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

Laboratoire d'**A**rithmétique, de **C**alcul formel et d'**O**ptimisation

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Mathématiques

présentée et soutenue

par

Mikaël LESCOP

le 23 septembre 2003

Sur les 2-extensions de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale

Jury

Président :	Jean-François JAULENT
	Professeur à l'université de Bordeaux 1
Rapporteurs :	Manfred KOLSTER
	Professeur à McMaster University (Hamilton, Canada)
	Florence SORIANO-GAFIUK
	Maître de conférences HDR à l'université de Metz
Examinateurs :	François LAUBIE
	Professeur à l'université de Limoges
	Alain SALINIER
	Maître de conférences HDR à l'université de Limoges
Directeur de thèse :	Abbas MOVAHHEDI
	Professeur à l'université de Limoges

Remerciements

Je voudrais avant tout exprimer toute ma gratitude à mon directeur de thèse Abbas Movahhedi pour la confiance qu'il m'a accordée, ainsi que pour ses conseils et ses idées qui ont grandement contribué à l'élaboration et l'amélioration de cette thèse.

Je tiens à remercier Manfred Kolster pour l'intérêt qu'il a manifesté à l'égard de mon travail, pour son enthousiasme communicatif, pour ses encouragements et pour ses nombreuses suggestions qui ont été une grande source d'inspiration.

Je remercie Florence Soriano-Gafiuk pour avoir accepté d'être rapporteur de cette thèse. Je lui suis aussi reconnaissant de m'avoir donné la chance d'exposer une partie des travaux effectués pendant cette thèse lors du colloque de Metz en juin 2002.

Mes remerciements vont aussi vers Jean-François Jaulent, François Laubie et Alain Salinier qui me font l'honneur de participer à mon jury de thèse.

Je tiens également à saluer les membres du LACO ainsi que les doctorants qui m'ont soutenu et qui, d'une façon ou d'une autre, ont contribué à l'animation de mon quotidien au laboratoire. Je remercie tout particulièrement Martine Guerletin, Nadine Tchéfranoff et Yolande Vieceli pour leur gentillesse et leur disponibilité, Anne Bellido pour avoir été ma tutrice pédagogique pendant mes trois années de monitorat, Mériem Héraoua et Jilali Assim pour leur sympathie et leurs encouragements. Je suis très reconnaissant envers Thomas Cluzeau et Matthieu Le Floc'h pour leurs commentaires, critiques et suggestions concernant la rédaction de mes travaux, pour leurs conseils en informatique et pour l'ambiance formidable qui a régné dans notre bureau pendant ces trois années. Mention spéciale à Matthieu sans qui ma vie à Limoges – et à travers elle, mes activités de recherche, d'enseignement, de course à pied et de détente – aurait été relativement bien monotone.

Je profite de l'occasion qui m'est donnée ici pour remercier l'université de McMaster et en particulier Manfred Kolster pour leur hospitalité lors de mon séjour effectué de septembre à décembre 2001 à Hamilton, au Canada. Un grand merci aussi à Kee Ip, Robert Osburn et Ion Rada pour leur accueil chaleureux et leur constante attention.

Je remercie du fond du cœur mes parents, Marie-Josèphe et Raymond

Lescop, ainsi que Erwan, Magalie et Chloé pour leur inestimable affection et leur immense soutien. Je n'oublie pas les familles Menguy de Pen Ar C'Hoat et Lescop de Prat-Paul qui n'ont jamais cessé de m'encourager et de s'intéresser à mon parcours.

Table des matières

Introduction

Nous nous intéressons ici à des questions relatives au noyau sauvage entrant dans le cadre plus général de l'étude du K_2 des corps de nombres. Dans une première partie de l'exposé, nous nous sommes attachés à définir les notions nécessaires à cette étude et à décrire les principaux théorèmes déjà connus. La description cohomologique du K_2 des corps globaux, qui est l'œuvre de J. Tate ([T]), est l'un des premiers résultats significatifs sur le sujet et il nous a semblé intéressant de le rappeler. D'autre part, l'identification du K_2 à un groupe d'homologie via la théorie des extensions centrales de groupes linéaires intervient fondamentalement dans la définition du morphisme de transfert d'une extension de corps de nombres, définition que l'on a reprise puisque cette application jouera un rôle important dans la suite. Quant aux symboles, ils sont incontournables puisque les définitions même du noyau sauvage, du noyau modéré ainsi que du noyau modéré positif reposent sur les symboles de Hilbert et modérés.

Concernant le noyau sauvage, de nombreux auteurs ont contribué à une meilleure connaissance du sujet en développant des méthodes bien différentes. En considérant l'analyse harmonique sur des espaces symétriques, H. Garland a prouvé ([Ga]) la finitude du noyau modéré, donc celle du noyau sauvage. De même, des résultats ont été trouvés en exploitant les liens entre les noyaux sauvage et modéré ([Br], [Gr1]) ; par exemple, la conjecture de Birch-Tate liant le noyau modéré à la fonction zêta de Dedekind (voir la remarque page 86 pour un énoncé complet) permet d'obtenir avec la suite exacte de Moore des informations sur le cardinal du noyau sauvage de certains corps de nombres. D'autre part, depuis l'origine, de nombreux calculs explicites ont été menés pour obtenir diverses propriétés qui concernent certains corps de nombres, et essentiellement les corps quadratiques ([BG]). Une autre technique consiste à exhiber explicitement des éléments non triviaux du noyau sauvage ; cette étude repose en partie sur la caractérisation de ces éléments en termes de symboles ([Mu], [Hut], [Ke]). Cependant, de façon générale, on connaît assez mal le noyau sauvage. On sait qu'il est trivial pour le corps $\mathbb{Q}$

des rationnels, ainsi que pour certains corps quadratiques imaginaires ([BT]). Néanmoins, lorsqu'on s'intéresse à la p-partie du noyau sauvage, on connaît des résultats plus précis. Sa structure a notamment fait l'objet de travaux reposant sur les classes logarithmiques ([Gr1], [J2], [Sor], [JS1]). On connaît aussi une formule de genre, analogue à celle des groupes de classes, pour les p-parties des noyaux sauvages d'une extension de corps de nombres de degré premier p ([KM1], [KM2], voir aussi sur ce thème [Ry]), sur laquelle on aura l'occasion de revenir. Signalons à ce propos qu'il existe une généralisation des noyaux sauvages en K-théorie supérieure (voir [Ng]) ; la formule de genre évoquée précédemment est également satisfaite pour ces noyaux sauvages supérieurs ([KM1]). Enfin, la théorie d'Iwasawa est aussi un outil intéressant pour l'étude des noyaux sauvages ([Kol]).

Lorsque p est un nombre premier impair, les p-extensions de $\mathbb{Q}$ pour lesquelles la p-partie du noyau sauvage est triviale s'obtiennent à l'aide de la formule de genre établie par M. Kolster et A. Movahhedi ([KM1]) pour les p-parties des noyaux sauvages d'une extension de corps de nombres de degré premier p. Le cas $p = 2$ s'avère être beaucoup plus difficile. J. Browkin et A. Schinzel ont apporté la première pierre à l'édifice en déterminant le 2-rang du noyau sauvage des corps quadratiques ([BS]). Plus récemment, en étudiant le morphisme de transfert entre noyaux sauvages, M. Kolster et A. Movahhedi ont établi ([KM2]) une autre formule de genre pour les 2-parties des noyaux sauvages, ce qui leur a permis de déterminer les extensions bi-quadratiques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. Enfin, R. Griffiths a traité le cas des extensions multi-quadratiques ([Gri]) en s'appuyant encore sur la formule de genre.

Par voie de conséquence, le but de cette thèse a été progressivement de chercher à déterminer les extensions cycliques de degré 4, les 2-extensions cycliques et les 2-extensions abéliennes de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. Les résultats que l'on a obtenus reposent principalement sur une amélioration que nous proposons de la formule de genre susmentionnée, en ce sens qu'on lève l'indécision sur la valeur d'un exposant intervenant dans la formule initiale. En particulier, on calcule explicitement la valeur de cet exposant dans le cas des corps quadratiques, ce qui nous permet de retrouver les résultats de J. Browkin et A. Schinzel sur le 2-rang du noyau sauvage. Nous constatons aussi pour cela que la formule de genre donne le 2-rang du noyau sauvage sous certaines conditions. Ensuite, nous traitons le cas des extensions cycliques et comparons nos résultats à ceux obtenus par G. Gras sur le problème analogue portant non plus sur le noyau sauvage mais sur le noyau modéré positif (cf [Gr1]). Notons que même si nos résultats et ceux de G. Gras se recoupent en certains points, ils sont toutefois obtenus par des techniques différentes reposant, dans notre cas, principalement sur la formule de genre pour les noyaux sauvages et, dans l'autre, sur les classes logarithmiques. Enfin, nous traitons le cas des 2-extensions abéliennes totalement réelles de $\mathbb{Q}$, regroupons les résultats de [Gr1], [KM2] et [Gri] afin d'avoir un récapitulatif des travaux réalisés sur cette question, puis décrivons quelques situations précises pour expliquer pourquoi le cas général des 2-extensions abéliennes de $\mathbb{Q}$ paraît plus difficile à résoudre.

À présent, nous détaillons le plan de la thèse :

Chapitre 1 : $\boldsymbol{K}$-groupes et $\boldsymbol{K_2}$ des corps de nombres

Ce chapitre consiste en quelques rappels sur la K-théorie de Milnor et, plus particulièrement, sur le K_2 des corps de nombres. On définit notamment le noyau sauvage $WK_2(F)$, le noyau modéré $K_2(o_F)$ et le noyau modéré positif $K_2(o_F)^+$ associés à un corps de nombres F.

Chapitre 2 : Formules de genre

Nous établissons (cf proposition 2.18) une formule de genre pour les 2-parties des noyaux sauvages d'une extension quadratique de corps de nombres E/F de groupe de Galois G. En pratique, cette formule s'applique lorsque F est totalement réel, et dans ce cas, elle s'écrit (voir corollaire 2.19) :

$$\frac{\mid WK_2(E)(2)_G \mid}{\mid WK_2(F)(2) \mid} = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]},$$

où $T_{E/F}$ est un ensemble dépendant essentiellement de la ramification de l'extension, l'indice normique $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]$ est lié au noyau de Tate D_F et ρ est un entier égal à 0 ou 1. Or, sur des exemples concrets, on peut estimer aisément le cardinal de $T_{E/F}$ et l'indice normique $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]$, mais, dans certains cas, la formule de genre donnée dans [KM2] ne permet pas de décider si ρ vaut 0 ou 1. C'est pourquoi, dans un souci de détail et d'amélioration, on reprend la démonstration de [KM2] et on donne une méthode, pour calculer ρ, reposant sur le calcul de symboles de Hilbert.

Chapitre 3 : Corps quadratiques

Nous constatons d'abord que, sous réserve que le corps de base F admette une 2-partie du noyau sauvage triviale, la formule de genre détermine en fait le 2-rang du noyau sauvage de E (pour une extension quadratique E/F). Par conséquent, en considérant un corps quadratique $E = \mathbb{Q}(\sqrt{d})$, nous déterminons précisément la valeur de ρ en fonction de la forme de l'entier d et retrouvons (théorème 3.4) la valeur du 2-rang du noyau sauvage de $\mathbb{Q}(\sqrt{d})$ établie par J. Browkin et A. Schinzel en 1982. Il s'ensuit aisément la détermination des corps quadratiques dont la 2-partie du noyau sauvage est triviale (théorème 3.1).

Chapitre 4 : 2-extensions cycliques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale

En appliquant la formule de genre, on établit la liste des 2-extensions cycliques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. Néanmoins, le cas le plus révélateur des difficultés rencontrées concerne le sous-corps de degré 4 du corps cyclotomique $\mathbb{Q}(\mu_p)$ où p est un nombre premier tel que $p \equiv 1 \bmod 8$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$. En effet, non seulement c'est le seul cas de corps cyclique de degré au moins 4 pour lequel le calcul de ρ est non trivial, mais aussi c'est l'un des rares cas pour lequel la 2-partie de son noyau sauvage est triviale, sans que celle du noyau modéré positif le soit (comparer avec la proposition 4.21 où l'on distingue nos résultats de ceux de G. Gras).

Chapitre 5 : 2-extensions abéliennes de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale

Après avoir traité le cas des 2-extensions cycliques, nous commençons par déterminer les 2-extensions abéliennes totalement réelles de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale (cf théorème 5.5). Pour cela, on applique une proposition prouvée par M. Kolster et A. Movahhedi ([KM2]) sur les extensions de corps de nombres relativement bi-quadratiques. Pour ce qui concerne les extensions imaginaires, nous savons que la 2-partie du noyau sauvage du sous-corps totalement réel maximal de l'extension considérée est soit triviale, soit d'ordre 2 ; dans le cas où elle est triviale, nous répondons au problème (section 5.2.2). Nous terminons la thèse en donnant un exemple de corps pour lequel on ne sait pas décider de la trivialité de la 2-partie de son noyau sauvage ; dans la situation décrite, si l'on cherche à appliquer la formule de genre, le problème devient équivalent à décider si la 2-partie du noyau sauvage d'un corps est cyclique d'ordre 2, ce qui semble aussi difficile que la question initiale.

Notations générales

p	un nombre premier
n	un entier naturel
A	un groupe abélien
${}_nA$	le noyau de la multiplication par n dans A
$A(p)$	le p-sous-groupe de Sylow de A
$r_{p^n}(A)$	le p^n-rang du groupe *fini* A
$[x,y]$	le commutateur $xyx^{-1}y^{-1}$ pour des éléments x, y d'un groupe G
$[G,G]$	le groupe dérivé d'un groupe G, *i.e.*, le sous-groupe de G engendré par les commutateurs
Λ	un anneau
$\Lambda^\times$	le groupe des éléments inversibles de Λ
$Cl(\Lambda)$	le groupe de classes d'idéaux de Λ
$\overline{\mathfrak{I}}$	la classe de l'idéal $\mathfrak{I}$ de Λ dans $Cl(\Lambda)$
G	un groupe fini
M	un G-module (dont la loi est notée additivement)
M^G	l'ensemble des G-invariants de M, *i.e.*, $M^G = \{x \in M / \forall \sigma \in G, \sigma x = x\}$
$I_G M$	le sous-module de M engendré par les éléments de la forme $\sigma x - x$, où $x \in M$ et $\sigma \in G$
M_G	l'ensemble des G-coinvariants de M, *i.e.*, $M_G = M/I_G M$

F	un corps
F^*	l'ensemble des éléments de F privé de 0
$\mu(F)$	le groupe des racines de l'unité contenues dans F
$[E:F]$	le degré de l'extension finie E/F
$\mathrm{Gal}(E/F)$	le groupe de Galois de l'extension galoisienne E/F
$\mathrm{N}_{E/F}$	l'application norme de l'extension galoisienne E/F
F_∞	la $\mathbb{Z}_p$-extension cyclotomique de F
F_n	le n-ième étage de F_∞

F	un corps de nombres (*i.e.*, une extension finie de $\mathbb{Q}$)
o_F	l'anneau des entiers de F
$Cl(F)$	le groupe de classes d'idéaux de o_F
U_F	le groupe des unités de o_F
F_v	le complété de F à la place v

Enfin, un peu de terminologie :

On appelle p-extension d'un corps F toute extension galoisienne finie de F, dont le groupe de Galois est un p-groupe.

Une place p-adique d'un corps de nombres F est une place de F qui divise p.

De plus, une place qui n'est pas 2-adique sera dite non 2-adique ou impaire.

Chapitre 1

K-groupes et K_2 des corps de nombres

Nous commençons par présenter la construction des premiers groupes de K-théorie K_0, K_1 et K_2 d'un anneau et donnons un aperçu des groupes de K-théorie supérieurs introduits par J. Milnor (voir les trois premières sections). L'essentiel des résultats énoncés sont donnés sans démonstration, mais on peut les trouver dans [Mi] et [Ro], qui sont les deux principales références pour ce sujet. Comme la structure des K-groupes de Milnor $K_n^M(F)$ d'un corps de nombres F est bien connue pour $n \neq 2$, nous nous proposons par la suite d'amorcer l'étude du K_2 d'un corps de nombres. Dans un premier temps, on s'intéresse au K_2 d'un point de vue cohomologique et on énonce sans démonstration des résultats classiques démontrés par J. Tate ([T]). Dans un deuxième temps, on étudie le K_2 d'un corps de nombres à travers les symboles classiques. On se concentre d'abord sur les symboles de Hilbert et modérés afin d'aboutir essentiellement aux définitions des noyaux sauvages et modérés et à leurs premières propriétés. On termine le chapitre par une allusion aux noyaux modérés positifs et aux noyaux modérés des S-entiers, notions qui se révéleront utiles aux prochains chapitres.

Dans toute la suite, Λ désignera un anneau. On notera $Cl(\Lambda)$ le groupe de classes d'idéaux de Λ et $\overline{\mathfrak{I}} \in Cl(\Lambda)$ la classe de l'idéal $\mathfrak{I}$ de Λ.

1.1 Le groupe K_0 de Grothendieck

Pour tout anneau Λ, le groupe $K_0(\Lambda)$ de Grothendieck est, par définition, le quotient du groupe abélien libre des classes d'isomorphisme $[P]$ des Λ-modules projectifs de type fini P par le sous-groupe engendré par les éléments de la forme $[P \oplus Q] - [P] - [Q]$ pour P, Q des Λ-modules projectifs de type fini.

Ainsi, tout élément de $K_0(\Lambda)$ peut s'écrire comme la différence $[P] - [Q]$ où P, Q sont des Λ-modules projectifs de type fini ; de plus, on peut montrer que $[P] = [Q]$ dans $K_0(\Lambda)$ si et seulement si il existe un entier r tel que $P \oplus \Lambda^r \cong Q \oplus \Lambda^r$.

Considérons maintenant un morphisme d'anneaux $f : \Lambda \to \Lambda'$. Alors, à partir de tout Λ-module P, on peut définir un Λ'-module, à savoir $\Lambda' \otimes_\Lambda P$. De plus, si P est un Λ-module projectif de type fini, alors il existe un Λ-module Q et un entier r tels que $P \oplus Q \cong \Lambda^r$; et, par conséquent, $(\Lambda' \otimes_\Lambda P) \oplus (\Lambda' \otimes_\Lambda Q) \cong \Lambda' \otimes_\Lambda \Lambda^r \cong (\Lambda')^r$. Autrement dit, $\Lambda' \otimes_\Lambda P$ est un Λ'-module projectif de type fini, de telle sorte que la correspondance $[P] \mapsto [\Lambda' \otimes_\Lambda P]$ permet de définir un morphisme de groupes abéliens

$$f_* : K_0(\Lambda) \to K_0(\Lambda').$$

Ainsi, K_0 est un foncteur covariant de la catégorie des anneaux vers la catégorie des groupes abéliens. Les propriétés suivantes sont donc vérifiées : $(\text{identité})_* = \text{identité}$ et $(f \circ g)_* = f_* \circ g_*$.

Avant de calculer K_0 pour des familles d'anneaux particuliers, rappelons la définition suivante. On dira que Λ est un anneau local si l'ensemble $\mathfrak{M} = \Lambda \smallsetminus \Lambda^\times$ formé des éléments de Λ qui ne sont pas dans $\Lambda^\times$, c'est-à-dire qui ne sont pas des unités, est un idéal à gauche de Λ. Il est à noter que, si Λ est local, alors un Λ-module est projectif si et seulement si il est libre. D'où la

Proposition 1.1. *Si Λ est un anneau local, alors $K_0(\Lambda) \cong \mathbb{Z}$, engendré par la classe du Λ-module libre de rang* 1, i.e., *par* $[\Lambda]$. *C'est donc vrai, en particulier, si Λ est un corps.*

Intéressons-nous maintenant au comportement du K_0 pour les anneaux de Dedekind. Nous allons constater que le groupe K_0 d'un anneau de Dedekind est étroitement lié à son groupe de classes d'idéaux.

Théorème 1.2. *Si Λ est un anneau de Dedekind, alors on a l'isomorphisme*

$$K_0(\Lambda) \cong \mathbb{Z} \oplus Cl(\Lambda).$$

On en déduit immédiatement les résultats suivants pour des anneaux de Dedekind bien particuliers :

Corollaire 1.3. *(i) Si Λ est un anneau principal, alors $K_0(\Lambda) \cong \mathbb{Z}$.*
(ii) Si F est un corps de nombres,

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

où o_F est l'anneau des entiers de F et $Cl(F) := Cl(o_F)$ est le groupe de classes d'idéaux de l'anneau o_F.

1.2 Le groupe K_1 de Whitehead

Soit n un entier $\geqslant 1$. Comme d'habitude, nous noterons $\mathrm{GL}_n(\Lambda)$ le groupe des matrices carrées $n \times n$, inversibles, à coefficients dans Λ. Comme $\mathrm{GL}_n(\Lambda)$ s'injecte dans $\mathrm{GL}_{n+1}(\Lambda)$ par la correspondance $A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$, on peut considérer la limite directe

$$\mathrm{GL}(\Lambda) := \varinjlim \mathrm{GL}_n(\Lambda) = \bigcup_{n=1}^{+\infty} \mathrm{GL}_n(\Lambda),$$

que l'on appelle le groupe linéaire général infini.

Pour i et j deux entiers distincts compris entre 1 et n, et pour tout $\lambda \in \Lambda$, désignons par $e_{ij}^{\lambda} \in \mathrm{GL}_n(\Lambda)$ la matrice $(a_{k,\ell})_{1 \leqslant k,\ell \leqslant n}$ définie par :

$$\begin{cases} a_{k,k} = 1 & \text{pour } 1 \leqslant k \leqslant n, \\ a_{i,j} = \lambda, & \\ a_{k,\ell} = 0 & \text{sinon.} \end{cases}$$

Une telle matrice est dite élémentaire. Par ailleurs, notons $\mathrm{E}_n(\Lambda)$ le sous-groupe de $\mathrm{GL}_n(\Lambda)$ engendré par toutes ces matrices, et posons

$$\mathrm{E}(\Lambda) := \varinjlim \mathrm{E}_n(\Lambda) = \bigcup_{n=1}^{+\infty} \mathrm{E}_n(\Lambda),$$

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

On déduit directement de la définition que

$$e_{ij}^{\lambda} e_{ij}^{\mu} = e_{ij}^{\lambda+\mu}.$$

En particulier, on a $(e_{ij}^{\lambda})^{-1} = e_{ij}^{-\lambda}$.

De plus, le commutateur $[A, B] = ABA^{-1}B^{-1}$ de deux matrices élémentaires se calcule aisément dans certains cas :

$$[e_{ij}^{\lambda}, e_{k\ell}^{\mu}] = \begin{cases} I_n & \text{si } j \neq k, i \neq \ell \\ e_{i\ell}^{\lambda\mu} & \text{si } j = k, i \neq \ell \\ e_{kj}^{-\lambda\mu} & \text{si } j \neq k, i = \ell \end{cases}$$

où I_n est la matrice identité de $\mathrm{GL}_n(\Lambda)$.
Nous pouvons maintenant énoncer un lemme d'importance capitale pour la suite :

Lemme 1.4 (Whitehead). *Le groupe dérivé de* $\mathrm{GL}(\Lambda)$*, c'est-à-dire le sous-groupe de* $\mathrm{GL}(\Lambda)$ *engendré par les commutateurs, est exactement le groupe* $\mathrm{E}(\Lambda)$*. Autrement dit, avec les notations usuelles,*

$$\mathrm{E}(\Lambda) = [\mathrm{GL}(\Lambda) : \mathrm{GL}(\Lambda)].$$

Par conséquent, $\mathrm{E}(\Lambda)$ est un sous-groupe distingué de $\mathrm{GL}(\Lambda)$, et on définit le groupe de Whitehead

$$K_1(\Lambda) := \mathrm{GL}(\Lambda) / \mathrm{E}(\Lambda),$$

qui est donc un groupe abélien, compte tenu du lemme précédent. En fait, $K_1(\Lambda)$ est l'abélianisé de $\mathrm{GL}(\Lambda)$, c'est-à-dire le groupe obtenu en quotientant $\mathrm{GL}(\Lambda)$ par son sous-groupe dérivé, ce qu'on peut traduire, en termes d'homologie, par la

Proposition 1.5. *Pour tout anneau* Λ*, on a*

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

Passons maintenant aux propriétés fonctorielles du K_1. Il est clair que tout morphisme d'anneaux $f : \Lambda \to \Lambda'$ permet de définir un morphisme de groupes $f_* : K_1(\Lambda) \to K_1(\Lambda')$. Ainsi, K_1 est un foncteur covariant de la catégorie des anneaux vers la catégorie des groupes abéliens.

Nous supposons jusqu'à la fin de cette partie que Λ est un anneau *commutatif.* Ainsi, la fonction déterminant est bien définie sur l'anneau des matrices carrées, à coefficients dans Λ, et on peut définir $\mathrm{SL}_n(\Lambda)$, le sous-groupe de $\mathrm{GL}_n(\Lambda)$ formé des matrices de déterminant $+1$, et

$$\mathrm{SL}(\Lambda) := \varinjlim \mathrm{SL}_n(\Lambda) = \bigcup_{n=1}^{+\infty} \mathrm{SL}_n(\Lambda),$$

que l'on appelle le groupe spécial linéaire infini.

Si $\Lambda^\times$ désigne les unités de Λ, on a une suite exacte

$$1 \longrightarrow \mathrm{SL}(\Lambda) \longrightarrow \mathrm{GL}(\Lambda) \xrightarrow{\text{dét}} \Lambda^\times \longrightarrow 1.$$

Comme $\mathrm{E}(\Lambda) \subset \mathrm{SL}(\Lambda)$, on obtient la suite exacte :

$$0 \longrightarrow \mathrm{SL}(\Lambda)/\,\mathrm{E}(\Lambda) \longrightarrow K_1(\Lambda) \xrightarrow{\text{dét}} \Lambda^\times \longrightarrow 1,$$

qui est scindée, puisque la composée $\Lambda^\times = \mathrm{GL}_1(\Lambda) = \mathrm{GL}_1(\Lambda)/\,\mathrm{E}_1(\Lambda) \subset \mathrm{GL}(\Lambda)/\,\mathrm{E}(\Lambda) = K_1(\Lambda) \xrightarrow{\text{dét}} \Lambda^\times$ est clairement l'identité. D'où la

Proposition 1.6. *Pour tout anneau commutatif* Λ*, on a*

$$K_1(\Lambda) \cong \Lambda^\times \oplus \mathrm{SK}_1(\Lambda),$$

où $\mathrm{SK}_1(\Lambda) := \mathrm{SL}(\Lambda)/\,\mathrm{E}(\Lambda)$.

Par conséquent, la connaissance de $\mathrm{SK}_1(\Lambda)$ suffit donc pour déterminer la structure de $K_1(\Lambda)$. Comme nous allons le voir, $\mathrm{SK}_1(\Lambda)$ s'annule pour différentes familles d'anneaux.

Théorème 1.7. *Si* Λ *est un anneau commutatif local ou un anneau euclidien (commutatif) ou l'anneau des entiers d'un corps de nombres, alors* $\mathrm{SK}_1(\Lambda) = 0$*, et le déterminant induit un isomorphisme*

$$K_1(\Lambda) \cong \Lambda^\times.$$

En particulier, cela signifie que, si F *est un corps de nombres, on a*

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

où o_F *est l'anneau des entiers de* F *et* $U_F := o_F^\times$ *est l'ensemble des unités de* F*.*

Remarque : notons que, dans le cas de l'anneau des entiers d'un corps de nombres, J. Milnor ([Mi], § 16) donne une preuve de ce théorème s'appuyant sur la suite exacte de Moore (que l'on retrouvera plus loin lorsque l'on parlera de noyau sauvage).

Corollaire 1.8.

$$K_1(\mathbb{Z}) \cong \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z},\ K_1(\mathbb{Z}[i]) \cong \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}.$$

1.3 Le groupe K_2 et les groupes supérieurs de Milnor

Soit n un entier $\geqslant 3$. Le groupe de Steinberg $\mathrm{St}_n(\Lambda)$ est, par définition, le groupe libre engendré par les éléments x_{ij}^{λ}, pour $1 \leqslant i, j \leqslant n$, $i \neq j$, et $\lambda \in \Lambda$, assujettis aux relations :
(1) $x_{ij}^{\lambda} x_{ij}^{\mu} = x_{ij}^{\lambda+\mu}$,
(2) $[x_{ij}^{\lambda}, x_{j\ell}^{\mu}] = x_{i\ell}^{\lambda\mu}$, pour $i \neq \ell$, et
(3) $[x_{ij}^{\lambda}, x_{k\ell}^{\mu}] = 1$ pour $j \neq k, i \neq \ell$.

On peut naturellement considérer le morphisme de groupes de $\mathrm{St}_n(\Lambda)$ dans $\mathrm{St}_{n+1}(\Lambda)$ qui, à l'élément $x_{ij}^{\lambda} \in \mathrm{St}_n(\Lambda)$, associe l'élément correspondant $x_{ij}^{\lambda} \in \mathrm{St}_{n+1}(\Lambda)$; ainsi, on peut définir la limite directe

$$\mathrm{St}(\Lambda) := \varinjlim \mathrm{St}_n(\Lambda),$$

que l'on appelle aussi le groupe de Steinberg.

Maintenant, en posant $\phi_n(x_{ij}^{\lambda}) = e_{ij}^{\lambda}$, on définit un morphisme canonique de groupes

$$\phi_n : \mathrm{St}_n(\Lambda) \to \mathrm{GL}_n(\Lambda),$$

dont l'image est clairement $\phi_n(\mathrm{St}_n(\Lambda)) = \mathrm{E}_n(\Lambda)$. En passant à la limite directe lorsque $n \to +\infty$, on obtient un nouveau morphisme de groupes

$$\phi : \mathrm{St}(\Lambda) \to \mathrm{GL}(\Lambda),$$

dont l'image est $\mathrm{E}(\Lambda)$.

On appelle K_2 de l'anneau Λ, et on note $K_2(\Lambda)$, le noyau du morphisme ϕ. Nous avons donc la suite exacte :

$$1 \longrightarrow K_2(\Lambda) \longrightarrow \mathrm{St}(\Lambda) \longrightarrow \mathrm{GL}(\Lambda) \longrightarrow K_1(\Lambda) \longrightarrow 1.$$

Théorème 1.9. *Le groupe $K_2(\Lambda)$ est exactement le centre du groupe de Steinberg* $\mathrm{St}(\Lambda)$. *En particulier, $K_2(\Lambda)$ est un groupe abélien.*

Quant aux propriétés fonctorielles du K_2, elles proviennent du fait que, si $f : \Lambda \to \Lambda'$ est un morphisme d'anneaux, alors on a le diagramme commutatif :

$$\begin{tikzcd}
0 \arrow[r] & K_2(\Lambda) \arrow[r] \arrow[d] & \mathrm{St}(\Lambda) \arrow[r] \arrow[d] & \mathrm{GL}(\Lambda) \arrow[r] \arrow[d] & K_1(\Lambda) \arrow[r] \arrow[d] & 1 \\
0 \arrow[r] & K_2(\Lambda') \arrow[r] & \mathrm{St}(\Lambda') \arrow[r] & \mathrm{GL}(\Lambda') \arrow[r] & K_1(\Lambda') \arrow[r] & 1
\end{tikzcd}$$

Ainsi, K_2 est un foncteur covariant de la catégorie des anneaux vers la catégorie des groupes abéliens.

À titre d'exemple de calcul du K_2 pour un anneau, on peut évoquer le résultat suivant dont l'utilité apparaîtra à la section 1.6 (il permettra en fait d'obtenir la trivialité du noyau sauvage de $\mathbb{Q}$).

Proposition 1.10. *On a l'isomorphisme de groupes $K_2(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.*

Plus précisément, si l'on pose

$$x = (x_{12}^1 x_{21}^{-1} x_{12}^1)^4 \ \in \mathrm{St}(\mathbb{Z}),$$

alors

$$\begin{aligned} \phi(x) &= \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)^4 \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

On constate donc que $x \in K_2(\mathbb{Z})$ et on peut montrer (cf [Mi], § 10) qu'en fait x est d'ordre 2 et qu'il engendre $K_2(\mathbb{Z})$.

Remarque : si l'on prend le problème à l'envers, il est possible de prouver d'abord la trivialité du noyau sauvage de $\mathbb{Q}$ (obtenue comme corollaire de Theorem 1B, [Bi]), et ensuite de retrouver la proposition précédente avec la suite exacte de Moore (comparer avec le 2° de la remarque page 31).

Comme pour le foncteur K_1, on a une description homologique du foncteur K_2, description qui repose sur la théorie des extensions centrales universelles dont on rappelle brièvement les notions mises en jeu.

Une extension centrale d'un groupe G est la donnée d'un couple (X, τ) où X est un groupe et τ est un morphisme surjectif de X dans G tels que le noyau $\mathrm{Ker}\,\tau$ est contenu dans le centre du groupe X.

Une extension centrale (U, ν) de G est dite universelle si, pour toute extension centrale (X, τ) de G, il existe un unique morphisme h rendant commutatif le diagramme suivant :

$$\begin{tikzcd} U \arrow[r, "\nu"] \arrow[d, dashed, "h"'] & G \\ X \arrow[ur, "\tau"'] & \end{tikzcd}$$

On peut remarquer que, s'il existe une telle extension centrale universelle, alors elle est unique à isomorphisme près.

Proposition 1.11. *Un groupe G admet une extension centrale universelle si et seulement si il est parfait.*

Rappelons qu'un groupe G est dit parfait s'il coïncide avec son groupe dérivé, c'est-à-dire si $G = [G : G]$.

Proposition 1.12. *Le groupe de Steinberg* $\mathrm{St}(\Lambda)$ *associé au morphisme naturel ϕ est l'extension centrale universelle du groupe parfait* $\mathrm{E}(\Lambda)$. *Par conséquent, $K_2(\Lambda)$ peut être identifié au multiplicateur de Schur $H_2(\mathrm{E}(\Lambda), \mathbb{Z})$; autrement dit, on a*

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

Passons maintenant à la caractérisation de $K_2(\Lambda)$ à partir de symboles (de Steinberg). Pour cela, nous supposerons, dans toute la suite, que Λ est un anneau commutatif.

Considérons $u, v \in \Lambda^\times$ et posons

$$\tilde{u} = \begin{pmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \tilde{v} = \begin{pmatrix} v & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & v^{-1} \end{pmatrix} \in \mathrm{E}_3(\Lambda).$$

Le fait que ces deux matrices soient des éléments de $\mathrm{E}_3(\Lambda)$ n'est pas *a priori* évident. C'est une conséquence de l'appartenance au groupe des matrices élémentaires de toute matrice triangulaire supérieure (ou inférieure) ne possédant que des 1 sur la diagonale (pour plus de précision, voir [Ro], Corollary 2.1.3).

Le morphisme $\phi : \mathrm{St}(\Lambda) \to \mathrm{E}(\Lambda)$ étant surjectif, il existe $U, V \in \mathrm{St}(\Lambda)$ tels que $\phi(U) = \tilde{u}$ et $\phi(V) = \tilde{v}$. Ainsi, puisque $\mathrm{Ker}\,\phi$ est le centre de $\mathrm{St}(\Lambda)$, on voit que le commutateur $[U, V] \in \mathrm{St}(\Lambda)$ ne dépend pas du choix des antécédents U, V de $\tilde{u}, \tilde{v}$. De plus, comme $\tilde{u}$ et $\tilde{v}$ commutent, $[U, V] \in K_2(\Lambda)$. On définit alors le symbole de Steinberg $\{u, v\}$ de u et v comme étant l'élément $[U, V] \in K_2(\Lambda)$.

Rappelons qu'un symbole sur un anneau Λ, à valeurs dans un groupe abélien G (noté multiplicativement), est une application $< , >: \Lambda^\times \times \Lambda^\times \to G$ telle que :

1. $< uv, w > = < u, w >< v, w >$, pour tous $u, v, w \in \Lambda^\times$,
2. $< u, vw > = < u, v >< u, w >$, pour tous $u, v, w \in \Lambda^\times$,

3. $< u, 1-u >= 1$, pour tout $u \in \Lambda^\times$ tel que $1-u \in \Lambda^\times$.

On peut dresser, dans un premier temps, les propriétés qui justifient, entre autres, le fait que les symboles de Steinberg sont effectivement des symboles.

Proposition 1.13. *Pour $u, v, w \in \Lambda^\times$, on a dans $K_2(\Lambda)$:*

1. $\{u, v\} = \{v, u\}^{-1}$,
2. $\{uv, w\} = \{u, w\}\{v, w\}$,
3. $\{u, vw\} = \{u, v\}\{u, w\}$,
4. $\{u, -u\} = 1$,
5. $\{u, 1-u\} = 1$, *si* $1-u \in \Lambda^\times$.

Donnons le principal résultat liant le K_2 d'un corps aux symboles de Steinberg.

Théorème 1.14 (Matsumoto). *Si F est un corps, $K_2(F)$ est le groupe abélien libre engendré par les symboles de Steinberg $\{u, v\}$ avec $u, v \in \Lambda^\times$, assujettis aux relations de bilinéarité des symboles et à la relation $\{u, 1-u\} = 1$.*

Proposition 1.15. *Si F est un corps fini, alors tous les symboles de Steinberg sont triviaux dans $K_2(F)$, et donc $K_2(F) = 0$.*

Enfin, pour conclure cette section, nous allons d'abord faire un lien entre les groupes K_0, K_1 et K_2 dans une situation particulière significative, puis, introduire les groupes supérieurs de la K-théorie de Milnor.

Théorème 1.16 (Bass, Tate). *Soit Λ un anneau de Dedekind de corps de fractions F. Alors, on a la suite exacte*

$$K_2(F) \to \oplus K_1(\Lambda/\mathfrak{p}) \to K_1(\Lambda) \to K_1(F) \to \oplus K_0(\Lambda/\mathfrak{p}) \to K_0(\Lambda) \to K_0(F) \to 0,$$

où, dans les deux sommes directes, $\mathfrak{p}$ décrit l'ensemble des idéaux premiers non nuls de Λ.

Nous allons maintenant décrire brièvement les groupes de K-théorie supérieurs, que J. Milnor a défini dans le but, en quelque sorte, de généraliser le théorème de Matsumoto. Pour tout corps commutatif F, considérons l'algèbre tensorielle sur le $\mathbb{Z}$-module F^* définie par

$$T(F^*) = \bigoplus_{n=0}^{+\infty} T^n(F^*),$$

où $T^0(F^*) = \mathbb{Z}$ et, pour $n \geqslant 1$,

$$T^n(F^*) = \underbrace{F^* \otimes \cdots \otimes F^*}_{n \text{ fois}}.$$

L'idéal bilatère I de $T(F^*)$, engendré par les éléments de la forme $u \otimes (1-u)$, avec $u \in F \smallsetminus \{0,1\}$, est gradué, c'est-à-dire

$$I = \bigoplus_{n=0}^{+\infty} I \cap T^n(F^*),$$

et l'anneau de Milnor de F est bien défini par

$$K_*^M(F) := T(F^*)/I = \bigoplus_{n=0}^{+\infty} K_n^M(F).$$

Autrement dit, on a :

$$K_n^M(F) = T^n(F^*)/I \cap T^n(F^*) = T^n(F^*)/ < u_1 \otimes \cdots \otimes u_n \,/\, \exists i,j : u_i + u_j = 1 > .$$

Ainsi, $K_n^M(F)$ est défini pour tout $n \geqslant 0$ et, pour $n \in \{0,1,2\}$, on voit que le groupe $K_n^M(F)$ coïncide avec le groupe $K_n(F)$ précédemment introduit. En effet, on a déjà constaté que $K_0(F) \cong \mathbb{Z}$, $K_1(F) \cong F^*$ et, d'après le théorème de Matsumoto, $K_2(F) \cong F^* \otimes F^* / < u \otimes (1-u)\,;\, u \in F \smallsetminus \{0,1\} >$.

L'anneau $K_*^M(F)$ est un anneau gradué anticommutatif, dont on note $*$ la loi de multiplication dans l'anneau.

Proposition 1.17. *Dans l'anneau de Milnor d'un corps commutatif F, les propriétés suivantes sont vérifiées :*

(1) $(aa') * b = (a * b) + (a' * b)\,;$
(2) $a * (bb') = (a * b) + (a * b')\,;$
(3) $a * (1 - a) = 0\,;$
(4) $a * (-a) = 0\,;$
(5) $a * a = a * (-1)$ *(et donc $2\, a * a = 0$)* ;
(6) $a * b = -b * a$ *(anticommutativité) ;*
(7) $a_1 * a_2 * \cdots * a_n = 0,$ *pour* $a_1 + a_2 + \cdots + a_n = 0$ *ou* 1;
(8) $a_1 * a_2 * \cdots * a_n = 0,$ *s'il existe* $i \neq j$ *tels que* $a_i + a_j = 1$,

où $a, a', b, b', a_1, \ldots, a_n$ sont des éléments de F^* (vus comme éléments de $K_*^M(F)$).

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

Théorème 1.18 (Bass, Tate). *Si F est un corps de nombres, pour tout $n \geqslant 3$, le groupe $K_n^M(F)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{r_1}$, où r_1 est le nombre de places réelles de F.*

(pour une preuve, voir [BT]).

Il est à noter que le bon cadre, pour traiter des groupes de K-théorie supérieurs, a été, comme chacun sait, défini par D. Quillen. Il a introduit les groupes $K_n(\Lambda)$, pour tout anneau Λ et $n \geqslant 1$, en lien étroit avec l'homologie sur $\mathbb{Z}$ du groupe $\mathrm{GL}(\Lambda)$ (comme le suggèrent les propositions 1.5 et 1.12). On pourra consulter [Ro] (Chapter 5) pour une introduction à la K-théorie de D. Quillen.

D'autre part, compte tenu de la proposition précédente, on s'intéressera par la suite au K_2 des corps de nombres, dont la structure est bien moins connue. Désormais, jusqu'à la fin du chapitre, F désigne un corps de nombres, *i.e.*, une extension finie du corps des rationnels $\mathbb{Q}$. Comme d'habitude, l'anneau des entiers de F est noté o_F. De plus, on note $\mathrm{N}_{L/K}$ l'application norme de l'extension finie de corps L/K.

Compte tenu du théorème de Matsumoto, on peut considérer que

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

et, on note $\{x, y\}_F$ ou, s'il n'y a pas de confusion possible, $\{x, y\}$ la classe de l'élément $x \otimes y$ dans $K_2(F)$.

1.4 Description cohomologique du K_2

Dans cette partie, nous reprenons les résultats de J. Tate (voir [T]).

Proposition 1.19. *$K_2(F)$ est un groupe de torsion sans sous-groupe divisible non-nul.*

Rappelons qu'un groupe de torsion est un groupe dont tous les éléments sont d'ordre fini. De plus, pour tout nombre premier p, un groupe G est dit p-divisible si le morphisme $G \to G,\ x \mapsto x^p$ est surjectif ; le groupe G est dit divisible s'il est p-divisible pour tout nombre premier p.

Une description cohomologique du K_2 d'un corps de nombres est donnée par le théorème suivant :

Théorème 1.20. *Si, pour tout nombre premier p, on note $K_2(F)(p)$ la partie p-primaire de $K_2(F)$, formée de tous les éléments de $K_2(F)$ d'ordre une puissance de p, alors*

$$K_2(F) = \bigoplus_{p \text{ premier}} K_2(F)(p),$$

et, pour tout nombre premier p, on a

$$K_2(F)(p) \cong H^2(F, \mathbb{Z}_p(2)),$$

où $H^2(F, \mathbb{Z}_p(2))$ est le deuxième groupe de cohomologie continue galoisienne à valeurs dans le module $\mathbb{Z}_p$ tordu deux fois à la Tate.

De l'isomorphisme précédent, on peut déduire quelques résultats intéressants que l'on regroupe dans le corollaire suivant :

Corollaire 1.21. *Supposons que F contienne une racine primitive p-ième de l'unité ζ (où p est un nombre premier). Alors, on a :*

(i) Tout élément d'ordre p de $K_2(F)$ s'écrit sous la forme $\{\zeta, a\}$, où $a \in F^*$.

(ii) Si l'on pose

$$D_F = \{a \in F^*/\{\zeta, a\} = 1 \text{ dans } K_2(F)\},$$

et, si r_2 est le nombre de places complexes de F, alors

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

Par définition, D_F est le noyau de Tate de F.

1.5 Symboles classiques

1.5.1 Symboles de Hilbert

Afin d'alléger les notations, nous noterons K le complété F_v de F à la place v (finie ou réelle) de F. Nous supposerons, de plus, que K^* contient le groupe des racines m-ièmes de l'unité, où m est un entier $\geqslant 2$.

La définition du symbole de Hilbert découle, d'une part, de la théorie du corps de classes et, d'autre part, de la théorie de Kummer (voir [N]). Plus précisément, considérons $L := K(\sqrt[m]{K^*})$ l'extension abélienne maximale d'exposant m ; autrement dit, L est engendrée par tous les éléments de la forme $\sqrt[m]{a}$, où $a \in K^*$. Alors, d'après la théorie de Kummer, on sait que l'application

$$\left\{ \begin{array}{ccc} K^*/K^{*m} & \to & \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m), \\ \bar{a} & \mapsto & \chi_a : \left(\sigma \mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}\right) \end{array} \right.$$

induit l'isomorphisme

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m) \cong K^*/K^{*m}.$$

On en déduit, en particulier, que $\mathrm{N}_{L/K}(L^*) = K^{*m}$.

Par ailleurs, en toute généralité, si L est une extension abélienne finie de K de groupe de Galois $\mathrm{Gal}(L/K)$, alors la théorie du corps de classes locale (voir, par exemple, [N]) nous donne l'existence d'un morphisme surjectif $(\ . \ , L/K) : K^* \to \mathrm{Gal}(L/K)$, appelé symbole des restes normiques, dont le noyau est $\mathrm{N}_{L/K}(L^*)$.

Par conséquent, si l'on revient au cas où L est l'extension abélienne maximale d'exposant m, la théorie du corps de classes nous donne l'isomorphisme

$$\mathrm{Gal}(L/K) \cong K^*/K^{*m}.$$

Ainsi, la forme bilinéaire

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m) \times \mathrm{Gal}(L/K) \to \mu_m \, , (\chi, \sigma) \mapsto \chi(\sigma),$$

induit une forme bilinéaire non dégénérée

$$(\ . \ , \ . \ )_{K,m} : K^*/K^{*m} \times K^*/K^{*m} \to \mu_m,$$

que l'on appelle symbole de Hilbert.

Autrement dit, on a :

Proposition 1.22. *Si $a, b \in K^*$, alors le symbole de Hilbert $(a,b)_{K,m}$ est donné par*

$$(b, K(\sqrt[m]{a})/K)(\sqrt[m]{a}) = (a,b)_{K,m} \sqrt[m]{a}.$$

Notations : comme on pourra se rendre compte dans la suite la notation $(\ . \ , \ . \ )_{K,m}$ se révélera parfois encombrante. C'est pourquoi nous nous proposons de la simplifier quelque peu dans des cas précis :

1° Lorsque $m = 2$, on notera

$$(a,b)_K := (a,b)_{K,m}.$$

2º Lorsque $K = F_v$ et que $m = |\mu(F_v)|$, on notera

$$(a,b)_v := (a,b)_{K,m} = (a,b)_{F_v,|\mu(F_v)|} \ .$$

3º Lorsque $K = F_v$ et que $m = n_v = |\mu(F_v)(2)|$, on notera

$$(a,b)_{n_v} := (a,b)_{K,m} = (a,b)_{F_v,|\mu(F_v)(2)|} \ .$$

Remarque : si $K = \mathbb{R}$, on a nécessairement $m = 2$, et, pour $a, b \in \mathbb{R}^*$,

$$(a,b)_{\mathbb{R},2} = (a,b)_{\mathbb{R}} = (-1)^{\frac{\operatorname{sign}(a)-1}{2}\frac{\operatorname{sign}(b)-1}{2}}.$$

Les symboles de Hilbert vérifient un certain nombre de propriétés dont une partie justifie le fait qu'ils sont bien des symboles (au sens rappelé page 20).

Proposition 1.23.

(i) $(aa', b)_{K,m} = (a,b)_{K,m}(a',b)_{K,m}$;

(ii) $(a, bb')_{K,m} = (a,b)_{K,m}(a,b')_{K,m}$;

(iii) $(a,b)_{K,m} = 1 \Leftrightarrow b$ *est une norme dans l'extension* $K(\sqrt[m]{a})/K$;

(iv) $(a,b)_{K,m} = (b,a)^{-1}_{K,m}$;

(v) $(a,-a)_{K,m} = 1$ *et* $(a, 1-a)_{K,m} = 1$;

(vi) *Si* $(a,b)_{K,m} = 1$ *pour tout* $a \in K^*$, *alors* $b \in K^{*m}$;

(vii) *Si* L/K *est une extension finie, alors, pour* $a \in K^*$ *et* $b \in L^*$,
$$(a,b)_{L,m} = (a, \mathrm{N}_{L/K}(b))_{K,m}.$$

Démonstration. Les propriétés ci-dessus découlent essentiellement des propriétés du symbole des restes normiques. Compte tenu du rôle essentiel que va jouer le point (vii) dans la suite, nous donnons le détail de sa démonstration. D'après la proposition 1.22, on a

$$(b, L(\sqrt[m]{a})/L)(\sqrt[m]{a}) = (a,b)_{L,m}\sqrt[m]{a}.$$

Or la situation est la suivante

$$\begin{tikzcd} & L(\sqrt[m]{a}) \arrow[dd, dash] \\ L \arrow[ur, dash] \arrow[dd, dash] & \\ & K(\sqrt[m]{a}) \\ K \arrow[ur, dash] & \end{tikzcd}$$

et on a donc, d'après [N], Chapter II, Proposition 5.4, le diagramme commutatif suivant :

$$\begin{tikzcd}
L^* \arrow[r, "{(\,.\,,L(\sqrt[m]{a})/L)}"] \arrow[d, "\mathrm{N}_{L/K}"'] & \mathrm{Gal}(L(\sqrt[m]{a})/L) \arrow[d, "\text{restriction}"] \\
K^* \arrow[r, "{(\,.\,,K(\sqrt[m]{a})/K)}"] & \mathrm{Gal}(K(\sqrt[m]{a})/K)
\end{tikzcd}$$

Par conséquent,

$$(b, L(\sqrt[m]{a})/L)(\sqrt[m]{a}) = (\mathrm{N}_{L/K}(b), K(\sqrt[m]{a})/K)(\sqrt[m]{a}) = (a, \mathrm{N}_{L/K}(b))_{K,m} \sqrt[m]{a}.$$

D'où le résultat annoncé. □

Avant de passer au calcul effectif de certains symboles de Hilbert, on énonce un résultat qui se révélera d'un intérêt certain pour comprendre la suite exacte de Moore.

Proposition 1.24 (Formule du produit). *Les symboles de Hilbert vérifient la formule du produit :*

$$\prod_v (a,b)_v^{\frac{|\mu(F_v)|}{|\mu(F)|}} = 1,$$

où $a, b \in F^*$.

Nous continuons cette partie consacrée aux symboles de Hilbert par le calcul de ces symboles dans le cas particulier où $K = \mathbb{Q}_p$ est le corps des nombres p-adiques (où p est un nombre premier) et $m = 2$. Fixons donc un nombre premier p et notons $(a,b)_p := (a,b)_{\mathbb{Q}_p}$ le symbole de Hilbert à valeurs dans μ_2 défini pour $a, b \in \mathbb{Q}_p^*$.

Nous attirons l'attention du lecteur sur le fait que la notation classique $(a,b)_p$ ne coïncide pas avec celle introduite précédemment, à savoir $(a,b)_v$, mais cela ne nuit pas vraiment pour la suite de ce travail. C'est notamment pour cette raison qu'à chaque fois que l'on calculera des symboles de Hilbert, on tâchera de préciser quelle définition on utilise précisément.

Soit p un nombre premier $\neq 2$ et $x \in \mathbb{F}_p^*$. On appelle symbole de Legendre de x, et on note $\left(\frac{x}{p}\right)$, l'entier $x^{\frac{p-1}{2}} \in \{\pm 1\}$.

On convient d'étendre ce symbole à $\mathbb{F}_p$ tout entier en posant $\left(\frac{0}{p}\right) = 0$. De plus, si y est une unité p-adique, on pose $\left(\frac{y}{p}\right) = \left(\frac{\bar{y}}{p}\right)$, où $\bar{y}$ est l'image de y par le morphisme de réduction modulo $p : \mathbb{Z}_p^\times \to \mathbb{F}_p^*$.

Rappelons un résultat bien connu sur les symboles de Legendre.

Proposition 1.25. *On a les formules :*
(i) $\left(\frac{1}{p}\right) = 1;$
(ii) $\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$
(iii) $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$

où, pour tout entier impair n*, les éléments* $\epsilon(n)$ *et* $\omega(n)$ *de* $\mathbb{Z}/2\mathbb{Z}$ *sont définis par :*

$$\epsilon(n) \equiv \frac{n-1}{2} \mod 2,$$

et

$$\omega(n) \equiv \frac{n^2-1}{8} \mod 2.$$

Démonstration. Voir [S2], Chapitre I, Théorème 5. □

Nous pouvons maintenant donner explicitement la valeur du symbole de Hilbert $(a, b)_p$.

Proposition 1.26. *Soit* $a = p^\alpha u$ *et* $b = p^\beta v$ *deux éléments de* $\mathbb{Q}_p$*, où* u *et* v *sont des unités* p*-adiques. Alors,*

$$(a, b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad \textit{si } p \neq 2,$$

et

$$(a, b)_p = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} \quad \textit{si } p = 2.$$

Démonstration. Voir [S2], Chapitre III, Théorème 1. □

1.5.2 Symboles modérés

Nous adoptons les notations suivantes : soit
v une place finie de F,
p le nombre premier au-dessus duquel vit v,
F_v le complété de F en v,
$\mathfrak{O}_v = \{x \in F_v / \ v(x) \geqslant 0\}$ l'anneau de valuation associé à F_v,
$\mathfrak{M}_v = \{x \in F_v / \ v(x) > 0\}$ l'idéal maximal de $\mathfrak{O}_v$,
$k_v = \mathfrak{O}_v/\mathfrak{M}_v$ le corps résiduel de F_v,
$\mathrm{N}v$ la norme de v, en tant qu'idéal premier.

On définit, pour a et b dans F^*, le symbole modéré $< a, b >_v \in k_v^*$ par

$$< a, b >_v = (-1)^{v(a)v(b)} \frac{a^{v(b)}}{b^{v(a)}} \pmod{\mathfrak{M}_v}.$$

Remarquons d'abord que cela définit bien un symbole.

Il est à noter que le groupe $\mu(F_v)$ des racines de l'unité contenues dans F_v est isomorphe à la somme directe de son p-sous-groupe de Sylow $\mu(F_v)(p)$ et de son sous-groupe formé des racines de l'unité d'ordre étranger à p. Il se trouve que ce dernier groupe est, en fait, isomorphe au groupe multiplicatif k_v^* de k_v. En particulier, le cardinal de ce groupe est $|k_v^*| = \mathrm{N}v - 1$. En considérant que le symbole modéré prend ses valeurs dans $\mu(F_v)$, on obtient la

Proposition 1.27. *Si v est une place finie de F, on a, pour $a, b \in F^*$,*

$$< a, b >_v = (a, b)_v^{\frac{|\mu(F_v)|}{\mathrm{N}v-1}}.$$

En particulier, le symbole de Hilbert $(a, b)_v$ coïncide avec le symbole modéré $< a, b >_v$, sauf en un nombre fini de places.

Démonstration. Voir, par exemple, [Gr2]. Néanmoins, expliquons ici pourquoi les deux symboles coïncident, sauf pour un nombre fini de places. En fait, $\frac{|\mu(F_v)|}{\mathrm{N}v-1}$ est le cardinal du p-Sylow de $\mu(F_v)$, et donc, si ζ_p désigne une racine p-ième de l'unité, on a

$$|\mu(F_v)| \neq \mathrm{N}v - 1 \Longleftrightarrow \zeta_p \in F_v.$$

Dans ce cas, la condition sur les degrés qui en résulte

$$[F : \mathbb{Q}] \geqslant [F_v : \mathbb{Q}_p] \geqslant [\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p - 1,$$

montre ainsi qu'il n'y a qu'un nombre fini de nombres premiers p, et donc de places v, pour lesquelles $|\mu(F_v)| \neq \mathrm{N}v - 1$. $\square$

1.6 Noyaux sauvages et modérés

• Les symboles de Hilbert définissent un morphisme

$$\begin{array}{rcl} \mathcal{H}: \quad K_2(F) & \to & \underset{v \text{ finie ou réelle}}{\oplus} \mu(F_v), \\ \{a,b\} & \mapsto & ((a,b)_v)_v \ . \end{array}$$

On appelle noyau sauvage de F, et on note $WK_2(F)$, le noyau de ce morphisme $\mathcal{H}$.

En gardant à l'esprit la formule du produit vérifiée par les symboles de Hilbert, on peut maintenant énoncer le

Théorème 1.28 (Moore). *On a une suite exacte*

$$0 \longrightarrow WK_2(F) \longrightarrow K_2(F) \xrightarrow{\mathcal{H}} \underset{v \textit{ finie ou réelle}}{\oplus} \mu(F_v) \xrightarrow{\Theta} \mu(F) \longrightarrow 0,$$

où Θ *est donnée par* $\Theta((\zeta_v)_v) = \prod_v \zeta_v^{\frac{|\mu(F_v)|}{|\mu(F)|}}$.

Démonstration. Voir [CW]. □

• De même, les symboles modérés définissent un morphisme

$$\begin{array}{rcl} \mathcal{M}: \quad K_2(F) & \to & \underset{v \text{ finie}}{\oplus} k_v^*, \\ \{a,b\} & \mapsto & (< a,b >_v)_v \ , \end{array}$$

dont le noyau coïncide avec le groupe $K_2(o_F)$ introduit à la section 1.3 (résultat bien connu, dû à D. Quillen ; voir [Q]). Par ailleurs, il découle du théorème de Moore que le morphisme $\mathcal{M}$ est surjectif. Autrement dit, on a la suite exacte

$$0 \longrightarrow K_2(o_F) \longrightarrow K_2(F) \xrightarrow{\mathcal{M}} \underset{v \text{ finie}}{\oplus} k_v^* \longrightarrow 0.$$

Dans la suite, on considèrera que $K_2(o_F) = \mathrm{Ker}(\mathcal{M})$ et on l'appellera noyau modéré de F.

H. Garland a montré que le groupe $K_2(o_F)$ est fini (voir [Ga]). Or la proposition 1.27 implique que le noyau sauvage $WK_2(F)$ est un sous-groupe du noyau modéré $K_2(o_F)$. Il en résulte que $WK_2(F)$ est un groupe fini. On peut même être un peu plus précis : on a le diagramme commutatif

$$\begin{tikzcd}
K_2(F) \arrow[r, "\mathcal{H}"] \arrow[d, "\mathcal{M}"'] & \bigoplus\limits_{v \text{ finie ou réelle}} \mu(F_v) \arrow[dl, "\phi"] \\
\bigoplus\limits_{v \text{ finie}} k_v^* &
\end{tikzcd}$$

où ϕ est défini par

$$\phi\left((\zeta_v)_{v \text{ finie ou réelle}}\right) = \left(\zeta_v^{\frac{|\mu(F_v)|}{|\mu(F)|}}\right)_{v \text{ finie}},$$

en identifiant encore k_v^* à un sous-groupe de $\mu(F_v)$. On a donc une suite exacte

$$0 \to \operatorname{Ker}\mathcal{H} \to \operatorname{Ker}\mathcal{M} \to \operatorname{Ker}\phi \to \operatorname{Coker}\mathcal{H} \to \operatorname{Coker}\mathcal{M} \to \operatorname{Coker}\phi \to 0.$$

En d'autres termes, on a grâce à la surjectivité de $\mathcal{M}$ la suite exacte

$$0 \to WK_2(F) \to K_2(o_F) \to \operatorname{Ker}\phi \to \mu(F) \to 0.$$

Or il est clair que

$$\operatorname{Ker}\phi = \Big(\bigoplus_{v \text{ réelle}} \mu_2\Big) \oplus \Big(\bigoplus_{v \text{ finie}} \operatorname{Ker}(\mu(F_v) \to k_v^*)\Big),$$

et, si $v|p$, $\operatorname{Ker}(\mu(F_v) \to k_v^*) \cong \mu(F_v)(p)$ puisque $\mu(F_v) \cong \mu(F_v)(p) \oplus k_v^*$.
Par conséquent, si l'on s'intéresse maintenant aux p-parties, *i.e.*, aux p-groupes de Sylow, pour un nombre premier p fixé, on obtient, pour p impair :

$$0 \to WK_2(F)(p) \to K_2(o_F)(p) \xrightarrow{\mathcal{H}_p} \bigoplus_{v|p} \mu(F_v)(p) \xrightarrow{\Theta_p} \mu(F)(p) \to 0,$$

et, pour $p = 2$:

$$0 \to WK_2(F)(2) \to K_2(o_F)(2) \xrightarrow{\mathcal{H}_2} \Big(\bigoplus_{v|2} \mu(F_v)(2)\Big) \oplus \Big(\bigoplus_{v \text{ réelle}} \mu_2\Big) \xrightarrow{\Theta_2} \mu(F)(2) \to 0.$$

Remarques :

1° Pour p quelconque, les morphismes $\mathcal{H}_p$ sont donnés par les symboles de Hilbert $(\ .\ ,\ .\ )_{F_v,|\mu(F_v)(p)|}$, à valeurs dans $\mu(F_v)(p)$ et les Θ_p sont obtenus en considérant le produit de tous les éléments, chacun élevé à la puissance $\frac{|\mu(F_v)(p)|}{|\mu(F)(p)|}$.

2° Comme on sait que $K_2(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ (cf la proposition 1.10), on déduit immédiatement des suites exactes précédentes que le groupe $WK_2(\mathbb{Q})$ est trivial.

1.7 Noyaux modérés positifs et noyaux modérés de l'anneau des S-entiers

Nous présentons ici deux objets dont la définition est proche de celle du noyau modéré $K_2(o_F)$. On verra leur utilité dans les prochains chapitres.

• On appelle noyau modéré positif de F, et on note $K_2(o_F)^+$, le noyau du morphisme

$$\begin{array}{rcl} K_2(o_F) & \to & \underset{v \text{ réelle}}{\oplus} \mu_2, \\ \{a,b\} & \mapsto & ((a,b)_v)_v \,. \end{array}$$

Le morphisme précédent étant surjectif, on a la suite exacte

$$0 \longrightarrow K_2(o_F)^+ \longrightarrow K_2(o_F) \longrightarrow \underset{v \text{ réelle}}{\oplus} \mu_2 \longrightarrow 0.$$

Comme à la section précédente, on peut montrer que, pour tout nombre premier p (impair ou pas), on a la suite exacte

$$0 \to WK_2(F)(p) \to K_2(o_F)^+(p) \to \underset{v|p}{\oplus} \mu(F_v)(p) \to \mu(F)(p) \to 0.$$

Il est à noter que, si E/F est une extension quadratique de corps de nombres, J. Hurrelbrink et M. Kolster ont proposé une méthode pour le calcul du 2-rang et du 4-rang de $K_2(o_E)^+$, sous réserve que $K_2(o_F)^+(2)$ soit triviale. Ce problème est évidemment lié de près à celui qui va nous concerner dans les prochains chapitres, à savoir celui de la détermination des 2-extensions de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale.

• Soit S_∞ l'ensemble des places infinies de F et S un ensemble de places de F contenant S_∞. On désigne par S_f les places finies de S. On dit que $x \in F$ est une S-unité si $v(x) = 0$ pour toute place v de F n'appartenant pas à S. L'anneau des S-entiers de F sera noté o_F^S. Alors, comme pour le noyau modéré, le groupe $K_2(o_F^S)$ coïncide avec le noyau du morphisme induit par $\mathcal{M}$:

$$K_2(F) \to \underset{v \notin S}{\oplus} k_v^*.$$

On a donc la suite exacte

$$0 \longrightarrow K_2(o_F^S) \longrightarrow K_2(F) \longrightarrow \underset{v \notin S}{\oplus} k_v^* \longrightarrow 0.$$

De plus, il est facile de constater l'exactitude de la suite

$$0 \longrightarrow K_2(o_F) \longrightarrow K_2(o_F^S) \longrightarrow \underset{v \in S_f}{\oplus} k_v^* \longrightarrow 0.$$

Pour obtenir un lien entre $WK_2(F)$ et $K_2(o_F^S)$, on procède comme on l'a déjà fait : à partir du diagramme commutatif

$$\begin{tikzcd}
K_2(F) \arrow[r, "\mathcal{H}"] \arrow[d, "\mathcal{M}"'] & \bigoplus_{v \text{ finie ou réelle}} \mu(F_v) \arrow[dl, "\varphi"] \\
\bigoplus_{v \notin S} k_v^* &
\end{tikzcd}$$

on obtient une suite exacte

$$0 \to WK_2(F) \to K_2(o_F^S) \to \operatorname{Ker} \varphi \to \mu(F) \to 0.$$

Or

$$\operatorname{Ker} \varphi = (\bigoplus_{v \text{ réelle}} \mu_2) \oplus (\bigoplus_{v \in S_f} \mu(F_v)) \oplus (\bigoplus_{v \notin S} \operatorname{Ker}(\mu(F_v) \to k_v^*)) \ .$$

On obtient ainsi un lien entre les p-parties de $WK_2(F)$ et $K_2(o_F^S)$: on a deux suites exactes, pour p impair,

$$0 \to WK_2(F)(p) \to K_2(o_F^S)(p) \to \bigoplus_{v \in S_f \text{ ou } v|p} \mu(F_v)(p) \to \mu(F)(p) \to 0,$$

et, pour $p = 2$,

$$0 \to WK_2(F)(2) \to K_2(o_F^S)(2) \to (\bigoplus_{v \text{ réelle}} \mu_2) \oplus (\bigoplus_{v \in S_f \text{ ou } v|2} \mu(F_v)(2)) \to \mu(F)(2) \to 0.$$

Chapitre 2

Formules de genre

Nous allons, dans ce chapitre, écrire une formule de genre pour les noyaux sauvages. Cette formule établie par M. Kolster et A. Movahhedi se révèlera par la suite d'un grand intérêt pour étudier l'éventuelle trivialité des noyaux sauvages de certaines extensions. Ce résultat est en quelque sorte l'analogue de la proposition suivante, à savoir la formule de genre (mieux connue) pour les groupes de classes d'idéaux.

Théorème 2.1 (Chevalley). *Soit E/F une extension cyclique de corps de nombres, de groupe de Galois G.*
Notons $e(E/F)$ le produit $\prod_v e(v)$ où v décrit l'ensemble des places (finies ou infinies) de F et $e(v)$ désigne l'indice de ramification de v dans E.
Alors, on a :

$$\frac{\mid Cl(E)_G \mid}{\mid Cl(F) \mid} = \frac{e(E/F)}{[E:F]\,[U_F : U_F \cap \mathrm{N}_{E/F}(E^*)]},$$

où U_F désigne le groupe des unités de F et $Cl(\cdot)$ le groupe de classes d'idéaux.

Démonstration. Voir, par exemple, Lemma 4.1. page 64 de [La]. □

Pour en revenir à la formule de genre pour les noyaux sauvages, elle porte sur la p-partie des noyaux sauvages (où p est un nombre premier) et elle est obtenue en étudiant l'application transfert

$$\mathrm{Tr}_{E/F} : WK_2(E)(p)_G \longrightarrow WK_2(F)(p),$$

associée à une extension cyclique E/F de corps de nombres de degré p. Cependant, les cas $p = 2$ et p impair se traitent de manières légèrement différentes, comme nous allons le voir. De plus, la formule de genre pour les noyaux sauvages fera aussi intervenir d'une certaine manière la ramification de l'extension E/F, mais l'indice normique apparaissant dans la formule dépendra non plus du groupe des unités U_F, mais d'un autre objet lié à F qui n'est rien d'autre que le noyau de Tate D_F (introduit à la section 1.4).

Enfin, signalons la raison pour laquelle nous nous intéressons à la formule de genre pour les noyaux sauvages. Rappelons d'abord que, pour tout nombre premier p, on a

$$WK_2(E)(p) = 0 \Longleftrightarrow WK_2(E)(p)^G = 0 \Longleftrightarrow WK_2(E)(p)_G = 0$$

(pour une démonstration, il suffit d'adapter la preuve de Lemma 1, Section 9, Chapter IV, [CF]). Par conséquent, l'objectif final de cette thèse étant d'étudier la trivialité des p-parties de noyaux sauvages, on pourra constater que cette formule qui calcule le cardinal de $WK_2(E)(p)_G$ est un outil relativement efficace.

D'autre part, nous reprenons dans ce chapitre la démonstration de la formule de genre ([KM2]) non seulement pour la détailler à quelques endroits mais aussi, et surtout, pour établir une légère amélioration inévitable pour obtenir les résultats des chapitres suivants. En effet, même dans le cas où le corps de base F est totalement réel, une indécision sur un coefficient ρ égal à 0 ou 1 peut intervenir lorsque l'on applique la formule de genre en pratique. Or, il s'est avéré que, contrairement aux travaux analogues effectués dans [KM2] ou [Gri], ce calcul de ρ était absolument nécessaire. On verra que ce calcul se ramène à celui (assez technique) de symboles de Hilbert.

Notations : si p est un nombre premier, lorsqu'il n'y a pas de confusion possible, on note $\mathbb{Q}_\infty$ la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$, et, si K est un corps local ou un corps de nombres, on note K_∞ la $\mathbb{Z}_p$-extension cyclotomique de K, *i.e.*, $K_\infty = K\mathbb{Q}_\infty$. Rappelons aussi qu'une p-extension de K désigne une extension galoisienne finie de K dont le groupe de Galois est un p-groupe.

2.1 Les morphismes d'extension et de transfert

2.1.1 Premières définitions et propriétés

Dans cette partie, on considère E/F une extension finie de corps, de degré $n = [E : F]$.

L'application canonique de $F^* \otimes_{\mathbb{Z}} F^*$ dans $E^* \otimes_{\mathbb{Z}} E^*$ induit par passage au quotient un morphisme de $K_2(F)$ dans $K_2(E)$, appelé morphisme d'extension et noté $i_{E/F}$ (ou i, s'il n'y a pas de confusion possible).

De plus, on peut aussi définir un morphisme naturel de $K_2(E)$ dans $K_2(F)$, appelé morphisme de transfert et noté $\mathrm{Tr}_{E/F}$ (ou Tr, s'il n'y a pas de confusion possible). La définition que l'on donne ici se trouve dans [Mi].

L'extension E/F étant de degré n, on peut définir un morphisme entre groupes parfaits

$$E_m(E) \longrightarrow E_{mn}(F)$$

en choisissant une base de E sur F. Si maintenant on applique le multiplicateur de Schur (proposition 1.12), on obtient un morphisme

$$H_2(\mathrm{E}_m(E), \mathbb{Z}) \longrightarrow H_2(\mathrm{E}_{mn}(F), \mathbb{Z}).$$

En passant à la limite directe lorsque $m \to +\infty$, on obtient

$$H_2(\mathrm{E}(E), \mathbb{Z}) \cong \lim_{m\to+\infty} H_2(\mathrm{E}_m(E), \mathbb{Z}) \longrightarrow \lim_{m\to+\infty} H_2(\mathrm{E}_{mn}(F), \mathbb{Z}) \cong H_2(\mathrm{E}(F), \mathbb{Z}).$$

Autrement dit, grâce à l'identification de $K_2(\Lambda)$ à $H_2(\mathrm{E}(\Lambda), \mathbb{Z})$ pour tout anneau Λ (proposition 1.12), on a donc défini ici un morphisme, que l'on appelle le transfert,

$$\mathrm{Tr}_{E/F} : K_2(E) \longrightarrow K_2(F).$$

Avant d'énoncer les principales propriétés des morphismes d'extension et de transfert, rappelons que si l'extension E/F est galoisienne de groupe de Galois $\mathrm{Gal}(E/F)$, alors $K_2(E)$ est un $\mathrm{Gal}(E/F)$-module dont l'action est induite par celle de $\mathrm{Gal}(E/F)$ sur E^*. Plus précisément, on a

$$\{a, b\}^\sigma = \{a^\sigma, b^\sigma\},\ \forall a, b \in E^*,\ \forall \sigma \in \mathrm{Gal}(E/F),$$

où $a^\sigma := \sigma(a)$.

Proposition 2.2. *Les morphismes d'extension et de transfert vérifient les égalités suivantes :*
(i) Si $x \in K_2(F)$, alors

$$\mathrm{Tr} \circ i(x) = x^n = x^{[E:F]}.$$

(ii) Si E/F est galoisienne et si $y \in K_2(E)$, alors

$$i \circ \mathrm{Tr}(y) = \prod_{\sigma\in\mathrm{Gal}(E/F)} y^\sigma.$$

(iii) Si $a \in F^*$ et si $b \in E^*$, alors

$$\mathrm{Tr}\{a, b\}_E = \{a, \mathrm{N}_{E/F}(b)\}_F \ .$$

(iv) Si $F \subset E \subset L$ est une tour d'extensions de corps, alors

$$i_{L/F} = i_{L/E} \circ i_{E/F} \ \textit{et} \ \mathrm{Tr}_{L/F} = \mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{L/E} \ .$$

(v) Pour l'action des automorphismes de Galois (relatifs à une clôture algébrique donnée), on a pour $x \in K_2(F)$ et $y \in K_2(E)$:

$$(i_{E/F}(x))^\sigma = i_{\sigma(E)/\sigma(F)}(x^\sigma) \ \textit{et} \ (\mathrm{Tr}_{E/F}(y))^\sigma = \mathrm{Tr}_{\sigma(E)/\sigma(F)}(y^\sigma).$$

2.1.2 Application au noyau de Tate

Soit F un corps de nombres totalement réel. On rappelle (voir page 24) que le noyau de Tate D_F de F est défini par :

$$D_F = \{x \in F^* \,/\, \{-1, x\}_F = 1 \text{ dans } K_2(F)\},$$

et que :

$$[D_F : F^{*2}] = 2.$$

Définissons une suite $(\alpha_k)_{k \geqslant 0}$ de réels positifs par :

$$\begin{cases} \alpha_0 = 0, \\ \alpha_{k+1} = \sqrt{2 + \alpha_k}. \end{cases}$$

Pour tout $n \geqslant 0$, fixons ζ_n une racine primitive n-ième de l'unité.

Lemme 2.3. *Pour tout $n \geqslant 0$, le n-ième étage $\mathbb{Q}_n$ de la $\mathbb{Z}_2$-extension cyclotomique $\mathbb{Q}_\infty$ de $\mathbb{Q}$ est $\mathbb{Q}(\alpha_n)$.*

Démonstration. Par définition, $\mathbb{Q}_n = \mathbb{Q}(\zeta_{n+2} + \zeta_{n+2}^{-1})$.
Or une récurrence facile montre que, pour tout $n \geqslant 0$, on a :

$$2 + \alpha_n = (\zeta_{n+3} + \zeta_{n+3}^{-1})^2 = 2 + \zeta_{n+2} + \zeta_{n+2}^{-1}. \tag{2.1}$$

D'où le résultat. □

Proposition 2.4. *Soit F un corps de nombres totalement réel. Soit n l'entier défini par $\mathbb{Q}_n = F \cap \mathbb{Q}_\infty$. Alors*

$$D_F/F^{*2} \ \textit{est engendré par la classe de} \ 2 + \alpha_n.$$

Démonstration. Par définition, on a

$$2+\alpha_n=\alpha_{n+1}^2.$$

Donc, si $2+\alpha_n$ était un carré dans F, alors $\mathbb{Q}_{n+1}$ serait contenue dans F, ce qui contredit la définition de n. D'où $2+\alpha_n \notin F^{*2}$.

Il reste donc à voir que $2+\alpha_n \in D_F$. Posons, pour cela, $E := F(\sqrt{-1})$. Alors l'égalité (2.1) implique que

$$2+\alpha_n=(1+\zeta_{n+2})(1+\zeta_{n+2}^{-1})=\mathrm{N}_{E/F}(1+\zeta_{n+2}).$$

On en déduit, avec le point (iii) de la proposition 2.2, que

$$\{-1,2+\alpha_n\}_F=\mathrm{Tr}_{E/F}\{-1,1+\zeta_{n+2}\}_E.$$

Mais, comme $-1=(\zeta_{n+2})^{2^{n+1}}$, on obtient :

$$\begin{aligned}\{-1,1+\zeta_{n+2}\}_E &= \{\zeta_{n+2},1+\zeta_{n+2}\}_E^{2^{n+1}}\\ &= \{-\zeta_{n+2},1+\zeta_{n+2}\}_E^{2^{n+1}}\,\{-1,1+\zeta_{n+2}\}_E^{2^{n+1}}.\end{aligned}$$

Or

$$\{-\zeta_{n+2},1+\zeta_{n+2}\}_E=1 \text{ et } \{-1,1+\zeta_{n+2}\}_E^{2^{n+1}}=\{+1,1+\zeta_{n+2}\}_E=1,$$

puisque $\{\,.\,,\,.\,\}_E$ est un symbole. D'où finalement

$$\{-1,1+\zeta_{n+2}\}_E=1 \text{ et donc } \{-1,2+\alpha_n\}_F=1.$$

□

2.1.3 Le transfert entre noyaux sauvages

On considère maintenant une extension E/F de corps de nombres. En connection avec la suite de Moore, on a (voir [BR]) le diagramme commutatif suivant

$$\begin{tikzcd} K_2(E) \arrow[r] \arrow[d, "\mathrm{Tr}"] & \bigoplus_v \big(\bigoplus_{w|v} \mu(E_w)\big) \arrow[r] \arrow[d, "\prod_v \varphi_v"] & \mu(E) \arrow[r] \arrow[d, "\varphi"] & 0 \\ K_2(F) \arrow[r] & \bigoplus_v \mu(F_v) \arrow[r] & \mu(F) \arrow[r] & 0 \end{tikzcd}$$

où φ_v et φ sont définies par

$$\begin{array}{rccc} \varphi_v : & \underset{w|v}{\oplus}\mu(E_w) & \to & \mu(F_v), \\ & (\zeta_w)_w & \mapsto & \prod_{w|v} \zeta_w^{\frac{|\mu(E_w)|}{|\mu(F_v)|}}, \end{array}$$

et

$$\begin{array}{rccc} \varphi : & \mu(E) & \to & \mu(F), \\ & \zeta & \mapsto & \zeta^{\frac{|\mu(E)|}{|\mu(F)|}}. \end{array}$$

Il en découle que le morphisme de transfert induit un morphisme $WK_2(E) \to WK_2(F)$ que l'on note encore Tr. De plus, si E/F est galoisienne de groupe de Galois G, alors on a (voir le point (v) de la proposition 2.2) :

$$\forall y \in K_2(E), \forall \sigma \in G, (\mathrm{Tr}_{E/F}(y))^\sigma = \mathrm{Tr}_{E/F}(y^\sigma).$$

Ainsi, on a un morphisme

$$\mathrm{Tr} : WK_2(E)_G \to WK_2(F).$$

Par un raisonnement analogue, on peut voir que le morphisme d'extension induit un morphisme $WK_2(F) \to WK_2(E)$ que l'on note encore i. De même (avec la proposition 2.2), on obtient un morphisme

$$i : WK_2(F) \to WK_2(E)^G.$$

Proposition 2.5. *Soit E/F une extension galoisienne de corps de nombres, de degré n quelconque et de groupe de Galois G. Alors les noyaux et conoyaux des morphismes $i : WK_2(F) \to WK_2(E)^G$ et $\mathrm{Tr} : WK_2(E)_G \to WK_2(F)$ sont annulés par n.*

Démonstration. Si $x \in \operatorname{Ker} i$, alors, d'après la proposition 2.2, on a

$$1 = \mathrm{Tr} \circ i(x) = x^{|G|} = x^n.$$

Si $y \in WK_2(E)^G$, alors, d'après la proposition 2.2, on a

$$i \circ \mathrm{Tr}(y) = \prod_{\sigma \in G} y^\sigma = \prod_{\sigma \in G} y = y^n,$$

donc $y^n = 1$ modulo $\operatorname{Im} i$.

De même, si $y \in WK_2(E)$ vérifie $\mathrm{Tr}(y) = 1$, on a

$$1 = i \circ \mathrm{Tr}(y) = \prod_{\sigma \in G} y^\sigma = \prod_{\sigma \in G} y \text{ modulo } I_G(WK_2(E)),$$

ce qui implique que $y^n = 1$ dans $WK_2(E)_G$.
Si maintenant $x \in WK_2(F)$, alors $\mathrm{Tr} \circ i(x) = x^{|G|} = x^n$, et donc $x^n = 1$ modulo $\mathrm{Im}\,\mathrm{Tr}$. D'où le résultat annoncé. $\square$

Corollaire 2.6. *Soit E/F une extension galoisienne de corps de nombres, de degré $n = [E : F]$ et de groupe de Galois G et p un nombre premier ne divisant pas n. Alors on a un isomorphisme*

$$\mathrm{Tr} : WK_2(E)(p)_G \xrightarrow{\simeq} WK_2(F)(p).$$

Démonstration. D'après la proposition précédente, on voit que les noyau et conoyau de ce morphisme sont annulés par $|G| = n$. De plus, ils sont aussi annulés par une certaine puissance de p. Noyau et conoyau sont donc triviaux. $\square$

On termine cette partie par un résultat sur le cas $p = 2$ qui se révèlera très utile par la suite.

Corollaire 2.7. *Soit E/F une extension quadratique de corps de nombres de groupe de Galois G. Supposons de plus que $WK_2(F)(2)$ est triviale. Alors, si $r = r_2(WK_2(E))$ désigne le 2-rang de $WK_2(E)$, on a :*

$$|WK_2(E)(2)_G| = 2^r.$$

Remarque : sous les hypothèses de ce corollaire, on constate que la formule de genre que l'on va énoncer au paragraphe 4 de ce chapitre donne en fait une formule pour le calcul du 2-rang du noyau sauvage de E.

Démonstration. Le groupe G étant cyclique, engendré par un certain σ, et $WK_2(E)(2)$ étant finie, il résulte de la suite exacte

$$0 \to WK_2(E)(2)^G \to WK_2(E)(2) \xrightarrow{\sigma-1} WK_2(E)(2) \to WK_2(E)(2)_G \to 0$$

l'égalité $|WK_2(E)(2)_G| = |WK_2(E)(2)^G|$. Le résultat provient alors du fait que $WK_2(E)(2)^G$ coïncide avec le groupe ${}_2WK_2(E)$ formé des éléments de $WK_2(E)$ annulés par 2. En effet, comme $WK_2(F)(2) = 0$, on a :

D'une part, si $y \in WK_2(E)(2)^G$, alors

$$1 = i \circ \mathrm{Tr}(y) = \prod_{\tau \in G} y^\tau = y\, y^\sigma = y^2.$$

D'autre part, si $y \in {}_2WK_2(E)$, on a en particulier $y^2 = 1$ ou encore $y^{-1} = y$; il découle alors des égalités suivantes

$$1 = i \circ \mathrm{Tr}(y) = \prod_{\tau \in G} y^\tau = y\, y^\sigma,$$

les relations $y^\sigma = y^{-1} = y$, et donc $y \in WK_2(E)(2)^G$. $\square$

2.2 Extensions cycliques de degré premier impair

Même si le but final de ce travail est de se concentrer sur le cas $p = 2$, on se propose de décrire dans ce paragraphe la situation lorsque p est impair ; pour cela, on reprend dans un cadre moins général les résultats démontrés dans [KM1].

Soit E/F une extension cyclique de corps de nombres, de degré un nombre premier impair p. Soit S_p l'ensemble des places de F divisant p et $ram(E/F)$ l'ensemble des places de F qui se ramifient dans E. Posons alors $S = S_p \cup ram(E/F)$.

Notons, de plus, $T_{E/F}$ l'ensemble des places v de S, non décomposées dans E et telles que, ou bien $\mu_p \subset F_v$, ou bien E_w n'est pas contenue dans la $\mathbb{Z}_p$-extension cyclotomique $F_{v,\infty}$ de F_v.

Proposition 2.8. *L'ensemble $T_{E/F}$ contient les places de F modérément ramifiées dans E ; en d'autres termes,*

$$S \setminus S_p \subset T_{E/F} \subset S.$$

Démonstration. Soit $v \in S \setminus S_p$; la place v est donc modérément ramifiée dans E. Si $w|v$, alors E_w/F_v est une extension totalement et modérément ramifiée, et donc, d'après [CF], Chapter I, Section 8, Proposition 1, on voit que $\mu_p \subset F_v$. D'où $v \in T_{E/F}$. □

Proposition 2.9. *L'application canonique*

$$WK_2(E)(p)_G \to WK_2(F)(p)$$

induite par le transfert est surjective si et seulement si l'une des conditions suivantes est satisfaite :
(i) $T_{E/F} \neq \emptyset$,
(ii) $T_{E/F} = \emptyset$ et, ou bien $\mu_p \not\subset F$, ou bien E est contenue dans la $\mathbb{Z}_p$-extension cyclotomique F_∞ de F.

Dans le cas exceptionnel où $T_{E/F} = \emptyset, \mu_p \subset F$ et $E \not\subset F_\infty$, le conoyau de $WK_2(E)(p)_G \to WK_2(F)(p)$ est cyclique d'ordre p.

Démonstration. Voir [KM1], Proposition 2.3. □

Exemple : Soit p un nombre premier irrégulier et posons $F = \mathbb{Q}(\mu_p)$.
Rappelons que p est dit irrégulier si p divise le cardinal du groupe de classes de $\mathbb{Q}(\mu_p)$.
Notons H le corps des classes de Hilbert de F (*i.e.*, l'extension abélienne non ramifiée maximale de F) et H' le corps des p-classes de Hilbert de F (*i.e.*, la p-extension abélienne non ramifiée maximale de F). Il est bien connu (cf [N] page 99 ou [W], page 399) que

$$\mathrm{Gal}(H/F) \cong Cl(F) \text{ et } \mathrm{Gal}(H'/F) \cong Cl(F)(p).$$

Maintenant, comme p est irrégulier, $H' \neq F$ et il existe une extension cyclique E de F, de degré p, qui est contenue dans H'. Nous allons montrer que $WK_2(E)(p)_G \to WK_2(F)(p)$ n'est pas surjective.

Notons d'abord que, si v est la place de F au-dessus de p, alors v se décompose dans E/F. En effet, comme $v = (1 - \zeta_p)$, où ζ_p est une racine primitive p-ième de l'unité, v est un idéal premier principal de F, qui se décompose donc totalement dans H (d'après [N], Chapter IV, Corollary 8.5). De là, il vient que $T_{E/F} = \emptyset$. De plus, il est facile de voir que $\mu_p \subset F$ et que $E \not\subset F_\infty$ (en regardant la ramification en p). On se trouve donc dans les conditions du cas exceptionnel cité précédemment, et par conséquent, $WK_2(E)(p)_G \to WK_2(F)(p)$ n'est pas surjective.

Proposition 2.10. *Si $T_{E/F} = \emptyset$, alors*

$$WK_2(E)(p)_G \cong WK_2(F)(p) \Longleftrightarrow (\mu_p \not\subset F \text{ ou } E \subset F_\infty).$$

Démonstration. Voir [KM1], Corollary 2.7. □

Remarque : dans une $\mathbb{Z}_p$-extension cyclotomique, les noyaux sauvages satisfont la codescente, tandis qu'en général ce n'est pas le cas pour les p-groupes de classes.

Nous allons maintenant écrire la formule de genre. Cependant, en comparaison de [KM1], nous l'énonçons avec une hypothèse supplémentaire dans un souci de simplification. Compte tenu de la proposition précédente, on peut se restreindre au cas où $T_{E/F} \neq \emptyset$:

Théorème 2.11. *Soit E/F une extension cyclique de degré premier impair p et de groupe de Galois G telle que $T_{E/F} \neq \emptyset$. Supposons que $\mu_p \subset F$ et qu'il existe une place v de $T_{E/F}$ qui est non décomposée dans le premier étage de*

la $\mathbb{Z}_p$-extension cyclotomique de F.
Alors $WK_2(E)(p)_G \to WK_2(F)(p)$ est surjective, et on a

$$\frac{|\ WK_2(E)(p)_G\ |}{|\ WK_2(F)(p)\ |} = \frac{p^{|T_{E/F}|-1}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]}.$$

Il est à noter que dans le cas où $\mu_p \not\subset F$, et sans la condition supplémentaire de non décomposition d'une place de $T_{E/F}$ dans le premier étage de F_∞, [KM1] (Theorem 2.11) fournit aussi une formule de genre, mais elle ne s'interprète pas en terme de noyau de Tate. Néanmoins, c'est cette formule améliorée qui permet d'établir en partie le résultat suivant :

Corollaire 2.12. *Soit M une p-extension de $\mathbb{Q}$. Alors :*

1) Si $p \geqslant 5$, alors $WK_2(M)(p) = 0$ si et seulement si M est un étage de la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$.

2) Si $p = 3$, alors $WK_2(M)(3) = 0$ si et seulement si, en dehors de 3, M est au-plus ramifiée en un nombre premier ℓ, qui est inerte dans la $\mathbb{Z}_3$-extension cyclotomique de $\mathbb{Q}$.

Remarque : lorsque p est impair, on a vu au chapitre 1, paragraphe 6 que l'on a une suite exacte

$$0 \to WK_2(M)(p) \to K_2(o_M)(p) \to \bigoplus_{v|p} \mu(M_v)(p) \to \mu(M)(p) \to 0.$$

Mais si, de plus, M est une p-extension, alors $\forall v|p,\ \mu(M_v)(p) = \mu(M)(p) = 1$. Par conséquent, avec la terminologie de [GrJ], on a les équivalences suivantes, valables pour toute p-extension M (où p est impair) :

$$\begin{aligned} WK_2(M)(p) = 0 &\iff K_2(o_M)(p) = 0 \\ &\iff M \text{ est } p-\text{régulier.} \end{aligned}$$

Or, si M contient le sous-corps réel maximal $\mathbb{Q}(\mu_p)^+$ du corps cyclotomique $\mathbb{Q}(\mu_p)$, alors M est p-régulier si et seulement si M est p-rationnel (dans la terminologie de [MN]). C'est la raison pour laquelle apparaît la distinction des cas $p = 3$ et $p \geqslant 5$ dans la proposition précédente, comme nous allons le constater dans la preuve qui suit.

Démonstration. Pour les raisons évoquées ci-dessus, nous ne donnons ici qu'un aperçu de la preuve. Intéressons-nous au cas où $p \geqslant 5$. Notons d'abord que l'extension p-ramifiée maximale de $\mathbb{Q}$, contenue dans M, est un étage $\mathbb{Q}_n$

de $\mathbb{Q}_\infty$. Maintenant, si $M = \mathbb{Q}_n$, la proposition 2.10 implique que $WK_2(M)(p) = 0$. Sinon, choisissons une tour d'extensions cycliques de degré p :

$$\mathbb{Q}_n = M_0 \subset M_1 \subset \cdots \subset M_r = M.$$

Puisque $T_{M_1/\mathbb{Q}_n} \neq \emptyset$, la formule de genre « améliorée » de [KM1] permet d'obtenir $WK_2(E)(p) \neq 0$ (admis). Quant aux extensions intermédiaires M_{k+1}/M_k, on voit (cf la proposition 2.9) que l'application canonique

$$WK_2(M_{k+1})(p)_{\mathrm{Gal}(M_{k+1}/M_k)} \to WK_2(M_k)(p),$$

est surjective, ce qui prouve que $WK_2(M)(p) \neq 0$. D'où le résultat pour $p \geqslant 5$.
Pour $p = 3$, il suffit de se reporter à la remarque précédente : on constate que M contient toujours $\mathbb{Q}(\mu_3)^+ = \mathbb{Q}$ et le résultat provient de [GrJ] ou [MN]. $\square$

2.3 Extensions relativement quadratiques

L'objectif de cette partie est d'étudier le morphisme de transfert

$$\mathrm{Tr} : WK_2(E)(p)_G \to WK_2(F)(p)$$

pour $p = 2$. Contrairement à ce qui précède dans le cas où p est impair, on se propose ici de reprendre partiellement l'article [KM2] en détaillant certaines démonstrations et en mettant l'accent sur les points essentiels de l'étude.

Fixons dès à présent quelques notations. Soit
E/F une extension relativement quadratique de corps de nombres,
G le groupe de Galois de E/F,
S_2 l'ensemble des places 2-adiques de F,
$ram(E/F)$ l'ensemble des places finies de F, qui se ramifient dans E,
S_∞ l'ensemble des places infinies réelles de F,
S_∞^r l'ensemble des places infinies réelles de F, qui se ramifient dans E,
S la réunion de S_2, de $ram(E/F)$ et de S_∞,
S_E l'ensemble des places non complexes de E vivant au-dessus d'une place de S,
o_F^S l'anneau des S-entiers de F,
o_E^S la clôture intégrale de o_F^S dans E.

On note aussi pour des places non complexes v de F et w de E :

$$n_v = |\mu(F_v)(2)| \text{ et } m_w = |\mu(E_w)(2)|,$$

ainsi que :

$$n = |\mu(F)(2)| \text{ et } m = |\mu(E)(2)|.$$

Proposition 2.13. *Le morphisme de transfert induit une suite exacte courte :*

$$0 \to K_2(o_E^S)_G \to K_2(o_F^S) \to \bigoplus_{v \in S_\infty^r} \mu_2 \to 0.$$

Démonstration. Voir [Ka], Théorème 5.1. □

Afin d'étudier le morphisme Tr : $WK_2(E)(2)_G \to WK_2(F)(2)$, on commence par rappeler un résultat de [Ha] (voir aussi [BR]) : nous avons un diagramme commutatif de G-modules, à lignes exactes :

$$\begin{tikzcd}
0 \arrow[r] & WK_2(E)(2) \arrow[r] \arrow[d, "\mathrm{Tr}"] & K_2(o_E^S)(2) \arrow[r] \arrow[d, "\mathrm{Tr}"] & \bigoplus_{v \in S \setminus S_\infty^r} \left(\bigoplus_{w|v} \mu(E_w)(2) \right) \arrow[r] \arrow[d, "\phi_S"] & \mu(E)(2) \arrow[r] \arrow[d, "\phi"] & 0 \\
0 \arrow[r] & WK_2(F)(2) \arrow[r] & K_2(o_F^S)(2) \arrow[r] & \bigoplus_{v \in S} \mu(F_v)(2) \arrow[r] & \mu(F)(2) \arrow[r] & 0
\end{tikzcd}$$

où ϕ_S et ϕ sont définies ci-après :

Pour toute place $v \in S \setminus S_\infty^r$ et toute place w divisant v, on définit

$$\begin{array}{rccc} \phi_{v,w} : & \mu(E_w)(2) & \to & \mu(F_v)(2), \\ & \zeta & \mapsto & \zeta^{\frac{m_w}{n_v}}. \end{array}$$

Posons alors

$$\phi_v = \prod_{w|v} \phi_{v,w} \quad \text{ et } \quad \phi_S = \bigoplus_{v \in S \setminus S_\infty^r} \phi_v.$$

De plus, on a aussi

$$\begin{array}{rccc} \phi : & \mu(E)(2) & \to & \mu(F)(2), \\ & \zeta & \mapsto & \zeta^{\frac{m}{n}}. \end{array}$$

Signalons que, pour une place $v \in S \setminus S_\infty^r$, l'action de G sur $\bigoplus_{w|v} \mu(E_w)(2)$ est donnée par

$$\sigma \cdot (\zeta_w)_w = (\zeta_w^\sigma)_{\sigma w},$$

où $\zeta_w^\sigma := \sigma(\zeta_w)$.

En considérant les G-invariants de la ligne supérieure dans le diagramme ci-dessus, on peut définir sans équivoque deux morphismes α et β de sorte que l'on ait :

$$K_2(o_E^S)(2)^G \xrightarrow{\alpha} \left(\bigoplus_{v \in S \smallsetminus S_\infty^r} \left(\bigoplus_{w|v} \mu(E_w)(2) \right) \right)^G \xrightarrow{\beta} \mu(E)(2)^G.$$

Alors, en tenant compte notamment de la proposition 2.13, [KM2] ont montré à travers une étude détaillée du diagramme précédent que

$$\operatorname{Coker}(WK_2(E)(2)_G \to WK_2(F)(2)) \cong \operatorname{Coker}\beta$$

et

$$\operatorname{Ker}(WK_2(E)(2)_G \to WK_2(F)(2)) \cong \operatorname{Ker}\beta / \operatorname{Im}\alpha.$$

• <u>**Étude du conoyau du transfert**</u>

Cette étude repose sur l'étude du diagramme commutatif suivant :

$$\begin{array}{ccccccccccc}
0 & \to & WK_2(F)(2) & \to & K_2(o_F^S)(2) & \longrightarrow & \bigoplus_{v \in S} \mu(F_v)(2) & \longrightarrow & \mu(F)(2) & \to & 0 \\
 & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle j} & & \\
0 & \to & WK_2(E)(2) & \to & K_2(o_E^S)(2) & \longrightarrow & \bigoplus_{w \in S_E} \mu(E_w)(2) & \to & \mu(E)(2) & \to & 0
\end{array}$$

où j_S et j sont définies ci-après :

Pour $v \in S \smallsetminus S_\infty^r$ et $w|v$, on considère un générateur ζ_w de $\mu(E_w)(2)$ et on forme l'élément $\zeta_v := {\zeta_w}^{\frac{m_w}{n_v}}$. Avec ces notations, on définit pour $v \in S \smallsetminus S_\infty^r$:

$$\begin{array}{rccc}
j_v : & \mu(F_v)(2) & \to & \bigoplus_{w|v} \mu(E_w)(2), \\
 & \zeta_v & \mapsto & \left(\mathrm{N}_{E_w/F_v}(\zeta_w)\right)_{w|v}.
\end{array}$$

Maintenant, on obtient l'application j_S du diagramme ci-dessus en composant l'application $\bigoplus_{v \in S \smallsetminus S_\infty^r} j_v$ avec la surjection naturelle $\bigoplus_{v \in S} \mu(F_v)(2) \longrightarrow \bigoplus_{v \in S \smallsetminus S_\infty^r} \mu(F_v)(2)$.

De manière analogue, on considère un générateur ζ_E de $\mu(E)(2)$ et on forme l'élément $\zeta_F := {\zeta_E}^{\frac{m}{n}}$. Alors, l'application j est donnée par

$$\begin{array}{rccc}
j : & \mu(F)(2) & \to & \mu(E)(2), \\
 & \zeta_F & \mapsto & \mathrm{N}_{E/F}(\zeta_E).
\end{array}$$

Afin d'étudier l'ordre de $\operatorname{Coker}(WK_2(E)(2)_G \to WK_2(F)(2)) \cong \operatorname{Coker}\beta$, intéressons-nous au diagramme suivant (que l'on déduit du précédent diagramme par passage aux invariants) :

$$\begin{tikzcd}
\bigoplus_{v\in S} \mu(F_v)(2) \arrow[r] \arrow[d, "j_S"] & \mu(F)(2) \arrow[r] \arrow[d, "j"] & 0 \\
\left(\bigoplus_{v\in S\setminus S_\infty^r} \left(\bigoplus_{w|v} \mu(E_w)(2)\right)\right)^G \arrow[r, "\beta"] & \mu(E)(2)^G &
\end{tikzcd}$$

Comme la flèche horizontale du haut est surjective, on voit que

$$\operatorname{Coker}\beta \cong \operatorname{Coker}\beta',$$

où $\beta' : \operatorname{Coker} j_S \to \operatorname{Coker} j$ est l'application naturelle induite par β. On est donc amené à étudier d'un peu plus près les applications j_S et j.

Étude des applications j_S et j

Notre but est ici de déterminer les noyaux et conoyaux des applications j_S et j. Pour ce qui concerne j_S, remarquons d'abord que l'on a le

Lemme 2.14. *Soit v une place de $S \setminus S_\infty^r$ qui se décompose dans E et, w et w' les deux places de E au-dessus de v. Alors $j_v : \mu(F_v)(2) \to (\mu(E_w)(2) \oplus \mu(E_{w'})(2))^G$ est un isomorphisme.*

Démonstration. En gardant les notations données dans la définition de j_v, on a $E_w = E_{w'} = F_v$, donc $\zeta_w = \zeta_{w'} = \zeta_v$ et $n_v = m_w = m_{w'}$. Par conséquent, pour $\zeta \in \mu(F_v)(2)$, on a $j_v(\zeta) = (\zeta, \zeta)$. Or, si σ engendre G, on a

$$\begin{aligned}
&(\mu(E_w)(2) \oplus \mu(E_{w'})(2))^G \\
&\quad = \{ (\zeta, \zeta') \in \mu(E_w)(2) \oplus \mu(E_{w'})(2) \ / \ (\zeta, \zeta') = (\zeta'^\sigma, \zeta^\sigma) \} \\
&\quad = \{ (\zeta, \zeta') \in \mu(E_w)(2) \oplus \mu(E_{w'})(2) \ / \ (\zeta, \zeta') = (\zeta', \zeta) \} \\
&\quad = \operatorname{Im} j_v.
\end{aligned}$$

D'où l'isomorphisme annoncé. $\square$

Par conséquent, pour étudier j_S, il nous reste à étudier j_v pour une place v de $S \setminus S_\infty^r$ non décomposée dans E. Afin de regrouper les études de j_S et de j, on va dorénavant prendre les notations suivantes : nous allons considérer une extension quadratique M/L de corps de nombres ou de corps locaux, de groupe de Galois G. Comme pour la définition des j_v ou de j, on considère un générateur ζ_M de $\mu(M)(2)$ et on forme l'élément $\zeta_L := \zeta_M^{\frac{|\mu(M)(2)|}{|\mu(L)(2)|}}$. On définit alors l'application $j_{M/L}$ par

$$\begin{array}{rccc} j_{M/L}: & \mu(L)(2) & \to & \mu(M)(2)^G, \\ & \zeta_L & \mapsto & \mathrm{N}_{M/L}(\zeta_M). \end{array}$$

Lemme 2.15. *En notant L_∞ la $\mathbb{Z}_2$-extension cyclotomique de L, on a :*

1. *Le conoyau de $j_{M/L}$ est isomorphe à $\mu(L)/\,\mathrm{N}_{M/L}(\mu(M))$.*
2. *L'application $j_{M/L}$ est un isomorphisme si et seulement si $|\mu(M)(2)| > |\mu(L)(2)|$ et $M \subset L_\infty$.*

Avant de démontrer ce lemme, nous devons décrire précisément l'action de G sur le groupe $\mu(M)(2)$. En effet, c'est l'un des points cruciaux qui distingue le cas $p = 2$ de celui de p impair.

Considérons fixé un générateur ζ_M de $\mu(M)(2)$ et notons s l'entier vérifiant $\mu(M)(2) = \mu_{2^s}$. Alors, pour tout τ de G, on peut écrire $\zeta_M^\tau = \zeta_M^{k_\tau}$, ce qui permet de définir un morphisme

$$\begin{array}{rccc} \psi: & G & \to & (\mathbb{Z}/2^s\mathbb{Z})^\times, \\ & \tau & \mapsto & k_\tau. \end{array}$$

À la différence du cas où p est impair, on sait que pour $s \geqslant 3$, le groupe $(\mathbb{Z}/2^s\mathbb{Z})^\times$ des éléments inversibles modulo 2^s n'est pas un groupe cyclique, et dans ce cas, $(\mathbb{Z}/2^s\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$. Néanmoins, comme ici G est d'ordre 2, on voit que l'on a que quatre possibilités pour $\psi(G)$, à savoir :

$$\psi(G) = 1 \text{ ou } < -1 > \text{ ou } < 1 + 2^{s-1} > \text{ ou } < -1 + 2^{s-1} >,$$

les deux derniers cas n'étant possibles que si $s \geqslant 3$.

Par ailleurs, il est clair que $\mu(M)(2)^G = \mu(L)(2)$, et, si on note σ le générateur de G, on peut maintenant s'intéresser aux quatre cas suivants :

* <u>1^er^ cas :</u> $\psi(G) = 1$, *i.e.*, $\zeta_M^\sigma = \zeta_M$. Alors
$$\mu(L)(2) = \mu(M)(2)^G = \mu(M)(2) = \mu_{2^s}.$$
* <u>2^ème^ cas :</u> $\psi(G) =< -1 >$, *i.e.*, $\zeta_M^\sigma = \zeta_M^{-1}$. Alors
$$\mu(L)(2) = \mu(M)(2)^G = \{\ \xi \ /\ \xi = \xi^{-1}\ \} = \mu_2.$$

* $\underline{3^{\text{ème}}\text{ cas :}}$ $s \geqslant 3$ et $\psi(G) =< 1 + 2^{s-1} >$, *i.e.*, $\zeta_M^\sigma = \zeta_M^{1+2^{s-1}}$. Alors

$$\mu(L)(2) = \mu(M)(2)^G = \{ \xi \ / \ \xi = \xi^{1+2^{s-1}} \} = \{ \xi \ / \ \xi^{2^{s-1}} = 1 \} = \mu_{2^{s-1}}.$$

* $\underline{4^{\text{ème}}\text{ cas :}}$ $s \geqslant 3$ et $\psi(G) =< -1 + 2^{s-1} >$, *i.e.*, $\zeta_M^\sigma = \zeta_M^{-1+2^{s-1}}$. Alors

$$\mu(L)(2) = \mu(M)(2)^G = \{ \xi \ / \ \xi = \xi^{-1+2^{s-1}} \} = \mu_2.$$

Démonstration. 1. Il est clair que

$$\operatorname{Coker} j_{M/L} \cong \mu(L)(2)/\operatorname{N}_{M/L}(\mu(M)(2)) \cong \mu(L)/\operatorname{N}_{M/L}(\mu(M)).$$

2. Si $\mu(M)(2) = \mu(L)(2)$, alors G agit trivialement sur $\mu(M)(2)$. Ainsi l'application norme $\operatorname{N}_{M/L} : \mu(M)(2) \to \mu(L)(2)$ est l'élévation au carré, et donc $|\operatorname{Ker} j_{M/L}| = |\operatorname{Coker} j_{M/L}| = 2$. En particulier, $j_{M/L}$ n'est pas un isomorphisme.

Supposons maintenant que $|\mu(M)(2)| > |\mu(L)(2)|$. Dans ce cas, $M = L(\zeta_M)$ et

$$M \subset L_\infty \Longleftrightarrow s \geqslant 3 \text{ et } G \text{ agit sur } \mu(M)(2) \text{ via } \zeta \mapsto \zeta^\sigma = \zeta^{\pm 1+2^{s-1}}.$$

Or sous ces conditions, l'application norme $\operatorname{N}_{M/L} : \mu(M)(2) \to \mu(L)(2)$ est surjective ; par conséquent, $j_{M/L}$ est un isomorphisme.

Dans le cas contraire, c'est-à-dire si G agit sur $\mu(M)(2)$ via $\zeta \mapsto \zeta^\sigma = \zeta^{-1}$, alors l'application norme $\operatorname{N}_{M/L} : \mu(M)(2) \to \mu(L)(2)$ est triviale, et $j_{M/L}$ n'est pas un isomorphisme. On peut même remarquer que $|\operatorname{Ker} j_{M/L}| = |\operatorname{Coker} j_{M/L}| = 2$, puisque $\mu(L)(2) = \mu(M)(2)^G = \mu_2$. □

Remarque : on constate en fait que, lorsque $j_{M/L}$ n'est pas un isomorphisme, ses noyau et conoyau sont toujours d'ordre 2.

Retour à l'étude du conoyau du transfert

D'après tout ce qui précède, on peut déjà noté que

$$\operatorname{Coker}(WK_2(E)(2)_G \to WK_2(F)(2)) \cong \operatorname{Coker} \beta \cong \operatorname{Coker} \beta'$$

est d'ordre inférieur ou égal à 2.

Soit $\boldsymbol{T_{E/F}}$ l'ensemble fini formé des places de F qui se ramifient modérément dans E et des places 2-adiques v de F qui sont non décomposées dans E et qui vérifient, soit $\mu(E_w)(2) = \mu(F_v)(2)$, soit $E_w \not\subset F_{v,\infty}$, où w désigne la place de E au-dessus de v. Autrement dit (voir le lemme 2.15) on voit que l'ensemble $T_{E/F}$ correspond à l'ensemble des places finies v de F pour lesquelles le morphisme $j_v : \mu(F_v)(2) \to \left(\underset{w|v}{\oplus} \mu(E_w)(2)\right)^G$ n'est pas un isomorphisme. En particulier, on obtient le diagramme commutatif :

$$\begin{tikzcd}
0 \arrow[d] & & 0 \arrow[d] & \\
\left(\underset{v\in T_{E/F}}{\oplus} \mu_2\right) \oplus \left(\underset{v\in S_\infty^r}{\oplus} \mu_2\right) \arrow[rr] \arrow[d] & & \operatorname{Ker} j \arrow[d] & \\
\underset{v\in S}{\oplus} \mu(F_v)(2) \arrow[rr] \arrow[d, "j_S"] & & \mu(F)(2) \arrow[r] \arrow[d, "j"] & 0 \\
\left(\underset{v\in S\setminus S_\infty^r}{\oplus} \left(\underset{w|v}{\oplus} \mu(E_w)(2)\right)\right)^G \arrow[rr, "\beta"] \arrow[d] & & \mu(E)(2)^G \arrow[d] & \\
\underset{v\in T_{E/F}}{\oplus} \mu(F_v)/\operatorname{N}_{E_w/F_v}(\mu(E_w)) \arrow[rr, "\beta'"] \arrow[d] & & \operatorname{Coker} j \arrow[d] & \\
0 & & 0 &
\end{tikzcd}$$

Grâce à l'ensemble $T_{E/F}$ défini précédemment, nous sommes maintenant en mesure de déterminer des conditions nécessaires et suffisantes pour la surjectivité du morphisme de transfert. En effet, si j est un isomorphisme, β' est clairement surjective, et sinon β' est surjective si et seulement si il existe une place v de $T_{E/F}$ telle que la restriction β'_v de β' à $\operatorname{Coker} j_v$ est aussi surjective. Notons que

$$\beta'_v : \operatorname{Coker} j_v = \mu(F_v)/\operatorname{N}_{E_w/F_v}(\mu(E_w)) \to \operatorname{Coker} j = \mu(F)/\operatorname{N}_{E/F}(\mu(E))$$

consiste en l'élévation à la puissance m_w/m. Cependant, si l'on note ζ_v un générateur de $\mu(F_v)(2)$ de sorte que ce soit un représentant du générateur de $\operatorname{Coker} j_v$, on voit que β'_v est surjective si et seulement si $\zeta_v^{\frac{m_w}{m}}$ engendre $\mu(F)(2)$, *i.e.*, si $\frac{m_w}{m} = \frac{n_v}{n}$. On en déduit la

Proposition 2.16. *Soit E/F une extension quadratique de corps de nombres. Alors le morphisme de transfert $WK_2(E)(2)_G \to WK_2(F)(2)$ est surjectif si* *et seulement si l'une des conditions suivantes est satisfaite :*

(i) $E \subset F_\infty = F(\mu_{2^\infty})$ *;*

(ii) $E = F(\sqrt{-1}) \not\subset F_\infty$ *et* $\exists v \in T_{E/F},\ \mu(E_w)(2) = \mu(E)(2)$ *où* $w|v$ *;*

(iii) $\exists v \in T_{E/F},\ \mu(E_w)(2) = \mu(F_v)(2)$ *où* $w|v$.

Sinon, le conoyau est d'ordre 2.

Démonstration. Le cas (i) correspond au cas où j est un isomorphisme (cf le lemme 2.15) : on est dans la situation où $|\mu(E)(2)| > |\mu(F)(2)|$ et $E \subset F_\infty$.

On se place maintenant dans le cas où j n'est pas un isomorphisme : ainsi, ou bien $|\mu(E)(2)| = |\mu(F)(2)|$ (*i.e.*, $m = n$), ou bien $|\mu(E)(2)| > |\mu(F)(2)|$ et $E \not\subset F_\infty$. Dans le cas où $m > n$ et $E \not\subset F_\infty$, la démonstration du lemme 2.15 implique que G agit via $\zeta \mapsto \zeta^{-1}$, et donc $n = |\mu(F)(2)| = 2$. On en déduit que $E = F(\sqrt{-1})$ et, si l'on considère une place $v \in T_{E/F}$, elle est non décomposée dans E et donc $n_v = |\mu(F_v)(2)| = 2$. On a alors $\frac{m_w}{m} = \frac{n_v}{n}$ si et seulement si $m_w = m$, *i.e.*, si $\mu(E_w)(2) = \mu(E)(2)$. D'où le cas (ii).
Si $m = n$, l'égalité $\frac{m_w}{m} = \frac{n_v}{n}$ est satisfaite si et seulement si $m_w = n_v$, *i.e.*, si $\mu(E_w)(2) = \mu(F_v)(2)$.

Par conséquent, on a montré que le morphisme de transfert $WK_2(E)(2)_G \to WK_2(F)(2)$ est surjectif si et seulement si l'une des conditions (i), (ii) ou (iii') est satisfaite, où la condition (iii') est la suivante :

$$\text{(iii')}\ m = n \text{ et } \exists v \in T_{E/F} \ /\ \mu(E_w)(2) = \mu(F_v)(2) \text{ où } w|v.$$

Il est alors clair que si le transfert est surjectif, alors (i), (ii) ou (iii) est satisfaite. Réciproquement, il reste à voir que si (iii) est vérifiée, alors le transfert est surjectif. Supposons donc que (iii) est satisfaite, *i.e.*, supposons que $\exists v \in T_{E/F},\ m_w = n_v$. Alors :
- ou bien $m = n$, et on est ramené au cas (iii') ;
- ou bien $m > n$ et $E \subset F_\infty$, et on retrouve (i) ;
- ou bien $m > n$ et $E \not\subset F_\infty$: alors, comme on l'a vu précédemment dans cette preuve, on a $n = 2$ et $E = F(\sqrt{-1})$. D'où $n_v = 2$, ce qui contredit $m_w = n_v$.

D'où le résultat. □

Corollaire 2.17. *Si l'extension quadratique E/F est modérément ramifiée, alors le morphisme de transfert $WK_2(E)(2)_G \to WK_2(F)(2)$ est surjectif.*

Démonstration. La condition (iii) est toujours satisfaite pour une place modérément ramifiée de F. En effet, localement, les corps résiduels sont les mêmes. $\square$

• Étude du noyau du transfert

On reprend l'un des diagrammes déjà vus, duquel on déduit le suivant :

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & & \operatorname{Ker} i \arrow[r] \arrow[d] & \operatorname{Ker} j_S \arrow[r] \arrow[d] & \operatorname{Ker} j \arrow[d] & \\
0 \arrow[r] & WK_2(F)(2) \arrow[r] \arrow[d, "i"] & K_2(o_F^S)(2) \arrow[r] \arrow[d, "i"] & \bigoplus_{v\in S} \mu(F_v)(2) \arrow[r] \arrow[d, "j_S"] & \mu(F)(2) \arrow[r] \arrow[d, "j"] & 0 \\
0 \arrow[r] & WK_2(E)(2)^G \arrow[r, "\gamma"] \arrow[d] & K_2(o_E^S)(2)^G \arrow[r, "\alpha"] \arrow[d] & \Big(\bigoplus_{w\in S_E} \mu(E_w)(2)\Big)^G \arrow[r, "\beta"] \arrow[d] & \mu(E)(2)^G \arrow[d] & \\
 & WK_2(E)(2)^G/\operatorname{Im} WK_2(F)(2) \arrow[r, "\gamma'"] \arrow[d] & \operatorname{Coker} i \arrow[r, "\alpha'"] \arrow[d] & \operatorname{Coker} j_S \arrow[r, "\beta'"] \arrow[d] & \operatorname{Coker} j \arrow[d] & \\
 & 0 & 0 & 0 & 0 &
\end{tikzcd}$$

où $\operatorname{Im} WK_2(F)(2)$ désigne l'image de $WK_2(F)(2)$ par i.
Rappelons que l'on a aussi vu que

$$\operatorname{Ker}(WK_2(E)(2)_G \to WK_2(F)(2)) \cong \operatorname{Ker} \beta / \operatorname{Im} \alpha.$$

Or une étude détaillée du diagramme ci-dessus mène au Lemma 2.3 de [KM2] qui affirme que l'on a la suite exacte $(*)$ suivante :

$$0 \to \operatorname{Ker} \alpha' / \operatorname{Im} \gamma' \to \operatorname{Coker}(\operatorname{Ker} j_S \to \operatorname{Ker} j) \to \operatorname{Ker} \beta / \operatorname{Im} \alpha \to \operatorname{Ker} \beta' / \operatorname{Im} \alpha' \to 0.$$

Nous allons bientôt pouvoir énoncer la formule de genre voulue. Néanmoins, même si l'on ne comprendra que pourquoi plus tard, il faut d'abord s'intéresser à déterminer l'ordre de $\operatorname{Im} \alpha'$.

Détermination de l'ordre de l'image de α'

Posons $E = F(\sqrt{\delta})$ et notons D_F et D_E les noyaux de Tate de F et E. Pour un corps local M, désignons par D_M le noyau du morphisme

$$\begin{array}{ccc} M^* & \to & \mu_2, \\ x & \mapsto & (-1, x)_{|\mu(M)(2)|}, \end{array}$$

où, comme d'habitude, $(\cdot,\cdot)_{|\mu(M)(2)|}$ est le symbole de Hilbert à valeurs dans $\mu(M)(2)$.

Pour $\epsilon \in D_F$, le symbole $\{\sqrt{\delta},\epsilon\}$ est un élément de $K_2(o_E^S)^G$ et le groupe quotient $K_2(o_E^S)^G/\operatorname{Im} K_2(o_F^S)(2)$ est engendré par les classes des symboles $\{\sqrt{\delta},\epsilon\}$, où ϵ parcourt D_F (cf [Ka], Théorème 2.3). Ainsi, par des arguments de cohomologie, [KM2] montre que l'application

$$\{\sqrt{\delta},\epsilon\} \bmod \operatorname{Im} K_2(o_F)(2) \mapsto \epsilon \bmod F^{*2}\,\mathrm{N}_{E/F}(D_E)$$

fournit un isomorphisme

$$K_2(o_E^S)(2)^G/\operatorname{Im} K_2(o_F)(2) \cong D_F/F^{*2}\,\mathrm{N}_{E/F}(D_E).$$

De façon analogue, si M/L est une extension quadratique de corps locaux de groupe de Galois G avec $M = L(\sqrt{\delta})$ et si $\epsilon \in D_L$, alors l'application

$$(\sqrt{\delta},\epsilon)_{|\mu(M)(2)|} \bmod j_{M/L}(\mu(L)(2)) \mapsto \epsilon \bmod L^{*2}\,\mathrm{N}_{M/L}(D_M)$$

fournit un isomorphisme

$$\mu(M)(2)^G/j_{M/L}(\mu(L)(2)) \cong D_L/L^{*2}\,\mathrm{N}_{M/L}(D_M).$$

Si maintenant on note $T^0_{E/F}$ l'ensemble des places 2-adiques v de $T_{E/F}$ telles que $E_w = F_v(\sqrt{-1})$ et $T^1_{E/F} = T_{E/F} \setminus T^0_{E/F}$, on a le digramme commutatif à lignes exactes (voir [KM2]) :

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
D_F \cap \mathrm{N}_{E/F}(E^*)/F^{*2}\,\mathrm{N}_{E/F}(D_E) \arrow[r, "\alpha'_0"] \arrow[d] & \bigoplus_{v\in T^0_{E/F}} D_{F_v}/F_v^{*2}\,\mathrm{N}_{E_w/F_v}(D_{E_w}) \arrow[d] \\
D_F/F^{*2}\,\mathrm{N}_{E/F}(D_E) \arrow[r, "\alpha'"] \arrow[d] & \bigoplus_{v\in T_{E/F}} D_{F_v}/F_v^{*2}\,\mathrm{N}_{E_w/F_v}(D_{E_w}) \arrow[d] \\
D_F/D_F \cap \mathrm{N}_{E/F}(E^*) \arrow[r, "\alpha'_1"] \arrow[d] & \bigoplus_{v\in T^1_{E/F}} D_{F_v}/F_v^{*2}\,\mathrm{N}_{E_w/F_v}(D_{E_w}) \arrow[d] \\
0 & 0
\end{tikzcd}$$

où α'_1 est en fait injective. Par conséquent, une simple application du lemme du serpent montre que

$$|\operatorname{Im}\alpha'| = |\operatorname{Im}\alpha'_0|\,|\operatorname{Im}\alpha'_1|.$$

Or, comme α'_1 est injective, $|\operatorname{Im}\alpha'_1| = [D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]$. Soit $r_{E/F}$ l'entier tel que $|\operatorname{Im}\alpha'_0| = 2^{r_{E/F}}$. Ainsi,

$$|\operatorname{Im}\alpha'| = [D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]\, 2^{r_{E/F}}.$$

Remarque : dans le cas où le corps de base F est totalement réel, on peut montrer que $r_{E/F} = 0$ (cf [KM2], Corollary 2.6).

Retour à la formule de genre

Nous sommes maintenant en mesure d'énoncer le résultat qui se révèlera essentiel pour les chapitres à venir, à savoir la formule de genre pour les 2-parties des noyaux sauvages :

Proposition 2.18 (Formule de genre). *Soit E/F une extension quadratique de corps de nombres, de groupe de Galois G.*

(a) Si $E \subset F_\infty$ et si $|\mu(E)(2)| > |\mu(F)(2)|$, alors $WK_2(E)(2)_G \cong WK_2(F)(2)$.

(b) Si une place infinie réelle de F se ramifie dans E, ou bien si $\mu(F_v)(2) = \mu(F)(2)$ pour une place $v \in T_{E/F}$, alors

$$\frac{|\, WK_2(E)(2)_G \,|}{|\, WK_2(F)(2) \,|} = \frac{2^{|T_{E/F}| - r_{E/F} - 1}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]}.$$

(c) Dans tous les autres cas,

$$\frac{|\, WK_2(E)(2)_G \,|}{|\, WK_2(F)(2) \,|} = \frac{2^{|T_{E/F}| - \rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]},$$

où $\rho = 0$ ou $\rho = 1$.

Démonstration. Rappelons d'abord que

$$\operatorname{Coker}(WK_2(E)(2)_G \to WK_2(F)(2)) \cong \operatorname{Coker}\beta \cong \operatorname{Coker}\beta'$$

et que

$$\operatorname{Ker}(WK_2(E)(2)_G \to WK_2(F)(2)) \cong \operatorname{Ker}\beta / \operatorname{Im}\alpha.$$

Ainsi, on a

$$\frac{|\, WK_2(E)(2)_G \,|}{|\, WK_2(F)(2) \,|} = \frac{|\operatorname{Ker}\beta|}{|\operatorname{Im}\alpha|\,|\operatorname{Coker}\beta'|}.$$

Sous les hypothèses de (a), l'ensemble $T_{E/F}$ est vide (revenir à la définition de $T_{E/F}$) et l'application j est un isomorphisme (voir le lemme 2.15). Par conséquent, comme j est injectif et j_S est surjective, une chasse dans le diagramme de la page 53 implique que $\operatorname{Ker}\beta = \operatorname{Im}\alpha$. De plus, j étant un isomorphisme, on a déjà signaler que cela force la surjectivité de β'. D'où l'isomorphisme annoncé.

Dans le cas (b), j n'est pas un isomorphisme. En effet, si une place infinie réelle de F se ramifie dans E, *i.e.*, si $S_\infty^r = \emptyset$, alors $E \not\subset F_\infty$. De plus, si $\mu(F_v)(2) = \mu(F)(2)$ pour une place $v \in T_{E/F}$ et si $E \subset F_\infty$, alors $v|2$ et $\mu(E_w)(2) = \mu(F_v)(2)$. Donc $\mu(E_w)(2) = \mu(F_v)(2) = \mu(F)(2) = \mu(E)(2)$.

Maintenant les hypothèses de (b) traduisent exactement la surjectivité de l'application $\operatorname{Ker} j_S \to \operatorname{Ker} j$; en effet, cette application

$$(\bigoplus_{v\in T_{E/F}} \mu_2) \oplus (\bigoplus_{v\in S_\infty^r} \mu_2) \to \mu_2$$

n'est autre que le produit de toutes les composantes élevées à la puissance $|\mu(F_v)(2)|/|\mu(F)(2)|$. Par conséquent, la suite exacte $(*)$ de la page 53 fournit l'isomorphisme

$$\operatorname{Ker}\beta/\operatorname{Im}\alpha \cong \operatorname{Ker}\beta'/\operatorname{Im}\alpha'.$$

D'où

$$\frac{|\,WK_2(E)(2)_G\,|}{|\,WK_2(F)(2)\,|} = \frac{|\operatorname{Ker}\beta'|}{|\operatorname{Im}\alpha'|\,|\operatorname{Coker}\beta'|}.$$

Or

$$\frac{|\operatorname{Ker}\beta'|}{|\operatorname{Coker}\beta'|} = \frac{|\operatorname{Coker} j_S|}{|\operatorname{Coker} j|} = \frac{2^{|T_{E/F}|}}{2}.$$

D'où le résultat.

(c) Définissons $\rho \in \{0,1\}$ par

$$2^\rho = |\operatorname{Ker}\alpha'/\operatorname{Im}\gamma'|.$$

Ici le conoyau de l'application $\operatorname{Ker} j_S \to \operatorname{Ker} j$ est d'ordre 2, et la suite exacte $(*)$ donne

$$\frac{|\,WK_2(E)(2)_G\,|}{|\,WK_2(F)(2)\,|} = \frac{2}{2^\rho}\,\frac{|\operatorname{Ker}\beta'|}{|\operatorname{Im}\alpha'|\,|\operatorname{Coker}\beta'|}.$$

De plus, on voit que $T_{E/F}^0 = \emptyset$ (puisque ici, pour toute place $v \in T_{E/F}$, on a $n_v > n$), et donc $r_{E/F} = 0$. On conclut alors comme au cas (b). $\square$

Corollaire 2.19. *Soit E/F une extension de corps de nombres de groupe de Galois G. Si l'on suppose de plus que F est totalement réel, alors*

$$\frac{|\, WK_2(E)(2)_G \,|}{|\, WK_2(F)(2) \,|} = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]},$$

où $\rho \in \{0,1\}$. Par ailleurs, si une place infinie réelle de F se ramifie dans E, ou bien si $\mu(F_v)(2) = \mu(F)(2)$ pour une place $v \in T_{E/F}$, alors $\rho = 1$; c'est en particulier le cas si E/F est une extension CM.

Rappelons qu'une extension CM est une extension quadratique totalement imaginaire d'un corps de nombres totalement réel.

Démonstration. Lorsque F est totalement réel, on voit, d'une part, que le cas (a) de la formule de genre 2.18 est impossible, et d'autre part, $r_{E/F} = 0$ dans le cas (b). $\square$

Remarque : dans le cas (c) de la formule de genre 2.18, il y a des extensions E/F pour lesquelles $\rho = 0$ et d'autres pour lesquelles $\rho = 1$ (cf [KM2]). En fait, on peut être plus précis concernant la valeur de ρ, comme nous allons le voir maintenant.

Plaçons-nous sous les hypothèses du cas (c). Alors

$$\rho = 0 \Longleftrightarrow \operatorname{Ker} \alpha' = \operatorname{Im} \gamma',$$

et nous sommes amenés à décider quand l'inclusion $\operatorname{Ker} \alpha' \subset \operatorname{Im} \gamma'$ a lieu.

Comme $T^0_{E/F} = \emptyset$, on a, avec le diagramme page 55, l'isomorphisme

$$\operatorname{Ker} \alpha' \cong D_F \cap \mathrm{N}_{E/F}(E^*)/F^{*2}\, \mathrm{N}_{E/F}(D_E).$$

Considérons alors $\epsilon \in D_F$ et supposons que $\epsilon = \mathrm{N}_{E/F}(\eta)$ pour un certain $\eta \in E^*$. Comme on l'a déjà fait remarquer, la classe de ϵ est représentée par $\{\sqrt{\delta}, \epsilon\} \in K_2(o_E^S)$. Or, si φ est un générateur du groupe de Galois de E/F, on a :

$$\{\sqrt{\delta}, \epsilon\} = \{\sqrt{\delta}, \eta\}\{\sqrt{\delta}, \eta^{\varphi}\} = \{\sqrt{\delta}, \eta\}\{\sqrt{\delta}, \eta\}^{\varphi}\{-1, \eta\},$$

dans $K_2(E)^G$, ce qui implique que la classe de ϵ est représentée dans $K_2(E)^G$ par $\{-1, \eta\}$.

Par ailleurs, compte tenu du chapitre précédent, on obtient le diagramme commutatif suivant :

$$\begin{array}{ccccccc} 0 \longrightarrow & K_2(o_F^S) & \longrightarrow & K_2(F) & \longrightarrow & \bigoplus\limits_{v \notin S} k_v^* & \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \longrightarrow & K_2(o_E^S)^G & \longrightarrow & K_2(E)^G & \longrightarrow & \left(\bigoplus\limits_{w \notin S_E} k_w^* \right)^G & \end{array}$$

Mais, puisque l'ensemble S contient les places de F ramifiées dans E, la flèche verticale de droite dans le diagramme ci-dessus est un isomorphisme. On obtient alors par le lemme du serpent l'isomorphisme :

$$K_2(o_E^S)^G / \operatorname{Im} K_2(o_F^S) \cong K_2(E)^G / \operatorname{Im} K_2(F).$$

Il en résulte un diagramme commutatif à lignes supérieures exactes :

$$\begin{array}{ccccccc} 0 & \longrightarrow & WK_2(F)(2) & \longrightarrow & K_2(F)(2) & \longrightarrow & \bigoplus\limits_v \mu(F_v)(2) \\ & & \downarrow & & \downarrow & & \downarrow j_S \\ 0 & \longrightarrow & WK_2(E)(2)^G & \xrightarrow{\gamma} & K_2(E)(2)^G & \xrightarrow{\alpha} & (\bigoplus\limits_w \mu(E_w)(2))^G \\ & & \downarrow & & \downarrow & & \downarrow \\ & & WK_2(E)(2)^G / \operatorname{Im} WK_2(F)(2) & \xrightarrow{\gamma'} & D_F / F^{*2} \mathrm{N}_{E/F}(D_E) & \xrightarrow{\alpha'} & \bigoplus\limits_{v \in T_{E/F}} D_{F_v} / F_v^{*2} \mathrm{N}_{E_w/F_v}(D_{E_w}) \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

Remarquons d'abord que si v est une place de $T_{E/F}$ et si w est la place de E au-desus de v, alors les symboles locaux $(-1, \eta)_{m_w}$ sont triviaux. En effet, par hypothèse sur ϵ et η, on voit que $(-1, \eta)_{m_w} \in \operatorname{Im} j_v$. Or, si $m_w > n_v$, la preuve du lemme 2.15 montre que j_v est l'application triviale. D'autre part, si $m_w = n_v$, le point (vii) de la proposition 1.23 implique que

$$(-1, \eta)_{m_w} = (-1, \mathrm{N}_{E/F}(\eta))_{n_v} = (-1, \epsilon)_{n_v} = 1,$$

puisque $\epsilon \in D_F$.

Pour $v \notin T_{E/F}$, l'application $j_v : \mu(F_v)(2) \to (\bigoplus\limits_{w|v} \mu(E_w)(2))^G$ est un isomorphisme, et donc pour ces places v, il existe $x_v \in F_v$ tel que $(-1, x_v)_{n_v} = (-1, \eta)_{m_w}$ pour toute place w divisant v. Ainsi, on peut constater, en effectuant une chasse dans le diagramme précédent, que

$$\epsilon \in \operatorname{Im} \gamma' \Longleftrightarrow \prod_v (-1, x_v)_{n_v}{}^{\frac{n_v}{n}} = 1.$$

En d'autres termes, définissons s_η le nombre de places $v \notin T_{E/F}$ telles que $(-1, x_v)_{n_v} = -1$ et $\mu(F_v)(2) = \mu(F)(2)$; en remarquant que s_η ne dépend que de la classe de ϵ, on définit $\rho_\epsilon = 0$ si s_η est pair, et 1 si s_η est impair. D'où

$$\prod_v (-1, x_v)_{n_v}{}^{\frac{n_v}{n}} = 1 \Longleftrightarrow \rho_\epsilon = 0.$$

En conclusion, on voit que

$$\rho = 0 \Longleftrightarrow \rho_\epsilon = 0 \text{ pour tout } [\epsilon] \in D_F \cap \mathrm{N}_{E/F}(E^*)/F^{*2}\,\mathrm{N}_{E/F}(D_E).$$

Malgré les apparences, les remarques précédentes permettent le calcul « explicite » de ρ dans certains cas précis. Un premier exemple d'un calcul de ce type est donné dans le prochain chapitre où l'on détermine ρ pour les corps quadratiques.

Chapitre 3

Corps quadratiques

Historiquement, la détermination des corps quadratiques dont la 2-partie du noyau sauvage est triviale est une conséquence directe de l'article [BS] de J. Browkin et A. Schinzel, où est notamment calculé le 2-rang du noyau sauvage d'un corps quadratique. Dans la première partie de ce chapitre, nous proposons une première application de la formule de genre en retrouvant le résultat de [BS] concernant le 2-rang du noyau sauvage d'un corps quadratique. Puis, dans une seconde partie, nous allons expliquer comment l'on déduit du calcul du 2-rang le théorème suivant :

Théorème 3.1. *Les corps quadratiques dont la 2-partie du noyau sauvage est triviale sont les corps $\mathbb{Q}(\sqrt{d})$ où d est un entier relatif sans facteur carré apparaissant dans la liste suivante :*

$$
\begin{array}{lcl}
d = & -1, \pm 2 & \\
d = & \pm p, \pm 2p & \textit{avec } p \equiv \pm 3 \bmod 8 \\
d = & -p & \textit{avec } p \equiv 7 \bmod 8 \\
d = & p & \textit{avec } p \equiv 1 \bmod 8 \textit{ et } p \neq x^2 - 32y^2,\ x > 0,\ x \equiv 1 \bmod 4 \\
d = & pq & \textit{avec } p \equiv q \equiv 3 \bmod 8 \\
d = & -pq & \textit{avec } p \equiv -q \equiv 3 \bmod 8
\end{array}
$$

où p et q sont des nombres premiers distincts.

Il est à noter qu'en considérant le 2-groupe des classes positives, il est aussi possible de déterminer les corps quadratiques dont la 2-partie du noyau sauvage est triviale (voir [JS2]).

Dans la suite du chapitre, E désigne un corps quadratique, et l'on écrit $E = \mathbb{Q}(\sqrt{d})$ où d est un entier relatif sans facteur carré. On note t le nombre de diviseurs premiers impairs de d.

3.1 Une nouvelle méthode de calcul du 2-rang du noyau sauvage d'un corps quadratique

On commence ce paragraphe en énonçant deux résultats qui se révéleront très utile dans la suite de ce travail.

Lemme 3.2 (Principe de Hasse). *Soit E/F une extension cyclique de corps de nombres et soit v_0 une place (finie ou infinie) de F. Alors un élément $x \in F^*$ est une norme globale dans E/F si et seulement si, pour toute place $v \neq v_0$ de F et toute place $w|v$ de E, l'élément x est une norme locale dans E_w/F_v.*

Démonstration. C'est le Theorem 2.87 de [Koc]. On peut aussi l'obtenir comme une conséquence des Corollary 5.2 et Corollary 6.7, Chapter IV de [N]. □

Corollaire 3.3. *Soit d un entier relatif sans facteur carré. Alors*
(i) -1 est une norme dans $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ si et seulement si $d > 0$ et tous les diviseurs premiers impairs de d sont $\equiv 1 \bmod 4$,
(ii) 2 est une norme dans $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ si et seulement si tous les diviseurs premiers impairs de d sont $\equiv \pm 1 \bmod 8$.

Démonstration. Soit $x \in \{-1, 2\}$. Alors, d'après le lemme 3.2, x est une norme (globale) dans $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ si et seulement si x est localement une norme en toutes les places finies de $\mathbb{Q}$, *i.e.*, si et seulement si (cf proposition 1.23), pour tout nombre premier p, le symbole de Hilbert $(x, d)_p \in \{\pm 1\}$ est égal à 1. On conclut avec les propositions 1.25 et 1.26. Il est à noter que la condition $d > 0$ dans (i) provient du calcul du symbole $(-1, d)_2$. □

Nous pouvons maintenant nous intéresser au problème qui nous intéresse principalement dans ce chapitre, à savoir le calcul du 2-rang du noyau sauvage des corps quadratiques à l'aide de la formule de genre. En conservant les notations des chapitres précédents, la formule de genre (voir corollaire 2.19) s'écrit de la façon suivante :

$$| WK_2(E)(2)_G | = \frac{2^{|T|-\rho}}{[D_{\mathbb{Q}} : D_{\mathbb{Q}} \cap \mathrm{N}_{E/\mathbb{Q}}(E^*)]} \tag{3.1}$$

où $T := T_{E/\mathbb{Q}}$ et $\rho \in \{0, 1\}$.

Par ailleurs, on sait que

$$[D_{\mathbb{Q}} : D_{\mathbb{Q}} \cap \mathrm{N}_{E/\mathbb{Q}}(E^*)] = 2 \iff 2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*).$$

Par conséquent, le corollaire 2.7 permet de calculer le 2-rang de $WK_2(E)$; en effet, on a

$$r_2(WK_2(E)) = \begin{cases} |T| - \rho & \text{si } 2 \in \mathrm{N}_{E/\mathbb{Q}}(E^*), \\ |T| - \rho - 1 & \text{si } 2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*). \end{cases}$$

En revenant à la définition de l'ensemble T (voir page 50), on voit que 2 est dans T si et seulement si, le premier 2 est non décomposé dans E et si, ou bien $\mu(E_w)(2) = \mu_2$, ou bien $E_w \neq \mathbb{Q}_2(\sqrt{2})$ (où w est la place de E au-dessus de 2). Par conséquent, si 2 est non décomposé dans E, le nombre premier 2 est dans T et puisque $\mu(\mathbb{Q}_2)(2) = \mu(\mathbb{Q})(2)$, on a aussi dans ce cas $\rho = 1$ (corollaire 2.19). En particulier, on obtient

$$2 \in T \Longleftrightarrow d \not\equiv 1 \bmod 8.$$

De plus, si $d < 0$, une place infinie se ramifie dans E et donc $\rho = 1$ (corollaire 2.19).

On peut donc déjà dresser le tableau suivant où l'on donne la valeur du 2-rang du noyau sauvage en fonction des différents paramètres :

		$2 \in \mathrm{N}_{E/\mathbb{Q}}(E^*)$	$2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*)$
$d < 0$	$d \not\equiv 1 \bmod 8$	$(t+1) - 1 = t$	$(t+1) - 1 - 1 = t - 1$
	$d \equiv 1 \bmod 8$	$t - 1$	$t - 1 - 1 = t - 2$
$d > 0$	$d \not\equiv 1 \bmod 8$	$(t+1) - 1 = t$	$(t+1) - 1 - 1 = t - 1$
	$d \equiv 1 \bmod 8$	$t - \rho$	$t - \rho - 1$

On constate dans le tableau ci-dessus qu'il y a deux cas pour lesquels la valeur de ρ est pour l'instant indéterminée. En fait, si on est dans le cas (b) de la formule de genre 2.18, on sait que $\rho = 1$. Lorsque $d > 0$ et $d \equiv 1 \bmod 8$, on est justement dans ce cas si et seulement si il existe $v \in T$, telle que $\mu(F_v)(2) = \mu(F)(2)$, *i.e.*, s'il existe un diviseur premier impair q de d tel que $\mu(\mathbb{Q}_q)(2) = \mu_2$. Autrement dit, s'il existe un diviseur premier impair de d congru à 3 modulo 4, alors $\rho = 1$, et sinon, on se trouve dans le cas (c) de la formule de genre et il faudra décider de la valeur de ρ.

Plaçons-nous alors maintenant dans le cas où $d > 0$, $d \equiv 1 \bmod 8$ et où tout diviseur premier impair de d est congru à 1 modulo 4.

1° Il est clair que si $2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*)$, alors $D_{\mathbb{Q}} \cap \mathrm{N}_{E/\mathbb{Q}}(E^*) = \mathbb{Q}^{*2}$. Ainsi, d'après la remarque page 57, $\operatorname{Ker}\alpha' \cong D_{\mathbb{Q}} \cap \mathrm{N}_{E/\mathbb{Q}}(E^*)/\mathbb{Q}^{*2}\, \mathrm{N}_{E/\mathbb{Q}}(D_E)$ est trivial, ce qui force $\rho = 0$.

2° Le cas où $2 \in \mathrm{N}_{E/\mathbb{Q}}(E^*)$ est un peu plus délicat. Remarquons d'abord que l'on peut écrire d sous la forme $d = r^2 - 8s^2$ avec $r, s \in \mathbb{Z}$. D'après les égalités

$$\begin{aligned} d &= \mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}\left(r + 2s\sqrt{2}\right) = \mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}\left((r + 2s\sqrt{2})(3 + 2\sqrt{2})\right) \\ &= (3r + 8s)^2 - 8(r + 3s)^2, \end{aligned}$$

on peut même supposer que $r > 0, r \equiv 1 \bmod 4$. En posant $\eta = r + \sqrt{d}$, nous avons $8s^2 = \mathrm{N}_{E/\mathbb{Q}}(\eta)$, et donc

$$\rho = 0 \Longleftrightarrow \prod_v (-1, \eta)_{m_w}^{\frac{n_v}{n}} = 1,$$

où les notations sont celles du chapitre précédent. On peut écrire ce produit sous la forme

$$\begin{aligned} \phi &:= \prod_v (-1, \eta)_{m_w}^{\frac{n_v}{n}} \\ &= \prod_{q \in U} (-1, r + \sqrt{d})_{m_w} \\ &= (-1, r + \sqrt{d})_{m_{w_2}} \prod_{q \in U,\, q \text{ impair}} (-1, r + \sqrt{d})_{m_w}\ , \end{aligned}$$

où U est l'ensemble des nombres premiers q tels que $q = 2$ ou $q \equiv 3 \bmod 4$ (ce qui traduit en fait la condition $n_v = n$), et, pour $q \in U$, w est une place de E au-dessus de q et w_2 est une place de E au-dessus de 2.

Or on voit que, pour un nombre premier impair q appartenant à U, on a $(-1, r + \sqrt{d})_{m_w} = (-1, r - \sqrt{d})_{m_w}$ (puisque le produit vaut 1) et, de plus, ces symboles sont triviaux si q ne divise pas s. Maintenant, si q divise s, soit $r + \sqrt{d}$, soit $r - \sqrt{d}$ est une unité ; ainsi, les symboles étant modérés, on a $(-1, r + \sqrt{d})_{m_w} = 1$ et donc

$$\phi = (-1, r + \sqrt{d})_{m_{w_2}} = (-1, r + \sqrt{d})_{\mathbb{Q}_2}.$$

Nous pouvons alors calculer ϕ.

Supposons dans un premier temps que $d \equiv 1 \bmod 16$. Dans ce cas, étant donné que $(-1, r+\sqrt{d})_{\mathbb{Q}_2} = (-1, r-\sqrt{d})_{\mathbb{Q}_2}$, on peut supposer que $\sqrt{d} \equiv 1 \bmod 8$ dans $\mathbb{Z}_2$; par conséquent, si $r \equiv 1 \bmod 8$, alors $r+\sqrt{d} \equiv 2 \bmod 8$ et donc $(-1, r+\sqrt{d})_{\mathbb{Q}_2} = 1$, ce qui signifie que $\rho = 0$. De même, si $r \equiv 5 \bmod 8$, alors $r+\sqrt{d} \equiv 6 \bmod 8$ et donc $(-1, r+\sqrt{d})_{\mathbb{Q}_2} = -1$ et $\rho = 1$.

Supposons, dans un second temps, que $d \equiv 9 \bmod 16$. Alors, par un raisonnement analogue au précédent, on peut supposer que $\sqrt{d} \equiv 5 \bmod 8$ dans $\mathbb{Z}_2$. On obtient alors $(-1, r+\sqrt{d})_{\mathbb{Q}_2} = 1$ si $r \equiv 5 \bmod 8$, ce qui implique $\rho = 0$. De même, $(-1, r+\sqrt{d})_{\mathbb{Q}_2} = -1$ si $r \equiv 1 \bmod 8$, d'où $\rho = 0$.

Pour résumer, on a donc obtenu

$$\rho = 1 \Longleftrightarrow \begin{cases} d \equiv 1 \bmod 16 \text{ et } r \equiv 5 \bmod 8, \\ \text{ ou} \\ d \equiv 9 \bmod 16 \text{ et } r \equiv 1 \bmod 8. \end{cases}$$

Mais, comme $d = r^2 - 8s^2$ avec $r > 0, r \equiv 1 \bmod 4$, il devient clair que $\rho = 1$ si et seulement si s est impair, ou de manière équivalente, si d ne s'écrit pas sous la forme $d = x^2 - 32y^2,\ x > 0,\ x \equiv 1 \bmod 4$.

En considérant le corollaire 3.3, on obtient le théorème ci-après ; ainsi, sous cette forme, on voit bien que l'on retrouve les résultats de [BS].

Théorème 3.4. *Soit $E = \mathbb{Q}(\sqrt{d})$ un corps quadratique, où d est un entier relatif sans facteur carré. Alors le 2-rang de $WK_2(E)$ est donné dans le tableau suivant :*

<table>
<tr><td colspan="3"></td><td>$2 \in \mathrm{N}_{E/\mathbb{Q}}(E^*)$</td><td>$2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*)$</td></tr>
<tr><td rowspan="2">$d < 0$</td><td colspan="2">$d \not\equiv 1 \bmod 8$</td><td>t</td><td>$t-1$</td></tr>
<tr><td colspan="2">$d \equiv 1 \bmod 8$</td><td>$t-1$</td><td>$t-2$</td></tr>
<tr><td rowspan="3">$d > 0$</td><td colspan="2">$d \not\equiv 1 \bmod 8$</td><td>t</td><td>$t-1$</td></tr>
<tr><td rowspan="2">$d \equiv 1 \bmod 8$</td><td>$-1 \in \mathrm{N}_{E/\mathbb{Q}}(E^*)$</td><td>$t$ *si* s *pair*
$t-1$ *si* s *impair*</td><td>$t-1$</td></tr>
<tr><td>$-1 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*)$</td><td>$t-1$</td><td>$t-2$</td></tr>
</table>

où l'on écrit $d = r^2 - 8s^2$ avec $r > 0, r \equiv 1 \bmod 4$, dans le cas où $d > 0, d \equiv$

1 mod 8 *et tous les diviseurs premiers impairs de d sont congrus à* 1 *modulo* 4.

3.2 Corps quadratiques dont la 2-partie du noyau sauvage est triviale

Nous sommes maintenant en mesure de démontrer le théorème 3.1 énoncé au début du chapitre. Pour simplifier, on s'intéresse d'abord aux corps quadratiques réels, puis ensuite aux corps quadratiques imaginaires.

Proposition 3.5. *Les corps quadratiques réels dont la* 2*-partie du noyau sauvage est triviale sont les corps* $\mathbb{Q}(\sqrt{d})$ *où* d *est un entier naturel sans facteur carré apparaissant dans la liste suivante :*

$$\begin{array}{cl} 2 & \\ p, 2p & \textit{avec } p \equiv \pm 3 \bmod 8 \\ p & \textit{avec } p \equiv 1 \bmod 8 \textit{ et } p \neq x^2 - 32y^2,\ x > 0,\ x \equiv 1 \bmod 4 \\ pq & \textit{avec } p \equiv q \equiv 3 \bmod 8 \end{array}$$

où p *et* q *sont des nombres premiers.*

Remarque : en fait, lorsque p est un nombre premier vérifiant $p \equiv 1 \bmod 8$, on peut remplacer la condition « $p \neq x^2 - 32y^2,\ x > 0,\ x \equiv 1 \bmod 4$ » par la condition « p n'est pas représenté sur $\mathbb{Z}$ par $X^2 + 32Y^2$ » (voir [BC]).

Démonstration. Posons $E = \mathbb{Q}(\sqrt{d})$. Alors, $WK_2(E)(2)$ est triviale si et seulement si le 2-rang de $WK_2(E)$ est nul. Il suffit maintenant d'appliquer le théorème 3.4 en gardant à l'esprit les résultats du corollaire 3.3.

Ainsi, pour $d \geqslant 2$, on a :
si $d \not\equiv 1 \bmod 8$, alors

$$WK_2(E)(2) = 0 \iff \left\{ \begin{array}{l} d = 2 \\ \text{ ou} \\ t = 1 \text{ et } 2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*) \end{array} \right.$$

$$\iff \left\{ \begin{array}{l} d = 2 \\ \text{ ou} \\ d = p \text{ ou } 2p \text{ avec } p \text{ premier } \equiv \pm 3 \bmod 8 \end{array} \right.$$

et si $d \equiv 1 \bmod 8$, alors

$$WK_2(E)(2)=0 \iff \begin{cases} t=2, -1\notin \mathrm{N}_{E/\mathbb{Q}}(E^*), \text{ et } 2\notin \mathrm{N}_{E/\mathbb{Q}}(E^*) \\ \text{ou} \\ t=1 \text{ et } d\neq x^2-32y^2,\ x>0,\ x\equiv 1 \bmod 4 \end{cases}$$

$$\iff \begin{cases} d=pq \text{ avec } p\equiv q\equiv 3 \bmod 8 \\ \text{ou} \\ d=p\neq x^2-32y^2,\ x>0,\ x\equiv 1 \bmod 4 \end{cases}$$

où p et q sont des nombres premiers. D'où le résultat. □

De même, on obtient dans le cas totalement imaginaire :

Proposition 3.6. *Les corps quadratiques imaginaires dont la 2-partie du noyau sauvage est triviale sont les corps $\mathbb{Q}(\sqrt{d})$ où d est un entier relatif sans facteur carré apparaissant dans la liste suivante :*

$$\begin{array}{cl} -1, -2 & \\ -p, -2p & \textit{avec } p\equiv \pm 3 \bmod 8 \\ -p & \textit{avec } p\equiv 7 \bmod 8 \\ -pq & \textit{avec } p\equiv -q\equiv 3 \bmod 8. \end{array}$$

où p et q sont des nombres premiers.

Démonstration. Pour $d\leqslant -1$, on a :
si $d\not\equiv 1 \bmod 8$, alors

$$WK_2(E)(2)=0 \iff \begin{cases} d=-1 \\ \text{ou} \\ d=-2 \\ \text{ou} \\ t=1 \text{ et } 2\notin \mathrm{N}_{E/\mathbb{Q}}(E^*) \end{cases}$$

$$\iff \begin{cases} d=-1 \\ \text{ou} \\ d=-2 \\ \text{ou} \\ d=-p \text{ ou } -2p \text{ avec } p \text{ premier } \equiv \pm 3 \bmod 8 \end{cases}$$

et si $d\equiv 1 \bmod 8$, alors

$$WK_2(E)(2) = 0 \iff \begin{cases} t = 2 \text{ et } 2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*) \\ \text{ou} \\ t = 1 \text{ et } 2 \in \mathrm{N}_{E/\mathbb{Q}}(E^*) \end{cases}$$

$$\iff \begin{cases} d = -pq \text{ avec } p \equiv -q \equiv 3 \bmod 8 \\ \text{ou} \\ d = -p \text{ avec } p \equiv 7 \bmod 8 \end{cases}$$

où p et q sont des nombres premiers. D'où le résultat. $\square$

Chapitre 4

2-extensions cycliques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale

L'objectif de ce chapitre est de déterminer toutes les 2-extensions cycliques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. Comme on connaît déjà la situation pour les corps quadratiques (cf le théorème 3.1), on ne s'intéressera ici qu'aux 2-extensions cycliques de degré $\geqslant 4$. Le principal outil utilisé est encore la formule de genre vue à la section 2.3.

On rappelle qu'on entend par 2-extension de $\mathbb{Q}$ une extension galoisienne finie de $\mathbb{Q}$ dont le groupe de Galois est d'ordre une puissance de 2.

4.1 Préliminaires sur les extensions cycliques

Proposition 4.1. *Soit K un corps ne contenant pas de racine primitive quatrième de l'unité. Considérons $L := K(\sqrt{a})$ où a est un élément de $K^* \setminus (K^*)^2$. Les conditions suivantes sont équivalentes :*

(1) a est la somme de deux carrés de K,
(2) -1 est une norme dans L/K,
(3) a est une norme dans L/K,
(4) il existe $b \in L$ tel que $\mathrm{N}_{L/K}(b) \equiv a \bmod (K^*)^2$,
(5) M/K est cyclique où $M := L(\sqrt{b})$ (avec le b du (4)),
(6) L est contenue dans une extension cyclique de degré 4 de K.

$$\begin{array}{c} M = L(\sqrt{b}) \\ | \\ L = K(\sqrt{a}) \\ | \\ K \end{array}$$

Démonstration. Voir [S3], Chapter I. □

Corollaire 4.2. *Soit $E/\mathbb{Q}$ une 2-extension cyclique de degré $\geqslant 4$. Alors, l'unique corps quadratique contenu dans E s'écrit sous la forme $\mathbb{Q}(\sqrt{d})$ où $d > 0$ est sans facteur carré, et, tout diviseur premier impair de d est congru à 1 modulo 4.*

Démonstration. C'est une conséquence immédiate de la proposition précédente et du corollaire 3.3. □

Proposition 4.3. *Soit $E/\mathbb{Q}$ une 2-extension cyclique de corps de nombres. Alors, un nombre premier doit d'abord se décomposer, puis rester inerte, et enfin, se ramifier dans E.*

Démonstration. L'inclusion est un ordre total sur l'ensemble des sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$. Par conséquent, pour obtenir le résultat, il suffit de considérer les groupes de décomposition et d'inertie associés au nombre premier dont on étudie la ramification. □

Corollaire 4.4. *Soit $E/\mathbb{Q}$ une 2-extension cyclique de corps de nombres qui est de degré au moins 4 et qui ne contient pas $\sqrt{2}$. Alors si $WK_2(E)(2)$ est triviale, il en est de même pour $WK_2(L)(2)$, où L décrit l'ensemble des sous-extensions de E.*

Démonstration. Comme $\sqrt{2} \notin E$, il est clair qu'un nombre premier impair se ramifie dans le sous-corps quadratique (réel) de E. Il découle de la proposition 4.3 que ce nombre premier impair se ramifie totalement dans $E/\mathbb{Q}$. Ainsi, si $\mathbb{Q} \subset K \subset L \subset E$ est une tour d'extensions telle que $[L : K] = 2$, on voit avec le corollaire 2.17 que le morphisme de transfert

$$WK_2(L)(2)_{\mathrm{Gal}(L/K)} \to WK_2(K)(2)$$

est surjectif. Comme $WK_2(E)(2) = 0$, on en déduit par une récurrence descendante que la trivialité des noyaux sauvages se propage aux sous-extensions de E. □

Avant de conclure ce paragraphe par une dernière proposition, rappelons quelques notations déjà vues au cours des chapitres précédents. Notons $\mathbb{Q}_\infty$ la $\mathbb{Z}_2$-extension cyclotomique de $\mathbb{Q}$, et $\mathbb{Q}_n$ le n-ième étage de $\mathbb{Q}_\infty$. Alors, si l'on définit encore la suite $(\alpha_k)_{k\geqslant 0}$ de réels positifs par :

$$\begin{cases} \alpha_0 = 0, \\ \alpha_{k+1} = \sqrt{2+\alpha_k}, \end{cases}$$

on sait (cf le lemme 2.3) que $\mathbb{Q}_n = \mathbb{Q}(\alpha_n)$.

Proposition 4.5. *Soit p et ℓ deux nombres premiers dictincts. Pour $n \geqslant 2$, soit M_n une extension cyclique de $\mathbb{Q}$ de degré 2^n vérifiant l'une des conditions suivantes :*

(i) $M_n/\mathbb{Q}$ est non ramifiée en dehors de 2 et p,
2 et p sont non décomposés dans $M_n/\mathbb{Q}$,

(ii) $M_n/\mathbb{Q}$ est non ramifiée en dehors de p et ℓ,
2 est totalement décomposé dans $M_n/\mathbb{Q}$,
p et ℓ sont non décomposés dans $M_n/\mathbb{Q}$.

Pour $i \in \{0, \ldots, n\}$, désignons par M_i l'unique sous-corps de degré 2^i de M_n, et par r l'entier tel que $\mathbb{Q}_r = M_n \cap \mathbb{Q}_\infty (= M_r)$. Alors, pour $n > r$, nous avons

$$2 + \alpha_r \in \mathrm{N}_{M_n/M_{n-1}}(M_n^*) \Longleftrightarrow 2 + \alpha_r \in \mathrm{N}_{M_{r+1}/M_r}(M_{r+1}^*).$$

Démonstration. Si $n = r + 1$, la proposition ne dit rien. Supposons donc que $n - r \geqslant 2$ et, pour $r \leqslant i \leqslant n - 2$, posons pour simplifier les notations, $K = M_i$, $L = M_{i+1}$ et $M = M_{i+2}$. Pour montrer la proposition, il suffit de montrer que

$$2 + \alpha_r \in \mathrm{N}_{M/L}(M^*) \Longleftrightarrow 2 + \alpha_r \in \mathrm{N}_{L/K}(L^*). \tag{4.1}$$

Pour cela, en vertu du principe de Hasse (voir le lemme 3.2), on peut se contenter de regarder cette équivalence localement. Mais, comme $2 + \alpha_r$ est une unité locale en toute place de K, il découle de [N], Chapter III, Corollary 1.4 que $2 + \alpha_r$ est une norme localement dans M/L (ou L/K), et ceci en toute place non ramifiée dans $M_n/\mathbb{Q}$. Compte tenu du fait que, sous les hypothèses (ii), 2 est totalement décomposé dans $M_n/\mathbb{Q}$, il est clair qu'en toute place 2-adique, $2 + \alpha_r$ est trivialement une norme localement dans M/L (ou L/K). Par conséquent, dans les deux cas (i) et (ii), $2 + \alpha_r$ est localement une norme dans M/L (ou L/K) en toutes les places à l'exception peut-être de deux places. D'après le lemme 3.2, il suffit de montrer que,

$$2 + \alpha_r \in \mathrm{N}_{M_{\mathcal{P}}/L_{\mathfrak{P}}}(M_{\mathcal{P}}^*) \Longleftrightarrow 2 + \alpha_r \in \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}^*),$$

où $\mathfrak{p}$ (respectivement $\mathfrak{P}$, $\mathcal{P}$) désigne la place de K (respectivement L, M) au-dessus de p.

Or, d'après la proposition 4.1, on peut écrire

$$\begin{array}{cc}
\mathcal{P} & M = L(\sqrt{b}) \\
| & | \\
\mathfrak{P} & L = K(\sqrt{a}) \\
| & | \\
\mathfrak{p} & K
\end{array}$$

où $a \in K^* \smallsetminus (K^*)^2$, $b \in M^* \smallsetminus (M^*)^2$ et $\exists\, c \in K^*$, $\mathrm{N}_{L/K}(b) = ac^2$. Il vient alors les équivalences suivantes :

$$\begin{aligned}
2+\alpha_r \in \mathrm{N}_{M_{\mathcal{P}}/L_{\mathfrak{P}}}(M_{\mathcal{P}}^*) &\iff (2+\alpha_r, b)_{L_{\mathfrak{P}}} = 1 \\
&\iff (2+\alpha_r, \mathrm{N}_{L/K}(b))_{K_{\mathfrak{p}}} = 1 \\
&\iff (2+\alpha_r, ac^2)_{K_{\mathfrak{p}}} = 1 \\
&\iff (2+\alpha_r, a)_{K_{\mathfrak{p}}} = 1 \\
&\iff 2+\alpha_r \in \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}^*)
\end{aligned}$$

où la première équivalence provient du point (iii) de la proposition 1.23 et la deuxième du point (vii) de cette même proposition. D'où le résultat. $\square$

4.2 2-extensions cycliques

Fixons pour commencer quelques notations : soit
E une 2-extension cyclique de $\mathbb{Q}$ de degré $[E:\mathbb{Q}] \geqslant 4$,
F l'unique sous-corps de E d'indice 2,
G le groupe de Galois de E/F,
K l'unique corps quadratique contenu dans E,
d l'unique entier positif, sans facteur carré vérifiant $K = \mathbb{Q}(\sqrt{d})$,
$T_{E/F}$ l'ensemble fini de places de F défini page 50.

Remarquons d'abord que si $K \neq \mathbb{Q}(\sqrt{2})$ et si $WK_2(E)(2)$ est triviale, alors $WK_2(K)(2)$ est aussi triviale d'après le corollaire 4.4. Par conséquent, il découle de la proposition 3.5 et du corollaire 4.2 la

Proposition 4.6. *Si $WK_2(E)(2)$ est triviale, alors d est de l'une des quatre formes suivantes :*

$d = 2$,
$d = p$, *p premier* $\equiv 5 \bmod 8$,
$d = 2p$, *p premier* $\equiv 5 \bmod 8$,
$d = p$, *p premier* $\equiv 1 \bmod 8$ *tel que* $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$.

Comme F est totalement réel, la formule de genre (cf corollaire 2.19) s'écrit

$$\frac{|\, WK_2(E)(2)_G \,|}{|\, WK_2(F)(2) \,|} = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]}, \tag{4.2}$$

où $\rho = 0$ ou $\rho = 1$.

Pour être plus précis, on sait que $\rho = 1$ si une place infinie réelle de F se ramifie dans E, ou bien, si $\mu(F_v)(2) = \mu(F)(2)$ pour une place $v \in T_{E/F}$. On sera justement dans ce cas lorsque d sera de l'une des trois premières formes apparaissant dans la proposition 4.6, ce qui explique pourquoi le résultat est assez direct. Par contre, si d est un nombre premier $p \equiv 1 \bmod 8$ avec $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$, alors la situation est plus délicate : en effet, on se trouve dans le cas (c) de la formule de genre 2.18 et on doit se ramener à des calculs de symboles locaux comme expliqué à la fin du chapitre 2.

Lemme 4.7. *Si $WK_2(E)(2)$ est triviale, alors l'ensemble $T_{E/F}$ a au plus deux éléments.*

Démonstration. C'est une conséquence directe de l'égalité (4.2). En effet, n'oublions pas que, F étant toalement réel, $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)] \leqslant 2$. $\square$

Lemme 4.8. *Une place 2-adique de F qui ne se décompose pas dans E appartient toujours à l'ensemble $T_{E/F}$.*

Démonstration. Soit w la place de E au-dessus de v. Supposons que $v \notin T_{E/F}$. Par définition de $T_{E/F}$, on a $|\mu(E_w)(2)| > |\mu(F_v)(2)|$ et E_w est contenue dans la $\mathbb{Z}_2$-extension cyclotomique $F_{v,\infty}$ de F_v. Il en résulte que $\sqrt{-1}$ et $\sqrt{2}$ sont dans E_w. Ainsi l'extension cyclique E_w de $\mathbb{Q}_2$ contient les deux extensions quadratiques $\mathbb{Q}_2(\sqrt{-1})$ et $\mathbb{Q}_2(\sqrt{2})$, ce qui est impossible. $\square$

Ces remarques d'ordre général étant faites, nous pouvons maintenant nous concentrer sur la détermination des 2-extensions cycliques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. Cependant, il nous a semblé opportun de commencer par traiter le cas des extensions cycliques de degré 4 afin d'illustrer les méthodes mises en jeu pour résoudre ce problème.

4.2.1 Extensions cycliques de degré 4

Comme pour le cas général, on mène une discussion, motivée par la proposition 4.6, portant sur la forme du sous-corps quadratique $K = \mathbb{Q}(\sqrt{d})$. Néanmoins, si $d = 2, p$ ou $2p$ (avec p premier $\equiv 5 \bmod 8$), la question se traite exactement comme pour le cas général ; c'est pourquoi l'intérêt d'étudier le cas du degré 4 séparément réside dans la spécificité du cas où le sous-corps quadratique est $\mathbb{Q}(\sqrt{p})$, où p est un nombre premier congru à 1 modulo 8 tel que $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$.

Plaçons-nous donc dans le cas où E est une extension cyclique de $\mathbb{Q}$ de degré 4 et où $F = K = \mathbb{Q}(\sqrt{d})$, avec $d = p \equiv 1 \bmod 8$ est un nombre premier tel que $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$.

Afin d'obtenir des conditions nécessaires à la trivialité de $WK_2(E)(2)$, on suppose aussi que $WK_2(E)(2)$ est triviale.

Comme p est ramifié dans $F/\mathbb{Q}$, donc dans E/F (cf proposition 4.3), il est clair que la place $\mathfrak{p}$ de F au-dessus de p appartient à $T_{E/F}$.

$$\begin{tikzcd}
E \arrow[d, dash] & & & & \\
F = \mathbb{Q}(\sqrt{p}) \arrow[d, dash] & \mathfrak{p} \arrow[d, dash] & \mathfrak{p}_2 \arrow[dr, dash] & & \mathfrak{p}'_2 \arrow[dl, dash] \\
\mathbb{Q} & p & & 2 &
\end{tikzcd}$$

Par ailleurs, 2 est décomposé dans F. Soit $\mathfrak{p}_2$ une place 2-adique de F ; si $\mathfrak{p}_2$ était non décomposée dans E/F, alors le lemme 4.8 impliquerait que $\mathfrak{p}_2 \in T_{E/F}$. Ainsi, l'ensemble $T_{E/F}$ contiendrait au moins trois éléments, ce qui contredit le lemme 4.7. Par conséquent, 2 doit être totalement décomposé dans $E/\mathbb{Q}$.

Il résulte des remarques ci-dessus qu'au plus une place impaire de F, autre que $\mathfrak{p}$, peut éventuellement se ramifier dans E/F (*i.e.*, appartenir à l'ensemble $T_{E/F}$). Mais alors, puisque $|T_{E/F}| \leqslant 2$, cette place de F est nécessairement non décomposée dans $F/\mathbb{Q}$. Or, comme 2 est totalement décomposée, on voit que les hypothèses du cas (ii) de la proposition 4.5 sont satisfaites. Il s'ensuit que $2 \in \mathrm{N}_{E/F}(E^*)$ si et seulement si $2 \in \mathrm{N}_{F/\mathbb{Q}}(F^*)$, ce qui est vrai puisque $p \equiv 1 \bmod 8$ (corollaire 3.3). Par conséquent, $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)] = 1$ et la formule de genre (4.2) devient

$$1 = \mid WK_2(E)(2)_G \mid = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]} = 2^{|T_{E/F}|-\rho},$$

ce qui force $|T_{E/F}| \leqslant 1$. Autrement dit, seul p se ramifie dans $E/\mathbb{Q}$ et $T_{E/F} = \{\mathfrak{p}\}$.

En résumé, si $WK_2(E)(2)$ est triviale, alors E est contenue dans le corps cyclotomique $\mathbb{Q}(\mu_p)$ et 2 est totalement décomposé dans $E/\mathbb{Q}$.

Afin d'écrire explicitement l'extension E, nous avons besoin d'établir quelques résultats sur l'unité fondamentale ϵ de $\mathbb{Q}(\sqrt{p})$.

Lemme 4.9. *Soit $p \equiv 1 \bmod 4$ un nombre premier et ϵ l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$. Alors,*

(i) ϵ est de norme -1 dans l'extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$.

(ii) Si, de plus, $p \equiv 1 \bmod 8$, alors ϵ s'écrit sous la forme $\epsilon = a + b\sqrt{p}$ où a et b sont des entiers tels que a est un multiple de 4 et b est impair.

Démonstration. (i) Cette preuve s'inspire de [Co]. On raisonne par l'absurde, et on suppose que ϵ est de norme 1 dans $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. D'après le théorème 90 de Hilbert, il existe $\gamma \in \mathbb{Q}(\sqrt{p})$ tel que

$$\epsilon = \frac{\gamma}{\gamma^\sigma},$$

où σ est le générateur du groupe de Galois de $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. En fait, comme $\mathbb{Q}$ est invariant par σ, on peut supposer que γ est un entier de $\mathbb{Q}(\sqrt{p})$, qui n'est divisible par aucun nombre rationnel. De plus, on obtient l'égalité $(\gamma) = (\gamma^\sigma)$ entre idéaux principaux.
Considérons $\mathfrak{q}$ un idéal premier de $\mathbb{Q}(\sqrt{p})$ tel que $\mathfrak{q}|(\gamma)$ et disons que $\mathfrak{q}$ vit au-dessus d'un nombre premier q. Alors $\mathfrak{q}|(\gamma^\sigma)$, ce qui implique que $\mathfrak{q}^\sigma|(\gamma)$. Par conséquent, si $\mathfrak{q} \neq \mathfrak{q}^\sigma$, alors $\mathfrak{q}\mathfrak{q}^\sigma|(\gamma)$, c'est-à-dire $(q)|(\gamma)$, ce qui contredit l'hypothèse précédemment faite. D'où $\mathfrak{q} = \mathfrak{q}^\sigma$, et q ne se décompose pas dans $\mathbb{Q}(\sqrt{p})$.
Si q était inerte, on aurait $\gamma = q\gamma'$, ce qui contredit une nouvelle fois l'hypothèse. Ainsi, q se ramifie et donc $q = p$ (puisque $p \equiv 1 \bmod 4$). Il en résulte que deux cas sont possibles : soit $(\gamma) = o_F$, soit $(\gamma) = (\sqrt{p})$. Il vient alors $\gamma = u$ ou $\gamma = u\sqrt{p}$ où u désigne une unité de F. On a alors, puisque $\mathrm{N}_{F/\mathbb{Q}}(u) = \pm 1$, dans le premier cas,

$$\epsilon = \frac{\gamma}{\gamma^\sigma} = \frac{u}{u^\sigma} = \frac{u^2}{\mathrm{N}_{F/\mathbb{Q}}(u)} = \pm u^2,$$

et, dans le second,

$$\epsilon = \frac{\gamma}{\gamma^\sigma} = \frac{u\sqrt{p}}{u^\sigma(\sqrt{p})^\sigma} = \frac{u^2\sqrt{p}}{\mathrm{N}_{F/\mathbb{Q}}(u)\cdot(-\sqrt{p})} = \pm u^2.$$

Mais ceci contredit le fait que ϵ est l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$. D'où $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = -1$.

(ii) Comme $p \equiv 1 \bmod 4$, l'anneau des entiers de $\mathbb{Q}(\sqrt{p})$ est $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ et donc $\epsilon = \frac{1}{2}(u + v\sqrt{p})$ avec u et v deux entiers de même parité. D'après (i), on a

$$-4 = u^2 - pv^2.$$

Si u et v sont impairs, la réduction modulo 8 de l'égalité précédente donne $-4 \equiv 0 \bmod 8$, ce qui force u et v d'être pairs. D'où $\epsilon = a + b\sqrt{p}$ où a et b sont des entiers vérifiant

$$a^2 - pb^2 = -1.$$

Si a est impair, nécessairement b est pair, et la réduction modulo 4 de l'égalité précédente donne $1 \equiv -1 \bmod 4$. D'où a est pair et par suite b est impair. Mais alors modulo 8 cette même égalité implique que $a^2 \equiv 0 \bmod 8$, ce qui signifie que $a \equiv 0 \bmod 4$. □

De plus, comme $p \equiv 1 \bmod 4$ est premier, p s'écrit comme somme de deux carrés, et même puisque $p \equiv 1 \bmod 8$, on peut écrire p sous la forme $p = 16m^2 + n^2$ avec n impair (où m et n sont des entiers). On peut maintenant énoncer un résultat de M. Stinner ([St]) dont on reprend ici la preuve pour la commodité du lecteur.

Proposition 4.10. *Soit $p = 16m^2 + n^2 \equiv 1 \bmod 8$ un nombre premier et $\epsilon = a + b\sqrt{p}$ l'unité fondamentale du corps quadratique $\mathbb{Q}(\sqrt{p})$. Alors*

$$4m \equiv na + (-1)^{\frac{n-1}{2}} n - 1 \bmod 8.$$

Démonstration. On a $a^2 + 1 = pb^2$. Donc dans $\mathbb{Z}[i]$, on obtient $(a+i)(a-i) = pb^2$ (où $i^2 = -1$). Or comme $\mathbb{Z}[i]$ est un anneau factoriel, on peut écrire

$$a + i = (x + iy)(c + id)^2, \tag{4.3}$$

où $x, y, c, d \in \mathbb{Z}$ et $x + iy$ est sans facteur carré.
Puisque $a + i$ et $a - i$ sont premiers entre eux, $x + iy$ et $x - iy$ le sont aussi. Ainsi l'égalité $(x^2 + y^2)(c^2 + d^2)^2 = a^2 + 1 = pb^2$ implique que

$$p = x^2 + y^2, \tag{4.4}$$
$$b = c^2 + d^2. \tag{4.5}$$

De plus, avec (4.3), on a

$$a = x(c^2 - d^2) - 2ycd, \tag{4.6}$$
$$1 = y(c^2 - d^2) + 2xcd. \tag{4.7}$$

Puisque b est impair et a est pair, il résulte successivement de (4.5) que $c^2 - d^2$ est impair (et donc c et d sont de parité opposée), de (4.6) que x est pair et de (4.4) que y est impair. Maintenant d'après (4.7), nous avons $y(c^2 - d^2) \equiv 1 \bmod 8$ et par conséquent, d'après (4.6), $ya = xy(c^2 - d^2) - 2y^2cd \equiv x - 2cd \bmod 8$. D'où

$$x \equiv ay + 2cd \bmod 8. \tag{4.8}$$

De plus, avec (4.7), on obtient $y = y^2(c^2 - d^2) + 2xycd \equiv c^2 - d^2 \bmod 8$. En écrivant $c^2 - d^2 = (c-d)^2 + 2cd - 2d^2$, il vient

$$y \equiv 1 + 2cd - 2d^2 \bmod 8. \tag{4.9}$$

Maintenant, si $y \equiv 1 \bmod 4$, la réduction modulo 4 dans (4.9) implique que d est pair et (4.9) donne alors $2cd \equiv y - 1 \bmod 8$. Si $y \equiv 3 \bmod 4$, la réduction modulo 4 dans (4.9) implique que d est impair et en remplaçant dans (4.9), on obtient finalement $2cd \equiv -2cd \equiv -y - 1 \bmod 8$. D'où dans les deux cas, on a $2cd \equiv (-1)^{\frac{y-1}{2}}y - 1 \bmod 8$ et, d'après (4.8), on obtient

$$x \equiv ya + (-1)^{\frac{y-1}{2}}y - 1 \bmod 8.$$

D'où la proposition, puisque la représentation de p comme somme de deux carrés est unique au signe près. $\square$

Remarque : on a en particulier montré que $b = c^2 + d^2$, et par conséquent que $b \equiv 1 \bmod 4$.

Nous avons alors les conditions équivalentes suivantes :

(i) $p = x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$,

(ii) $(-1)^{\frac{n-1}{2}}n - 1 \equiv 4m \bmod 8$,

(iii) $a \equiv 0 \bmod 8$.

La première équivalence entre (i) et (ii) est une partie du « Main Theorem » de [BC] et la seconde entre (ii) et (iii) découle immédiatement de la proposition 4.10.

Revenons au cas où $p \equiv 1 \bmod 8$ est un nombre premier satisfaisant la condition $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$. Alors, compte tenu de ce qui précède et du point (ii) du lemme 4.9, on obtient $a \equiv 4 \bmod 8$.

Proposition 4.11. *Soit E l'unique sous-extension de $\mathbb{Q}(\mu_p)$ de degré 4 sur $\mathbb{Q}$ où $p \equiv 1 \bmod 8$ est un nombre premier satisfaisant la condition $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$. Alors*

$$E = \mathbb{Q}\left(\sqrt{\epsilon\sqrt{p}}\right),$$

et l'on a l'équivalence

$$2 \text{ est totalement décomposé dans } E/\mathbb{Q} \Longleftrightarrow p \equiv 9 \bmod 16.$$

Démonstration. Soit L l'extension $\mathbb{Q}\left(\sqrt{\epsilon\sqrt{p}}\right)$.
En ce qui concerne la première affirmation, on peut déjà remarquer que $\mathrm{N}_{F/\mathbb{Q}}(\epsilon\sqrt{p}) = (-1) \times (-p) = p$ et donc l'extension L est bien cyclique de degré 4 sur $\mathbb{Q}$ (cf proposition 4.1). Elle est de plus non ramifiée en dehors de p : en effet, comme $\mathrm{N}_{F/\mathbb{Q}}(\epsilon\sqrt{p}) = p$, il suffit de montrer que $L/\mathbb{Q}$ est non ramifiée en 2. Pour cela, écrivons $p = u^2$ avec $u \in \mathbb{Q}_2^*$; on a alors $\epsilon\sqrt{p} = au + bp \in \mathbb{Q}_2^*$ et donc dans $\mathbb{Q}_2^*$, on a la congruence :

$$\epsilon\sqrt{p} \equiv b \bmod 4,$$

car $a \equiv 0 \bmod 4$ (cf le lemme 4.9). D'après la remarque suivant la preuve de la proposition 4.10, on obtient

$$\epsilon\sqrt{p} \equiv 1 \bmod 4,$$

ce qui force le complété de L à la place 2-adique d'être l'extension quadratique non ramifiée de $\mathbb{Q}_2$.

Quant à l'équivalence annoncée, il suffit de constater que 2 est totalement décomposé dans $E/\mathbb{Q}$ si et seulement si $\epsilon\sqrt{p}$ est un carré dans $\mathbb{Q}_2^*$. Ainsi, avec les notations précédentes, on obtient :

$$\begin{aligned}
\epsilon\sqrt{p} \in (\mathbb{Q}_2^*)^2 \quad &\Longleftrightarrow \quad (a+bu)u \equiv 1 \bmod 8 \text{ dans } \mathbb{Q}_2^*\ , \\
&\Longleftrightarrow \quad au + bp \equiv 1 \bmod 8, \\
&\Longleftrightarrow \quad au + b \equiv 1 \bmod 8, \\
&\Longleftrightarrow \quad 4 + b \equiv 1 \bmod 8 \quad (\text{puisque } a \equiv 4 \bmod 8), \\
&\Longleftrightarrow \quad b \equiv 5 \bmod 8, \\
&\Longleftrightarrow \quad p \equiv 9 \bmod 16.
\end{aligned}$$

□

Par conséquent, il découle de ce qui précède la

Proposition 4.12. *Soit* $p \equiv 1 \bmod 8$ *un nombre premier satisfaisant la condition* $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$ *et soit* E *une extension cyclique de* $\mathbb{Q}$ *de degré* 4 *contenant le corps quadratique* $\mathbb{Q}(\sqrt{p})$. *Si* $WK_2(E)(2)$ *est triviale, alors nécessairement* $p \equiv 9 \bmod 16$ *et* $E = \mathbb{Q}\left(\sqrt{\epsilon\sqrt{p}}\right)$ *est l'unique sous-corps de* $\mathbb{Q}(\mu_p)$ *de degré* 4 *sur* $\mathbb{Q}$.

Il reste donc à voir si la réciproque est vraie, à savoir si une telle extension a une 2-partie du noyau sauvage triviale. Par conséquent, soit $E = \mathbb{Q}\left(\sqrt{\epsilon\sqrt{p}}\right)$ l'unique sous-corps de $\mathbb{Q}(\mu_p)$ de degré 4 sur $\mathbb{Q}$, où $p \equiv 9 \bmod 16$ est un nombre premier satisfaisant la condition $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$. Le but de ce qui suit est de montrer que $WK_2(E)(2)$ est effectivement triviale.

On sait déjà que :

1. le nombre premier 2 est totalement décomposé dans E,
2. l'ensemble $T_{E/F}$ est réduit à $\{\mathfrak{p}\}$,
3. et $2 \in \mathrm{N}_{E/F}(E^*)$.

Par conséquent, la formule de genre devient :

$$\mid WK_2(E)(2)_G \mid = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]} = 2^{1-\rho},$$

où $\rho \in \{0, 1\}$.

Ainsi, $WK_2(E)(2)$ est triviale si et seulement si $\rho = 1$. Or, comme on l'a déjà fait remarquer page 59, on sait que, si η vérifie $\mathrm{N}_{E/F}(\eta) = 2$, alors

$$\rho = 1 \Longleftrightarrow \prod_v (-1, \eta)_{m_w}^{\frac{n_v}{n}} = -1,$$

où les notations sont toujours celles déjà utilisées dans les chapitres précédents.

Pour choisir correctement η, remarquons d'abord que 2 est une norme dans l'extension $E/\mathbb{Q}$. En effet, puisque les nombres premiers différents de 2 et de p sont non ramifiés dans E, on voit que 2 est localement une norme partout, à l'exception peut-être d'une place, à savoir la place ramifiée p. On conclut alors avec le principe de Hasse (cf le lemme 3.2).

Considérons alors ξ un élément de E^* tel que $2 = \mathrm{N}_{E/\mathbb{Q}}(\xi)$ et notons σ un générateur du groupe de Galois de l'extension $E/\mathbb{Q}$. Posons alors $\eta = \xi\xi^\sigma$ de sorte que $2 = \mathrm{N}_{E/F}(\eta)$. Nous devons donc calculer le produit

$$\phi = \prod_v (-1, \eta)_{m_w}^{\frac{n_v}{n}} = \prod_{v \in V} (-1, \eta)_{m_w},$$

où V est l'ensemble des places v de F telles que $n_v = n = 2$.

Remarquons que, si v est une place impaire de V divisant un nombre premier q, alors $q \equiv 3 \bmod 4$ (puisque $\mathbb{Q}_q \hookrightarrow F_v$) et v est décomposée dans $F/\mathbb{Q}$

(en effet, sinon le corps résiduel de F_v serait le corps fini à q^2 éléments et $q^2-1 \equiv 0 \bmod 8$).

Soit U l'ensemble des nombres premiers q telle qu'une place de V divise q. En fait, U est l'ensemble formé du nombre premier 2 et des nombres premiers congrus à 3 modulo 4. Alors

$$\phi = \prod_{q \in U} (-1, \eta\eta^{\sigma})_{m_w},$$

où w est une place de E divisant q. Mais, $\eta\eta^{\sigma} = \xi\xi^{\sigma^2}(\xi^{\sigma})^2$ et par conséquent

$$\phi = \prod_{q \in U} (-1, \mathrm{N}_{E/F}(\xi))_{m_w}.$$

Puisque $p \equiv 9 \bmod 16, p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$, on peut écrire $p = r^2 - 8s^2$ avec $r > 0, r \equiv 1 \bmod 8$ et s impair. Ainsi $2 = \mathrm{N}_{F/\mathbb{Q}}(x)$ où $x = \frac{r+\sqrt{p}}{2s}$ et on a $2 = \mathrm{N}_{F/\mathbb{Q}}(x) = \mathrm{N}_{F/\mathbb{Q}}(\mathrm{N}_{E/F}(\xi))$. En d'autres termes, $\mathrm{N}_{E/F}(\xi) = xy$ où $y \in F^*$ avec $\mathrm{N}_{F/\mathbb{Q}}(y) = 1$. Ceci signifie avec le théorème 90 de Hilbert qu'il existe $z \in F^*$ tel que $y = \frac{z}{z^{\sigma}}$. D'où

$$\phi = \phi_1\phi_2 \text{ où } \phi_1 = \prod_{q \in U} (-1, x)_{m_w} \text{ et } \phi_2 = \prod_{q \in U} (-1, y)_{m_w} = \prod_{q \in U} (-1, zz^{\sigma})_{m_w}.$$

Calculons d'abord ϕ_2 : on remarque que, si $v \in V$ et w est une place de E au-dessus de v, alors on a $(-1, z)_{m_w} = (-1, z)_{n_v}$, puisque $v(z) = w(z)$ (en effet v est non ramifiée dans E) et ces deux symboles de Hilbert sont modérés et ne dépendent que de la valuation v (cf [S1], Proposition 8, §3, Chap. XIV). Il en résulte que

$$\phi_2 = \prod_{q \in U} (-1, zz^{\sigma})_{m_w} = \prod_{v \in V} (-1, z)_{m_w} = \prod_{v \in V} (-1, z)_{n_v} = \prod_{v} (-1, z)_{n_v}^{\frac{n_v}{n}} = 1,$$

d'après la formule du produit.

Calculons maintenant ϕ_1 :

$$\phi_1 = \prod_{q \in U} (-1, x)_{m_w} = \prod_{q \in U} (-1, x)_{n_v},$$

pour des raisons analogues à celles fournies pour le calcul de ϕ_2 ; précisons encore que dans le premier produit, w désigne une place de E au-dessus de q et dans le second, v est une place de F au-dessus de q. Or, si $q \in U$, alors

$v \in V$ et $n_v = 2$; ainsi, si $(.,.)_{F_v}$ désigne le symbole de Hilbert classique à valeurs dans μ_2, alors $(-1,x)_{n_v} = (-1,x)_{F_v}$ et

$$\begin{aligned}\phi_1 &= \prod_{q\in U}(-1,x)_{F_v} = \prod_{q\in U}(-1,\frac{r+\sqrt{p}}{2s})_{F_v} \\ &= \prod_{q\in U}(-1,(r+\sqrt{p})s)_{F_v} = \prod_{q\in U}(-1,r+\sqrt{p})_{F_v}\ \prod_{q\in U}(-1,s)_{F_v}.\end{aligned}$$

Il est à noter que, si $q \in U$ et si v divise q alors $F_v = \mathbb{Q}_q$ et, de plus, si q divise s, alors $q \in U$ (en effet, $p = r^2 - 8s^2$). Par conséquent, on obtient

$$\prod_{q\in U}(-1,s)_{F_v} = (-1,s)_2 \prod_{q|s,\, q\,\text{impair}}(-1,s)_q = 1,$$

d'après la formule de produit. D'où

$$\phi_1 = \prod_{q\in U}(-1,r+\sqrt{p})_{F_v} = (-1,r+\sqrt{p})_2 \prod_{q\in U,\, q\,\text{impair}}(-1,r+\sqrt{p})_q\ .$$

Si $q \in U$ est impair, on a $(-1,r+\sqrt{p})_q = (-1,r-\sqrt{p})_q$ (il suffit de calculer le produit) et il est facile de voir que ces symboles sont triviaux si $q \nmid s$. Maintenant, si $q \mid s$, soit $r+\sqrt{p}$ soit $r-\sqrt{p}$ est une unité q-adique : sinon, en estimant la somme, q diviserait $2r$ ce qui est impossible puisque q divise déjà s. Il en résulte que l'un des symboles précédents est trivial, car modéré, et donc les deux sont triviaux. On obtient donc

$$\phi_1 = (-1,r+\sqrt{p})_2.$$

Écrivons $p = u^2$ avec $u \in \mathbb{Q}_2^*$. Puisque $p \equiv 9 \bmod 16$, on a $u \equiv \pm 3 \bmod 8$ dans $\mathbb{Q}_2^*$. Mais l'égalité $(-1,r+u)_2 = (-1,r-u)_2$ permet de choisir une racine carrée de p : ainsi posons $u \equiv 5 \bmod 8$. Or $r \equiv 1 \bmod 8$ de sorte que l'on peut écrire $r+u = 2(3+4\lambda)$ avec $\lambda \in \mathbb{Z}_2$. On conclut alors avec [S2] à l'égalité

$$\phi_1 = (-1,r+u)_2 = -1.$$

Ainsi, $\phi = \phi_1\ \phi_2 = -1$ et donc $\rho = 1$. Il en résulte la trivialité de $WK_2(E)(2)$.

On a donc montré la proposition suivante dont le contenu constitue la réciproque de la proposition 4.12 :

Proposition 4.13. *Soit* $p \equiv 1 \bmod 8$ *un nombre premier satisfaisant la condition* $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$ *et soit* E *une extension cyclique de* $\mathbb{Q}$ *de degré* 4 *qui contient* $\mathbb{Q}(\sqrt{p})$. *Alors, pour que* E *ait une 2-partie du noyau sauvage triviale, il faut et il suffit que* $p \equiv 9 \bmod 16$ *et que* E *soit l'unique sous-corps de* $\mathbb{Q}(\mu_p)$ *de degré* 4 *sur* $\mathbb{Q}$. *Plus précisément, dans ce cas,* E *est l'extension* $\mathbb{Q}\left(\sqrt{\epsilon\sqrt{p}}\right)$ *où* ϵ *est l'unité fondamentale de* $\mathbb{Q}(\sqrt{p})$.

4.2.2 Le cas général

On conserve toujours les notations introduites au début du paragraphe 2 de ce chapitre.
Comme suggéré par la proposition 4.6, la discussion sur le sous-corps quadratique $K = \mathbb{Q}(\sqrt{d})$ est le fil directeur de la détermination des 2-extensions cycliques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale.

• **Le cas $d = 2$, *i.e.*, $K = \mathbb{Q}(\sqrt{2})$**

Nous allons d'abord déterminer des conditions nécessaires à la trivialité de $WK_2(E)(2)$. Supposons donc que E contient $K = \mathbb{Q}(\sqrt{2})$ et que $WK_2(E)(2)$ est triviale. Le nombre premier 2 est totalement ramifié dans $E/\mathbb{Q}$ (cf proposition 4.3), et le lemme 4.8 assure que la place 2-adique de F appartient à $T_{E/F}$. Donc (lemme 4.7), au plus une place impaire $\mathfrak{L}$ de F se ramifie dans E. On peut même affirmer que, si $\mathfrak{L}$ est au-dessus du nombre premier ℓ, alors ℓ est inerte dans $K/\mathbb{Q}$, ce qui signifie que $\ell \equiv \pm 3 \bmod 8$.
Mais alors, comme E est non ramifiée en dehors de 2 et ℓ, on en déduit que E est contenue dans $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_\ell)$ (puisque E est une extension de degré une puissance de 2). En résumé, on a montré que si $WK_2(E)(2)$ est triviale, alors $E \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_\ell)$, où ℓ est un nombre premier tel que $\ell \equiv \pm 3 \bmod 8$.

Réciproquement, on montre par récurrence que toute 2-extension cyclique de $\mathbb{Q}$ contenue dans $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_\ell)$ avec ℓ premier $\equiv \pm 3 \bmod 8$ a une 2-partie du noyau sauvage triviale. Pour cela, il suffit de considérer une telle extension E et de supposer que $WK_2(F)(2) = 0$.

Il est facile de voir que la place 2-adique de F appartient à $T_{E/F}$ et donc

$$|T_{E/F}| = \begin{cases} 1 & \text{si } E \subset \mathbb{Q}(\mu_{2^\infty})\,; \\ 2 & \text{sinon.} \end{cases}$$

De plus, comme 2 est totalement ramifié dans $E/\mathbb{Q}$ et comme $\mu(\mathbb{Q}_2(\sqrt{2}))(2) = \mu_2$, on obtient $\mu(E_w)(2) = \mu_2$, où w est la place 2-adique de E. Par conséquent, d'après le corollaire 2.19, on voit que $\rho = 1$ et on a :

$$|\ WK_2(E)(2)_G\ | = \frac{2^{|T_{E/F}|-1}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]}\,.$$

Distinguons alors deux cas :

1° Supposons que $E \subset \mathbb{Q}(\mu_{2^\infty})$. Alors, $|T_{E/F}| = 1$ et on obtient directement la trivialité de $WK_2(E)(2)$.

2° Supposons que $E \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_\ell)$, où $\ell \equiv \pm 3 \bmod 8$, est ramifiée en ℓ. Alors $|T_{E/F}| = 2$ et $WK_2(E)(2)$ est triviale si et seulement si l'indice normique $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]$ vaut 2. Or avec les notations de la proposition 4.5, on a :

$$\begin{aligned}
[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)] = 2 &\iff 2+\alpha_r \notin \mathrm{N}_{E/F}(E^*), \\
&\iff 2+\alpha_r \notin \mathrm{N}_{M_{r+1}/M_r}(M_{r+1}^*).
\end{aligned}$$

En fait, $M_r = \mathbb{Q}_r = \mathbb{Q}(\sqrt{2+\alpha_r})$ et ℓ est le seul nombre premier qui se ramifie modérément dans M_{r+1}. Donc, comme M_{r+1} est cyclique, on a

$$M_{r+1} = \mathbb{Q}\left(\sqrt{(-1)^\alpha \ell (2+\alpha_r)}\right),$$

où $\alpha \in \{0, 1\}$.

Notons $\mathfrak{L}$ la place de M_r au-dessus de ℓ et $(\,.\,,\,.\,)_{\mathfrak{L}}$ le symbole de Hilbert défini sur le complété de M_r en $\mathfrak{L}$, à valeurs dans μ_2.
Ainsi le symbole local $(2+\alpha_r, (-1)^\alpha \ell(2+\alpha_r))_{\mathfrak{L}} = (2+\alpha_r, -(-1)^\alpha \ell)_{\mathfrak{L}}$ est non trivial, puisque, d'après le point (vii) de la proposition 1.23, on a :

$$\begin{aligned}
(2+\alpha_r, -(-1)^\alpha \ell)_{\mathfrak{L}} &= (\mathrm{N}_{M_r/\mathbb{Q}}(2+\alpha_r), -(-1)^\alpha \ell)_\ell\,, \\
&= (2, -(-1)^\alpha \ell)_\ell\,, \\
&= (2, \ell)_\ell \,=\, -1\,,
\end{aligned}$$

car $\ell \equiv \pm 3 \bmod 8$. Ainsi, on a montré que $2+\alpha_r$ n'est pas une norme localement à la place $\mathfrak{L}$, et donc $2+\alpha_r$ n'est pas non plus une norme globalement dans M_{r+1}/M_r. D'où $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)] = 2$, ce qui prouve la trivialité de $WK_2(E)(2)$.

En résumé, on a prouvé la proposition suivante :

Proposition 4.14. *Les 2-extensions cycliques de $\mathbb{Q}$ qui contiennent $\mathbb{Q}(\sqrt{2})$ et qui ont une 2-partie du noyau sauvage triviale sont exactement celles qui sont contenues dans la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_\ell)$ où ℓ est un nombre premier satisfaisant $\ell \equiv \pm 3 \bmod 8$.*

• **Le cas $d = p$ ou $2p$, avec $p \equiv 5 \bmod 8$**

Comme précédemment, on commence par déterminer des conditions nécessaires à la trivialité de $WK_2(E)(2)$. Supposons donc que E est une extension cyclique de $\mathbb{Q}$ de degré $\geqslant 4$ qui contient $K = \mathbb{Q}(\sqrt{d})$, avec $d = p$ ou $2p$ (où $p \equiv 5 \bmod 8$) et qui vérifie $WK_2(E)(2) = 0$. Le nombre premier p est ramifié dans $K/\mathbb{Q}$, donc dans E/F. Ainsi, la place $\mathfrak{p}$ de F au-dessus de p est un élément de $T_{E/F}$. De plus, comme $p \equiv 5 \bmod 8$, le premier 2 est non décomposé dans $K/\mathbb{Q}$, ce qui implique (cf proposition 4.3) que la place 2-adique de F est aussi non décomposée dans E. D'après le lemme 4.8, cette place est dans $T_{E/F}$. Par conséquent, le lemme 4.7 force $|T_{E/F}| = 2$. En particulier, cela signifie que E est non ramifiée en dehors de 2 et p ; autrement dit, on a montré que si $WK_2(E)(2)$ est triviale, alors E est contenue dans la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$.

Étudions maintenant la réciproque. Soit E une 2-extension cyclique de $\mathbb{Q}$ contenant $K = \mathbb{Q}(\sqrt{d})$ et contenue dans $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$. On veut montrer que $WK_2(E)(2) = 0$ et, pour cela, on procède par récurrence comme pour le cas précédent. Supposons alors que $WK_2(F)(2) = 0$. Il est facile de voir :
a) que l'ensemble $T_{E/F}$ est formé de la place 2-adique v de F et de la place de F au-dessus de p,
b) que $\mu(F_v)(2) = \mu(\mathbb{Q}_2(\sqrt{d}))(2) = \mu_2 = \mu(F)(2)$, car F est cyclique sur $\mathbb{Q}$.

Il en résulte que $|T_{E/F}| = 2$ et que $\rho = 1$ dans le corollaire 2.19, ce qui donne :

$$| WK_2(E)(2)_G | = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]} = \frac{2}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]}.$$

Puisque $2 \notin F^{*2}$, on a $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)] = 1$ si et seulement si $2 \in \mathrm{N}_{E/F}(E^*)$, ce qui est le cas, d'après la proposition 4.5, si et seulement si $2 \in \mathrm{N}_{K/\mathbb{Q}}(K^*)$. Or, comme $p \equiv 5 \bmod 8$, le corollaire 3.3 implique que $2 \notin \mathrm{N}_{K/\mathbb{Q}}(K^*)$. On obtient alors $[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)] = 2$, d'où la trivialité de $WK_2(E)(2)$.

On a ainsi prouvé la

Proposition 4.15. *Soit $d = p$ ou $2p$, avec p un nombre premier tel que $p \equiv 5 \bmod 8$. Alors les 2-extensions cycliques de $\mathbb{Q}$ qui contiennent $\mathbb{Q}(\sqrt{d})$ et qui ont une 2-partie du noyau sauvage triviale sont exactement celles qui sont contenues dans la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$.*

• **Le cas $d = p$, avec $p \equiv 1 \bmod 8$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$**

Considérons une 2-extension cyclique E de $\mathbb{Q}$ de degré $\geqslant 4$. Supposons de plus que $WK_2(E)(2)$ est triviale. Par un raisonnement analogue à celui fait pour les extensions cycliques de degré 4 (voir le début de la section 4.2.1), il n'est pas difficile de voir que nécessairement E est contenue dans le corps cyclotomique $\mathbb{Q}(\mu_p)$ et 2 doit être totalement décomposé dans $E/\mathbb{Q}$.

Or, d'après le corollaire 4.4, pour toute sous-extension L de E, le groupe $WK_2(L)(2)$ est aussi trivial. C'est le cas en particulier pour la sous-extension de E de degré 4 sur $\mathbb{Q}$. Ainsi, la proposition 4.13 implique que $p \equiv 9 \bmod 16$. Par conséquent, comme $[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p - 1 \equiv 8 \bmod 16$, il est clair que si $WK_2(E)(2)$ est triviale, alors E est soit l'unique sous-corps de $\mathbb{Q}(\mu_p)$ de degré 4 sur $\mathbb{Q}$, soit celui de degré 8. Pour ce qui concerne celui de degré 4, il suffit de se reporter à la proposition 4.13. Quant au cas du degré 8, on procède de la façon suivante.

Considérons donc l'unique sous-corps E de $\mathbb{Q}(\mu_p)$ de degré 8 sur $\mathbb{Q}$. Supposons, par ailleurs, que $p \equiv 9 \bmod 16$ et que 2 est totalement décomposé dans $E/\mathbb{Q}$. On veut savoir si $WK_2(E)(2)$ est triviale. On constate déjà que $|T_{E/F}| = 1$ puisque seul p se ramifie dans E et 2 est totalement décomposé dans E. Par ailleurs, il est facile de voir que E est totalement imaginaire et que F est totalement réel, ce qui veut dire que $\rho = 1$ dans la formule de genre du corollaire 2.19. En d'autres termes, de la formule suivante

$$\frac{\mid WK_2(E)(2)_G \mid}{\mid WK_2(F)(2) \mid} = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]},$$

il vient

$$\mid WK_2(E)(2)_G \mid = \frac{1}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]} = 1.$$

D'où la trivialité de $WK_2(E)(2)$.

Avant de conclure ce cas, donnons un lemme qui permet de traduire de manière un peu plus agréable le fait que 2 soit totalement décomposé dans E.

Lemme 4.16. *Soit $p \equiv 9 \bmod 16$ un nombre premier tel que $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$. Notons E l'unique sous-corps de $\mathbb{Q}(\mu_p)$ de degré 8 sur $\mathbb{Q}$. Alors*

$$2 \textit{ est totalement décomposé dans } E/\mathbb{Q} \Longleftrightarrow 2^{\frac{p-1}{8}} \equiv 1 \bmod p.$$

Démonstration. Soit f le degré résiduel du nombre premier 2 dans $\mathbb{Q}(\mu_p)/\mathbb{Q}$. Rappelons qu'alors (voir [W]) f est l'ordre de 2 dans le groupe multiplicatif

$(\mathbb{Z}/p\mathbb{Z})^\times$, *i.e.*, f est le plus petit entier non nul satisfaisant la congruence $2^f \equiv 1 \bmod p$. On en déduit successivement les équivalences suivantes :

$$\begin{aligned} \text{2 est totalement décomposé dans } E/\mathbb{Q} &\iff f \text{ est impair} \\ &\iff f \mid \tfrac{p-1}{8} \\ &\iff 2^{\frac{p-1}{8}} \equiv 1 \bmod p. \end{aligned}$$

$\square$

Il en résulte aisément la proposition suivante :

Proposition 4.17. *Soit* $p \equiv 1 \bmod 8$ *un nombre premier tel que* $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$. *Alors les* 2*-extensions cycliques de* $\mathbb{Q}$ *de degré* $\geqslant 4$*, qui contiennent* $\mathbb{Q}(\sqrt{p})$ *et qui ont une* 2*-partie du noyau sauvage triviale, sont :*

1^o *l'unique sous-corps* $\mathbb{Q}\left(\sqrt{\epsilon\sqrt{p}}\right)$ *de* $\mathbb{Q}(\mu_p)$ *de degré* 4 *sur* $\mathbb{Q}$*, où* $p \equiv 9 \bmod 16$ *et* ϵ *est l'unité fondamentale de* $\mathbb{Q}(\sqrt{p})$*,*

2^o *l'unique sous-corps de* $\mathbb{Q}(\mu_p)$ *de degré* 8 *sur* $\mathbb{Q}$*, où* $p \equiv 9 \bmod 16$ *et* $2^{\frac{p-1}{8}} \equiv 1 \bmod p$.

Remarquons au passage que $73, 89, 233, 281, 601, 937, 1049, 1097, 1193$ sont les dix plus petits nombres premiers p vérifiant $p \equiv 9 \bmod 16, p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$. Parmi ces nombres, seuls $73, 89, 233, 601, 937$ satisfont en plus la condition $2^{\frac{p-1}{8}} \equiv 1 \bmod p$.

Remarque : à l'aide du logiciel PARI, la conjecture de Birch-Tate permet de décider sur des exemples concrets de la trivialité de certains corps de nombres abéliens. Plus précisément, si E est un corps de nombres abélien, la conjecture de Birch-Tate affirme que

$$\zeta_E(-1) = \pm \frac{|K_2(o_E)|}{w_2(E)},$$

où ζ_E est la fonction zeta de Dedekind associée au corps E et $w_2(E)$ est un entier bien identifié : en effet, pour tout nombre premier p, la p-partie de $w_2(E)$ est la puissance maximale p^n telle que le groupe de Galois $\mathrm{Gal}(E(\mu_{p^n})/E)$ soit d'exposant 2. Par conséquent, lorsque l'on peut appliquer cette conjecture, *e.g.* lorsque E est un corps abélien totalement réel, on peut déterminer $|K_2(o_E)|$ et donc $|WK_2(E)(2)|$. Ainsi on retrouve avec PARI la trivialité de la 2-partie du noyau sauvage des extensions du 1^o de la proposition précédente pour les dix valeurs de p mentionnées ci-dessus.

• **Synthèse des résultats**

En regroupant les résultats démontrés dans les propositions 4.14, 4.15 et 4.17, on obtient le théorème suivant :

Théorème 4.18. *Les 2-extensions cycliques de $\mathbb{Q}$ de degré $\geqslant 4$ dont la 2-partie du noyau sauvage est triviale sont :*

1. *les 2-extensions cycliques de $\mathbb{Q}$ de degré $\geqslant 4$, contenues dans la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$, où p est un nombre premier tel que $p \equiv \pm 3 \bmod 8$,*
2. *l'unique sous-corps de $\mathbb{Q}(\mu_p)$ de degré 4 sur $\mathbb{Q}$, où $p \equiv 9 \bmod 16$,*
3. *l'unique sous-corps de $\mathbb{Q}(\mu_p)$ de degré 8 sur $\mathbb{Q}$, où $p \equiv 9 \bmod 16$ et $2^{\frac{p-1}{8}} \equiv 1 \bmod p$.*

On peut être légèrement plus explicite concernant le point 1. du théorème. En effet, on peut remarquer (comme cela est fait dans [Gr1]) que lorsque $p \equiv 3 \bmod 8$, la 2-extension maximale contenue dans $\mathbb{Q}(\mu_p)$ est $\mathbb{Q}(\sqrt{-p})$, et lorsque $p \equiv 5 \bmod 8$, la 2-extension maximale contenue dans $\mathbb{Q}(\mu_p)$ est $\mathbb{Q}\left(\sqrt{2\sqrt{p}(a-\sqrt{p})}\right)$, où $p = a^2+b^2$ avec a impair. Par conséquent, le théorème précédent devient :

Théorème 4.19. *Les 2-extensions cycliques de $\mathbb{Q}$ de degré $\geqslant 4$ dont la 2-partie du noyau sauvage est triviale sont :*

1. *les sous-extensions cycliques de $\mathbb{Q}$ de degré $\geqslant 4$, contenues dans la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\sqrt{-p})$, où p est un nombre premier tel que $p \equiv 3 \bmod 8$,*
2. *les sous-extensions cycliques de $\mathbb{Q}$ de degré $\geqslant 4$, contenues dans la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}\left(\sqrt{2\sqrt{p}(a-\sqrt{p})}\right)$, où p est un nombre premier tel que $p \equiv 5 \bmod 8$ et $p = a^2 + b^2$ (avec a impair),*
3. *l'unique sous-corps de $\mathbb{Q}(\mu_p)$ de degré 4 sur $\mathbb{Q}$, où $p \equiv 9 \bmod 16$,*
4. *l'unique sous-corps de $\mathbb{Q}(\mu_p)$ de degré 8 sur $\mathbb{Q}$, où $p \equiv 9 \bmod 16$ et $2^{\frac{p-1}{8}} \equiv 1 \bmod p$.*

4.3 Analogie avec le noyau modéré positif

Le problème de la détermination des 2-extensions de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale est évidemment à mettre en relation avec celui de la détermination des 2-extensions de $\mathbb{Q}$ dont la 2-partie du noyau modéré positif est triviale. Or ce dernier problème a été résolu par G. Gras dans l'article [Gr1]. La notion de noyau modéré positif ayant été introduite au chapitre 1, on peut énoncer le résultat suivant (c'est un corollaire de Theorem 2, [Gr1]) :

Théorème 4.20. *Les 2-extensions* abéliennes *de $\mathbb{Q}$ dont la 2-partie du noyau modéré positif est triviale sont :*

1. *les sous-corps de la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\sqrt{-p})$, où p est un nombre premier tel que $p \equiv 3 \bmod 8$,*
2. *les sous-corps de la composée $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}\left(\sqrt{2\sqrt{p}(a-\sqrt{p})}\right)$, où p est un nombre premier tel que $p \equiv 5 \bmod 8$ et $p = a^2 + b^2$ (avec a impair).*

Comme le noyau sauvage est un sous-groupe du noyau modéré positif, il n'est pas étonnant de retrouver certaines extensions mentionnées ci-dessus dans le théorème 4.19. Cependant, il est intéressant de mettre l'accent sur les extensions dont la 2-partie du noyau sauvage est triviale sans que la 2-partie du noyau modéré positif le soit.

Proposition 4.21. *Les 2-extensions cycliques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale et dont la 2-partie du noyau modéré positif ne l'est pas sont les suivantes :*

(i) $\mathbb{Q}(\sqrt{-p})$ *où p est un nombre premier tel que $p \equiv 7 \bmod 8$,*

(ii) $\mathbb{Q}(\sqrt{p})$ *où p est un nombre premier tel que $p \equiv 1 \bmod 8$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$,*

(iii) $\mathbb{Q}(\sqrt{pq})$ *où p, q sont des nombres premiers tels que $p \equiv q \equiv 3 \bmod 8$,*

(iv) $\mathbb{Q}(\sqrt{-pq})$ *où p, q sont des nombres premiers tels que $p \equiv -q \equiv 3 \bmod 8$,*

(v) l'unique sous-corps de degré 4 de $\mathbb{Q}(\mu_p)$ où p est un nombre premier tel que $p \equiv 9 \bmod 16, p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$,

(vi) l'unique sous-corps de degré 8 de $\mathbb{Q}(\mu_p)$ où p est un nombre premier tel que $p \equiv 9 \bmod 16$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$ et $2^{\frac{p-1}{8}} \equiv 1 \bmod p$.

À présent, l'objectif serait d'obtenir un résultat analogue à celui de G. Gras en déterminant les 2-extensions *abéliennes* de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. C'est l'objet du chapitre qui suit.

Chapitre 5

2-extensions abéliennes de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale

Pour conclure sur l'étude de la trivialité de la 2-partie du noyau sauvage des 2-extensions abéliennes de $\mathbb{Q}$, on se propose dans ce chapitre de regrouper quelques résultats sur le sujet. Dans un premier temps, on détermine toutes les 2-extensions abéliennes de $\mathbb{Q}$ qui sont totalement réelles et dont la 2-partie du noyau sauvage est triviale. Dans un second temps, après avoir rappelé les résultats de [Gr1], [KM2] et [Gri], on s'intéresse à un cas particulier qui concerne les extensions imaginaires. Enfin, on termine le chapitre en décrivant certaines extensions pour lesquelles on n'est pas encore en mesure de décider de l'éventuelle trivialité de la 2-partie du noyau sauvage.

5.1 Extensions totalement réelles

Nous allons consacrer cette partie à la détermination des 2-extensions *abéliennes de $\mathbb{Q}$ totalement réelles* dont la 2-partie du noyau sauvage est triviale. Rappelons d'abord que la proposition 3.5 traite le cas des extensions quadratiques, et le théorème 4.19 contient celui des extensions cycliques de degré 4. Quant aux autres cas, l'étude repose essentiellement sur la proposition suivante démontrée par M. Kolster et A. Movahhedi (cf [KM2], Proposition 1.2) :

Proposition 5.1. *Considérons E/F une extension bi-quadratique de corps de nombres totalement réels telle que $E/\mathbb{Q}$ soit abélienne. Notons F_i, $i = 1, 2, 3,$ les sous-corps quadratiques de E/F. Soit $\delta = \delta_{E/F}$ le nombre de* *places 2-adiques de F non décomposées dans E, telles que $|\mu(F_v)(2)| = 2$, et E_w est le premier étage de la $\mathbb{Z}_2$-extension cyclotomique de $F_v(\sqrt{-1})$. Alors*

$$2^{\delta}\,|WK_2(F)(2)|^2\,|WK_2(E)(2)| = \prod_{i=1}^{3} |WK_2(F_i)(2)|\,.$$

Remarquons que la preuve de cette proposition repose essentiellement sur la conjecture de Birch-Tate évoquée page 86. De plus, il en découle immédiatement le résultat suivant (cf [KM2], Proposition 4.1), qui traite donc le cas des extensions bi-quadratiques totalement réelles de $\mathbb{Q}$:

Proposition 5.2. *Les extensions bi-quadratiques totalement réelles dont la 2-partie du noyau sauvage est triviale sont celles apparaissant dans la liste suivante :*

$$(L) : \begin{cases} \mathbb{Q}(\sqrt{2}, \sqrt{p}) & p \equiv \pm 3 \bmod 8 \\ \mathbb{Q}(\sqrt{2^a p}, \sqrt{2^a q}) & p \equiv q \equiv 3 \bmod 8, a \in \{0,1\} \\ \mathbb{Q}(\sqrt{pq}, \sqrt{qr}) & p \equiv q \equiv r \equiv 3 \bmod 8 \end{cases}$$

où p, q et r sont des nombres premiers distincts.

Par conséquent, afin d'avoir la complète résolution de ce problème, il nous reste à étudier le cas des 2-extensions abéliennes de $\mathbb{Q}$ qui sont totalement réelles et de degré au moins 8 sur $\mathbb{Q}$. Nous commençons par rappeler un résultat de [Gri] :

Proposition 5.3. *Il n'existe pas d'extension multi-quadratique totalement réelle de degré au moins 8 sur $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale.*

Démonstration. Cela découle du fait qu'il n'existe pas d'extension tri-quadratique totalement réelle de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. Pour la commodité du lecteur, nous allons en donner une preuve. Soit $E/\mathbb{Q}$ une extension tri-quadratique (c'est-à-dire $\mathrm{Gal}(E/\mathbb{Q}) \simeq C_2 \times C_2 \times C_2$). On peut écrire $E = \mathbb{Q}(\sqrt{d}, \sqrt{d_1}, \sqrt{d_2})$ où d, d_1, d_2 sont des entiers $\geqslant 2$; on peut aussi supposer que d est divisible par un nombre premier impair, qui ne divise ni d_1 ni d_2. Ainsi, l'extension E/K, où $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, est modérément ramifiée et le corollaire 2.17 implique que $WK_2(K)(2) = 0$ (car $WK_2(E)(2) = 0$). Le corps K doit donc apparaître dans la liste (L) de la proposition 5.2.

Si K est de la forme $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ avec $p \equiv \pm 3 \bmod 8$, on peut supposer que ni 2, ni p ne divise d. Par conséquent, un argument de ramification modérée montre que $\mathbb{Q}(\sqrt{2}, \sqrt{d})$ apparaît dans (L), ce qui implique que d est un nombre premier $\equiv \pm 3 \bmod 8$.

$$\begin{tikzcd}[column sep=small]
 & E = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{d}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt{2}, \sqrt{p}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}, \sqrt{pd}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}, \sqrt{d}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2}) &
\end{tikzcd}$$

Si l'on applique maintenant la proposition 5.1 à l'extension $E/\mathbb{Q}(\sqrt{2})$, on obtient $\delta_{E/\mathbb{Q}(\sqrt{2})} = 0$ et les trois corps intermédiaires doivent apparaître dans (L). D'où une contradiction, puisque $\mathbb{Q}(\sqrt{2}, \sqrt{pd})$ n'apparaît pas dans (L).

Si K est de la forme $\mathbb{Q}(\sqrt{2^a p}, \sqrt{2^a q})$ avec $p \equiv q \equiv 3 \bmod 8, a \in \{0, 1\}$, on peut supposer que ni p, ni q ne divise d. Comme précédemment, le corps $\mathbb{Q}(\sqrt{2^a p}, \sqrt{d})$ est dans la liste (L), et donc $d = 2^a \ell$, pour un certain nombre premier $\ell \equiv 3 \bmod 8$ distinct de p et q.

$$\begin{tikzcd}[column sep=small]
 & E = \mathbb{Q}(\sqrt{2^a p}, \sqrt{2^a q}, \sqrt{2^a \ell}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt{2^a p}, \sqrt{2^a q}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2^a p}, \sqrt{2^a \ell}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2^a p}, \sqrt{q\ell}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2^a p}) &
\end{tikzcd}$$

La formule du produit de la proposition 5.1 donne $\delta_{E/\mathbb{Q}(\sqrt{2^a p})} = 0$, ce qui est contradictoire puisque le corps intermédiaire $\mathbb{Q}(\sqrt{2^a p}, \sqrt{q\ell})$ n'apparaît pas dans (L).

Enfin, si K est de la forme $\mathbb{Q}(\sqrt{pq}, \sqrt{qr})$, où $p \equiv q \equiv r \equiv 3 \bmod 8$, on a le diagramme

$$\begin{tikzcd}[column sep=small]
 & E = \mathbb{Q}(\sqrt{pq}, \sqrt{qr}, \sqrt{d}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt{pq}, \sqrt{qr}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{pq}, \sqrt{d}) \arrow[d, dash] & \mathbb{Q}(\sqrt{pq}, \sqrt{dqr}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{pq}) &
\end{tikzcd}$$

On obtient encore $\delta_{E/\mathbb{Q}(\sqrt{pq})} = 0$ et la proposition 5.1 implique que $\mathbb{Q}(\sqrt{pq}, \sqrt{d})$ est un corps intervenant dans la liste (L). Quitte à échanger les rôles de p et q, il en résulte que $d = q\ell$ pour un nombre premier $\ell \equiv 3 \bmod 8$ distinct de p, q et r. Mais, l'autre corps intermédiaire $\mathbb{Q}(\sqrt{pq}, \sqrt{dqr}) = \mathbb{Q}(\sqrt{pq}, \sqrt{\ell r})$ devrait aussi appartenir à la liste (L). D'où une contradiction. $\square$

Nous sommes maintenant en mesure de traiter le cas général des 2-extensions abéliennes totalement réelles de $\mathbb{Q}$:

Proposition 5.4. *Soit E une 2-extension abélienne de $\mathbb{Q}$ qui est totalement réelle, de degré supérieur ou égal à 8 sur $\mathbb{Q}$, et qui vérifie $WK_2(E)(2) = 0$. Alors, il existe un nombre premier $p \equiv \pm 3 \bmod 8$ tel que $E \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$.*

Démonstration. Raisonnons par récurrence sur le degré $[E : \mathbb{Q}]$.
a) Le cas $[E : \mathbb{Q}] = 8$
(i) Si $E/\mathbb{Q}$ est cyclique, le travail a été fait au chapitre 4.

(ii) D'après la proposition 5.3, E ne peut pas être tri-quadratique.

(iii) Si $\mathrm{Gal}(E/\mathbb{Q}) \simeq C_4 \times C_2$, nous devons préalablement fixer quelques notations : désignons par F_1 et F_2 les deux C_4-extensions contenues dans E et par F_3 l'unique extension bi-quadratique contenue dans E. Soit K l'intersection de F_1 et F_2 . Pour résumer, nous avons le diagramme suivant :

$$\begin{tikzcd}[column sep=small]
 & E \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
F_1 \arrow[dr, no head] & F_2 \arrow[d, no head] & F_3 \arrow[dl, no head] \\
 & K \arrow[d, no head] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Supposons, dans un premier temps, que $K \neq \mathbb{Q}(\sqrt{2})$. Alors E/F_3 est modérément ramifiée, et donc $WK_2(F_3)(2) = 0$. D'après la proposition 5.2 et le corollaire 4.2, nous avons $F_3 = \mathbb{Q}(\sqrt{2}, \sqrt{p})$, où $p \equiv 5 \bmod 8$. Or, $\delta_{E/K} = 0$ dans la formule du produit, et par suite, nous obtenons $WK_2(F_i)(2) = 0, i = 1, 2, 3$. Ainsi, $E \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$ en appliquant le théorème 4.19 à F_1 et F_2.
Supposons maintenant que $K = \mathbb{Q}(\sqrt{2})$. La proposition 5.1 nous donne :

$$2^{\delta_{E/K}} = \prod_{i=1}^{3} |WK_2(F_i)(2)| \, ,$$

où $\delta_{E/K}$ est égal à 0 ou 1. Supposons que $WK_2(F_3)(2) \neq 0$; alors $\delta_{E/K} = 1$ et $WK_2(F_1)(2) = WK_2(F_2)(2) = 0$; ainsi, F_1 ou F_2 est de la forme $\mathbb{Q}\left(\sqrt{p(2+\sqrt{2})}\right)$ avec p premier tel que $p \equiv \pm 3 \bmod 8$ et, pour une place 2-adique w de E, $E_w = \mathbb{Q}_2(\mu_{16})$ devrait contenir $\mathbb{Q}_2(\sqrt{\pm 3})$, ce qui mène à une contradiction. D'où, $WK_2(F_3)(2) = 0$ et donc $F_3 = \mathbb{Q}(\sqrt{2}, \sqrt{p})$, où p est un nombre premier $\equiv \pm 3 \bmod 8$. Par un argument similaire au précédent, nous obtenons $\delta_{E/K} = 0$, ce qui donne $WK_2(F_1)(2) = WK_2(F_2)(2) = 0$; il est maintenant clair avec le chapitre 4 que $E = F_1F_2 \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$.

b) Le cas $[E : \mathbb{Q}] > 8$
On peut déjà supposer que $E/\mathbb{Q}$ n'est pas cyclique. D'autre part, si E est non ramifiée en dehors de 2, E est contenue dans $\mathbb{Q}(\mu_{2^\infty})$, ce qui démontre ce qu'on voulait. Sinon, au moins un nombre premier impair se ramifie dans $E/\mathbb{Q}$. Ainsi, si on considère le groupe d'inertie de ce nombre premier, on peut montrer qu'il existe un corps F_1 tel que $[E : F_1] = 2$ et E/F_1 est modérément ramifiée. Comme $E/\mathbb{Q}$ n'est pas cyclique, il existe un sous-corps F de F_1 tel que E/F est bi-quadratique. Par ailleurs, notons F_2 et F_3 les deux autres corps intermédiaires de E/F. La situation est donc la suivante :

$$\begin{tikzcd}
F_1 \arrow[rr, dash] \arrow[dd, dash] & & E \arrow[dd, dash] \\
& F_2 \arrow[ur, dash] & \\
F \arrow[rr, dash] \arrow[ur, dash] & & F_3
\end{tikzcd}$$

Si $WK_2(E)(2) = 0$, alors $WK_2(F_1)(2) = 0$ (car E/F_1 est modérément ramifiée). D'où, par hypothèse de récurrence, il existe un nombre premier $p \equiv \pm 3 \bmod 8$ tel que $F_1 \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$ et donc $WK_2(F)(2) = 0$ (car $F \subset F_1$). La formule du produit mène à :

$$2^{\delta_{E/F}} = \prod_{i=2}^{3} |WK_2(F_i)(2)| \,.$$

Mais, puisque F ne possède qu'une seule place 2-adique, $\delta_{E/F} = 0$ ou 1, et donc, sans restriction, on peut supposer que $WK_2(F_2)(2) = 0$. Ainsi, il existe un nombre premier $q \equiv \pm 3 \bmod 8$ tel que $F_2 \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_q)$. Il ne reste plus qu'à montrer que $p = q$.

Si $p \neq q$, alors F est nécessairement un corps de nombres totalement réel, non ramifié en dehors de 2, et par conséquent F est contenue dans la $\mathbb{Z}_2$-

extension cyclotomique de $\mathbb{Q}$; autrement dit, si $[E:\mathbb{Q}]=2^{n+2}$ et si la suite $(\alpha_k)_{k\in\mathbb{N}}$ est définie par $\alpha_0=0$ et $\alpha_{k+1}=\sqrt{2+\alpha_k}$, alors $F=\mathbb{Q}(\alpha_n)$. Par ailleurs, on peut supposer que F_1/F est ramifiée en p et F_2/F en q (sinon le résultat est facile à obtenir). Si $\delta_{E/F}=1$, nous aurions pour une place 2-adique w de E : $E_w=\mathbb{Q}_2(\mu_{2^{n+3}})=\mathbb{Q}_2(\sqrt{-1},\sqrt{2+\alpha_n})$; d'où, le groupe de Galois de $E/\mathbb{Q}$ serait $C_{2^{n+1}}\times C_2$ et, quitte à échanger F_1 et F_2, nous pourrions supposer que F_1 est cyclique. Ainsi, nous aurions $F_1=\mathbb{Q}(\sqrt{p(2+\alpha_n)})$ et donc E_w contiendrait $\mathbb{Q}_2(\sqrt{p})=\mathbb{Q}_2(\sqrt{\pm 3})$, ce qui est contradictoire. Nous en déduisons donc que $\delta_{E/F}=0$ et, par conséquent, $WK_2(F_3)(2)=0$. Maintenant, $F_3\subset\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_r)$ avec $r\equiv\pm 3 \bmod 8$. $E=F_1F_2$ est non ramifiée en dehors de 2, p et q, ce qui nous permet de supposer que $r=p$ (quitte à remplacer p par q). Finalement, on a $E=F_1F_3\subset\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$, ce qui contredit le fait que q se ramifie dans $E/\mathbb{Q}$. Donc l'hypothèse $p\neq q$ était absurde, et on a effectivement $p=q$. □

En conclusion, nous avons démontré le

Théorème 5.5. *Les 2-extensions abéliennes de $\mathbb{Q}$ totalement réelles dont la 2-partie du noyau sauvage est triviale sont :*

(1) $\mathbb{Q}(\sqrt{p})$ *où p est un nombre premier tel que* $p\equiv 1 \bmod 8$, $p\neq x^2-32y^2$, $x>0$, $x\equiv 1 \bmod 4$,

(2) $\mathbb{Q}(\sqrt{pq})$ *où p,q sont deux nombres premiers tels que* $p\equiv q\equiv 3 \bmod 8$,

(3) l'unique sous-corps de degré 4 de $\mathbb{Q}(\mu_p)$ *où p est un nombre premier tel que* $p\equiv 9 \bmod 16, p\neq x^2-32y^2, x>0, x\equiv 1 \bmod 4$,

(4) $\mathbb{Q}(\sqrt{2^a p},\sqrt{2^a q})$ *où p,q sont des nombres premiers distincts tels que* $p\equiv q\equiv 3 \bmod 8, a\in\{0,1\}$,

(5) $\mathbb{Q}(\sqrt{pq},\sqrt{qr})$ *où p,q,r sont des nombres premiers distincts tels que* $p\equiv q\equiv r\equiv 3 \bmod 8$,

(6) les 2-extensions totalement réelles contenues dans $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$ *où p est un nombre premier tel que* $p\equiv\pm 3 \bmod 8$.

Remarque : pour les 2-extensions abéliennes de $\mathbb{Q}$ totalement réelles de degré $\geqslant 8$, la trivialité de la 2-partie du noyau sauvage est équivalente à celle de la 2-partie du noyau modéré positif.

5.2 Extensions imaginaires

Nous nous intéressons pour finir à l'étude de la trivialité de la 2-partie du noyau sauvage des 2-extensions abéliennes de $\mathbb{Q}$ imaginaires. Il est facile de voir que cela revient à considérer les extensions CM. En dehors des cas déjà traités dans les chapitres précédents, ce problème a aussi été résolu pour les 2-extensions multi-quadratiques de $\mathbb{Q}$, comme nous allons le rappeler ci-dessous. Pour le reste, cela semble plus délicat, et c'est pourquoi on termine ce dernier chapitre par un exemple concret d'extension qui illustre les difficultés rencontrées dans le cas imaginaire.

5.2.1 Quelques résultats bien connus

• Pour le cas général, on sait avec [Gr1] que toutes les sous-extensions de $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$, avec p premier tel que $p \equiv \pm 3 \bmod 8$, ont une 2-partie du noyau sauvage triviale.

• D'autre part, l'étude de la trivialité de la 2-partie du noyau sauvage des 2-extensions abéliennes de $\mathbb{Q}$ a été traitée pour la classe des extensions multi-quadratiques. En effet, M. Kolster et A. Movahhedi (cf [KM2]) ont démontré que la liste des extensions bi-quadratiques de $\mathbb{Q}$, imaginaires, dont la 2-partie du noyau sauvage est triviale est la suivante :

$\mathbb{Q}(\sqrt{-1}, \sqrt{2})$

$\mathbb{Q}(\sqrt{-1}, \sqrt{q})$ avec $q \equiv \pm 3 \bmod 8$

$\mathbb{Q}(\sqrt{-1}, \sqrt{2q})$ avec $q \equiv \pm 3 \bmod 8$

$\mathbb{Q}(\sqrt{-2}, \sqrt{q})$ avec $q \equiv \pm 3 \bmod 8$

$\mathbb{Q}(\sqrt{-2}, \sqrt{2q})$ avec $q \equiv \pm 3 \bmod 8$

$\mathbb{Q}(\sqrt{-1}, \sqrt{q})$ avec $q \equiv 7 \bmod 16$

$\mathbb{Q}(\sqrt{-1}, \sqrt{2q})$ avec $q \equiv 7 \bmod 16$

$\mathbb{Q}(\sqrt{-2}, \sqrt{q})$ avec $q \equiv 7 \bmod 16$

$\mathbb{Q}(\sqrt{-2}, \sqrt{2q})$ avec $q \equiv 7 \bmod 16$

$\mathbb{Q}(\sqrt{-1}, \sqrt{pq})$ avec $p \equiv -q \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{-1}, \sqrt{2pq})$ avec $p \equiv -q \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{-2}, \sqrt{pq})$ avec $p \equiv -q \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{-2}, \sqrt{2pq})$ avec $p \equiv -q \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{2}, \sqrt{-q})$ avec $q \equiv \pm 3 \bmod 8$

$\mathbb{Q}(\sqrt{2}, \sqrt{-pq})$ avec $p \equiv -q \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{2}, \sqrt{-q})$ avec $q \equiv 7 \bmod 16$

$\mathbb{Q}(\sqrt{p}, \sqrt{-q})$ avec $p \equiv -q \equiv \pm 3 \bmod 8$

$\mathbb{Q}(\sqrt{2p}, \sqrt{-2q})$ avec $p \equiv -q \equiv \pm 3 \bmod 8$

$\mathbb{Q}(\sqrt{p}, \sqrt{-q})$ avec $p \equiv \pm 3 \bmod 8,\ q \equiv 7 \bmod 8$ et $\left(\dfrac{p}{q}\right) = -1$

$\mathbb{Q}(\sqrt{2p}, \sqrt{-q})$ avec $p \equiv \pm 3 \bmod 8,\ q \equiv 7 \bmod 8$ et $\left(\dfrac{p}{q}\right) = -1$

$\mathbb{Q}(\sqrt{p}, \sqrt{-q})$ avec $p \equiv -q \equiv 1 \bmod 8,$
$p \neq x^2 - 32y^2,\ x > 0,\ x \equiv 1 \bmod 4$ et $\left(\dfrac{p}{q}\right) = -1$

$\mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ avec $p \equiv q \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{-2p}, \sqrt{-2q})$ avec $p \equiv q \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{pq}, \sqrt{-r})$ avec $p \equiv q \equiv 3 \bmod 8,\ r \equiv 7 \bmod 8$ et $\left(\dfrac{pq}{r}\right) = -1$

$\mathbb{Q}(\sqrt{pq}, \sqrt{-qr})$ avec $p \equiv q \equiv -r \equiv 3 \bmod 8$

$\mathbb{Q}(\sqrt{-2^b p}, \sqrt{-q})$ avec $b \in \{0, 1\},\ p \equiv \pm 3 \bmod 8,\ q \equiv 7 \bmod 8$
et $\left(\dfrac{p}{q}\right) = -1$

$\mathbb{Q}(\sqrt{-pq}, \sqrt{-r})$ avec $p \equiv -q \equiv 3 \bmod 8,\ r \equiv 7 \bmod 8$ et $\left(\dfrac{q}{r}\right) = -1$

$\mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ avec $p \equiv q \equiv 7 \bmod 8, \left(\dfrac{q}{p}\right) = -1$ et
$q^{\frac{h}{4}} \neq n^2 + 2pm^2, q \not| m,$ où $h = |Cl(\mathbb{Q}(\sqrt{-2p}))|$

où p, q et r sont des nombres premiers distincts.

De plus, R. Griffiths (cf [Gri]) a complété ce travail pour déterminer finalement l'ensemble des 2-extensions multi-quadratiques de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale. Il faut donc ajouter à la liste ci-dessus et à la liste de la proposition 5.2 les extensions suivantes :

$$\begin{array}{lll}
\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{pq}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p}) & \text{avec} & p \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{t}) & \text{avec} & t \equiv 7 \bmod 16 \\
\mathbb{Q}(\sqrt{-1}, \sqrt{p}, \sqrt{q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{-1}, \sqrt{2p}, \sqrt{2q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{-1}, \sqrt{2p}, \sqrt{q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{-2}, \sqrt{p}, \sqrt{q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{-2}, \sqrt{2p}, \sqrt{2q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \text{ et } \left(\dfrac{p}{q}\right) = 1 \\
\\
\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p}, \sqrt{q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8
\end{array}$$

où p, q et t sont des nombres premiers distincts.

• Il résulte de ce qui précède que, si F est l'une des extensions suivantes :

$$\begin{array}{lll}
\mathbb{Q}(\sqrt{-1}, \sqrt{pq}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8 \\
\mathbb{Q}(\sqrt{-1}, \sqrt{t}) & \text{avec} & t \equiv 7 \bmod 16 \\
\mathbb{Q}(\sqrt{-1}, \sqrt{p}, \sqrt{q}) & \text{avec} & p \equiv -q \equiv \pm 3 \bmod 8
\end{array}$$

où p, q et t sont des nombres premiers distincts, alors tous les étages de la $\mathbb{Z}_2$-extension cyclotomique de F ont aussi une 2-partie du noyau sauvage triviale, ce qui fournit de nouvelles familles de 2-extensions abéliennes de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale.

Remarquons que ce dernier résultat est une application directe du cas (a) de la formule de genre 2.18.

5.2.2 Une première approche

Soit E une 2-extension imaginaire, abélienne de $\mathbb{Q}$ et F son sous-corps réel maximal. On sait, d'après la Proposition 2.16, que, si $WK_2(E)(2) = 0$, alors $WK_2(F)(2) = 0$ ou $WK_2(F)(2) \cong \mathbb{Z}/2\mathbb{Z}$. Nous allons dans la suite déterminer des conditions nécessaires et suffisantes à la trivialité de

$WK_2(E)(2)$ sous réserve que $WK_2(F)(2)$ est triviale.

Désormais, nous supposons que $WK_2(F)(2) = 0$. L'intérêt de faire cette hypothèse réside dans le fait que l'on sache décrire de telles extensions puisque l'on a déjà traité le cas des 2-extensions abéliennes totalement réelles de $\mathbb{Q}$ à la section 5.1. Ainsi, on peut espérer en déduire des conditions équivalentes à $WK_2(E)(2) = 0$. Or, d'après ce qui a déjà été fait, on peut supposer que $[F : \mathbb{Q}] \geqslant 4$, *i.e.*, $[E : \mathbb{Q}] \geqslant 8$, et, d'après le théorème 5.5, on est dans l'un des cas suivants :

(i) $K_2(o_F)^+(2) = 0$;

(ii) F est l'unique sous-corps de degré 4 de $\mathbb{Q}(\mu_p)$ où p est un premier tel que $p \equiv 9 \bmod 16$, $p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4$;

(iii) $F = \mathbb{Q}(\sqrt{2^c p}, \sqrt{2^c q})$ où p, q sont des premiers tels que $p \equiv q \equiv 3 \bmod 8, c \in \{0, 1\}$;

(iv) $F = \mathbb{Q}(\sqrt{pq}, \sqrt{qr})$ où p, q, r sont des premiers tels que $p \equiv q \equiv r \equiv 3 \bmod 8$.

Dans ce cas, le corollaire 2.19 nous donne une équivalence que l'on va constamment utiliser dans la suite :

$$WK_2(E)(2) = 0 \Longleftrightarrow |T_{E/F}| = 1 + a, \tag{5.1}$$

où, par définition, $2^a = [D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]$.

Le cas (i) où $K_2(o_F)^+(2) = 0$

I. S'il existe une sous-extension M de F telle que E/M est une extension cyclique de degré 4, alors on a nécessairement $K_2(o_E)^+(2) = 0$. En effet, par hypothèse, on sait (voir page 32) qu'il existe une unique place v de F telle que $\mu(F_v)(2) = \mu(F)(2) = \mu_2$. Comme E/M est cyclique, il existe une unique place w de E au-dessus de v ; par ailleurs, on peut montrer que $\mu(E_w)(2) = \mu(F_v)(2) = \mu_2$. D'où, avec la suite exacte page 32, $WK_2(E)(2) \cong K_2(o_E)^+(2)$ et donc la trivialité de $WK_2(E)(2)$ est équivalente à celle de $K_2(o_E)^+(2)$, problème que l'on sait résoudre (cf [Gr1]).

II. Sinon, en considérant la décomposition d'un p-groupe abélien en produit de groupes cycliques, il est facile de voir que l'on peut écrire $E = F(\sqrt{-d})$ où d est un entier positif. On peut aussi supposer que $K_2(o_E)^+(2) \neq 0$; en particulier, $d > 2$. Rappelons que

$$WK_2(F)(2) = 0 \Longleftrightarrow F \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p),$$

où p est un nombre premier congru à ± 3 modulo 8, et

$$WK_2(E)(2) = 0 \Longrightarrow |T_{E/F}| \leqslant 2.$$

II.A. Si F est cyclique sur $\mathbb{Q}$, on doit distinguer quelques cas. Notons d'abord K le sous-corps quadratique de F. Puisque F est totalement réel et contenu dans $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$, on obtient trois possibilités pour K :

II.A.1. Si $K = \mathbb{Q}(\sqrt{2})$
On peut supposer sans restriction que d est impair.

II.A.1.a. Si F est non ramifiée en dehors de 2, on peut écrire $F = \mathbb{Q}(\alpha_n)$ où $n \geqslant 2$. L'entier impair d a au plus deux diviseurs premiers ; si $d = q$ est un nombre premier, alors, d'après l'équivalence (5.1), $WK_2(E)(2) = 0$ si et seulement si les conditions suivantes sont satisfaites :
$q \equiv \pm 1 \bmod 8$ (rappelons que $K_2(o_E)^+(2) \neq 0$),
q est décomposé dans K et non décomposé dans F/K,
la place 2-adique de F est décomposée dans E/F, *i.e.*, $-q \equiv 1 \bmod 8$,
et $a = 1$, *i.e.* $2 + \alpha_n$ n'est pas une norme dans E/F.
Il résulte de la Proposition 3.5 de [KM2] que les trois premières conditions sont équivalentes à $q \equiv 7 \bmod 16$. La dernière condition est, elle, équivalente au fait que le symbole de Hilbert $(2 + \alpha_n, -q)_{F_\mathfrak{Q}}$ à valeurs dans μ_2 vaut -1, où $\mathfrak{Q}$ désigne la place de F au-dessus de q. En fait, le point (vii) de la proposition 1.23 implique que

$$(2 + \alpha_n, -q)_{F_\mathfrak{Q}} = (\mathrm{N}_{F/K}(2 + \alpha_n), -q)_{K_\mathfrak{q}} = (2 + \sqrt{2}, -q)_{K_\mathfrak{q}} = -1,$$

où $\mathfrak{q}$ est la place de K au-dessus de q, et la dernière égalité est une conséquence de la Proposition 3.5 de [KM2].

Si maintenant $d = pq$ est le produit de deux nombres premiers distincts, alors $WK_2(E)(2) = 0$ si et seulement si
p et q sont congrus à ± 3 modulo 8,
la place 2-adique de F est décomposée dans E/F (afin d'avoir $|T_{E/F}| = 2$),
et $a = 1$, *i.e.* $2 + \alpha_n$ n'est pas une norme dans E/F.
Les deux premières conditions sont équivalentes à $p \equiv -q \equiv \pm 3 \bmod 8$ et par conséquent la dernière est satisfaite puisque nous avons

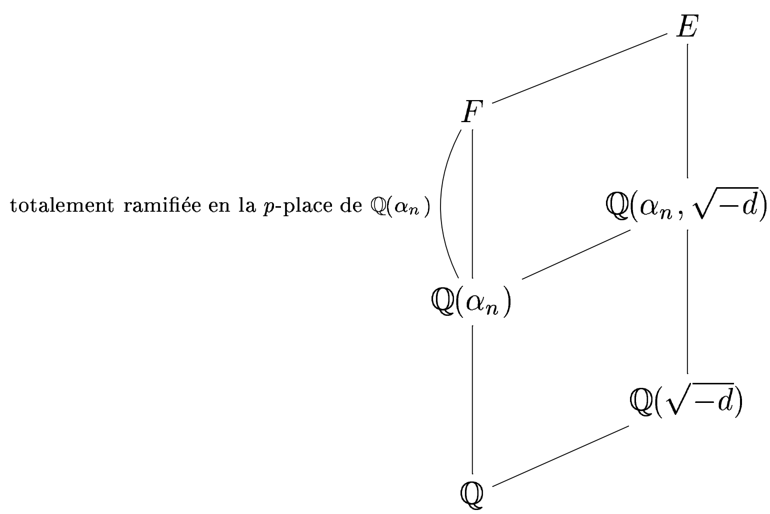
$$(2 + \alpha_n, -q)_{F_\mathfrak{Q}} = (\mathrm{N}_{F/\mathbb{Q}}(2 + \alpha_n), -q)_{\mathbb{Q}_q} = (2, -q)_{\mathbb{Q}_q} = -1.$$

Autrement dit, on a montré que pour tout $n \geqslant 2$:

$$WK_2(\mathbb{Q}(\alpha_n, \sqrt{-d}))(2) = 0 \Longleftrightarrow \begin{cases} d = q & \text{avec } q \equiv 7 \bmod 16 \\ \text{ou} & \\ d = pq & \text{avec } p \equiv -q \equiv \pm 3 \bmod 8 \end{cases}$$

où p et q sont premiers.

II.A.1.b. Sinon, p se ramifie dans $F/\mathbb{Q}$. Ainsi, quelle que soit la valeur de d, la place de F au-dessus de p n'appartient pas à $T_{E/F}$. De plus, la place 2-adique de F est dans $T_{E/F}$ si et seulement si $d \not\equiv -1 \bmod 8$. Soit maintenant $\mathbb{Q}(\alpha_n)$ l'intersection $F \cap \mathbb{Q}_\infty$.

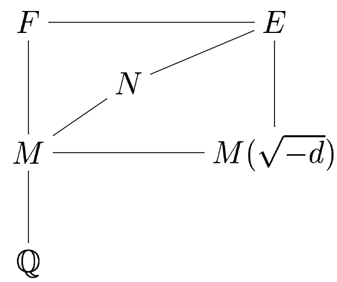


Si p ne divise pas d, l'extension $E/\mathbb{Q}(\alpha_n, \sqrt{-d})$ est totalement et modérément ramifiée en toute p-place de $\mathbb{Q}(\alpha_n, \sqrt{-d})$ et donc la trivialité de $WK_2(E)(2)$ implique celle de $WK_2(\mathbb{Q}(\alpha_n, \sqrt{-d}))(2)$. Donc le cas II.A.1.a nous donne :

$$\begin{array}{ll} d = qt & \text{avec } q \equiv -t \equiv \pm 3 \bmod 8 \\ \text{ou} & \\ d = q & \text{avec } q \equiv \pm 3 \bmod 8 \\ \text{ou} & \\ d = t & \text{avec } t \equiv 7 \bmod 16. \end{array}$$

En fait, dans ces trois cas, on remarque que $|T_{E/F}| = 2$ et il reste à étudier si $2+\alpha_n$ est une norme dans E/F. Mais, $2+\alpha_n$ et $-d$ appartenant à $\mathbb{Q}(\alpha_n)$, on voit que le symbole de Hilbert $(2+\alpha_n, -q)_F$ est trivial puisque 2 et les diviseurs premiers de d sont non décomposés dans $F/\mathbb{Q}(\alpha_n)$. En d'autres termes, $WK_2(E)(2)$ n'est pas triviale et il nous reste à étudier le cas où p divise d.

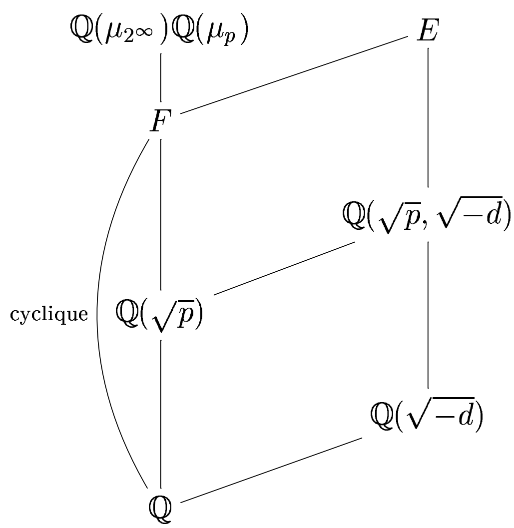
Supposons donc que p divise d et écrivons $d = pd'$. Soit M l'unique sous-corps de F d'indice 2 ; alors F et $M(\sqrt{-d})$ sont deux sous-corps quadratiques de E/M et notons N le troisième.



Alors E/N est modérément ramifiée (en tout diviseur premier impair de d') et donc $WK_2(E)(2) = 0$ implique que $WK_2(N)(2) = 0$. Mais, N étant cyclique, on a nécessairement (voir le chapitre 4) $d' = q$, où q est un nombre premier congru à ± 3 modulo 8. Ainsi, il y a une unique place de F au-dessus de q. Néanmoins, comme précédemment, le symbole de Hilbert $(2+\alpha_n, -pq)_F$ est trivial et $a = 0$. D'où, la place 2-adique de F ne peut pas appartenir à $T_{E/F}$, ce qui signifie que $p \equiv -q \equiv \pm 3 \bmod 8$.

II.A.2. Si $K = \mathbb{Q}(\sqrt{p})$

Notons d'abord que $p \equiv 5 \bmod 8$ (corollaire 4.2) et qu'on peut supposer que p ne divise pas d. La situation est la suivante :



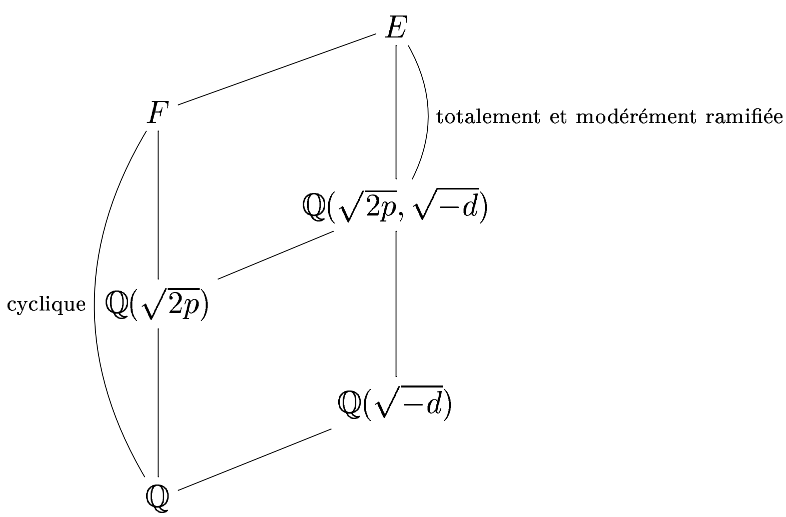
Puisque $E/\mathbb{Q}(\sqrt{p}, \sqrt{-d})$ est totalement et modérément ramifiée en toute place p-adique de $\mathbb{Q}(\sqrt{p}, \sqrt{-d})$, la trivialité de $WK_2(E)(2)$ implique celle de $WK_2(\mathbb{Q}(\sqrt{p}, \sqrt{-d}))(2)$. Ce corps étant bi-quadratique, la liste donnée au paragraphe précédent permet d'obtenir :

$$
\begin{array}{l}
d = q \quad \text{avec } p \equiv -q \equiv 5 \bmod 8, \\
\text{ou} \\
d = q \quad \text{avec } q \equiv 7 \bmod 8 \text{ et } \binom{p}{q} = -1.
\end{array}
$$

Si $d = q$ avec $p \equiv -q \equiv 5 \bmod 8$, on voit que $|T_{E/F}| = 1$ et donc $WK_2(E)(2) = 0$. Si $d = q$ avec $q \equiv 7 \bmod 8$ et $\binom{p}{q} = -1$, alors un calcul similaire de symboles de Hilbert montre que $a = 0$ et par conséquent q ne doit pas être décomposé dans K, ce qui est le cas puisque $\binom{p}{q} = -1$.

II.A.3. Si $K = \mathbb{Q}(\sqrt{2p})$

On a encore $p \equiv 5 \bmod 8$. Comme précédemment, on a



et la liste d'extensions bi-quadratiques fournit :

$$
\begin{array}{l}
d = q \quad \text{avec } q \equiv 7 \bmod 8 \text{ et } \binom{p}{q} = +1, \\
\text{ou} \\
d = 2q \quad \text{avec } p \equiv -q \equiv 5 \bmod 8.
\end{array}
$$

Le raisonnement est exactement le même que dans le cas où $K = \mathbb{Q}(\sqrt{p})$ et on obtient alors que $WK_2(E)(2) = 0$ si et seulement si

$$
\begin{array}{ll}
d = q & \text{avec } q \equiv 7 \bmod 8 \text{ et } \left(\dfrac{p}{q}\right) = +1, \\
\text{ou} & \\
d = 2q & \text{avec } p \equiv -q \equiv 5 \bmod 8 \text{ et } \left(\dfrac{p}{q}\right) = +1.
\end{array}
$$

II.B. Si F n'est pas cyclique sur $\mathbb{Q}$ et si F est de la forme $F = \mathbb{Q}(\alpha_n, \sqrt{p})$, où $n \geqslant 1$ et $p \equiv \pm 3 \bmod 8$, alors $E = \mathbb{Q}(\alpha_n, \sqrt{p}, \sqrt{-d})$ où d est un entier positif impair non divisible par p.

$$
\begin{tikzcd}
 & E = \mathbb{Q}(\alpha_n, \sqrt{p}, \sqrt{-d}) \arrow[dd, dash] \\
F = \mathbb{Q}(\alpha_n, \sqrt{p}) \arrow[ur, dash] \arrow[dd, dash] & \\
 & \mathbb{Q}(\alpha_n, \sqrt{-d}) \\
\mathbb{Q}(\alpha_n) \arrow[ur, dash] \arrow[d, dash] & \\
\mathbb{Q} &
\end{tikzcd}
$$

L'extension $E/\mathbb{Q}(\alpha_n, \sqrt{-d})$ est alors totalement et modérément ramifiée (en la place p-adique) et $WK_2(E)(2) = 0$ implique que $WK_2(\mathbb{Q}(\alpha_n, \sqrt{-d}))(2) = 0$, ce qui est vrai (cf le cas II.A.1.a.) si

$$
\begin{array}{ll}
d = q & \text{avec } q \equiv 7 \bmod 16, \\
\text{ou} & \\
d = qr & \text{avec } q \equiv -r \equiv \pm 3 \bmod 8, \\
\text{ou} & \\
d = q & \text{avec } q \equiv \pm 3 \bmod 8.
\end{array}
$$

De plus, dans tous les cas, q se décompose dans $\mathbb{Q}(\sqrt{2}, \sqrt{p})$, ce qui signifie qu'au moins deux places de F au-dessus de q sont dans $T_{E/F}$ et la place 2-adique de F doit être décomposée dans E (puisque $|T_{E/F}| \leqslant 2$). Nous en déduisons que le second cas dans la liste ci-dessus est impossible et le dernier devient : $d = q$ où $p \equiv -q \equiv \pm 3 \bmod 8$.

Si $d = q$ avec $q \equiv 7 \bmod 16$, on voit que si $WK_2(E)(2) = 0$, alors $|T_{E/F}| = 2$, mais ceci est en contradiction avec la valeur de a, calculée comme d'habitude à l'aide des symboles de Hilbert.

Si $d = q$ avec $p \equiv -q \equiv \pm 3 \bmod 8$, alors il y a exactement deux places de F au-dessus de q et la place 2-adique de F est décomposée dans E (puisque $-pq \equiv 1 \bmod 8$). Par conséquent, on obtient

$$\begin{aligned} WK_2(E)(2) = 0 \quad & \Longleftrightarrow \quad 2 + \alpha_n \notin \mathrm{N}_{E/F}(E^*) \\ & \Longleftrightarrow \quad (2 + \alpha_n, -q)_{F_\mathfrak{Q}} = -1 \\ & \Longleftrightarrow \quad (2, -q)_{\mathbb{Q}_p(\sqrt{p})} = -1 \\ & \Longleftrightarrow \quad q \text{ est décomposé dans } \mathbb{Q}(\sqrt{p}) \\ & \Longleftrightarrow \quad \left(\begin{array}{c} p \\ q \end{array} \right) = +1. \end{aligned}$$

II.C. Si l'on n'est pas dans les cas II.A. ou II.B., alors F s'obtient nécessairement comme la composée de $\mathbb{Q}(\alpha_n)$, où $n \geqslant 1$, et d'une extension $L/\mathbb{Q}$ cyclique de degré 4 contenant $\mathbb{Q}(\sqrt{p})$.

$$\begin{tikzcd}
 & & \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p) \arrow[d, dash] & \\
\mathbb{Q}(\alpha_n) \arrow[rr, dash] \arrow[d, dash] & & F \arrow[r, dash] \arrow[d, dash] & E = F(\sqrt{-d}) \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Q}(\sqrt{p}) \arrow[r, dash] & L &
\end{tikzcd}$$

Par conséquent, l'extension $E/\mathbb{Q}(\alpha_n, \sqrt{p}, \sqrt{-d})$ est totalement et modérément ramifiée en toute place p-adique de $\mathbb{Q}(\alpha_n, \sqrt{p}, \sqrt{-d})$. Ainsi, si $WK_2(E)(2) = 0$, alors $WK_2(\mathbb{Q}(\alpha_n, \sqrt{p}, \sqrt{-d}))(2) = 0$. D'après le cas II.B. on a nécessairement $d = q$ un nombre premier tel que $p \equiv -q \equiv \pm 3 \bmod 8$ et $\left(\begin{array}{c} p \\ q \end{array} \right) = +1$.
Par conséquent, q se décompose dans $\mathbb{Q}(\sqrt{p})$ mais pas dans L si l'on veut avoir $WK_2(E)(2) = 0$. Par une méthode analogue aux précédentes, cette condition implique que $a = 0$. D'où une contradiction avec l'équivalence (5.1). Autrement dit, dans ce cas, il n'y a pas d'extension dont la 2-partie du noyau sauvage est triviale.

Le cas (ii)

Ici, on suppose que F est l'unique sous-corps de degré 4 de $\mathbb{Q}(\mu_p)$ où p est un premier tel que $p \equiv 9 \bmod 16$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$. Ainsi, E est de degré 8 sur $\mathbb{Q}$. Si E est cyclique, le travail a déjà été fait au chapitre 4 : $WK_2(E)(2)$ est triviale si et seulement si E est l'unique sous-corps de degré 8 de $\mathbb{Q}(\mu_p)$ où p est un nombre premier tel que $p \equiv 9 \bmod 16$, $2^{\frac{p-1}{8}} \equiv 1 \bmod p$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$. Sinon, on peut écrire $E = F(\sqrt{-d})$ où d est un entier positif sans facteur carré et non divisible par p et nous sommes dans la situation suivante :

$$
\begin{tikzcd}
\mathbb{Q}(\mu_p) \arrow[dd, dash] & \\
 & E \arrow[dd, dash] \\
F \arrow[ur, dash] \arrow[dd, dash] & \\
 & \mathbb{Q}(\sqrt{p}, \sqrt{-d}) \arrow[dd, dash] \\
\mathbb{Q}(\sqrt{p}) \arrow[ur, dash] \arrow[dd, dash] & \\
 & \mathbb{Q}(\sqrt{-d}) \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}
$$

L'extension $E/\mathbb{Q}(\sqrt{p}, \sqrt{-d})$ est totalement et modérément ramifiée (en la place p-adique) et $WK_2(E)(2) = 0$ implique que c'est aussi le cas de ce corps bi-quadratique. Alors, on voit que $d = q$ où $q \equiv 7 \bmod 8$ et $\left(\begin{array}{c} p \\ q \end{array}\right) = -1$. Sous ces hypothèses, 2 est totalement décomposé dans $E/\mathbb{Q}$ et il y a une unique place de F au-dessus de q. Nous en déduisons que $|T_{E/F}| = 1$ et donc $WK_2(E)(2) = 0$.

Les cas restants (iii) et (iv)

On suppose maintenant que $F = \mathbb{Q}(\sqrt{2^c p}, \sqrt{2^c q})$ où p, q sont des premiers tels que $p \equiv q \equiv 3 \bmod 8, c \in \{0, 1\}$ ou $F = \mathbb{Q}(\sqrt{pq}, \sqrt{qr})$ où p, q, r sont des premiers tels que $p \equiv q \equiv r \equiv 3 \bmod 8$. Alors E est une extension tri-quadratique de $\mathbb{Q}$; en effet, puisque tous les nombres premiers impliqués sont congrus à 3 modulo 4, aucun sous-corps quadratique de F ne peut être plongé dans une extension cyclique de degré 4. Dans ce cas, on sait avec [Gri] que $WK_2(E)(2)$ est non triviale.

En regroupant les résultats des cas précédents, on obtient le théorème suivant :

Théorème 5.6. *Soit E une 2-extension abélienne de $\mathbb{Q}$ et F son sous-corps réel maximal. Supposons que $[F:\mathbb{Q}] \geqslant 4$ et que $WK_2(F)(2)$ est triviale. Alors $WK_2(E)(2)$ est triviale si et seulement si l'une des conditions suivantes est satisfaite :*
(1) $E \subset \mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\mu_p)$, avec $p \equiv \pm 3 \bmod 8$;
(2) $E = \mathbb{Q}(\alpha_n, \sqrt{-d})$ où $d = q \equiv 7 \bmod 16$ ou $d = pq$ avec $p \equiv -q \equiv \pm 3 \bmod 8$;
(3) F est cyclique, contient $\sqrt{2}$, se ramifie en un premier $p \equiv \pm 3 \bmod 8$ et $E = F(\sqrt{-pq})$ où $p \equiv -q \equiv \pm 3 \bmod 8$;
(4) F est cyclique, contient $\sqrt{p}$ avec $p \equiv 5 \bmod 8$ et $E = F(\sqrt{-d})$ où $d = pq$ avec $p \equiv -q \equiv 5 \bmod 8$ ou $d = q \equiv 7 \bmod 8$ et $\left(\frac{p}{q}\right) = -1$;
(5) F est cyclique, contient $\sqrt{2p}$ avec $p \equiv 5 \bmod 8$ et $E = F(\sqrt{-d})$ où $d = 2q$ avec $p \equiv -q \equiv 5 \bmod 8$ et $\left(\frac{p}{q}\right) = +1$ ou $d = q \equiv 7 \bmod 8$ et $\left(\frac{p}{q}\right) = +1$;
(6) $E = \mathbb{Q}(\alpha_n, \sqrt{p}, \sqrt{-q})$ où $p \equiv -q \equiv \pm 3 \bmod 8$ et $\left(\frac{p}{q}\right) = +1$;
(7) E est l'unique sous-corps de degré 8 de $\mathbb{Q}(\mu_p)$ où p est un premier tel que $p \equiv 9 \bmod 16$, $2^{\frac{p-1}{8}} \equiv 1 \bmod p$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$;
(8) $E = F(\sqrt{-q})$ où F est l'unique sous-corps de degré 4 de $\mathbb{Q}(\mu_p)$ où p est un premier que $p \equiv 9 \bmod 16$, $p \neq x^2 - 32y^2$, $x > 0$, $x \equiv 1 \bmod 4$, $q \equiv 7 \bmod 8$ et $\left(\frac{p}{q}\right) = -1$.

5.2.3 Conclusion

On termine cette thèse par une question ouverte qui met en lumière les limites des méthodes utilisées jusqu'ici pour traiter le cas général des 2-extensions abéliennes de $\mathbb{Q}$.

Pour cela, considérons E la composée de l'unique sous-corps de degré 8 de $\mathbb{Q}(\mu_p)$ avec le corps $\mathbb{Q}(\sqrt{-q})$ où p et q sont deux nombres premiers impairs distincts satisfaisant les conditions suivantes :

$$\begin{array}{ll} (i) & p \equiv 9 \bmod 16, \\ (ii) & q \equiv 7 \bmod 8, \\ (iii) & \left(\begin{array}{c} p \\ q \end{array} \right) = -1, \\ (iv) & p \neq x^2 - 32y^2, x > 0, x \equiv 1 \bmod 4, \\ (v) & 2^{\frac{p-1}{8}} \equiv 1 \bmod p. \end{array}$$

Question : $WK_2(E)(2)$ est-elle triviale ?

Bibliographie

[A] D. Arlettaz, *Algebraic K-Theory of rings from a topological viewpoint,* Publ. Mat. **44** (2000), n° 1, 3-84.

[BR] A. Bak and U. Rehmann, *K_2-analogs of Hasse's norm theorems,* Comment. Math. Helvetici **59** (1984), 1-11.

[BC] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity,* J. reine angew. Math. **238** (1969), 67-70.

[BT] H. Bass and J. Tate, *The Milnor ring of a global field,* Algebraic K-Theory II, Lecture Notes in Math. **342** (1973).

[Bi] B.J. Birch, *K_2 of global fields,* Proc. Sympos. Pure Math. **20** (1971), 87-95

[Br] J. Browkin, *The functor K_2 of the ring of integers of a number field,* Banach Center Publications **9** (1982), 187-195

[BG] J. Browkin and H. Gangl, *Tame and wild kernels of quadratic imaginary number fields,* Math. Comp. **68** (1999), n° 225, 291-305

[BS] J. Browkin and A. Schinzel, *On 2-Sylow subgroups of $K_2(o_F)$ for quadratic fields,* J. reine angew. Math. **331** (1982), 104-113.

[CF] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London and New-York (1967).

[CW] S.U. Chase and W.C. Waterhouse, *Moore's Theorem on Uniqueness of Reciprocity Laws,* Inv. Math. **16** (1972), 267-270.

[Co] H. Cohn, *A second course in number theory,* Wily, New-York (1962).

[FT] A. Fröhlich and M.J. Taylor, *Algebraic Number Theory,* Cambridge University Press (1991).

[Ga] H. Garland, *A finiteness theorem for K_2 of a number field,* Ann. of Math. **94** (1971), 534-548.

[Gr1] G. Gras, *Remarks on K_2 of Number Fields,* Journal of Number Theory **23** (1986), 322-335.

[Gr2] G. Gras, *Class Field Theory,* Springer (2003).

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

[Gri] R.A.W. Griffiths, *Multi-quadratic Extensions of $\mathbb{Q}$ with Trivial 2-Primary Hilbert Kernel,* Thesis for the Degree Master of Science, McMaster University (2000).

[Ha] G. Habdank, *Funktorielle Eigenschaften von Normrestsymbolen,* Diplomarbeit Bielefeld (1981).

[HK] J. Hurrelbrink and M. Kolster, *Tame kernels under relative quadratic extensions and Hilbert symbols,* J. reine angew. Math. **499** (1998), 145-188.

[Hut] K. Hutchinson, *The 2-Sylow subgroup of the wild kernel of exceptional number fields,* J. Number Theory **87** (2001), n° 2, 222-238.

[J1] J.-F. Jaulent, *Introduction au K_2 des corps de nombres,* Publ. Math. Fac. Sci. Besançon, Théor. Nombres 1981/82 1982/83 (1983).

[J2] J.-F. Jaulent, *Sur le noyau sauvage des corps de nombres,* Acta Arith. **67** (1994), n° 4, 335-348.

[JS1] J.-F. Jaulent et F. Soriano-Gafiuk, *Sur le noyau sauvage des corps de nombres et le groupe des classes logarithmiques,* Math. Z. **238** (2001), n° 2, 335-354.

[JS2] J.-F. Jaulent et F. Soriano-Gafiuk, 2-*Groupe des classes positives et noyau sauvage de la K_2-théorie,* soumis.

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

[Ke] F. Keune, *Quadratic number fields having $\{-1,-1\}$ as a non-trivial element of their wild kernel,* J. Number Theory **63** (1997), n° 1, 30-33.

[Koc] H. Koch, *Algebraic Number Theory,* Springer (1997).

[Kol] M. Kolster, *An idelic approach to the wild kernel,* Invent. Math. **103** (1991), n° 1, 9-24.

[KM1] M. Kolster and A. Movahhedi, *Galois co-descent for étale wild kernels and capitulation,* Ann. Inst. Fourier, Grenoble **50**, 1 (2000), 35-65.

[KM2] M. Kolster and A. Movahhedi, *Bi-quadratic number fields with trivial 2-primary Hilbert kernel,* Proc. London Math. Soc. **87** (2003), 109-136.

[La] S. Lang, *Cyclotomic Fields II,* Springer-Verlag (1980).

[Le] M. Lescop, *Abelian 2-extensions of $\mathbb{Q}$ with trivial 2-primary Hilbert kernel,* à paraître dans Acta Arithmetica.

[Mi] J. Milnor, *Introduction To Algebraic K-Theory,* Annals of Math. Studie, vol. 72, Princeton Univ. Press, Princeton (1971).

[MN] A. Movahhedi et T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels,* Séminaire de Théorie des nombres, Paris 1988-89, Birkhäuser 1990, 155-200.

[Mu] T. Mulders, *Generating the tame and wild kernels by Dennis-Stein symbols,* K-Theory **5** (1991/92), n° 5, 449-470.

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

[Ng] T. Nguyen Quang Do, *Analogues supérieurs du noyau sauvage,* Sém. Théor. Nombres Bordeaux **4** (1992), n° 2, 263-271.

[Q] D. Quillen, *Higher K-theory for categories with exact sequences,* Proc. of the Symp. "New developments in topology" (1972), 95-103.

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

[Ry] D. Ryan, *Galois Co-Descent for Wild Kernels,* Thesis, University College Dublin (2002).

[S1] J.-P. Serre, *Corps locaux,* Hermann, Paris (1968).

[S2] J.-P. Serre, *Cours d'arithmétique,* P.U.F. (1970).

[S3] J.-P. Serre, *Topics in Galois Theory,* Bartlett and Jones Publishers (1992).

[Sor] F. Soriano-Gafiuk, *Sur le noyau hilbertien d'un corps de nombres,* C.R.A.S. Paris Sér. 1 Math. **330** (2000), n° 10, 863-866.

[St] M. Stinner, *Pell's Equation and Integers of the form x^2+32y^2,* Thesis for the Degree Master of Science, McMaster University (2001).

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

[W] L.C. Washington, *Introduction to Cyclotomic Fields,* Second Edition, Springer (1997).

Sur les 2-extensions de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale

Résumé : Nous nous intéressons dans cette thèse à l'étude de la trivialité de la 2-partie du noyau sauvage de certaines 2-extensions abéliennes du corps $\mathbb{Q}$ des rationnels. Le cas général des extensions multi-quadratiques ayant déjà été résolu, nous traitons ici le cas des 2-extensions cycliques, puis celui des 2-extensions abéliennes totalement réelles. Les résultats que nous obtenons reposent principalement sur une amélioration que nous proposons de la formule de genre démontrée par M. Kolster et A. Movahhedi. En particulier, on retrouve la valeur du 2-rang du noyau sauvage des corps quadratiques. Nous terminons la thèse par quelques exemples illustrant les difficultés rencontrées pour élucider le cas général des 2-extensions abéliennes de $\mathbb{Q}$.

Mots-clés : théorie algébrique des nombres, K_2 des corps de nombres, noyau sauvage (ou hilbertien), noyau modéré (positif), formule de genre, 2-rang.

About the 2-extensions of $\mathbb{Q}$ with trivial 2-primary wild kernel

Abstract : In this thesis, we are interested in the study of the triviality of the 2-primary wild kernel of some abelian 2-extensions of the rationals $\mathbb{Q}$. Since the general case of multi-quadratic extensions has been already solved, we deal with the case of cyclic 2-extensions, and then with that of totally real abelian 2-extensions. The results we obtain are based on an improvement we propose of the genus formula proved by M. Kolster and A. Movahhedi. As a consequence, we also retrieve the 2-rank of the wild kernel of quadratic fields. We end the thesis by some examples illustrating the hurdles we have to overcome to determine the general case of abelian 2-extensions of $\mathbb{Q}$.

Keywords : algebraic number theory, K_2 of number fields, wild (or Hilbert) kernel, (positive) tame kernel, genus formula, 2-rank.

Laboratoire d'accueil : **L**aboratoire d'**A**rithmétique, de **C**alcul formel et d'**O**ptimisation (LACO), 123, avenue Albert Thomas, 87060 Limoges Cedex