dans [4]

On considère toujours ℓ un nombre premier fixé. On définit le logarithme d'Iwasawa, noté log sur le groupe $1 + \ell\mathbb{Z}_\ell$ des unités principales du complété ℓ-adique de $\mathbb{Z}$ par son développement en série entière :

$$\log(1+x) = \sum_{k\geq 1}(-1)^{k+1}\frac{x^k}{k}.$$

Il se prolonge classiquement au groupe multiplicatif $\mathbb{Z}_\ell^\times$ des éléments inversibles de $\mathbb{Z}_\ell$ au moyen de l'équation fonctionnelle :

$$\log(xy) = \log x + \log y$$

De plus, si l'on convient d'écrire $x = \omega(x) < x >$ la factorisation canonique d'un élément x de $\mathbb{Z}_\ell^\times$ dans la décomposition directe $\mathbb{Z}_\ell^\times = \mu_\ell \times (1 + 2\mathbb{Z}_\ell)$ du groupe multiplicatif $\mathbb{Z}_\ell^\times$ comme produit de son sous-module de torsion μ_ℓ et du sous-groupe principal $1 + 2\mathbb{Z}_\ell$. On a $\log x = \log < x >$, pour tout x de $\mathbb{Z}_\ell^\times$; l'image du logarithme est le sous-module $2\ell\mathbb{Z}_\ell$ de $\mathbb{Z}_\ell$ et son noyau est le groupe μ_ℓ des racines de l'unité dans $\mathbb{Q}_\ell$.

Définition 1.2.7 *On appelle degré ℓ-adique d'un nombre premier p la quantité :*

(i) deg p= $\log p$= $\log < p >$, pour $p \neq \ell$;

(ii) deg ℓ= ℓ, pour $\ell \neq 2$ et deg $\ell = 4$, pour $\ell = 2$.

Ceci étant posé, on prend $K_\mathfrak{p}$ un corps local, de degré fini $d_\mathfrak{p} = [K_\mathfrak{p} : \mathbb{Q}_p]$ sur $\mathbb{Q}_p$. On note $v_\mathfrak{p}$ la valuation associée et désignons par $|\ |_p$ la valeur absolue ℓ-adique principale qui est définie sur $K_\mathfrak{p}^\times$ par la formule :

$$|x|_\mathfrak{p} = \begin{cases} < N\mathfrak{p}^{-v_p(x)} >, \text{ pour } \mathfrak{p} \nmid \ell, \\ < N_{K_\mathfrak{p}/\mathbb{Q}_\ell}(x) N\mathfrak{p}^{-v_p(x)} >, \text{ pour } \mathfrak{p} | \ell, \end{cases}$$

où $N\mathfrak{p}$ est la norme absolue de $\mathfrak{p}$.

On définit ensuite l'extension $\widehat{\mathbb{Q}}_p^c$, la $\widehat{\mathbb{Z}}$-extension cyclotomique, c'est-à-dire la composée des $\mathbb{Z}_q$-extensions cyclotomiques de $\mathbb{Q}_p$ pour tous les nombres premiers q. Cette notation étant introduite, on a les définitions suivantes :

Définition 1.2.8 *On note alors :*

(i) $\widetilde{e}_{\mathfrak{p}} = [K_{\mathfrak{p}} : K_{\mathfrak{p}} \cap \widehat{\mathbb{Q}}_p^c]$ *est l'indice de ramification logarithmique de* $K_{\mathfrak{p}}$ *;*

(ii) $\widetilde{f}_{\mathfrak{p}} = [K_{\mathfrak{p}} \cap \widehat{\mathbb{Q}}_p^c : \mathbb{Q}_p]$ *est son degré d'inertie logarithmique de* $K_{\mathfrak{p}}$ *;*

(iii) $deg\ \mathfrak{p} = \widetilde{f}_{\mathfrak{p}}\ deg\ p$ *est le degré* ℓ*-adique de l'idéal* $\mathfrak{p}$ *;*

(iv) $\widetilde{v}_{\mathfrak{p}} = -\log|\ |_{\mathfrak{p}}/\,deg\,\mathfrak{p}$ *est la* ℓ*-valuation logarithmique attachée à* $\mathfrak{p}$*.*

Définition 1.2.9 *On appelle* ℓ*-groupe des diviseurs logarithmiques d'un corps de nombres* K*, le* $\mathbb{Z}_\ell$*-module libre* $\mathcal{D}\ell_K$ *construit sur les places finies de* K *:*

$$\mathcal{D}\ell_K = \bigoplus_{\mathfrak{p} \in Pl_K 0} \mathbb{Z}_\ell \mathfrak{p}.$$

Pour chaque diviseur logarithmique $\mathfrak{d} = \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}\ \mathfrak{p}$*, nous écrivons* $deg_K\ \mathfrak{d} = \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}\ deg\,\mathfrak{p}$ *son degré dans* K*. Nous notons enfin* $\widetilde{\mathcal{D}\ell}_K$ *le sous-module de* $\mathcal{D}\ell_K$ *formé des diviseurs logarithmiques de degré nul.*

L'introduction du sous-module $\widetilde{\mathcal{D}\ell}_K$ est motivée par le résultat suivant (cf [4] proposition 2.2) :

Définition et proposition 1.2.10 *Pour chaque place finie* $\mathfrak{p}$ *de* K*, on note* $\widetilde{v}_{\mathfrak{p}}$ *l'application définie sur le tensorisé* ℓ*-adique* $\mathcal{R}_K = \mathbb{Z} \otimes_{\mathbb{Z}} K^\times$ *du groupe multiplicatif* $K^\times$ *induite par la* ℓ*-valuation logarithmique associée à* $\mathfrak{p}$*. L'application* $\mathbb{Z}_\ell$*-linéaire à valeurs dans* $\mathcal{D}\ell_K$

$$\widetilde{div}_K \mid \qquad x \mapsto \sum_{\mathfrak{p} \in Pl_K 0} \widetilde{v}_{\mathfrak{p}}(x)\ \mathfrak{p}$$

envoie $\mathcal{R}_K$ *sur un sous-module* $\widetilde{P\ell}_K$ *du groupe* $\widetilde{\mathcal{D}\ell}_K$ *des diviseurs logarithmiques de degré nul.*

On dit que le quotient $\widetilde{\mathcal{C}\ell}_K = \widetilde{\mathcal{D}\ell}_K/\widetilde{P\ell}_K$ *est le* ℓ*-groupe des classes logarithmiques du corps* K*.*

1.3 Corps ℓ-rationnels

Avant de définir la notion de corps ℓ-rationnel, il nous faut faire un bref rappel sur les symboles sur un corps commutatif vus dans [3].

1.3.1 Symboles sur un corps commutatif

Définition 1.3.1 *Un symbole sur un corps commutatif K, à valeurs dans un groupe abélien G, est une application $< \cdot, \cdot >$ de $K^\times \times K^\times$ dans G qui est bilinéaire et prend la valeur 1 sur tous les couples (a, b) qui vérifient $a + b = 1$, cela peut se résumer par les trois conditions :*

(i) $< aa', b >=< a, b >< a', b >$, $\forall (a, a', b) \in K^\times \times K^\times \times K^\times$;

(ii) $< a, bb' >=< a, b >< a, b' >$, $\forall (a, b, b') \in K^\times \times K^\times \times K^\times$;

(iii) $< a, 1 - a >= 1$, $\forall a \in K^\times \setminus \{0, 1\}$

En particulier, un symbole est une application bilinéaire antisymétrique.

Nous pouvons à présent introduire le K_2 d'un corps de nombres.

Définition 1.3.2 *Par $K_2(K)$ on entend ici le quotient $K^\times \otimes_{\mathbb{Z}} K^\times / \prod_{a+b=1} (a \otimes b)^{\mathbb{Z}}$ du carré tensoriel du groupe multiplicatif de K par le sous-groupe engendré par les éléments de la forme $x \otimes (1 - x)$ lorsque x décrit $K \setminus \{0, 1\}$. Le groupe $K_2(K)$ est caractérisé par la propriété universelle suivante :*

Propriété 1.3.3 *(Propriété universelle) Pour chaque symbole $< \cdot, \cdot >$ sur un corps commutatif K, à valeurs dans un groupe abélien G, il existe un unique morphisme de groupe φ de $K_2(K)$ dans G, qui rend commutatif le diagramme :*

$$\begin{tikzcd} K^\times \times K^\times \arrow[r, "<\cdot,\cdot>"] \arrow[d, "\{\cdot,\cdot\}"'] & G \\ K_2(K) \arrow[ur, "\varphi"'] & \end{tikzcd}$$

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

Pour finir cette partie de rappels, il nous reste à définir deux catégories de symboles : les symboles modérés et réguliers. À présent, K désigne un corps de nombres algébriques.

Définition 1.3.4 *Pour chaque place finie $\mathfrak{p}$ du corps de nombres K, l'application de $K^\times \times K^\times$, à valeurs dans le groupe multiplicatif $k_{\mathfrak{p}}^\times$ du corps résiduel $k_{\mathfrak{p}}$, qui à un couple (a, b) d'éléments de $K^\times$ associe la classe dans $k_{\mathfrak{p}}^\times$ du produit :*

$$(-1)^{v_{\mathfrak{p}}(a)v_{\mathfrak{p}}(b)} \frac{a^{v_{\mathfrak{p}}(a)}}{b^{v_{\mathfrak{p}}(b)}},$$

est un symbole sur K, appelé symbole modéré associé à la place $\mathfrak{p}$ et noté $(\cdot,\cdot)_{\mathfrak{p}}$.

On vient de définir les symboles modérés uniquement pour les places finies mais on peut étendre cette définition aux places à l'infini. Pour cela il suffit de définir une valuation $v_{\mathfrak{p}}$ pour une place $\mathfrak{p}$ infinie.

On suppose maintenant que $\mathfrak{p}$ soit une place à l'infini. On note $K_{\mathfrak{p}}$ le complété de K en $\mathfrak{p}$, puis $k_{\mathfrak{p}}^{\times}$ le groupe résiduel $K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}$. L'application $v_{\mathfrak{p}}$ de $K^{\times}$ dans $\{0,1\}$ définie par :

- $v_{\mathfrak{p}}(x)=0$, si x est un carré dans $K_{\mathfrak{p}}^{\times}$,
- $v_{\mathfrak{p}}(x)=1$, sinon,

est alors une valuation sur K.

Définition 1.3.5 *Pour chaque place à l'infini $\mathfrak{p}$ du corps de nombres K, l'application de $K^{\times}\times K^{\times}$ dans le groupe résiduel $k_{\mathfrak{p}}^{\times}$, qui à un couple (a,b) d'éléments de $K^{\times}$ associe la classe dans $k_{\mathfrak{p}}^{\times}$ du produit :*

$$(-1)^{v_{\mathfrak{p}}(a)v_{\mathfrak{p}}(b)}\frac{a^{v_{\mathfrak{p}}(a)}}{b^{v_{\mathfrak{p}}(b)}},$$

est un symbole sur K, appelé symbole modéré associé à la place $\mathfrak{p}$ noté $(\cdot,\cdot)_{\mathfrak{p}}$.

Le symbole $(\cdot,\cdot)_{\mathfrak{p}}$ est trivial lorsque $\mathfrak{p}$ est complexe. Si $\mathfrak{p}$ est une place réelle, la quantité $(a,b)_{\mathfrak{p}}$ n'est pas 1 si et seulement si les images de a et de b dans le complété $K_{\mathfrak{p}}$ sont toutes deux négatives.

Enfin, nous pouvons définir les symboles dont nous aurons besoin pour la suite. Il s'agit des symboles réguliers.

Définition 1.3.6 *On appelle symbole régulier associé à une place non complexe $\mathfrak{p}$ du corps K le relèvement canonique, noté encore $(\cdot,\cdot)_{\mathfrak{p}}$, du symbole modéré dans le sous-groupe régulier $\mu_{\mathfrak{p}}^{0}$, formé des racines d'ordre étranger à $\mathfrak{p}$, du groupe $\mu_{\mathfrak{p}}$ des racines de l'unité dans le complété $K_{\mathfrak{p}}$.*

Maintenant que nous avons fini d'introduire les notions nécessaires à la compréhension, nous pouvons définir les corps que nous allons utiliser tout au long de notre travail. Commençons donc par les corps ℓ-rationnels.

1.3.2 Définition des corps ℓ-rationnels

Définition 1.3.7 *On dit qu'un corps de nombres K est :*

(i) ℓ-régulier, lorsque le ℓ-sous-groupe de Sylow $R_2(K)$ du noyau dans $K_2(K)$ des symboles réguliers est trivial ;

(ii) ℓ-rationnel lorsque le groupe de Galois $\mathcal{G}_K = Gal(M/K)$ de la pro-extension maximale M/K qui est ℓ-ramifiée et ∞-décomposée est un pro-ℓ-groupe libre.

Lorsque K contient le sous-corps réel maximal $\mathbb{Q}[\zeta+\zeta^{-1}]$ du ℓ-ième corps cyclotomique $\mathbb{Q}[\zeta]$, il est équivalent d'affirmer que K est ℓ-régulier ou qu'il est ℓ-rationnel.

L'équivalence entre régularité et rationalité, sous la condition suffisante $(\zeta+\zeta^{-1}) \in K$, résulte de l'égalité entre les ℓ-rangs :

$$rg_\ell R_2(K) \;=\; rg_\ell \mathcal{T}_K \;+\; \delta_{Leopoldt}$$

qui fait intervenir le défaut de la conjecture de Leopoldt dans K et le sous-module de torsion $\mathcal{T}_K$ de $Gal(M^{ab}/K)$; et de la caractérisation suivante : (cf [7], Théorème 1.2)

Théorème 1.3.8 *Pour tout corps de nombres K, on a équivalence des conditions suivantes :*

(i) Le groupe de Galois $\mathcal{G}_K = Gal(M/K)$ de la pro ℓ-extension maximale de K qui est ℓ-ramifiée et ∞-décomposée est un pro-ℓ-groupe libre (nécessairement sur $1+c_K$ générateurs, si c_K est le nombre de places complexes de K).

(ii) Le groupe de Galois $\mathcal{G}_K^{ab} = Gal(M^{ab}/K)$ de la pro-ℓ-extension abélienne maximale de K qui est ℓ-ramifiée et ∞-décomposée est un $\mathbb{Z}_\ell$-module libre de rang $1+c_K$.

(iii) Le corps K vérifie la conjecture de Leopoldt (pour le nombre premier ℓ) et le sous-module de torsion $\mathcal{T}_K$ de $Gal(M^{ab}/K)$ est nul.

(iv) Le groupe V_K des éléments ℓ-hyperprimaires du corps K se réduit à $K^{\times\ell}$, et l'on a l'identité entre les ℓ-rangs des ℓ-groupes de racines de l'unité :

$$rg_\ell \mu_K = \sum_{\mathfrak{l}|\ell} rg_\ell \mu_{K_\mathfrak{l}}.$$

(v) Le corps K vérifie l'une des deux conditions suivantes :

(a) ou bien K contient une racine primitive ℓ-ième de l'unité ζ_0, auquel cas K possède une unique place $\mathfrak{l}$ au-dessus de ℓ et le ℓ-groupe des ℓ-classes d'idéaux au sens restreint $\mathcal{C}\ell'_K$ est nul ;

(b) ou bien K ne contient pas ζ, auquel cas les places de K au-dessus de ℓ ne se décomposent pas complètement dans l'extension cyclotomique $K[\zeta]/K$ et la ω-composante du ℓ-groupe des ℓ-classes d'idéaux au sens restreint $\mathcal{C}\ell'_{K[\zeta]}$ du corps $K[\zeta]$ est nulle, si ω désigne le caractère cyclotomique de $Gal(K[\zeta]/K)$.

Ces notions sont aussi abordées sous un autre angle dans [10] et [11].

Corollaire 1.3.9 *Exemples de corps ℓ-réguliers ou ℓ-rationnels*

(i) Le corps $\mathbb{Q}$ est ℓ-régulier et ℓ-rationnel pour tout nombre premier ℓ.

(ii) Pour tout premier ℓ, le corps cyclotomique $\mathbb{Q}[\zeta_{\ell^n}]$ engendré par une racine primitive ℓ^n-ième de l'unité est ℓ-régulier (et ℓ-rationnel) si et seulement si le nombre premier ℓ est régulier.

(iii) Les corps quadratiques imaginaires $K = \mathbb{Q}[\sqrt{-d}]$ 2-réguliers (et 2-rationnels) sont $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{-2}]$, ainsi que les corps $\mathbb{Q}[\sqrt{-p}]$ et $\mathbb{Q}[\sqrt{-2p}]$ pour p premier impair de la forme $p \equiv \pm 3 \mod 8$.

Démonstration du corollaire: (cf [7] Corollaire 1.3) Distinguons les divers cas :

(i) Pour le corps des rationnels, on traite la rationalité et le régularité séparément. Par un calcul direct, on montre que le noyau régulier $R_2(\mathbb{Q})$ est nul, de sorte que $\mathbb{Q}$ est ℓ-rationnel pour tout ℓ. Puis, la théorie élémentaire du corps de classes assure que la ℓ-extension abélienne, ℓ-ramifiée, ∞-décomposée maximale de $\mathbb{Q}$ est bien la $\mathbb{Z}_\ell$-extension cyclotomique de $\mathbb{Q}$, ce qui établit la régularité.

(ii) Pour les corps cyclotomiques $\mathbb{Q}[\zeta_{\ell^n}]$, la définition 1.3.7 assure l'équivalence entre ℓ-régularité et ℓ-rationalité. Maintenant la condition (v, a) du théorème 1.3.8 montre que la rationalité se lit sur le nombre de classes du corps $\mathbb{Q}[\zeta_{\ell^n}]$.

(iii) Pour les corps quadratiques imaginaires $\mathbb{Q}[\sqrt{d}]$, en vertu de la définition 1.3.7 pour $\ell = 2$, les notions de ℓ-régularité et de ℓ-rationalité coïncident. De plus, la condition (v,a) du théorème 1.3.8 exige que le corps $\mathbb{Q}[\sqrt{d}]$ n'admette qu'une place au-dessus de 2, ce qui exclut $d \equiv -1 \mod 8$. Il faut de plus que son nombre de 2-classes d'idéaux soit impair ce qui impose, d'après la formule des classes ambiges de Chevalley généralisée (cf.[J2]), qu'il y ait au plus une place modérément ramifiée dans l'extension $K/\mathbb{Q}$, ce qui nous donne $K = \mathbb{Q}[\sqrt{-1}]$ ou $\mathbb{Q}[\sqrt{-2}]$, soit $K = \mathbb{Q}[\sqrt{-\ell}]$ ou $\mathbb{Q}[\sqrt{-2\ell}]$, avec ℓ premier impair tel que 2 ne soit pas norme dans l'extension $K/\mathbb{Q}$, ce qui s'écrit $\ell \equiv \pm 3 \mod 8$.

Corollaire 1.3.10 *Toute ℓ-extension ℓ-ramifiée ∞-décomposée d'un corps ℓ-rationnel est encore un corps ℓ-rationnel.*

Dans la section suivante, on étend cette propriété de montée de la ℓ-rationalité à certaines ℓ-extensions L/K qui admettent de la ramification en dehors de ℓ. Pour cela nous avons besoin de rappeler quelques résultats sur l'arithmétique des ℓ-extensions des corps ℓ rationnels.

1.3.3 ℓ-extensions des corps ℓ-rationnels

Proposition 1.3.11 *Étant donné un corps de nombres K et un ensemble S de s places modérées de K (i.e. de s places finies étrangères à ℓ), les conditions suivantes sont équivalentes :*

(i) Les symboles d'Artin $(\mathfrak{p}, Z/K)$ des places de S pris dans la composée Z des $\mathbb{Z}_\ell$-extensions de K, engendrent un sous-module pur de $Gal(Z/K)$, de dimension s.

(ii) *Les mêmes symboles* $(\mathfrak{p}, Z^{él}/K)$, *pris dans la sous-extension élémentaire de* Z, *engendrent un sous-*$\mathbb{F}_\ell$*-espace vectoriel de* $Gal(Z^{él}/K)$ *de dimension* s.

(iii) *L'intersection* $Z^{él}(S)$ *des sous-corps de décomposition dans* $Z^{él}$ *des places de* S *est d'indice* ℓ^s *dans* $Z^{él}$.

Lorsqu'elles sont vérifiées, nous disons que S *est primitif.*

Exemples d'ensembles primitifs de places modérées.

(i) Soit K un corps totalement réel satisfaisant la conjecture de Leopoldt (pour le nombre premier ℓ). Dans ce cas, les ensembles primitifs de places modérées de K sont exactement les singletons $S = \{\mathfrak{l}\}$, où $\mathfrak{l}$ est une place de K totalement inerte dans la $\mathbb{Z}_\ell$-extension cyclotomique Z/K.

(ii) Soit K le corps cyclotomique $\mathbb{Q}[\zeta_\ell]$ engendré par une racine primitive ℓ-ième de l'unité. Pour $\ell = 3$, l'ensemble $S = \{\mathfrak{l}_7, \mathfrak{l}_{19}\}$ où $\mathfrak{l}_7$ (resp $\mathfrak{l}_{19}$) est une place de K au-dessus de 7 (resp de 19), est 3-primitif.

On peut alors poser la définition suivante :

Définition 1.3.12 *Une* ℓ*-extension* ∞*-décomposée* L/K *est dite primitivement ramifiée lorsque l'ensemble* $\mathcal{R}_{L/K}$ *des places modérément ramifiées dans* L/K *est* ℓ*-primitif.*

Cela étant posé, nous avons : (cf [7], Théorème 3.5)

Théorème 1.3.13 *Étant donné une* ℓ*-extension (finie) de corps de nombres, les deux conditions suivantes sont équivalentes :*

(i) *Le corps* L *est* ℓ*-rationnel.*

(ii) *Le corps* K *est* ℓ*-rationnel et l'extension* L/K *est primitivement ramifiée.*

Ce théorème va nous permettre de donner une autre démonstration du résultat 1.3.9 qui sera énoncée dans le chapitre 2.

Scolie 1.3.14 *Si* K *est totalement réel et vérifie la conjecture de Leopoldt (ce qui est le cas des corps* ℓ*-rationnels), les ensembles primitifs sont les singletons* $\{\mathfrak{p}\}$ *où* $\mathfrak{p}$ *est totalement inerte dans la* $\mathbb{Z}_\ell$*-extension cyclotomique* K^c/K.

1.3.4 Corps $\mathfrak{l}$-rationnels

Définition 1.3.15 *On dit qu'un corps de nombres* K *contenant les racines* ℓ*-ièmes de l'unité est* $\mathfrak{l}$*-rationnel en une place* $\mathfrak{l}$ *au-dessus de* ℓ*, lorsque la* ℓ*-extension (abélienne),* ℓ*-ramifiée,* $\mathfrak{l}$*-décomposée maximale de* K *est triviale.*

On peut alors interpréter la notion de la $\mathfrak{l}$-rationalité de la manière suivante :

Proposition 1.3.16 *Un corps* K *contenant les racines* ℓ*-ièmes de l'unité est* $\mathfrak{l}$*-rationnel si et seulement si on a l'identité entre les groupes d'idèles :*

$$(1)\ \mathcal{J} = \mathcal{R}\mathcal{R}_{\mathfrak{l}} \prod_{\mathfrak{p}\nmid \ell\infty} \mu_{\mathfrak{p}}.$$

Théorème 1.3.17 *La condition* (1) *est satisfaite dans un corps de nombres K (contenant ou non les racines ℓ-ièmes de l'unité) si et seulement si les deux conditions suivantes se trouvent réunies :*

(2) le groupe des ℓ-classes d'idéaux (au sens ordinaire) $\mathcal{C}\ell'$ du corps K est trivial ;

(3) l'application de semi-localisation $s'_{\mathfrak{l}}$ induit une surjection du tensorisé $\mathcal{E}'$ du groupe des ℓ-unités (au sens ordinaire) de K sur le produit $\mathcal{R}_{\mathfrak{l}'} = \prod_{\mathfrak{p}|\ell\infty} \mathcal{R}_{\mathfrak{p}}$ étendu aux places $\mathfrak{l}' \neq \mathfrak{l}$ divisant ℓ et aux places réelles.

Corollaire 1.3.18 *Soit K satisfaisant la condition (1). Alors K est logarithmiquement principal, en ce sens que son ℓ-groupe des classes logarithmiques $\widetilde{\mathcal{C}\ell}$ est trivial. En d'autres termes, une ℓ-extension de K est cyclotomique (i.e. contenue dans la $\mathbb{Z}_\ell$-extension cyclotomique K^c de K) dès qu'elle l'est localement. En particulier, K vérifie banalement la conjecture de Gross généralisée (pour le premier ℓ).*

Ces définitions générales étant posées, nous pouvons spécifier au cas où $\ell = 2$.

1.4 Corps 2-birationnels

1.4.1 Définitions

Dans le cas $\ell = 2$ on peut traduire différemment la notion de 2-rationalité.

Définition 1.4.1 *Un corps totalement réel K est dit 2-rationnel lorsque sa 2-extension galoisienne 2-ramifiée, ∞-décomposée maximale, K' coïncide avec sa $\mathbb{Z}_2$-extension cyclotomique K^c, ce qui a lieu si et seulement si les deux conditions suivantes sont réunies :*

(1a) K admet une unique place 2-adique $\mathfrak{l}$.

(1b) le 2-groupe $\mathcal{C}\ell'_K$ des 2-classes est trivial, en d'autres termes ici le 2-sous-groupe de Sylow du groupe des classes d'idéaux au sens restreint de K est engendré par l'image de $\mathfrak{l}$.

Définition 1.4.2 *Un corps totalement imaginaire L est dit 2-birationnel lorsqu'il est $\mathfrak{l}$-rationnel en chacune des places 2-adiques (en ce sens qu'il n'admet pas de 2-extension, 2-ramifiée, $\mathfrak{l}$-décomposée non triviale), ce qui a lieu si et seulement si les trois conditions suivantes sont vérifiées :*

(a) L admet exactement 2 places 2-adiques $\mathfrak{l}$ et $\mathfrak{l}'$;

(b) le 2-groupe $\mathcal{C}\ell'_L$ des 2-classes de diviseurs de L est trivial, en d'autres termes ici le 2-sous-groupe de Sylow du groupe des classes d'idéaux de L (au sens ordinaire comme au sens restreint) est engendré par les images de $\mathfrak{l}$ et de $\mathfrak{l}'$.

(c) les plongements canoniques de $L^\times$ dans $L_{\mathfrak{l}}^\times$ et $L_{\mathfrak{l}'}^\times$ induisent des isomorphismes $\mathcal{E}'_L \simeq \mathcal{R}_{\mathfrak{l}} \simeq \mathcal{R}_{\mathfrak{l}'}$ du tensorisé 2-adique du groupe des 2-unités de L sur les compactifiés des groupes multiplicatifs des complétés de L aux places 2-adiques.

Cette définition peut être généralisée à tout nombre premier ℓ (cf [9], définition et proposition 1.9).

Définition 1.4.3 *Nous disons qu'un corps de nombres K contenant les racines ℓ-ièmes de l'unité est ℓ-birationnel lorsqu'il est rationnel pour au moins (et donc exactement) deux places au-dessus de ℓ. Un tel corps est totalement imaginaire et possède en tout et pour tout deux places au-dessus de ℓ.*

Grâce à ces définitions nous pouvons énoncer le résultat suivant : (cf [9] Corollaire 1.13)

Proposition 1.4.4 *Les corps quadratiques 2-birationnels sont les corps quadratiques imaginaires $K = \mathbb{Q}[\sqrt{-p}]$ pour p premier de la forme $p \equiv 7 \mod 16$, et $K = \mathbb{Q}[\sqrt{-pq}]$ pour p et q premiers $p \equiv -q \equiv 3 \mod 8$.*

Démonstration de la proposition: D'après ce qui précède, K est totalement imaginaire, admet exactement deux places au-dessus de 2 et son nombre de 2-classes est impair. Il est donc de la forme $\mathbb{Q}[\sqrt{-d}]$ avec $d \equiv -1 \mod 8$, sans facteur carré, et la formule des 2-classes ambiges montre que d admet au plus deux diviseurs premiers (cf [5], Th III, 1.9). Plus précisément, nous avons ici :

$$| \mathcal{C}\ell_K^G |= \frac{\prod_{p|d} e_p(K\mathbb{Q})}{2(2^{\mathbb{Z}}:2^{\mathbb{Z}}\cap N_{K/\mathbb{Q}})} \text{ ; donc}$$

– ou bien $d = p$ premier et le nombre de classes de K est impair en vertu de la formule des classes d'ambiges de Chevalley ;
– ou bien $d = pq$ avec p et q premiers et 2 non carré $\mod p$ (comme $\mod q$) c'est-à-dire $p \equiv \pm 3 \mod 8$, par exemple $p \equiv -q \equiv 3 \mod 8$. De plus, le nombre de classes de K est ici pair.

Examinons successivement les deux éventualités :

1^{er} cas : $K = \mathbb{Q}[\sqrt{-p}]$ avec $p \equiv -1 \mod 8$.

Notons h l'ordre (impair) de l'idéal premier $\mathfrak{l}$ et faisons le choix d'une racine carrée δ de $-p$ dans $\mathbb{Z}_2$. Écrivons $\pi = \frac{1}{2}(a + b\delta)$ l'image dans $\mathbb{Z}_2$ d'un générateur de $\mathfrak{l}^h$ (avec a et b dans $\mathbb{Z}$) ; son conjugué $\overline{\pi} = \frac{1}{2}(a - b\delta)$ est alors une unité de $\mathbb{Z}_2$ et K est 2-birationnel si et seulement si $\pm\overline{\pi}$ n'est pas un carré dans $\mathbb{Z}_2$, i.e. si et seulement si l'on a $\overline{\pi} \not\equiv \pm 1 \mod 8$.

Maintenant, de l'identité normique $N(\mathfrak{l}^h) = 2^h = \pi\overline{\pi} = \frac{1}{4}(a2 + pb2)$ nous tirons $a2 + pb2 = 2^{h+2}$, ce qui nous prouve, puisque h est impair, que 2 est un carré $\mod b$, et nous donne $b \equiv \pm 1 \mod 8$. D'un autre côté, puisque $\overline{\pi}$ est un inversible dans $\mathbb{Z}_2$, nous avons $\overline{\pi}^{-1} \equiv \overline{\pi} \mod 8$ donc, puisque 2^h vaut 2 ou 0 $\mod 8$:

$$b\delta = \pi - \overline{\pi} = 2^h/\overline{\pi} - \pi \equiv (2^h - 1)\overline{\pi} \equiv \pm\overline{\pi} \mod 8.$$

En résumé il vient $\overline{\pi} \equiv \pm b\delta \equiv \pm\delta \mod 8$, d'où comme attendu :

$$\overline{\pi} \not\equiv \pm 1 \mod 8 \Leftrightarrow \delta \not\equiv \pm 1 \mod 8 \Leftrightarrow p \not\equiv \pm 1 \mod 16.$$

2^{nd} cas : $K = \mathbb{Q}[\sqrt{-pq}]$ avec $p \equiv -q \equiv 3 \mod 8$.

L'extension abélienne 2-ramifiée, 2-élémentaire M de K est ici encore de degré 8 sur K. Il en résulte que le corps M est $M = \mathbb{Q}[\sqrt{p}, \sqrt{q}, \sqrt{-1}, \sqrt{-2}]$. Pour vérifier que K est birationnel, il suffit alors de constater que M ne possède que 2 places au-dessus de 2 ce qui résulte clairement du fait que la seule sous-extension de M quadratique et 2-décomposée sur $\mathbb{Q}$ est le corps $K = \mathbb{Q}[\sqrt{-pq}]$.

1.4.2 Caractérisation de la 2-birationalité

Cette définition étant posée, nous avons maintenant besoin d'introduire la notion de place primitive.

Etant donné un corps de nombres K, notons K^z le compositum des $\mathbb{Z}_2$-extensions de K et K^c la $\mathbb{Z}_2$-extension cyclotomique de K ; dans [GJ] une place modérée de K (i.e. une place finie étrangère à 2) est dite *primitive* lorsque son image dans $Gal(K^z/K)$ par l'application d'Artin n'est pas un carré ; elle est dite dans [J1] logarithmiquement primitive lorsque c'est son image dans $Gal(K^z/K)$ qui n'est pas un carré. Il se trouve que, lorsque K est totalement réel et vérifie la conjecture de Leopoldt en 2, le compositum K^z des $\mathbb{Z}_2$-extensions se réduit à la $\mathbb{Z}_2$-extension cyclotomique K^c, de sorte que les deux notions coïncident. Nous adopterons donc dans ce qui suit la convention suivante :

Définition 1.4.5 *Soit K un corps de nombres totalement réel qui satisfait la conjecture de Leopoldt en $\ell = 2$. Nous dirons qu'une place modérée $\mathfrak{p}$ de K (i.e. une place finie ne divisant pas 2) est (relativement au nombre premier 2) :*

- primitive, lorsque son image dans le groupe procyclique $Gal(K^c/K)$ n'est pas un carré, autrement dit lorsqu'elle n'est pas décomposée dans la $\mathbb{Z}_2$-extension cyclotomique K^c/K ;

- semi-primitive, lorsque son image est un carré mais non une puissance 4-ième, autrement dit lorsqu'elle se décompose dans le premier étage de la $\mathbb{Z}_2$-extension cyclotomique K^c/K mais pas au-delà.

Cela étant posé nous avons les résultats suivants : (cf [8] Théorème 4 et Proposition 5)

Théorème 1.4.6 *Soit L/K une extension quadratique totalement imaginaire d'un corps de nombres totalement réel. Les assertions suivantes sont équivalentes :*

(i) Le corps L est 2-birationnel,

(ii) Le corps K est 2-rationnel, son unique place 2-adique est décomposée dans L/K et l'extension L/K est ramifiée modérement soit en une place semi-primitive $\mathfrak{p}$ soit en deux places primitives $\mathfrak{p}$ et $\mathfrak{q}$.

Proposition 1.4.7 *Soit L une extension quadratique totalement imaginaire d'un corps de nombres totalement réel K. Il y a alors équivalence entre :*

(i) Le corps L est 2-birationnel,

(ii) Le corps K est 2-rationnel, l'extension L/K est 2-décomposée, ramifiée modérément en au moins une place finie et le corps L est 2-logarithmiquement principal.

Le théorème ci-dessus donne une condition nécessaire et suffisante de propagation de la 2-birationalité dans le cas d'une extension quadratique d'un corps de nombres. Notre travail consiste à généraliser ce théorème de la manière suivante :

Nous avons choisi de prendre une extension 2-birationnelle L/K et une extension K'/K totalement réelle de K. Nous nous sommes alors posé la question suivante :

À quelles conditions sur L et la ramification dans L/K ou K'/K, le compositum $L' = LK$ est-il un corps 2 -birationnel ?

Puis nous regardons si ces conditions sont nécessaires et suffisantes.

Notre travail se découpe en deux étapes, la démonstration directe s'avérant très délicate. Nous avons commencé par traiter un cas plus simple, en l'occurrence lorsque l'extension K'/K est quadratique. Cette étude fait l'objet du chapitre 2 qui est elle-même partagée en deux. Ensuite, dans le chapitre 3, nous généralisons au cas où K'/K est une 2-extension de degré quelconque.

Chapitre 2

Propagation quadratique de la 2-birationalité

Ce chapitre est consacré à l'étude de la propagation de la 2-birationalité dans le cas particulier des extensions quadratiques. Nous sommes dans la situation suivante : soient K un corps 2-rationnel, K' une extension quadratique totalement réelle de K, L une extension quadratique totalement imaginaire de K, et L' le compositum LK'. Nous voyons dans ce cas qu'il existe une unique extension L'/K' pour laquelle la 2-birationalité de L/K équivaut à celle de L'/K'.

Nous avons choisi de traiter le cas quadratique en deux temps. Tout d'abord, nous commençons par le cas des corps multiquadratiques qui sont par essence plus faciles à manipuler que des extensions quadratiques quelconques d'un corps de nombres. Ceci nous a surtout permis de nous familiariser avec la notion de 2-birationalité et de résoudre des problèmes sur des cas simples, cela nous a donné un bon éclairage pour la suite.

Une fois le cas multiquadratique réglé, nous avons généralisé à une extension quadratique quelconque d'un corps de nombres. Cependant, il s'avère par la suite que le cas quadratique contient le cas général

2.1 Corps multiquadratiques

Le but ce cette section est de lister les corps multiquadratiques 2-birationnels. Or, en vertu du théorème 1.4.6, ils peuvent être vus comme des extensions quadratiques de corps 2-rationnels réels eux aussi multiquadratiques. Nous suivons donc la démarche suivante : dans un premier temps nous listons les corps multiquadratiques réels 2-rationnels puis l'application du théorème 1.4.6 nous donne les corps 2-birationnels.

2.1.1 Corps multiquadratiques 2-rationnels

Théorème 2.1.1 *Les corps réels multiquadratiques 2-rationnels sont les sous-corps des* $\mathbb{Q}[\sqrt{2},\sqrt{p}]$ *pour les nombres premiers p 2-primitifs, c'est-à-dire vérifiant* $p \equiv \pm 3 \mod 8$. *En d'autres termes ce sont $\mathbb{Q}$, les corps quadratiques* $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{p}]$, $\mathbb{Q}[\sqrt{2p}]$ *et les corps biquadratiques* $\mathbb{Q}[\sqrt{2},\sqrt{p}]$.

Démonstration du théorème:

Un corps multiquadratique 2-rationnel est le compositum d'extensions quadratiques 2-rationnelles. On cherche donc à lister les extensions quadratiques réelles de $\mathbb{Q}$ qui sont 2-rationnelles.

D'après le théorème 1.3.13, on a l'équivalence suivante pour L/K une extension de corps :

i) Le corps L est 2-rationnel.

ii) Le corps K est 2-rationnel et l'extension L/K est primitivement ramifiée.

Ici, K est un corps quadratique et 2 rationnel. On cherche donc les extensions K de $\mathbb{Q}$ qui sont primitivement ramifiées. Il s'agit des extensions 2-ramifiées (i.e. non ramifiées en dehors de 2) ou bien ramifiées modérément en une seule place primitive $\mathfrak{p}$ (i.e. non ramifiées en dehors de $\mathfrak{p}$ et de 2).

Il vient ainsi $K = \mathbb{Q}[\sqrt{d}]$ avec :

1. $d = -1$ ou ± 2
2. $d = \pm p$ ou $\pm 2p$.

Finalement, les corps multiquadratiques réels qui sont 2-rationnels sont les sous-corps de $\mathbb{Q}[\sqrt{2}, \sqrt{p}]$ pour les premiers $p \equiv \pm 3 \mod 8$.

Nous retrouvons ici le résultat du corollaire 1.3.9, mais présenté sous un autre éclairage. En effet, dans le corollaire, la démonstration est basée sur la définition des corps 2-rationnels, alors que celle présentée ci-dessus voit les corps multiquadratiques réels 2-rationnels comme des extensions de $\mathbb{Q}$. Le corps des rationnels étant justement 2-rationnel, l'étude est ramenée au cas du théorème 1.3.13.

2.1.2 Corps multiquadratiques 2-birationnels

Nous cherchons à établir dans ce paragraphe la liste des corps multiquadratiques 2-birationnels lesquels sont par définition des extensions quadratiques imaginaires de corps multiquadratiques réels 2-rationnels. En vue de lister, ces corps nous avons besoin du résultat suivant :

Proposition 2.1.2 *Soit L une extension quadratique totalement imaginaire d'un corps totalement réel K. Soient K_n le n-ième étage de la $\mathbb{Z}_2$-extension cyclotomique K^c et $L_n = K_nL$ le compositum. On a alors les équivalences :*

(i) L 2-birationnel $\iff \exists\, n \in \mathbb{N}$ avec L_n 2-birationnel $\iff \forall n \in \mathbb{N}$, L_n 2-birationnel.

(ii) K 2-rationnel $\iff \exists\, n \in \mathbb{N}$ avec K_n 2-rationnel $\iff \forall n \in \mathbb{N}$, K_n 2-rationnel.

Démonstration de la proposition:

i) Nous sommes dans la situation suivante :

L/K est une extension quadratique à conjugaison complexe, 2-décomposée ramifiée modérement en une place au moins. On a de plus, en vertu du résultat 1.4.7 que :

K est 2-rationnel et L est 2-logarithmiquement principal $\Leftrightarrow$ L est 2-birationnel. $(*)$

Or, L 2 logarithmiquement principal s'écrit $\widetilde{\mathcal{C}\ell}_L = 1$. Ceci est équivalent à $\mathcal{C}_L^c = 1$, où $\mathcal{C}_L^c$ est le groupe de Galois $Gal(M_{L^c}/L^c)$ de la 2-extension abélienne non ramifiée 2-décomposée maximale M_{L^c} de L^c, puisque $\widetilde{\mathcal{C}\ell}_L$ est le quotient des co-points fixes de $\mathcal{C}_L^c$ pour l'action de $\Gamma = Gal(L^c/L) \simeq \mathbb{Z}_2$.

Comme la condition $\mathcal{C}_L^c = 1$ est indépendante de n, on peut remplacer K par n'importe quel étage de K^c, ce qui nous donne l'équivalence (i).

ii) Cette équivalence résulte alors (i) et du résultat $(*)$.

Grâce à ce résultat on a le théorème suivant :

Théorème 2.1.3 *Soit K un corps multiquadratique réel 2-rationnel, c'est-à-dire un sous-corps de $\mathbb{Q}[\sqrt{2}, \sqrt{p}]$ avec $p \equiv \pm 3 \mod 8$. Dans ces conditions, les corps multiquadratiques imaginaires 2-birationnels qui contiennent K sont les $K[\sqrt{-d}]$, avec $d \in \mathbb{N}^*$ sans facteur carré et l'une des quatre configurations suivantes :*

a) Lorsque $K[\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$:

(i) $d = q$ premier avec $q \equiv 7 \mod 16$;

(ii) $d = qq'$ avec q, q' premiers et $q \equiv -q' \equiv \pm 3 \mod 8$.

(b) $K[\sqrt{2}] = \mathbb{Q}[\sqrt{2}, \sqrt{p}]$

(i) $d = q \neq p$ premier avec $-q \equiv p \equiv \pm 3 \mod 8$ et $(\frac{p}{q})$=−1 ;

(ii) $d = q \neq p$ premier avec $-q \equiv p \equiv \pm 3 \mod 8$ et $(\frac{p}{q})$=+1.

Ce résultat généralise la proposition 1.4.4 qui ne donne que les corps quadratiques 2-birationnels. Comme pour le cas des corps 2-rationnels, la première démonstration s'appuie essentiellement sur la définition des corps 2-birationnels, alors que celle présentée ci-dessous repose sur l'utilisation du théorème 1.4.6.

Démonstration du théorème:

a) On suppose d'abord $\mathbb{Q}[\sqrt{p}] \not\subseteq K$ et $\mathbb{Q}[\sqrt{2p}] \not\subseteq K$.

K étant un sous-corps de $\mathbb{Q}[\sqrt{2}, \sqrt{p}]$, on a donc deux possibilités. Soit $K = \mathbb{Q}$, soit $K = \mathbb{Q}[\sqrt{2}]$. Or, en vertu de la proposition 2.1.2, ces deux cas sont équivalents. On peut donc supposer que l'on a : $K = \mathbb{Q}$.

On pose $L = \mathbb{Q}[\sqrt{-d}]$. D'après le théorème 1.4.6, on a l'équivalence suivante :

$$L \text{ 2-birationnel} \Leftrightarrow \begin{cases} K \text{ est 2-rationnel (1)} \\ L/K \text{ est 2-décomposée (2)} \\ L/K \text{ est ramifiée modérement en } \mathfrak{q} \text{ semi-primitive} \\ \text{ou bien en } \mathfrak{q} \text{ et } \mathfrak{q}' \text{ primitives (3).} \end{cases}$$

Les assertions (1), (2) et (3) vont nous donner des conditions que doit vérifier d pour que L soit 2-birationnelle.

(1) Comme $K = \mathbb{Q}$, on a bien que K est 2-rationnel.

(2) Le fait que 2 soit décomposé dans L/K se traduit par le fait que $-d$ soit un carré dans $\mathbb{Q}_2^* = \{\pm 1\}(1+4\mathbb{Z}_2)2^{\mathbb{Z}}$. Comme d est réputé sans facteur carré dans $\mathbb{N}$, on a donc :

$$-d \text{ carré dans } \mathbb{Q}_2 \Leftrightarrow -d \equiv 1 \mod 8 \Leftrightarrow d \equiv -1 \mod 8.$$

Finalement, on conclut avec l'équivalence suivante :

$$L/K \text{ 2-décomposée} \Leftrightarrow d \equiv -1 \mod 8.$$

(3) Grâce aux hypothèses sur la ramification modérée dans L/K on a :

$$\begin{cases} \text{ou bien } d = q \text{ et } q \text{ doit être semi-primitive dans } K, \\ \text{ou bien } d = qq' \text{ et } q, q' \text{ doivent être primitives dans } K. \end{cases}$$

Nous regardons alors dans les deux situations suivantes quelles congruences doivent vérifier q et q' pour que L soit 2-birationnelle. Ces congruences reposent essentiellement sur le fait que les places q ou q' doivent être primitives ou semi-primitives dans K.

\+ **Premier cas :** $d = q$.

La place q ramifiée dans L doit donc être semi-primitive pour que L soit 2-birationnelle. On rappelle que cela signifie que q est décomposée dans le premier étage de l'extension cyclotomique, K^c de K mais pas dans le second. On a alors les équivalences suivantes :

$$q \text{ décomposée dans le premier étage } \begin{cases} \Leftrightarrow q \text{ décomposée dans } \mathbb{Q}[\sqrt{2}]/\mathbb{Q}. \\ \Leftrightarrow (\dfrac{p}{q}) = 1 \Leftrightarrow (-1)^{\frac{q^2-1}{8}}. \\ \Leftrightarrow q2 \equiv 1 \mod 16 \Leftrightarrow q \equiv \pm 1 \mod 8. \end{cases}$$

On a de plus q non-décomposée dans le deuxième étage de l'extension cyclotomique ; cela signifie qu'on a $q \equiv \pm 1 \mod 16$ (car dans ce cas le groupe de décomposition de q est $< q \mod 16 >$). Ainsi, le fait que la place q soit semi-primitive se traduit par $q \equiv \pm 1 \mod 8$ et $q \not\equiv \pm 1 \mod 16$. Finalement en regroupant ces deux congruences on obtient :

$$q \text{ semi-primitive} \Leftrightarrow q \equiv \pm 7 \mod 16$$

De plus, la condition (2), de 2-décomposition se traduit par $d \equiv -1 \mod 8$.
En conclusion, le seul cas qui convient est $d = q \equiv 7 \mod 16$.

\+ **Deuxième cas :** $d = qq'$.

Dans ce cas, pour que L soit 2-birationnelle il faut que les deux places q et q' ramifiées modérément dans L/K soient primitives dans K, ce qui signifie que q et q' ne sont pas décomposées dans le premier étage de l'extension cyclotomique $\mathbb{Q}^c$. Ceci se lit sur le symbole de Legendre ; on a :

$$q \text{ primitive} \Leftrightarrow (\frac{2}{q}) = 1.$$

On a donc : q primitive $\Leftrightarrow q \equiv \pm 3 \mod 8$; il en est de même pour q'. De plus par (2), on a toujours $d = qq' \equiv -1 \mod 8$.

Finalement, en regroupant ces résultats on a $d = qq'$ avec $q \equiv -q' \equiv \pm 3 \mod 8$. Cela achève la démonstration du a).

b) On suppose à présent $\mathbb{Q}[\sqrt{p}] \subseteq K$ ou $\mathbb{Q}[\sqrt{2p}] \subseteq K$.

Dans ce cas, on a $K = \mathbb{Q}[\sqrt{p}]$ ou $K = \mathbb{Q}[\sqrt{2p}]$ ou $K = \mathbb{Q}[\sqrt{2}, \sqrt{p}]$. D'après la proposition 2.1.2, nous savons que ces trois cas sont équivalents. On peut donc supposer $K = \mathbb{Q}[\sqrt{p}]$.

On pose $L = K[\sqrt{-d}]$. D'après le théorème 1.4.6, on a toujours l'équivalence suivante :

$$L \text{ 2-birationnel} \Leftrightarrow \begin{cases} -K \text{ est 2-rationnel (1).} \\ -L/K \text{ est 2-décomposée (2).} \\ -L/K \text{ est ramifiée modérement en } \mathfrak{q} \text{ semi-primitve} \\ \text{ou en } \mathfrak{q}, \mathfrak{q}' \text{primitives (3).} \end{cases}$$

Nous allons regarder à quelles conditions sur d et p, (1), (2) et (3) sont vérifiées.

(1) K est 2-rationnel par hypothèse.

(2) Nous souhaitons que l'extension L/K soit 2-décomposée. Nous sommes dans la situation suivante :

$$\begin{tikzcd}
k = \mathbb{Q}[\sqrt{-d}] \arrow[rr, dash] \arrow[dd, dash] & & L \arrow[dd, dash] \\
& k^* = \mathbb{Q}[\sqrt{-dp}] \arrow[ur, dash] & \\
\mathbb{Q} \arrow[rr, dash] \arrow[ur, dash] & & K = \mathbb{Q}[\sqrt{p}]
\end{tikzcd}$$

On veut L/K est 2-décomposée donc :

(i) ou bien $k/\mathbb{Q}$ est 2-décomposée, ce qui a lieu pour $d \equiv -1 \mod 8$;

(ii) ou bien $k/\mathbb{Q}$ est 2-inerte ; ce qui nécessite que $K/\mathbb{Q}$ soit également 2-inerte donc qu'on ait $-d \equiv p \equiv 5 \mod 8$, de telle sorte que $k^*/\mathbb{Q}$ est 2-décomposée ;

(iii) ou bien $k/\mathbb{Q}$ est 2-ramifiée ; cela nécessite que $K/\mathbb{Q}$ soit également 2-ramifiée et que $k^*/\mathbb{Q}$ soit 2-décomposée (ce qui n'est pas automatique) ; auquel cas cela impose :

$$-d \equiv 2, 3 \mod 4, \quad p \equiv 3 \mod 8, \quad -dp \equiv 1 \mod 8.$$

c'est à dire, finalement :

$$-d \equiv 3 \mod 8, \quad p \equiv 3 \mod 8, \quad -dp \equiv 1 \mod 8.$$

En conclusion le fait que L/K soit 2-décomposée se traduit par :

(i) $-d \equiv 1 \mod 8$;

ou

(ii) $-d \equiv p \equiv 5 \mod 8$;

ou

(iii) $-d \equiv 3 \mod 8, \quad p \equiv 3 \mod 8, \quad -dp \equiv 1 \mod 8.$

(3) Regardons à présent la ramification. Nous sommes toujours dans la situation suivante :

$$\begin{tikzcd}
k = \mathbb{Q}[\sqrt{-d}] \arrow[rr, dash] \arrow[dd, dash] & & L \arrow[dl, dash] \arrow[dd, dash] \\
& k^* = \mathbb{Q}[\sqrt{-dp}] \arrow[dl, dash] & \\
\mathbb{Q} \arrow[rr, dash] & & K = \mathbb{Q}[\sqrt{p}]
\end{tikzcd}$$

Le corps L est 2-birationnel si L/K est ramifiée modérément en deux places $\mathfrak{q}$ et $\mathfrak{q}'$ primitives, ou encore en une seule place $\mathfrak{q}$ semi-primitive. Pour étudier cela on va regarder la ramification dans $k/\mathbb{Q}$. En effet, la ramification dans L/K provient de celle dans $k/\mathbb{Q}$.

\+ Supposons d'abord que $k = \mathbb{Q}[\sqrt{-d}]$ est ramifiée modérément en q et q' distincts de p. Ces deux places doivent alors être les seules places modérément ramifiées dans L/K. Donc il faut qu'elles soient :

i) inertes dans $K/\mathbb{Q}$, car sinon il y aurait trop de places ramifiées dans L/K. Cela signifie que l'on a $(\frac{p}{q}) = (\frac{p}{q'})$=1.

ii) primitives dans L, c'est-à-dire non décomposées dans le premier étage de $L[\sqrt{2}]/L$ de L^c/L ; ce qui implique non décomposées dans $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$.

Traduisons cela : nous nous plaçons à présent dans l'extension $L[\sqrt{2}]/\mathbb{Q}$ qui est biquadratique. Les conditions requises se traduisent par l'indice de ramification e =2 et le degré résiduel f=4.

Or, dans ce cas la sous-extension $\mathbb{Q}[\sqrt{2}, \sqrt{p}]$ devrait être totalement inerte en q et en q'. Et cette dernière n'étant pas cyclique, ce cas est impossible.

En conclusion, $K/\mathbb{Q}$ ne peut être ramifiée qu'en une seule place modérée autre que p.

\+ Nous avons donc $L = K[\sqrt{-d}]$ avec $d = q$ ou $d = pq$ (puisque nous avons vu que d est impair dans les trois cas à considérer) ; ainsi, quitte à remplacer k par k^*, on peut supposer que p ne divise pas d ; autrement dit : $d = q$. Nous avons de plus, toujours par la 2-décomposition de L/K :

(i) soit $q \equiv -1 \mod 8$;

(ii) soit $q \equiv -p \equiv 3 \mod 8$;

(iii) soit $q \equiv 5 \mod 8$ avec $p \equiv 3 \mod 8$ et $pq \equiv -1 \mod 8$.

Plusieurs situations se profilent alors, suivant le comportement de q dans $K/\mathbb{Q}$.

Premier cas : La place q est inerte dans $K/\mathbb{Q}$, i.e. $(\frac{p}{q})$=-1.

Dans ce cas q doit être semi-primitive dans K. On a alors le schéma cyclotomique :

$$\begin{tikzcd}
\mathbb{Q}[\sqrt{2+\sqrt{2}}] \arrow[r, dash] \arrow[d, dash] & K[\sqrt{2+\sqrt{2}}] \arrow[d, dash] \\
\mathbb{Q}[\sqrt{2}] \arrow[r, dash] \arrow[d, dash] & K[\sqrt{2}] \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & K
\end{tikzcd}$$

dans lequel q est inerte dans $K/\mathbb{Q}$, décomposée dans le premier étage $K[\sqrt{2}]/K$ de la $\mathbb{Z}_2$-extension cyclotomique de K et inerte dans le second $K[\sqrt{2+\sqrt{2}}]/K[\sqrt{2}]$. On constate que cela a lieu si et seulement si q est inerte dans $K/\mathbb{Q}$ et dans $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$; ce qui s'écrit : $q \equiv \pm 3 \mod 8$.

Compte tenu des congruences données plus haut, on a ainsi un premier cas favorable :

$$d = q \neq p \text{ premier avec } -q \equiv p \equiv \pm 3 \mod 8 \text{ et } (\tfrac{p}{q})\!=\!-1.$$

Deuxième cas : La place q est décomposée dans $K/\mathbb{Q}$, i.e. $(\frac{p}{q})$=1.

Ici q s'écrit $\mathfrak{q}_1\mathfrak{q}_2$ dans K. Nous voulons de plus que $\mathfrak{q}_1$ et $\mathfrak{q}_2$ soient primitives dans K, i.e. inertes dans $K[\sqrt{2}]/K$ ou, ce qui revient au même, dans $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$; ce qui se traduit en termes de congruences par : $q \equiv \pm 3 \mod 8$.

$$\begin{tikzcd}
\mathbb{Q}[\sqrt{2}] \arrow[r, dash] \arrow[d, dash] & K[\sqrt{2}] \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & K
\end{tikzcd}$$

Il ne reste donc qu'à vérifier les hypothèses sur la 2-décomposition de L/K. Compte tenu des congruences données plus haut, on obtient ainsi un deuxième cas favorable :

$$d = q \neq p \text{ premier avec } -q \equiv p \equiv \pm 3 \mod 8 \text{ et } (\tfrac{p}{q})\!=\!+1.$$

Cela termine le b) et la démonstration du théorème.

Remarque. Il peut être intéressant d'observer pour la suite que dans le second cas du théorème, sous la condition $p \nmid d$ qui traduit la non-ramification de p dans $k/\mathbb{Q}$, on a obtenu $d = q$ et $-dp \equiv 1 \mod 8$. Le sous-corps de décomposition de 2 dans $L/\mathbb{Q}$ est alors k^*, lequel est alors ramifié en p.

Nous venons d'obtenir tous les corps multiquadratiques 2-birationnels. Nous allons utiliser la même démarche de démonstration pour étudier la propagation de la 2-birationalité. Nous allons commencer par traiter le cas quadratique.

2.2 Extensions quadratiques ramifiées modérément

Nous venons de lister les corps multiquadratiques 2-birationnels, nous allons tenter de géneraliser ce résultat en étudiant des extensions quadratiques d'un corps 2-rationnel K, quelconque en présence de ramification modérée.

Définition 2.2.1 *Nous rappelons qu'une* 2*-extension* K'/K *est ramifiée modérément lorsqu'il existe au moins une place modérée (i.e. une place finie étrangère à* 2*) qui se ramifie dans* K'/K*.*

Nous sommes donc dans le contexte suivant. Soient K un corps 2-rationnel, K' une extension quadratique, ramifiée modérément et totalement réelle de K, i.e. $K' = K[\sqrt{d}]$, L une extension quadratique totalement imaginaire de K, i.e. $L = K[\sqrt{\delta}]$ avec $(\delta << 0)$. Enfin nous posons L' le compositum LK' et $L^* = K[\sqrt{d\delta}]$. Nous sommes dans le schéma suivant :

$$\begin{tikzcd}
L = K[\sqrt{\delta}] \arrow[rr, dash] & & L' \\
& L^* \arrow[ur, dash] & \\
K \arrow[uu, dash] \arrow[ur, dash] \arrow[rr, dash] & & K' = K[\sqrt{d}] \arrow[uu, dash]
\end{tikzcd}$$

Nous voulons regarder comment se propage la notion de 2-birationalité dans ces extensions ; plus explicitement nous cherchons à savoir à quelles conditions L' est 2-birationnel si L l'est et réciproquement. Pour faciliter le travail, nous allons étudier séparement la descente (i.e. nous supposons L' 2-birationnel et nous regardons quelles hypothèses doit vérifier L' pour que L soit aussi 2-birationnel) puis la montée (i.e la réciproque) ; enfin nous regroupons nos résultats dans un théorème final.

Théorème de descente

Le but de cette section est de démontrer le résultat suivant :

Théorème 2.2.2 (Descente en présence de ramification modérée) .

Soient K *un corps* 2*-rationnel,* $K' = K[\sqrt{d}]$ *(avec* $d >> 0$*) une extension quadratique totalement réelle de* K*, primitivement ramifiée en une place modérée* $\mathfrak{p}$*, et* $L = K[\sqrt{\delta}]$ *(avec* $\delta << 0$*) une extension quadratique totalement imaginaire de* K*. Soit enfin* L' *le compositum* LK' *et* $L^* = K[\sqrt{d\delta}]$*. Supposons l'extension* L'/K' *2-birationnelle. Alors :*

(i) Le corps K' *possède une une unique place* $\mathfrak{l}$ *au-dessus de 2, laquelle se décompose dans l'extension* L'/K' *de sorte qu'une et une seule des extensions* L/K *et* L^*/K *est 2-décomposée. Quitte à les échanger, on peut supposer que c'est* L/K*.*

(ii) Cela étant, deux cas dès lors se présentent :

(a) ou bien l'extension L'/K' *est biramifiée modérément en deux places primitives au-dessus d'une même place* $\mathfrak{q}$ *de* K*, nécessairement distincte de* $\mathfrak{p}$ *;*

(b) ou bien l'extension L'/K' est ramifiée modérément en une unique place semi-primitive au-dessus d'une place primitive $\mathfrak{q}$ de K inerte dans K'/K.

Et dans les deux cas l'extension L/K est 2-birationnelle si et seulement si elle est aussi ramifiée en $\mathfrak{p}$.

Démonstration du théorème:

On suppose donc que l'extension L'/K' est 2-birationnelle. Par le théorème 1.4.6, on sait que :

- K' est 2-rationnel (possédant une unique place 2-adique $\mathfrak{l}'$),
- L'/K' est 2-décomposée,
- l'extension L'/K' est modérément ramifiée en deux places primitives ou en une seule semi-primitive.

De plus, nous savons par hypothèse que l'extension K'/K est ramifiée modérément en une place $\mathfrak{p}$ primitive, ainsi d'après le théorème 1.3.13, on en déduit que : K est 2-rationnel.

De ce fait, on tire : K possède une unique place 2-adique $\mathfrak{l}$ qui est non décomposée dans K'/K et décomposée dans L'/K'. Son sous-groupe de décomposition dans L'/K est donc d'indice 2 et son sous-corps de décomposition est de degré 2. On en déduit donc qu'il s'agit de L ou de L^*. On peut supposer que c'est L. ce qui établit le point (i) du théorème.

Il ne reste plus qu'à regarder la ramification dans L/K, en étudiant celle dans L'/K'.

+ **Premier cas :** L'/K' est modérément ramifiée en deux places primitives $\mathfrak{q}'_1$ et $\mathfrak{q}'_2$.

a) Si $\mathfrak{q}'_1$ et $\mathfrak{q}'_2$ sont au-dessus d'un même $\mathfrak{q}$, décomposé dans K'/K.

On a alors le schéma ci-dessous :

$$\begin{tikzcd}
K^c \arrow[r, dash] \arrow[d, dash] & K'^c \arrow[d, dash] \\
K_1 \arrow[r, dash] \arrow[d, dash] & K'_1 \arrow[d, dash] \\
K \arrow[r, dash] & K'
\end{tikzcd}$$

où K^c (resp K'^c) désigne l'extension cyclotomique de K (resp de K'), K_1 (resp K'_1) le premier étage de l'extension cyclotomique K^c (resp de K'^c).

Ici, $\mathfrak{q}'_1$ et $\mathfrak{q}'_2$ sont inertes dans K'_1/K' car primitives dans K', $\mathfrak{q}$ étant décomposée dans K'/K, il en résulte que $\mathfrak{q}$ est forcément inerte dans K_1/K donc primitive dans K. Cette place est de plus ramifiée dans L/K.

Si $\mathfrak{q}$ est la seule place modérément ramifiée dans L/K, alors, en vertu du théorème 1.4.6, L/K n'est pas 2-birationnelle, car elle devrait être modérément ramifiée en deux places primitives. Il suit donc que L/K doit être ramifiée en une seconde place primitive qui ne peut se ramifier dans L'/K'. Cette place est forcément $\mathfrak{p}$, car toute autre place entrainerait de la ramification dans L'/K'. Vérifions alors que $\mathfrak{p}$ convient.

En utilisant la théorie de Kummer, en notant $\mathfrak{p}'$ la place au dessus de $\mathfrak{p}$ dans K', on a : $\nu_{\mathfrak{p}'}(\delta) = 2\nu_{\mathfrak{p}}(\delta)$ qui est paire. Donc $\mathfrak{p}'$ est non ramifiée dans L'/K'.

Finalement on conclut dans ce cas que l'extension L/K est donc 2-birationnelle.

b) Si les deux places $\mathfrak{q}'_1$ et $\mathfrak{q}'_2$ proviennent de $\mathfrak{q}_1$ et $\mathfrak{q}_2$.

L'extension L/K est alors ramifiée en $\mathfrak{q}_1$ et $\mathfrak{q}_2$. De plus, l'une au moins de ces deux places par exemple $\mathfrak{q}_1$, est distincte de $\mathfrak{p}$ donc inerte dans K'/K.

On se place dans le schéma ci-dessous :

$$\begin{tikzcd}
K^c \arrow[r, dash] \arrow[d, dash] & K'^c \arrow[d, dash] \\
K_1 \arrow[r, dash] \arrow[d, dash] & K'_1 \arrow[d, dash] \\
K \arrow[r, dash] & K'
\end{tikzcd}$$

où K^c (resp K'^c) désigne l'extension cyclotomique de K (resp de K'), K_1 (resp K'_1) le premier étage de l'extension cyclotomique K^c (resp de K'^c).

Ainsi $\mathfrak{q}_1$ est inerte dans K'/K et aussi dans K'_1/K' car primitive ; donc elle est totalement inerte dans l'extension K'_1/K. Or, cette dernière n'étant pas cyclique, c'est impossible ; donc ce sous-cas est exclu.

$+$ **Deuxième cas :** L'/K' est modérément ramifiée en une place semi-primitive $\mathfrak{q}'$.

La place $\mathfrak{q}'$ provient de $\mathfrak{q}$, ramifiée dans L/K.

Cette place ne peut pas se décomposer dans K'/K car sinon il y aurait deux places ramifiées dans K'/K ce qui n'est pas le cas.

Si $\mathfrak{q}$ est ramifiée dans K'/K, en utilisant la théorie de Kummer, on a :

– $\mathfrak{q}$ ramifiée dans L/K, donc la valuation $\nu_{\mathfrak{q}}(\delta)$ est impaire ;

– $\mathfrak{q}$ ramifiée dans K'/K, donc la valuation $\nu_{\mathfrak{q}}(d)$ est aussi impaire.

Il en résulte que la valuation $\nu_{\mathfrak{q}}(d\delta)$ est paire, donc la place $\mathfrak{q}$ n'est pas ramifiée dans L^*/K et a fortiori dans L'/K' ce qui est exclu.

Finalement la place $\mathfrak{q}$ ne peut être qu'inerte dans K'/K.

Plaçons nous maintenant dans le schéma cyclotomique : On note K_1 (resp K'_1) le premier étage de K^c (resp K'^c), puis K_2 (resp K'_2) le second. Ce qui nous donne le schéma suivant :

$$\begin{tikzcd}
K^c \arrow[r, dash] \arrow[d, dash] & K'^c \arrow[d, dash] \\
K_2 \arrow[r, dash] \arrow[d, dash] & K'_2 \arrow[d, dash] \\
K_1 \arrow[r, dash] \arrow[d, dash] & K'_1 \arrow[d, dash] \\
K \arrow[r, dash] & K'
\end{tikzcd}$$

Si $\mathfrak{q}$ était décomposée dans K_1/K, elle serait totalement inerte dans K'_2/K'_1, qui est non cyclique, ce qui est exclu. On en déduit donc que $\mathfrak{q}$ est primitive dans K.

Ici encore, L/K est donc birationnelle si et seulement si elle est aussi ramifiée en $\mathfrak{p}$.

Ce qui termine la démonstration.

On s'intéresse à présent à la montée, pour voir si nous pouvons trouver une équivalence dans les conditions.

Théorème de montée

L'objet de ce paragraphe est de démontrer le résultat suivant :

Théorème 2.2.3 (Montée en présence de ramification modérée) .

Soient K un corps 2-rationnel, $K' = K[\sqrt{d}]$ (avec $d >> 0$) une extension quadratique totalement réelle de K, ramifiée modérément en une unique place $\mathfrak{p}$ primitive ; et $L = K[\sqrt{\delta}]$ (avec $\delta << 0$) une extension quadratique totalement imaginaire de K. Soit enfin L' le compositum LK'. Alors :

Si L/K 2-birationnelle et modérément ramifiée en une place primitive $\mathfrak{q}$ comme en $\mathfrak{p}$, l'extension L'/K' est 2-birationnelle.

Démonstration du théorème:

On suppose que L/K est 2-birationnelle. On suppose de plus ici que K'/K est ramifiée modérément en exactement une place $\mathfrak{p}$, laquelle est primitive, de sorte que K est bien un corps 2-rationnel totalement réel.. On se demande si L'/K' est 2-birationnelle.

On sait déjà que L'/K' est 2-décomposée car L/K l'est. On regarde donc la ramification modérée dans L/K.

Par hypothèse, L/K est ramifiée en $\mathfrak{p}$ et $\mathfrak{q}$ primitives et en aucune autre place modérée. Il en résulte que L'/K' ne peut se ramifier modérément qu'aux places au-dessus de $\mathfrak{p}$ ou de $\mathfrak{q}$.

En utilisant la théorie de Kummer, on remarque que l'unique place $\mathfrak{p}'$ de K' au-dessus de $\mathfrak{p}$ ne se ramifie plus dans L'/K' : on a, en effet, $L' = K'[\sqrt{\delta}]$ et la valuation $v'_{\mathfrak{p}}(\delta) = 2v_{\mathfrak{p}}(\delta)$ est paire.

Finalement, seules les places au-dessus de $\mathfrak{q}$ sont ramifiées dans L'/K', pour lesquelles deux cas se présentent.

+ **Premier cas :** Si $\mathfrak{q}$ est inerte dans K'/K.

On note $\mathfrak{q}'$ la place au-dessus de $\mathfrak{q}$ dans K'. On regarde alors la nature de $\mathfrak{q}'$. Pour cela, on se place dans le schéma ci-dessous : en notant K_1 (resp K'_1) le premier étage de K^c (resp K'^c), puis K_2 (resp K'_2) le second.

$$\begin{array}{ccc} K_2 & \text{———} & K'_2 \\ | & & | \\ K_1 & \text{———} & K'_1 \\ | & & | \\ K & \text{———} & K' \end{array}$$

Il vient dans ce schéma :

– La place $\mathfrak{q}$ est primitive dans K, elle est donc inerte dans K_1/K et dans K_2/K_1,
– La place $\mathfrak{q}$ est inerte dans K'/K.

Le sous-groupe d'inertie de $\mathfrak{q}$ dans l'extension composée K_1'/K étant cyclique, on en déduit que $\mathfrak{q}'$ est décomposée dans K_1'/K'.

Cela étant, on voit que :
– $\mathfrak{q}$ est inerte dans K_2/K_1
– $\mathfrak{q}$ est décomposée dans K_1'/K_1

De ce fait, les deux places au-dessus de $\mathfrak{q}'$ dans K_1' sont inertes dans K_2'/K_1'. Ainsi, $\mathfrak{q}'$ est semi-primitive dans K' et l'extension L'/K' est 2-birationnelle.

+ **Deuxième cas :** Si $\mathfrak{q}$ se décompose dans K'/K.

On note $\mathfrak{q}_1'$ et $\mathfrak{q}_2'$ les deux places au dessus de $\mathfrak{q}$ dans K'. Reprenons le schéma galoisien :

$$\begin{tikzcd}[arrows=dash]
K^c \arrow[r] \arrow[d] & K'^c \arrow[d] \\
K_1 \arrow[r] \arrow[d] & K_1' \arrow[d] \\
K \arrow[r] & K'
\end{tikzcd}$$

où K^c (resp K'^c) désigne l'extension cyclotomique de K (resp de K'), K_1 (resp K_1') le premier étage de l'extension cyclotomique K^c (resp de K'^c).

Dans ce dernier cas, $\mathfrak{q}$ est inerte dans K_1/K et décomposée dans K'/K ; on en déduit que les deux places $\mathfrak{q}_1'$ et $\mathfrak{q}_2'$ sont aussi inertes dans K_1'/K' : elles sont donc primitives.

Finalement, l'extension L'/K' est 2-birationnelle.

Cela achève la démonstration.

Théorème général en présence de ramification modérée

Rassemblant ce qui précède en un seul résultat, on en déduit le théorème suivant :

Théorème 2.2.4 (Propagation quadratique modérée de la 2-birationalité) .

Soient K un corps 2-rationnel, $K' = K[\sqrt{d}]$ (avec $d >> 0$) une extension quadratique totalement réelle de K, primitivement ramifiée en une place modérée $\mathfrak{p}$, et $L = K[\sqrt{\delta}]$ (avec $\delta << 0$) une extension quadratique totalement imaginaire de K. Soit enfin L' le compositum LK' et $L^* = K[\sqrt{d\delta}]$. Supposons l'extension L/K 2-décomposée et ramifiée en la place $\mathfrak{p}$.

Les assertions suivantes sont alors équivalentes :

(i) L/K 2-birationnelle et modérément ramifiée en une place primitive $\mathfrak{q}$ et en $\mathfrak{p}$.

(ii) L'extension L'/K' est 2-birationnelle.

Remarque 1. Comme expliqué plus haut, une et une seule parmi les deux extensions L/K et L^*/K se trouve être 2-décomposée dès que l'extension L'/K' est 2-décomposée.

Quitte à échanger les rôles de L et de L^*, il est toujours possible naturellement de supposer que c'est L/K sans restreindre pour autant la généralité. De même, par un argument de théorie de Kummer, une et une seule parmi les deux extensions L/K et L^*/K est ramifiée en la place $\mathfrak{p}$. Mais rien n'assure alors que ce soit la même. D'où la nécessité d'en faire l'hypothèse pour réaliser la descente.

Remarque 2. Si on ne suppose plus l'extension L/K ramifiée modérément en $\mathfrak{p}$, il peut arriver lors de la descente que cette dernière ne soit ramifiée modérément qu'en la seule place primitive $\mathfrak{q}$. Or, le corps K étant 2-rationnel, en vertu du théorème 1.3.13, il vient que L/K est alors 2-rationnelle. On note donc, que l'on a dans ce cas une dégénérescence de la 2-rationalité en 2-rationalité.

Une fois ce théorème démontré, nous avons cherché à aller plus loin. En effet dans ce qui précède, nous considérions toujours une extension K'/K quadratique. Il vient alors une question légitime, que se passe-t-il si l'on remplace K' par une 2-extension totalement réelle arbitraire de K, peut-on encore avoir un théorème de propagation de la 2-birationalité ?

Cette étude fait l'objet du chapitre 3. Avant cela nous allons traiter la cas particulier où l'extension K'/K n'est pas ramifiée ou bien si elle est ramifiée uniquement en 2

2.3 Propagation quadratique de la 2-birationalité

Pour l'instant nous avons traité uniquement le cas où l'extension K'/K est ramifiée modérément, mais que se passe-t-il dans le cas contraire ?

Cas non ramifié modérément

Nous sommes donc dans la situation suivante : Soit L une extension quadratique totalement imaginaire d'un corps totalement réel K, 2-rationnel. Soient K' une extension quadratique totalement réelle de K. Nous supposons à présent que l'extension K'/K n'est pas ramifiée modérément, cela peut donc signifier deux choses :

- Soit K'/K n'est pas ramifiée,
- Soit K'/K est 2-ramifiée.

Autrement dit, K'/K est 2-ramifiée.

K étant 2-rationnel, on sait, d'après la définition 1.4.1, que la 2-extension galoisienne 2-ramifiée, ∞-décomposée maximale de K coïncide avec sa $\mathbb{Z}_2$-extension cyclotomique K^c. De ce fait, K' n'étant pas ramifiée modérément, elle est contenue dans K^c. De ce fait, les hypothèses du théorème 2.1.2 sont vérifiées, nous en déduisons donc que la 2-rationalité de K est équivalente à celle de K' et de même que la 2-birationalité de L est équivalente à celle de L' où $L' = LK'$.

Nous pouvons alors énoncer le résultat suivant :

Proposition 2.3.1 *Soit L une extension quadratique totalement imaginaire d'un corps totalement réel K. Soient K' une extension quadratique totalement réelle de K, non ramifiée modérément et soit $L' = LK'$ le compositum. Nous avons alors les équivalences :*

(i) L 2-birationnel $\Longleftrightarrow$ L' 2-birationnel.

(ii) K 2-rationnel $\Longleftrightarrow$ K' 2-rationnel.

Maintenant que nous avons étudié ce cas, nous pouvons énoncer un théorème général de propagation quadratique de la 2-birationalité.

Théorème général

En regroupant nos résultats, nous obtenons l'énoncé suivant :

Théorème 2.3.2 *Soit L une extension quadratique totalement imaginaire d'un corps totalement réel K. Soient K' une extension quadratique totalement réelle de K et $L' = LK'$ le compositum. Nous avons alors les résultats suivants :*

(i) Si K'/K n'est pas ramifiée modérément, nous avons alors les équivalences suivantes :

L 2-birationnel $\Longleftrightarrow$ L' 2-birationnel.

K 2-rationnel $\Longleftrightarrow$ K' 2-rationnel.

(ii) Sinon K'/K est ramifiée modérément et nous avons :

K'/K primitivement ramifiée en une place $\mathfrak{p}$ et L/K 2-birationnelle, modérément ramifiée en une place primitive $\mathfrak{q}$ en $\mathfrak{p}$ $\Leftrightarrow$ L'/K' est 2-birationnelle.

Le cas quadratique étant totalement résolu, nous pouvons à présent étudier le cas général.

Chapitre 3

Étude du cas général

Nous avons étudié dans le chapitre précédent la propagation de la 2-birationalité dans le cas d'une extension quadratique. Nous allons à présent essayer de généraliser ce résultat dans le cas d'une 2-extension quelconque. On se place donc dans la situation suivante :

Soit L une extension quadratique à conjugaison complexe d'un corps totalement réel K. Soient K' une 2-extension totalement réelle de K et $L' = LK'$ leur compositum.

Le but de ce chapitre est de relier la 2-birationalité de L/K à celle de L'/K'. Par analogie avec le chapitre précédent, nous allons traiter cette question en deux temps, mais en commençant cette fois par l'étude (plus facile) de la propagation. En résumé, nous donnons tout d'abord un théorème de montée ; puis nous énonçons une réciproque, à savoir un théorème de descente ; et enfin nous regroupons ces résultats.

Pour faciliter la lecture nous introduisons les dénominations suivantes :

Définition 3.0.3 *Nous appelons extension biramifiée (resp monoramifiée), une extension ramifiée modérément en* 2 *(resp en* 1*) place(s).*

Définition 3.0.4 *Rappelons qu'une extension modérément ramifiée est une extension ramifiée uniquement aux places modérées. Nous disons qu'une extension est ramifiée modérément lorsqu'elle est ramifiée en au moins une place modérée.*

Remarque 3.0.5 *Une extension modérément ramifiée n'est donc pas ramifiée modérément si elle est non ramifiée.*

Inversement, une extension ramifiée modérément n'est pas nécessairement modérément ramifiée (elle peut aussi être ramifiée aux places sauvages).

3.1 Extension 2-ramifiée

Comme dans le cas quadratique nous traitons à part le cas où l'extension K'/K est 2-ramifiée. Nous sommes donc dans la situation suivante : L est une extension quadratique totalement imaginaire d'un corps totalement réel K, 2-rationnel ; K' est une 2-extension totalement réelle de K. Nous supposons d'abord que l'extension K'/K est 2-ramifiée.

Le corps de nombres K étant 2-rationnel,on sait, d'après la définition 1.4.1 que la 2-extension galoisienne 2-ramifiée, ∞-décomposée maximale de K coïncide avec sa $\mathbb{Z}_2$-extension cyclotomique K^c. De ce fait, K' étant 2-ramifiée, elle est contenue dans K^c. Par suite, les hypothèses du théorème 2.1.2 sont vérifiées ; nous en déduisons donc que la 2-rationalité de K est équivalente à celle de K' et de même que la 2-birationalité de L est équivalente à celle de L' où $L' = LK'$.

Nous pouvons alors énoncer le résultat suivant :

Proposition 3.1.1 *Soit L une extension quadratique totalement imaginaire d'un corps totalement réel K. Soient K' une extension quadratique totalement réelle de K, non ramifiée modérément, et $L' = LK'$ le compositum. Nous avons alors les équivalences :*

(i) L est 2-birationnel $\Longleftrightarrow$ L' est 2-birationnel.

(ii) K est 2-rationnel $\Longleftrightarrow$ K' est 2-rationnel.

Le cas 2-ramifié étant ainsi résolu, nous supposons à présent que l'extension K'/K est ramifiée modérément.

Nous pouvons alors faire la réduction suivante : en vertu du théorème 2.1.2, on peut remplacer K par n'importe quel étage fini de la $\mathbb{Z}_2$-extension cyclotomique K^c. De ce fait, quitte à monter dans la $\mathbb{Z}_2$-extension cyclotomique, on peut supposer que K'/K et K^c/K sont linéairement disjointes.

Dans toute la suite, nous faisons donc l'hypothèse :

Hypothèse 3.1.2 *Les extensions K'/K et K^c/K sont prises linéairement disjointes. Cela entraîne en particulier que K'/K est ramifiée modérément en une (unique) place primitive $\mathfrak{p}$ et que celle-ci est totalement ramifiée dans K'/K.*

Remarque. L'unicité et la primitivité de la place modérée $\mathfrak{p}$ ramifiée dans K'/K résulte évidemment du théorème de propagation de la 2-rationalité pour les corps totalement réels.

3.2 Théorème de montée

Le but de cette section est de démontrer le théorème suivant :

Théorème 3.2.1 (Montée en ramification modérée) *Soit L une extension quadratique à conjugaison complexe d'un corps totalement réel K. Soient K' une 2-extension totalement réelle de K, avec K'/K et K^c/K linéairement disjointse et $L' = LK'$. On suppose de plus que K'/K est primitivement ramifiée en une place modérée $\mathfrak{p}$. Alors :*

La transition de la 2-birationnalité de L/K à L'/K' n'est possible que dans le cas où l'extension K'/K est quadratique.

Démonstration du théorème:

Pour démontrer ce résultat, nous allons essayer d'appliquer le théorème 1.4.6 à l'extension L'/K'. Avant cela, listons nos hypothèses et tirons en les premières conclusions.

L'extension L/K est 2-birationnelle ; on en déduit d'après le théorème 1.4.6 :

(i) L/K est 2-décomposée,

(ii) K est 2-rationnel,

(iii) L/K est modérément ramifiée en deux places $\mathfrak{q}$ et $\mathfrak{r}$ primitives, ou bien L/K est modérément ramifiée en une place $\mathfrak{q}$ semi-primitive.

L'assertion (i) entraîne la 2-décomposition de L'/K'. De plus, K'/K est par hypothèse primitivement ramifiée en une place $\mathfrak{p}$, ce qui, associé à (ii), nous donne grâce au théorème 1.3.13 que le corps K' est 2-rationnel.

Finalement, K' est 2-rationnel et L'/K' est 2-décomposée. Ainsi, pour appliquer le théorème 1.4.6, il ne reste plus qu'à regarder la ramification dans L'/K'. Or, la ramification dans L'/K' se déduit de celle de L/K ; nous avons donc deux cas à envisager : L/K est biramifiée modérément ou L/K est monoramifiée modérément.

Premier cas : L/K biramifiée modérément.

Nous supposons dans cette section que L/K est modérément ramifiée en deux places $\mathfrak{q}$ et $\mathfrak{r}$ primitives avec, par exemple, $\mathfrak{q} \neq \mathfrak{p}$. Nous commençons par chercher quelles sont les places ramifiées dans L'/K', puis nous regardons la nature de ces places. Il faut cependant distinguer les deux cas suivant : $\mathfrak{r} = \mathfrak{p}$ ou $\mathfrak{r} \neq \mathfrak{p}$.

a) Pour $\mathfrak{r} \neq \mathfrak{p}$

Dans ce paragraphe, on suppose $\mathfrak{r} \neq \mathfrak{p}$. Quel est alors le comportement des places $\mathfrak{q}$ et $\mathfrak{r}$ dans K'/K ?

- $\mathfrak{q}$ et $\mathfrak{r}$ ne peuvent se ramifier dans K'/K, car elles sont distinctes de $\mathfrak{p}$, seule place ramifiée dans K'/K,
- $\mathfrak{q}$ et $\mathfrak{r}$ ne peuvent non plus se décomposer dans K'/K, car dans ce cas il y aurait au moins trois places ramifiées dans L'/K', ce qui empêcherait cette extension d'être 2-birationnelle.

On conclut que les deux places $\mathfrak{q}$ et $\mathfrak{r}$ sont totalement inertes dans K'/K.

Sous ces hypothèses, pour que l'extension L'/K' soit 2-birationnelle ; il faut que ces deux places primitives dans K le restent dans K'. Regardons le comportement de ces places dans les extensions cyclotomiques. Soient K^c (resp K'^c) l'extension cyclotomique de K (resp de K'), K_1 (resp K'_1) le premier étage de l'extension cyclotomique K^c (resp de K'^c). Nous avons ainsi le schéma suivant :

$$\begin{tikzcd}[arrows=-]
K^c \arrow[r] \arrow[d] & K'^c \arrow[d] \\
K_1 \arrow[r] \arrow[d] & K'_1 \arrow[d] \\
K \arrow[r] & K'
\end{tikzcd}$$

Les places $\mathfrak{q}$ et $\mathfrak{r}$ étant primitives, elles sont inertes dans K_1/K et elles le sont aussi dans K'/K. Et comme les groupes d'inertie de ces places dans l'extension K'_1/K sont cycliques, il en résulte que les places au-dessus de $\mathfrak{q}$ et $\mathfrak{r}$ ne peuvent être inertes dans K'_1/K_1 : elles ne sont donc pas primitives dans K'. Ainsi, l'extension L'/K' n'est pas 2-birationnelle dans ce cas.

b) si $\mathfrak{r} = \mathfrak{p}$

Dans ce cas, que peut-on en déduire sur la ramification dans L'/K' ?

Nous avons supposé K'/K totalement ramifiée en la place $\mathfrak{p}$, mais pour voir que L'/K' ne peut alors se ramifier en $\mathfrak{p}$, il nous suffit de savoir que $\mathfrak{p}$ se ramifie dans K'/K. Pour voir cela, nous allons utiliser la théorie de Kummer. Nous rappelons que L/K est une extension quadratique de K, c'est-à-dire $L = K[\sqrt{\delta}]$, et que K'/K est une 2-extension linéairement disjointe de L/K. Ainsi, K'/K est une tour d'extensions quadratiques que nous pouvons noter de la manière suivante :

$$\begin{tikzcd}[arrows=-]
K_0 = K \arrow[r] & K_1 \arrow[r, dotted] & K_i \arrow[r, dotted] & K_n = K'
\end{tikzcd}$$

où chaque étage K_{i+1}/K_i est une extension quadratique totalement réelle.

La place $\mathfrak{p}$ étant ramifiée modérément dans K'/K, on en déduit qu'il existe une extension K_{i+1}/K_i quadratique dans laquelle la place $\mathfrak{p}$ est modérément ramifiée. On prend alors le plus petit indice i pour lequel cela se produit. On considère alors le schéma suivant :

$$\begin{tikzcd}[arrows=-]
L \arrow[r, dotted] \arrow[dd] & L_i = K_i[\sqrt{\delta_i}] \arrow[rr] \arrow[dd] & & L_{i+1} \arrow[r, dotted] \arrow[dd] \arrow[dl] & L' \arrow[dd] \\
& & L_i^* = K_i[\sqrt{d_i\delta_i}] \arrow[dl] & & \\
K \arrow[r, dotted] & K_i \arrow[rr] & & K_{i+1} = K_i[\sqrt{d_i}] \arrow[r, dotted] & K'
\end{tikzcd}$$

Dans ce schéma, on a $\mathfrak{p}$ modérément ramifiée dans L/K, mais elle ne l'est pas dans K_i/K. On en déduit que $\mathfrak{p}$ est modérément ramifiée dans L_i/K_i. Il vient alors :

- $\mathfrak{p}$ modérément ramifiée dans L_i/K_i, donc la valuation $v_\mathfrak{p}(\delta_i)$ est impaire,
- $\mathfrak{p}$ est modérément ramifiée dans K_{i+1}/K_i par hypothèse. Il vient donc $v_\mathfrak{p}(d_i)$ est impaire.

Sous ces conditions, la valuation $v_\mathfrak{p}(d_i\delta_i)$ est paire ; ainsi $\mathfrak{p}$ n'est pas modérément ramifiée dans L_i^*/K_i ; il vient que $\mathfrak{p}$ n'est pas ramifiée modérément dans L_{i+1}/K_{i+1} puis dans L'/K'.

Scolie 3.2.2 *Ce résultat est un cas particulier du lemme d'Abhyankar qui affirme que pour K un corps local, L et L' deux extensions finies de K telles que L/K est modérément ramifiée et l'indice de ramification $e = e(L/K)$ divise $e' = e(L'/K)$. Alors $L'L/L'$ est non ramifiée.(cf [12] corollaire 4 page 236)*

Ainsi, si on suppose que $\mathfrak{r}$ est égale à la place $\mathfrak{p}$, cette dernière n'est plus ramifiée dans L'/K'.

Il en résulte que seules les places au dessus de $\mathfrak{q}$ sont ramifiées dans L'/K'. Nous regardons à présent le comportement de $\mathfrak{q}$ dans K'/K. Il y a deux possibilités à envisager, $\mathfrak{q}$ peut être inerte ou décomposée dans K'/K, car elle est différente de $\mathfrak{p}$ donc non ramifiée.

Traitons ces deux cas séparément.

1) Si $\mathfrak{q}$ est inerte dans K'/K

Dans ce cas, la place au dessus de $\mathfrak{q}$ est la seule place modérément ramifiée dans L'/K', notons la $\mathfrak{q}'$. Quelle est alors sa nature ?

Pour cela nous nous plaçons dans le schéma galoisien suivant, où on introduit une chaîne d'extensions quadratiques totalement réelles : $K \subset K^{(1)} \subset K^{(2)} \subset \cdots \subset K'$. On note K_1 (resp K_1', resp $K_1^{(1)}$, resp $K_1^{(2)}$) le premier étage de l'extension cyclotomique K^c (resp de K'^c, resp $K^{(1)c}$, resp $K^{(2)c}$), puis K_2 (resp K_2', resp $K_2^{(1)}$, resp $K_2^{(2)}$) le deuxième étage de l'extension cyclotomique K^c (resp de K'^c, resp $K^{(1)c}$, resp $K^{(2)c}$). Ce qui nous donne :

$$\begin{tikzcd}[arrows=-]
K_2 \arrow[r] \arrow[d] & K_2^{(1)} \arrow[r] \arrow[d] & K_2^{(2)} \arrow[r] \arrow[d] & K_2' \arrow[d] \\
K_1 \arrow[r] \arrow[d] & K_1^{(1)} \arrow[r] \arrow[d] & K_1^{(2)} \arrow[r] \arrow[d] & K_1' \arrow[d] \\
K \arrow[r] & K^{(1)} \arrow[r] & K^{(2)} \arrow[r] & K'
\end{tikzcd}$$

Ici, la place $\mathfrak{q}$ primitive est inerte dans K_1/K et totalement inerte dans K'/K. Il suit, comme le groupe d'inertie de $\mathfrak{q}$ est cyclique, que la place au dessus de $\mathfrak{q}$ dans $K^{(1)}$, notée $\mathfrak{q}^{(1)}$ est décomposée dans $K_1^{(1)}/K^{(1)}$. Soient donc $\mathfrak{q}'^{(1)}$ et $\mathfrak{q}''^{(1)}$ les deux places au dessus de $\mathfrak{q}^{(1)}$ dans $K_1^{(1)}$.

Comme $\mathfrak{q}$ est inerte dans K_1/K_2, car primitive, on en déduit qu'elle est décomposée dans $K_1^{(1)}/K_1$. Finalement il vient que $\mathfrak{q}'^{(1)}$ et $\mathfrak{q}''^{(1)}$ sont inertes dans $K_2^{(1)}/K_1^{(1)}$. De ce fait, la place $\mathfrak{q}^{(1)}$ est semi-primitive dans $K^{(1)}$, en particulier en notant $L^{(1)} = LK^{(1)}$, on a que l'extension $L^{(1)}/K^{(1)}$ est 2-birationnelle.

Ensuite, en notant $\mathfrak{q}^{(2)}$ la place au-dessus de $\mathfrak{q}$ dans $K^{(2)}$, on sait d'après ce qui précède que $\mathfrak{q}^{(2)}$ est décomposée dans $K_1^{(2)}$. On note $\mathfrak{q}'^{(2)}$ et $\mathfrak{q}''^{(2)}$ les deux places au-dessus de $\mathfrak{q}^{(2)}$ dans $K_1^{(2)}$.

On rappelle que les deux places $\mathfrak{q}'^{(1)}$ et $\mathfrak{q}''^{(1)}$ sont inertes dans $K_2^{(1)}/K_1^{(1)}$, elles le sont aussi dans $K_1^{(2)}/K_1^{(1)}$. Finalement, il vient que les places $\mathfrak{q}'^{(2)}$ et $\mathfrak{q}''^{(2)}$ sont décomposées dans $K_2^{(2)}/K_1^{(2)}$.

Ainsi, la place $\mathfrak{q}^{(2)}$ n'est pas semi-primitive. Dans ce cas, sachant que la décomposition se propage, on a que la place $\mathfrak{q}'$ au dessus de $\mathfrak{q}$ dans K' est décomposée dans K'_1/K' et K'_2/K'_1, elle n'est donc pas semi-primitive et l'extension L'/K' n'est donc pas 2-birationnelle.

En conclusion, dans le cas ou la place $\mathfrak{q}$ est inerte la montée n'est possible que dans le cas quadratique. Traitons à présent, le cas où $\mathfrak{q}$ est décomposée dans K'/K.

2) Si $\mathfrak{q}$ est décomposée dans K'/K.

Dans ce cas, nous notons $\mathcal{D}_\mathfrak{q}$ le groupe de décomposition de $\mathfrak{q}$. Pour que L'/K' soit 2-birationnelle, il faut qu'elle soit ramifiée en au plus deux places, donc nécessairement $\mathcal{D}_\mathfrak{q}$ est d'indice 2 dans le groupe de Galois de K'/K. Nous notons alors, K_2 le sous-corps de K' fixé par $\mathcal{D}_\mathfrak{q}$, avec $[K_2 : K] = 2$ et $\mathfrak{q}_1$, $\mathfrak{q}_2$ les deux places au-dessus de $\mathfrak{q}$ dans K_2. Ceci nous donne la situation suivante :

$$\begin{array}{ccccc} L & — & L_2 & — & L' \\ | & & | & & | \\ K & — & K_2 & — & K' \end{array}$$

Nous allons commencer par essayer de monter la notion de 2-birationalité à L_2/K_2 ou $L_2 = LK_2$. Pour cela, nous appliquons le cas quadratique. Nous avons les hypothèses suivantes :

- L/K est 2-birationnelle ramifiée modérément en une place $\mathfrak{q}$ primitive et en $\mathfrak{p}$,
- on suppose K_2/K ramifiée modérément en $\mathfrak{p}$, car si ce n'est pas le cas, on ne pourrait pas monter la 2-birationalité à L_2/K_2. On verra plus tard que l'on ne perd pas de généralité,
- K_2/K est extension quadratique totalement réelle d'un corps totalement réel K,
- $\mathfrak{q}$ se décompose dans K_2/K.

Ainsi d'après le théorème 2.2.3, l'extension L_2/K_2 est 2-birationnelle, modérément ramifiée en $\mathfrak{q}_1$ et $\mathfrak{q}_2$ primitives, les deux places au-dessus de $\mathfrak{p}$ dans K_2.

Ainsi l'extension L_2/K_2 est 2-birationnelle.

Ce résultat étant établi peut-on continuer à monter à L'/K' ? On a la tour d'extension suivante :

$$\begin{array}{ccccc} L & — & L_2 & — & L' \\ | & & | & & | \\ K & — & K_2 & — & K' \end{array}$$

Nous voulons monter de L_2/K_2 à L'/K'.

Or, l'extension L_2/K_2 est ramifiée modérement en deux places primitives $\mathfrak{q}_1$ et $\mathfrak{q}_2$ différentes de la place $\mathfrak{p}$. Il s'agit du cas a) traité précédemment et nous avons vu que sous ces hypothèses la 2-birationalité ne se propage pas à L'/K'. Finalement, si l'extension K'/K n'est pas quadratique : nous ne pouvons pas monter.

Donc nous n'avons pas perdu de généralité en supposant K_2/K ramifiée en $\mathfrak{p}$, car pour monter il nous faut une extension quadratique c'est-à-dire $K_2 = K'$. Par suite, K_2/K est, dans le cas présent, ramifiée modérément en $\mathfrak{p}$.

De ce fait, le cas où l'extension L/K est biramifiée est entièrement traité. Nous passons alors au cas où L/K est monoramifiée.

Deuxième cas : L/K monoramifiée

Nous supposons dans ce paragraphe que L/K est modérément ramifiée en une place $\mathfrak{q}$ semi-primitive. Nous pouvons commencer par faire la remarque suivante : la place $\mathfrak{q}$ est différente de $\mathfrak{p}$ car $\mathfrak{p}$ est primitive dans K.

Ainsi, seules les places au-dessus de $\mathfrak{q}$ sont ramifiées modérément dans L'/K'. De plus, nous pouvons noter que comme la décomposition se propage, l'imprimitivité de $\mathfrak{q}$ engendre celle des places au-dessus de $\mathfrak{q}$. Ainsi, pour pouvoir monter $\mathfrak{q}$ doit être nécessairement totalement inerte dans K'/K.

Dans ce cas, on note $\mathfrak{q}'$, la place au dessus de $\mathfrak{q}$ dans K', il s'agit alors de la seule place ramifiée dans L'/K', quelle est donc sa nature ?

Nous regardons son comportement dans le schéma galoisien ci-dessus. Nous introduisons K'' le premier étage d'une chaîne d'extensions relativement quadratiques de K à K'. Puis, nous notons K_1 (resp K_1', resp K_1'') le premier étage de K^c (resp K'^c, resp K''^c), puis K_2 (resp K_2', resp K_2'') le second. Ce qui nous donne le schéma suivant :

$$\begin{tikzcd}[arrows=dash]
K_2 \arrow[r] \arrow[d] & K_2'' \arrow[r] \arrow[d] & K_2' \arrow[d] \\
K_1 \arrow[r] \arrow[d] & K_1'' \arrow[r] \arrow[d] & K_1' \arrow[d] \\
K \arrow[r] & K'' \arrow[r] & K'
\end{tikzcd}$$

Ici la place $\mathfrak{q}$ étant semi-primitive dans K, elle est décomposée dans K_1/K et inerte ensuite dans les autres étages de K^c/K, en particulier inerte dans K_2/K_1. De plus, $\mathfrak{q}$ est inerte dans K'/K ; on en déduit par cyclicité du groupe d'inertie que $\mathfrak{q}''$ la place au dessus de $\mathfrak{q}$ est décomposée dans K_1''/K_1. On note $\mathfrak{q}_1''$ et $\mathfrak{q}_2''$ les deux places au dessus de $\mathfrak{q}''$ dans K_1''.

En outre, $\mathfrak{q}$ est inerte dans K_2/K_1, elle l'est donc aussi dans K_1''/K_1. Comme son groupe d'inertie est cyclique, on en déduit que $\mathfrak{q}_1''$ et $\mathfrak{q}_2''$ sont décomposées dans K_2''/K_1'' .

Il en résulte que K_2''/K'' est complètement décomposée en $\mathfrak{q}''$ au dessus de $\mathfrak{q}$, on en déduit de même que K_2'/K' est complètement décomposée en $\mathfrak{q}'$ au dessus de $\mathfrak{q}$ et donc que L'/K' n'est pas 2-birationnelle.

Ceci achève la démonstration du théorème de montée.

3.3 Théorème de descente

Nous rappelons notre situation :

Soit L une extension quadratique à conjugaison complexe d'un corps totalement réel K. Soient K' une 2-extension totalement réelle de K, avec K'/K et K^c/K linéairement disjointe et $L' = LK'$. On suppose de plus que K'/K est primitivement ramifiée en une place $\mathfrak{p}$.

Nous venons de voir dans la section précédente que la propagation de la 2-birationalité de L/K à L'/K' n'a lieu que pour une extension quadratique. Or, si la 2-birationalité peut se descendre, elle peut forcément se monter. Le théorème 3.2.1 nous permet donc de nous ramener à l'étude de la descente dans le seul cas quadratique, question justement résolue au second chapitre de ce travail.

Ainsi, nous avons le théorème suivant :

Théorème 3.3.1 (Descente en ramification modérée) *Soit L une extension quadratique totalement imaginaire d'un corps totalement réel K. Soit K' une 2-extension totalement réelle de K, telle que K'/K et K^c/K soient linéairement disjointes ; et soit $L' = LK'$. On suppose de plus que K'/K est primitivement ramifiée en une place modérée $\mathfrak{p}$. Alors :*

La transition de la 2-birationnalité de L'/K' à L/K n'est possible que dans le cas où l'extension K'/K est quadratique.

3.4 Théorème général de propagation

En conclusion des trois sections précédentes, nous pouvons énoncer un théorème général de propagation de la 2-birationalité qui est le suivant :

Théorème 3.4.1 (Théorème général) *Soit L une extension quadratique à conjugaison complexe d'un corps totalement réel K, 2-décomposée. Soient K' une 2-extension totalement réelle de K et $L' = LK'$.*

(1) Si K'/K est 2-ramifiée, nous avons alors les équivalences suivantes :

(i) K' est 2-rationnel $\Longleftrightarrow$ K est 2-rationnel.

(ii) L' est 2-birationnel $\Longleftrightarrow$ L est 2-birationnel.

(2) Sinon K'/K est ramifiée modérément en (au moins) une place $\mathfrak{p}$ et dans ce cas nous avons alors l'équivalence suivante :

(i) K' est 2-rationnel $\Longleftrightarrow$ K est 2-rationnel, la place $\mathfrak{p}$ est primitive et est l'unique place modérée ramifiée dans K'/K.

(ii) De plus, lorsque ces conditions sont satisfaites, L' est 2-birationnel si et seulement si les deux conditions qui suivent sont réalisées :

(a) L est 2-birationnel et L/K est ramifiée modérément en exactement deux places : en la place $\mathfrak{p}$ et en une autre place primitive $\mathfrak{q}$;

(b) il existe un entier $n \in \mathbb{N}$ tel qu'on ait $K' = K_n K''$, avec K_n le n-ième étage de la $\mathbb{Z}_2$ extension cyclotomique K^c/K et $[K'' : K] = 2$.

Nous avons donc un théorème général de propagation de la 2-birationalité dans une 2-extension totalement réelle. Cependant, notre théorème nous dit que hormis le long de la tour cyclotomique, nous pouvons propager la 2-birationalité uniquement dans le cas quadratique, ceci est donc très restrictif.

Nous notons cependant une construction particulière de nos corps 2-birationnels, lorsque les extensions K'/K et K^c/K sont linéairement disjointes. En effet, nous les obtenons de la manière suivante :

(i) On se donne K_0 un corps 2-rationnel.

(ii) On se donne L_0/K_0 une extension quadratique, 2-birationnelle totalement imaginaire modérément ramifiée en deux primitives $\mathfrak{p}$ et $\mathfrak{q}$.

(iii) On construit alors K_1 une extension quadratique totalement réelle de K_0 dans laquelle une deux places modérément ramifiée dans L_0/K_0 est ramifiée (par exemple $\mathfrak{p}$), tandis que l'autre est décomposée.

(iv) Par le théorème 3.4.1, le corps $L_1 = L_0 K_1$ est 2-birationnel.

Ceci peut se résumer en le schéma suivant :

$$\begin{tikzcd} L_0 \arrow[r, dash] \arrow[d, dash, "{p\,,\,q \text{ ramifiés}}"'] & L_1 \arrow[d, dash, "{q_1\,,\,q_1' \text{ ramifiés}}"] \\ K_0 \arrow[r, dash, "{p \text{ ramifié, } q = q_1 q_1'}"'] & K_1 \end{tikzcd}$$

Cette construction atypique, soulève la question suivante : Peut-on continuer cette construction indéfiniment afin de construire une tour d'extensions 2-birationnelles dans le cas où K'/K et K^c/K sont linéairement disjointes ? Une réponse partielle a cette question est l'objet de la partie suivante.

3.5 Illustrations numériques

3.5.1 Extensions quadratiques

Dans le cas quadratique, nous avons vu que la 2-birationalité se propage, lorsque l'extension L/K est modérément ramifiée en deux places primitives $\mathfrak{p}$ et $\mathfrak{q}$ et avec K'/K modérément ramifiée en $\mathfrak{p}$. Dans, ce cas là la place $\mathfrak{q}$ peut faire ce qu'elle veut dans K'/K.

Cependant, nous remarquons que si nous voulons construire des extensions de degré supérieur, il faut que la place $\mathfrak{q}$ se décompose. En effet, si elle est inerte dans K'/K, alors l'extension L'/K' est monoramifié cas, pour lequel la propagation n'est plus possible.

Ici, nous donnons une liste de nombres premiers p et q, permettant d'obtenir des corps L et L' 2-birationnel. Nous regroupons ces résultats dans le tableau suivant :

p	q	Comportement de q dans K'/K
3	5	inerte
3	11	décomposée
3	13	décomposée
$\vdots$	$\vdots$	$\vdots$
5	3	inerte
5	11	décomposée
5	13	inerte
$\vdots$	$\vdots$	$\vdots$
29	11	inerte
29	13	décomposée
29	19	inerte
$\vdots$	$\vdots$	$\vdots$
83	3	inerte

Cette liste bien qu'étant non exhaustive nous montre que tout couple de premiers (p, q) primitifs permet de construire à partir d'un corps L 2-birationnel, un autre corps L' 2-birationnel. Nous cherchons à présent à aller plus loin.

Dans tout ce qui suit, nous faisons l'hypothèse suivante : les extensions K_i/K_0 et K_0^c/K_0 sont linéairement disjointes. Nous cherchons donc à construire une tour d'extensions 2-birationnelles à partir du schéma suivant :

$$\begin{tikzcd}
L_0 \arrow[r, dash] \arrow[d, dash, "{p\,,\, q \text{ ramifiés}}"'] & L_1 \arrow[d, dash, "{q_1\,,\, q_1' \text{ ramifiés}}"] \\
K_0 \arrow[r, dash, "{p \text{ ramifié, } q = q_1 q_1'}"'] & K_1
\end{tikzcd}$$

La construction se fait alors de la manière suivante :

- K_2/K_1 est une extension quadratique totalement réelle,
- la place $\mathfrak{q}_1$ se décompose dans K_2/K_1 en $\mathfrak{q}_1 = \mathfrak{q}_2\mathfrak{q}_2'$,
- la place $\mathfrak{q}_1'$ se ramifie dans K_2/K_1.

Ensuite de la même manière on construit K_3 avec :

- K_3/K_2 est une extension quadratique totalement réelle,
- la place $\mathfrak{q}_2$ se décompose dans K_3/K_2 en $\mathfrak{q}_2 = \mathfrak{q}_3\mathfrak{q}_3'$,
- la place $\mathfrak{q}_2'$ se ramifie dans K_2/K_1.

Et ainsi de suite le but est de savoir si on peut construire pour tout $n \in \mathbb{N}$, un corps K_n tel que

- K_n/K_{n-1} est une extension quadratique totalement réelle,
- la place $\mathfrak{q}_{n-1}$ se décompose dans K_n/K_{n-1} en $\mathfrak{q}_{n-1} = \mathfrak{q}_n\mathfrak{q}_n'$,
- la place $\mathfrak{q}_{n-1}'$ se ramifie dans K_n/K_{n-1}.

Nous commençons par chercher s'il existe des nombres premiers p et q permettant de construire K_2. Pour ce faire, nous allons utiliser le logiciel GP PARI qui nous a permis de faire des calculs rapides.

3.5.2 Extensions de degré 4

Dans un premier temps, nous cherchons un exemple de construction des corps L_0, K_0, K_1 et K_2 comme définis ci-dessus.

Pour nous faciliter la construction, nous partons $K_0 = \mathbb{Q}$ qui est 2-rationnel. Nous cherchons alors $L_0 = \mathbb{Q}[\sqrt{-pq}]$ telle que p et q soient primitives et $K_1 = \mathbb{Q}[\sqrt{p}]$ dans lequel q est décomposée. Nous souhaitons de plus que les idéaux au-dessus de q dans K_1 vérifie la chose suivante : un est décomposé et l'autre est ramifié dans K_2.

Grâce au logiciel PARI nous pouvons trouver de tels exemples. Pour cela, nous avons utilisé le programme suivant :

```
p=5;
K1=bnfinit (a2-p);
forprime (q=2,1000,
      if(q%8==3 && kronecker(p,q)==1,
      id=idealprimedec(K1, q);
      m=idealmul(K1,$4$,id[1]);
      bnr=bnrinit(K1,m,1);
      R=rnfkummer(bnr,Mat(2));
      P=rnfequation(K1,R);
      K2=nfinit(P);
      rid=idealprimedec(K2,q);
      if(#rid)==$3$,
      print(q,":",P,":",rid)
          )))
```

Ce programme nous donne, grâce à la théorie du corps de classes toutes les extensions quadratiques de $\mathbb{Q}[\sqrt{5}]$ pour lesquelles la décomposition de l'idéal q dans cette extension soit de longueur 3. De plus on remarque que cette décomposition est de la forme $(1^1, 1^2, 1^1)$ pour tous les nombres premiers q qui conviennent.

Pour $p = 5$ regroupons nos résultats obtenus dans le tableau suivant :

q	Polynôme
19	$x^4 - 9x^2 + 19$
59	$x^4 - 16x^2 + 59$
139	$x^4 - 24x^2 + 139$
179	$x^4 - 29x^2 + 179$
379	$x^4 - 39x^2 + 379$
419	$x^4 - 41x^2 + 419$
499	$x^4 - 49x^2 + 499$
619	$x^4 - 51x^2 + 619$
659	$x^4 - 56x^2 + 659$
739	$x^4 - 56x^2 + 739$
859	$x^4 - 59x^2 + 859$

Cependant, en faisant varier le conducteur dans le programme précédent, nous obtenons d'autres nombres premiers q convenables, par exemple $q = 11, 51, 91, ...$ Finalement pour $p = 5$, nous voyons que les nombres premiers q qui conviennent sont les nombres premiers congrus à 19 ou 11 modulo 40.

Ainsi, pour $p = 5$, si q convient, il vérifie les deux conditions suivantes :

- $q \equiv 3 \mod 8$, ce qui assure la primitivité ; et
- $q \equiv \pm 1 \mod 5$, pour que q soit un résidu quadratique mod 5.

Il vient donc $q \equiv 11$ ou $19 \mod 40$. Expérimentalement, nous trouvons que tous les nombres premiers de cette forme conviennent. Il est alors naturel de se demander si c'est réellement le cas, si la théorie confirme notre intuition.

Avant d'étudier ce point, nous complétons nos exemples en faisant varier p dans le programme précédent. Nous obtenons ainsi d'autres couples de premiers qui conviennent. Quelques exemples sont présentés dans le tableau ci-après :

p	q	Polynôme
13	43	$x^4 - 17x^2 + 43$
13	179	$x^4 - 27x^2 + 179$
13	251	$x^4 - 48x^2 + 251$
13	283	$x^4 - 40x^2 + 283$
$\vdots$	$\vdots$	$\vdots$
29	67	$x^4 - 23x^2 + 67$
29	179	$x^4 - 65x^2 + 179$
$\vdots$	$\vdots$	$\vdots$
37	3	$x^4 - 7x^2 + 3$
37	11	$x^4 - 9x^2 + 11$
37	67	$x^4 - 40x^2 + 67$
37	139	$x^4 - 112x^2 + 139$
$\vdots$	$\vdots$	$\vdots$
53	11	$x^4 - 16x^2 + 11$
53	43	$x^4 - 15x^2 + 43$
53	59	$x^4 - 17x^2 + 59$
53	131	$x^4 - 43x^2 + 131$
53	163	$x^4 - 57x^2 + 163$
53	211	$x^4 - 99x^2 + 211$
$\vdots$	$\vdots$	$\vdots$
157	3	$x^4 - 13x^2 + 3$
173	67	$x^4 - 21x^2 + 67$
173	163	$x^4 - 47x^2 + 163$
173	211	$x^4 - 49x^2 + 211$
173	227	$x^4 - 40x^2 + 227$
173	251	$x^4 - 73x^2 + 251$
$\vdots$	$\vdots$	$\vdots$
197	107	$x^4 - 25x^2 + 107$
197	163	$x^4 - 88x^2 + 163$
229	11	$x^4 - 25x^2 + 99$
$\vdots$	$\vdots$	$\vdots$
269	11	$x^4 - 115x^2 + 11$
269	43	$x^4 - 21x^2 + 43$
269	211	$x^4 - 87x^2 + 211$
$\vdots$	$\vdots$	$\vdots$

A la lumière de ces exemples, nous voyons qu'il n'y a a priori pas de restriction sur les nombres premiers p et q, dès lors qu'ils sont primitifs et que q est résidu quadratique mod p. Une approche théorique de la question fait l'objet de l'appendice suivante.

Chapitre 4

Tours d'extensions 2-birationnelles

Les résultats expérimentaux précédents nous incitent à étudier l'existence de tours d'extensions 2-birationnelles qui semble être possible dès lors qu'ils sont primitifs et que q est résidu quadratique mod p

Nous commençons par faire la remarque suivante :

Remarque 4.0.1 *Grâce au théorème 3.4.1, nous voyons que la question de la propagation de la 2-birationalité se ramène à construire, pour une extension 2-birationnelle L/K donnée, ramifiée modérément en exactement deux places primitives $\mathfrak{p}$ et $\mathfrak{q}$, une extension quadratique totalement réelle K' de K décomposée en $\mathfrak{q}$ et ramifiée modérément en $\mathfrak{p}$ seulement.*

En vertu de la théorie 2-adique du corps de classes, une telle extension existe si et seulement si le 2-groupe des $\infty\mathfrak{q}$-classes $2\mathfrak{p}$-infinitésimales est non trivial.

Regardons si c'est toujours le cas. Rappelons pour cela le contexte de notre étude :

1. K est un corps de nombres totalement réel et 2-rationnel ; ce qui peut se traduire par les deux propriétés suivantes :
   (a) le corps K possède une seule place dyadique $\mathfrak{l}$; d'où : $[K_{\mathfrak{l}} : \mathbb{Q}_2] = [K : \mathbb{Q}] = r$;
   (b) la 2-extension abélienne 2-ramifiée ∞-décomposée maximale de K est sa $\mathbb{Z}_2$-extension cyclotomique ; cela entraîne que le groupe d'idèles qui définit l'extension cyclotomique est donnée par la formule suivante :
$$\widetilde{\mathcal{J}_K} = \prod_{\mathfrak{r} \neq \mathfrak{l}} \mu_{\mathfrak{r}} \mathcal{R}_K$$
2. L est une extension quadratique de K totalement imaginaire et ramifiée modérément en deux places $\mathfrak{p}$ et $\mathfrak{q}$ qui sont primitives. En termes idéliques, cette primitivité s'écrit :
$$\mathcal{J}_K = \widetilde{\mathcal{J}_K} \mathcal{R}_{\mathfrak{p}} = \widetilde{\mathcal{J}_K} \mathcal{R}_{\mathfrak{q}}$$

Cela étant, nous cherchons une extension quadratique K'/K satisfaisant les quatre propriétés suivantes :

(i) elle est ramifiée modérément en $\mathfrak{p}$ seulement,

(ii) elle est décomposée en $\mathfrak{q}$,

(iii) elle est non décomposée en 2,

(iv) elle est complètement décomposée à l'infini.

Pour l'instant, considérons la 2-extension abélienne maximale N de K qui est totalement réelle, $\mathfrak{p}$-modérément ramifiée et $\mathfrak{q}$-décomposée. Le sous-groupe d'idèles qui lui correspond est ainsi :

$$\prod_{\mathfrak{r}|\infty} \mu_{\mathfrak{r}} (\prod_{\mathfrak{r}\neq\mathfrak{p},\, \mathfrak{r}\nmid\mathfrak{l}\infty} \mu_{\mathfrak{r}}) \mathcal{R}_{\mathfrak{q}} \mathcal{R}_K$$

Et il vient donc :

$$Gal(N/K) = \mathcal{J}_K / \prod_{\mathfrak{r}\nmid\mathfrak{p}\mathfrak{l}} \mu_{\mathfrak{r}} \mathcal{R}_{\mathfrak{q}} \mathcal{R}_K \simeq \mu_{\mathfrak{p}} / \mu_{\mathfrak{p}} \cap (\prod_{\mathfrak{r}\nmid\mathfrak{p}\mathfrak{l}} \mu_{\mathfrak{r}} \mathcal{R}_{\mathfrak{q}} \mathcal{R}_K),$$

en vertu des égalités rappelées plus haut :

$$\mathcal{J}_K = \widetilde{\mathcal{J}_K} \mathcal{R}_{\mathfrak{q}} \qquad \text{et} \qquad \widetilde{\mathcal{J}_K} = \prod_{\mathfrak{r}\neq\mathfrak{l}} \mu_{\mathfrak{r}} \mathcal{R}_K.$$

Dans le quotient obtenu, les idèles principaux (i.e. les éléments de $\mathcal{R}_K$) qui apparaissent au dénominateur sont dans $\prod_{\mathfrak{r}\neq\mathfrak{l}} \mu_{\mathfrak{r}}$: ce sont des $\mathfrak{q}$-unités infinitésimales. Or, nous avons ici :

Lemme 4.0.2 *Dans un corps de nombres totalement réel qui est 2-rationnel, pour toute place modérée* $\mathfrak{q}$ *de* K *le pro-2-groupe* $\mathcal{E}^{\mathfrak{q}}_{\infty}$ *des* $\mathfrak{q}$*-unités infinitésimales est trivial.*

Il s'agit de vérifier que l'image locale $s_{\mathfrak{l}}(\mathcal{E}^{\mathfrak{q}})$ du 2-adifié $\mathcal{E}^{\mathfrak{q}} = \mathbb{Z}_2 \otimes_{\mathbb{Z}} E^{\mathfrak{q}}$ du groupe des $\mathfrak{q}$-unités de K est encore un $\mathbb{Z}_2$-module de rang r. Pour voir cela, observons que K, puisqu'il est présumé 2-rationnel, vérifie la conjecture de Leopoldt ; autrement dit que le 2-adifié groupe des unités $\mathcal{E} = \mathbb{Z}_2 \otimes_{\mathbb{Z}} E$ s'injecte dans le groupe des unités locales $\mathcal{U}_{\mathfrak{l}}$ attaché à l'unique place dyadique $\mathfrak{l}$ de K. En particulier $\mathcal{E}$, qui est de rang $r-1 = [K:\mathbb{Q}]-1$, s'envoie avec un indice fini dans la préimage $\mathcal{U}^*_{\mathfrak{l}}$ dans $\mathcal{U}_{\mathfrak{l}}$ du groupe $\mu_2 = \{\pm 1\}$ des racines de l'unité pour la norme arithmétique $\nu = N_{K/\mathbb{Q}}$. Soit alors x l'image canonique dans $\mathcal{E}^{\mathfrak{q}}$ d'un générateur arbitraire d'une puissance principale de l'idéal $\mathfrak{q}$. La norme x^{ν} est (au signe près) une puissance non triviale de $N\mathfrak{q}$, et son logarithme 2-adique n'est donc pas nul. De sorte que le $\mathbb{Z}_2$-module $s_{\mathfrak{l}}(\mathcal{E}^{\mathfrak{q}})$, qui contient $s_{\mathfrak{l}}(\mathcal{E})$ et $s_{\mathfrak{l}}(x)$, est de rang au moins $(r-1)+1 = r$; et finalement de rang exactement r, tout comme $\mathcal{U}_{\mathfrak{l}}$.

En d'autres termes, le sous-module $\mathcal{E}^{\mathfrak{q}}_{\infty}$ des $\mathfrak{q}$-unités infinitésimales est bien trivial.

Ce point acquis, nous avons obtenu :

Proposition 4.0.3 *Pour toute place primitive* $\mathfrak{q}$ *d'un corps de nombres 2-rationnel totalement réel* K*, la 2-extension abélienne maximale* N *de* K *qui est totalement réelle,* $\mathfrak{q}$*-décomposée et ramifiée modérément en une unique place* $\mathfrak{p} \neq \mathfrak{q}$*, est cyclique, de groupe de Galois :*

$$Gal(N/K) \simeq \mu_{\mathfrak{p}}.$$

En particulier, N/K *contient une unique sous-extension quadratique* K'/K*.*

Il suit de là que, sous les hypothèses de la proposition, l'unique sous-extension quadratique K'/K de N/K est l'unique extension quadratique qui satisfait aux conditions (i), (ii) et (iv) listées plus haut. Reste à voir si elle vérifie également la condition (iii) qui postule l'existence d'une unique place dyadique dans K'. Or c'est là qu'intervient précisément la condition de primitivité de la place $\mathfrak{p}$, que nous n'avons pas utilisée jusqu'ici : les résultats sur la propagation de la 2-rationalité rappelés dans le chapitre 1 assurent que K' est encore 2-rationnel si et seulement si la place $\mathfrak{p}$ est primitive dans K. Lorsque c'est le cas, K' ne peut alors contenir qu'une seule place dyadique (cf. Th. 1.3.8) ; et la condition (iii) est, de ce fait, automatiquement vérifiée.

L'ensemble de cette discussion peut donc se résumer comme suit :

Théorème 4.0.4 *Soient K un corps 2-rationnel totalement réel et L une extension quadratique 2-birationnelle totalement imaginaire de K ramifiée modérément en deux places primitives $\mathfrak{p}$ et $\mathfrak{q}$. Il existe alors exactement deux extensions quadratiques K'/K totalement réelles, 2-rationnelles et ramifiées modérément, telles que l'extension composée $L' = LK'$ soit 2-birationnelle : celle qui est ramifiée modérément en $\mathfrak{p}$ et décomposée en $\mathfrak{q}$; et celle qui est ramifiée modérément en $\mathfrak{q}$ et décomposée en $\mathfrak{p}$.*

Comme vu plus avant, l'extension L'/K' vérifie à son tour les mêmes hypothèses que l'extension de départ. Itérant le théorème, on obtient ainsi :

Scolie 4.0.5 *Sous les hypothèses du théorème, il existe une infinité de tours infinies d'extensions relativement quadratiques $K \subset K_1 \subset K_2 \subset \cdots \subset K_i \subset \cdots$ de corps 2-rationnels totalement réels telles que les extensions composées $L_i = LK_i$ pour $i \in \mathbb{N}$ soient 2-birationnelles.*

Il convient, en effet, à chaque étage $i \in \mathbb{N}$ déjà construit, de choisir celle des deux places primitives du corps K_i ramifiées dans L_i/K_i qu'on autorise à se ramifier modérément dans l'extension quadratique K_{i+1}/K_i.

Remarque 4.0.6 *Il peut être instructif de relire les résultats ci-dessus à la lumière des identités du miroir qui fournissent une seconde preuve du théorème.*

Reprenons pour cela les calculs effectués au début de ce chapitre : l'isomorphisme donné par le corps de classses

$$Gal(N/K) \simeq \mu_{\mathfrak{p}}/\mu_{\mathfrak{p}} \cap (\prod_{\mathfrak{r} \nmid \mathfrak{p}\mathfrak{l}} \mu_{\mathfrak{r}} \mathcal{R}_{\mathfrak{q}} \mathcal{R}_K),$$

nous assure que l'extension N/K est cyclique (éventuellement triviale). Posons $S = \{\mathfrak{q}\infty\}$ et $T = \{\mathfrak{l}\mathfrak{p}\}$. Par construction, le groupe de Galois $Gal(N/K)$ s'identifie alors au ℓ-groupe des S-classes T-infinitésimales $\mathcal{C}\ell_T^S$; et le résultat précédent se lit tout simplement :

$$rg_2 \, \mathcal{C}\ell_T^S \leq 1.$$

Nous allons à présent minorer ce rang grâce à la formule de réflexion de Gras (cf théorème 4.6 page 45 de [1]).

Reprenant les notations de Gras, nous avons : $S = \{\mathfrak{q}\infty\}$, $T = \{\mathfrak{l}\mathfrak{p}\}$, $S_0 = \{\mathfrak{q}\}$, $T_2 = \{\mathfrak{l}\}$, $S_2 = \emptyset$ et $\Delta_\infty = \emptyset$; donc :

$$rg_2\,\mathcal{C}\ell_T^S \;-\; rg_2\,\mathcal{C}\ell_{\{\mathfrak{q}\}}^{\{\mathfrak{l}\mathfrak{p}\}} = |T| + [K_\mathfrak{l} : \mathbb{Q}_2] - r - |S_0| - |\Delta_\infty| = 2 + r - r - 1 - 0 = 1$$

De cette formule, il suit en particulier :

$$rg_2\,\mathcal{C}\ell_T^S \geq 1;$$

de sorte qu'en fin de compte nous avons simultanément :

$$rg_2\,\mathcal{C}\ell_T^S = 1 \qquad \text{et} \qquad \mathcal{C}\ell_{\{\mathfrak{q}\}}^{\{\mathfrak{l}\mathfrak{p}\}} = 1.$$

Le groupe $\mathcal{C}\ell_T^S$ est donc cyclique mais non trivial (comme nous l'avons déjà établi à l'aide du lemme d'indépendance 4.0.2 plus haut), tandis que le ℓ-groupe $\mathcal{C}\ell_{\{\mathfrak{q}\}}^{\{\mathfrak{l}\mathfrak{p}\}}$ des $\{\mathfrak{l}\mathfrak{p}\}$-classes $\{\mathfrak{q}\}$-infinitésimales, lui, est nécessairement trivial.

De l'identité $rg_2\,\mathcal{C}\ell_T^S = 1$, on conclut qu'il existe une unique extension quadratique K'/K qui est non-ramifiée modérément en dehors de $\mathfrak{p}$ et $\infty\mathfrak{q}$-décomposée. Il reste alors à vérifier que cette extension est effectivement ramifiée en $\mathfrak{p}$ et qu'elle est non décomposée en 2, pour qu'elle réalise la propagation de la 2-birationalité.

- Le premier point est évident, puisque le groupe de Galois $Gal(N/K)$ est engendré par l'image du sous-groupe d'inertie de la place $\mathfrak{p}$.
- Il reste à voir que la place dyadique $\mathfrak{l}$ est non décomposée. Pour cela, reprenons le raisonnement précédent en échangeant les rôles de $\mathfrak{p}$ et de $\mathfrak{q}$. Ce faisant, nous obtenons : $rg_2\,\mathcal{C}\ell_{\{\mathfrak{p}\}}^{\{\mathfrak{l}\mathfrak{q}\}} = 0$, i.e. $\mathcal{C}\ell_{\{\mathfrak{q}\}}^{\{\mathfrak{l}\mathfrak{p}\}} = 1$; ce qui est précisément le résultat attendu.

En conclusion, nous retrouvons le fait que pour un couple de places $\mathfrak{p}$ et $\mathfrak{q}$ primitives fixé, il existe une unique extension K'/K vérifiant les hypothèses du théorème 3.4.1 et permettant la propagation de la 2-birationalité.

De ce fait, ce processus peut être réitéré à l'infini et ainsi nous pouvons construire des extensions K' de K de degrés arbitrairement grands de telle manière que le corps L' de notre théorème soit encore 2-birationnel.

Conclusion

Dans ce travail, nous avons étudié la propagation de la 2-birationalité dans des 2-extensions totalement réelles. Cette question a été complètement résolue et la réponse fait l'objet du théorème 3.4.1. De ce résultat, nous tirons la constatation suivante : si l'on enlève la tour cyclotomique, on ne peut propager la 2-birationalité par 2-extension totalement réelle que dans le seul cas quadratique. En revanche, nous dégageons une construction atypique pour obtenir une tour d'extensions qui à chaque étage est 2-birationnelle. Il faut noter cependant que la tour ainsi obtenue n'est pas galoisienne.

Dans la fin du chapitre 3, nous donnons des exemples numériques de cette construction pour des extensions de degré 2 et 4. Ces résultats expérimentaux incitent à penser que la construction de tours d'extensions 2-birationnelles est possible dans un cadre général.

Il apparait que, la propagation de la 2-birationnalité se ramène à construire, pour une extension 2-birationnelle L/K donnée, ramifiée modérément en exactement deux places primitives $\mathfrak{p}$ et $\mathfrak{q}$, une extension quadratique totalement réelle K' de K décomposée en $\mathfrak{q}$ et ramifiée modérément en $\mathfrak{p}$ seulement. Cette question est entièrement résolue dans le chapitre 4, en effet grâce la théorie du corps de classes nous retrouvons le fait que pour un couple de places $\mathfrak{p}$ et $\mathfrak{q}$ primitives fixé, il existe une unique extension K'/K vérifiant les hypothèses du théorème 3.4.1 et permettant la propagation de la 2-birationalité.

Bibliographie

[1] G. GRAS. *Class Field Theory From Theory To Practice.* Springer-Verlag, 2003.

[2] G. GRAS & J.-F. JAULENT. Sur les corps de nombres réguliers. *Math. Z.*, 202 : 343–365, 1989.

[3] J.-F. JAULENT. Introduction au K_2 des corps de nombres. *Pub. Math. Fac. Sci. Besançon, Théor. Nombres*, 1983.

[4] J.-F. JAULENT. Classes logarithmiques des corps de nombres. *J. Théor. Nombres Bordeaux*, 6 : 301–325, 1994.

[5] J.-F. JAULENT. Classes logarithmiques des corps de nombres. *J. Théor. Nombres. Bordeaux*, 6 : 301–325, 1995.

[6] J.-F. JAULENT. Théorie ℓ-adique du corps de classes. *J. Théor. Nombres. Bordeaux*, 10 : 355–397, 1999.

[7] J.-F. JAULENT & T. NGUYEN QUANG DO. Corps p-rationnels, corps p-réguliers et ramification restreinte. *J. Théor. Nombres. Bordeaux*, 5 : 343–365, 1993.

[8] J.-F. JAULENT & O. SAUZET. Extensions quadratiques 2-birationnelles de corps totalement réels. *J. Number. Th.*, 65 : 240–267, 1997.

[9] J.-F. JAULENT & O. SAUZET. Pro-ℓ-extension de corps l-rationnels. *J. Numb. Th.*, 65 et 80 : 240–267 et 318–319, 1997 et 2000.

[10] A. MOVAHHEDI. Sur les p-extensions des corps p-rationnels. *Math. Nachr.*, 149 : 163–176, 1990.

[11] A. MOVAHHEDI & T. NGUYEN QUANG DO. Sur l'arithmétique des corps de nombres p-rationnels. *Sém. Th. Nombres Paris (1987/1988), Prog. in Math.*, 89 : 155–200, 1990.

[12] W. NARKIEWICZ. *Elementary and Analytic Theory of Algebraic Numbers.* Springer-Verlag, second edition, 1990.

Propagation de la 2-birationalité

Résumé : L'objet de cette thèse est l'étude de la propagation de la 2-birationalité pour les 2-extensions de corps de nombres. Le problème étudié se présente comme suit : étant donnés un corps 2-rationnel totalement réel K, une extension quadratique totalement imaginaire L de K, et une 2-extension totalement réelle de K' de K, à quelles conditions la 2-birationalité du compositum $L' = KL$ se lit-elle sur L ?

La thèse se structure en trois parties : l'étude du cas absolument quadratique d'abord, le cas relativement quadratique ensuite ; le cas général enfin. Le résultat principal de la thèse résout complètement le problème posé en toute généralité. En fin de thèse, diverses illustrations numériques sont proposées à l'aide du PARI, ainsi qu'une étude des tours d'extensions 2-birationnelles.

Mots Clés : 2-birationalité, 2-rationalité, corps p-rationnel, ramification modérée, place primitive, place semi-primitive, tour d'extensions.

Abstract : This thesis deals with the propagation of 2-birationality for 2-extensions of numbers fields. More precisely, le t K be a 2-rational totally real number field, L a CM quadratic extension of K, and let K' be a totally real 2-extension of K. Under which conditions can one read the 2-birationaltiy of the compositum $L' = LK'$ from L ?

This work is divided into three parts : we first study the absolute quadratic case, then the relatively quadratic case, then finally the general case. The thesis's main result solves the whole problem. We also illustrate the result with various numeric examples, obtained with PARI and a focus at the end on 2-birational extensions' towers.

Keywords : 2-birationality, 2-rationality, p-rational number field, tame ramification, primitive place, semi primitive place, extensions tower.