N° d'ordre : 2313

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX 1

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Stéphane VINATIER**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

Arithmétique des extensions faiblement ramifiées

Soutenue le : 18 Décembre 2000

Après avis de :

MM.	J. COUGNARD, Professeur, Université de Caen	**Rapporteurs**
	M.J. TAYLOR, Professor, University of Manchester	

Devant la commission d'examen formée de :

M.	J. COUGNARD, Professeur, Université de Caen	**Président**
Mme	C. BACHOC, Chargée de Recherche, C.N.R.S.	**Rapporteur**
MM.	Ph. CASSOU-NOGUÈS, Professeur, Université Bordeaux 1	**Examinateurs**
	B. EREZ, Professeur, Université Bordeaux 1	
	M.J. TAYLOR, Professor, University of Manchester	

– 2000 –

Je voudrais exprimer ici ma gratitude envers les personnes qui ont rendu possible l'élaboration de ce travail.

Mes remerciements vont en premier lieu à mes deux directeurs de thèse : Philippe Cassou-Noguès, dont les encouragements et les explications m'ont constamment poussé de l'avant, et Boas Erez, pour m'avoir confié le sujet qui m'a occupé pendant plus de trois années, riche en enseignements et en perspectives.

Je voudrais aussi particulièrement remercier Christine Bachoc qui, en plus de participer à mon jury de thèse, a donné l'impulsion d'une partie de ce travail et m'a patiemment initié au maniement des réseaux à l'aide du logiciel Magma.

Martin J. Taylor et Jean Cougnard ont accepté d'être les rapporteurs de cette thèse et de faire partie de mon jury. Je les remercie vivement pour le temps qu'ils ont consacré et l'intérêt qu'ils ont apporté à mon travail.

Mes progrès ont beaucoup bénéficié de l'environnement offert par l'Institut de Mathématiques de Bordeaux. Parmi les personnes qui y travaillent et qui m'ont fait profiter de leurs compétences, j'ai plaisir à citer ici Bill Allombert, Arnaud Jehanne, Christian Maire, Fransisco Diaz y Diaz et Jacques Martinet. Je joins Yves Eichenlaub à cette liste, bien qu'il ait quitté Bordeaux après avoir effectué sa thèse à l'A2X puisque, par le seul biais du courrier électronique, il a répondu avec une grande précision à mes questions relatives à son domaine de prédilection.

Je ne peux clore cette page sans mentionner notre secrétaire d'école doctorale, Joëlle Pargade, dont les compétences et la gentillesse ouvrent à tous un chemin sûr au travers des diverses embûches administratives. Je remercie enfin Mauricette Jaubert pour avoir assuré l'impression "à la corrézienne" de cette thèse.

Arithmétique des extensions faiblement ramifiées

Stéphane Vinatier

Table des matières

Introduction

La question de l'existence d'une base normale pour l'anneau des entiers d'une extension galoisienne finie de $\mathbb{Q}$ a suscité de nombreuses recherches en théorie algébrique des nombres. En terme de structure galoisienne, l'existence d'une telle base équivaut à la liberté de l'anneau d'entiers comme module sur la $\mathbb{Z}$-algèbre du groupe de Galois G de l'extension. Le théorème de Nœther affirme que ce module est localement libre si et seulement si l'extension est modérément ramifiée, ce qui donne une condition nécessaire à l'existence de la base normale. Sous cette condition, on associe à l'anneau d'entiers une classe dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres. On sait par le théorème de Taylor ([Tay1]) que cette classe est d'ordre 1 ou 2 et on peut la déterminer en fonction des caractères irréductibles symplectiques de G. Lorsqu'elle n'est pas triviale, l'anneau d'entiers ne peut pas posséder de base normale.

La démarche nécessaire pour établir ce résultat comporte plusieurs étapes. On utilise d'abord la Hom-description de Fröhlich ([Frö]) du groupe des classes pour représenter la classe de l'anneau d'entiers par certaines fonctions de caractères. Celles-ci sont fabriquées à l'aide de résolvantes et de sommes de Gauss locales. Ces dernières proviennent des constantes locales de l'équation fonctionnelle des fonctions L de corps de nombres et sont donc de nature analytique, tandis que les résolvantes sont des objets algébriques. Le point crucial est alors de pouvoir établir des relations entre ces objets de nature différente. C'est ce qu'a fait Taylor dans le cas des extensions modérées. On verra qu'un des principaux résultats de cette thèse est obtenu en trouvant une relation nouvelle entre ces objets en des places faiblement et sauvagement ramifiées.

En effet, toutes les extensions de corps de nombres ne sont pas modérées et on peut se demander ce qui se passe dans le cas de la ramification sauvage. En ce qui concerne l'anneau d'entiers, on sait qu'alors il n'est plus localement libre en tant que $\mathbb{Z}[G]$-module. Une voie possible pour contourner ce problème est d'étudier sa structure sur un ordre contenant $\mathbb{Z}[G]$ sur lequel il soit localement libre. Le choix de l'ordre en question n'est pas canonique et sa définition peut obliger à faire des restrictions sur l'extension. Plusieurs travaux sur ce thème ont été publiés dans le cas local (par exemple [B]) et dans le cas global (par exemple [HW1], [Tay2] et [CNT2]).

Une alternative à ce procédé est d'étudier la structure d'autres modules galoisiens liés à l'extension. Cette voie a été préparée par des travaux d'Ullom qui donnent des conditions nécessaires et suffisantes pour qu'un idéal ambige

(i.e. stable sous l'action de G) soit localement libre sur l'anneau de groupe. Erez ([Er1]) en a déduit que l'idéal racine carrée de la codifférente, lorsqu'il existe, est localement libre si et seulement si l'extension est faiblement ramifiée, c'est-à-dire si, pour tout idéal premier divisant la différente de l'extension, le second groupe de ramification est trivial. Cette condition autorise la ramification sauvage (qui correspond au premier groupe de ramification) tout en la limitant au maximum (seul le premier groupe de ramification peut être non trivial).

Le résultat d'Erez donne un analogue du théorème de Nœther dans le cas de la ramification faible. Si l'on se restreint au cas des extensions de degré impair pour assurer l'existence de l'idéal racine carrée de la codifférente $\mathcal{A}$, on peut alors s'attendre, vu le théorème de Taylor pour l'anneau d'entiers et du fait qu'il n'y a pas de caractère irréductible symplectique en degré impair, à ce que $\mathcal{A}$ soit libre sur $\mathbb{Z}[G]$ dès que l'extension est faiblement ramifiée. Mais le fait d'être confronté à la ramification sauvage oblige à trouver de nouvelles relations entre résolvantes et sommes de Gauss locales. Si Erez a pu montrer que $\mathcal{A}$ est libre sur $\mathbb{Z}[G]$ quand l'extension est modérée ([Er3]), il n'a pu faire de même dans le cas général d'une extension faiblement ramifiée de corps de nombres de degré impair. Cependant, et ce résultat sera fort utile dans la suite, il a établi que les valeurs de la somme de Gauss (tordue par une opération d'Adams) et de la résolvante (associée à une base normale de la racine carrée de la codifférente locale) appliquées en un caractère de G sont des unités.

Enfin, on peut munir $\mathcal{A}$ d'une structure plus riche que celle de module galoisien. Conner et Perlis avaient noté dans [CP] que la racine carrée de la codifférente d'une extension finie galoisienne de $\mathbb{Q}$, lorsqu'elle existe, est le seul idéal fractionnaire auto-dual pour la forme trace de l'extension, ce qui en fait un réseau entier unimodulaire. Cette propriété, qui reste vraie pour une extension relative, est ce qui a d'abord motivé l'étude de cet idéal par Erez. Il montre dans sa thèse ([Er1]) qu'une extension abélienne de $\mathbb{Q}$ est faiblement ramifiée si et seulement si le réseau associé à la racine carrée de la codifférente $\mathcal{A}$ est isométrique au réseau standard de même dimension, via une isométrie qui commute à l'action du groupe de Galois. Ceci entraîne en particulier que le $\mathbb{Z}[G]$-module $\mathcal{A}$ est libre sous les mêmes hypothèses.

D'autres travaux ont suivi cette voie en traitant en parallèle le réseau associé à l'anneau d'entiers, notamment [ErM] (cas modéré abélien) et [ErT], où il est établi que le réseau associé à $\mathcal{A}$ est stablement isométrique au réseau standard dès que l'extension est modérément ramifiée. Enfin, [BuCh] retrouve et étend les résultats de ces deux articles grâce à un travail sur les opérations d'Adams de certains groupes de Grothendieck.

L'objet initial de cette thèse est d'améliorer les résultats existants concernant la structure galoisienne de la racine carrée de la codifférente d'extensions faiblement ramifiées de corps de nombres de degré impair. Comme nous l'avons dit plus haut, la condition essentielle pour parvenir à cet objectif est de pouvoir établir de nouvelles relations entre sommes de Gauss et résolvantes locales aux places sauvagement ramifiées. Nous allons voir que cela mène aussi à d'autres thèmes de recherche : description des extensions abéliennes faiblement ramifiées de $\mathbb{Q}_p$, critères de ramification faible pour les extensions locales ou globales,

construction de familles infinies d'exemples d'extensions faiblement ramifiées, calcul sur certains exemples de la structure du réseau associé à la racine carrée de la codifférente. Nous présentons maintenant les résultats obtenus dans ces différentes directions dans l'ordre où ils apparaîtront dans la thèse.

Le premier pas dans notre démarche est l'étude des propriétés des extensions faiblement ramifiées. Si les extensions modérées ont fait l'objet de nombreux travaux, il n'en va pas de même pour les extensions sauvagement et faiblement ramifiées. [Er2], qui présente l'état des connaissances sur le sujet au début des années 90, n'a été suivi que de peu de publications consacrées à ce thème (voir cependant [ElM] ainsi que la partie 4 de [B] pour des études locales).

Le chapitre 1 de cette thèse rappelle les notions basiques de théorie des nombres qui permettent de définir la ramification faible dans les cas local et global et énonce quelques propriétés des extensions faiblement ramifiées, dont certaines sont des résultats nouveaux. Le principal d'entre eux est la description de toutes les extensions abéliennes faiblement ramifiées de $\mathbb{Q}_p$ pour p premier impair. Etant donné une racine primitive p^2-ième de l'unité ζ, on sait que la sous-extension L de degré p de $\mathbb{Q}_p(\zeta)$ est faiblement ramifiée. On fixe une clôture algébrique $\mathbb{Q}_p^c$ de $\mathbb{Q}_p$ et on note, pour tout entier m, $\mathbb{Q}_p\{m\}$ l'unique extension non ramifiée de degré m de $\mathbb{Q}_p$ contenue dans $\mathbb{Q}_p^c$. On obtient :

Théorème 1 *Soit $n \geq 1$ un entier divisible par p. Alors les extensions abéliennes sauvagement et faiblement ramifiées de $\mathbb{Q}_p$ de degré n sont les sous-extensions de degré n de $L.\mathbb{Q}_p\{n\}$ distinctes de $\mathbb{Q}_p\{n\}$.*

Ce résultat sera très utile au moment d'étudier la structure galoisienne de la racine carrée de la codifférente dans une extension faiblement ramifiée de $\mathbb{Q}$ et abélienne aux places sauvages.

Le chapitre 1 contient aussi une étude des p-extensions de $\mathbb{Q}$ qui sont faiblement ramifiées et dont le groupe de Galois est isomorphe à $C_{p^2} \rtimes C_p$. Ce groupe étant transitif de degré p^2, elles sont corps de décomposition d'un polynôme $P(x)$ de degré p^2. On montre alors certains critères de ramification faible portant sur la valuation p-adique du discriminant du corps de rupture $R = \mathbb{Q}[x]/(P(x))$ de ce polynôme. Ces résultats sont utilisés dans le deuxième chapitre consacré aux exemples d'extensions faiblement ramifiées.

Au regard de l'histoire de la structure galoisienne de l'anneau d'entiers, dans laquelle la construction par Martinet d'un exemple pour lequel il n'est pas libre a été une étape stimulante ([M2]), il ne semble pas inutile de construire des extensions faiblement ramifiées pour y calculer la structure galoisienne de la racine carrée de la codifférente. Les exemples les plus simples d'extensions faiblement et sauvagement ramifiées sont les extensions cycliques de $\mathbb{Q}$ de degré premier. Ce sont presque les seuls qui étaient jusqu'alors présentés dans la littérature ([Er2]). Par rapport au problème de la structure galoisienne de la racine carrée de la codifférente, ces extensions ne sont pas intéressantes puisqu'on sait par [Er1] que le réseau associé à celle-ci y est isométrique au réseau standard. Les extensions intéressantes pour illustrer de nouveaux résultats (théorème 3 présenté

plus loin) ou tester des conjectures (théorème 5) sont les extensions de degré impair, non abéliennes et faiblement ramifiées.

Pour en obtenir, il a paru plus simple de concentrer la ramification sauvage en une seule place en considérant des p-extensions, où p est un nombre premier impair. Le plus petit degré pour lequel on peut trouver des extensions non abéliennes est alors p^3 et dans ce cas, il y a deux possibilités pour le groupe de Galois de l'extension : il est isomorphe à $(C_p \times C_p) \rtimes C_p$ ou à $C_{p^2} \rtimes C_p$. Le critère du chapitre 1 présenté ci-dessus a poussé à considérer le deuxième cas au détriment du premier (pour lequel un travail similaire pourrait certainement être mené). Enfin, les capacités de calcul ont incité à choisir $p = 3$.

Pour construire des extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois isomorphe à $C_9 \rtimes C_3$, on utilise les travaux d'Eichenlaub dont la thèse ([Ei1]) donne une méthode pour construire un polynôme paramétré $P_t(x)$ tel que, pour une infinité de spécialisations en des valeurs entières du paramètre t (que l'on convient d'appeler de *bonnes valeurs*), l'extension qui est corps de décomposition sur $\mathbb{Q}$ du polynôme obtenu soit galoisienne de groupe de Galois isomorphe à $C_9 \rtimes C_3$. Il s'agit du polynôme suivant (où $w = t^2 - t + 1$) :

$$\begin{aligned} P_t(x) = \quad & x^9 - 9wx^7 + 27w^2x^5 - 30w^3x^3 + 9w^4x \\ & -(2t-1)(t^6 - 3t^5 - 12t^4 + 29t^3 - 3t^2 - 12t + 1)w \end{aligned}$$

Le critère du chapitre 1 permet alors de savoir, en utilisant un logiciel de calcul adapté, si l'extension est faiblement ramifiée ou non pour chaque bonne valeur de t. En fait, la méthode de construction de $P_t(x)$ utilise une extension kummérienne (dépendant de t) de $\mathbb{Q}(\zeta_9)$, où ζ_9 est une racine primitive 9-ième de l'unité, et l'étude de la ramification en 3 dans cette extension grâce à des critères dus à Hecke ([He]) et Greither ([Gr]) permet de montrer le résultat suivant.

Théorème 2 *On considère la famille $\mathcal{F}$ des extensions D qui sont corps de décomposition sur $\mathbb{Q}$ du polynôme $P_t(x)$ spécialisé en une bonne valeur t avec t congru à 5 modulo 9. Alors :*

(i) $\mathcal{F}$ est constituée d'une infinité d'extensions de $\mathbb{Q}$.

(ii) Chacune des extensions $D \in \mathcal{F}$ est faiblement ramifiée sur $\mathbb{Q}$.

(iii) Soit $D \in \mathcal{F}$ correspondant à $t = 5+9u$. On note e l'indice de ramification, f le degré résiduel et g le degré de décomposition en 3 dans $D/\mathbb{Q}$. Si $u \equiv 0$ ou 2 mod 3, alors $e = 9$ et $f = 3$. Si $u \equiv 1$ mod 3, alors $e = f = g = 3$ ou $e = 3$ et $g = 9$.

La même méthode est employée pour construire une famille infinie d'extensions modérées de $\mathbb{Q}$ de groupe de Galois isomorphe à $C_7 \rtimes C_3$ (théorème 2.4.2). Ces deux familles d'extensions faiblement ramifiées fournissent la plus grande part des exemples pour lesquels le chapitre 5 présente des résultats de calcul de structure galoisienne et de réseau pour la racine carrée de la codifférente.

Le chapitre 2 contient aussi une grande variété d'exemples d'extensions faiblement ramifiées, à la fois pour rendre possibles d'éventuels calculs dans

d'autres situations et pour montrer que les extensions faiblement ramifiées ne sont pas une rareté au sein des extensions galoisiennes. En fait, parmi la soixantaine de polynômes de la table de Magma ([BoCa]) dont le groupe de Galois est transitif de degré compris entre 2 et 11 et qui ont été testés, plus du quart fournissent une extension faiblement et sauvagement ramifiée. On illustre aussi le théorème 1 en construisant les trois extensions abéliennes faiblement ramifiées de $\mathbb{Q}_3$ de degré 45.

Les chapitres 3 et 4 reviennent aux problèmes de structure galoisienne pour la racine carrée de la codifférente $\mathcal{A}$ d'une extension faiblement ramifiée de corps de nombres de degré impair. Le premier d'entre eux est consacré à des préliminaires : on définit les objets à étudier, on présente la Hom-description de Fröhlich ([Frö]) du groupe des classes de $\mathbb{Z}[G]$-modules localement libres et on donne un représentant correspondant à la classe de $\mathcal{A}$. La partie 3.3 est consacrée aux sommes de Gauss locales qui interviennent dans ce représentant. On revient sur leur définition et, à l'aide d'un article de Tate consacré aux constantes locales de l'équation fonctionnelle de la fonction L d'une extension de corps de nombres ([Tat2]), on donne quelques propriétés des sommes de Gauss locales de caractères abéliens. Ceci nous permet de montrer une formule de restriction de la somme de Gauss locale d'une extension à groupe d'inertie abélien (théorème 3.4.4).

Le chapitre 4 consacré aux résultats de structure galoisienne peut alors commencer. On découpe le représentant de la classe de $\mathcal{A}$ en un produit de fonctions de caractères de G. Certains facteurs sont aisément contrôlables à l'aide de résultats antérieurs ([Tay1] et [Er3]). Le travail véritablement nouveau vient avec ceux qui font intervenir une résolvante et une somme de Gauss en une place sauvagement ramifiée, puisqu'on ne connaît pas alors de relation entre ces deux objets. Les auteurs confrontés à ce problème le résolvent en se plaçant dans des circonstances favorables, soit en étudiant des classes de modules galoisiens à l'intérieur de groupes "plus gros" que le groupe des classes (par exemple [CNQ] et [HW1]), soit en faisant des hypothèses restrictives sur les extensions considérées. Parmi les travaux appartenant à cette deuxième catégorie, [Tay2] étudie la structure galoisienne de l'anneau d'entiers d'une extension finie abélienne de corps de nombres tandis que [CNT2] se concentre sur les extensions finies galoisiennes de $\mathbb{Q}$ dont les premiers groupes de ramification sont abéliens, facteurs directs du groupe de décomposition et distingués dans le groupe de Galois. Le résultat qui suit se restreint aussi au cas d'une extension absolue ; il généralise alors le résultat d'Erez pour les extensions modérées (théorème 2 de [Er3]). Néanmoins, il ne concerne pas toutes les extensions faiblement ramifiées de $\mathbb{Q}$ puisqu'il fait aussi intervenir une hypothèse sur les groupes de décomposition aux places sauvages (un peu moins forte que celle évoquée ci-dessus).

Théorème 3 *Soit $N/\mathbb{Q}$ une extension faiblement ramifiée de degré impair, de groupe de Galois G. On suppose que les groupes de décomposition aux places sauvages sont abéliens. Alors la racine carrée de la codifférente $\mathcal{A}_N$ de l'extension est un $\mathbb{Z}[G]$-module libre.*

Notons qu'un des exemples d'extensions faiblement ramifiées issus des tables du logiciel Magma vérifie les hypothèses du théorème 3, mais pas celles des résultats connus auparavant : elle n'est ni abélienne ni modérée. Il en va de même pour les extensions de la famille $\mathcal{F}$ du théorème 2 correspondant à de bonnes valeurs du paramètre $t = 5 + 9u$ avec u congru à 1 modulo 3.

Ce résultat est obtenu grâce à la connaissance des extensions abéliennes faiblement ramifiées de $\mathbb{Q}_p$ (théorème 1), qui permet le calcul explicite de la somme de Gauss et de la résolvante locales aux places sauvagement ramifiées. Il ne reste alors qu'à constater que leur produit a les propriétés voulues. Il semble que de nouvelles idées soient nécessaires pour l'élargir à toutes les extensions faiblement ramifiées de corps de nombres de degré impair. Dans cette optique, un article récent de Byott [B] montre une voie pour passer au cas relatif en décrivant les extensions abéliennes d'une extension finie F de $\mathbb{Q}_p$ grâce aux corps de division associés à des groupes formels de Lubin-Tate. Cela lui permet notamment de prouver que l'anneau d'entiers d'une extension abélienne faiblement ramifiée de F est libre sur son ordre associé et de décrire celui-ci. Cette voie semble bien adaptée aux techniques développées pour montrer le théorème 3.

Une autre direction pour étendre ce résultat est de s'intéresser aux extensions non abéliennes aux places sauvages. Là encore, il semble souhaitable dans un premier temps d'imposer quelques restrictions sur les extensions considérées. On fixe un premier p supérieur ou égal à 3 et on montre dans la partie 4.3 :

Théorème 4 *Soit $N/\mathbb{Q}$ une p-extension finie et faiblement ramifiée de groupe de Galois G. On note $(\mathcal{A}_N)$ la classe de la racine carrée de la codifférente de l'extension dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres et $e(p)$ le degré de ramification en p dans $N/\mathbb{Q}$. Alors $(\mathcal{A}_N)^{e(p)} = 1$.*

L'un des éléments de la preuve de ce théorème est une formule de restriction de la résolvante locale au groupe d'inertie de l'extension complétée en p. On sait que celui-ci est abélien (par un résultat du chapitre 1) et donc, là encore, une meilleure connaissance des extensions locales relatives faiblement ramifiées et abéliennes pourrait permettre d'améliorer la majoration de l'ordre de $(\mathcal{A}_N)$, éventuellement de l'abaisser jusqu'à p. Même alors, le résultat ne serait sans doute pas optimal. En effet, un nouvel algorithme ([A]) de calcul explicite des automorphismes d'une extension galoisienne de $\mathbb{Q}$ a permis de déterminer la structure galoisienne de $\mathcal{A}$ pour de nombreux exemples de 3-extensions faiblement ramifiées de groupe de Galois isomorphe à $C_9 \rtimes C_3$. On trouve à chaque fois que c'est un module galoisien libre. De nouvelles méthodes sont à développer pour prouver que c'est toujours le cas.

Les calculs de structure galoisienne qui viennent d'être évoqués ont suivis des calculs menés avec l'aide de C. Bachoc pour déterminer la structure du réseau entier unimodulaire obtenu en munissant $\mathcal{A}$ de la forme trace Tr. Les résultats théoriques dont on dispose sur ce problème sont eux aussi lacunaires. D'une part, on ne sait rien dire si l'extension faiblement ramifiée considérée n'est ni modérée, ni absolue abélienne ; d'autre part, dans le cas modéré, on sait que le réseau est stablement isométrique au réseau standard ($\mathbb{Z}[G]$ muni de la forme

q_G qui rend orthonormale la base constituée des éléments de G) mais on ne sait pas si la simplification a lieu, c'est-à-dire s'il lui est isométrique.

Les exemples d'extensions faiblement ramifiées construits dans le chapitre 2 fournissent l'occasion de tester si ces résultats peuvent être améliorés. Des calculs menés sur plusieurs familles d'exemples sont présentés dans le chapitre 5. La principale conséquence qu'on en tire est :

Théorème 5 *Soit N/K une extension faiblement ramifiée de corps de nombres de degré impair, de groupe de Galois G. Le réseau $(\mathcal{A}_{N/K}, \mathrm{Tr})$ n'est pas toujours isométrique à $(\mathbb{Z}[G], q_G)$. En particulier, il existe des extensions vérifiant les hypothèses du théorème 3 ainsi que des extensions modérées pour lesquelles ce n'est pas le cas.*

Il découle de ce résultat que l'isomorphisme de $\mathbb{Z}[G]$-modules du théorème 3 ne provient pas nécessairement d'une isométrie, alors que cela est le cas lorsque l'extension est abélienne absolue. Par ailleurs, on voit que la simplification n'a pas forcément lieu dans le cas modéré. On peut rapprocher ce résultat d'un travail effectué par Cougnard pour construire des extensions galoisiennes de $\mathbb{Q}$ dont les anneaux d'entiers soient stablement libres et non libres en tant que modules galoisiens ([Cou]).

En fait, les différents réseaux obtenus en testant notamment des exemples provenant de la famille infinie du théorème 2 semblent survenir avec une certaine régularité qu'on aimerait pouvoir expliquer (voir la proposition 5.1.1). Cependant, des calculs effectués sur une autre famille à même groupe de Galois montrent que le fait que le groupe de décomposition de l'extension en 3 soit ou non abélien n'est pas équivalent au fait que le réseau soit de minimum 1 ou 3. On montre toutefois qu'un seul des trois réseaux entiers unimodulaires de dimension 27 et de minimum 3 (à consulter dans [BV]) peut être réalisé à l'aide de la racine carrée de la codifférente d'une extension faiblement ramifiée de $\mathbb{Q}$ de degré 27 (théorème 5.1.2).

Les calculs laissent donc beaucoup de questions ouvertes. Il pourrait être intéressant de les reprendre dans le cas faiblement et sauvagement ramifié pour tester si le réseau est alors stablement isométrique à $\mathbb{Z}[G]$. En dehors de ce problème, il semble qu'il faille maintenant chercher de nouvelles réponses théoriques. Ainsi, les techniques utilisées pour déterminer la structure galoisienne de $\mathcal{A}$ dans le cas absolu abélien aux places sauvages pourraient être adaptées pour tenter de montrer que le réseau associé est stablement isométrique à $\mathbb{Z}[G]$ sous les mêmes hypothèses.

En définitive, les résultats contenus dans cette thèse semblent être pour la plupart susceptibles d'améliorations. Une meilleure connaissance des extensions locales, abéliennes et faiblement ramifiées dans le cas relatif permettrait d'abaisser la majoration de l'ordre de $(\mathcal{A})$ dans le théorème 4 et de s'affranchir de l'hypothèse sur le corps de base dans ce résultat ainsi que dans le théorème 3. Avec un progrès supplémentaire sur les p-extensions, il n'est pas exclu que les techniques développées dans [CNT2] (certaines opérations d'Adams) permettent

alors d'arriver à un résultat optimal pour la structure galoisienne de la racine carrée de la codifférente d'une extension faiblement ramifiée de degré impair.

La deuxième voie pour des recherches ultérieures est celle évoquée ci-dessus et qui concerne le réseau associé à la racine carrée de la codifférente d'une extension faiblement ramifiée de degré impair. Elle se divise en deux branches : trouver un algorithme pour déterminer sur des exemples s'il est stablement isométrique au réseau standard et tenter d'élargir l'étude théorique menée dans [ErT] aux places sauvagement et faiblement ramifiées.

Enfin, pour conclure cette introduction, notons que d'autres directions de recherche, bien que moins directement reliées à ces travaux, pourraient être explorées à l'aide des connaissances acquises. D'une part, dans le domaine de la théorie algébrique des nombres, il est tentant d'essayer de faire le lien entre la classe définie par la racine carrée de la codifférente dans le groupe des classes et certains invariants de Chinburg, comme cela a été fait pour la classe définie par l'anneau d'entiers dans le cas modéré (voir [Ch] et [HW2]). Par ailleurs, on sait qu'un analogue de l'étude de la structure galoisienne des anneaux d'entiers et des conjectures de Fröhlich a été considéré en "dimension supérieure" dans un cadre géométrique (voir [Er5]). On peut se poser la question de l'étude dans ce cadre de la racine carrée de la codifférente.

Chapitre 1

Extensions faiblement ramifiées

Une extension finie galoisienne de corps de nombres est dite *faiblement ramifiée* si tous les seconds groupes de ramification de l'extension sont triviaux.

Lorsque tous les premiers groupes de ramification sont triviaux, on dit que l'extension est modérément ramifiée. L'arithmétique de telles extensions et notamment la structure galoisienne de leurs anneaux d'entiers ont fait l'objet de nombreuses études de Fröhlich et de son école. Cette étude, qui a donné lieu à une abondante littérature, a suscité le développement de techniques utilisables dans un cadre plus vaste que celui dans lequel elles ont été introduites. Nous ferons largement usage de ces outils dans notre travail pour lequel le livre de Fröhlich ([Frö]) servira souvent de référence.

Lorsqu'au moins un premier groupe de ramification de l'extension est non trivial, l'extension est dite sauvagement ramifiée. On s'intéresse essentiellement aux extensions sauvagement et faiblement ramifiées.

On commence ce chapitre en rappelant les définitions de base qui vont préciser ce qui vient d'être dit. On donne ensuite des propriétés générales des extensions faiblement ramifiées (partie 1.2), puis on considère le cas local abélien (partie 1.3). On termine par l'étude des extensions faiblement ramifiées de $\mathbb{Q}$ de groupe de Galois isomorphe à $C_{p^2} \rtimes C_p$ avec p premier impair (partie 1.4).

1.1 Fondations

Soit N/K une extension finie galoisienne de corps de nombres, de groupe de Galois G. On note $\mathcal{O}_K$ et $\mathcal{O}_N$ les anneaux d'entiers de K et N. Soit $\wp$ un idéal premier non nul de $\mathcal{O}_K$.

1.1.1 Décomposition dans une extension galoisienne

On rappelle brièvement quelques notations et définitions relatives aux idéaux premiers d'un corps de nombres. On peut se reporter à [Sa] pour plus de détails et pour les démonstrations des propriétés énoncées. Soit R un anneau de Dedekind. Tout idéal fractionnaire $\mathfrak{a}$ non nul s'écrit comme produit sur l'ensemble des idéaux premiers non nuls de R :

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \tag{1.1}$$

où $v_{\mathfrak{p}}(\mathfrak{a})$ est un entier qui est nul pour presque tout idéal premier $\mathfrak{p}$. On associe ainsi à chaque idéal premier $\mathfrak{p}$ une valuation discrète du corps de fractions M de R définie pour tout $x \in M$, $x \neq 0$, par $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(xR)$.

Puisque $\mathcal{O}_N$ est un anneau de Dedekind, on en déduit qu'il existe une décomposition :

$$\wp\,\mathcal{O}_N = \prod_{k=1}^{g} \mathfrak{p}_k^{e_k}$$

où les $\mathfrak{p}_k$ sont des idéaux premiers distincts de $\mathcal{O}_N$ au-dessus de $\wp$ et les e_k sont des entiers strictement positifs. L'entier g est le *degré de décomposition* de $\wp$ dans l'extension N/K. Le groupe G opère transitivement sur l'ensemble des idéaux premiers de $\mathcal{O}_N$ au-dessus de $\wp$. Ceci permet de montrer que les entiers e_k ont tous la même valeur e, qu'on appelle *l'indice de ramification* de $\wp$ dans l'extension N/K. On dit que $\wp$ est *ramifié* dans N/K si $e > 1$.

On appelle *groupe de décomposition* de $\mathfrak{p}_k/\wp$ et on note $G(\mathfrak{p}_k/\wp)$ le sous-groupe de G constitué des σ tels que $\sigma\mathfrak{p}_k = \mathfrak{p}_k$. Soit $\overline{N}$ (resp. $\overline{K}$) le corps résiduel $\mathcal{O}_N/\mathfrak{p}_k$ (resp. $\mathcal{O}_K/\wp$). Tout élément σ de $G(\mathfrak{p}_k/\wp)$ définit par passage au quotient un $\overline{K}$-automorphisme de $\overline{N}$. On obtient ainsi un homomorphisme surjectif :

$$G(\mathfrak{p}_k/\wp) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(\overline{N}/\overline{K}) \tag{1.2}$$

Le degré f de l'extension résiduelle $\overline{N}/\overline{K}$ est indépendant du choix de $\mathfrak{p}_k$; il ne dépend que de $\wp$ et s'appelle le *degré résiduel* de $\wp$ dans N/K. On a l'égalité :

$$[N : K] = efg \tag{1.3}$$

L'action de G sur l'ensemble des idéaux premiers $\mathfrak{p}_k$, $1 \leq k \leq g$, étant transitive, on note que les groupes de décomposition associés à deux premiers au-dessus de $\wp$ sont conjugués. Le noyau de (1.2) est le sous-groupe de G constitué des éléments σ tels que :

$$\forall x \in \mathcal{O}_N,\ \sigma(x) \equiv x \bmod \mathfrak{p}_k$$

On le note $G_0(\mathfrak{p}_k/\wp)$ et on l'appelle *groupe d'inertie* de $\mathfrak{p}_k/\wp$, son ordre est égal à e. C'est aussi le 0-ième groupe de ramification en $\mathfrak{p}_k/\wp$ dans la suite de groupes de ramification que l'on définit dans le prochain paragraphe.

1.1.2 Des témoins de la ramification

Pour tout entier $i \geq -1$, on pose :

$$G_i(\mathfrak{p}_k/\wp) = \{\sigma \in G(\mathfrak{p}_k/\wp),\ \forall x \in \mathcal{O}_N,\ \sigma(x) \equiv x \bmod \mathfrak{p}_k^{i+1}\}$$

On remarque que $G_{-1}(\mathfrak{p}_k/\wp) = G(\mathfrak{p}_k/\wp)$. Les $G_i(\mathfrak{p}_k/\wp)$ forment une suite décroissante de sous-groupes invariants de $G(\mathfrak{p}_k/\wp)$. De plus, $G_i(\mathfrak{p}_k/\wp) = \{1\}$ pour i assez grand. Si $\mathfrak{p}_k$ et $\mathfrak{p}_j$ sont deux idéaux premiers de $\mathcal{O}_N$ au-dessus de $\wp$ tels que $\sigma\mathfrak{p}_k = \mathfrak{p}_j$, on a pour tout $i \geq -1$:

$$G_i(\mathfrak{p}_j/\wp) = \sigma G_i(\mathfrak{p}_k/\wp)\sigma^{-1} \tag{1.4}$$

On peut maintenant préciser la notion de ramification faible pour une extension finie galoisienne de corps de nombres N/K de groupe de Galois G.

Définition 1.1.1 *On dit que l'extension N/K est faiblement ramifiée si, pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_N$, le deuxième groupe de ramification $G_2(\mathfrak{p}/(\mathfrak{p} \cap \mathcal{O}_K))$ est réduit à l'élément neutre.*

On présente maintenant un autre témoin de la ramification. Il s'agit de la *différente* $\mathcal{D}_{N/K}$ de l'extension. C'est un idéal entier de $\mathcal{O}_N$ dont l'inverse (appelé la *codifférente* de l'extension) est donné par :

$$\mathcal{D}_{N/K}^{-1} = \{x \in N,\ \mathrm{Tr}_{N/K}(x\mathcal{O}_N) \subset \mathcal{O}_K\}$$

Il est bien connu que seuls les idéaux premiers de $\mathcal{O}_N$ qui sont ramifiés dans N/K divisent la différente et qu'elle est reliée au discriminant $d_{N/K}$ de l'extension par :

$$d_{N/K} = \mathrm{N}_{N/K}(\mathcal{D}_{N/K}) \tag{1.5}$$

Lorsqu'on a une tour d'extensions finies de corps de nombres $K \subset M \subset N$, la différente et le discriminant de N/K s'expriment en fonction de ceux des extensions intermédiaires :

$$\mathcal{D}_{N/K} = \mathcal{D}_{N/M}\mathcal{D}_{M/K} \quad \text{et} \quad d_{N/K} = \mathrm{N}_{M/K}(d_{N/M}){d_{M/K}}^{[N:M]} \tag{1.6}$$

C'est la formule de Hilbert qui donne la valuation de la différente en un idéal premier $\mathfrak{p}$ de $\mathcal{O}_N$ au-dessus de $\wp$, en fonction de la suite des groupes de ramification en $\mathfrak{p}/\wp$, faisant ainsi le lien entre les deux témoins de la ramification qui ont été introduits :

$$v_{\mathfrak{p}}(\mathcal{D}_{N/K}) = \sum_{i \geq 0}(|G_i(\mathfrak{p}/\wp)| - 1) \tag{1.7}$$

Remarque 1.1.2 A l'aide de (1.4), on voit que, si deux idéaux premiers de $\mathcal{O}_N$ divisent un même idéal premier de $\mathcal{O}_K$, l'ordre de la différente en ces deux idéaux premiers est le même. Il s'ensuit que la différente est stable sous l'action du groupe de Galois de l'extension, ce qu'on peut exprimer en disant qu'elle a une structure de $\mathbb{Z}[G]$-module, ou encore que c'est un idéal *ambige*. On reviendra sur ce point dans le chapitre 3.

Cette formule permet aussi de donner une caractérisation de la ramification faible en termes des exposants des idéaux premiers qui divisent la différente. Cependant, on va voir qu'il est plus pratique de l'énoncer pour une extension de corps locaux et qu'il en va de même pour toutes les notions déjà introduites. C'est pourquoi on explique maintenant le...

1.1.3 Passage au local

Soit M un corps de nombres d'anneau d'entiers $\mathcal{O}$ et $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$. On sait associer à la valuation discrète $v_\mathfrak{p}$ introduite en (1.1) une valeur absolue ultramétrique sur M. On note $M_\mathfrak{p}$ le complété de M pour la topologie définie par cette valeur absolue. On sait que $v_\mathfrak{p}$ se prolonge en une valuation discrète sur $M_\mathfrak{p}$ que l'on note encore $v_\mathfrak{p}$. On désigne par $\mathcal{O}_\mathfrak{p}$ l'anneau de valuation de $v_\mathfrak{p}$ et encore par $\mathfrak{p}$ son idéal de valuation. On a l'égalité :

$$\mathcal{O}_\wp = \{x \in M_\mathfrak{p},\ v_\mathfrak{p}(x) \geq 0\}$$

Dans ce paragraphe, on fixe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_N$ au-dessus de $\wp$. On obtient ainsi une extension finie $N_\mathfrak{p}/K_\wp$ qui est galoisienne de groupe de Galois isomorphe à $G(\mathfrak{p}/\wp)$. On note $\mathcal{U}_\mathfrak{p}$ (resp. $\mathcal{U}_\wp$) le groupe des éléments inversibles de $\mathcal{O}_\mathfrak{p}$ (resp. $\mathcal{O}_\wp$). Un élément π de $K_\wp$ de valuation 1 s'appelle une *uniformisante*. Pour un tel élément, on a l'égalité :

$$K_\wp{}^* = \pi^\mathbb{Z} \times \mathcal{U}_\wp$$

Si p désigne la caractéristique du corps résiduel $\overline{K}_\wp$ de $K_\wp$, la réduction modulo $\wp$ fournit un isomorphisme du groupe des racines de l'unité de $K_\wp$ d'ordre premier à p (qu'on note $\mu^*_{K_\wp}$) sur le groupe $\overline{K}^*_\wp$. On a la décomposition en produit direct de groupes :

$$\mathcal{U}_\wp \simeq \mu^*_{K_\wp} \times (1 + \wp\,\mathcal{O}_\wp)$$

On introduit alors une filtration du groupe des unités de $K_\wp$ en posant :

$$\mathcal{U}^0_\wp = \mathcal{U}_\wp \quad \text{et, pour } i \geq 1, \quad \mathcal{U}^i_\wp = 1 + \wp^i\,\mathcal{O}_\wp$$

Dans le prochain paragraphe, on étudiera les rapports entre la filtration $(\mathcal{U}^i_\wp)_{i\geq 0}$ et la suite des groupes de ramification de l'extension $N_\mathfrak{p}/K_\wp$ que l'on définit maintenant. On note $\Gamma = \mathrm{Gal}(N_\mathfrak{p}/K_\wp)$. Pour tout entier $i \geq -1$, on pose :

$$\Gamma_i = \{\sigma \in \Gamma,\ \forall x \in \mathcal{O}_\mathfrak{p},\ \sigma(x) \equiv x \bmod \mathfrak{p}^{i+1}\}$$

On sait que Γ_i est isomorphe à $G_i(\mathfrak{p}/\wp)$. On peut maintenant donner une définition locale de la ramification faible.

Définition 1.1.3 *$N_\mathfrak{p}/K_\wp$ est faiblement ramifiée si Γ_2 est trivial.*

On remarque que N/K est faiblement ramifiée si et seulement si $N_\mathfrak{p}/K_\wp$ est faiblement ramifiée pour tout idéal premier $\wp$ de $\mathcal{O}_K$ et pour tout idéal premier

$\mathfrak{p}$ de $\mathcal{O}_N$ au-dessus de $\wp$. Les deux définitions sont donc cohérentes. On définit la différente "locale" $\mathcal{D}_{N_\mathfrak{p}/K_\wp}$ par la relation :

$$\mathcal{D}^{-1}_{N_\mathfrak{p}/K_\wp} = \{x \in N_\mathfrak{p},\ \mathrm{Tr}_{N_\mathfrak{p}/K_\wp}(x\mathcal{O}_\mathfrak{p}) \subset \mathcal{O}_\wp\}$$

On a l'égalité $\mathcal{D}_{N/K}\mathcal{O}_\mathfrak{p} = \mathcal{D}_{N_\mathfrak{p}/K_\wp}$.

1.1.4 Propriétés locales

Soit l/k une extension finie galoisienne de corps locaux de caractéristique 0 de groupe de Galois Γ. On entend par corps locaux des extensions finies de $\mathbb{Q}_p$ où p est la caractéristique résiduelle. On veut comparer la suite $(\Gamma_i)_{i\geq 0}$ et la filtration $(\mathcal{U}_l^i)_{i\geq 0}$ du groupe des unités $\mathcal{U}_l$ de l^*. On note $\bar{l}$ le corps résiduel de l. Nous énonçons sans démonstration les résultats de [Se1] IV.2 qui seront utiles à notre étude.

Proposition 1.1.4 *On a $\mathcal{U}_l^0/\mathcal{U}_l^1 = \bar{l}^*$ et, pour tout $i \geq 1$, $\mathcal{U}_l^i/\mathcal{U}_l^{i+1} \simeq \bar{l}$.*

Le résultat suivant fait le lien entre les quotients de deux termes successifs de chacune des suites Γ_i et $\mathcal{U}_l^i$.

Proposition 1.1.5 *Soit π une uniformisante de l et soit $i \geq 0$. L'application qui à $\sigma \in \Gamma_i$ associe $\sigma(\pi)/\pi$ définit par passage au quotient un isomorphisme de Γ_i/Γ_{i+1} sur un sous-groupe de $\mathcal{U}_l^i/\mathcal{U}_l^{i+1}$.*

On en déduit la propriété suivante.

Corollaire 1.1.6 *Pour tout $i \geq 1$, Γ_i/Γ_{i+1} est abélien p-élémentaire. En particulier, Γ_1 est un p-groupe et Γ_0 est le produit semi-direct d'un sous-groupe cyclique d'ordre e_0 premier à p par un p-sous-groupe invariant, égal à Γ_1.*

On voit maintenant que e est premier à p si et seulement si Γ_1 est réduit à l'élément neutre, c'est-à-dire si et seulement si l'extension l/k est modérée. Cette propriété permet de définir la ramification modérée (et donc aussi son contraire, la ramification sauvage) même lorsque l'extension n'est pas galoisienne. Par contre, on n'a pas une telle caractérisation pour la ramification faible : on ne peut définir celle-ci que pour les extensions galoisiennes.

On tire aussi de la proposition ci-dessus des propriétés sur les "sauts de ramification".

Corollaire 1.1.7

(i) Les entiers i tels que $\Gamma_i \neq \Gamma_{i+1}$ sont congrus entre eux modulo p.

(ii) Si Γ est abélien et si i est un entier non divisible par $e_0 = |\Gamma_0/\Gamma_1|$, alors $\Gamma_i = \Gamma_{i+1}$.

On revient à la situation du paragraphe précédent pour tirer la caractérisation suivante de la ramification faible à partir des propriétés énoncées ci-dessus. On tire de (1.7) que $\mathcal{D}_{N_\mathfrak{p}/K_\wp} = \mathfrak{p}^s$ avec $s = \sum_{i\geq 0}(|\Gamma_i| - 1)$. On note p la caractéristique résiduelle de $K_\wp$ et $e = e_0 p^\alpha$ l'ordre de Γ_0 avec $(e_0, p) = 1$.

Lemme 1.1.8 *$N_\mathfrak{p}/K_\wp$ est faiblement ramifiée si et seulement si :*

$$s = (e_0 + 1)p^\alpha - 2$$

1.2 Premières conséquences

On commence cette partie en donnant un exemple simple d'extension faiblement ramifiée de $\mathbb{Q}$ qui jouera un rôle important dans la partie 1.3. Il apparaissait déjà dans [Er1]. Soit p un nombre premier impair et ζ_{p^2} une racine primitive p^2-ième de l'unité.

Proposition 1.2.1 *La sous-extension $L/\mathbb{Q}$ de degré p de $\mathbb{Q}(\zeta_{p^2})$ est totalement, faiblement et sauvagement ramifiée.*

Preuve. Puisque $L/\mathbb{Q}$ est une p-extension, toutes les places autres que p sont modérément ramifiées. Puisque $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$ est totalement ramifiée en p, il est immédiat que $L/\mathbb{Q}$ est totalement et donc sauvagement ramifiée en p. Soit $\mathfrak{p}$ l'idéal premier de $\mathbb{Q}(\zeta_{p^2})$ au-dessus de p, $\wp = \mathfrak{p} \cap L$ et $s = v_\wp(\mathcal{D}_{L/\mathbb{Q}})$. Comme $\mathbb{Q}(\zeta_{p^2})/L$ est modérément ramifiée, on tire de (1.6) et de (1.7) :

$$\mathcal{D}_{\mathbb{Q}(\zeta_{p^2})} = \mathfrak{p}^{p-2+s(p-1)}$$

Comme $d_{\mathbb{Q}(\zeta_{p^2})} = p^{p(2p-3)}$ (cf [W] Proposition 2.1), on en déduit que $s = 2(p-1)$ et, à l'aide du lemme 1.1.8, que $G_2(\wp/p) = \{1\}$. ∎

Remarque 1.2.2 Cet exemple illustre le mauvais comportement de la ramification faible par rapport à la composition des extensions. En effet, $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$ est un composé non faiblement ramifié de $L/\mathbb{Q}$ et $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ (où l'on note ζ_p une racine primitive p-ième de l'unité), qui sont toutes deux faiblement ramifiées.

1.2.1 Propriétés de la ramification faible

Soit l/k une extension finie galoisienne de corps locaux de caractéristique 0 de groupe de Galois Γ. La ramification faible impose des contraintes sur la structure du groupe d'inertie. On note $e = e_0 p^\alpha$ son ordre, avec e_0 premier à la caractéristique résiduelle p et f_l le degré résiduel de $l/\mathbb{Q}_p$.

Proposition 1.2.3 *On suppose l/k faiblement ramifiée. Alors Γ_0 est le produit semi-direct d'un sous-groupe cyclique d'ordre e_0, où e_0 divise $p^{f_l} - 1$, par un p-sous-groupe normal élémentaire d'ordre p^α avec $\alpha \leq f_l$. Si de plus l/k est abélienne, alors $e_0 = 1$.*

Preuve. Cela découle des résultats du paragraphe 1.1.4. ▌

On a vu plus haut que la ramification faible ne se comporte pas toujours bien vis-à-vis de la composition des extensions. On revient maintenant sur ce point et on regarde si elle est préservée dans les sous-extensions.

Proposition 1.2.4 *(i) Toute sous-extension galoisienne d'une extension faiblement ramifiée est faiblement ramifiée.*

(ii) Soient l_1/k une extension finie galoisienne de groupe de Galois Δ, l_2/k une extension finie non ramifiée et $l = l_1 l_2$. On note $\Gamma = \mathrm{Gal}(l/k)$. Alors l'homomorphisme de restriction de Γ dans Δ induit un isomorphisme de Γ_i sur Δ_i pour tout entier $i \geq 0$.

Preuve. Soit l/k une extension faiblement ramifiée de groupe de Galois Γ et soit Θ un sous-groupe distingué de Γ. On sait déterminer grâce au théorème de Herbrand ([Se1] IV3 lemme 5) la suite des groupes de ramification dans la sous-extension de l/k fixée par Θ (donc de groupe de Galois isomorphe à Γ/Θ). En particulier :

$$(\Gamma/\Theta)_{\varphi(2)} \simeq \Gamma_2\Theta/\Theta = \{1\}$$

où φ est la fonction de Herbrand de l/l^{Θ}. Or $\varphi(2) \leq 2$ et par conséquent $(\Gamma/\Theta)_2 = \{1\}$, d'où (i).

Soit i un entier positif et $\sigma \in \Gamma_i$, alors $\sigma(x) \equiv x \bmod \mathfrak{p}_l{}^{i+1}$ pour tout $x \in \mathcal{O}_l$. Comme l/l_1 est non ramifiée, on a $\mathfrak{p}_{l_1} = \mathfrak{p}_l$ donc $\sigma_{|l_1}(x) \equiv x \bmod \mathfrak{p}_{l_1}{}^{i+1}$ pour tout $x \in \mathcal{O}_{l_1}$, si bien que $\sigma \mapsto \sigma_{|l_1}$ induit un homomorphisme de Γ_i dans Δ_i. Il est injectif car son noyau est $\Gamma_i \cap \mathrm{Gal}(l/l_1) = \{1\}$, si bien que $|\Gamma_i| \leq |\Delta_i|$ pour tout $i \geq 0$. Par la formule de transitivité (1.6), on obtient $\mathcal{D}_{l/k} = \mathcal{D}_{l_1/k}$ et la formule de Hilbert (1.7) entraîne :

$$\sum_{i\geq 0}(|\Gamma_i| - 1) = \sum_{i\geq 0}(|\Delta_i| - 1)$$

On en tire $|\Gamma_i| = |\Delta_i|$ pour tout $i \geq 0$, d'où (ii). ▌

1.2.2 Caractérisation à l'aide du polynôme minimal

On conserve les notations du paragraphe précédent. Si l/k est totalement ramifiée, on sait qu'il existe une uniformisante π qui est un élément primitif pour l'anneau d'entiers, c'est-à-dire tel que $\mathcal{O}_l = \mathcal{O}_k[\pi]$. On souhaite obtenir une caractérisation de la ramification faible portant sur les cœfficients du polynôme minimal de π. Pour cela, on a besoin de la propriété suivante de la différente de l'extension. Soit $x \in \mathcal{O}_l$ un élément primitif de l/k et $f(X) \in k[X]$ son polynôme caractéristique. On sait que $\mathcal{D}_{l/k}$ divise l'idéal principal $(f'(x))$ avec égalité si et seulement si $\mathcal{O}_l = \mathcal{O}_k[x]$ ([Se1] III.7 corollaire 2). On en déduit le critère suivant.

Proposition 1.2.5 *Soit l/k une extension galoisienne finie de corps locaux de caractéristique 0. On suppose que l/k est sauvagement ramifiée d'indice de ramification $e = e_0 p^\alpha$ avec $(e_0, p) = 1$. Alors l/k est totalement et faiblement ramifiée si et seulement si il existe $\pi \in \mathcal{O}_l$ tel que $l = k(\pi)$ et dont les cœfficients du polynôme minimal sur k (que l'on écrit $f(X) = \sum_{0 \leq i \leq e} a_i X^{e-i}$ avec $a_0 = 1$) vérifient :*

(i) $v_k(a_i) \geq 1$ *pour* $1 \leq i \leq e$,

(ii) $v_k(a_e) = v_k(a_{i_0}) = 1$ *avec* $i_0 = (e_0 - 1)p^\alpha + 1$,

(iii) $v_k(a_i) \geq 2$ *si* $i > i_0$ *et* $(i, p) = 1$.

Preuve. On suppose l/k totalement et faiblement ramifiée. Soit π une uniformisante de l. Puisque l/k est totalement ramifiée, le polynôme minimal f de π sur k est un polynôme d'Eisenstein, ce qui implique $v_k(a_i) \geq 1$ pour $1 \leq i \leq e$ et $v_k(a_e) = 1$. En outre, $\mathcal{O}_l = \mathcal{O}_k[\pi]$, donc $v_l(\mathcal{D}_{l/k}) = v_l(f'(\pi))$. Le lemme suivant calcule cette valuation.

Lemme 1.2.6 *Avec les notations précédentes, on a :*

$$v_l(f'(\pi)) = \mathrm{Inf}\,\{v_l((e-i)a_i\pi^{e-i-1}),\ 0 \leq i \leq e-1\}$$

Preuve. On a $f'(\pi) = \sum_{0 \leq i \leq e-1} (e-i)a_i\pi^{e-i-1}$ et, pour tout entier $0 \leq i \leq e-1$ tel que $a_i \neq 0$,

$$v_l((e-i)a_i\pi^{e-i-1}) = (e-i-1) + ev_k(a_i) + ev_k(e-i) \tag{1.8}$$

donc

$$v_l((e-i)a_i\pi^{e-i-1}) \equiv -i - 1 \bmod e$$

Par conséquent, les valuations de chaque terme de $f'(\pi)$ sont distinctes, d'où le résultat. ∎

Par le lemme 1.1.8, on sait que :

$$v_l(\mathcal{D}_{l/k}) = (e-1) + p^\alpha - 1 \tag{1.9}$$

donc $\mathrm{Inf}\,\{v_l((e-i)a_i\pi^{e-i-1}),\ 0 \leq i \leq e-1\}$ est obtenu pour l'entier i_0 tel que $0 \leq i_0 \leq e-1$ et :

$$-i_0 - 1 \equiv p^\alpha - 2 \bmod e$$

Ceci équivaut à $i_0 \equiv e - (p^\alpha - 1) \bmod e$ et, puisque $1 \leq e - (p^\alpha - 1) < e$, on trouve $i_0 = e - (p^\alpha - 1) = (e_0 - 1)p^\alpha + 1$. A l'aide de (1.8) et (1.9), on en déduit que les deux conditions suivantes sont nécessaires :

$$(e - i_0 - 1) + ev_k(a_{i_0}) + ev_k(e - i_0) = (e-1) + p^\alpha - 1 \tag{1.10}$$

et, pour $i \neq i_0$,

$$(e-i-1) + ev_k(a_i) + ev_k(e-i) > (e-1) + p^\alpha - 1 \tag{1.11}$$

Puisque $(e_0, p) = 1$, on a que (1.10) équivaut à $v_k(a_{i_0}) = 1$. La condition (1.11) équivaut à $ev_k(a_i) + ev_k(e-i) > p^\alpha - 1 + i$, donc elle est vérifiée si p divise i. Si p

ne divise pas i, elle est vérifiée dès que $v_k(a_i) \geq 2$; si $v_k(a_i) = 1$, (1.11) équivaut à $i < i_0$. On a donc montré que l/k faiblement ramifiée implique $v_k(a_0) = 0$, $v_k(a_e) = v_k(a_{i_0}) = 1$, $v_k(a_i) \geq 1$ pour $1 \leq i \leq e$ et $v_k(a_i) \geq 2$ pour $i > i_0$ et $(i, p) = 1$.

Réciproquement, on suppose réalisées ces conditions pour $\pi \in \mathcal{O}_l$, ainsi que la condition $l = k(\pi)$. Puisque le polynôme caractéristique f de π sur k est d'Eisenstein, l/k est totalement ramifiée et $\mathcal{O}_l = \mathcal{O}_k[\pi]$ donc $v_l(\mathcal{D}_{l/k}) = v_l(f'(\pi))$. On vérifie que les conditions énumérées ci-dessus entraînent $v_l(f'(\pi)) = (e-1)+ p^\alpha - 1$ et donc $v_l(\mathcal{D}_{l/k}) = |\Gamma_0| - 1 + |\Gamma_1| - 1$, c'est-à-dire l/k est faiblement ramifiée. ▮

On a le cas particulier suivant (où $i_0 = 1$) :

Corollaire 1.2.7 *Si l/k est une p-extension galoisienne finie de corps locaux de caractéristique 0, alors l/k est totalement et faiblement ramifiée si et seulement si il existe $\pi \in \mathcal{O}_l$ tel que $l = k(\pi)$ et dont les cœfficients du polynôme minimal sur k (que l'on écrit $f(X) = \sum_{0 \leq i \leq e} a_i X^{e-i}$ avec $a_0 = 1$) vérifient :*

(i) $v_k(a_i) \geq 1$ *pour* $1 \leq i \leq e$,

(ii) $v_k(a_e) = v_k(a_1) = 1$,

(iii) $v_k(a_i) \geq 2$ *si* $i \geq 2$ *et* $(i, p) = 1$.

Cette caractérisation, inspirée de la preuve de la proposition 13 de [Se1] III.7, n'est pas souvent applicable en pratique. D'une part, il n'est pas toujours aisé de trouver un élément primitif de l'anneau d'entiers ; d'autre part, si on se donne un polynôme à cœfficients entiers vérifiant les conditions de la proposition 1.2.5, son corps de rupture est très rarement galoisien sur $\mathbb{Q}$ et ne peut donc pas en être une extension faiblement ramifiée à la place considérée. En ce qui concerne les p-extensions de $\mathbb{Q}$, on montrera, dans le cas où le groupe de Galois est isomorphe à $C_{p^2} \rtimes C_p$, des critères de ramification faible beaucoup plus efficaces dans la partie 1.4, qui permettront de trouver des exemples d'extensions faiblement ramifiées de $\mathbb{Q}$ de degré 27 (voir chapitre 2).

1.3 Etude locale dans le cas abélien

Dans cette partie, on fixe un nombre premier p supérieur ou égal à 3 et on s'intéresse aux extensions $N/\mathbb{Q}_p$ abéliennes de groupe de Galois G qui sont faiblement ramifiées. Le fait de considérer des extensions absolues abéliennes permet d'utiliser la version locale du théorème de Kronecker-Weber et, *in fine*, de décrire toutes celles qui sont sauvagement et faiblement ramifiées de degré donné (théorème 1).

Un article récent de Byott présente l'esquisse d'une étude similaire dans le cas non absolu en remplaçant le théorème de Kronecker-Weber par la description des extensions abéliennes d'un corps local à l'aide des corps de division associés à des groupes formels de Lubin-Tate (voir [Se2] pour cette théorie). Il l'utilise pour montrer que l'anneau d'entiers d'une extension locale abélienne faiblement

ramifiée est libre sur son ordre associé et pour décrire explicitement celui-ci ([B] théorème 5), mais n'en tire pas une description aussi précise que celle qu'on va énoncer dans le cas absolu.

Ici, on se concentre sur les extensions abéliennes sauvagement et faiblement ramifiées de $\mathbb{Q}_p$. On adopte en conséquence la terminologie suivante.

Définition 1.3.1 *On dira qu'une extension finie de $\mathbb{Q}_p$ est pure si elle est abélienne, sauvagement et faiblement ramifiée.*

On commence par préciser quelques notations. On fixe une fois pour toutes une clôture algébrique $\mathbb{Q}_p^c$ de $\mathbb{Q}_p$; pour toute extension K de $\mathbb{Q}_p$ contenue dans $\mathbb{Q}_p^c$ et pour tous entiers $f, m \geq 1$, on note $K\{f\}$ l'unique extension non ramifiée de degré f de K contenue dans $\mathbb{Q}_p^c$ et $K[m]$ le corps obtenu en adjoignant à K les racines m-ièmes de l'unité dans $\mathbb{Q}_p^c$.

On introduit maintenant un exemple d'extension pure qui jouera un rôle important dans la suite de cette partie.

Proposition 1.3.2 *La sous-extension L de degré p de $\mathbb{Q}_p[p^2]$ est pure et totalement ramifiée.*

Preuve. Ceci découle de la proposition 1.2.1. ▌

On déduit alors facilement de la proposition 1.2.4 le résultat suivant.

Corollaire 1.3.3 *Soit f un entier supérieur ou égal à 1, alors toute sous-extension de $L.\mathbb{Q}_p\{f\}$ (resp. non contenue dans $\mathbb{Q}_p\{f\}$) est faiblement ramifiée (resp. pure).*

Preuve. Puisque L est pure, on déduit de (ii) de la proposition 1.2.4 que le compositum $L.\mathbb{Q}_p\{f\}$ l'est aussi et, par (i), on sait que toutes ses sous-extensions $M/\mathbb{Q}_p$ sont faiblement ramifiées. On note $e(A)$ l'indice de ramification d'une extension A de $\mathbb{Q}_p$. On a $e(L.\mathbb{Q}_p\{f\}) = p$ donc $e(M) = 1$ ou p, ce qui montre le résultat. ▌

On est maintenant prêt à démontrer le résultat principal de cette partie.

Théorème 1 *Soit $n \geq 1$ un entier divisible par p. Alors les extensions pures de $\mathbb{Q}_p$ de degré n sont les sous-extensions de degré n de $L.\mathbb{Q}_p\{n\}$ distinctes de $\mathbb{Q}_p\{n\}$.*

Preuve. On sait par le corollaire 1.3.3 que toute sous-extension de $L.\mathbb{Q}_p\{n\}$ de degré n distincte de $\mathbb{Q}_p\{n\}$ est pure. Il suffit donc de montrer que toute extension pure de degré n est contenue dans $L.\mathbb{Q}_p\{n\}$. Pour cela, on fixe $A/\mathbb{Q}_p$ une extension pure de degré n.

Lemme 1.3.4 *On a les égalités : $G_0(A) = G_1(A) \simeq \mathbb{Z}/p\mathbb{Z}$.*

Preuve. On pose $e_0 = [G_0(A) : G_1(A)]$. Puisque $G_1(A) \neq G_2(A)$ alors $e_0 = 1$ d'après le corollaire 1.1.7. En outre, $G_1(A) = G_1(A)/G_2(A)$ est p-élémentaire (corollaire 1.1.6). On sait de plus que $A/\mathbb{Q}_p$ est contenue dans une extension cyclotomique sauvage. Plus précisément, il existe $\alpha \geq 1$ et m avec $(p, m) = 1$ tels

que $A \subset \mathbb{Q}_p[p^{\alpha+1}m]$. Puisque $G_0(A)$ est un quotient de $G_0(\mathbb{Q}_p[p^{\alpha+1}m])$ et que ce dernier groupe est isomorphe à $(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^*$, on en déduit que $G_0(A)$ est cyclique, ce qui démontre le lemme. ▮

On sait maintenant que $n = pf$ avec $p = e(A)$ et $f = f(A)$ le degré résiduel de A sur $\mathbb{Q}_p$. On écrit $f = p^\beta f'$ avec $\beta \geq 0$ et $(f', p) = 1$. Soit $G = \mathrm{Gal}(A/\mathbb{Q}_p)$. Puisque G est abélien, on le décompose en produit direct de ses sous-groupes de Sylow et on obtient :

$$G = G(p) \times G'$$

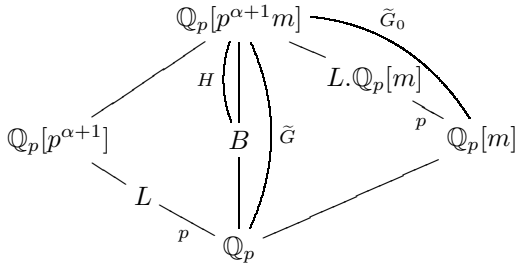
avec $|G(p)| = p^{\beta+1}$ et $|G'| = f'$. On en déduit la décomposition $A = B.\mathbb{Q}_p\{f'\}$ où $B/\mathbb{Q}_p$ est une extension pure de groupe de Galois isomorphe à $G(p)$. Comme précédemment, on a $B \subset \mathbb{Q}_p[p^{\alpha+1}m]$; on note $\widetilde{G} = \mathrm{Gal}(\mathbb{Q}_p[p^{\alpha+1}m]/\mathbb{Q}_p)$, $\widetilde{G}_0 \subset \widetilde{G}$ le groupe d'inertie et $H = \mathrm{Gal}(\mathbb{Q}_p[p^{\alpha+1}m]/B)$. En outre, $\mathbb{Q}_p[p^{\alpha+1}m]$ est le compositum des extensions $\mathbb{Q}_p[p^{\alpha+1}]$ et $\mathbb{Q}_p[m]$ qui sont linéairement disjointes sur $\mathbb{Q}_p$, et $\widetilde{G}_0 \simeq \mathrm{Gal}(\mathbb{Q}_p[p^{\alpha+1}m]/\mathbb{Q}_p[m])$. Puisque

$$G_0(B) \simeq \widetilde{G}_0/(H \cap \widetilde{G}_0)$$

on en déduit que $|H \cap \widetilde{G}_0| = p^{\alpha-1}(p-1)$, et donc

$$H \cap \widetilde{G}_0 = \mathrm{Gal}(\mathbb{Q}_p[p^{\alpha+1}m]/L.\mathbb{Q}_p[m])$$

si bien que $\mathrm{Gal}(\mathbb{Q}_p[p^{\alpha+1}m]/L.\mathbb{Q}_p[m]) \subset H$ et, par conséquent $B \subset L.\mathbb{Q}_p[m]$.



On écrit $[\mathbb{Q}_p[m] : \mathbb{Q}_p] = p^\gamma r$ avec $(p, r) = 1$, on a $\mathbb{Q}_p[m] = \mathbb{Q}_p\{p^\gamma r\}$. Puisque $B/\mathbb{Q}_p$ est une p-extension, on obtient que $B \subset L.\mathbb{Q}_p\{p^\gamma\}$ (et donc $\gamma \geq \beta$). On est ainsi ramené à la situation suivante :

$$B = (L.\mathbb{Q}_p\{p^\gamma\})^H$$

où H est un sous-groupe de $\mathrm{Gal}(L.\mathbb{Q}_p\{p^\gamma\}/\mathbb{Q}_p)$ d'indice $p^{\beta+1}$. Si $\beta = \gamma$ alors $B = L.\mathbb{Q}_p\{p^\gamma\}$ et $A \subset L.\mathbb{Q}_p\{n\}$. Sinon, comme $B/\mathbb{Q}_p$ est ramifiée et comme $\mathrm{Gal}(L.\mathbb{Q}_p\{p^\gamma\}/\mathbb{Q}_p)$ est le produit direct d'un groupe cyclique C_p d'ordre p par un groupe cyclique C_{p^γ} d'ordre p^γ, on sait que $C_p \times \{1\} \not\subset H$, donc le sous-groupe $(C_p \times \{1\})H$ est d'ordre $p^{\gamma-\beta+1}$ et se décompose en produit direct $C_p \times C_{p^{\gamma-\beta}}$. On en déduit que le sous-groupe H^p des puissances p-ièmes des éléments de H vérifie $H^p = C_{p^{\gamma-\beta-1}}$, ce qui entraîne $B \subset (L.\mathbb{Q}_p\{p^\gamma\})^{H^p} = L.\mathbb{Q}_p\{p^{\beta+1}\}$. On conclut là encore que $A \subset L.\mathbb{Q}_p\{p^{\beta+1}f'\} = L.\mathbb{Q}_p\{n\}$ et cela achève la preuve du théorème. ▮

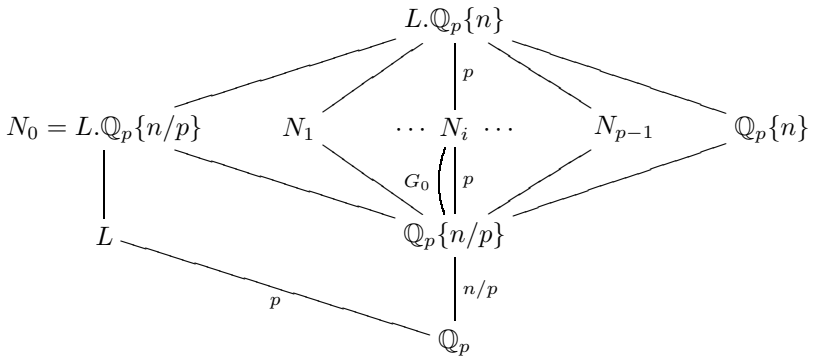
Corollaire 1.3.5 *Soit $n \geq 1$ un entier divisible par p. Alors il existe p extensions pures de $\mathbb{Q}_p$ de degré n. En outre :*

(i) Si $v_p(n) = 1$, ce sont les extensions cycliques $F.\mathbb{Q}_p\{n/p\}$ où F parcourt l'ensemble des sous-extensions propres de $L.\mathbb{Q}_p\{p\}$ distinctes de $\mathbb{Q}_p\{p\}$.

(ii) Si $v_p(n) \geq 2$, on obtient l'extension (non cyclique) $L.\mathbb{Q}_p\{n/p\}$ et $p-1$ extensions cycliques.

Preuve. On écrit $n = p^{\beta+1}f'$ avec $\beta \geq 0$ et $(p, f') = 1$. D'après la démonstration précédente, on sait qu'une extension convenable est de la forme $M.\mathbb{Q}_p\{f'\}$ avec $M \subset L.\mathbb{Q}_p\{p^{\beta+1}\}$, ce qui ramène à chercher les sous-groupes d'ordre p de $C_p \times C_{p^{\beta+1}}$ distincts de $C_p \times \{1\}$. Le groupe $C_p \times C_{p^{\beta+1}}$ contient $p^2 - 1$ éléments d'ordre p, d'où l'on déduit $p+1$ sous-groupes d'ordre p et donc p sous-groupes convenables. Ils possèdent un générateur de la forme uv avec $u \in C_p$ et $v \in C_{p^{\beta+1}}$ d'ordre p. Si $u = 1$, on obtient le sous-groupe $\{1\} \times C_p$; si $u \neq 1$, alors $C_p \times C_{p^{\beta+1}}$ se décompose en produit direct $< uv > \times < w >$ où w est un générateur de $C_{p^{\beta+1}}$ (en effet, si ce n'est pas le cas, $uv \in < w >$ et donc $u \in < w >$, ce qui est absurde). L'extension associée au cas $u = 1$ est $L.\mathbb{Q}_p\{p^\beta\}$. Dans les autres cas, $(C_p \times C_{p^{\beta+1}})/H$ est donc cyclique. ∎

Les p extensions pures de $\mathbb{Q}_p$ de degré n sont les N_i, $(0 \leq i \leq p-1)$, du diagramme :



Remarque 1.3.6 Si $v_p(n) = 1$, toute extension pure est "décomposée", c'est le compositum d'une extension non ramifiée de $\mathbb{Q}_p$ de degré n/p par une extension pure de $\mathbb{Q}_p$ de degré p. Si $v_p(n) \geq 2$, seule $N_0 = L.\mathbb{Q}_p\{n/p\}$ est décomposée ; c'est donc la seule extension pure de degré n telle que G_1 soit facteur direct du groupe de Galois. Pour $i \geq 1$, les $N_i/\mathbb{Q}_p$ sont cycliques, donc non décomposées. Dans ce dernier cas, l'hypothèse (H) de [CNT2] (partie 1), qui permet l'étude de la structure galoisienne d'un sous-réseau de l'anneau d'entiers, ne peut pas être satisfaite.

Remarque 1.3.7 $L.\mathbb{Q}_p\{n\}/N_i$ étant non ramifiée, on a toujours :

$$\mathcal{D}_{N_i} = \mathrm{Tr}_{L.\mathbb{Q}_p\{n\}/N_i}(\mathcal{D}_{L.\mathbb{Q}_p\{n\}})$$

Le théorème 1 sera illustré pour $p = 3$ et $n = 45$ dans la partie 2.2.2.

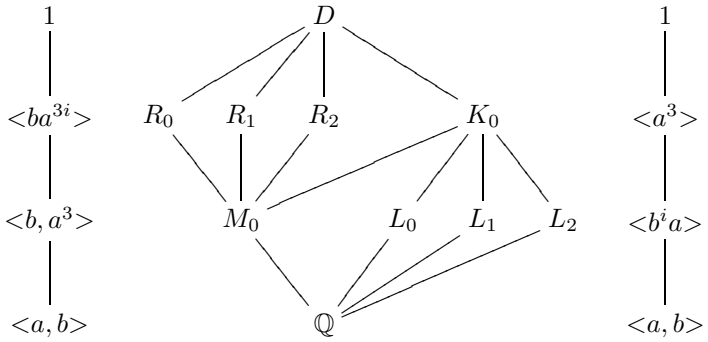
1.4 Etude globale dans le cas $C_{p^2} \rtimes C_p$

Dans cette partie, on fixe un nombre premier p impair. On se donne une extension R de $\mathbb{Q}$ de degré p^2 de clôture galoisienne D avec $G = \mathrm{Gal}(D/\mathbb{Q})$ non abélien d'ordre p^3 d'exposant p^2, c'est-à-dire (voir [Ha] 4.4.4 p.52) :

$$G \simeq C_{p^2} \rtimes C_p$$

Puisque G est transitif de degré p^2, il existe un polynôme $P(x)$ unitaire, à cœfficients entiers, irréductible et de degré p^2, dont R est le corps de rupture (c'est-à-dire $R = \mathbb{Q}[x]/(P(x))$) et D le corps de décomposition (contenant toutes les racines de P). Les calculs à l'aide de logiciels étant plus aisés dans R (car P donne directement accès à R, qui de plus, est de degré moindre que D), il est pratique d'avoir un critère de ramification faible dans le corps de décomposition à partir du discriminant du corps de rupture. C'est l'objet de cette partie.

On commence par donner le diagramme de Hasse des sous-corps de D dans le cas $p = 3$. On note a et b deux générateurs de G vérifiant $a^9 = b^3 = 1$ et $b^{-1}ab = a^4$ (voir [Ha] 4.4) :



Le corps de rupture R de $P(x)$ est isomorphe aux sous-extensions R_i de D $(0 \leq i \leq 2)$ fixées respectivement par les sous-groupes $< ba^{3i} >$ (conjugués par l'action de G). Les autres sous-extensions de D sont galoisiennes sur $\mathbb{Q}$.

Les résultats de cette partie seront appliqués dans le chapitre 2 sur une famille de polynômes de groupe de Galois G isomorphe à $C_9 \rtimes C_3$.

1.4.1 Une condition nécessaire pour la ramification faible

Ce paragraphe est consacré à la preuve de la proposition suivante :

Proposition 1.4.1 *Si $D/\mathbb{Q}$ est faiblement ramifiée, alors $v_p(d_R) \leq 2(p^2 - 1)$.*

On note e, f et g l'indice de ramification, le degré résiduel et le degré de décomposition de p dans $D/\mathbb{Q}$; on note s la valuation de la différente de $D/\mathbb{Q}$ en n'importe quel idéal premier de D au-dessus de p.

On a plusieurs cas à envisager. Tout d'abord, si $R/\mathbb{Q}$ est non ramifiée en p, $v_p(d_R) = 0$ et la proposition est vraie. On suppose donc que $R/\mathbb{Q}$ est ramifiée en p. La formule de transitivité (1.6) pour le discriminant se traduit ici par :

$$v_p(d_R) = \frac{1}{p}\big(v_p(d_D) - v_p(\mathrm{N}_{R/\mathbb{Q}}(d_{D/R}))\big)$$

On a $v_p(d_D) = fgs$ et, puisque $D/\mathbb{Q}$ est faiblement ramifiée, on tire de (1.7) que $s = 2(e-1)$, si bien que :

$$v_p(d_R) = 2p^2\,\frac{e-1}{e} - \frac{1}{p}\,v_p(\mathrm{N}_{R/\mathbb{Q}}(d_{D/R})) \tag{1.12}$$

Dans un premier temps, on considère les cas où p n'est pas décomposé dans $R/\mathbb{Q}$.

Lemme 1.4.2 *On suppose que $D/\mathbb{Q}$ est faiblement ramifiée et que $R/\mathbb{Q}$ est totalement ramifiée en p, alors $v_p(d_R) = 2(p^2-1)$.*

Preuve. On a $e = p^2$ car $G_0 = G_1 = G_1/G_2$ est p-élémentaire donc $G_0 \neq G$. Il s'ensuit que D/R est non ramifiée et $v_p(d_R) = 2(p^2-1)$ par (1.12). ∎

Lemme 1.4.3 *On suppose que $D/\mathbb{Q}$ est faiblement ramifiée et que $e(p, R/\mathbb{Q}) = f(p, R/\mathbb{Q}) = p$, alors $v_p(d_R) = 2p(p-1)$.*

Preuve. Soit $\wp$ l'unique idéal premier de R au-dessus de p. Si $\wp$ est ramifié dans D/R, alors $e = p^2$ et, puisque D/R est faiblement ramifiée, $v_\wp(d_{D/R}) = 2(p-1)$ donc $v_p(d_R) = 2(p^2-1) - 2(p-1) = 2p(p-1)$ par (1.12). Si $\wp$ n'est pas ramifié dans D/R, alors $e = p$ et $v_p(d_R) = 2p(p-1)$ aussi. ∎

On considère maintenant les cas où p est décomposé dans $R/\mathbb{Q}$. Soient $\wp_1, \cdots, \wp_{g_R}$ les idéaux premiers de R au-dessus de p. On a encore deux situations à traiter séparément.

Lemme 1.4.4 *On suppose que $D/\mathbb{Q}$ est faiblement ramifiée et que p se décompose dans $R/\mathbb{Q}$ en g_R idéaux premiers qui sont tous ramifiés dans $R/\mathbb{Q}$. Alors $g_R = p$ et $v_p(d_R) = 2p(p-1)$.*

Preuve. Comme $e(\wp_i/p) = p$ pour tout $1 \leq i \leq g_R$, on tire de

$$[R:\mathbb{Q}] = p^2 = \sum_{1\leq i\leq g_R} e(\wp_i/p) f(\wp_i/p) \tag{1.13}$$

que tous les $f(\wp_i/p)$ valent 1 et que $g_R = p$. De plus, les $\wp_i$ ont tous le même comportement dans D/R. Si aucun n'y est ramifié, alors D/R est non ramifiée en p, $e = p$ et $v_p(d_R) = 2p(p-1)$. Si tous sont ramifiés dans D/R, alors $e = p^2$ et pour tout $1 \leq k \leq p$, $v_{\wp_k}(d_{D/R}) = 2(p-1)$, donc $v_p(d_R) = 2(p^2-1) - 2(p-1) = 2p(p-1)$. ∎

Lemme 1.4.5 *On suppose que $D/\mathbb{Q}$ est faiblement ramifiée et que p se décompose dans $R/\mathbb{Q}$ en g_R idéaux premiers dont exactement j sont ramifiés dans $R/\mathbb{Q}$ avec $1 \leq j \leq p-1$. Alors $v_p(d_R) = 2j(p-1)$.*

Preuve. On note $\wp_1, \cdots, \wp_j$ les idéaux premiers de R au-dessus de p qui sont ramifiés dans $R/\mathbb{Q}$ et $\wp_{j+1}, \cdots, \wp_{g_R}$ ceux qui ne le sont pas. On sait que ces derniers sont tous ramifiés dans D/R, cela entraîne qu'ils ont tous le même degré résiduel f_R dans $R/\mathbb{Q}$ et que $e = p$. Les $\wp_k$ avec $1 \leq k \leq j$ ne sont donc pas ramifiés dans D/R. Comme D/R est faiblement ramifiée, on a :

$$d_{D/R} = \wp' \prod_{k=j+1}^{g_R} \wp_k^{2(p-1)}$$

où $\wp'$ est un idéal de R premier à p, donc $v_p(\mathrm{N}_{R/\mathbb{Q}}(d_{D/R})) = 2(p-1)f_R(g_R - j)$. Si $f_R = 1$, la formule (1.13) donne $g_R - j = p(p-j)$; sinon $f_R = p$ et la formule (1.13) donne $g_R = p$. Dans les deux cas, $f_R(g_R - j) = p(p-j)$ et on déduit de (1.12) que $v_p(d_R) = 2p(p-1) - 2(p-1)(p-j) = 2j(p-1)$. ∎

Ceci achève la preuve de la proposition 1.4.1.

1.4.2 Une condition nécessaire et suffisante de ramification faible

On se place maintenant dans les conditions du lemme 1.4.3 pour établir une condition nécessaire et suffisante de ramification faible que l'on applique ensuite à un exemple.

Théorème 1.4.6 *Soit R une extension de $\mathbb{Q}$ de degré p^2 de clôture galoisienne D avec $G = \mathrm{Gal}(D/\mathbb{Q})$ non abélien d'ordre p^3 d'exposant p^2. On suppose que $e(p, R/\mathbb{Q}) = f(p, R/\mathbb{Q}) = p$.*

(i) Lorsque $p \geq 5$, $D/\mathbb{Q}$ est faiblement ramifiée si et seulement si $v_p(d_R) \leq 2(p^2-1)$.

(ii) Lorsque $p = 3$, $D/\mathbb{Q}$ est faiblement ramifiée si et seulement si $v_p(d_R) < 16$.

En outre, si $D/\mathbb{Q}$ est faiblement ramifié, alors $v_p(d_R) = 2p(p-1)$.

Ce résultat contient le lemme 1.4.3 et sa réciproque. On commence par rappeler quelques propriétés de l'extension galoisienne $D/\mathbb{Q}$ et de son groupe de Galois G. A l'instar de [Ha] (*loc. cit.*), on note a et b des générateurs de G tels que $a^{p^2} = b^p = 1$ et $b^{-1}ab = a^{1+p}$. On sait que G contient p sous-groupes non distingués d'ordre p conjugués deux à deux ; ce sont les $a^k B a^{-k}$ avec $B = < b >$ et $0 \leq k \leq p-1$. D contient donc p sous-extensions de degré p^2 non galoisiennes conjuguées deux à deux. Soient $R_0 = D^B$ et x_0 un générateur de R_0 sur $\mathbb{Q}$; soit $R_k = D^{a^k B a^{-k}}$ pour $0 \leq k \leq p-1$, alors $R_k = \mathbb{Q}(a^k(x_0))$. Puisque $\mathrm{Gal}(D/R_0) = B$, on a $a^s(x_0) \neq x_0$ pour $0 \leq s \leq p^2 - 1$ et on pose $x_s = a^s(x_0)$. G opère fidèlement sur $\{x_0, \cdots, x_{p^2-1}\}$, si bien qu'on a un plongement :

$$\begin{array}{rccll} \varphi \ : & G & \hookrightarrow & S_{p^2} & \\ & g & \longmapsto & \tau_g & \text{avec } g(x_k) = x_{\tau_g(k)} \text{ pour tout } k \end{array}$$

où S_{p^2} est le groupe de permutations à p^2 éléments. On sait que $\varphi(a)$ est le cycle $(0, 1, 2, \cdots, p^2-1)$. Pour déterminer la décomposition en cycles de $\varphi(b)$, on regroupe les racines x_s dans les corps auxquels elles appartiennent :

$$\begin{array}{cccc} R_0 & R_1 & \cdots & R_{p-1} \\ x_0 & x_1 & \cdots & x_{p-1} \\ x_p & x_{p+1} & \cdots & x_{2p-1} \\ x_{2p} & x_{2p+1} & \cdots & x_{3p-1} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ x_{(p-1)p} & x_{(p-1)p+1} & \cdots & x_{p^2-1} \end{array}$$

Pour tous entiers k et l avec $1 \leq k, l \leq p-1$, on a :

$$ba^{k+lp} = a^{k+(l-k)p}b$$

On en déduit que $b(x_{k+lp}) = x_{k+(l-k)p}$ (resp. $x_{k+(p+l-k)p}$) si $l \geq k$ (resp. $l < k$). On constate donc que b se décompose en $p-1$ cycles disjoints de longueur p, avec b trivial sur la colonne R_0 et b est un cycle de longueur p sur chaque colonne R_k. Par exemple sur la colonne R_1, b est le cycle $(1, (p-1)p+1, (p-2)p+1, \cdots, p+1)$ (on pourra se reporter à [BMK] pour la décomposition complète de b en cycles dans le cas où $p = 3$).

On considère maintenant un $\mathbb{C}$-espace vectoriel V de dimension p^2 de base $\{e_0, e_1, \cdots, e_{p^2-1}\}$. On définit une action de G sur V par :

$$g(e_s) = e_{\tau_g(s)}$$

pour tout $g \in G$ et $0 \leq s \leq p^2-1$. On note $G_i = G_i(p, D/\mathbb{Q})$ la suite des groupes de ramification de p dans $D/\mathbb{Q}$ et $g_i = |G_i|$ pour tout $i \geq 0$. On sait alors par [Se1] VI.3, corollaire 1, qu'on a :

$$v_p(d_{R_0}) = \sum_{i \geq 0} \frac{g_i}{g_0} \operatorname{codim} V^{G_i} = 2 \operatorname{codim} V^{G_0} + \sum_{i \geq 2} \frac{g_i}{g_0} \operatorname{codim} V^{G_i}$$

On note que $V^{G_i} = V$ si et seulement si G_i est trivial. On peut donc écrire :

Lemme 1.4.7 *$D/\mathbb{Q}$ est faiblement ramifiée si et seulement si l'égalité suivante est vérifiée :*

$$v_p(d_{R_0}) = 2 \operatorname{codim} V^{G_0}$$

On en vient maintenant à la preuve du théorème 1.4.6. On note $R = R_0$, $\wp$ l'idéal premier de $\mathcal{O}_R$ au-dessus de p et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_D$ au-dessus de $\wp$. Compte-tenu de la proposition 1.4.1, il nous suffit de montrer que si $v_p(d_R) \leq 2(p^2-1)$ (resp. < 16) lorsque $p \geq 5$ (resp. $p = 3$), alors l'extension $D/\mathbb{Q}$ est faiblement ramifiée. Nous nous plaçons dorénavant sous cette hypothèse.

Lemme 1.4.8 *$\wp$ est ramifié ou décomposé dans D/R.*

Preuve. Si $\wp$ est inerte dans D/R, alors le groupe de décomposition de $\mathfrak{p}$ dans $D/\mathbb{Q}$ est $G(\mathfrak{p}) = G$ et $G_0(\mathfrak{p})$ est cyclique d'ordre p distingué dans G. Il n'y a qu'un seul tel sous-groupe de G, $< a^p >$, mais $G/< a^p >$ n'est pas cyclique, d'où une contradiction. ∎

On commence par supposer que $\wp$ est ramifié dans D/R. De nouveau on a $G(\mathfrak{p}) = G$; $G_0(\mathfrak{p})$ est cette fois d'ordre p^2. Montrons d'abord que $G_0(\mathfrak{p})$ est cyclique. S'il ne l'est pas, on sait qu'alors :

$$G_0(\mathfrak{p}) =< a^p, b >$$

qui est l'unique sous-groupe de G d'ordre p^2 d'exposant p. On constate que a^p induit un cycle de longueur p dans chaque colonne. Soit $E_k = x_k + x_{p+k} + \ldots + x_{p(p-1)+k}$, alors $V^{<a^p>} = \oplus_{k=0}^{p-1} \mathbb{C}E_k$ et $b(E_k) = E_k$ d'où :

$$V^{G_0} = \bigoplus_{k=0}^{p-1} \mathbb{C}E_k \quad \text{et} \quad v_p(d_R) = 2(p^2-p) + \sum_{i\geq 2} \frac{g_i}{g_0} \operatorname{codim} V^{G_i}$$

On commence par observer que si $G_2 = G_1$ ou $G_2 =< a^p >$, alors $V^{G_2} = V^{G_0}$ et par conséquent $v_p(d_R) \geq 3(p^2-p) > 2(p^2-1)$, ce qui est absurde. Il ne reste à examiner que le cas où G_2 est d'ordre p non distingué, alors $G_2 =< b^k a^{rp} >$ avec $1 \leq k, r \leq p-1$. Or a^{rp} induit une permutation des éléments de chaque colonne et b^k définit un élément d'ordre 1 sur la première colonne et d'ordre p sur les autres. On aurait donc :

$$V^{G_2} = \mathbb{C}e_0 \oplus \mathbb{C}e_p \oplus \cdots \oplus \mathbb{C}e_{(p-1)p} \oplus \mathbb{C}E_1 \oplus \cdots \oplus \mathbb{C}E_{p-1}$$

d'où l'on tire $\operatorname{codim} V^{G_2} = p^2-2p+1$. Soit q le plus petit entier tel que $G_q = G_2$ et $G_{q+1} = 1$. On sait que q est congru à 1 modulo p, donc

$$\sum_{i\geq 2} \frac{g_i}{g_0} \operatorname{codim} V^{G_i} = \frac{q-1}{p} \operatorname{codim} V^{G_2} \geq p^2 - 2p + 1$$

donc $v_p(d_R) \geq 2(p^2-p)+p^2-2p+1 = 3p^2-4p+1$. Or $(3p^2-4p+1)-2(p^2-1) = (p-1)(p-3)$, d'où :

$$v_p(d_R) \begin{cases} > 2(p^2-1) & \text{si } p \geq 5 \\ \geq 16 & \text{si } p = 3 \end{cases}$$

ce qui contredit l'hypothèse sur $v_p(d_R)$.

On sait maintenant que si $\wp$ est ramifié dans D/R, alors $G_0(\mathfrak{p})$ est cyclique. Il contient donc un élément σ d'ordre p^2, qui est un cycle dans S_{p^2}. Il s'ensuit que

$$\{e_0, e_1, \cdots, e_{p^2-1}\} = \{\sigma^s(e_0),\ 0 \leq s \leq p^2-1\}$$

Par conséquent, $V^{G_0} = V^{G_1} = \mathbb{C}(e_0 + e_1 + \ldots + e_{p^2-1})$, donc

$$v_p(d_R) = 2(p^2-1) + \sum_{i\geq 2} \frac{g_i}{g_0} \operatorname{codim} V^{G_i}$$

et l'hypothèse sur $v_p(d_R)$ entraîne l'égalité, donc $D/\mathbb{Q}$ est faiblement ramifiée par le lemme 1.4.7.

On considère maintenant le cas où $\wp$ est décomposé dans D/R. Alors $G(\mathfrak{p})$ est d'ordre p^2 donc soit $G(\mathfrak{p})$ est cyclique, soit $G(\mathfrak{p}) =< a^p, b >$ l'unique sous-groupe non cyclique d'ordre p^2 de G . Dans la deuxième éventualité, soit $M = D^{G(\mathfrak{p})}$. Alors p est décomposé dans $M/\mathbb{Q}$, donc aussi dans $R = D^{<b>}/\mathbb{Q}$, ce qui contredit l'hypothèse du théorème 1.4.6. C'est donc que $G(\mathfrak{p})$ est cyclique. Comme le seul sous-groupe d'ordre p de G inclus dans un sous-groupe cyclique d'ordre p^2 est $< a^p >$, on a $G_0(\mathfrak{p}) =< a^p >$, d'où :

$$V^{G_0} = \mathbb{C}E_0 \oplus \cdots \oplus \mathbb{C}E_{p-1}$$

et donc $\operatorname{codim} V^{G_0} = p^2 - p$. Puisque $v_p(d_R) \leq 2(p^2-1)$ et que $3(p^2-p) > 2(p^2-1)$, on en déduit que $G_2 = \{1\}$. Ceci termine la preuve du théorème 1.4.6.

1.4.3 Un exemple d'application

On illustre le résultat précédent en étudiant un exemple tiré de la thèse de S. Monier-Derviaux ([MD]). On considère le problème de plongement suivant : soit M_1 (resp. M_2) l'extension cubique galoisienne de $\mathbb{Q}$ définie par le polynôme irréductible $x^3 - 21x - 7$ (resp. $x^3 - 39x - 26$) et $M = M_1.M_2$ le compositum. Il s'agit de plonger $M/\mathbb{Q}$ dans une extension galoisienne de $\mathbb{Q}$ de degré 27. On montre que le corps de décomposition D du polynôme suivant vérifie ces conditions :

$$x^9 - 105x^7 - 147x^6 + 3276x^5 + 6279x^4 - 35581x^3 - 63882x^2 + 131313x + 164437$$

et que son groupe de Galois est non abélien d'ordre 27 d'exposant 9. Le discriminant du corps de rupture R est :

$$3^{12} \times 7^8 \times 13^4$$

et les indices de ramification et d'inertie de 3 dans $R/\mathbb{Q}$ sont :

$$e(3, R/\mathbb{Q}) = f(3, R/\mathbb{Q}) = 3$$

Le théorème 1.4.6 montre que $D/\mathbb{Q}$ est faiblement ramifiée.

Pour une étude théorique du problème de plongement d'une extension d'ordre p ou p^2 dans une surextension non abélienne d'ordre p^3, on peut consulter [Gi] ou [MN].

Chapitre 2

Exemples

Les exemples d'extensions faiblement ramifiées apparaissaient jusqu'à présent de façon discrète dans la littérature. Si l'exemple donné dans la proposition 1.2.1 jouait déjà un rôle important dans [Er1] et si [Er2] note que, plus généralement, toutes les extensions galoisiennes de $\mathbb{Q}$ de degré premier impair sont faiblement ramifiées, cet article ne donne, en dehors des extensions modérément ramifiées, qu'un seul exemple qui ne rentre pas dans cette famille : le compositum de $\mathbb{Q}(\sqrt{-3})$ avec $\mathbb{Q}(\sqrt[3]{2})$.

Les extensions faiblement ramifiées sont cependant présentes dans différents contextes. L'étude des extensions diédrales de $\mathbb{Q}$ menée par Martinet dans [M1] montre que celles de degré $2p$ avec p premier supérieur ou égal à 5 sont faiblement ramifiées en p (théorème III.1). On les a déjà vues surgir dans un problème de plongement (exemple 1.4.3) et on verra au chapitre suivant leur importance dans l'arithmétique de la racine carrée de la codifférente. Elles interviennent aussi dans des problèmes liés à la théorie de Galois inverse explicite. C'est ce dernier aspect qui nous intéresse ici.

Les polynômes fournis par les tables du logiciel Magma ([BoCa]) comme équations d'extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois donné engendrent souvent des extensions faiblement ramifiées, car ce sont elles qui minimisent (heuristiquement) le discriminant. On donne dans la partie 2.1 des exemples d'extensions faiblement ramifiées obtenues de cette façon, les unes modérées, les autres non.

Dans la partie 2.2, on présente des exemples de corps locaux faiblement ramifiés. D'une part, des extensions provenant de la table de Magma qui sont faiblement ramifiées (et non décomposées) en une place et très sauvagement ramifiées ailleurs. D'autre part, on construit des polynômes dont les corps de rupture sur $\mathbb{Q}_3$ sont les trois extensions pures de degré 45 prévues par le théorème 1 ; on remarque que cette construction permet d'obtenir facilement des extensions abéliennes faiblement ramifiées de $\mathbb{Q}$.

Dans sa thèse ([Ei1]), Eichenlaub réalise des extensions galoisiennes de $\mathbb{Q}(t)$ de groupe de Galois donné G (avec $G \subset S_n$ et $8 \leq n \leq 11$), où t est une indéterminée. En spécialisant t en des valeurs entières, on obtient une famille

infinie d'extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois G. L'étude de la ramification dans une telle famille permet souvent d'en extraire une sous-famille elle aussi infinie d'extensions faiblement ramifiées. La partie 2.3 est consacrée au cas où $G \simeq C_9 \rtimes C_3$. La même méthode est utilisée dans la partie 2.4 pour construire une famille infinie d'extensions modérées de $\mathbb{Q}$ de groupe de Galois isomorphe à $C_7 \rtimes C_3$.

Beaucoup des exemples d'extensions faiblement ramifiées non abéliennes de degré impair serviront à tester dans le chapitre 5 des propriétés de structure galoisienne et de structure hermitienne pour l'idéal racine carrée de la codifférente (que l'on étudie dans le prochain chapitre).

2.1 Une liste d'exemples globaux

Lorsqu'on cherche des exemples d'extensions faiblement ramifiées données par des polynômes, la première contrainte est que l'extension soit galoisienne. C'est donc le corps de décomposition du polynôme qu'il faut considérer. Cependant, on sait que la plupart des polynômes de degré d ont pour groupe de Galois le groupe S_d de toutes les permutations d'ordre d. On ne peut donc pas chercher au hasard (par exemple parmi des polynômes vérifiant le critère 1.2.5), à moins de se restreindre à des degrés très bas, puisque pour $d = 5$, on a $|S_5| = 120$ et les calculs deviennent impossibles.

Il existe des tables donnant pour chaque groupe transitif G d'un certain degré un polynôme dont le groupe de Galois est G. De plus, les polynômes sont choisis pour minimiser le discriminant de l'extension, ce qui assure la possibilité de conduire des calculs sur ces exemples. On s'intéresse ici aux polynômes de la table fournie par le logiciel Magma ([BoCa]) pour les groupes transitifs de degré d compris entre 2 et 11. Chaque groupe est désigné par un couple de nombres (d, n) où n correspond à la numérotation de [BMK].

On a vu dans la partie 1.4 qu'il est possible pour un groupe donné de déterminer sur le discriminant du corps de rupture si le corps de décomposition est faiblement ramifié. Comme on passe en revue un grand nombre de groupes distincts, on ne peut pas ici utiliser une telle méthode. Par contre, tant que l'ordre du groupe G reste raisonnable (jusqu'à l'ordre 42, tous les groupes ont été testés), on peut calculer un polynôme de degré égal à l'ordre de G et pour lequel l'extension correspondant à G dans la table est corps de rupture. On a alors directement accès au discriminant de l'extension et à la décomposition des premiers ramifiés, ce qui permet (toujours à l'aide de la formule de Hilbert) de déterminer si la ramification est modérée, faible ou "très sauvage".

Une soixantaine de polynômes ont été testés dans la table du logiciel Magma. Parmi eux, on compte 17 extensions faiblement et sauvagement ramifiées de $\mathbb{Q}$ (plus d'un quart !) qui sont présentées dans le prochain paragraphe, 14 extensions modérément ramifiées qui se trouvent dans le suivant et quelques extensions localement faiblement ramifiées qui prennent place dans la partie 2.2.

L'auteur tient à remercier ici Bill Allombert qui lui a indiqué cette source d'extensions faiblement ramifiées et lui a aussi fourni le polynôme de groupe de

Galois $(5,1)$ du prochain paragraphe qui est le seul à ne pas provenir de la table du logiciel Magma.

2.1.1 Extensions faiblement ramifiées

Tous les polynômes qui suivent ont un corps de rupture galoisien faiblement ramifié sur $\mathbb{Q}$. On donne pour chacun le groupe de Galois (nomenclature de [BMK]), le discriminant factorisé de l'extension et le comportement des premiers sauvagement ramifiés.

1. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(2,1)$, de discriminant -2^2.

$$x^2+1$$

2. Le polynôme suivant (qui ne provient pas de la table du logiciel Magma) a un corps de rupture de groupe de Galois isomorphe à $(5,1)$, de discriminant $5^8 11^4$.

$$x^5-80x^4+1460x^3-7960x^2+6480x-1376$$

3. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(6,2)$, de discriminant $-2^4 3^7$. Le degré résiduel en 2 est égal à 2 tandis que 3 est totalement ramifié.

$$x^6-3x^5+5x^3-3x+1$$

4. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,4)$, de discriminant $2^{12}3^6$. 2 ne s'y décompose pas et son degré résiduel est égal à 2.

$$x^8-2x^7+2x^6-2x^5+7x^4-10x^3+8x^2-4x+1$$

5. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(9,2)$, de discriminant $3^{12}7^6$. Le degré résiduel en 3 est égal à 3.

$$x^9-15x^7-4x^6+54x^5+12x^4-38x^3-9x^2+6x+1$$

6. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(4,4)$, de discriminant $2^{18}3^{16}$. 2 ne s'y décompose pas et son degré résiduel est égal à 3 ; 3 se décompose en 4 idéaux premiers.

$$x^{12}-2x^9+18x^8-18x^7+14x^6-30x^5+45x^4-52x^3+42x^2-18x+3$$

7. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(7,2)$, de discriminant -7^{19}. 7 y est totalement ramifié.

$$x^{14}+98x^{10}+343x^8+343x^6+3773x^4-2058x^2+343$$

8. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,6)$, de discriminant $2^{24}7^{14}$. 2 s'y décompose en 2 idéaux premiers, chacun de degré résiduel égal à 2 ; 7 est non décomposé de degré résiduel égal à 2.

$$x^{16} + 2x^{14} - 21x^{12} - 14x^{10} + 217x^8 - 308x^6 + 168x^4 - 40x^2 + 4$$

9. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,9)$, de discriminant $2^{24}3^87^8$. 2 s'y décompose en 2 idéaux premiers, chacun de degré résiduel égal à 2.

$$x^{16} - 4x^{15} + 12x^{14} - 20x^{13} + 29x^{12} - 30x^{11} + 48x^{10} - 66x^9 + 51x^8 \\ -82x^7 + 76x^6 - 60x^5 + 90x^4 - 72x^3 + 48x^2 - 16x + 4$$

10. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(9,4)$, de discriminant $-3^{21}7^{12}$. 3 ne s'y décompose pas et son degré résiduel est égal à 3.

$$x^{18} - 3x^{15} + 115x^{12} + 104x^9 + 511x^6 + 196x^3 + 343$$

11. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(5,3)$, de discriminant $2^{16}5^{23}$. 2 ne s'y décompose pas et son degré résiduel est égal à 4 ; 5 y est totalement ramifié.

$$x^{20} + 2500x^{10} + 50000$$

12. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(10,3)$, de discriminant $2^{20}47^{10}$. 2 s'y décompose en 2 idéaux premiers, chacun de degré résiduel égal à 5.

$$x^{20}-11x^{18}+52x^{16}-139x^{14}+241x^{12}-287x^{10}+241x^8-139x^6+52x^4-11x^2+1$$

13. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(6,6)$, de discriminant $2^{42}3^{32}$. 2 ne s'y décompose pas et son degré résiduel est égal à 3 ; 3 s'y décompose en 4 idéaux premiers, chacun de degré résiduel égal à 2.

$$x^{24} + 24x^{20} + 126x^{16} + 322x^{12} + 453x^8 + 198x^4 + 1$$

14. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,12)$, de discriminant $2^{24}397^{16}$. 2 s'y décompose en 6 idéaux premiers, chacun de degré résiduel égal à 2.

$$x^{24}-85x^{22}+2521x^{20}-38422x^{18}+344506x^{16}-1913170x^{14}+6614773x^{12}-13747729x^{10} \\ +15732421x^8-8410276x^6+1954960x^4-163072x^2+4096$$

15. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,13)$, de discriminant $2^{24}23^{12}31^{16}$. 2 s'y décompose en 6 idéaux premiers, chacun de degré résiduel égal à 2.

$$x^{24}+342x^{22}+49301x^{20}+3912326x^{18}+187678554x^{16}+5650086198x^{14}+108154225181x^{12} \\ +1319599431258x^{10}+10174131603706x^8+48299321756202x^6+133582201676853x^4 \\ +191341955314810x^2+104669084485681$$

16. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(9,6)$ (c'est-à-dire $C_9 \rtimes C_3$), de discriminant $3^{36}73^{24}$. 3 s'y décompose en 3 idéaux premiers, chacun de degré résiduel égal à 3.

$$x^{27}-3x^{26}-120x^{25}+509x^{24}+4722x^{23}-27144x^{22}-61224x^{21}+581982x^{20}-87738x^{19}$$
$$-5555987x^{18}+6703416x^{17}+25769718x^{16}-49229658x^{15}-59710338x^{14}+164739690x^{13}$$
$$+60931548x^{12}-294582501x^{11}-1830519x^{10}+289590417x^{9}-45379521x^{8}-151838064x^{7}$$
$$+33431940x^{6}+39296016x^{5}-9058554x^{4}-4214349x^{3}+866052x^{2}+137781x-19683$$

17. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,20)$, de discriminant $2^{48}17^{24}$. 2 s'y décompose en 4 idéaux premiers, chacun de degré résiduel égal à 2 ; 17 se décompose en 8 idéaux premiers, chacun de degré résiduel égal à 1.

$$x^{32}-2x^{30}+15x^{28}+58x^{26}+697x^{24}+196x^{22}+702x^{20}-112x^{18}+2074x^{16}-112x^{14}$$
$$+702x^{12}+196x^{10}+697x^{8}+58x^{6}+15x^{4}-2x^{2}+1$$

18. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(7,4)$, de discriminant $-2^{36}7^{47}$. 2 s'y décompose en 2 idéaux premiers, chacun de degré résiduel égal à 3 (2 est modérément ramifié) ; 7 est totalement ramifié.

$$x^{42} + 48020x^{28} + 96001584x^{14} + 52706752$$

2.1.2 Extensions modérées

Tous les polynômes qui suivent ont un corps de rupture galoisien modérément ramifié sur $\mathbb{Q}$. On donne pour chacun le groupe de Galois (nomenclature de [BMK]), le discriminant factorisé de l'extension et le comportement des premiers ramifiés.

1. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(3,1)$, de discriminant 7^2.

$$x^3 + x^2 - 2x - 1$$

2. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(4,1)$, de discriminant 5^3 ; 5 y est totalement ramifié.

$$x^4 + x^3 + x^2 + x + 1$$

3. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(5,1)$, de discriminant 11^4.

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$

4. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(6,1)$, de discriminant -7^5 ; 7 y est totalement ramifié.

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

5. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(7,1)$, de discriminant 29^6.

$$x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$$

6. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,1)$, de discriminant 17^7 ; 17 y est totalement ramifié.

$$x^8 - 17x^6 + 68x^4 - 85x^2 + 17$$

7. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(8,2)$, de discriminant $5^4 17^6$. Le degré résiduel est 4 en 5 et 2 en 17 ; le degré de ramification en 17 est 4.

$$x^8 - x^7 - 19x^6 - 2x^5 + 46x^4 - 2x^3 - 19x^2 - x + 1$$

8. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(10,1)$, de discriminant -11^9 ; 11 y est totalement ramifié.

$$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

9. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(11,1)$, de discriminant 23^{10}.

$$x^{11}+x^{10}-10x^9-9x^8+36x^7+28x^6-56x^5-35x^4+35x^3+15x^2-6x-1$$

10. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(11,2)$, de discriminant -167^{11} ; 167 s'y décompose en 11 idéaux premiers.

$$x^{22} + 24x^{20} + 250x^{18} + 1464x^{16} + 5189x^{14} + 11253x^{12} + 15224x^{10} \\ +14538x^8 + 9602x^6 + 4600x^4 + 1337x^2 + 167$$

11. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(6,7)$, de discriminant 229^{12} ; 229 s'y décompose en 6 idéaux premiers, chacun de degré résiduel égal à 2.

$$x^{24}-80x^{20}+340x^{18}+7520x^{16}+23120x^{14}-973378x^{12}-462400x^{10}+50899280x^8 \\ +74190340x^6+67773664x^4+2114616240x^2+266962921$$

12. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(6,8)$, de discriminant 229^{12} ; 229 s'y décompose en 6 idéaux premiers, chacun de degré résiduel égal à 2.

$$x^{24}+12x^{23}+114x^{22}+748x^{21}+4057x^{20}+17932x^{19}+68274x^{18}+223788x^{17}+660446x^{16} \\ +1757564x^{15}+4534274x^{14}+11185948x^{13}+27788031x^{12}+64634552x^{11}+140677848x^{10} \\ +268118788x^9+527507906x^8+950649552x^7+2089102884x^6+3628184976x^5+8367636821x^4 \\ +11478945892x^3+21189734384x^2+15943995288x+5607107728$$

13. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(9,7)$ (c'est-à-dire $(C_3 \times C_3) \rtimes C_3$), de discriminant $7^{18}13^{18}43^{18}$. Les indices de ramification et degrés résiduels sont respectivement 3 et 1 en 7, 3 et 3 en 13 et en 43.

$$x^{27}-853x^{25}+1677x^{24}+300981x^{23}-1096758x^{22}-56977801x^{21}+292628115x^{20}$$
$$+6262298949x^{19}-41388105096x^{18}-401368678145x^{17}+3378112766301x^{16}$$
$$+13896190603229x^{15}-162481805891262x^{14}-178578895495435x^{13}+4529497506622959x^{12}$$
$$-2989340523410765x^{11}-69693749268510822x^{10}+124612551331390513x^{9}$$
$$+527907780509368077x^{8}-1403175114327466233x^{7}-1522558748101069692x^{6}$$
$$+5706545152536212569x^{5}+1997685375401190423x^{4}-1005224003758175548 1x^{3}$$
$$-2565262903158932886x^{2}+676947847659058 9305x+3066016863824092269$$

14. Le polynôme suivant a un corps de rupture de groupe de Galois isomorphe à $(9,8)$, de discriminant $2^{24}5^{18}7^{18}11^{18}$. Les indices de ramification et degrés résiduels sont respectivement 3 et 2 en 2, 2 et 3 en 5 et en 11, 2 et 2 en 7.

$$x^{36}-8x^{34}+40x^{32}-179x^{30}+340x^{28}+520x^{26}-2941x^{24}-1224x^{22}+37148x^{20}$$
$$-120885x^{18}+211956x^{16}-74092x^{14}-332840x^{12}+588160x^{10}$$
$$-586384x^{8}+337968x^{6}-49536x^{4}+19456x^{2}+256$$

2.2 Exemples locaux

Deux paragraphes dans cette partie : dans le premier, on présente les extensions localement faiblement ramifiées trouvées dans la table du logiciel Magma ; dans le second, en guise d'application du théorème 1, on se propose de déterminer des équations des 3 extensions pures de $\mathbb{Q}_3$ de degré 45.

2.2.1 Quelques extensions localement faiblement ramifiées

Quelques unes des extensions produites par les polynômes de la table du logiciel Magma sont faiblement ramifiées en une place et "très sauvagement" (c'est-à-dire non faiblement) ramifiées en une autre. Lorsque le premier p qui est faiblement ramifié ne se décompose pas dans le corps de rupture du polynôme sur $\mathbb{Q}$, on sait que l'extension complétée en p a le même groupe de Galois que celle dont on est parti. On obtient donc des extensions locales faiblement ramifiées de groupe de Galois connu. Voici les trois qui sont apparues.

1. Le polynôme suivant a un corps de rupture galoisien sur $\mathbb{Q}_5$ de groupe de Galois isomorphe à $(10,2)$, de discriminant 5^{13} ; 5 y est totalement ramifié.

$$x^{10} - 35x^6 + 130x^4 + 160$$

2. Le polynôme suivant a un corps de rupture galoisien sur $\mathbb{Q}_3$ de groupe de Galois isomorphe à $(9,9)$, de discriminant 3^{50} ; le degré résiduel est 2 et

l'indice de ramification est 18.

$$x^{36}+12x^{34}-144x^{32}-5040x^{30}-61290x^{28}-220968x^{26}+9627444x^{24}+148891392x^{22}$$
$$+622214865x^{20}-323381700x^{18}-4405276044x^{16}+20225527632x^{14}+108505417536x^{12}$$
$$-737226774720x^{10}+1790972907840x^{8}-2437435411200x^{6}$$
$$+1387815379200x^{4}+141647616000x^{2}+1492992000$$

3. Le polynôme suivant a un corps de rupture galoisien sur $\mathbb{Q}_5$ de groupe de Galois isomorphe à $(10, 5)$, de discriminant 5^{46} ; le degré résiduel est 2 et l'indice de ramification est 20.

$$x^{40}+70392x^{30}+5660441624x^{20}-6771345011232x^{10}+13114052591692816$$

2.2.2 Extensions pures de $\mathbb{Q}_3$ de degré 45

Par le théorème 1, on sait qu'il existe trois extensions abéliennes faiblement et sauvagement ramifiées de $\mathbb{Q}_3$ de degré 45. Le but de ce paragraphe est d'en donner des équations, c'est-à-dire de trouver des polynômes dont elles soient le corps de rupture sur $\mathbb{Q}_3$.

Puisque $v_3(45) = 2$, on sait par le corollaire 1.3.5 que l'une d'elles est décomposée tandis que les deux autres sont cycliques. On considère la sous-extension $L/\mathbb{Q}$ de $\mathbb{Q}[9]/\mathbb{Q}$ de degré 3 sur $\mathbb{Q}$. On sait que :

$$L = \mathbb{Q}(\zeta + \zeta^{-1})$$

où ζ est une racine primitive 9-ième de l'unité. Le polynôme minimal de $\zeta+\zeta^{-1}$ est $x^3 - 6x^2 + 9x - 1$; une équation réduite de L est $x^3 - 3x - 1$. Enfin, $L/\mathbb{Q}$ est totalement et faiblement ramifiée en 3 et l'extension locale correspondante $L'/\mathbb{Q}_3$ a la même équation.

Pour obtenir l'extension décomposée $N_0 = L'.\mathbb{Q}_3\{15\}$, on cherche d'abord une équation de l'extension non ramifiée $\mathbb{Q}_3\{15\}/\mathbb{Q}_3$. Pour cela, on construit deux extensions linéairement disjointes de $\mathbb{Q}$ de degrés respectifs 3 et 5 dans lesquelles 3 est inerte. Par exemple, soit $M_3/\mathbb{Q}$ la sous-extension de $\mathbb{Q}[19]/\mathbb{Q}$ de degré 3 sur $\mathbb{Q}$, d'équation $x^3 - x^2 - 6x + 7$; soit $M_5/\mathbb{Q}$ la sous-extension de $\mathbb{Q}[25]/\mathbb{Q}$ de degré 5 sur $\mathbb{Q}$, d'équation $x^5 - 10x^3 - 5x^2 + 10x - 1$. Puis soit $M_{15} = M_3.M_5$ le compositum. C'est une extension galoisienne de $\mathbb{Q}$ de groupe de Galois isomorphe à $C_3 \times C_5$; grâce au système PARI ([3BCO]), on calcule son équation :

$$x^{15} - 5x^{14} - 50x^{13} + 260x^{12} + 745x^{11} - 4439x^{10} - 2980x^{9} + 29685x^{8} - 4955x^{7}$$
$$-81705x^{6} + 43089x^{5} + 82545x^{4} - 55625x^{3} - 17710x^{2} + 9800x + 2401$$

Comme 3 est inerte dans $M_{15}/\mathbb{Q}$, c'est aussi une équation de l'extension complétée $M'_{15}/\mathbb{Q}_3$. Celle-ci est non ramifiée de degré 15, donc égale à $\mathbb{Q}_3\{15\}$. Enfin, PARI permet de calculer une équation du compositum $L.M_{15}/\mathbb{Q}$ et, puisque 3 est non décomposé dans $L.M_{15}/\mathbb{Q}$, elle est aussi valable pour l'extension complétée

$L'.\mathbb{Q}_3\{15\}/\mathbb{Q}_3$:

$$x^{45}+15x^{44}-120x^{43}-2815x^{42}+1620x^{41}+224802x^{40}+479025x^{39}-10026810x^{38}-38644770x^{37}$$
$$+273065985x^{36}+1515726891x^{35}-4544322840x^{34}-37160907985x^{33}+39081136125x^{32}$$
$$+616991075820x^{31}+68664306270x^{30}-7172389157550x^{29}-6629386884960x^{28}+58976389802730x^{27}$$
$$+93805841326500x^{26}-340128898957200x^{25}-768972822546450x^{24}+1328437994070570x^{23}$$
$$+4196052351689820x^{22}-3166557771443045x^{21}-1583025272391572 7x^{20}+2680502879807820x^{19}$$
$$+41572978332109705x^{18}+9060689872804200x^{17}-75284975052067710x^{16}-37204622615578640x^{15}$$
$$+91850467669425045x^{14}+65190461721018660x^{13}-72324203726438210x^{12}-65455387762851915x^{11}$$
$$+33779488940503884x^{10}+3849607853635545 0x^{9}-7541943432223485x^{8}-12353528043171330x^{7}$$
$$+84023864753945x^{6}+1773369307201098x^{5}+190403503959255x^{4}-61926305785145x^{3}$$
$$-10985504592630x^{2}-478636802235x-2756065357$$

Le corps de rupture de ce polynôme sur $\mathbb{Q}$ est une extension faiblement ramifiée de discriminant $3^{60}5^{72}19^{30}$. Le degré résiduel est égal à 15 en 3, 3 en 5 et 5 en 19. L'indice de ramification est égal à 5 en 5 et 3 en 19.

Remarque 2.2.1 On peut obtenir une autre équation de $L'.\mathbb{Q}_3\{15\}/\mathbb{Q}_3$ en utilisant par exemple la sous-extension de degré 3 de $\mathbb{Q}[7]$ au lieu de celle de $\mathbb{Q}[19]$. On arrive au polynôme suivant :

$$x^{45}-15x^{44}-60x^{43}+1885x^{42}-2040x^{41}-101202x^{40}+311765x^{39}+3047850x^{38}-13836810x^{37}$$
$$-56233935x^{36}+350120073x^{35}+633104670x^{34}-5830674825x^{33}-3562534725x^{32}+67900516830x^{31}$$
$$-8811832866x^{30}-570012099810x^{29}+363551152530x^{28}+3500084604520x^{27}-3561821285760x^{26}$$
$$-15780909231030x^{25}+20967413543760x^{24}+51969072704640x^{23}-83875969742220x^{22}$$
$$-123098477735735x^{21}+236202785911401x^{20}+205185361938 90x^{19}-471698438724575x^{18}$$
$$-221119359949170x^{17}+663554122709700x^{16}+134651527867418x^{15}-646921459066665x^{14}$$
$$-12466362862410x^{13}+426379899760640x^{12}-46180133146155x^{11}-183349948835292x^{10}$$
$$+36095195866890x^{9}+48658228800645x^{8}-12548836318980x^{7}-7224049427545x^{6}+2159798482104x^{5}$$
$$+489407749485x^{4}-159595022545x^{3}-7987967970x^{2}+2965525035x-76831343$$

On obtient, en prenant le corps de rupture de ce polynôme sur $\mathbb{Q}$, une autre extension faiblement ramifiée de $\mathbb{Q}$ de degré 45, de discriminant $3^{60}5^{72}7^{30}$. Le degré résiduel est égal à 15 en 3, 9 en 5, 3 en 7 ; 7 se décompose en 5 idéaux premiers.

La détermination des deux autres extensions pures de $\mathbb{Q}_3$ de degré 45 demande plus de moyens de calcul : il faut en effet d'abord trouver une équation de l'extension $L'.\mathbb{Q}_3\{45\}/\mathbb{Q}_3$ (de degré 135 !), puis déterminer ses sous-extensions de degré 45 et reconnaître parmi elles celle qui est non ramifiée. Heureusement, le fait que toutes les extensions considérées soient abéliennes permet d'utiliser (malgré le degré élevé) des algorithmes puissants développés pour PARI par Bill Allombert ([A]).

On reprend $M_5/\mathbb{Q}$, la sous-extension de $\mathbb{Q}[25]/\mathbb{Q}$ de degré 5 sur $\mathbb{Q}$, d'équation $x^5-10x^3-5x^2+10x-1$ et on la compose avec M_9, sous-corps totalement réel maximal de $\mathbb{Q}(\zeta_{19})$ d'équation $x^9-x^8-8x^7+7x^6+21x^5-15x^4-20x^3+10x^2+5x-1$, dans lequel 3 est inerte. On obtient ainsi $M_{45}=M_5.M_9$, puis $L.M_{45}$,

dont on ne reproduira pas ici l'équation car cela prendrait trop de place. La fonction `galoisfixedfield` de PARI permet alors de déterminer les équations des quatre sous-extensions de $L'.\mathbb{Q}_3\{45\}$ de degré 45. Les équations des deux extensions pures cycliques de $\mathbb{Q}_3$ de degré 45 sont :

$$x^{45}-1140x^{43}-570x^{42}+526680x^{41}+155610x^{40}-133869250x^{39}+17592480x^{38}+21115608390x^{37}$$
$$-11864179405x^{36}-2200181238792x^{35}+1960239124275x^{34}+157411972688675x^{33}-169263607145220x^{32}$$
$$-7948759855306560x^{31}+8816467209951892x^{30}+2891215736428889375x^{29}-291406710438698130x^{28}$$
$$-7677256055536067295x^{27}+613355579366540544 0x^{26}+149626107904526776515x^{25}$$
$$-773554758612102604 75x^{24}-213181015171918576338 0x^{23}+427834616477205988 55x^{22}$$
$$+218831517540405226100 10x^{21}+243160536198048123912 3x^{20}-157700225230320713166375x^{19}$$
$$-602287870040532807906 65x^{18}+769046481002233454319315x^{17}+444643206204303979387695x^{16}$$
$$-243208318180345467389689 2x^{15}-162923144627474225946022 5x^{14}$$
$$+481230274796092011109999 5x^{13}+307055556447136501291156 5x^{12}$$
$$-580145386197110363607127 5x^{11}-286493612530565887395469 5x^{10}+397524915245449522138967 5x^{9}$$
$$+119082485740584262408020 0x^{8}-129989682227004869723791 5x^{7}-227712482117785595974680x^{6}$$
$$+186450263040417098362398x^{5}+128399699888072641170 00x^{4}-116572904473647682085 10x^{3}$$
$$+260465420559722732055x^{2}+243693094985125434630x-19362616980998436001$$

et :

$$x^{45}-1140x^{43}-570x^{42}+526680x^{41}+417240x^{40}-131347000x^{39}-122087160x^{38}+19868967090x^{37}$$
$$+18135332135x^{36}-1940559464502x^{35}-1471259480025x^{34}+126818384130365x^{33}+62765721798570x^{32}$$
$$-5649749136567330x^{31}-915395219853098x^{30}+172465628833790325x^{29}-33783110524141380x^{28}$$
$$-3582381608820868845x^{27}+191135098395785637 0x^{26}+497163354518673076 35x^{25}$$
$$-4026860308727775557 5x^{24}-4486054140283359335 40x^{23}+4441494541192050689 55x^{22}$$
$$+2560478171391261040080x^{21}-2688521643876399268401x^{20}-9149190812981077026075x^{19}$$
$$+9193416277173366824185x^{18}+2019149886023695997023 5x^{17}-1797951801178806947095 5x^{16}$$
$$-2679404683259118287515 2x^{15}+2013912667344995492287 5x^{14}+2087931298828809764029 5x^{13}$$
$$-1269325585497117333103 5x^{12}-9521941748982410772225x^{11}+4248949054798661621001x^{10}$$
$$+260544839190493941017 5x^{9}-6827097775344848980 20x^{8}-4258551071847318703 65x^{7}$$
$$+35996001909940678320x^{6}+3690931736339369793 0x^{5}+2105849347962831900x^{4}$$
$$-1147180002277723890x^{3}-197138679381767835x^{2}-10441368400362750x-171702502583743$$

Les corps de rupture sur $\mathbb{Q}$ de ces deux polynômes sont des extensions faiblement ramifiées de discriminant $3^{60}5^{72}19^{40}$. Le degré résiduel est égal à 15 en 3, à 9 en 5 et à 5 en 19, l'indice de ramification en 19 égal à 9. Elles ne sont pas isomorphes : le degré résiduel en 11 est égal à 5 dans la première et à 15 dans la seconde.

On trouve aussi une autre équation de $L.M_{15}$ et donc de l'extension pure

décomposée $L'.\mathbb{Q}_3\{15\}/\mathbb{Q}_3$:

$$x^{45}-780x^{43}-30x^{42}+254520x^{41}-2610x^{40}-45862075x^{39}+4161060x^{38}+5075885430x^{37}-864277480x^{36}$$
$$-363877048179x^{35}+83786128350x^{34}+17397855391820x^{33}-4488584557500x^{32}-563892412167195x^{31}$$
$$+139810215715708x^{30}+12497709572802000x^{29}-2552409534466980x^{28}-190195245644778210x^{27}$$
$$+26356049724071070x^{26}+1989143653106337645x^{25}-127971548485900825x^{24}$$
$$-14245220616013492920x^{23}-1165201648855534480x^{22}+691927394653992365585x^{21}$$
$$+5063431791600121806x^{20}-2241655789670811253 50x^{19}-28758159403316124035x^{18}$$
$$+472630409464536056038 5x^{17}+816312927971348622 90x^{16}-627384440230568111328x^{15}$$
$$-128881698558138837675x^{14}+501757090353549150750x^{13}+110358010059963132390x^{12}$$
$$-230223879665565480135x^{11}-468555984378705532 89x^{10}+598994206947870569 50x^{9}$$
$$+960179295798152640 0x^{8}-862485283772903920 5x^{7}-858942781042043880x^{6}$$
$$+636126226586967942x^{5}+213724798665698 25x^{4}-192919861007538 00x^{3}$$
$$+392400492148350x^{2}+122080153112820x-4747561509943$$

Enfin, on donne l'équation de la sous-extension non ramifiée (en 3) de $L.M_{45}$:

$$x^{45}-170x^{43}+20x^{42}+12490x^{41}-2584x^{40}-524275x^{39}+140520x^{38}+14015335x^{37}-4243420x^{36}$$
$$-252023613x^{35}+78997500x^{34}+3141774650x^{33}-952132340x^{32}-27602491285x^{31}+7595347288x^{30}$$
$$+172181168600x^{29}-40208930820x^{28}-763163288745x^{27}+138637230220x^{26}+2392251539231x^{25}$$
$$-294420145625x^{24}-5250650187985x^{23}+324514703370x^{22}+7936713727340x^{21}-20865342890x^{20}$$
$$-8052264417950x^{19}-393223041345x^{18}+5278285316375x^{17}+451774870355x^{16}$$
$$-2122427470590x^{15}-210325970400x^{14}+494601580310x^{13}+41803454040x^{12}$$
$$-64201575055x^{11}-3693992215x^{10}+4371801300x^{9}+189884045x^{8}-155351895x^{7}$$
$$-6088320x^{6}+2769605x^{5}+107250x^{4}-21650x^{3}-775x^{2}+50x+1$$

Le corps de rupture de ce polynôme sur $\mathbb{Q}$ est une extension faiblement ramifiée. En effet, son discriminant est $5^{72}19^{40}$ et le degré résiduel en 5 est égal à 9.

Remarque 2.2.2 La méthode de construction utilisée dans ce paragraphe, qui consiste à composer des extensions de $\mathbb{Q}$ linéairement disjointes où 3 est inerte ou ramifié, permet d'obtenir des extensions abéliennes faiblement ramifiées de $\mathbb{Q}$ de tout degré, avec éventuellement des contraintes sur les premiers qui sont ramifiés. Par exemple, en prenant pour M_5 la sous-extension de degré 5 de $\mathbb{Q}[11]$, 5 n'aurait pas été ramifié dans les extensions finales.

2.3 Une famille infinie d'extensions

Dans cette partie, on s'attache à décrire une famille infinie d'extensions galoisiennes faiblement ramifiées de $\mathbb{Q}$ de groupe de Galois G isomorphe à $C_9 \rtimes C_3$. Cette famille est obtenue par spécialisation en des valeurs adéquates d'une indéterminée t pour laquelle on connaît une extension de $\mathbb{Q}(t)$ de groupe de Galois isomorphe à $C_9 \rtimes C_3$. Celle-ci est construite en utilisant des résultats contenus dans [Ei1] ; pour le lecteur intéressé ne disposant pas de ce document, [Ei2] présente une approche plus théorique du même problème.

On précise maintenant les éléments de cette construction qui seront utiles pour la suite. On note $K = \mathbb{Q}(\zeta_9)$ le corps de nombres obtenu en adjoignant à

$\mathbb{Q}$ la racine primitive 9-ième de l'unité ζ_9 et on pose $j = {\zeta_9}^3$. Soit t un entier, on considère :

$$\alpha = (t+j)^8(t+j^2) \ \in \ \mathbb{Q}(j)$$

Alors, pour une infinité de spécialisations de t en des valeurs entières (on convient de les appeler de *bonnes valeurs*), l'extension $K(\sqrt[9]{\alpha})/\mathbb{Q}$ est galoisienne de groupe de Galois $\mathcal{G}$ isomorphe à $C_9 \rtimes C_6$. De plus, $\mathcal{G}$ contient un unique 2-Sylow H, si bien que la sous-extension D de $K(\sqrt[9]{\alpha})$ fixée par H est galoisienne sur $\mathbb{Q}$ de groupe de Galois G isomorphe à $C_9 \rtimes C_3$. Enfin, on détermine un polynôme paramétré par t pour lequel D est corps de rupture. On pose $w = t^2 - t + 1$, il s'agit de :

$$\begin{aligned} P_t(x) = \quad & x^9 - 9wx^7 + 27w^2x^5 - 30w^3x^3 + 9w^4x \\ & -(2t-1)(t^6 - 3t^5 - 12t^4 + 29t^3 - 3t^2 - 12t + 1)w \end{aligned}$$

Remarque 2.3.1 Dans l'annexe 4 de [Ei1], Eichenlaub donne des polynômes réalisant tous les groupes de Galois possibles en degrés 9 à 11. Son polynôme $P_6(x,t)$ de degré 9 (correspondant au groupe $T_6 \simeq C_9 \rtimes C_3$ dans la nomenclature de [BMK]) donne lorsqu'on le spécialise en un entier n impair une extension isomorphe à celle obtenue en spécialisant $P_t(x)$ en $(n+1)/2$.

Le calcul sur ordinateur pour un grand nombre de valeurs du paramètre semble indiquer que le comportement de 3 dans $D/\mathbb{Q}$ est déterminé par la congruence de t modulo 9. De plus, l'utilisation du critère de ramification faible donné dans la proposition 1.4.1 permet de prédire quand l'extension est faiblement ramifiée. Le principal résultat de cette partie est le suivant.

Théorème 2 *On considère la famille $\mathcal{F}$ des extensions D qui sont corps de décomposition sur $\mathbb{Q}$ du polynôme P_t spécialisé en une bonne valeur t avec t congru à 5 modulo 9. Alors :*

(i) $\mathcal{F}$ est constituée d'une infinité d'extensions de $\mathbb{Q}$.

(ii) Chacune des extensions $D \in \mathcal{F}$ est faiblement ramifiée sur $\mathbb{Q}$.

(iii) Soit $D \in \mathcal{F}$ correspondant à $t = 5+9u$. On note e l'indice de ramification, f le degré résiduel et g le degré de décomposition en 3 dans $D/\mathbb{Q}$. Si $u \equiv 0$ ou 2 mod 3, alors $e = 9$ et $f = 3$. Si $u \equiv 1$ mod 3, alors $e = f = g = 3$ ou $e = 3$ et $g = 9$.

La preuve de ce théorème se fait en plusieurs morceaux. (*i*) est prouvé dans la partie 2.3.1 à partir d'une version raffinée (due à Fried) du théorème d'irréductibilité de Hilbert. Le plus gros du travail concerne les points (*ii*) et (*iii*). On commence par l'étude du comportement de l'idéal $\wp$ de K au-dessus de 3 dans l'extension $K(\sqrt[3]{\alpha})/K$ (partie 2.3.2), à l'aide d'un critère dû à Hecke pour les extensions kummériennes de degré premier. On utilise ensuite un critère local dû à Greither pour déterminer si $\wp$ est ramifié ou non dans $K(\sqrt[9]{\alpha})/K$ (partie 2.3.3). On déduit alors facilement (*iii*) des corollaires 2.3.11 et 2.3.17. Fort de ces résultats, on prouve le point (*ii*) dans la partie 2.3.4 en utilisant la formule

de la différente de Hilbert pour relier la valuation en 3 du discriminant de $D/\mathbb{Q}$ et la suite des groupes de ramification $G_i(3, D/\mathbb{Q})$.

On applique ensuite (partie 2.3.5) aux extensions faiblement ramifiées de cette famille les résultats de la partie 1.4. Grâce à une étude détaillée du comportement de 3 dans $R/\mathbb{Q}$ et dans $D/\mathbb{Q}$, on fait le lien entre la valuation v en 3 du discriminant du corps de rupture et l'ordre du groupe d'inertie en 3 dans $D/\mathbb{Q}$. On montre (proposition 2.3.22) que les seules valeurs possibles de v sont 8 et 12, ainsi que les calculs pour un grand nombre de valeurs du paramètre le laissaient prévoir.

2.3.1 Le théorème d'irréductibilité de Hilbert

Cette partie est consacrée à la preuve du point (i) du théorème 2. Pour cela, on a besoin de résultats de théorie de Galois inverse. Le premier d'entre eux est le théorème d'irréductibilité de Hilbert qui stipule que le corps $\mathbb{Q}$ est hilbertien. Cela signifie que, si $f(x,t)$ est un polynôme irréductible en deux variables x et t sur $\mathbb{Q}$, de degré au moins égal à 1, il existe une infinité de $b \in \mathbb{Q}$ tels que le polynôme spécialisé $f(x,b)$ soit irréductible (voir [Vö], corollaire 1.8, pour d'autres caractérisations). Ceci entraîne (par la proposition 1.7 de *loc. cit.*) qu'il existe une infinité de $b \in \mathbb{Q}$ tels que les groupes de Galois de $\mathbb{Q}[x,t]/(f(x,t))$ sur $\mathbb{Q}(t)$ et de $\mathbb{Q}[x]/(f(x,b))$ sur $\mathbb{Q}$ soient isomorphes.

Dans la situation considérée ici, on prend $f(x,t) = P_t(x)$. On sait par le théorème 1 de [Ei1], partie 3.4.2, que le groupe de Galois G de $\mathbb{Q}[x,t]/(P_t(x))$ sur $\mathbb{Q}(t)$ est isomorphe à $C_9 \rtimes C_3$ et on en déduit qu'il existe une infinité d'entiers n pour lesquels le groupe de Galois du polynôme P_t spécialisé en $t = n$ est égal à G. On appelle *bonnes valeurs* celles qui satisfont cette condition. Le résultat suivant (exprimé en termes plus généraux dans [Fri]) est un raffinement du théorème d'irréductibilité de Hilbert qui permet d'en préciser la proportion. Pour N entier positif, on note $\nu(N)$ le nombre de valeurs du paramètre t comprises entre 0 et N qui ne sont pas bonnes.

Proposition 2.3.2 (Fried) *Il existe une constante $c > 0$ telle que, pour tout N entier positif, $\nu(N) < c\sqrt{N}$.*

On en déduit aussitôt :

Corollaire 2.3.3 *L'ensemble des valeurs de t congrues à 5 modulo 9 telles que le corps de décomposition D sur $\mathbb{Q}$ du polynôme P_t est de groupe de Galois isomorphe à $C_9 \rtimes C_3$ est infini.*

Preuve. On suppose qu'il n'y a qu'un nombre fini M de bonnes valeurs de t congrues à 5 modulo 9. Alors, pour tout N,

$$\nu(N) \geq \frac{N - M}{9} \;=\; \mathrm{O}(N)$$

quand N tend vers l'infini, ce qui contredit la proposition précédente. ∎

On a montré le point (i) du théorème 2.

2.3.2 Comportement de $\wp$ dans l'extension $K(\sqrt[3]{\alpha})/K$

On rappelle que K désigne $\mathbb{Q}(\zeta_9)$ et $\wp$ l'idéal premier de K au-dessus de 3. Dans cette partie, on étudie le comportement de $\wp$ dans l'extension kummérienne $K(\sqrt[3]{\alpha})/K$, où $\alpha = (t+j)^8(t+j^2)$ avec $j = {\zeta_9}^3$ et t est un entier congru à 5 modulo 9 qui est une bonne valeur. On note u l'entier tel que :

$$t = 5 + 9u$$

En premier lieu, on remarque que

$$\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha) = (t^2 - t + 1)^9 = 3^9.(27u^2 + 27u + 7)^9$$

Puisque $27u^2 + 27u + 7$ n'est jamais divisible par 3, il s'ensuit que la valuation de α en l'idéal $(1-j)$ de $\mathbb{Q}(j)$ au-dessus de 3 est :

$$v_{(1-j)}(\alpha) = v_3(\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha)) = 9$$

c'est-à-dire qu'on peut écrire $\alpha = \alpha'(1-j)^9$ avec $\alpha' \in \mathbb{Z}[j]$ et $v_{(1-j)}(\alpha') = 0$. De plus, il est clair que α et α' engendrent les mêmes extensions kummériennes sur K. On note désormais

$$\alpha = \frac{(t+j)^8(t+j^2)}{(1-j)^9}$$

alors $\alpha \notin \wp$. Par ailleurs, $(1-j)\mathcal{O}_K = \wp^3$ et le théorème 119 de Hecke ([He], V, 39) se traduit par :

Proposition 2.3.4 *Pour $\xi \in K$, on considère les congruences :*

$$(i)\ \alpha \equiv \xi^3 \bmod \wp^9 \quad \textit{et} \quad (ii)\ \alpha \equiv \xi^3 \bmod \wp^{10}$$

Alors, dans $K(\sqrt[3]{\alpha})/K$, $\wp$ est ramifié si (i) n'a pas de solution ; $\wp$ est inerte si (i) a des solutions et si (ii) n'en a pas ; $\wp$ est décomposé si (ii) a des solutions.

On commence par déterminer si 1 est solution des équations ci-dessus. Pour cela, on calcule la valuation en $\wp$ de $\alpha - 1$.

Lemme 2.3.5

$$v_\wp(\alpha - 1) = \begin{cases} 9 & \textit{si} \quad u \equiv 0 \textit{ ou } 2 \bmod 3 \\ 15 & \textit{si} \quad u \equiv 1 \textit{ ou } 7 \bmod 9 \\ 18 & \textit{si} \quad u \equiv 4 \bmod 9 \end{cases}$$

Preuve. Comme $\alpha - 1 \in \mathbb{Q}(j)$, on sait que

$$v_\wp(\alpha - 1) = 3.v_3(\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha - 1))$$

Un calcul avec PARI ([3BCO]) montre que

$$\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha - 1) = 3^3.Q_1(u)$$

avec $Q_1(u) \equiv u^2+u+1 \bmod 3$. Il s'ensuit que si $u \equiv 0$ ou $2 \bmod 3$, $v_3(\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha-1)) = 3$. Si $u \equiv 1 \bmod 3$, on écrit $u = 1+3v$ et on trouve

$$\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha-1) = 3^5.Q_2(v)$$

avec $Q_2(v) \equiv v^2+v+1 \bmod 3$. Là encore, on en tire que pour $v \equiv 0$ ou $2 \bmod 3$, c'est-à-dire $u \equiv 1$ ou $7 \bmod 9$, $v_3(\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha-1)) = 5$. Et si $v \equiv 1 \bmod 3$, on écrit $v = 1+3w$ et on trouve

$$\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha-1) = 3^6.Q_3(w)$$

avec $Q_3(w) \equiv 1 \bmod 3$. Donc, pour $v \equiv 1 \bmod 3$, c'est-à-dire $u \equiv 4 \bmod 9$, $v_3(\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha-1)) = 6$. ▮

En appliquant la proposition 2.3.4, on en déduit :

Corollaire 2.3.6 *Si $u \equiv 1 \bmod 3$, $\wp$ se décompose dans $K(\sqrt[3]{\alpha})/K$.*

On étudie maintenant le cas où $v_\wp(\alpha-1) = 9$.

Proposition 2.3.7 *Si $u \equiv 0$ ou $2 \bmod 3$, $\wp$ est inerte dans $K(\sqrt[3]{\alpha})/K$.*

Preuve. On note $K_\wp$ le complété de K en $\wp$, $\mathcal{O}_{K_\wp}$ son anneau d'entiers et $\mathcal{U}_{K_\wp} = \mathcal{O}_{K_\wp}^*$ son groupe d'unités. On commence par montrer :

Lemme 2.3.8 *Si $\xi \in \mathcal{U}_K$ est solution de (ii) : $\alpha \equiv \xi^3 \bmod \wp^{10}$, alors il existe $y \in \mathcal{U}_{K_\wp}$ avec $v_\wp(y) = 3$ tel que (iii) : $\alpha - 1 \equiv 3y + y^3 \bmod \wp^{10}$.*

Preuve. Puisque $\alpha \in \mathcal{O}_K \setminus \wp$, les solutions ξ de l'équation (ii) appartiennent aussi à $\mathcal{O}_K \setminus \wp$. A fortiori elles appartiennent au complété $\mathcal{U}_{K_\wp}$. Or

$$\mathcal{U}_{K_\wp} \simeq \pm(1 + \wp\mathcal{O}_{K_\wp})$$

donc tout $\xi \in \mathcal{U}_{K_\wp}$ s'écrit $\xi = \varepsilon(1+y)$ avec $\varepsilon = \pm 1$ et $y \in \wp$. Il s'ensuit que

$$\xi^3 = \varepsilon(1 + 3y + 3y^2 + y^3) \equiv \varepsilon \bmod \wp^3$$

car $3 \in \wp^6$. Si ξ est solution de (ii), on a alors $\alpha \equiv \varepsilon \bmod \wp^3$. Un calcul formel montre que pour toutes les valeurs du paramètre :

$$v_\wp(\alpha + 1) = 0$$

et donc ε est nécessairement égal à $+1$. D'autre part, si l'on suppose $\alpha \equiv (1+y)^3 \bmod \wp^{10}$, alors $\alpha - 1 \equiv y^3 \bmod \wp^7$ et donc $y \in \wp^3$. Cela entraîne $\alpha - 1 \equiv 3y + y^3 \bmod \wp^{10}$, d'où l'on tire $v_\wp(3y + y^3) = 9$ et donc $v_\wp(y) = 3$. ▮

On choisit $\pi = 1 - \zeta$ comme uniformisante de $K_\wp$. Soit $\mathcal{R}$ un système de représentants dans $\mathcal{O}_{K_\wp}$ de $\mathcal{O}_{K_\wp}/\wp$, alors y solution de (iii) s'écrit $y = a_3\pi^3 + a_4\pi^4 + \cdots$ avec $a_i \in \mathcal{R}$ pour tout i et $a_3 \notin \wp$. On vérifie :

$$3y + y^3 \equiv 3a_3\pi^3 + a_3^3\pi^9 \bmod \wp^{10}$$

donc y est solution de (iii) si et seulement si

$$v_3(\mathrm{N}_{K/\mathbb{Q}}(\alpha - 1 - 3a_3\pi^3 - a_3^3\pi^9)) \geq 10$$

Pour le calcul, on choisit $\mathcal{R} = \{0, 1, 2\}$, donc $a_3 \in \{1, 2\}$. On constate que dans les deux cas

$$v_3(\mathrm{N}_{K/\mathbb{Q}}(\alpha - 1 - 3a_3\pi^3 - a_3^3\pi^9)) = 9$$

d'où il s'ensuit que (ii) n'a pas de solution et la proposition suit. ∎

2.3.3 Ramification de $\wp$ dans $K(\sqrt[9]{\alpha})/K$

Ici, la référence est [Gr]. Cet article donne une description explicite de l'ensemble $E_n(R)$ des éléments $x \in R$ tels que $k(\sqrt[p^n]{x})/k$ soit non ramifiée, où R est l'anneau d'entiers d'un corps local k de caractéristique 0 et caractéristique résiduelle p et R contient une racine primitive p^n-ième de l'unité ζ. On rappelle les résultats de [Gr] qui seront utiles. On note $\pi = 1 - \zeta$. On introduit le sous-groupe de congruence de R^* :

$$U_{n,+} = \{x \in R^*,\ x - 1 \text{ est divisible par } p^n\pi^{p^{n-1}}\}$$

Le théorème 1.5 de [Gr] est :

Théorème 2.3.9 (Greither) $U_{n,+} \subset E_n(R)$.

Application : on prend $p = 3$, $n = 2$, $\zeta = \zeta_9$ et $k = \mathbb{Q}_3(\zeta)$. Alors $(p^n\pi^{p^{n-1}}) = (9(1-\zeta)^3) = \wp^{15}$ donc si $x \in \mathbb{Z}_3[\zeta]^*$,

$$x \in U_{2,+} \Leftrightarrow v_\wp(x - 1) \geq 15$$

On reprend le lemme 2.3.5 pour en déduire :

Corollaire 2.3.10 *Si $u \equiv 1 \bmod 3$, alors $K(\sqrt[9]{\alpha})/K$ est non ramifiée en $\wp$.*

En rapprochant du corollaire 2.3.6, on en tire :

Corollaire 2.3.11 *Si $u \equiv 1 \bmod 3$, alors soit $\wp$ est complètement décomposé dans $K(\sqrt[9]{\alpha})/K$, soit $f = g = 3$ où f et g sont le degré résiduel et le degré de décomposition de $\wp$ dans $K(\sqrt[9]{\alpha})/K$.*

Remarque 2.3.12 Des calculs pour un grand nombre de valeurs du paramètre font penser que $\wp$ est complètement décomposé dans $K(\sqrt[9]{\alpha})/K$ pour tout $u \equiv 4 \bmod 9$ et $f = g = 3$ pour tout $u \equiv 1$ ou $7 \bmod 9$.

Par ailleurs, on voit que pour u congru à 0 ou 2 modulo 3, $\alpha - 1$ n'appartient pas à $U_{2,+}$. Le théorème 4.2 de [Gr] décrit les éléments du quotient

$$D_n(R) = E_n(R)/U_{n,+}$$

On note $\zeta_{p^i} = \zeta^{p^{n-i}}$.

Théorème 2.3.13 (Greither) *Il existe des polynômes explicites $f_i \in \mathbb{Z}[\zeta_{p^i}][X]$ $(2 \leq i \leq n)$, définis modulo $p^n(1-\zeta_p)$, tels que :*

$$D_n(R) = \left\{ r^{p^n} \prod_{i=2}^{n} f_i(r_i)^{p^{n-i}} \bmod^{\times} U_{n,+},\ r \in R^*,\ r_i \in R \right\}$$

Le deuxième exemple à la fin de la partie 5 de [Gr] traite le cas $n = 2$. Il n'y a alors qu'un polynôme f_2 qui peut s'écrire :

$$f_2(X) = 1 + p^2\eta X + (p^2\eta + p\eta^p)X^p \quad \text{avec} \quad \eta \equiv \sum_{\nu=1}^{p-1} \frac{\pi^\nu}{\nu} \mod \pi^p$$

Application : on revient à $p = 3$, $n = 2$, $\zeta = \zeta_9$ et $k = \mathbb{Q}_3(\zeta)$. On a :

$$f_2(X) \equiv 1 + 9\pi(1+\pi/2)X + (9\pi(1+\pi/2) + 3\pi^3(1+\pi^3/8))X^3 \bmod \wp^{15}$$

Soient $r \in R^*$ et $r_2 \in R$ tels que

$$\alpha \equiv r^9 f_2(r_2) \bmod^{\times} U_{2,+} \tag{2.1}$$

alors $\alpha \equiv r^9 f_2(r_2) \bmod \wp^{15}$, ce qui entraîne

$$\alpha - 1 \equiv r^9 - 1 + 9\pi(1+\pi/2)r^9 r_2 + 3\pi^3(1+\pi^3/8))r^9 r_2^3 \bmod \wp^{12}$$

Comme $v_\wp(\alpha - 1) = 9$ et $v_\wp(9\pi(1+\pi/2)r^9 r_2 + 3\pi^3(1+\pi^3/8))r^9 r_2^3) \geq 9$, on a $v_\wp(r^9 - 1) \geq 9$ donc $r^9 \in 1 + \wp^9$ et $r \in 1 + \wp$. Soit $y \in \wp$ tel que $r = 1 + y$, alors

$$r^9 \equiv 1 + 9y + 9 \times 4y^2 + 3 \times 28(y^3 + y^6) + y^9 \mod \wp^{15}$$

et

$$\alpha - 1 \equiv y^9 + 3 \times 28y^3 + 3\pi^3 r_2^3 \mod \wp^{12}$$

On commence par montrer :

Lemme 2.3.14 *Si la congruence (2.1) est vérifiée, alors $r_2 \in R^*$.*

Preuve. Si $r_2 \in \wp$, alors $\alpha - 1 \equiv y^9 + 3 \times 28y^3 \bmod \wp^{12}$. On écrit $y = a\pi + y'\pi^2$ avec $a \in \mathcal{R}$ système de représentants de $R/\wp$ et $y' \in R$. Alors

$$\alpha - 1 \equiv a^9\pi^9 + 3\pi^3 28a^3 \mod \wp^{12} \tag{2.2}$$

On choisit $\mathcal{R} = \{0, 1, 2\}$. Un calcul à l'aide du logiciel PARI permet de montrer que pour tout $a \in \{0, 1, 2\}$ et pour tout u congru à 0 ou 2 modulo 3 :

$$v_3(\mathrm{N}_{K/\mathbb{Q}}(\alpha - 1 - a^9\pi^9 - 3\pi^3 28a^3)) = 9$$

ce qui contredit l'assertion (2.2). On a donc $r_2 \in R \setminus \wp = R^*$. ∎

On continue le calcul modulo $\wp^{12}$. On écrit $r_2 = \varepsilon(1 + z)$ avec $\varepsilon = \pm 1$ et $z \in \wp$. On en tire :

$$\alpha - 1 \equiv a^9\pi^9 + 3\pi^3(28a^3 + \varepsilon) \mod \wp^{12} \tag{2.3}$$

Lemme 2.3.15 *Si $\varepsilon = +1$, la congruence (2.3) n'est possible que pour $u \equiv 2 \bmod 3$; si $\varepsilon = -1$, elle n'est possible que pour $u \equiv 0 \bmod 3$.*

Preuve. Soit $N = \mathrm{N}_{K/\mathbb{Q}}(\alpha - 1 - a^9\pi^9 - 3\pi^3(28a^3 + \varepsilon))$. Le calcul permet de montrer, lorsque $\varepsilon = +1$:

$$v_3(N) \begin{cases} = 9 & \text{si} \quad u \equiv 0 \bmod 3 \\ \geq 12 & \text{si} \quad u \equiv 2 \bmod 3 \end{cases}$$

et, lorsque $\varepsilon = -1$:

$$v_3(N) \begin{cases} \geq 12 & \text{si} \quad u \equiv 0 \bmod 3 \\ = 9 & \text{si} \quad u \equiv 2 \bmod 3 \end{cases}$$

∎

On revient maintenant à la congruence modulo $\wp^{15}$. On écrit $r = 1 + y = 1 + a\pi + b\pi^2 + y''\pi^3$ avec a, b dans $\mathcal{R}$ et $y'' \in R$; de même soient $c \in \mathcal{R}$ et $z' \in R$ tels que $r_2 = \varepsilon(1 + c\pi + z'\pi^2)$. Alors la congruence (2.1) entraîne :

$$\begin{gathered}\alpha - 1 \equiv 3\pi^3(\varepsilon + 28a^3) + \pi^9 a^9 + 3\pi^6(28(a^6 + b^3) + \varepsilon(1/8 + c^3)) \\ +9\pi(2\varepsilon + a) + 9\pi^2(4a^2 + b + \varepsilon(1 + c)) \mod \wp^{15}\end{gathered}$$

Soit N la norme de K à $\mathbb{Q}$ de la différence des deux membres de la congruence ci-dessus. Lorsque $\varepsilon = +1$, on sait par le lemme 2.3.15 que u doit être congru à 2 modulo 3. On écrit $u = 2 + 3s$, alors un calcul avec PARI montre que, pour tous les triplets (a, b, c) possibles ($(a, b, c) \in \{0, 1, 2\}^3$) :

$$N = 3^v Q(s) \quad \text{avec} \quad Q(s) \equiv 1 \bmod 3$$

avec $v = 12$ ou $v = 13$. Puisque $v_3(Q(s)) = 0$ pour tout s, on en déduit que

$$v_3(N) = v < 15$$

ce qui montre que la congruence (2.1) n'a pas de solution avec $\varepsilon = +1$. Un calcul analogue avec $\varepsilon = -1$ et u congru à 0 modulo 3 donne la même conclusion. On a donc prouvé :

Proposition 2.3.16 *Si u est congru à 0 ou 2 modulo 3, α n'appartient pas à $E_2(\mathbb{Z}_3[\zeta_9])$, c'est-à-dire l'extension $K(\sqrt[9]{\alpha})/K$ est ramifiée en $\wp$.*

En rapprochant ce résultat de la proposition 2.3.7, on en déduit :

Corollaire 2.3.17 *Si u est congru à 0 ou 2 modulo 3, $\wp$ est inerte dans $K(\sqrt[3]{\alpha})/K$ et ramifié dans $K(\sqrt[9]{\alpha})/K(\sqrt[3]{\alpha})$.*

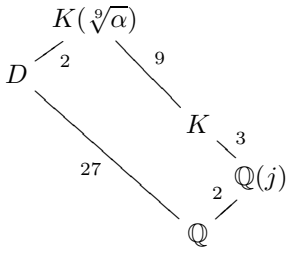
Conjointement avec le corollaire 2.3.11, ce résultat entraîne le point (*iii*) du théorème 2.

2.3.4 Preuve du point (ii) du théorème 2

On a maintenant les informations nécessaires pour montrer que l'extension $D/\mathbb{Q}$ est faiblement ramifiée en 3. On note encore f et g le degré résiduel et le degré de décomposition de 3 dans $K(\sqrt[9]{\alpha})/\mathbb{Q}$. On commence par prouver :

Lemme 2.3.18 *On a l'égalité :* $2v_3(d_D) + fg = 81 + v_3(\mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K}))$.

Preuve. Le lemme découle du diagramme :



et de la formule de transitivité du discriminant. En effet, en passant par la droite du diagramme, on obtient :

$$d_{K(\sqrt[9]{\alpha})} = (d_K)^9 \mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K}) = 3^{81}\, \mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K}) \tag{2.4}$$

(en utilisant [W] proposition 2.1). En passant par la gauche :

$$d_{K(\sqrt[9]{\alpha})} = (d_D)^2\, \mathrm{N}_{D/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/D}) \tag{2.5}$$

Comme chaque idéal de D au-dessus de 3 est modérément ramifié dans $K(\sqrt[9]{\alpha})/D$, on a

$$\mathcal{D}_{K(\sqrt[9]{\alpha})/D} = \mathfrak{a}\,\mathfrak{p}_1 \dots \mathfrak{p}_g$$

où les $\mathfrak{p}_i$ sont les idéaux premiers de $K(\sqrt[9]{\alpha})$ au-dessus de 3 et $\mathfrak{a}$ est un idéal de $K(\sqrt[9]{\alpha})$ premier à 3. Il s'ensuit que

$$\mathrm{N}_{D/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/D}) = \mathrm{N}_{K(\sqrt[9]{\alpha})/\mathbb{Q}}(\mathcal{D}_{K(\sqrt[9]{\alpha})/D}) = 3^{fg}\mathrm{N}(\mathfrak{a})$$

avec $(3, \mathrm{N}(\mathfrak{a})) = 1$. On tire maintenant de (2.4) et (2.5) l'égalité qui était à prouver. ∎

Soit s la valuation de la différente $\mathcal{D}_D$ en les idéaux premiers $\mathfrak{p}_i$ de D au-dessus de 3. Alors $\mathcal{D}_D = \mathfrak{a}\,(\mathfrak{p}_1 \dots \mathfrak{p}_g)^s$, où $\mathfrak{a}$ est un idéal de D premier à 3 et

$$d_D = \mathrm{N}_{D/\mathbb{Q}}(\mathcal{D}_D) = 3^{fgs}\,\mathrm{N}(\mathfrak{a}) \tag{2.6}$$

On déduit immédiatement du lemme précédent :

$$2s + 1 = \frac{81 + v_3(\mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K}))}{fg} \tag{2.7}$$

Lorsque $K(\sqrt[9]{\alpha})/K$ est non ramifiée, on a $v_3(\mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K})) = 0$ et $fg = [K(\sqrt[9]{\alpha}) : K] = 9$. Il découle de (2.7) que $s = 4$ et la formule de Hilbert (1.7) permet de conclure que $D/\mathbb{Q}$ est faiblement ramifiée.

On traite maintenant le cas où $K(\sqrt[9]{\alpha})/K$ est ramifiée. Pour simplifier les écritures, on note $\beta = \sqrt[3]{\alpha}$, $K' = K(\beta)$, $\gamma = \sqrt[3]{\beta}$ et $K'' = K'(\gamma)$. On sait par le corollaire 2.3.17 que K''/K' est ramifiée au-dessus de 3 tandis que K'/K y est inerte. Soient $\mathfrak{q}$ et $\mathfrak{p}$ les idéaux premiers de K' et K'' au-dessus de 3. On a besoin du résultat suivant.

Lemme 2.3.19 *$\mathcal{O}_{K'}[\gamma]$ n'est pas un ordre $\mathfrak{q}$-maximal de $\mathcal{O}_{K''}$.*

Remarque 2.3.20 Un ordre $\mathcal{O}$ de $\mathcal{O}_{K''}$ est dit $\mathfrak{q}$-maximal si, dans la décomposition du $\mathcal{O}_{K'}$-module de torsion $\mathcal{O}_{K''}/\mathcal{O}$:

$$\mathcal{O}_{K''}/\mathcal{O} \simeq \bigoplus_i \mathcal{O}_{K'}/\mathfrak{d}_i$$

$\mathfrak{q}$ ne divise pas $\prod_i \mathfrak{d}_i$ (les $\mathfrak{d}_i$ sont des idéaux entiers de $\mathcal{O}_{K'}$ distincts de $\mathcal{O}_{K'}$). On pourra se reporter à [Coh] théorème 1.2.30 et définition 2.4.1 pour de plus amples détails.

Preuve. Le théorème 2.4.8 de [Coh] généralise aux extensions relatives le critère de Dedekind :

Théorème 2.3.21 *Soit l/k une extension finie de corps de nombres avec $l = k(\theta)$ où θ est un entier algébrique de polynôme minimal unitaire $T(X) \in k(X)$. Soient $\mathfrak{q}$ un idéal premier de $\mathcal{O}_k$ et $\mu \in \mathcal{O}_k$ tel que $v_{\mathfrak{q}}(\mu) = -1$. Soit $\overline{T}(X) = \prod_i \overline{T}_i(X)^{e_i}$ la factorisation de $\overline{T}(X)$ dans $(\mathcal{O}_k/\mathfrak{q})[X]$ avec les $T_i(X) \in k(X)$ unitaires. On pose :*

$$g(X) = \prod_i T_i(X), \quad h(X) = \prod_i T_i(X)^{e_i - 1} \quad \text{et} \quad f(X) = \mu(g(X)h(X) - T(X))$$

alors $f(X) \in \mathcal{O}_k[X]$ et $\mathcal{O}_k[\theta]$ est $\mathfrak{q}$-maximal si et seulement si $(\overline{f}, \overline{g}, \overline{h}) = 1$ dans $(\mathcal{O}_k/\mathfrak{q})[X]$.

Application : On prend $k = K'$, $l = K''$ donc $\theta = \gamma$ et $T(X) = X^3 - \beta$; $\mathfrak{q}$ est l'idéal premier de K' au-dessus de 3. Comme $\mathfrak{q} = \wp\mathcal{O}_{K'}$, on peut choisir $\mu = (1 - \zeta)^{-1}$. On sait que $3 \in \mathfrak{q}^6$ et

$$v_{\mathfrak{q}}(\beta - 1) = \frac{1}{3} v_{\wp}(\mathrm{N}_{K'/K}(\beta - 1)) = \frac{1}{3} v_{\wp}(\alpha - 1) = 3$$

donc $\beta \equiv 1 \bmod \mathfrak{q}^3$. La factorisation de $T(X)$ dans $(\mathcal{O}_{K'}/\mathfrak{q})[X]$ est

$$\overline{T}(X) = X^3 - \overline{\beta} = X^3 - 1 = (X - 1)^3$$

d'où $g(X) = X - 1$, $h(X) = (X - 1)^2$, $f(X) = ((X - 1)^3 - (X^3 - \beta))/(1 - \zeta)$ et

$$\overline{f}(X) = \frac{3(-X^2 + X) + (\beta - 1)}{1 - \zeta} = 0$$

donc $(\overline{f},\overline{g},\overline{h}) = (\overline{g},\overline{h}) = (X-1)(\mathcal{O}_{K'}/\mathfrak{q})[X]$ et le lemme est démontré. ∎

On est maintenant en mesure de terminer la démonstration. Puisque

$$\mathrm{disc}(1,\gamma,\gamma^2) = \mathrm{disc}(X^3-\beta) = -3^3\beta^2$$

et $v_{\mathfrak{q}}(\beta) = v_{\wp}(\alpha) = 0$, on a $v_{\mathfrak{q}}(\mathrm{disc}(1,\gamma,\gamma^2)) = 18$ et donc, par le lemme précédent,

$$v_{\mathfrak{q}}(d_{K''/K'}) < 18$$

Comme $v_3(\mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K})) = 3v_{\mathfrak{q}}(d_{K''/K'})$, on tire de (2.7) que $s < 22$. Les deux premiers groupes de ramification $G_0 = G_1$ de $D/\mathbb{Q}$ en 3 étant d'ordre 9, on en déduit par la formule de Hilbert (1.7) que l'ordre de G_2 est au plus 3. Alors $i = 1$ est tel que $G_i \neq G_{i+1}$ et la proposition 11 de [Se1] IV2 entraîne que $G_2 = G_3 = G_4$. Mais $8+8+2+2+2 = 22 > s$ donc G_2 est trivial et $D/\mathbb{Q}$ est faiblement ramifiée en 3. Ceci termine la preuve du théorème 2.

2.3.5 Les valeurs de $v_3(d_R)$

Dans ce paragraphe, on applique les résultats de la partie 1.4 aux extensions de la famille infinie qu'on vient de décrire, pour faire le lien entre l'indice de ramification dans le corps de décomposition D et la valuation en 3 du discriminant du corps de rupture R du polynôme $P_t(x)$. On rappelle que e, f et g désignent l'indice de ramification, le degré résiduel et le degré de décomposition de 3 dans $D/\mathbb{Q}$. L'indéterminée t est toujours supposée prendre de bonnes valeurs.

Proposition 2.3.22 *Si u est congru à 1 modulo 3 (ou t congru à 14 modulo 27), alors $e = 3$ et $v_3(d_R) = 8$; si u est congru à 0 ou 2 modulo 3, alors $e = 9$ et $v_3(d_R) = 12$.*

Preuve. On commence par montrer une propriété intéressante de $D/\mathbb{Q}$.

Lemme 2.3.23 *Soit L l'unique sous-extension de $\mathbb{Q}(\zeta_9)$ de degré 3. Soit K_0 la sous-extension de D fixée par l'unique sous-groupe distingué d'ordre 3 de G. Alors :*

$$L \subset K_0 \subset D$$

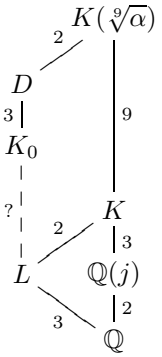
Preuve. On sait que $H = \mathrm{Gal}(K(\sqrt[9]{\alpha})/D)$ est l'unique 2-Sylow de $\mathcal{G} = \mathrm{Gal}(K(\sqrt[9]{\alpha})/\mathbb{Q})$, donc

$$H \subset \mathrm{Gal}(K(\sqrt[9]{\alpha})/L)$$

et $L \subset D$. De plus, $\mathrm{Gal}(D/L) \simeq C_9$ contient l'unique sous-groupe distingué d'ordre 3 de $G = \mathrm{Gal}(D/\mathbb{Q})$, si bien que

$$L \subset K_0$$

et le lemme en découle. ∎



Corollaire 2.3.24 *Soit $\mathfrak{p}$ un idéal premier de D au-dessus de 3. On suppose que $e = 3$. Alors $G_0(\mathfrak{p}/3)$ est un sous-groupe d'ordre 3 non distingué dans G.*

Preuve. Si $G_0(\mathfrak{p}/3)$ est distingué dans G, alors D/K_0 est ramifiée au-dessus de 3. Comme $L/\mathbb{Q}$ est ramifiée en 3 ($L \subset \mathbb{Q}(\zeta_9)$), cela entraîne $e = 9$ qui contredit l'hypothèse. ▮

Lorsque u est congru à 1 modulo 3, on sait par le corollaire 2.3.11 que $e = 3$ et $f = g = 3$ ou $g = 9$. On est donc dans les conditions d'application du corollaire 2.3.24. On se place dans le cas où $e = f = g = 3$. Soient $\mathfrak{p}_1$, $\mathfrak{p}_2$ et $\mathfrak{p}_3$ les idéaux premiers de D au-dessus de 3. Les $G_0(\mathfrak{p}_k/3)$ sont des sous-groupes d'ordre 3 conjugués par G, tous distincts et $\mathrm{Gal}(D/R)$ est égal à l'un d'eux, par exemple $G_0(\mathfrak{p}_1/3)$. Il s'ensuit que $\mathfrak{p}_1$ est ramifié dans D/R et que $\mathfrak{p}_2$ et $\mathfrak{p}_3$ y sont inertes. Pour $1 \leq k \leq 3$, on note $\wp_k = \mathfrak{p}_k \cap \mathcal{O}_R$. On voit que 3 est décomposé dans $R/\mathbb{Q}$ et que $\wp_2/3$ et $\wp_3/3$ sont ramifiés tandis que $\wp_1/3$ est inerte. Le lemme 1.4.5 permet de conclure.

On se place dans le cas où $e = 3$ et $g = 9$. Soient $\mathfrak{p}_1 \dots \mathfrak{p}_9$ les idéaux premiers de D au-dessus de 3. On montre :

Lemme 2.3.25 *Chaque sous-groupe d'ordre 3 non distingué de G est égal à $G_0(\mathfrak{p}_k/3)$ pour exactement trois valeurs de k.*

Preuve. La présentation du groupe non abélien d'ordre 27 d'exposant 9 par générateurs et relations est la suivante (cf [Ha] 4.4) :

$$G =< a, b > /\{a^9 = b^3 = 1,\ b^{-1}ab = a^4\} \tag{2.8}$$

et les sous-groupes d'ordre 3 non distingués de G sont les $< b^i a >$ pour $i \in \{1, 2, 3\}$. Soit $\mathfrak{p}$ l'un des $\mathfrak{p}_k$ tels que $G_0(\mathfrak{p}_k/3) =< b >$. On vérifie que :

$$\begin{array}{ccccccc}
< b > & = & G_0(\mathfrak{p}/3) & = & G_0(a^3\mathfrak{p}a^{-3}/3) & = & G_0(a^6\mathfrak{p}a^{-6}/3) \\
< ba^3 > & = & G_0(a\mathfrak{p}a^{-1}/3) & = & G_0(a^4\mathfrak{p}a^{-4}/3) & = & G_0(a^7\mathfrak{p}a^{-7}/3) \\
< ba^6 > & = & G_0(a^2\mathfrak{p}a^{-2}/3) & = & G_0(a^5\mathfrak{p}a^{-5}/3) & = & G_0(a^8\mathfrak{p}a^{-8}/3)
\end{array}$$

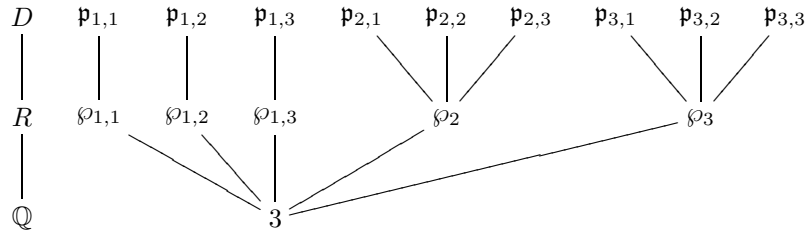
ce qui démontre le lemme. ▮

On sait que $\mathrm{Gal}(D/R)$ est l'un des sous-groupes d'ordre 3 non distingués de G. On renumérote les $\mathfrak{p}_k$ de sorte que :

$$\begin{array}{ccccccc}
G_0(\mathfrak{p}_{1,1}/3) & = & G_0(\mathfrak{p}_{1,2}/3) & = & G_0(\mathfrak{p}_{1,3}/3) & = & \mathrm{Gal}(D/R) \\
G_0(\mathfrak{p}_{2,1}/3) & = & G_0(\mathfrak{p}_{2,2}/3) & = & G_0(\mathfrak{p}_{2,3}/3) & & \\
G_0(\mathfrak{p}_{3,1}/3) & = & G_0(\mathfrak{p}_{3,2}/3) & = & G_0(\mathfrak{p}_{3,3}/3) & &
\end{array}$$

On voit que $\mathfrak{p}_{1,1}$, $\mathfrak{p}_{1,2}$ et $\mathfrak{p}_{1,3}$ sont ramifiés dans D/R et que les autres y sont non ramifiés donc décomposés. On note $\wp_{1,k} = \mathfrak{p}_{1,k} \cap \mathcal{O}_R$ pour $1 \leq k \leq 3$ et $\wp_i = \mathfrak{p}_{i,k} \cap \mathcal{O}_R$ pour $i = 2$ ou 3 et n'importe quel k. Alors $\wp_2/3$ et $\wp_3/3$ sont ramifiés tandis que les $\wp_{1,k}/3$ sont décomposés. Le lemme 1.4.5 permet à

nouveau de conclure. On illustre la situation par le diagramme :



On traite maintenant le cas u congru à 0 ou 2 modulo 3. On sait qu'alors $e = 9$ et $f = 3$. Soit $\mathfrak{p}$ l'idéal premier de D au-dessus de 3.

Lemme 2.3.26 *$G_0(\mathfrak{p}/3)$ est l'unique sous-groupe de G d'ordre 9 d'exposant 3. On a $G_0(\mathfrak{p}/3) =< a^3, b >$ avec les notations de (2.8).*

Preuve. On se remémore le diagramme du lemme 2.3.23. On a $G = \mathrm{Gal}(D/\mathbb{Q})$, on note $\mathcal{G} = \mathrm{Gal}(K(\sqrt[9]{\alpha})/\mathbb{Q})$ et $H = \mathrm{Gal}(K(\sqrt[9]{\alpha})/D)$. Alors :

$$G_0 = \mathcal{G}_0 H/H$$

Les seuls éléments d'ordre 9 de $\mathcal{G}$ sont les générateurs de $\mathrm{Gal}(K(\sqrt[9]{\alpha})/K)$. Comme $K(\sqrt[9]{\alpha})/K$ n'est pas totalement ramifiée, il s'ensuit que $\mathcal{G}_0$ ne contient pas d'élément d'ordre 9 ; à fortiori la même chose est vraie pour G_0, qui est donc d'exposant 3. Or G n'admet qu'un sous-groupe d'ordre 9 d'exposant 3, engendré par a^3 et b. ∎

De plus, on sait que $< a^3, b >$ contient tous les sous-groupes d'ordre 3 de G. Il s'ensuit que D/R est ramifiée au-dessus de 3, donc $e(3, R/\mathbb{Q}) = f(3, R/\mathbb{Q}) = 3$ et le lemme 1.4.3 permet de conclure. La proposition 2.3.22 est donc démontrée. ∎

2.4 Une autre famille infinie

On considère le polynôme paramétré par $t \in \mathbb{Z}$:

$$\begin{aligned} Q_t(X) \quad = \quad & X^7 - 7(t^2-t+2)X^5 + 14(t^2-t+2)^2X^3 - 7(t^2-t+2)^3X \\ & -(2t-1)(t^2-t+2)(t^4-2t^3-16t^2+17t+11) \end{aligned}$$

On va montrer, à l'aide des résultats de [Ei1] (3.4.2), dans le paragraphe 2.4.1 :

Proposition 2.4.1 *Le corps de décomposition D sur $\mathbb{Q}$ de Q_t spécialisé en une valeur entière de t est galoisien de groupe de Galois isomorphe à $C_7 \rtimes C_3$ pour une infinité de valeurs entières de t.*

L'étude de la ramification en 7 menée dans les paragraphes 2.4.2 et 2.4.3 permet de prouver :

Théorème 2.4.2 *Pour toutes les bonnes valeurs de t congrues à 25 modulo 49, l'extension $D/\mathbb{Q}$ est modérément ramifiée.*

Remarque 2.4.3 La preuve est plus simple que celle du théorème 2, le critère de Greither n'étant pas nécessaire. Si t est congru à 25 modulo 49, on trouve que 7 se décompose en 7 idéaux premiers dans $D/\mathbb{Q}$, chacun d'indice de ramification égal à 3.

2.4.1 Construction des extensions

On construit ici une famille infinie d'extensions de groupe $C_7 \rtimes C_3$ en utilisant la méthode décrite dans la thèse d'Eichenlaub ([Ei1] 3.4.2). On note $K = \mathbb{Q}(\zeta)$ le corps de nombres obtenu en adjoignant à $\mathbb{Q}$ la racine primitive 7-ième de l'unité ζ. Soit $K_2 = \mathbb{Q}(\sqrt{-7})$ la sous-extension quadratique de K. Pour tout entier naturel t, on considère l'élément $\alpha \in K_2$ défini par :

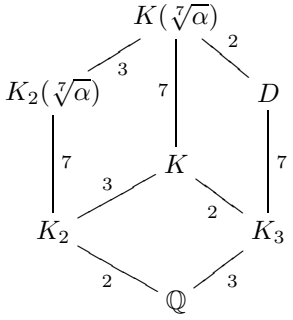
$$\alpha = (t + \zeta + \zeta^2 + \zeta^4)^6 (t + \zeta^3 + \zeta^6 + \zeta^5)$$

On sait par les résultats de [Ei1] que, pour toutes les valeurs de t sauf un nombre fini, $K(\sqrt[7]{\alpha})/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $C_7 \rtimes C_6$ et contenant un unique 2-Sylow (d'ordre 2). Il en découle que l'unique sous-extension galoisienne D de $K(\sqrt[7]{\alpha})$ de degré 21 est de groupe de Galois isomorphe à $C_7 \rtimes C_3$. Le polynôme minimal de $\sqrt[7]{\alpha}$ a pour corps de rupture $K_2(\sqrt[7]{\alpha})$ et pour corps de décomposition $K(\sqrt[7]{\alpha})$; si l'on note $\bar{\alpha}$ le conjugué de α, il est égal à $(X^7 - \alpha)(X^7 - \bar{\alpha})$, c'est-à-dire :

$$X^{14} - 2(2t-1)(t^2 - t + 2)(t^4 - 2t^3 - 16t^2 + 17t + 11)X^7 + (t^2 - t + 2)^7$$

Par calcul de résolvantes de degré 7 de ce polynôme pour plusieurs valeurs du paramètre et interpolation des cœfficients trouvés, on obtient le polynôme paramétré Q_t qui est donc une équation paramétrée de D.

Le diagramme ci-contre illustre la situation :



2.4.2 Un critère explicite de ramification

Dans ce paragraphe, on se place dans la situation plus générale où $K = \mathbb{Q}(\zeta_p)$ pour p premier impair et ζ_p racine primitive p-ième de l'unité. Soit $\wp = (1 - \zeta_p)$

l'idéal premier de K au-dessus de p, soit $\alpha \in K^* \setminus K^{*p}$, le comportement de $\wp$ dans l'extension $K(\sqrt[p]{\alpha})/K$ est donné par le critère de Hecke ([He] théorème 119) qui s'exprime comme suit dans la situation présente :

Proposition 2.4.4 *On suppose $\alpha \notin \wp$. Pour $\xi \in K$, on considère les congruences :*

$$(i)\ \alpha \equiv \xi^p \bmod \wp^p \qquad et \qquad (ii)\ \alpha \equiv \xi^p \bmod \wp^{p+1}$$

Alors, dans $K(\sqrt[p]{\alpha})/K$, $\wp$ est ramifié si (i) n'a pas de solution ; $\wp$ est inerte si (i) a des solutions et si (ii) n'en a pas ; $\wp$ est décomposé si (ii) a des solutions.

Soient e un entier divisant $p-1$ et K_e la sous-extension de K de degré e. On va déduire de la proposition précédente le critère explicite suivant :

Proposition 2.4.5 *On suppose $\alpha \in K_e \setminus (\wp \cap K_e)$. Alors, dans $K(\sqrt[p]{\alpha})/K$, $\wp$ est ramifié si et seulement si, pour tout $k \in \{1, 2, \ldots, p-1\}$,*

$$v_p(\mathrm{N}_{K_e/\mathbb{Q}}(\alpha - k^p)) \leq e$$

Si de plus $e < p-1$, $\wp$ est ramifié ou décomposé.

Preuve. On note $K_\wp$ le complété de K en $\wp$ et $\mathcal{U}_{K_\wp}$ son groupe des unités. On commence par montrer :

Lemme 2.4.6 *Soit $\xi \in \mathcal{U}_{K_\wp}$, alors il existe $k \in \{1, 2, \ldots, p-1\}$ tel que $\xi^p \equiv k^p \bmod \wp^p$.*

Preuve. On sait que $\mathcal{U}_{K_\wp} \simeq \mu_{p-1} \times (1+\wp)$ donc $\xi \in \mathcal{U}_{K_\wp}$ s'écrit $\xi = x(1+y)$ avec $x \in \mu_{p-1}$ et $y \in \wp$. On a :

$$\xi^p = x^p(1+y)^p = x(1 + py + \cdots + y^p)$$

donc, comme $p \in \wp^{p-1}$,

$$\xi^p \equiv x \mod \wp^p \tag{2.9}$$

Par ailleurs, soit $k \in \{1, 2, \ldots, p-1\}$ alors $k \in \mathcal{U}_{K_\wp}$ donc k s'écrit $k = x_k(1+z)$ avec $x_k \in \mu_{p-1}$ et $z \in \wp$. Comme

$$k^{p-1} \equiv 1 \mod p$$

on a $(1+z)^{p-1} \equiv 1 \bmod \wp^{p-1}$, donc

$$\sum_{i=1}^{p-2} \binom{p-1}{i} z^i \in \wp^{p-1}$$

Or

$$\binom{p-1}{i} = \frac{(p-1)(p-2)\ldots(p-i)}{i(i-1)\ldots 2} \equiv (-1)^i \bmod p$$

d'où

$$-z+z^2-\cdots-z^{p-2}=-z(1-z+z^2-\cdots+z^{p-3}) \ \in \ \wp^{p-1}$$

et donc $z\in\wp^{p-1}$, d'où l'on déduit $k\equiv x_k \bmod \wp^{p-1}$ et

$$k^p=x_k(1+z)^p\equiv x_k \mod \wp^{2p-2}$$

Enfin, si $k'\in\{1,2,\ldots,p-1\}$ avec $k'=x_{k'}(1+z')$, on a :

$$x_k=x_{k'}\Leftrightarrow k\equiv k' \bmod^{\times}(1+\wp)\Leftrightarrow k\equiv k' \bmod \wp\Leftrightarrow k\equiv k' \bmod p\Leftrightarrow k=k'$$

et

$$|\mu_{p-1}|=p-1=|\{1,2,\ldots,p-1\}|$$

ce qui, à l'aide de (2.9), termine la preuve du lemme. ▌

On déduit du lemme et de la proposition 2.4.4 que $\wp$ est ramifié dans $K(\sqrt[p]{\alpha})/K$ si et seulement si, pour tout $k\in\{1,2,\ldots,p-1\}$,

$$v_\wp(\alpha-k^p)<p$$

c'est-à-dire, en notant $f=(p-1)/e$:

$$fv_p(\mathrm{N}_{K_e/\mathbb{Q}}(\alpha-k^p))\leq p-1$$

ou encore

$$v_p(\mathrm{N}_{K_e/\mathbb{Q}}(\alpha-k^p))\leq e$$

ce qui constitue la première assertion de la proposition 2.4.5. On suppose maintenant que $f>1$. Si $\wp$ n'est pas ramifié dans $K(\sqrt[p]{\alpha})/K$, soit $k\in\{1,2,\ldots,p-1\}$ tel que $v_p(\mathrm{N}_{K_e/\mathbb{Q}}(\alpha-k^p))>e$, alors

$$v_\wp(\alpha-k^p)\geq f(e+1)=p-1+f\geq p+1$$

donc $\wp$ est décomposé par la proposition 2.4.4. ▌

2.4.3 Application

On revient à $p=7$ et $\alpha=(t+\zeta+\zeta^2+\zeta^4)^6(t+\zeta^3+\zeta^6+\zeta^5)\in K_2$. On va montrer :

Proposition 2.4.7 *Si t est congru à 25 modulo 49, alors 7 est décomposé dans $K(\sqrt[7]{\alpha})/K$; pour toutes les autres valeurs de t, 7 est ramifié dans $K(\sqrt[7]{\alpha})/K$.*

Preuve. On détermine d'abord si $\alpha\in\wp$. Pour cela, on calcule

$$N=\mathrm{N}_{K_2/\mathbb{Q}}(\alpha)=\alpha\bar{\alpha}=(t+\zeta+\zeta^2+\zeta^4)^7(t+\zeta^3+\zeta^6+\zeta^5)^7$$

On trouve :

$$\begin{aligned}N \ = \ & t^{14}-7t^{13}+35t^{12}-119t^{11}+329t^{10}-721t^9+1337t^8-2045t^7\\ & +2674t^6-2884t^5+2632t^4-1904t^3+1120t^2-448t+128\end{aligned}$$

En réduisant les cœfficients de N modulo 7, on obtient :

$$N \equiv t^{14} + 6t^7 + 2 \mod 7$$

d'où l'on déduit que $v_7(N) = 0$ pour tout t non congru à 4 modulo 7 et $v_7(N) = 7$ pour t congru à 4 modulo 7.

Si t n'est pas congru à 4 modulo 7, la proposition 2.4.5 s'applique, donc $\wp$ est ramifié dans $K(\sqrt[7]{\alpha})/K$ si et seulement si pour tout $k \in \{1, 2, \ldots, 6\}$,

$$v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\alpha - k^7)) \leq 2$$

Un calcul à l'aide du logiciel PARI montre que $v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\alpha - k^7))$ est au plus 1 et donc la proposition est démontrée pour t non congru à 4 modulo 7.

Si t est congru à 4 modulo 7, on a vu que $v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\alpha)) = 7$. Or $K_2 = \mathbb{Q}(\sqrt{-7})$ contient $\pi = \sqrt{-7}$ qui vérifie $v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\pi)) = 1$. Soit

$$\beta = \alpha\pi^{-7}$$

alors $v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\beta)) = 0$ et $K(\sqrt[7]{\alpha}) = K(\sqrt[7]{\beta})$. On applique la proposition 2.4.5 à β : $\wp$ est ramifié dans $K(\sqrt[7]{\alpha})/K$ si et seulement si, pour tout $k \in \{1, 2, \ldots, 6\}$,

$$v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\beta - k^7)) \leq 2$$

On écrit $t = 4 + 7s$. Pour $k \neq 4$, on trouve $v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\beta - k^7)) = 0$ pour tout s. Pour $k = 4$, on a :

$$v_7(\mathrm{N}_{K_2/\mathbb{Q}}(\beta - 4^7)) \begin{cases} \geq 3 & \text{si } s \equiv 3 \bmod 7 \\ = 1 & \text{sinon} \end{cases}$$

et donc $K(\sqrt[7]{\alpha})/K$ est ramifiée en $\wp$ si t n'est pas congru à 25 modulo 49. Si $t \equiv 25 \bmod 49$, $\wp$ est non ramifié et, comme $e = 2 > 1$, la proposition 2.4.5 entraîne que $\wp$ est décomposé dans $K(\sqrt[7]{\alpha})/K$. ∎

En se remémorant le diagramme du paragraphe 2.4.1, on en déduit aisément :

Corollaire 2.4.8 *Si t est congru à 25 modulo 49, alors 7 se décompose en 7 idéaux premiers de D, chacun d'indice de ramification égal à 3 ; pour toutes les autres valeurs de t, 7 est totalement ramifié dans $D/\mathbb{Q}$.*

Le théorème 2.4.2 en découle puisque les premiers distincts de 7 ne sont pas ramifiés dans $\mathbb{Q}(\zeta)/\mathbb{Q}$ et donc sont nécessairement modérément ramifiés dans $D/\mathbb{Q}$.

Remarque 2.4.9 Lorsque t n'est pas congru à 25 modulo 49, des calculs du discriminant de $K_2(\sqrt[7]{\alpha})/\mathbb{Q}$ menés avec PARI pour un grand nombre de valeurs de t montrent que $D/\mathbb{Q}$ n'est pas faiblement ramifiée : on a $G_1(7, D/\mathbb{Q}) = G_2(7, D/\mathbb{Q}) \simeq C_7$ et $G_3(7, D/\mathbb{Q})$ est trivial ($v_7(d_D) = 32$).

Chapitre 3

Structure galoisienne : préliminaires

L'intérêt pour les extensions faiblement ramifiées s'est d'abord manifesté dans des problèmes de structure galoisienne et c'est sous cet aspect que ce chapitre et le suivant les abordent. Lorsque N/K est une extension finie galoisienne de corps de nombres de groupe de Galois G, on sait par le théorème de Nœther que l'anneau d'entiers de N est un $\mathcal{O}_K[G]$-module localement libre si et seulement si l'extension est modérément ramifiée. Erez a montré un résultat similaire pour les extensions faiblement ramifiées de degré impair, dans lequel l'anneau d'entiers est remplacé par un idéal fractionnaire $\mathcal{A}_{N/K}$ que l'on définit dans la partie 3.1 et qu'on appelle la *racine carrée de la codifférente*.

Ce résultat permet de considérer la classe $(\mathcal{A}_{N/K})$ de cet idéal dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres $\mathrm{Cl}(\mathbb{Z}[G])$. Comme G est d'ordre impair, on sait que $\mathcal{A}_{N/K}$ est un $\mathbb{Z}[G]$-module libre si et seulement si $(\mathcal{A}_{N/K})$ est triviale. On est donc ramené à travailler dans $\mathrm{Cl}(\mathbb{Z}[G])$, dont il est nécessaire d'avoir une description adaptée. C'est pourquoi on introduit dans la partie 3.2 la Hom-description de Fröhlich de $\mathrm{Cl}(\mathbb{Z}[G])$ en terme de quotient d'un groupe d'homomorphismes équivariants sur les caractères virtuels de G, laquelle se révèle avoir de très bonnes propriétés fonctorielles. On donne un représentant de $(\mathcal{A}_{N/K})$ dans ce groupe quotient, inspiré de celui utilisé dans [Er3]. Il fait intervenir des résolvantes construites à partir des bases locales de $\mathcal{A}_{N/K}$ et des sommes de Gauss galoisiennes. On étudie ces dernières dans la partie 3.3, à partir d'articles de Martinet ([M3]) et de Tate ([Tat2]) ; on montre une formule de restriction au groupe d'inertie dans le cas où celui-ci est abélien et l'extension locale faiblement ramifiée.

3.1 L'idéal racine carrée de la codifférente

Soit N/K une extension finie galoisienne de corps de nombres de groupe de Galois G, que l'on suppose d'ordre impair. Sous cette condition, on voit

facilement à l'aide de la formule de Hilbert (1.7) qu'il existe un idéal fractionnaire $\mathcal{A}_{N/K}$ de l'anneau d'entiers de N vérifiant :

$$(\mathcal{A}_{N/K})^2 = (\mathcal{D}_{N/K})^{-1}$$

où $\mathcal{D}_{N/K}$ est la différente de l'extension. On appelle $\mathcal{A}_{N/K}$ l'idéal *racine carrée de la codifférente*.

Cet idéal existe parfois dans des extensions de degré pair. Ainsi, parmi les exemples de la partie 2.1, les numéros 1, 6, 13 et 14 de la liste d'extensions faiblement ramifiées possèdent une racine carrée de la codifférente (ce sont les seuls en degré pair). On se restreint toutefois dans ce chapitre au cas où l'extension est de degré impair.

En plus d'être un idéal fractionnaire de $\mathcal{O}_N$, la racine carrée de la codifférente a deux propriétés importantes : elle est stable sous l'action du groupe de Galois de l'extension et, munie de la forme trace, devient un réseau entier unimodulaire. On explore ces deux aspects dans les prochains paragraphes.

3.1.1 Structure d'idéal ambige

De par les propriétés de la différente (voir la remarque 1.1.2), $\mathcal{A}_{N/K}$ est stable sous l'action de G, ce qui en fait un $\mathbb{Z}[G]$-module. On dit aussi que c'est un idéal *ambige*. L'étude de la structure de $\mathbb{Z}[G]$-module de $\mathcal{A}_{N/K}$, c'est-à-dire de sa structure galoisienne, a principalement été menée par B. Erez. Ses résultats les plus aboutis sur cette question se trouvent dans [Er3]. Celui qui nous intéresse au premier abord, notamment parce qu'il fait le lien avec les chapitres précédents, est l'analogue du théorème de Nœther pour l'anneau d'entiers et s'énonce comme suit ([Er3] théorème 1).

Théorème 3.1.1 (Erez) *$\mathcal{A}_{N/K}$ est un $\mathcal{O}_K[G]$-module localement libre si et seulement si l'extension N/K est faiblement ramifiée.*

On se place dorénavant sous l'hypothèse de ramification faible. On connaît peu de choses sur la structure relative globale des modules galoisiens, qu'il s'agisse de l'anneau d'entiers (le plus étudié) ou de l'idéal racine carrée de la codifférente. On suit ici la démarche habituelle : par restriction des scalaires de $\mathcal{O}_K$ à $\mathbb{Z}$, on peut voir $\mathcal{A}_{N/K}$ comme un $\mathbb{Z}[G]$-module. Comme $\mathcal{O}_K[G]$ est un $\mathbb{Z}[G]$-module libre, un $\mathcal{O}_K[G]$-module localement libre (resp. libre) est à fortiori un $\mathbb{Z}[G]$-module localement libre (resp. libre). $\mathcal{A}_{N/K}$ est donc un $\mathbb{Z}[G]$-module localement libre, de rang égal à $[K : \mathbb{Q}]$.

Comme dans le cas de l'anneau d'entiers, se pose alors la question de savoir si $\mathcal{A}_{N/K}$ est un $\mathbb{Z}[G]$-module libre. [Er3] apporte deux réponses partielles à cette question. D'une part, si $\mathcal{M}$ est un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$, alors $\mathcal{A}_{N/K} \otimes_{\mathbb{Z}[G]} \mathcal{M}$ est un $\mathcal{M}$-module libre ; d'autre part, si N/K est modérément ramifiée, alors $\mathcal{A}_{N/K}$ est un $\mathbb{Z}[G]$-module libre.

Remarque 3.1.2 On peut interpréter le premier de ces résultats de la façon suivante. On introduit le *groupe noyau* de l'extension des scalaires $D(\mathbb{Z}[G])$, défini par la suite exacte :

$$1 \longrightarrow D(\mathbb{Z}[G]) \longrightarrow \mathrm{Cl}(\mathbb{Z}[G]) \longrightarrow \mathrm{Cl}(\mathcal{M}) \longrightarrow 1$$

On peut montrer que ce groupe noyau ne dépend pas du choix de l'ordre maximal $\mathcal{M}$ considéré. Le fait que $\mathcal{A}_{N/K} \otimes_{\mathbb{Z}[G]} \mathcal{M}$ soit un $\mathcal{M}$-module libre équivaut à l'appartenance de $(\mathcal{A}_{N/K})$ au groupe noyau $D(\mathbb{Z}[G])$.

On verra plus loin (corollaire 3.2.4) une conséquence importante de ce résultat. Dans le prochain chapitre, on présentera des résultats sur la structure galoisienne de $\mathcal{A}_{N/K}$ dans le cas d'une extension sauvagement et faiblement ramifiée. Lorsque l'extension est absolue, ils élargissent le champ de validité du deuxième résultat rappelé ci-dessus.

3.1.2 La structure de réseau de $\mathcal{A}_{N/K}$

La racine carrée de la codifférente a été étudiée en premier lieu pour ses propriétés par rapport à la forme trace de l'extension. Il s'agit de la forme bilinéaire symétrique non dégénérée qui, à un couple (x, y) d'éléments de N associe :

$$\mathrm{Tr}(x, y) = \mathrm{Tr}_{N/K}(xy)$$

On voit facilement que cette forme ne prend que des valeurs entières sur $\mathcal{A}_{N/K}$. En effet, si x et y appartiennent à $\mathcal{A}_{N/K}$, alors $xy \in \mathcal{D}_{N/K}^{-1}$ et, par définition de la codifférente, $\mathrm{Tr}_{N/K}(xy) \in \mathcal{O}_K$. Il s'ensuit que $\mathcal{A}_{N/K}$ muni de la forme trace est un réseau entier. On le note $(\mathcal{A}_{N/K}, \mathrm{Tr})$.

Le dual d'un idéal I de $\mathcal{O}_N$ pour la forme trace est défini par :

$$I^\sharp = \{x \in N,\ \forall\, y \in I,\ \mathrm{Tr}(x, y) \in \mathcal{O}_K\}$$

Il découle de cette définition et de celle de la codifférente que $I^\sharp = I^{-1}\mathcal{D}_{N/K}^{-1}$ et donc que $I^\sharp$ n'est égal à I que pour $I = \mathcal{A}_{N/K}$, c'est-à-dire que $\mathcal{A}_{N/K}$ est le seul idéal auto-dual. Il s'ensuit que $(\mathcal{A}_{N/K}, \mathrm{Tr})$ est un réseau *unimodulaire* et si $K = \mathbb{Q}$, son discriminant est égal à 1.

Ce réseau a une propriété supplémentaire importante. Du fait que, pour tout $g \in G$ et tout couple $(x, y) \in N^2$, $\mathrm{Tr}(x^g, y^g) = \mathrm{Tr}(x, y)$, on déduit que la forme trace est *équivariante* et que le réseau $(\mathcal{A}_{N/K}, \mathrm{Tr})$ est stable sous l'action de G, ce qui en fait un G-réseau. Notons dès à présent que la structure de G-réseau de $\mathcal{A}_{N/K}$ contient sa structure de $\mathbb{Z}[G]$-module. On peut en particulier se demander si $(\mathcal{A}_{N/K}, \mathrm{Tr})$ est G-isométrique à $\mathbb{Z}[G]$ muni de sa forme standard q_G (celle qui fait de l'ensemble des éléments de G une base orthonormale), ce qui signifie qu'il existe une isométrie qui commute à l'action de G. Si la réponse est oui, alors $\mathcal{A}_{N/K}$ est un $\mathbb{Z}[G]$-module libre.

La question qui a suscité l'intérêt de B. Erez pour la racine carrée de la codifférente concernait sa structure de G-réseau. Il y apporte une réponse complète

dans le cas d'une extension abélienne N de $\mathbb{Q}$ dans [Er1] : $(\mathcal{A}_{N/\mathbb{Q}}, \mathrm{Tr})$ est G-isométrique à $(\mathbb{Z}[G], q_G)$ si et seulement si $N/\mathbb{Q}$ est faiblement ramifiée (ce qui entraîne que $\mathcal{A}_{N/K}$ est un $\mathbb{Z}[G]$-module libre). Il revient sur ce problème avec M.J. Taylor dans le cadre général d'une extension finie galoisienne de corps de nombres N/K de groupe de Galois G dans [ErT]. Le principal résultat qui y est démontré est que, si l'extension est modérée, alors $(\mathcal{A}_{N/K}, \mathrm{Tr})$ est stablement G-isométrique à $(\mathbb{Z}[G], q_G)$, c'est-à-dire qu'ils deviennent isométriques après somme orthogonale de chacun avec un même réseau standard.

On présente dans le chapitre 5 des calculs explicites du réseau associé à la racine carrée de la codifférente d'extensions faiblement ramifiées, provenant notamment de la famille infinie de la partie 2.3.

3.1.3 Interprétation en terme de structure hermitienne

Une autre façon de voir le réseau $(\mathcal{A}_{N/K}, \mathrm{Tr})$ est de considérer la forme hermitienne associée à la trace :

$$\begin{array}{rccc} t_{N/K} \ : & N \times N & \longrightarrow & K[G] \\ & (x,y) & \longmapsto & \sum_{g\in G} \mathrm{Tr}_{N/K}(xy^g)g^{-1} \end{array}$$

tandis que l'on munit $K[G]$ de la forme hermitienne associée à la multiplication :

$$\begin{array}{rccc} m_G \ : & K[G] \times K[G] & \longrightarrow & K[G] \\ & (x,y) & \longmapsto & \overline{x}y \end{array}$$

où $\overline{x}$ est induit sur $K[G]$ par l'application inverse de G dans lui-même. $\mathcal{A}_{N/K}$ muni de $t_{N/K}$ et $\mathbb{Z}[G]$ muni de m_G sont des modules hermitiens dont on peut comparer la structure. Il n'y a qu'un changement de vocabulaire entre le paragraphe précédent et celui-ci. En particulier, les réseaux $(\mathcal{A}_{N/K}, \mathrm{Tr})$ et $(\mathbb{Z}[G], q_G)$ sont G-isométriques si et seulement si les modules hermitiens $(\mathcal{A}_{N/K}, t_{N/K})$ et $(\mathcal{O}_K[G], m_G)$ sont isomorphes.

Le principal résultat concernant la structure hermitienne de la racine carrée de la codifférente est prouvé dans [ErT] à l'aide de techniques pour lesquelles l'interprétation en terme de module hermitien est préférable à celle en terme de réseau. Il sera présenté et illustré dans le chapitre 5.

3.2 Hom-description du groupe des classes

Dans toute la suite, N/K est une extension finie galoisienne de degré impair, de groupe de Galois G, faiblement ramifiée. Les groupes d'idèles qu'on va être amené à considérer faisant intervenir à la fois les places ultramétriques et les places archimédiennes du corps de nombres M concerné, on adopte la convention suivante.

Notation 3.2.1 Un *premier* de M désigne un représentant d'une place quelconque de M, ultramétrique ou archimédienne ; un *idéal premier* (resp. *nombre premier*) de $\mathcal{O}_M$ (resp. $\mathbb{Z}$) est un représentant d'une place ultramétrique de M (resp. $\mathbb{Q}$).

3.2.1 Le groupe des classes

On donne ici quelques précisions concernant le groupe des classes. On se réfère à la définition donnée dans [Frö], I.2.

Soit H un groupe fini, K un corps de nombres et Λ un *ordre* de $K[H]$, c'est-à-dire un sous-anneau de $K[H]$ contenant 1, de type fini sur l'anneau d'entiers $\mathcal{O}_K$ et tel que $\Lambda \otimes_{\mathcal{O}_K} K = K[H]$. On sera par exemple amené à considérer les cas $\Lambda = \mathcal{O}_K[G]$, $\Lambda = \mathbb{Z}[G]$ ou encore Λ égal à un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$.

Un Λ-module X de type fini est dit *localement libre* si, pour tout premier $\wp$ de K, le $\Lambda_\wp$-module $X_\wp = X \otimes_\Lambda \Lambda_\wp$ est libre. Le rang de X est, par définition, le rang du $K[H]$-module libre $X \otimes_{\mathcal{O}_K} K$. Il est fini et égal au rang de $X_\wp$ sur $\mathcal{O}_\wp[H]$ pour tout $\wp$. Ainsi, lorsque N/K est faiblement ramifiée, on sait par le théorème 3.1.1 que la racine carrée de la codifférente $\mathcal{A}_{N/K}$ est un $\mathbb{Z}[G]$-module localement libre de rang $[K : \mathbb{Q}]$.

On introduit alors le groupe de Grothendieck $\mathcal{K}_0(\Lambda)$. C'est le groupe abélien dont les générateurs sont les classes d'isomorphismes de Λ-modules localement libres (notées $[X]$) avec les relations :

$$[X \oplus Y] = [X] + [Y]$$

L'application $\mathbb{N} \to \mathcal{K}_0(\Lambda)$ définie par $n \mapsto [\Lambda^n]$ s'étend en un homomorphisme $\mathbb{Z} \to \mathcal{K}_0(\Lambda)$. Le groupe des classes $\mathrm{Cl}(\Lambda)$ est alors défini par la suite exacte :

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{K}_0(\Lambda) \longrightarrow \mathrm{Cl}(\Lambda) \longrightarrow 1$$

Cette suite exacte est scindée. Le rang d'un Λ-module X induit une application $\mathcal{K}_0(\Lambda) \to \mathbb{Z} \to 0$ dont le noyau est $\mathrm{Cl}(\Lambda)$ (voir [Frö] II.1). On note (X) l'image de $[X]$ dans $\mathrm{Cl}(\Lambda)$.

Lorsque deux $\mathbb{Z}[H]$-modules localement libres X et Y ont même rang et même classe dans $\mathrm{Cl}(\mathbb{Z}[H])$, ils sont dits *stablement isomorphes*. On a alors l'isomorphisme de $\mathbb{Z}[H]$-modules :

$$X \oplus \mathbb{Z}[H] \simeq Y \oplus \mathbb{Z}[H]$$

Ceci n'implique que X et Y sont isomorphes que sous certaines conditions (de simplification), par exemple lorsque l'ordre de H est impair (voir la note 2 de [Frö] p. 50), ce qui sera le cas pour $H = G$. La liberté de $\mathcal{A}_{N/K}$ comme $\mathbb{Z}[G]$-module et la trivialité de la classe $(\mathcal{A}_{N/K})$ dans $\mathrm{Cl}(\mathbb{Z}[G])$ sont donc équivalentes. On a maintenant besoin d'une description plus explicite du groupe des classes, c'est l'objet du prochain paragraphe.

3.2.2 Hom-description de Fröhlich

Pour tout ordre Λ de $\mathbb{Q}[G]$, on a un isomorphisme de groupes :

$$\mathrm{Cl}(\Lambda) \simeq \frac{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^*)\mathrm{Det}(\mathcal{U}(\Lambda))} \tag{3.1}$$

où, ayant fixé une clôture algébrique $\mathbb{Q}^c$ de $\mathbb{Q}$, R_G est le groupe additif des caractères virtuels de G dans $\mathbb{Q}^c$, $E \subset \mathbb{Q}^c$ un corps de nombres "suffisamment gros" pour contenir les valeurs des fonctions de R_G considérées, $J(E)$ désigne le groupe des idèles de E, dans lequel E^* est plongé diagonalement, $\Omega_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ et $\mathcal{U}(\Lambda) = \prod_l \Lambda_l^*$, l parcourant l'ensemble des premiers de $\mathbb{Q}$. On rappelle brièvement la définition de l'application Det sur $\mathbb{Q}_l[G]^*$ (pour le cas général, voir [Frö], I.2).

$$\begin{array}{rccc} \mathrm{Det}\ : & \mathbb{Q}_l[G]^* & \longrightarrow & \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, (E \otimes_{\mathbb{Q}} \mathbb{Q}_l)^*) \\ & b = \sum_G b_g g & \longmapsto & \mathrm{Det}(b) \end{array}$$

où $\mathrm{Det}(b)$ est défini sur les caractères χ provenant d'une représentation T de G par :

$$\mathrm{Det}_\chi(b) = \det\Big(\sum_G b_g T(g)\Big)$$

Le groupe $\mathrm{Det}(\mathcal{U}(\Lambda))$ est difficile à décrire explicitement en général. Néanmoins, on sait le faire lorsque Λ est un ordre maximal. On note $J_l(E)$ le produit des complétés de E en les premiers qui divisent l et $U_l(E)$ son groupe d'unités. On a alors le résultat suivant ([Frö] I proposition 2.2).

Proposition 3.2.2 *Soit $\mathcal{M}$ un ordre maximal de $\mathbb{Q}[G]$. Alors pour tout nombre premier l, on a l'égalité :*

$$\mathrm{Det}(\mathcal{M}_l^*) = \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, U_l(E))$$

Lorsque l est premier à l'ordre de $|G|$, $\mathbb{Z}_l[G]$ est un ordre maximal de $\mathbb{Q}_l[G]$. On a donc :

$$(l, |G|) = 1 \ \Rightarrow\ \mathrm{Det}(\mathbb{Z}_l[G]^*) = \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, U_l(E)) \tag{3.2}$$

Soit $\mathcal{M}$ un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$. La proposition 3.2.2 nous permet via (3.1) de disposer d'une bonne description de $\mathrm{Cl}(\mathcal{M})$. En fait, la suite exacte de la remarque 3.1.2 peut se réécrire dans notre situation de la façon suivante (voir [Frö] I, 2.17). On note que puisque G est d'ordre impair, il n'a pas de caractère symplectique irréductible.

$$1 \to D(\mathbb{Z}[G]) \to \mathrm{Cl}(\mathbb{Z}[G]) \to \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, E^*)\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, U(E))} \to 1 \tag{3.3}$$

La liberté de $\mathcal{A}_{N/K} \otimes \mathcal{M}$ comme $\mathcal{M}$-module se traduit alors par le fait que, si $f \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J(E))$ correspond à $(\mathcal{A}_{N/K})$ via l'isomorphisme (3.1), alors f est dans le dénominateur du dernier terme de (3.3).

La Hom-description a de très bonnes propriétés fonctorielles. Ainsi, les changements de groupes induisent des homomorphismes naturels sur les groupes de classes, qui se traduisent bien dans la description de Fröhlich. En particulier, si H désigne un sous-groupe de G, l'extension des scalaires induit un homomorphisme de $\mathrm{Cl}(\mathbb{Z}[H])$ dans $\mathrm{Cl}(\mathbb{Z}[G])$. Il découle par passage au quotient de l'homomorphisme

$$\mathrm{Ind}_H^G\ :\ \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_H, J(E)) \longrightarrow \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J(E))$$

défini par :

$$\mathrm{Ind}_H^G(f)(\chi) = f(\mathrm{Res}_H^G(\chi)), \quad \forall \chi \in R_G$$

où Res_H^G désigne la restriction de caractères de G à H. On utilisera souvent l'inclusion suivante, pour toute extension finie M de $\mathbb{Q}_l$ d'anneau d'entiers $\mathcal{O}_M$:

$$\mathrm{Ind}_H^G(\mathrm{Det}(\mathcal{O}_M[H]^*)) \subset \mathrm{Det}(\mathcal{O}_M[G]^*) \tag{3.4}$$

On peut se reporter à [Frö], II, Théorème 12, pour plus de précisions.

3.2.3 Un représentant semi-local

On décrit maintenant un élément f de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$ qui représente la classe $(\mathcal{A}_{N/K})$ (donc $f \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^*)\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, U(E))$ d'après ce qui précède). Puisque N/K est faiblement ramifiée, on sait par le théorème 3.1.1 que $\mathcal{A}_{N/K}$ est un $\mathcal{O}_K[G]$-module localement libre, ce qui signifie que, pour tout premier ℓ de K, il existe une base a_ℓ du $\mathcal{O}_{K_\ell}[G]$-module $\mathcal{A}_\ell = \mathcal{A}_{N/K} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\ell}$. On note que

$$a_\ell \in N_\ell = N \otimes_K K_\ell \simeq \prod_{\mathcal{L}|\ell} N_\mathcal{L}$$

et donc, si l est la caractéristique résiduelle de K_ℓ, on a $a_\ell \in J_l(N)$. On définit maintenant la résolvante $(a_\ell \,|\, \chi) \in J_l(E)$ d'un caractère $\chi \in R_G$. Si χ est le caractère de la représentation T de G, on pose :

$$(a_\ell \,|\, \chi) = \mathrm{Det}\Big(\sum_{g\in G} (a_\ell)^g T(g^{-1})\Big)$$

et on vérifie que le résultat ne dépend que de χ. Soit Δ un système de représentants de $\Omega_\mathbb{Q}/\Omega_K$ dans $\Omega_\mathbb{Q}$, on pose :

$$\mathcal{N}_{K/\mathbb{Q}}(a_\ell \,|\, \chi) = \prod_{\delta\in\Delta} (a_\ell \,|\, \chi^{\delta^{-1}})^\delta$$

Cette *norme-résolvante* dépend du système de représentants Δ choisi. Cependant, la proposition 4.4 de [Frö] montre que, modulo le dénominateur de (3.1), la dépendance disparaît.

A tout caractère χ de G, on associe l'idèle $R_\ell(\chi)$ de E dont la composante semi-locale en $J_q(E)$ au-dessus d'un premier q de $\mathbb{Q}$ est donnée par :

$$R_\ell(\chi)_q = \begin{cases} 1 & \text{si } q \neq l \\ \mathcal{N}_{K/\mathbb{Q}}(a_\ell \,|\, \chi) & \text{si } q = l \end{cases}$$

On désigne par $T_\ell(\chi)$ l'élément de E^* défini par :

$$T_\ell(\chi) = \begin{cases} 1 & \text{si } \ell \text{ est une place archimédienne,} \\ \tau_\ell(\chi) & \text{sinon.} \end{cases}$$

où τ_ℓ désigne la somme de Gauss locale associée au caractère χ. On peut se reporter à [M3] ou à [Frö] III pour la définition des sommes de Gauss, ainsi qu'à la partie 3.3 de cette thèse.

On injecte E^* diagonalement dans $J(E)$, ce qui permet pour tout ℓ de considérer $T_\ell(\chi)$ comme un élément de $J(E)$. On sait (grâce aux théorèmes 4 et 20 de [Frö]) que l'application $\prod_\ell R_\ell T_\ell^{-1}$ est un représentant de $(\mathcal{A}_{N/K})$, mais on le modifie pour pouvoir utiliser les résultats de [Tay1] et de [Er3]. Lorsque ℓ est modérément ramifié dans N/K, on note τ_ℓ^* la somme de Gauss locale modifiée (voir [Tay1] 3.9) et T_ℓ^* l'application de R_G dans E^* correspondante. A l'instar de [Er3] (voir sa remarque 7.4 pour une explication heuristique), on introduit la seconde opération d'Adams $\psi = \psi_2$: c'est l'application de R_G dans lui-même définie par $\psi(\chi)(g) = \chi(g^2)$. Elle induit par dualité un endomorphisme Ψ sur $\mathrm{Hom}(R_G, J(E))$. Soit S_W l'ensemble des premiers de $\mathcal{O}_K$ qui sont sauvagement ramifiés dans N/K. On désigne par $\widetilde{T}_\ell$ si $\ell \in S_W$ (resp. $\widetilde{T}_\ell^*$ si $\ell \notin S_W$) l'application $\Psi(T_\ell)/T_\ell$ (resp. $\Psi(T_\ell^*)/T_\ell^*$). On déduit de [Tay1], partie 3 et de [Er3], Théorème 3.6 :

Proposition 3.2.3 *Soit $f_{(\ell)}$ (resp. $f^*_{(\ell)}$) l'application $R_\ell \widetilde{T}_\ell^{-1}$ (resp. $R_\ell \widetilde{T}_\ell^{*-1}$) pour $\ell \in S_W$ (resp. $\ell \notin S_W$). Alors :*

$$f = \prod_{\ell \in S_W} f_{(\ell)} \prod_{\ell \notin S_W} f^*_{(\ell)}$$

est un représentant de $(\mathcal{A}_{N/K})$ dans $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$.

Pour tout premier l de $\mathbb{Q}$ et toute application $g \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$, on note $g_l \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J_l(E))$ la l-composante de g. On déduit alors de la remarque 3.1.2, de (3.2) et de (3.3) le corollaire suivant.

Corollaire 3.2.4 *On suppose l premier à $|G|$, alors $f_l \in \mathrm{Det}(\mathbb{Z}_l[G]^*)$.*

Au vu de l'isomorphisme (3.1), on peut donc se concentrer, pour étudier la classe $(\mathcal{A}_{N/K})$, sur les diviseurs premiers p de l'ordre de G. La présentation des résultats est grandement facilitée par l'isomorphisme qui fait l'objet du prochain paragraphe.

3.2.4 Passage du semi-local au local

Ce paragraphe reprend le début de la partie 3 de [CNT2]. On fixe pour tout premier p un plongement :

$$j_p : \mathbb{Q}^c \hookrightarrow \mathbb{Q}_p^c.$$

Si M est un sous-corps de $\mathbb{Q}^c$, on désigne par M_p la fermeture de $j_p(M)$ dans $\mathbb{Q}_p^c$ et on note encore j_p l'homomorphisme d'algèbres induit :

$$M \otimes_\mathbb{Q} \mathbb{Q}_p \longrightarrow\!\!\!\!\!\rightarrow M_p$$

La restriction de j_p à K, N et E y définit des idéaux premiers que l'on note respectivement $\wp$, $\mathcal{P}$ et $\mathfrak{p}$. Ainsi j_p induit-il des isomorphismes de corps :

$$K_\wp \xrightarrow{\sim} K_p \ , \quad N_\mathcal{P} \xrightarrow{\sim} N_p \ , \quad E_\mathfrak{p} \xrightarrow{\sim} E_p$$

Soit $G(p)$ le groupe de décomposition de $\mathcal{P}$ dans N/K. C'est un sous-groupe de $\mathrm{Gal}(N/K)$. On associe à j_p un plongement j_p^* de $\Omega_{\mathbb{Q}_p}$ dans $\Omega_{\mathbb{Q}}$ en posant, pour tout $x \in \mathbb{Q}^c$ et $\omega \in \Omega_{\mathbb{Q}_p}$

$$x^{j_p^*(\omega)} = j_p^{-1}(j_p(x)^\omega)$$

On obtient un morphisme injectif $\Omega_{\mathbb{Q}_p} \hookrightarrow \Omega_{\mathbb{Q}}$ qui permet d'identifier les groupes $\mathrm{Gal}(N_p/K_p)$ et $G(p)$. Soit $R_{G,p}$ l'anneau des caractères virtuels de G dans $\mathbb{Q}_p^c$, alors l'application $\chi \mapsto \chi^{j_p}$ est un isomorphisme d'anneaux de R_G sur $R_{G,p}$. On obtient ainsi un homomorphisme de groupes encore noté j_p^* :

$$\begin{array}{rccc} j_p^* \ : & \mathrm{Hom}(R_G, J_p(E)) & \longrightarrow & \mathrm{Hom}(R_{G,p}, E_p^*) \\ & f & \longmapsto & \left(\chi \mapsto f(\chi^{j_p^{-1}})^{j_p}\right) \end{array} \tag{3.5}$$

Il induit par restriction un homomorphisme :

$$\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J_p(E)) \longrightarrow \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G,p}, E_p^*)$$

lequel se factorise en l'isomorphisme de groupes ([Frö], II, lemme 2.1) :

$$j_p^* \ : \ \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J_p(E))}{\mathrm{Det}(\mathbb{Z}_p[G]^*)} \ \simeq \ \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G,p}, E_p^*)}{\mathrm{Det}(\mathbb{Z}_p[G]^*)} \tag{3.6}$$

A l'aide du corollaire 3.2.4, on en tire immédiatement la condition suffisante suivante pour la trivialité de $(\mathcal{A}_{N/K})$:

$$\forall\, p \text{ diviseur premier de } |G|,\ j_p^*(f_p) \in \mathrm{Det}(\mathbb{Z}_p[G]^*)$$

Cette condition n'est pas nécessaire car on sait que le représentant f de $(\mathcal{A}_{N/K})$ peut être remplacé par son produit avec une application de $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, E^*)$. Cette propriété se traduit en termes locaux par le résultat suivant qui sera fort utile.

Lemme 3.2.5 *Soient p un nombre premier et $k \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, \mathcal{O}_E^*)$. On note k_l la composée de k avec le plongement diagonal $E^* \hookrightarrow J_l(E)$ et on suppose que pour tout premier l distinct de p :*

(i) $j_l^*(k_l) \in \mathrm{Det}(\mathbb{Z}_l[G]^*)$ *et* $j_l^*(f_l) \in \mathrm{Det}(\mathbb{Z}_l[G]^*)$,

(ii) $j_p^*\left(\dfrac{f_p}{k_p}\right) \in \mathrm{Det}(\mathbb{Z}_p[G]^*)$.

Alors $(\mathcal{A}_{N/K}) = 1$.

3.2.5 Un représentant local

On voit que le cœur du problème réside dans l'étude de $j_p^*(f_p)$ pour les diviseurs premiers p de l'ordre de G. On fixe un tel p et on veut déterminer l'image du représentant semi-local f_p de $(\mathcal{A}_{N/K})$ par j_p^*. Comme f_p est le produit de norme-résolvantes par des sommes de Gauss locales, on étudie l'image de ces facteurs. On note encore $\wp$ (resp. $\mathcal{P}$) le premier de K (resp. N) défini par j_p.

L'élément semi-local $a_\wp$, base de $\mathcal{A}_\wp$ comme $\mathcal{O}_{K_p}[G]$-module, peut être choisi de sorte que, via l'isomorphisme :

$$\mathcal{A}_\wp \simeq \prod_{\mathcal{P}'/\wp} \mathcal{A}_{N_{\mathcal{P}'}/K_\wp}$$

on ait $a_\wp = (a_{\mathcal{P}'})_{\mathcal{P}'/\wp}$ avec $a_{\mathcal{P}'} = 0$ pour $\mathcal{P}' \neq \mathcal{P}$ tandis que $a_\mathcal{P} = \alpha_p$ est une base de $\mathcal{A}_{N_p/K_p}$ comme $\mathcal{O}_{K_p}[G(p)]$-module (voir [Er3] partie 5). On sait par le théorème 19 de [Frö] que, pour tout $\chi \in R_G$, l'égalité suivante est vraie modulo le dénominateur de (3.1) :

$$\mathcal{N}_{K/\mathbb{Q}}(a_\wp \,|\, \chi)^{j_p} = \mathcal{N}_{K_p/\mathbb{Q}_p}(\alpha_p \,|\, \chi_p^{j_p})$$

où χ_p désigne la restriction de χ à $G(p)$. On tire alors de (3.5) :

$$j_p^*\big(\mathcal{N}_{K/\mathbb{Q}}(a_\wp \,|\, .\,)\big) = \mathrm{Ind}_{G(p)}^G \mathcal{N}_{K_p/\mathbb{Q}_p}(\alpha_p \,|\, .\,)$$

On examine maintenant $j_p^*(\widetilde{T}_\ell)$. Il découle de la définition des sommes de Gauss locales que, pour tout $\chi \in R_{G,p}$:

$$j_p^*(\widetilde{T}_\ell)(\chi) = \widetilde{T}_\ell(\chi l^{j_p^{-1}})^{j_p}$$

On en déduit que $j_p^*(\widetilde{T}_l) \in \mathrm{Ind}_{G(l)}^G(\mathrm{Hom}(R_{G(l),p}, E_p^*))$. On a un résultat analogue pour $j_p^*(\widetilde{T}_l^*)$.

3.3 Etude des sommes de Gauss

On a vu plus haut que les sommes de Gauss sont un ingrédient essentiel pour la description et l'étude de la classe de la racine carrée de la codifférente dans le groupe des classes $\mathrm{Cl}(\mathbb{Z}[G])$. On revient ici sur leur définition. Dans le cas où elles sont appliquées à un caractère abélien, elles sont données par une formule explicite (3.7), mais celle-ci ne permet pas toujours un calcul direct. C'est pourquoi on dérive de résultats de [Tat2] une expression simplifiée pour les sommes de Gauss locales de caractères abéliens, qui sera utilisée dans la partie 3.4.

On rappelle ensuite par quel procédé on étend la définition des sommes de Gauss locales à tous les caractères du groupe des représentations virtuelles R_G. On n'a plus alors de formule explicite pour la somme de Gauss, qui est caractérisée par certaines propriétés. Cela permet néanmoins d'obtenir la formule d'action galoisienne sur les sommes de Gauss locales que l'on énonce à cause de son importance dans la suite.

3.3.1 La somme de Gauss d'un caractère abélien

On reprend quelques éléments de l'introduction de l'article [Tat2] de Tate. L'équation fonctionnelle de la fonction L d'un corps de nombres K, complétée

par des facteurs adéquats aux places archimédiennes et évaluée en une représentation ϕ du groupe de Galois G d'une extension finie L de K, fait apparaître une constante (par rapport à la variable complexe) $W(\phi)$. Langlands et Deligne ont montré que cette constante se décompose en un produit de facteurs locaux :

$$W(\phi) = \prod_{\wp} W(\phi_\wp)$$

où le produit est indicé par les premiers $\wp$ de K et $\phi_\wp$ est la restriction de ϕ au groupe de décomposition en $\wp$ dans L/K (défini à conjugaison près, ce qui suffit pour définir $W(\phi_\wp)$).

Plus précisément, lorsque ϕ est une représentation de G de degré 1, on peut la voir comme un caractère de Hecke, c'est-à-dire un caractère d'ordre fini du groupe d'idèles $J(K)$ trivial sur K^*. Pour toute place $\wp$ de K, $\phi_\wp$ est la restriction de ϕ à $K_\wp^*$. On peut alors déterminer explicitement la constante locale $W(\phi_\wp)$. En particulier, si $\phi_\wp$ est un caractère modéré, alors $W(\phi_\wp)$ est le produit d'une puissance de la caractéristique résiduelle de $K_\wp$ par une expression qui s'identifie à une somme de Gauss "classique" (ou de congruence). Pour des détails sur ce point, on peut consulter le chapitre 5 de [Er4], notamment la proposition 3.3.c.

On en vient à la définition de la constante locale associée à un caractère abélien. On définit chemin faisant la somme de Gauss locale. Soient p un nombre premier de $\mathbb{Z}$ et κ une extension finie de $\mathbb{Q}_p$, d'anneau de valuation $\mathcal{O}_\kappa$. On définit le caractère additif canonique ψ_κ de κ comme étant l'application composée :

$$\kappa \xrightarrow{\mathrm{Tr}_{\kappa/\mathbb{Q}_p}} \mathbb{Q}_p \longrightarrow\!\!\!\!\rightarrow \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{\mathrm{e}^{2i\pi\cdot}} (\mathbb{Q}^c)^*$$

En particulier, on note $\psi_p = \psi_{\mathbb{Q}_p}$. Soit χ un caractère abélien de κ^*, le conducteur de χ est le plus grand idéal $f(\chi)$ de $\mathcal{O}_\kappa$ tel que χ soit trivial sur $1 + f(\chi)$. Si $f(\chi) = \mathcal{O}_\kappa$, on convient que $1 + f(\chi) = \mathcal{O}_\kappa^*$. A l'instar de [Tat2], on note $\mathcal{D}(\chi) = f(\chi)\mathcal{D}_\kappa$, où $\mathcal{D}_\kappa = \mathcal{D}_{\kappa/\mathbb{Q}_p}$ est la différente absolue de κ et on choisit $d \in \kappa$ tel que $d\mathcal{O}_\kappa = \mathcal{D}(\chi)$. La somme de Gauss en χ est définie par la formule :

$$\tau_\kappa(\chi) = \sum_x \chi(d^{-1}x)\psi_\kappa(d^{-1}x) \tag{3.7}$$

où x décrit un ensemble de représentants de $\mathcal{O}_\kappa^*$ modulo $1 + f(\chi)$. On vérifie que cette quantité ne dépend pas des choix effectués (voir [M3] p. 29). Si χ est non ramifié, c'est-à-dire de conducteur $f(\chi) = \mathcal{O}_\kappa$, la somme se réduit à un seul terme $\tau_\kappa(\chi) = \chi(\mathcal{D}_\kappa^{-1})$. La constante locale est reliée à la somme de Gauss par la formule :

$$W(\chi) = \mathrm{N}_{\kappa/\mathbb{Q}_p}(f(\chi))^{-1/2}\tau_\kappa(\chi^{-1}) \tag{3.8}$$

3.3.2 Exemple de calcul d'une somme de Gauss

On calcule ici la somme de Gauss d'un caractère abélien $\widetilde{\chi}$ d'ordre fini de $\mathbb{Q}_p^*$ de conducteur $p^2\mathbb{Z}_p$ et d'ordre 1 ou p, où p est un premier impair. Un tel

caractère se factorise, via l'application d'Artin de $\mathbb{Q}_p^*$, en un caractère χ du groupe de Galois Γ d'une extension abélienne faiblement ramifiée $\nu/\mathbb{Q}_p$:

$$\mathbb{Q}_p^* \longrightarrow\!\!\!\!\!\rightarrow G \xrightarrow{\chi} (\mathbb{Q}_p^c)^*$$

Réciproquement, tout caractère χ de Γ composé avec l'application d'Artin de l'extension $\nu/\mathbb{Q}_p$ donne un caractère abélien $\widetilde{\chi}$ d'ordre fini de $\mathbb{Q}_p^*$. Vu le lemme 1.3.4 du chapitre 1, le conducteur de $\widetilde{\chi}$ est $p^2\,\mathbb{Z}_p$ si χ est ramifié, $\mathbb{Z}_p$ sinon. La formule (3.7) donne :

$$\tau_p(\chi) = \begin{cases} 1 & \text{si } \chi \text{ est non ramifié} \\ \widetilde{\chi}(p)^{-2} \sum_x \widetilde{\chi}(x)\psi_p(p^{-2}x) & \text{si } \chi \text{ est ramifié} \end{cases}$$

où x décrit un système de représentants de $\mathbb{Z}_p^*/(1+p^2\mathbb{Z}_p)$. On suppose maintenant que χ est ramifié. On écrit $x = \sum_{i\geq 0} x_i p^i$ avec $0 \leq x_i \leq p-1$, et $0 < u = x_0 < p$. Soient $0 \leq w \leq p-1$ et $y \in \mathbb{Z}_p$ tels que $x/u = 1 + pw + p^2 y$, alors :

$$x = u(1+pw)\left(1 + p^2 \frac{y}{u(1+pw)}\right)$$

et, comme $\widetilde{\chi}$ est trivial sur $1+p^2\mathbb{Z}_p$, $\widetilde{\chi}(x) = \widetilde{\chi}(u(1+pw)) = \widetilde{\chi}(u)\widetilde{\chi}(1+pw)$. On pose $\zeta = \psi_p(1/p^2)$ (c'est une racine primitive p^2-ième de l'unité). On a :

$$\tau_p(\chi) = \widetilde{\chi}(p^{-2}) \sum_{\substack{1\leq u\leq p-1 \\ 0\leq w\leq p-1}} \widetilde{\chi}(u)\widetilde{\chi}(1+pw)\zeta^u \left(\zeta^{pu}\right)^w$$

Puisque $1+pw \equiv (1+p)^w \bmod p^2\mathbb{Z}_p$, alors $\widetilde{\chi}(1+pw) = \widetilde{\chi}(1+p)^w$, si bien que :

$$\tau_p(\chi) = \widetilde{\chi}(p^{-2}) \sum_{1\leq u\leq p-1} \widetilde{\chi}(u)\zeta^u B(u,\chi)$$

avec $B(u,\chi) = \sum_{0\leq w\leq p-1} \left(\widetilde{\chi}(1+p)\zeta^{pu}\right)^w$. Comme $\widetilde{\chi}$ est trivial sur $1+p^2\mathbb{Z}_p$ et non identiquement égal à 1 sur $1+p\mathbb{Z}_p$, $\widetilde{\chi}(1+p)$ est une racine primitive p-ième de l'unité. Puisque ζ^{-p} en est une aussi, il existe un unique entier $u(\chi)$ avec $1 \leq u(\chi) \leq p-1$, tel que :

$$\widetilde{\chi}(1+p) = \zeta^{-pu(\chi)} \tag{3.9}$$

On a donc $B(u,\chi) = 0$ (resp. p) si $u \neq u(\chi)$ (resp. si $u = u(\chi)$), et on obtient :

$$\tau_p(\chi) = \begin{cases} 1 & \text{si } \chi \text{ est non ramifié} \\ p\,\widetilde{\chi}(u(\chi)/p^2)\,\zeta^{u(\chi)} & \text{si } \chi \text{ est ramifié} \end{cases} \tag{3.10}$$

3.3.3 Propriétés des sommes de Gauss abéliennes

Ce paragraphe est une adaptation aux sommes de Gauss de caractères abéliens des résultats relatifs à la constante locale de la première partie de [Tat2]. On note encore κ une extension finie de $\mathbb{Q}_p$ avec p premier impair et v_κ la valuation normalisée de κ ; on se donne une uniformisante π. Le résultat qui suit permet d'obtenir une expression simplifiée de la somme de Gauss.

Proposition 3.3.1 *Soient χ un caractère d'ordre fini de κ^*, $\overline{\chi}$ son inverse et $\mathfrak{a}$ un idéal de $\mathcal{O}_\kappa$ tel que $\mathfrak{a}^2 \mid f(\chi)$.*

(i) Il existe $c = c(\chi) \in \kappa$ tel que $c\mathcal{O}_\kappa = \mathcal{D}(\chi)$ et, pour tout $y \in \mathfrak{b} = \mathfrak{a}^{-1} f(\chi)$,

$$\overline{\chi}(1+y) = \psi_\kappa(c^{-1}y)$$

(ii) Pour un tel c, on a :

$$\tau_\kappa(\chi) = \mathrm{N}_{\kappa/\mathbb{Q}_p}(\mathfrak{a}) \sum_x \chi(c^{-1}x)\psi_\kappa(c^{-1}x)$$

où x parcourt un système de représentants de $1+\mathfrak{a}$ modulo $1+\mathfrak{b}$.

On en déduit l'expression simplifiée suivante pour la somme de Gauss d'un caractère dont le conducteur est de valuation paire, en particulier pour un caractère non ramifié ou sauvagement et faiblement ramifié.

Corollaire 3.3.2 *Soient χ un caractère d'ordre fini de κ^* tel que $v_\kappa(f(\chi)) = 2n$ avec n entier et $c \in \kappa$ vérifiant la condition (i) de la proposition ci-dessus relativement à χ et $\mathfrak{a} = (\pi)^n$. Alors la somme de Gauss de κ en χ s'écrit :*

$$\tau_\kappa(\chi) = \mathrm{N}_{\kappa/\mathbb{Q}_p}(f(\chi))^{1/2}\chi(c^{-1})\psi_\kappa(c^{-1})$$

Preuve. On remarque que $\mathfrak{b} = \mathfrak{a}$, si bien que la somme est réduite à un seul terme. ∎

Remarque 3.3.3 Cette formule généralise celle du paragraphe 3.3.2. En effet, on voit facilement que $c(\chi) = p^2 u(\chi)^{-1}$ vérifie la condition (i) de la proposition 3.3.1 relativement au caractère $\widetilde{\chi}$ de $\mathbb{Q}_p^*$ et à $\mathfrak{a} = p\mathbb{Z}_p$. De même, si χ est non ramifié, $c \in \mathcal{D}_\kappa^{-1}$, donc $\psi_\kappa(c^{-1}) = 1$ et on retrouve que $\tau_\kappa(\chi) = \chi(\mathcal{D}_\kappa^{-1})$. Le corollaire 1 de [Tat2], page 96, montre plus généralement que $W(\chi)$ est une racine de l'unité dès que $v_\kappa(f(\chi)) \neq 1$.

On démontre maintenant la proposition 3.3.1. Sa preuve est calquée sur celle de la proposition 1 de [Tat2], pages 95-96.

Preuve. Si $\mathfrak{a} = \mathcal{O}_\kappa$, soit $c \in \kappa$ vérifiant $c\mathcal{O}_\kappa = \mathcal{D}(\chi)$, alors pour tout $y \in \mathfrak{b} = f(\chi) = f(\overline{\chi})$, $\overline{\chi}(1+y) = 1$ par définition de $f(\overline{\chi})$ et, comme $c^{-1}y \in \mathcal{D}_\kappa^{-1}$, on a $\mathrm{Tr}_{\kappa/\mathbb{Q}_p}(c^{-1}y) \in \mathbb{Z}_l$ donc $\psi_\kappa(c^{-1}y) = 1$ lui aussi. Quant à la formule qui donne la somme de Gauss, elle est dans ce cas identique à (3.7).

On suppose maintenant $\mathfrak{a} \neq \mathcal{O}_\kappa$. On voit que $(\pi) \mid \mathfrak{a} \mid \mathfrak{b} \mid f(\chi)$ et que, si y et y' appartiennent à $\mathfrak{b}$, yy' appartient à $f(\chi) = f(\overline{\chi})$. Il s'ensuit que :

$$\overline{\chi}(1+y)\overline{\chi}(1+y') = \overline{\chi}(1+y+y')$$

et donc $\lambda : y \mapsto \overline{\chi}(1+y)$ est un caractère additif de $\mathfrak{b}$. On peut prolonger λ à κ, obtenant ainsi un homomorphisme du dual de κ^+. Or on sait par le lemme 2.2.1 de [Tat1], page 308, que ψ_κ engendre $\widehat{\kappa^+}$ sur κ^+ par $x \mapsto (y \mapsto \psi_\kappa(xy))$.

Il s'ensuit qu'il existe $c = c(\chi) \in \kappa$ tel que $\lambda(y) = \psi_\kappa(c^{-1}y)$ pour tout $y \in \kappa$ et donc $\overline{\chi}(1+y) = \psi_\kappa(c^{-1}y)$ pour tout $y \in \mathfrak{b}$.

Comme $f(\chi)$ est strictement inclus dans $\mathfrak{b}$, on a $\pi^{-1}f(\chi) \subset \mathfrak{b}$. On en déduit que $y \mapsto \psi_\kappa(c^{-1}y)$ est trivial sur $f(\chi)$ mais pas sur $\pi^{-1}f(\chi)$. Or le conducteur de ψ_κ est $\mathcal{D}_\kappa^{-1}$, si bien que $c^{-1}f(\chi) = \mathcal{D}_\kappa^{-1}$ et donc $c\mathcal{O}_\kappa = f(\chi)\mathcal{D}_\kappa = \mathcal{D}(\chi)$. Le point (i) de la proposition est donc démontré.

On calcule maintenant la somme de Gauss. Puisque $c\mathcal{O}_\kappa = \mathcal{D}(\chi)$, on a par (3.7) :

$$\begin{aligned}
\tau_\kappa(\chi) &= \sum_{\substack{x \in \mathcal{O}_\kappa^* \\ \bmod 1+f(\chi)}} \chi(c^{-1}x)\psi_\kappa(c^{-1}x) \\
&= \sum_{\substack{z \in \mathcal{O}_\kappa^* \\ \bmod 1+\mathfrak{b}}} \sum_{\substack{y \in \mathfrak{b} \\ \bmod f(\chi)}} \chi(c^{-1}z(1+y))\psi_\kappa(c^{-1}z(1+y)) \\
&= \sum_z \Big(\chi(c^{-1}z)\psi_\kappa(c^{-1}z) \sum_y \psi_\kappa(c^{-1}y(z-1))\Big)
\end{aligned}$$

par définition de c et additivité de ψ_κ. Or $\sum_y \psi_\kappa(c^{-1}y(z-1)) = 0$ sauf si, pour tout $y \in \mathfrak{b} \bmod f(\chi)$, $\psi_\kappa(c^{-1}y(z-1)) = 1$, c'est-à-dire $c^{-1}y(z-1) \in \mathcal{D}_\kappa^{-1}$ ou encore $z - 1 \in \mathfrak{a}$. Dans ce cas,

$$\sum_y \psi_\kappa(c^{-1}y(z-1)) = \Big|\frac{\mathfrak{b}}{f(\chi)}\Big| = \Big|\frac{\pi^{v_\kappa(\mathfrak{b})}}{\pi^{v_\kappa(f(\chi))}}\Big| = \mathrm{N}_{\kappa/\mathbb{Q}_p}(\pi)^{v_\kappa(f(\chi))-v_\kappa(\mathfrak{b})} = \mathrm{N}_{\kappa/\mathbb{Q}_p}(\mathfrak{a})$$

et le point (ii) de la proposition en découle. ∎

Remarque 3.3.4 La preuve montre que la condition (i) peut être affaiblie tout en gardant les mêmes propriétés pour c.

1. si $\mathfrak{a} = \mathcal{O}_\kappa$, (i) et (ii) sont impliqués par :

$$(i') \quad \text{Soit } c \in \mathcal{O}_\kappa \text{ tel que } c\mathcal{O}_\kappa = \mathcal{D}(\chi)$$

2. si $\mathfrak{a} \neq \mathcal{O}_\kappa$, (i) et (ii) sont impliqués par :

$$(i'') \quad \text{Il existe } c \in \mathcal{O}_\kappa \text{ tel que, pour tout } y \in \mathfrak{b},\ \overline{\chi}(1+y) = \psi_\kappa(c^{-1}y)$$

Le résultat suivant n'apparaît pas dans [Tat2] mais il sera utile dans la suite. On note que la seconde opération d'Adams agit sur les caractères abéliens par $\psi(\chi) = \chi^2$.

Lemme 3.3.5 *Soient χ un caractère d'ordre fini de κ^* et $c(\chi) \in \kappa$ vérifiant la condition (i) de la proposition 3.3.1 relativement à χ et à un idéal $\mathfrak{a}$ dont le carré divise $f(\chi)$. Alors*

$$c(\psi(\chi)) = c(\chi)/2$$

vérifie la condition (i) de la proposition 3.3.1 relativement à $\psi(\chi)$ et à $\mathfrak{a}$.

Preuve. Il est clair que χ et χ^2 ont même conducteur. La vérification du premier terme de la condition (i) pour $c(\chi)/2$ relativement à $\psi(\chi)$ et à $\mathfrak{a}$ est alors immédiate puisque $2 \in \mathcal{O}_\kappa^*$. Soit $y \in \mathfrak{b} = \mathfrak{a}^{-1} f(\chi)$, on a $\overline{\psi(\chi)}(1+y) = \overline{\chi}(1+y)^2$, tandis que $\psi_\kappa((c(\chi)/2)^{-1}y) = \psi_\kappa(2c(\chi)^{-1}y) = \psi_\kappa(c(\chi)^{-1}y)^2$, d'où le résultat. ∎

On s'intéresse maintenant à la somme de Gauss d'un produit de deux caractères dont l'un est "moins ramifié" que l'autre (voir [Tat2] corollary 2 page 98).

Corollaire 3.3.6 *Soient χ, $\mathfrak{a}$ et c comme dans la proposition précédente. Soit ρ un caractère d'ordre fini de κ^* tel que $f(\rho) \mid \mathfrak{a}$. Alors $\tau_\kappa(\rho\chi) = \rho(c^{-1})\tau_\kappa(\chi)$. En particulier, si ρ est non ramifié, alors :*

$$\tau_\kappa(\rho\chi) = \rho(\mathcal{D}(\chi)^{-1})\tau_\kappa(\chi)$$

Preuve. On montre tout d'abord que la proposition 3.3.1 s'applique à $\rho\chi$ avec le même $\mathfrak{a}$ et le même c que pour χ. Comme $f(\rho) \mid \mathfrak{a} \mid f(\chi)$, on a $f(\rho\chi) = f(\chi)$. On voit donc que $\mathfrak{a}^2 \mid f(\rho\chi)$ et que $c\mathcal{O}_\kappa = \mathcal{D}(\rho\chi)$. De plus, puisque $\mathfrak{b} \subset \mathfrak{a} \subset f(\rho)$, on a $\overline{\rho}(1+y) = 1$ pour tout $y \in \mathfrak{b}$, si bien que c vérifie les conditions (i) de la proposition 3.3.1 relativement à $\mathfrak{a}$ et à $\rho\chi$. On en tire :

$$\tau_\kappa(\rho\chi) = \mathrm{N}_{\kappa/\mathbb{Q}_p}(\mathfrak{a}) \sum_{\substack{x \in 1+\mathfrak{a} \\ \mathrm{mod}\ 1+\mathfrak{b}}} \rho\chi(c^{-1}x)\psi_\kappa(c^{-1}x)$$

mais $\rho(x) = 1$ pour $x \in 1 + \mathfrak{a}$, ce qui achève la preuve du corollaire. ∎

3.3.4 Action galoisienne sur la somme de Gauss

Grâce à (3.7) et (3.8), la constante locale $W(\chi)$ est définie pour les caractères abéliens χ du groupe multiplicatif de toute extension finie κ de $\mathbb{Q}_p$. Via l'application d'Artin, ceux-ci correspondent aux représentations de degré 1 de Ω_κ. Comme l'équation fonctionnelle de la fonction L d'un corps de nombres est valable pour les représentations de tous degrés, l'existence de constantes locales n'est possible que si on peut étendre $W(\chi)$ à toutes les représentations (de degré fini) de Ω_κ. Il faut de plus que la fonction étendue ait de bonnes propriétés.

Plus précisément, soit κ une extension finie de $\mathbb{Q}_p$. On note $R(\kappa)$ l'ensemble des paires (ν, ρ) avec ν/κ extension finie et ρ représentation virtuelle de Ω_ν (c'est-à-dire une somme à cœfficients entiers de caractères irréductibles de Ω_ν, ou encore la différence de deux représentations linéaires de dimension finies de Ω_ν). Une fonction F définie sur les caractères d'ordre fini de ν^* pour toute extension finie ν de κ et à valeurs dans un groupe abélien A est dite *extensible* si elle peut être étendue à une fonction de $R(\kappa)$ à valeurs dans A qui vérifie les conditions suivantes :

(i) $\quad F(\nu, \rho_1 + \rho_2) = F(\nu, \rho_1)F(\nu, \rho_2) \quad$ pour tous $(\nu, \rho_i) \in R(\kappa)$

(ii) si $(\nu, \rho) \in R(\kappa)$ avec $\dim(\rho) = 0$ et $\kappa \subset \nu' \subset \nu$, alors :

$$F(\nu, \rho) = F(\nu', \mathrm{Ind}_{\nu/\nu'}(\rho))$$

où $\mathrm{Ind}_{\nu/\nu'}(\rho)$ est la représentation de $\Omega_{\nu'}$ induite de ρ. Une fonction extensible admet une seule extension vérifiant (i) et (ii) (voir [Tat2] Remark 1 pp. 102-103).

Les propriétés de la constante locale d'un caractère abélien, que l'on a traduites en terme de sommes de Gauss dans le paragraphe précédent, sont exposées dans [Tat2] en vue de présenter la preuve de Deligne du théorème de Langlands, qui stipule que la constante locale d'une extension κ de $\mathbb{Q}_p$ est extensible. Comme il est facile de voir que le conducteur $f(\chi)$ est une fonction extensible, ce résultat équivaut au fait que la somme de Gauss soit extensible ([M3], pp. 38-39). La conséquence principale est que la constante globale W et la somme de Gauss τ définie à partir d'elle (voir [Frö] I.5.22) se décomposent en produit de facteurs locaux. Soient K un corps de nombres et χ un caractère virtuel de Ω_K, alors :

$$\tau_K(\chi) = \prod_{\wp \text{ finie}} \tau_{K_\wp}(\chi_\wp) \qquad\qquad W(\chi) = \prod_{\wp} W(\chi_\wp)$$

où $\chi_\wp$ est l'image de χ par j_p^* (p étant la caractéristique résiduelle de $K_\wp$). On peut consulter [Frö], pp. 108-111, pour des détails.

Comme l'inductivité en degré 0 (ii) détermine $\tau_\kappa(\chi)$ pour tous $\kappa/\mathbb{Q}_p$ et χ, on notera dorénavant en général $\tau(\chi)$ en place de $\tau_\kappa(\chi)$.

Le théorème de Langlands a d'autres implications. Ainsi, Tate montre que l'analogue de la formule du corollaire 3.3.6 pour la constante locale peut être prolongée aux caractères virtuels ([Tat2] corollaire 5 p. 115). Il calcule les produits $W(\chi)W(\overline{\chi})$ et $W(\chi)\overline{W(\chi)}$ (corollaire 1 p. 109) ; Martinet fait de même pour la somme de Gauss (proposition 4.1 de [M3]). L'application la plus utile pour l'étude des modules galoisiens est la formule d'action galoisienne de la somme de Gauss locale ([M3] p. 42), montrée auparavant par Fröhlich pour la somme de Gauss globale.

Théorème 3.3.7 *Soit κ une extension finie de $\mathbb{Q}_p$ et χ un caractère de Ω_κ. Pour tout $\omega \in \Omega_{\mathbb{Q}}$, on a l'égalité :*

$$\tau(\chi^{\omega^{-1}}) = \tau(\chi)\mathrm{Det}_\chi(u_p(\omega))$$

où $u_p(\omega)$ est l'unique unité p-adique telle que, pour toute racine de l'unité η d'ordre une puissance de p, on ait $\eta^{\omega^{-1}} = \eta^{u_p(\omega)}$.

3.4 Extensions à groupe d'inertie abélien

Dans cette partie, on considère une extension finie faiblement ramifiée de corps locaux ν/κ de degré impair, de caractéristique résiduelle p. On note Γ le groupe de Galois et on suppose que le groupe d'inertie Γ_0 est abélien. On se propose d'illustrer les résultats de la partie précédente en donnant une expression "simple" de la somme de Gauss d'un caractère irréductible de Γ (à valeurs dans $\mathbb{Q}^c$). Pour cela, il est indispensable d'avoir une...

3.4.1 Description des caractères irréductibles de Γ

Comme la suite exacte :

$$1 \longrightarrow \Gamma_0 \longrightarrow \Gamma \longrightarrow \frac{\Gamma}{\Gamma_0} \longrightarrow 1$$

n'est pas nécessairement scindée, on ne peut pas appliquer directement le "lemme des petits groupes" de [Se3] (proposition 25). Cependant, on va montrer que ce résultat s'étend à la situation présente (Γ_0 abélien et Γ/Γ_0 cyclique). Il est à noter que des résultats plus généraux sur ce type de questions peuvent être trouvés dans [F1] et [F2].

Le groupe Γ agit sur les caractères irréductibles de Γ_0. Soient $\gamma \in \Gamma$ et $\varphi \in \widehat{\Gamma_0}$, on définit le caractère φ^γ par :

$$\varphi^\gamma(x) = \varphi(\gamma^{-1}x\gamma),\ \forall x \in \Gamma_0$$

On note $\Sigma_\varphi = \{\gamma \in \Gamma, \varphi^\gamma = \varphi\}$ le stabilisateur de φ. Alors $\Gamma_0 \subset \Sigma_\varphi$ et, comme Γ/Γ_0 est cyclique, on a Σ_φ distingué dans Γ et Σ_φ/Γ_0 est cyclique. On déduit alors du corollaire (11.47) de [CR1] que φ s'étend en un caractère abélien de Σ_φ. De plus, si φ' et φ'' étendent tous les deux φ, alors $\varphi''\varphi'^{-1}$ est inflaté d'un caractère de Σ_φ/Γ_0. Il s'ensuit que φ possède $|\Sigma_\varphi/\Gamma_0|$ extensions distinctes à Σ_φ.

On fixe maintenant un système de représentants $\{\varphi_1, \ldots, \varphi_r\}$ du groupe des caractères irréductibles de Γ_0 sous l'action de Γ et, pour $1 \leq i \leq r$, on note $\Sigma_i = \Sigma_{\varphi_i}$ et $n_i = [\Sigma_i : \Gamma_0]$. On écrit $\{\varphi_{i,1}, \ldots, \varphi_{i,n_i}\}$ pour les différentes extensions de φ_i et on pose $\theta_{i,j} = \mathrm{Ind}_{\Sigma_i}^{\Gamma} \varphi_{i,j}$. On a le résultat suivant.

Proposition 3.4.1

(i) $\theta_{i,j}$ *est un caractère irréductible de* Γ *;*

(ii) $\theta_{i,j} = \theta_{k,l} \Leftrightarrow i = k$ *et* $j = l$ *;*

(iii) tout caractère irréductible de Γ *est égal à l'un des* $\theta_{i,j}$*.*

Preuve. Le point (i) est une conséquence immédiate du critère de Mackey : comme $\varphi_{i,j}$ est abélien donc irréductible, on doit montrer, pour $s \in \Gamma \setminus \Sigma_i$, que $\varphi_{i,j}$ et ${\varphi_{i,j}}^s$ sont deux représentations abéliennes distinctes de Σ_i. Or leurs restrictions à Γ_0 sont $\varphi_{i,j\,|\Gamma_0} = \varphi_i$ et ${\varphi_{i,j}}^s_{|\Gamma_0} = {\varphi_i}^s$, avec $s \notin \Sigma_i$.

On prouve maintenant le point (iii). Soit χ un caractère irréductible de Γ, sa restriction $\chi_{|\Gamma_0}$ à Γ_0 est une somme de caractères abéliens et il existe un caractère irréductible φ de Γ_0 tel que $< \chi_{|\Gamma_0}, \varphi >_{\Gamma_0} \neq 0$, c'est-à-dire :

$$\frac{1}{|\Gamma_0|} \sum_{a \in \Gamma_0} \chi(a^{-1})\varphi(a) \neq 0$$

Comme Γ_0 est distingué dans Γ, ceci entraîne que pour tout $s \in \Gamma$, on a :

$$\frac{1}{|\Gamma_0|} \sum_{a \in \Gamma_0} \chi(sa^{-1}s^{-1})\varphi(sas^{-1}) \neq 0$$

si bien que, pour tout $s \in \Gamma$, $< \chi_{|\Gamma_0}, \varphi^s > \neq 0$ puisque χ est central. Il existe donc un entier i avec $1 \leq i \leq r$ tel que $< \chi_{|\Gamma_0}, \varphi_i > \neq 0$ et l'on considère $\mathrm{Ind}_{\Gamma_0}^{\Sigma_i} \varphi_i$. Tout d'abord, on note que, pour tout $1 \leq j \leq n_i$:

$$< \mathrm{Ind}_{\Gamma_0}^{\Sigma_i} \varphi_i, \varphi_{i,j} >_{\Sigma_i} = < \varphi_i, \varphi_{i,j\,|\Gamma_0} >_{\Gamma_0} = < \varphi_i, \varphi_i > = 1$$

Il s'ensuit qu'on peut écrire $\mathrm{Ind}_{\Gamma_0}^{\Sigma_i} \varphi_i = \sum_{j=1}^{n_i} \varphi_{i,j} + a_1\psi_1 + \cdots + a_t\psi_t$, où les a_k sont des entiers positifs et les ψ_k des caractères irréductibles de Σ_i distincts des $\varphi_{i,j}$. En comparant les degrés, on obtient :

$$\mathrm{Ind}_{\Gamma_0}^{\Sigma_i} \varphi_i = \sum_{j=1}^{n_i} \varphi_{i,j}$$

Mais $< \chi_{|\Sigma_i}, \mathrm{Ind}_{\Gamma_0}^{\Sigma_i} \varphi_i > = < \chi_{|\Gamma_0}, \varphi_i > \neq 0$, donc il existe un entier j avec $1 \leq j \leq n_i$ tel que $< \chi_{|\Sigma_i}, \varphi_{i,j} > \neq 0$, si bien que :

$$< \chi, \mathrm{Ind}_{\Sigma_i}^{\Gamma} \varphi_{i,j} > \neq 0$$

et, comme χ et $\mathrm{Ind}_{\Sigma_i}^{\Gamma} \varphi_{i,j}$ sont deux caractères irréductibles, cela entraîne qu'ils sont égaux.

On en vient à la preuve du point (ii). On suppose donc que $\theta_{i,j} = \theta_{k,l}$. Ceci entraîne que leurs restrictions à Γ_0 sont égales, et donc :

$$\sum_{g \in \Gamma/\Sigma_i} {\varphi_i}^g = \sum_{h \in \Gamma/\Sigma_k} {\varphi_k}^h$$

Alors φ_i et φ_k sont conjugués et donc égaux, c'est-à-dire $i = k$. L'égalité des restrictions de $\theta_{i,j}$ et $\theta_{i,l}$ à Σ_i nous assure l'existence de $g \in \Gamma$ tel que $\varphi_{i,j} = {\varphi_{i,l}}^g$. En restreignant à Γ_0, on trouve que $g \in \Sigma_i$. Mais $\varphi_{i,l}$ est un caractère abélien de Σ_i, donc ${\varphi_{i,l}}^g = \varphi_{i,l}$ et $j = l$, ce qui termine la preuve de la proposition 3.4.1. ∎

Pour tout $1 \leq i \leq r$, on fixe maintenant un caractère abélien $\widetilde{\varphi}_i$ de Σ_i qui étend φ_i. On peut interpréter le point (iii) de la proposition 3.4.1 en disant que tout caractère irréductible χ de Γ est de la forme $\mathrm{Ind}_{\Sigma_i}^{\Gamma}(\widetilde{\varphi}_i\widetilde{\rho})$, où $\widetilde{\rho}$ est l'inflaté à Σ_i d'un caractère ρ de Σ_i/Γ_0, pour un entier i avec $1 \leq i \leq r$. On s'intéresse au comportement d'une représentation irréductible par rapport à la restriction de Γ à Γ_0. On note que Σ_i est distingué dans Γ. On fixe S_i un système de représentants de Γ/Σ_i. La proposition 22 de [Se3] permet de montrer le résultat suivant.

Proposition 3.4.2 *Soit* $\chi = \mathrm{Ind}_{\Sigma_i}^{\Gamma}(\widetilde{\varphi}_i\widetilde{\rho})$ *comme ci-dessus, alors* $\mathrm{Res}\,\chi = \bigoplus_{s \in S_i} {\varphi_i}^s$.

3.4.2 Une expression simple pour la somme de Gauss

On note μ_i la sous-extension de ν fixée par Σ_i et ν_0 la sous-extension de ν fixée par Γ_0. La proposition suivante est un premier pas pour obtenir la formule de restriction au groupe d'inertie pour la somme de Gauss.

Proposition 3.4.3 *Pour tout $1 \leq i \leq r$, on a les égalités :*

(i) $\tau(\varphi_i - \psi(\varphi_i)) = \tau(\widetilde{\varphi}_i - \psi(\widetilde{\varphi}_i))^{[\nu_0:\mu_i]}$,

(ii) pour tout $s \in S_i$, $\tau(\varphi_i) = \tau(\varphi_i{}^s)$.

Preuve. On a l'égalité $\mathrm{Ind}_{\Gamma_0}^{\Sigma_i}\varphi_i = \sum_\alpha \widetilde{\varphi}_i\alpha$, où α décrit le groupe Δ des caractères abéliens de Σ_i obtenus par inflation de caractères de Σ_i/Γ_0. Comme $[\Sigma_i : \Gamma_0]$ est premier à 2, la deuxième opération d'Adams ψ commute à l'induction de Γ_0 à Σ_i. Or $\varphi_i - \psi(\varphi_i)$ est un caractère de dimension 0. Par inductivité en degré 0 de la somme de Gauss, on en déduit, à l'aide du corollaire 3.3.6 :

$$\tau(\varphi_i - \psi(\varphi_i)) = \tau(\mathrm{Ind}_{\Gamma_0}^{\Sigma_i}\varphi_i - \psi(\mathrm{Ind}_{\Gamma_0}^{\Sigma_i}\varphi_i)) = A(\varphi_i)\tau(\widetilde{\varphi}_i - \psi(\widetilde{\varphi}_i))^{[\nu_0:\mu_i]}$$

avec $A(\varphi_i) = \prod_\alpha \alpha^2(\mathcal{D}(\varphi_i))/\alpha(\mathcal{D}(\varphi_i))$. Or $\alpha \mapsto \alpha^2$ est un automorphisme de Δ et donc $A(\varphi_i) = 1$, ce qui démontre (i).

Soit $s \in S_i$, alors φ_i et $\varphi_i{}^s$ ont même stabilisateur Σ_i. De plus, $\widetilde{\varphi}_i^s$ est un caractère abélien de Σ_i qui prolonge φ_i^s et, par définition d'un caractère induit, on a l'égalité $\mathrm{Ind}_{\Sigma_i}^{\Gamma}\widetilde{\varphi}_i = \mathrm{Ind}_{\Sigma_i}^{\Gamma}\widetilde{\varphi}_i^s$. On en tire que $\tau(\widetilde{\varphi}_i - \widetilde{\varphi}_i^s) = 1$. Or, $\mathrm{Ind}_{\Gamma_0}^{\Sigma_i}\varphi_i = \sum_\alpha \widetilde{\varphi}_i\alpha$ et $\mathrm{Ind}_{\Gamma_0}^{\Sigma_i}\varphi_i^s = \sum_\alpha \widetilde{\varphi}_i^s\alpha$, d'où l'on déduit que

$$\tau(\varphi_i^s - \varphi_i) = \tau(\widetilde{\varphi}_i - \widetilde{\varphi}_i^s)^{[\nu_0:\mu_i]} = 1$$

∎

On peut maintenant énoncer la formule de restriction au groupe d'inertie pour la somme de Gauss.

Théorème 3.4.4 *Avec les notations introduites ci-dessus, soit $\chi = \mathrm{Ind}_{\Sigma_i}^{\Gamma}(\widetilde{\varphi}_i\widetilde{\rho})$ un caractère irréductible de Γ. Il existe $c_i \in \mathcal{O}_{\mu_i}$ tel que :*

$$\tau(\chi - \psi(\chi)) = \tau(\mathrm{Res}\,\chi - \psi(\mathrm{Res}\,\chi))\,\widetilde{\rho}(\mathcal{D}(\widetilde{\varphi}_i))\,\widetilde{\varphi}_i(c_i/4)^{1-f}\,\psi_{\mu_i}((f-1)/c_i)$$

où f est le degré résiduel de l'extension ν/κ.

Le nombre c_i sera précisé dans le lemme 3.4.6.

Preuve. Comme $[\Gamma : \Sigma_i]$ est premier à 2, la deuxième opération d'Adams ψ commute à l'induction de Σ_i à Γ. De plus, $\widetilde{\varphi}_i\widetilde{\rho} - \psi(\widetilde{\varphi}_i\widetilde{\rho})$ est un caractère de dimension 0, d'où

$$\tau(\chi - \psi(\chi)) = \tau(\widetilde{\varphi}_i\widetilde{\rho} - \psi(\widetilde{\varphi}_i\widetilde{\rho}))$$

Comme $\widetilde{\varphi}_i$ et $\widetilde{\rho}$ sont des caractères abéliens avec $\widetilde{\rho}$ non ramifié, on en déduit, à l'aide du corollaire 3.3.6 :

$$\tau(\chi - \psi(\chi)) = \widetilde{\rho}(\mathcal{D}(\widetilde{\varphi}_i))\tau(\widetilde{\varphi}_i - \psi(\widetilde{\varphi}_i)) \tag{3.11}$$

Soit π une uniformisante de κ. Comme $\kappa \subset \mu_i \subset \nu_0$ est non ramifiée, π est aussi une uniformisante de μ_i et de ν_0. Les conducteurs de φ_i et de $\widetilde{\varphi}_i$ vérifient :

Lemme 3.4.5

$$f(\varphi_i) = f(\widetilde{\varphi}_i)\mathcal{O}_{\nu_0} = \begin{cases} \mathcal{O}_{\nu_0} & \text{si } \varphi_i \text{ est trivial} \\ (\pi^2) & \text{sinon} \end{cases}$$

Preuve. Comme ν_0/κ est non ramifiée, la première égalité est claire. On sait par le théorème 1 de [Se2] p.155 que

$$\varphi_i(1+\pi^2\mathcal{O}_{\nu_0}) = \varphi_i\big((1+\pi^2\mathcal{O}_{\nu_0}, \nu/\nu_0)\big) = \varphi_i(\Gamma_{\psi(2)}) = \{1\}$$

puisque $\Gamma_{\psi(2)} \subset \Gamma_2 = \{1\}$. Si $\varphi_i(1+\pi\mathcal{O}_{\nu_0}) = 1$, alors φ_i est trivial sur Γ_1. Mais $\Gamma_0 = \Gamma_1$ par la proposition 1.2.3 donc φ_i est le caractère trivial de $\Gamma_0 = \mathrm{Gal}(\nu/\nu_0)$. ▮

On est maintenant en mesure de faire usage de la proposition 3.3.1 et du corollaire 3.3.2.

Lemme 3.4.6 *Soit $c_i \in \mathcal{O}_{\mu_i}$ vérifiant la condition de la proposition 3.3.1 appliquée à $\widetilde{\varphi}_i$ avec $\mathfrak{a} = (\pi)$ (resp. $\mathfrak{a} = \mathcal{O}_{\mu_i}$) si φ_i est non trivial (resp. trivial). Alors*

$$\tau(\widetilde{\varphi}_i - \psi(\widetilde{\varphi}_i)) = \widetilde{\varphi}_i(c_i/4)\psi_{\mu_i}(-c_i^{-1})$$

Preuve. Par le corollaire 3.3.2, on a :

$$\tau(\widetilde{\varphi}_i) = \mathrm{N}_{\mu_i/\mathbb{Q}_p}(f(\widetilde{\varphi}_i))^{1/2}\widetilde{\varphi}_i(c_i^{-1})\psi_{\mu_i}(c_i^{-1}) \tag{3.12}$$

Il faut maintenant exprimer $\tau(\psi(\widetilde{\varphi}_i))$ en fonction de $c_i = c(\widetilde{\varphi}_i)$. Or, on sait par le lemme 3.3.5 que le nombre $c(\widetilde{\varphi}_i)/2$ vérifie la condition (i) de la proposition 3.3.1 relativement à $\psi(\widetilde{\varphi}_i)$ et à $\mathfrak{a} = (\pi)$ (resp. $\mathfrak{a} = \mathcal{O}_{\mu_i}$) si φ_i est non trivail (resp. trivial). On en déduit l'égalité suivante :

$$\tau(\psi(\widetilde{\varphi}_i)) = \mathrm{N}_{\mu_i/\mathbb{Q}_p}(f(\widetilde{\varphi}_i))^{1/2}\widetilde{\varphi}_i(2c_i^{-1})^2\psi_{\mu_i}(c_i^{-1})^2$$

et le point (ii) du lemme en découle à l'aide de (3.12). ▮

On est maintenant en mesure de terminer la preuve du théorème 3.4.4. On déduit des propositions 3.4.2 et 3.4.3 :

$$\tau(\mathrm{Res}\,\chi - \psi(\mathrm{Res}\,\chi)) = \tau(\varphi_i - \psi(\varphi_i))^{[\mu_i:\kappa]} = \tau(\widetilde{\varphi}_i - \psi(\widetilde{\varphi}_i))^f$$

A l'aide de (3.11), on obtient :

$$\tau(\chi - \psi(\chi)) = \tau(\mathrm{Res}\,\chi - \psi(\mathrm{Res}\,\chi))\widetilde{\rho}(\mathcal{D}(\widetilde{\varphi}_i))\tau(\widetilde{\varphi}_i - \psi(\widetilde{\varphi}_i))^{1-f}$$

et le lemme 3.4.6 permet de conclure. ▮

Chapitre 4

Structure galoisienne : résultats

Comme son titre l'indique, ce chapitre est consacré à des résultats de structure galoisienne de la racine carrée de la codifférente. Jusqu'à la fin, N/K est une extension finie galoisienne de corps de nombres, de degré impair, de groupe de Galois G, faiblement ramifiée.

On a vu précédemment que la détermination de la structure de $\mathbb{Z}[G]$-module de la racine carrée de la codifférente $\mathcal{A}_{N/K}$ passe par l'étude de $j_p^*(f_p)$ pour tout diviseur premier p de l'ordre de G. Cet homomorphisme équivariant peut s'écrire comme un produit de fonctions de caractères. Certaines de ces fonctions se traitent facilement, ce sont celles dans lesquelles la ramification sauvage ne joue pas un rôle déterminant ; on peut alors utiliser les techniques de Taylor du cas modéré ([Tay1]) et de [Er3]. On présente le travail d'adaptation nécessaire dans la partie 4.1.

Le traitement des fonctions dans lesquelles intervient la ramification sauvage s'avère plus délicat. Dans [Er3], le calcul de leur valuation permet d'établir que ce sont des unités, ce qui montre que la racine carrée de la codifférente est libre sur l'ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$ et mène au théorème 2 que l'on a déjà évoqué. Pour aller plus loin, il paraît souhaitable, au moins dans un premier temps, de se placer dans des situations plus favorables que le cas général. Ainsi, [Tay2] étudie la structure galoisienne de l'anneau d'entiers d'une extension finie abélienne de corps de nombres, [B] fait de même dans le cas local tandis que [CNT2] se concentre sur les extensions finies galoisiennes de $\mathbb{Q}$ dont les premiers groupes de ramification (aux places sauvages) sont abéliens, facteurs directs du groupe de décomposition et distingués dans le groupe de Galois. Le résultat présenté ici fait intervenir une hypothèse légèrement moins forte sur l'extension (cependant, la ramification y est supposée faible). On se restreint au cas d'une extension absolue.

Théorème 3 *Soit N/K comme ci-dessus avec $K = \mathbb{Q}$. On suppose que le groupe*

de décomposition de l'extension est abélien en toute place sauvage. Alors $\mathcal{A}_{N/\mathbb{Q}}$ est un $\mathbb{Z}[G]$-module libre.

Ce résultat se déduit aisément des propositions 4.2.2 et 4.2.10 qui seront montrées dans la partie 4.2. La première, même si elle traite le cas des places modérées, utilise l'hypothèse sur les groupes de décomposition aux places sauvages mais reste valable pour une extension relative ; la seconde, qui traite les places sauvages utilise en plus le fait que $K = \mathbb{Q}$ puisqu'on l'obtient grâce à l'étude locale des extensions pures de $\mathbb{Q}_p$ menée dans la partie 1.3. En fait, on détermine explicitement le facteur $j_p^*(f_{(p),p})$, ce qui permet de prouver qu'il est de la forme souhaitée.

On a vu que les extensions galoisiennes de $\mathbb{Q}$ données par le polynôme numéro 16 de la liste d'extensions faiblement ramifiées du chapitre 2 et l'exemple présenté dans le paragraphe 1.4.3 sont faiblement ramifiées de groupe de Galois isomorphe à $C_9 \rtimes C_3$. Ces deux extensions éclairent deux aspects distincts du théorème 3 : la première en satisfait les hypothèses, montrant que son champ d'application n'est pas vide ; la seconde ne les satisfait pas, mais le calcul permet d'y trouver une base normale pour la racine carrée de la codifférente, ce qui laisse espérer une généralisation de ce théorème.

Jusqu'à présent, tous les exemples d'extensions faiblement ramifiées de groupe de Galois isomorphe à $C_9 \rtimes C_3$ étudiés par l'auteur ont permis de trouver une base normale de la racine carrée de la codifférente (voir le chapitre 5). Il semble probable que $\mathcal{A}_N$ soit toujours un $\mathbb{Z}[G]$-module libre lorsque N est une extension faiblement ramifiée de $\mathbb{Q}$ de groupe de Galois G et de degré une puissance de p avec p premier impair.

Le théorème 4 présenté dans la partie 4.3 fait un pas dans cette direction. On y montre que l'ordre de la classe de la racine carrée de la codifférente d'une p-extension faiblement ramifiée divise l'ordre du groupe d'inertie en p.

4.1 Adaptation de résultats existants

Dans cette partie, on considère une extension N/K vérifiant les conditions énoncées en début de chapitre. Si l est un nombre premier de $\mathbb{Z}$, on rappelle (voir le chapitre précédent) que le plongement $j_l : \mathbb{Q}^c \to \mathbb{Q}_l^c$ définit de manière unique un idéal premier ℓ (resp. $\mathcal{L}$) de $\mathcal{O}_K$ (resp. $\mathcal{O}_N$). On note $G(l)$ le groupe de décomposition de $\mathcal{L}$ sur ℓ et S_W l'ensemble des nombres premiers l de $\mathbb{Z}$ tels que ℓ soit sauvagement ramifié dans N/K.

On fixe un diviseur premier p de l'ordre de G. On constate que $j_p^*(f_p)$ est un produit d'au plus trois types de facteurs choisis parmi les suivants :

$$j_p^*(f_{(p),p}) \text{ ou } j_p^*(f_{(p),p}^*), \quad j_p^*(f_{(l),p}^*),\ l \notin S_W, \quad j_p^*(f_{(l),p}),\ l \in S_W$$

où $l \neq p$ décrit l'ensemble des nombres premiers de $\mathbb{Z}$ correspondant à une place ramifiée dans N/K. On note que le premier facteur n'intervient que si $p \in S_W$, le deuxième seulement si $p \notin S_W$. Dans cette partie, on mène l'étude des facteurs "modérés" $j_p^*(f_{(p),p}^*)$ (pour lequel $p \notin S_W$) et $j_p^*(f_{(l),p}^*)$, pour lequel

$l \neq p$, $l \notin S_W$ (mais p peut indifféremment appartenir ou non à S_W), à partir de résultats de [Tay1] et [Er3]. On commence par l'étude du premier d'entre eux.

Lemme 4.1.1 *On suppose que $p \notin S_W$. Il existe une extension galoisienne et modérément ramifiée $L_p/\mathbb{Q}_p$ telle que :*

$$j_p^*(f_{(p),p}^*) \in \mathrm{Ind}_{G(p)}^G \mathrm{Det}(\mathcal{O}_{L_p}[G(p)]^*)$$

Preuve. On commence par observer que $j_p^*(f_{(p),p}^*) = \mathrm{Ind}_{G(p)}^G(g_p)$ où g_p est l'élément de $\mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G(p),p}, \mathcal{O}_{E_p}^*)$ défini par :

$$g_p(\chi) = \mathcal{N}_{K_p/\mathbb{Q}_p}(\alpha_p|\chi) j_p^*(\widetilde{T}_p^*)^{-1}(\chi), \quad \forall \chi \in R_{G(p),p}$$

Comme dans la démonstration du lemme 8.4 (a) de [Er3], on reprend celle du théorème 31 de [Frö] en remplaçant les théorèmes 23 et 25 de [Frö] par le théorème 5.2 et l'égalité (6.3) de [Er3] ; on obtient alors, en spécialisant le théorème 31 à $F = K_p$, $L = N_p$, $\Gamma = G(p)$, $j = j_p$ et $a = \alpha_p$ l'analogue de ce théorème pour $\widetilde{T}_p^*$ en place de τ^* (et χ en place de χ^j), à savoir qu'il existe une extension galoisienne modérément ramifiée $L_p/\mathbb{Q}_p$ telle que $g_p \in \mathrm{Det}(\mathcal{O}_{L_p}[G(p)]^*)$. ∎

L'objet du lemme suivant est le comportement du deuxième facteur. Ici, le fait que p corresponde ou non à une place sauvage est sans importance.

Lemme 4.1.2 *Pour tout nombre premier l de $\mathbb{Z}$ tel que $l \notin S_W$ et $l \neq p$, il existe une extension galoisienne non ramifiée $F_l/\mathbb{Q}_p$ telle que*

$$j_p^*(f_{(l),p}^*) \in \mathrm{Ind}_{G(l)}^G \mathrm{Det}(\mathcal{O}_{F_l}[G(l)]^*)$$

Preuve. On note d'abord que $j_p^*(f_{(l),p}^*) = \mathrm{Ind}_{G(l)}^G(h_p^*)$ avec $h_p^*(\chi) = j_p^*(\widetilde{T}_l^*)^{-1}(\chi)$, pour tout $\chi \in R_{G(l),p}$. Le théorème 3 de [Tay1] assure que

$$\tau_l^* \in \mathrm{Det}(\mathcal{O}_{\mathbb{Q}_p[l]}[G(l)]^*)$$

où $\mathbb{Q}_p[l]$ est l'extension de $\mathbb{Q}_p$ obtenue en lui adjoignant les racines l-ièmes de l'unité. Les résultats de [CNT1] (inclusions (2-7)) permettent alors d'affirmer que :

$$\Psi(\tau_l^*) \in \mathrm{Det}(\mathcal{O}_{\mathbb{Q}_p[l]}[G(l)]^*)$$

et donc il en va de même pour h_p^*. On note enfin que $F_l = \mathbb{Q}_p[l]$ est non ramifiée sur $\mathbb{Q}_p$. ∎

Les facteurs "sauvages" $j_p^*(f_{(p),p})$ avec $p \in S_W$ et $j_p^*(f_{(l),p})$ avec $l \neq p$, $l \in S_W$ (et p appartient ou non à S_W), ne se traitent pas aussi facilement. On a besoin d'une hypothèse sur les groupes de décomposition aux places sauvages.

4.2 Extensions abéliennes aux places sauvages

N/K est encore une extension finie galoisienne de corps de nombres de groupe de Galois G, de degré impair, faiblement ramifiée. On suppose dorénavant qu'elle vérifie :

Hypothèse 4.2.1 *Pour tout $l \in S_W$, le groupe de décomposition $G(l)$ est abélien.*

On va montrer la proposition suivante dans le prochain paragraphe.

Proposition 4.2.2 *Soit N/K comme dans l'introduction de ce chapitre, vérifiant l'hypothèse 4.2.1 et soit p un nombre premier correspondant à une place modérée de N/K. Alors $j_p^*(f_p) \in \mathrm{Det}(\mathbb{Z}_p[G]^*)$.*

4.2.1 Le dernier facteur des places modérées

Dans ce paragraphe, on fixe un diviseur premier p de l'ordre de G (p sauvage ou modéré) et on montre :

Lemme 4.2.3 *Pour tout nombre premier $l \in S_W$, $l \neq p$, il existe $M_l/\mathbb{Q}_p$ non ramifiée telle que $j_p^*(f_{(l),p}) \in \mathrm{Ind}_{G(l)}^G(\mathrm{Det}(\mathcal{O}_{M_l}[G(l)]^*))$.*

Dans le cas où p est une place modérée, on en déduit, à l'aide des lemmes 4.1.1 et 4.1.2, qu'il existe une extension modérément ramifiée $V/\mathbb{Q}_p$ telle que :

$$j_p^*(f_p) = j_p^*(f_{(p),p}^*) \prod_{\substack{l \notin S_W \\ l \neq p}} j_p^*(f_{(l),p}^*) \prod_{l \in S_W} j_p^*(f_{(l),p})$$

appartienne à $\mathrm{Det}(\mathcal{O}_V[G]^*)$. Puisque $j_p^*(f_p)$ est un $\Omega_{\mathbb{Q}_p}$-homomorphisme, le théorème des points fixes de Taylor ([Tay1], Théorème 6) entraîne alors la proposition 4.2.2. On prouve maintenant le lemme 4.2.3.

Preuve. Puisque $G(l)$ est abélien, on peut le décomposer en produit direct $G'(l) \times G''(l)$ où $G'(l)$ (resp. $G''(l)$) est le produit des q-sous-groupes de Sylow pour $q \neq l$ (resp. le l-sous-groupe de Sylow) de $G(l)$. Tout caractère irréductible χ de $G(l)$ se décompose en un produit $\chi'\chi''$ où χ' (resp. χ'') est égal à la restriction de χ à $G'(l)$ (resp. $G''(l)$). Puisque N_l/K_l est abélienne, $G_0(l) = G_1(l)$ par la proposition 1.2.3 du premier chapitre, donc $G_0(l) \subset G''(l)$ et le caractère χ' est non ramifié. Soit π une uniformisante de K_l, alors, pour tout caractère χ irréductible de $G(l)$, on a $f(\chi) = f(\chi'') = (\pi)^2$ (resp. $\mathcal{O}_{K_l}$) si χ'' est ramifié (resp. non ramifié). Comme χ' et χ'' sont des caractères abéliens, on sait par la définition (3.7) et par le corollaire 3.3.6 que :

$$\tau_l(\chi) = \begin{cases} \chi(\mathcal{D}_{K_l})^{-1} & \text{si } \chi \text{ est non ramifié} \\ \chi'\big(f(\chi'')\mathcal{D}_{K_l}\big)^{-1}\tau_l(\chi'') & \text{si } \chi \text{ est ramifié} \end{cases}$$

On pose $r(\chi) = r(\chi'') = 2 + v_\pi(\mathcal{D}_{K_l})$ (resp. $v_\pi(\mathcal{D}_{K_l})$) si χ est ramifié (resp. non ramifié). On a donc :

$$j_p^*(f_{(l),p}) = \mathrm{Ind}_{G(l)}^G(uv)$$

où u est défini sur les caractères irréductibles de $G(l)$ par $u(\chi) = \chi'(\pi^{r(\chi)})$ et où $v = \mathrm{Ind}_{G''(l)}^{G(l)} \widetilde{T}_l^{-1}$. On déduit du corollaire 3.3.2 et du lemme 3.3.5 l'expression suivante de la somme de Gauss :

$$\tau_l(\chi'' - \psi(\chi'')) = \chi''(c/4)\psi_{K_l}(-c^{-1})$$

où c est comme dans le corollaire 3.3.2. Comme χ'' est un caractère d'un l-groupe, il est à valeurs dans les racines l-ièmes de l'unité ; de par sa définition, il en va de même pour ψ_{K_l}. On en déduit qu'il existe une extension non ramifiée M_l de $\mathbb{Q}_p$, obtenue en lui adjoignant les racines l-ièmes de l'unité d'ordre suffisant, telle que $\tau_l \in \mathrm{Hom}_{\Omega_{M_l}}(R_{G''(l),p}, \mathcal{O}_{E_p}^*)$. Mais comme $p \neq l$, on a :

$$\mathrm{Hom}_{\Omega_{M_l}}(R_{G''(l),p}, \mathcal{O}_{E_p}^*) = \mathrm{Det}(\mathcal{O}_{M_l}[G''(l)]^*) \tag{4.1}$$

et par conséquent :

$$\mathrm{Ind}_{G''(l)}^{G(l)}(\tau_l) \in \mathrm{Det}(\mathcal{O}_{M_l}[G(l)]^*) \tag{4.2}$$

En outre, grâce à [CNT1], on sait qu'il en est de même de $\Psi(\mathrm{Ind}_{G''(l)}^{G(l)}\tau_l)$. On a donc démontré :

Lemme 4.2.4 *Il existe une extension non ramifiée $M_l/\mathbb{Q}_p$ telle que*

$$\mathrm{Ind}_{G(l)}^{G}(v) \in \mathrm{Det}(\mathcal{O}_{M_l}[G]^*)$$

On examine maintenant le facteur $u \in \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G(l)}, \mathcal{O}_{E_p}^*)$. On a le résultat suivant :

Lemme 4.2.5 *Il existe $t \in \mathbb{Z}_p[G(l)]^*$ tel que $u = \mathrm{Det}(t)$.*

Preuve. On décompose $G(l)$ en produit direct de trois sous-groupes :

$$G(l) = H_1 \times H_2 \times H_3$$

avec $H_1 = G''(l)$ le l-sous-groupe de Sylow de $G(l)$, H_2 le produit des q-sous-groupes de Sylow avec $q \neq p$ et $q \neq l$, H_3 le p-sous-groupe de Sylow de $G(l)$. On observe que si $H_3 = \{1\}$, le résultat est immédiat par un argument similaire à (4.1). On suppose donc que $H_3 \neq \{1\}$. Tout caractère χ de $G(l)$ se décompose en un produit $\chi = \chi''\chi_2\chi_3$ avec les notations précédentes. On pose $m = |H_1|.|H_2|$ (on a $(m,p) = 1$). On se donne un système de représentants $\{\theta_1, \theta_2, \ldots, \theta_r\}$ des orbites des caractères de H_1H_2 sous l'action de $\Omega_{\mathbb{Q}_p}$ (si θ et φ sont dans la même orbite, on écrit $\theta \sim \varphi$). Pour tout $\theta \in \widehat{H_1H_2}$, on pose :

$$e_\theta = \frac{1}{m} \sum_{h \in H_1H_2} \theta(h^{-1})h \quad \text{et} \quad e_i = \sum_{\theta \sim \theta_i} e_\theta$$

Puisque $(m,p) = 1$, on note que $e_i \in \mathbb{Z}_p[H_1H_2]$, $1 \leq i \leq r$ et que l'on a : $1 = \sum_1^r e_i$, ${e_i}^2 = e_i$ et $e_ie_j = 0$ si $i \neq j$. On note aussi que si $\theta_i = \chi''\varphi$ avec χ''

caractère de $G''(l)$, alors si χ'' est ramifié (resp. non ramifié), tous les éléments de l'orbite de θ_i ont la même propriété. On ordonne les e_i de façon à ce que les e_i, $1 \leq i \leq s$ (resp. les e_j, $s+1 \leq j \leq r$) soient associés à un θ_i ramifié (resp. non ramifié). Si $\chi \in \widehat{G(l)}$, $\chi = \theta\chi_3$ avec $\theta \in \widehat{H_1H_2}$, alors

$$\chi(e_i) = \begin{cases} 1 & \text{si } \theta \sim \theta_i \\ 0 & \text{sinon} \end{cases}$$

Par la théorie du corps de classes, on associe à $\pi^{2+v_\pi(\mathcal{D}_{K_l})}$ (resp. $\pi^{v_\pi(\mathcal{D}_{K_l})}$) un élément de $G(l)$ et on note σ (resp. γ) sa composante sur H_2H_3. On pose maintenant :

$$t = \sigma \sum_1^s e_i + \gamma \sum_{s+1}^r e_j$$

On note que $t \in \mathbb{Z}_p[G(l)]$. De plus, il est inversible et son inverse est $\sigma^{-1}\sum_1^s e_i + \gamma^{-1}\sum_{s+1}^r e_j$. Soit $\chi = \chi''\chi'$ avec $\chi' = \chi_2\chi_3$. On a :

$$\mathrm{Det}_\chi(t) = \chi(\sigma)\sum_1^s \chi(e_i) + \chi(\gamma)\sum_{s+1}^r \chi(e_j)$$

On note que $\chi(\gamma) = \chi'(\pi^{v_\pi(\mathcal{D}_{K_l})}) = \chi'(\mathcal{D}_{K_l})$ et que $\chi(\sigma) = \chi'(\pi^{2+v_\pi(\mathcal{D}_{K_l})}) = \chi'\big(f(\chi'')\mathcal{D}_{K_l}\big)$. En outre, si χ est ramifié, il existe i_0, $1 \leq i_0 \leq s$ tel que $\chi''\chi_2 \sim \theta_{i_0}$ et donc on a : $\sum_1^s \chi(e_i) = \chi(e_{i_0}) = 1$, $\sum_{s+1}^r \chi(e_j) = 0$. Si χ est non ramifié alors $\chi''\chi_2 \sim \theta_{j_1}$ avec $s+1 \leq j_1 \leq r$ et $\sum_1^s \chi(e_i) = 0$, $\sum_{s+1}^r \chi(e_j) = \chi(e_{j_1}) = 1$. On a ainsi démontré que $u = \mathrm{Det}(t)$. ▌

Le lemme 4.2.3 se déduit aisément des lemmes 4.2.4 et 4.2.5. ▌

4.2.2 Les places sauvages (cas absolu)

On se restreint maintenant au cas absolu. On veut montrer l'analogue de la proposition 4.2.2 pour les places sauvages.

Soit $N/\mathbb{Q}$ une extension finie galoisienne de groupe de Galois G, de degré impair, faiblement ramifiée, qui vérifie l'hypothèse 4.2.1, dans laquelle p est sauvagement ramifié. Comme $G(p) \simeq \Gamma = \mathrm{Gal}(N_p/\mathbb{Q}_p)$ est abélien, l'extension $N_p/\mathbb{Q}_p$ est pure (voir définition 1.3.1) et on sait par le théorème 1 que N_p est égale à l'une des sous-extensions ramifiées de degré $n = [N_p : \mathbb{Q}_p]$ de $L.\mathbb{Q}_p\{n\}$, où L est la sous-extension de degré p de $\mathbb{Q}_p[p^2]$. On se propose d'expliciter le facteur $j_p^*(f_{(p),p}) = \mathrm{Ind}_\Gamma^G h_p$, où

$$h_p(\chi) = (\alpha_p|\chi)j_p^*(\tau_p)(\chi - \psi(\chi)) \quad \forall \chi \in R_{\Gamma,p}$$

On a déjà la formule (3.10) pour la somme de Gauss. On en déduit :

Lemme 4.2.6

$$j_p^*(\tau_p)(\chi - \psi(\chi)) = \begin{cases} 1 & \text{si } \chi \text{ est non ramifié} \\ \widetilde{\chi}(p^2/4u(\chi))\zeta^{-u(\chi)} & \text{si } \chi \text{ est ramifié} \end{cases}$$

Preuve. On suppose χ ramifié. Comme Γ est abélien, on a $\psi(\chi) = \chi^2$. De plus, puisque $\widetilde{\chi}^2(1+p) = \zeta^{-2pu(\chi)}$, $u(\chi^2)$ vaut $2u(\chi)$ ou $2u(\chi) - p$. Le résultat est immédiat dans le premier cas. Si $u(\chi^2) = 2u(\chi) - p = 2u - p$, on trouve que

$$\tau_p(\chi - \psi(\chi)) = \widetilde{\chi}(p^2/4u)\widetilde{\chi}(1 + p/(2u-p))^2\zeta^{p-u}$$

Soit $v = 1/(2u-p) = \sum_{i\geq 0} v_i p^i$ avec $0 \leq v_i \leq p-1$. On a $1 + pv \equiv 1 + pv_0 \equiv (1+p)^{v_0} \bmod p^2\mathbb{Z}_p$ donc

$$\widetilde{\chi}(1 + p/(2u-p))^2 = \widetilde{\chi}(1+p)^{2v_0} = \zeta^{-pu2v_0}$$

en utilisant (3.9). On conclut en notant que $2uv_0p \equiv p \bmod p^2\mathbb{Z}_p$. ∎

Le calcul de la résolvante demande de faire une étape supplémentaire.

4.2.3 L'extension pure décomposée

On sait par le théorème 1 et l'hypothèse 4.2.1 que N_p est l'une des sous-extensions ramifiées de degré $n = [N_p : \mathbb{Q}_p]$ de $L.\mathbb{Q}_p\{n\}$. Dans ce paragraphe, on considère le cas où $N_p = L.\mathbb{Q}_p\{n/p\}$. On a alors $\Gamma = C_p \times C_m$ et, pour tout caractère χ de Γ, on peut écrire $\chi = \chi_1\chi_2$, où χ_1 (resp. χ_2) est égal à la restriction de χ à C_p (resp. C_m).

On commence par adapter la formule pour la somme de Gauss à la situation présente. Comme χ_2 est non ramifié, on sait que :

$$\tau_p(\chi_1\chi_2) = \chi_2\big(p^{-r(\chi_1)}\big)\tau_p(\chi_1)$$

où $r(\chi_1) = 2$ si χ_1 est ramifié, 0 sinon. Comme Γ est abélien, on en tire :

$$\tau_p(\chi - \psi(\chi)) = \chi_2\big(p^{r(\chi_1)}\big)\tau_p(\chi_1 - \psi(\chi_1)) \tag{4.3}$$

On déduit du lemme 4.2.6 que pour χ ramifié,

$$\tau_p(\chi_1 - \psi(\chi_1)) = \widetilde{\chi}_1(p^2/4u(\chi_1))\zeta^{-u(\chi_1)} \tag{4.4}$$

en remarquant que $u(\chi) = u(\chi_1)$. On s'intéresse au premier facteur de (4.3). Soit l un premier distinct de p. Comme dans la démonstration du lemme 4.2.5, on considère

$$t = \sigma \sum_{i=1}^{p-1} e_{\theta^i} + e_1 \in \mathbb{Z}_l[\Gamma]^*$$

où θ est un caractère de C_p qui engendre $\widehat{C}_p$, e_{θ^i} est l'idempotent associé au caractère θ^i, e_1 est l'idempotent associé au caractère trivial de C_p, et $\sigma \in C_m$ correspond à p^2 par l'application d'Artin. On a alors :

$$\chi_2\big(p^{r(\chi_1)}\big) = \mathrm{Det}_\chi(t) \tag{4.5}$$

Soit $t_{(p)}$ l'élément de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma, \mathcal{O}_E^*)$ défini par $t_{(p)}(\chi) = \chi_2\left(p^{r(\chi_1)}\right)$. On déduit de (4.5) que $n_{(p)} = \mathrm{Ind}_\Gamma^G t_{(p)}$ appartient à $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, \mathcal{O}_E^*)$ et vérifie, pour tout $l \neq p$:

$$j_l^*(n_{(p)}) \in \mathrm{Det}(\mathbb{Z}_l[G]^*)$$

On peut donc appliquer le lemme 3.2.5 à $k = n_{(p)}$ et $F = \mathbb{Q}$, ce qui ramène à étudier l'application :

$$\chi \in R_G \mapsto (\alpha_p \,|\, \chi)\tau_p(\chi_1 - \psi(\chi_1))$$

On en vient au calcul de la résolvante. On remarque que :

$$\mathcal{A}_{N_p} \simeq \mathcal{A}_L \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{Q}_p\{m\}}$$

si bien que $\alpha_p = \alpha \otimes \beta$, où α_p, α et β sont respectivement des bases locales de $\mathcal{A}_{N_p}$ comme $\mathbb{Z}_p[\Gamma]$-module, de $\mathcal{A}_L$ comme $\mathbb{Z}_p[C_p]$-module et de $\mathcal{O}_{\mathbb{Q}_p\{m\}}$ comme $\mathbb{Z}_p[C_m]$-module. On vérifie :

$$(\alpha_p \,|\, \chi) = (\alpha \,|\, \chi_1)(\beta \,|\, \chi_2) \tag{4.6}$$

Comme C_m est abélien, on a :

$$(\beta \,|\, \chi_2) = \sum_{\sigma \in C_m} \beta^\sigma \chi_2(\sigma^{-1}) = \mathrm{Det}_{\chi_2}\Big(\sum_{\sigma \in C_m} \beta^\sigma \sigma^{-1}\Big)$$

et donc, par [Frö], proposition I.4.3 et à l'aide de (3.4) :

$$\chi \mapsto (\beta \,|\, \chi_2) \in \mathrm{Det}(\mathcal{O}_{\mathbb{Q}_p\{m\}}[\Gamma]^*) \tag{4.7}$$

avec $\mathbb{Q}_p\{m\}/\mathbb{Q}_p$ non ramifiée. On étudie maintenant $(\alpha \,|\, \chi_1)$.

Lemme 4.2.7 *Soit χ_1 un caractère de C_p. Il existe une base locale α de $\mathcal{A}_L$ comme $\mathbb{Z}_p[C_p]$-module et un entier $v(\chi_1)$ avec $0 \leq v(\chi_1) \leq p-1$ tels que :*

$$(\alpha \,|\, \chi_1) = \begin{cases} 1 & \text{si } \chi_1 \text{ est non ramifié} \\ \zeta^{u(\chi_1)+pv(\chi_1)} & \text{si } \chi_1 \text{ est ramifié} \end{cases}$$

Preuve. On sait par [Er1] que $\alpha = \frac{1}{p}(1 + \mathrm{Tr}_{\mathbb{Q}_p[p^2]/L}(\zeta))$ est une base de $\mathcal{A}_L$. Soit r un entier tel que $< r >$ soit d'ordre $p-1$ dans $(\mathbb{Z}/p^2\mathbb{Z})^*$, alors :

$$\alpha = \frac{1}{p}\left(1 + \zeta + \zeta^r + \cdots + \zeta^{r^{p-2}}\right)$$

On doit maintenant calculer $(\alpha \,|\, \chi_1) = \sum_{h \in C_p} \alpha^h \chi_1(h^{-1})$. Soit $h \in C_p \subset \mathrm{Gal}(\mathbb{Q}_p[p^2]/\mathbb{Q}_p)$. On choisit un $\omega' \in \mathrm{Gal}(\mathbb{Q}_{p^\infty}/\mathbb{Q}_p) \subset \Omega^{\mathrm{ab}}_{\mathbb{Q}_p}$ égal à h modulo $\Omega^{\mathrm{ab}}_{\mathbb{Q}_p[p^2]}$. On sait par la remarque 1 de [M3], page 44, que

$$\omega' = A(u_p(\omega))$$

avec $\omega = j_p \omega' j_p^{-1} \in \Omega^{\mathrm{ab}}_{\mathbb{Q}}$ et $u_p(\omega) \in \mathbb{Z}_p^*$ est tel que, si η est une racine de l'unité d'ordre une puissance de p, alors $\eta^{\omega^{-1}} = \eta^{u_p(\omega)}$. De plus, le théorème 2 de [Se2] 3.1, page 146, donne l'action de $A(u_p(\omega))$ sur $\mathbb{Q}_{p^\infty}$. Il découle de ces deux résultats que $\zeta^h = \zeta^{\omega'} = \zeta^{u_p(\omega^{-1})}$. Par ailleurs, on a $\chi_1(h^{-1}) = \widetilde{\chi}_1(u_p(\omega^{-1}))$ et

on note que, puisque $h^p = 1$, on peut écrire $u_p(\omega^{-1}) = 1 + pw + p^2 x$ avec $x \in \mathbb{Z}_p$ et $w \in \{0, 1, \cdots, p-1\}$. On en déduit :

$$\zeta^h = \zeta^{1+wp} \quad \text{et} \quad \chi_1(h^{-1}) = \widetilde{\chi}_1(1+wp) = \widetilde{\chi}_1(1+p)^w$$

Si χ_1 est ramifié, on sait de plus que $\widetilde{\chi}_1(1+p) = \zeta^{-pu(\chi_1)}$, si bien que :

$$\begin{aligned}(\alpha \,|\, \chi_1) &= \frac{1}{p} \sum_{w=0}^{p-1} \left(\zeta^{-pu(\chi_1)w} + \zeta\, \zeta^{pw(1-u(\chi_1))} + \cdots + \zeta^{r^{p-2}} \zeta^{pw(r^{p-2}-u(\chi_1))} \right) \\ &= \frac{1}{p} \underbrace{\sum_{w=0}^{p-1} \zeta^{-pu(\chi_1)w}}_{0} + \frac{1}{p} \sum_{k=0}^{p-2} \zeta^{r^k} \underbrace{\left(\sum_{w=0}^{p-1} \zeta^{pw(r^k - u(\chi_1))} \right)}_{0 \text{ si } r^k \not\equiv u(\chi_1) \bmod p}\end{aligned}$$

Soit k l'unique entier tel que $0 \leq k \leq p-2$ et $r^k \equiv u(\chi_1) \mod p$. Alors :

$$(\alpha \,|\, \chi_1) = \zeta^{u(\chi_1) + pv(\chi_1)}$$

où $v(\chi_1)$ est tel que $0 \leq v(\chi_1) \leq p-1$ et $v(\chi_1) \equiv \frac{r^k - u(\chi_1)}{p} \mod p$. Enfin, si χ_1 est non ramifié, on trouve $(\alpha \,|\, \chi_1) = \frac{1}{p} \sum_w \left(1 + \sum_k \zeta^{r^k(1+wp)} \right) = 1$, ce qui termine la preuve du lemme. ∎

On considère l'application $\varphi \in \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{C_p,p}, \mathcal{O}_{E_p}^*)$ définie sur $\chi_1 \in R_{C_p,p}$ par :

$$\varphi(\chi_1) = (\alpha \,|\, \chi_1) \tau_p(\chi_1 - \psi(\chi_1))$$

On sait par [Er3], théorème 2', que $\varphi \in \mathrm{Det}(\mathcal{M}^*)$, où $\mathcal{M}$ est l'ordre maximal de $\mathbb{Q}_p[C_p]$ contenant $\mathbb{Z}_p[C_p]$. Dans la situation présente, on en tire le résultat :

Lemme 4.2.8 $\varphi \in \mathrm{Det}(\mathbb{Z}_p[C_p]^*)$.

Preuve. On déduit du lemme 4.2.7 et de l'égalité (4.4) que pour tout $\chi_1 \in R_{C_p,p}$:

$$\varphi(\chi_1) = \begin{cases} 1 & \text{si } \chi_1 \text{ est non ramifié} \\ \widetilde{\chi}_1(p^2/4u(\chi_1)) \zeta^{pv(\chi_1)} & \text{si } \chi_1 \text{ est ramifié} \end{cases}$$

Soit ε_1 le caractère trivial de C_p. Puisque $\widetilde{\chi}_1$ est à valeurs dans les racines p-ièmes de l'unité, on observe que

$$\varphi(\chi_1 - \varepsilon_1) = \varphi(\chi_1) \equiv 1 \mod \mathcal{P} \tag{4.8}$$

où $\xi = \zeta^p$ et $\mathcal{P} = (1-\xi)$ est l'idéal maximal de l'anneau $\mathbb{Z}_p[\xi]$. Or on a une injection :

$$\begin{array}{ccccccc} \mathbb{Z}_p[C_p] & \hookrightarrow & \mathbb{Z}_p & \oplus & \mathbb{Z}_p[\xi] & \simeq & \mathcal{M} \\ \sum n_g g & \mapsto & \left(\sum n_g \varepsilon_1(g) \right. & , & \left. \sum n_g \theta(g) \right) & & \end{array}$$

où θ est le caractère de C_p tel que $\theta(g) = \xi^g$ via l'identification $C_p \simeq \mathbb{Z}/p\mathbb{Z}$. Pour $(a,b) \in \mathcal{M}$, on a l'équivalence :

$$(a,b) \in \mathbb{Z}_p[C_p] \Leftrightarrow a \equiv b \bmod \mathcal{P}$$

En effet, si $(a,b) \in \mathbb{Z}_p[C_p]$, alors $a = \sum n_g$ et $b = \sum n_g\theta(g)$ pour des $n_g \in \mathbb{Z}_p$ et donc $a - b = \sum n_g(1-\theta(g)) \in \mathcal{P}$. Si $a \equiv b \bmod \mathcal{P}$ et $b = \sum n_g\xi^g$, alors $a \equiv \sum n_g \bmod \mathcal{P}$ et $a - \sum n_g \in \mathcal{P} \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Soit $c \in \mathbb{Z}_p$ tel que $a = pc + \sum n_g$. On pose $n'_g = n_g + c$, alors :

$$a = \sum n'_g \quad \text{et} \quad b = \sum n'_g\xi^g$$

et $(a,b) \in \mathbb{Z}_p[C_p]$.

Soit $u = (a,b) \in \mathcal{M}^*$ tel que $\varphi = \mathrm{Det}(u)$. Alors $a = \varphi(\varepsilon_1)$ et $b = \varphi(\theta)$. On tire de (4.8) :

$$a \equiv b \mod \mathcal{P}$$

si bien que $u \in \mathbb{Z}_p[C_p]^*$ et $\varphi \in \mathrm{Det}(\mathbb{Z}_p[C_p]^*)$. ▮

On déduit immédiatement de ce lemme que $\mathrm{Ind}_{C_p}^{\Gamma}\varphi \in \mathrm{Det}(\mathbb{Z}_p[\Gamma]^*)$ puis, grâce à (4.6) et (4.7) :

$$\chi \in R_{\Gamma,p} \mapsto (\alpha_p \,|\, \chi)\tau_p(\chi_1 - \psi(\chi_1)) \in \mathrm{Det}(\mathcal{O}_{\mathbb{Q}_p\{m\}}[\Gamma]^*)$$

Il ne reste qu'à reprendre le lemme 3.2.5 pour en déduire :

Lemme 4.2.9 *On suppose $N_p = L.\mathbb{Q}_p\{n/p\}$, alors il existe une extension non ramifiée $B_p/\mathbb{Q}_p$ telle que $h_{(p)} \in \mathrm{Det}(\mathcal{O}_{B_p}[\Gamma]^*)$.*

4.2.4 Toutes les extensions pures

On traite maintenant le cas général, c'est-à-dire que N_p est l'une quelconque des sous-extensions ramifiées de degré n de $L.\mathbb{Q}_p\{n\} = \widetilde{N}_p$. On remarque que $\widetilde{N}_p/\mathbb{Q}_p$ est faiblement ramifiée et décomposée et que $\widetilde{N}_p/N_p$ est non ramifiée. On note Γ le groupe de Galois de $N_p/\mathbb{Q}_p$ et $\widetilde{\Gamma}$ celui de $\widetilde{N}_p/\mathbb{Q}_p$. D'après le lemme 4.2.9, on sait qu'il existe une extension non ramifiée $\widetilde{B}_p/\mathbb{Q}_p$ telle que l'application $\widetilde{h}_{(p)}$ associée à $\widetilde{N}_p/\mathbb{Q}_p$ vérifie :

$$\widetilde{h}_{(p)} \in \mathrm{Det}(\mathcal{O}_{\widetilde{B}_p}[\widetilde{\Gamma}]^*)$$

De plus, puisque Γ est un quotient de $\widetilde{\Gamma}$, on a l'application :

$$\begin{array}{ccc} \mathrm{Hom}(R_{\widetilde{\Gamma}}, O_E^*) & \to & \mathrm{Hom}(R_\Gamma, O_E^*) \\ \varphi & \mapsto & \varphi' \end{array}$$

avec, pour tout caractère χ de Γ, $\varphi'(\chi) = \varphi(\mathrm{Inf}_\Gamma^{\widetilde{\Gamma}}(\chi))$. On veut connaître l'image $\widetilde{h}'_{(p)}$ de $\widetilde{h}_{(p)}$ par cette application. Or, pour $\widetilde{\chi} \in R_{\widetilde{\Gamma},p}$,

$$\widetilde{h}_{(p)}(\widetilde{\chi}) = (\widetilde{\alpha}_p \,|\, \widetilde{\chi})\tau_p(\widetilde{\chi} - \psi(\widetilde{\chi}))$$

où $\widetilde{\alpha}_p$ est une base de $A_{\widetilde{N}_p}$. On sait que, pour $\chi \in R_{\Gamma,p}$, $\tau_p(\mathrm{Inf}_\Gamma^{\widetilde{\Gamma}}(\chi)) = \tau_p(\chi)$ et, comme $\widetilde{N}_p/N_p$ est non ramifiée :

$$(\widetilde{\alpha}_p \,|\, \mathrm{Inf}_\Gamma^{\widetilde{\Gamma}}(\chi)) = \sum_{g\in\widetilde{\Gamma}} \widetilde{\alpha}_p{}^g \mathrm{Inf}_\Gamma^{\widetilde{\Gamma}}(\chi)(g^{-1}) = \left(\mathrm{Tr}_{\widetilde{N}/N}(\widetilde{\alpha}_p) \,|\, \chi\right) = (\alpha_p \,|\, \chi)$$

grâce à la remarque 1.3.7, valable aussi pour la racine carrée de la codifférente. On a donc $\widetilde{h}'_{(p)} = h_{(p)}$. On en déduit, à l'aide des propriétés fonctorielles :

$$h_{(p)} \in \mathrm{Det}(\mathcal{O}_{\widetilde{B}_p}[\Gamma]^*)$$

où $\Gamma = G(p)$, puis $j_p^*(f_{(p),p}) \in \mathrm{Det}(\mathcal{O}_{\widetilde{B}_p}[G]^*)$ avec $\widetilde{B}_p/\mathbb{Q}_p$ non ramifiée. Conjointement avec les lemmes 4.1.2 et 4.2.3, ceci entraîne qu'il existe une extension modérément ramifiée $W/\mathbb{Q}_p$ telle que :

$$j_p^*(f_p) \in \mathrm{Det}(\mathcal{O}_W[G]^*)$$

Il ne reste qu'à appliquer le théorème des points fixes pour en déduire :

Proposition 4.2.10 *Soit N/K avec $K = \mathbb{Q}$ comme dans l'introduction de ce chapitre, vérifiant l'hypothèse 4.2.1 et soit p un nombre premier correspondant à une place sauvage de $N/\mathbb{Q}$. Alors $j_p^*(f_p) \in \mathrm{Det}(\mathbb{Z}_p[G]^*)$.*

Conjointement avec la proposition 4.2.2, ce résultat prouve le théorème 3.

4.3 Majoration dans les p-extensions

Soient p un premier supérieur ou égal à 3 et $N/\mathbb{Q}$ une p-extension finie galoisienne de groupe G, faiblement ramifiée. On sait par le corollaire 1.1.6 que le groupe d'inertie Γ_0 de $N_p/\mathbb{Q}_p$ est abélien p-élémentaire. On note $e(p) = |\Gamma_0|$ l'indice de ramification en p dans $N/\mathbb{Q}$. Cette partie est consacrée à la preuve du résultat suivant.

Théorème 4 *Avec les notations introduites ci-dessus, on a $(\mathcal{A}_N)^{e(p)} = 1$.*

Si le groupe de décomposition en p est abélien, on sait que $(\mathcal{A}_N)$ est trivial par le théorème 3. Sinon, on sait par le théorème 2 de [Er3] que $(\mathcal{A}_N) \in D(\mathbb{Z}[G])$. Soit n tel que $|G| = p^n$, alors l'exposant de $D(\mathbb{Z}[G])$ divise p^{n-1} par le théorème 3.1 de [U], si bien que :

$$(\mathcal{A}_N)^{p^{n-1}} = 1$$

Le théorème 4 améliore cette majoration en la ramenant à l'ordre du groupe d'inertie en p. Si l'on considère l'extension faiblement ramifiée de groupe de Galois isomorphe à $C_9 \rtimes C_3$ présentée dans le paragraphe 1.4.3, il donne le même résultat que l'estimation ci-dessus : l'ordre de $(\mathcal{A}_N)$ divise 9. Par contre, si on la compose avec une 3-extension dans laquelle 3 est inerte, le théorème 4 montre que l'ordre divise encore 9, tandis que l'exposant de l'estimation ci-dessus augmente.

4.3.1 Etude de la somme de Gauss

Par le corollaire 3.2.4, on ne doit se préoccuper que de :

$$j_p^*(f_p) = j_p^*(f_{(p),p}) \prod_{l \neq p} j_p^*(f_{(l),p}^*)$$

où l décrit l'ensemble des diviseurs premiers distincts de p du discriminant de l'extension. Le lemme 4.1.2 traite les facteurs en l, ce qui nous ramène à étudier $j_p^*(f_{(p),p})$. C'est le produit d'une résolvante par une somme de Gauss et on a le résultat suivant pour la puissance p-ième de la somme de Gauss.

Lemme 4.3.1 *Sous les hypothèses du théorème 4, soit $m_p \in \mathrm{Hom}(R_G, E^*)$ la fonction définie par $m_p(\chi) = \tau_p(\chi - \psi(\chi))$ pour tout $\chi \in R_G$. Alors ${m_p}^p \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, \mathcal{O}_E^*)$ et, pour tout nombre premier l distinct de p, on a $j_l^*({m_p}^p) \in \mathrm{Det}(\mathbb{Z}_l[G]^*)$.*

Preuve. Puisque G est un p-groupe, la deuxième assertion découle de la première. Montrons celle-ci. Par définition des sommes de Gauss locales, on note que $m_p = \mathrm{Ind}_\Gamma^G n_p$, où Γ est le groupe de Galois de l'extension $N_p/\mathbb{Q}_p$ (identifié au groupe de décomposition en p) et, pour tout $\chi \in R_\Gamma$, $n_p(\chi) = \tau_p(\chi - \psi(\chi))$. Supposons χ irréductible. On sait par la proposition 3.4.1 que $\chi = \mathrm{Ind}_{\Sigma_i}^\Gamma \varphi_{i,j}$ où $\varphi_{i,j}$ est un caractère abélien de Σ_i. On a donc par la propriété d'induction en degré 0 des sommes de Gauss :

$$n_p(\chi) = \tau_p(\varphi_{i,j} - \varphi_{i,j}^2)$$

Le lemme 3.4.6 montre qu'il s'agit d'une racine de l'unité d'ordre une puissance de p, si bien que n_p et m_p sont à valeurs dans $\mathcal{O}_E^*$. Etudions maintenant l'action galoisienne sur n_p. Soit $\omega \in \Omega_\mathbb{Q}$, on déduit du corollaire 5.2 de [M3] :

$$n_p(\chi^{\omega^{-1}})^\omega = \varphi_{i,j}(u_p(\omega))^{-1} n_p(\chi)$$

où $u_p(\omega)$ est l'unique élément de $\mathbb{Z}_p^*$ tel que $\eta^{\omega^{-1}} = \eta^{u_p(\omega)}$ pour tout η racine p^n-ième de l'unité de $\mathbb{Q}_p^c$ (n entier quelconque). Puisque $u_p(\omega)$ est une unité, son image dans $\mathrm{Gal}(N_p/N_p^{\Sigma_i})$ par l'application d'Artin est un élément du groupe d'inertie Γ_0, donc son ordre est 1 ou p. Comme $\varphi_{i,j}$ est un caractère abélien, on en tire que $\varphi_{i,j}(u_p(\omega))^p = 1$, c'est-à-dire que ${n_p}^p$ et donc ${m_p}^p$ commutent à l'action de $\Omega_\mathbb{Q}$. ∎

On en déduit que $(\mathcal{A}_N)^p$ est représenté dans $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$ par la fonction $g = (f{m_p}^{-1})^p$, ce qui ramène à étudier $j_p^*(f_{(p),p}{m_p}^{-1})^p = \mathrm{Ind}_\Gamma^G(h_p)^p$ où h_p est l'élément de $\mathrm{Hom}(R_{\Gamma,p}, \mathcal{O}_{E_p}^*)$ défini par :

$$h_p(\chi) = (\alpha_p \,|\, \chi)$$

α_p étant une base normale de la racine carrée de la codifférente locale $\mathcal{A}_{N_p/\mathbb{Q}_p}$.

4.3.2 Etude de la résolvante

L'objet de ce paragraphe est de montrer :

Proposition 4.3.2 $h_p^{(q-1)e(p)} \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma]^*)$.

Preuve. On commence par se ramener au groupe d'inertie Γ_0 de l'extension. L'égalité (6.3) de [Er3], que l'on retranscrit dans le lemme suivant, donne le comportement de la résolvante par rapport à la restriction $\mathrm{Res} = \mathrm{Res}_{\Gamma_0}^{\Gamma}$ des caractères au groupe d'inertie. On note N_0 la sous-extension de $N_p/\mathbb{Q}_p$ fixée par Γ_0 et β_p une base de $\mathcal{A}_{N_p/\mathbb{Q}_p}$ comme $\mathcal{O}_{N_0}[\Gamma_0]$-module. On a :

Lemme 4.3.3 *Il existe $\lambda \in \mathcal{O}_{N_0}[\Gamma]^*$ tel que, pour tout $\chi \in R_\Gamma$:*

$$(\alpha_p \,|\, \chi) = (\beta_p \,|\, \mathrm{Res}\,\chi)\mathrm{Det}_\chi(\lambda)$$

Soit k_p l'élément de $\mathrm{Hom}(R_{\Gamma_0,p}, E_p^*)$ défini par $k_p(\theta) = (\beta_p \,|\, \theta)$ pour tout $\theta \in R_{\Gamma_0,p}$. On déduit du lemme précédent que

$$h_p = \mathrm{Ind}_{\Gamma_0}^{\Gamma}(k_p)\mathrm{Det}(\lambda) \tag{4.9}$$

Soit θ un caractère de Γ_0, on sait par la preuve de la proposition 7.6 de [Er3] que $(\beta_p \,|\, \theta)$ est à valeurs dans les unités, si bien que k_p est une fonction de caractères à valeurs dans $\mathcal{O}_{E_p}^*$. La proposition I.4.4 de [Frö] donne l'action de $\omega \in \Omega_{N_0}$ sur la résolvante :

$$(\beta_p \,|\, \theta^{\omega^{-1}})^\omega = (\beta_p \,|\, \theta)\mathrm{Det}_\theta(\omega)$$

Comme Det_θ est un caractère de Γ_0 qui est d'exposant p, on en déduit :

$$(k_p)^p \in \mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0,p}, \mathcal{O}_{E_p}^*)$$

Soit $\mathcal{M}_0$ un ordre maximal de $N_0[\Gamma_0]$ contenant $\mathcal{O}_{N_0}[\Gamma_0]$. On sait par le lemme précédent qu'il existe $u \in \mathrm{Det}(\mathcal{M}_0^*)$ tel que $(k_p)^p = \mathrm{Det}(u)$. De plus, en notant $|\Gamma_0| = p^m$ et $r = 1 + p + \cdots + p^{m-1}$, on a les décompositions :

$$N_0[\Gamma_0] = N_0 \oplus \left(N_0(\zeta_p)^{\oplus r}\right), \qquad \mathcal{M}_0 = \mathcal{O}_{N_0} \oplus \left(\mathcal{O}_{N_0(\zeta_p)}{}^{\oplus r}\right)$$

donc u s'écrit $(u_0, u_1, \ldots, u_r)$, avec $u_0 \in \mathcal{O}_{N_0}^* \simeq \mu_{q-1} \times (1 + p\mathcal{O}_{N_0})$ et $u_i \in \mathcal{O}_{N_0(\zeta_p)}^* \simeq \mu_{q-1} \times (1 + \pi\mathcal{O}_{N_0(\zeta_p)})$ pour $1 \leq i \leq r$, où $q = p^f$ est le cardinal du corps résiduel de N_0 et π est une uniformisante de $N_0(\zeta_p)$.

Lemme 4.3.4 *On a $u^{(q-1)p^{m-1}} \in \mathcal{O}_{N_0}[\Gamma_0]^*$.*

Preuve. Le théorème de Jacobinski ([CR1] 27.8) décrit le conducteur F de $\mathcal{M}_0$ dans $\mathcal{O}_{N_0}[\Gamma_0]$. Le calcul donne :

$$F = p^m\mathcal{O}_{N_0} \oplus \left(p^m\pi^{1-p}\mathcal{O}_{N_0(\zeta_p)}{}^{\oplus r}\right)$$

Soit $x = u^{q-1} = (1 + pa_0, 1 + \pi a_1, \ldots, 1 + \pi a_r)$, où $a_0 \in \mathcal{O}_{N_0}$ et $a_i \in \mathcal{O}_{N_0(\zeta_p)}$. On a :

$$x_0{}^{p^{m-1}} = 1 + \sum_{k=1}^{p^{m-1}} \binom{p^{m-1}}{k} (pa_0)^k \quad \text{et} \quad x_i{}^{p^{m-1}} = 1 + \sum_{k=1}^{p^{m-1}} \binom{p^{m-1}}{k} (\pi a_i)^k$$

Or, la valuation du cœfficient binômial, qui est minimale lorsque k est divisible par p, disons $k = p^b u$ avec $(p, u) = 1$, vaut dans ce cas $m - 1 - b$ (voir [U] pour un calcul similaire). On en déduit aisément que $x_0{}^{p^{m-1}} \equiv 1 \bmod p^m \mathcal{O}_{N_0}$ et que $x_i{}^{p^{m-1}}$ est congru à 1 modulo $\pi^{(p-1)(m-1)}\mathcal{O}_{N_0(\zeta_p)} = p^m \pi^{1-p} \mathcal{O}_{N_0(\zeta_p)}$, si bien que $x^{p^{m-1}} = u^{(q-1)p^{m-1}} \in F\mathcal{M}_0 = \mathcal{O}_{N_0}[\Gamma_0]$. Il ne reste qu'à noter que

$$\mathcal{M}_0^* \cap \mathcal{O}_{N_0}[\Gamma_0] = \mathcal{O}_{N_0}[\Gamma_0]^*$$

pour achever la démonstration du lemme. ∎

On sait maintenant que $k_p{}^{(q-1)e(p)} \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma_0]^*)$. On termine la preuve de la proposition 4.3.2 grâce à (4.9) et aux propriétés relatives à l'induction. ∎

4.3.3 Fin de la preuve du théorème 4

On est maintenant en mesure de terminer la preuve du théorème 4. On déduit de la proposition précédente que

$$j_p^*(f_{(p),p} m_p{}^{-1})^{(q-1)e(p)} \in \mathrm{Det}(\mathcal{O}_{N_0}[G]^*)$$

On voit alors à l'aide des lemmes 4.1.2 et 4.3.1 qu'il existe une extension non ramifiée $B_p/\mathbb{Q}_p$ telle que $j_p^*(f_p m_p{}^{-1})^{(q-1)e(p)} \in \mathrm{Det}(\mathcal{O}_{B_p}[G]^*)$ Le théorème des points fixes entraîne alors :

$$j_p^*(f_p m_p{}^{-1})^{(q-1)e(p)} \in \mathrm{Det}(\mathbb{Z}[G]^*)$$

c'est-à-dire $(\mathcal{A}_N)^{(q-1)e(p)} = 1$. Mais on sait que $(\mathcal{A}_N) \in D(\mathbb{Z}[G])$ et, comme G est un p-groupe, $D(\mathbb{Z}[G])$ en est un aussi. Il s'ensuit que $(\mathcal{A}_N)^{e(p)} = 1$, ce qui est le résultat annoncé.

Chapitre 5

Calculs de réseaux

On s'intéresse ici au réseau obtenu en munissant de la forme trace la racine carrée de la codifférente d'une extension galoisienne N/K de corps de nombres de degré impair, de groupe de Galois G. On a vu dans la partie 3.1 que ce réseau est entier unimodulaire et stable sous l'action de G. On peut donc le comparer au G-réseau entier unimodulaire "standard", obtenu en munissant $\mathbb{Z}[G]$ de la forme q_G qui rend orthonormale la base de $\mathbb{Z}[G]$ formée des éléments de G. Plus précisément, on veut déterminer s'il existe une isométrie commutant à l'action de G entre ces deux réseaux (une G-isométrie) ou, de façon équivalente, si les modules hermitiens $(\mathcal{A}_{N/K}, t_{N/K})$ et $(\mathbb{Z}[G], m_G)$ sont isomorphes (voir le paragraphe 3.1.3). Notons pour faire le lien avec le chapitre précédent que l'existence d'une G-isométre entre les deux réseaux (ou d'un isomorphisme entre les deux modules hermitiens) entraîne la liberté de la racine carrée de la codifférente $\mathcal{A}_{N/K}$ comme $\mathbb{Z}[G]$-module.

Plusieurs travaux ont été consacrés à cette question ainsi qu'à un problème similaire pour l'anneau d'entiers. Les principaux résultats concernant la racine carrée de la codifférente dont on dispose sont :

1. on suppose G abélien et $K = \mathbb{Q}$. Alors $N/\mathbb{Q}$ est faiblement ramifiée si et seulement si $(\mathcal{A}_N, \mathrm{Tr})$ est G-isométrique à $(\mathbb{Z}[G], q_G)$;
2. on suppose N/K modérément ramifiée, alors $(\mathcal{A}_{N/K}, t_{N/K})$ est stablement isomorphe à $(\mathbb{Z}[G], m_G)$,

où *stablement isomorphe* signifie qu'il existe un module hermitien H tel que $\mathcal{A}_{N/K} \oplus H$ et $\mathbb{Z}[G] \oplus H$ soient isomorphes. Le premier de ces résultats se trouve dans la thèse d'Erez ([Er1]) ; il est repris dans [ErM] qui traite en parallèle le réseau associé à l'anneau d'entiers. Le second et son analogue pour l'anneau d'entiers apparaissent dans [ErT]. Précisons que des résultats analogues valables dans la situation très sauvagement ramifiée se trouvent dans [BEr].

Lorsque N/K est une extension faiblement ramifiée qui n'est ni abélienne absolue, ni modérée, on ne sait rien du réseau associé à sa racine carrée de la codifférente. L'idée de calculer celui-ci sur les exemples de telles extensions présentés dans la partie 2.3 est venue de C. Bachoc. Son aide pour programmer

l'algorithme de calcul (que l'on présente dans le paragraphe 5.4) sur le logiciel Magma ([BoCa]) a été déterminante. Une des conséquences de ces calculs est le résultat suivant.

Théorème 5 *Soit N/K une extension faiblement ramifiée de corps de nombres de degré impair, de groupe de Galois G. Le réseau $(\mathcal{A}_{N/K}, \mathrm{Tr})$ n'est pas toujours isométrique à $(\mathbb{Z}[G], q_G)$. En particulier, il existe des extensions vérifiant les hypothèses du théorème 3 ainsi que des extensions modérées pour lesquelles ce n'est pas le cas.*

Le résultat de l'item 1 ne se généralise donc pas aux extensions non abéliennes et "stablement" ne peut pas être omis dans l'énoncé du résultat de l'item 2. De plus, on voit que l'isomorphisme de $\mathbb{Z}[G]$-modules énoncé dans le théorème 3 ne provient pas nécessairement d'une G-isométrie comme cela est le cas pour les extensions abéliennes absolues d'après l'item 1.

Le théorème 5 provient des calculs menés sur plusieurs familles d'exemples d'extensions faiblement ramifiées non abéliennes, dont les résultats sont présentés dans les parties 5.1 et 5.2 pour le cas sauvage, et dans la partie 5.3 pour le cas modéré. Un résultat supplémentaire est obtenu pour les extensions absolues faiblement ramifiées de degré 27 : si le réseau associé à la racine carrée de la codifférente d'une telle extension est de minimum 3, on le détermine explicitement grâce à la classification de [BV] (théorème 5.1.2).

Jusqu'à présent, l'auteur ne connaît pas de moyen pour interpréter plus avant les résultats de ces calculs. En particulier, est-il possible de prévoir quand $(\mathcal{A}_N, \mathrm{Tr})$ et $(\mathbb{Z}[G], q_G)$ sont isométriques ? Une autre question, sans doute plus abordable avec les techniques connues, est de déterminer si la propriété de l'item 2 ci-dessus est encore valable pour une extension faiblement ramifiée, par exemple avec des hypothèses semblables à celles du théorème 3. Enfin, pour en revenir aux calculs, il pourrait être intéressant d'essayer de déterminer, sur les exemples où il n'y a pas isométrie, si les modules hermitiens associés aux deux réseaux sont tout de même stablement isomorphes.

Un autre aspect des résultats présentés dans les prochaines parties concerne la structure galoisienne de la racine carrée de la codifférente $\mathcal{A}$. Dès les premiers calculs, des réseaux non isométriques à $\mathbb{Z}[G]$ sont apparus. Il était alors très tentant d'essayer de savoir —par le calcul— si $\mathcal{A}$ était tout de même libre en tant que $\mathbb{Z}[G]$-module. Il a fallu pour cela trouver d'autres outils ; c'est B. Allombert qui les a fourni, en même temps que des conseils d'utilisation très précieux. L'algorithme ([A]) qu'il a récemment implanté dans le logiciel Pari ([3BCO]) donne de façon explicite l'action du groupe de Galois d'une extension de $\mathbb{Q}$. On l'applique pour trouver les images sous l'action de G d'un vecteur du réseau associé à $\mathcal{A}$ et on regarde si le sous-réseau engendré par son orbite est égal au réseau tout entier. On constate que, si quelques vecteurs minimaux (mais pas tous) engendrent des bases normales dans certains cas, il faut parfois considérer les vecteurs de norme 5 (de réseaux de minimum 2) pour en obtenir. Il ne semble d'ailleurs pas y avoir de raison pour que ce soient des vecteurs de petite norme qui fournissent des bases normales. Précisons pour finir que,

dans tous les cas où le calcul a été mené, la racine carrée de la codifférente s'est révélée être un $\mathbb{Z}[G]$-module libre.

On présente maintenant les résultats de tous ces calculs et on termine par la description succinte de l'algorithme utilisé.

5.1 La famille d'extensions de la partie 2.3

Soit $t \in \mathbb{Z}$. On note $v = t^2 - t + 1$ et on considère la famille de polynômes paramétrée par t :

$$\begin{aligned} P_t(x) &= x^9 - 9vx^7 + 27v^2x^5 - 30v^3x^3 + 9v^4x \\ &\quad -(2t-1)(t^6 - 3t^5 - 12t^4 + 29t^3 - 3t^2 - 12t + 1)v \end{aligned}$$

On sait par le théorème 2 que le corps de décomposition D de P_t spécialisé en une valeur entière de t est galoisien sur $\mathbb{Q}$ de groupe de Galois isomorphe à $C_9 \rtimes C_3$ et faiblement ramifié pour une infinité de valeurs de t congrues à 5 modulo 9. Les calculs sur le réseau associé à la racine carrée de la codifférente donnent les résultats suivants.

Proposition 5.1.1 *Pour $t \in \{5, 14, 23, 41\}$, D est une extension galoisienne de $\mathbb{Q}$ de groupe de Galois G isomorphe à $C_9 \rtimes C_3$.*

(i) Pour $t \in \{14, 41\}$, $(\mathcal{A}_D, \mathrm{Tr})$ est isométrique à $(\mathbb{Z}[G], q_G)$. En particulier, $\mathcal{A}_D$ est un $\mathbb{Z}[G]$-module libre.

(ii) Pour $t \in \{5, 23\}$, $(\mathcal{A}_D, \mathrm{Tr})$ est un réseau unimodulaire de rang 27 de minimum 3; $\mathcal{A}_D$ est un $\mathbb{Z}[G]$-module libre acceptant certains vecteurs minimaux de $(\mathcal{A}_D, \mathrm{Tr})$ comme base.

On note que (i) correspond au cas où le groupe de décomposition en 3 est abélien, tandis que (ii) correspond au cas où il est égal à G. On verra apparaître un autre type de comportement dans le prochain paragraphe.

On peut déterminer précisément le réseau de minimum 3 obtenu dans le deuxième cas grâce à la classification de Bacher et Venkov ([BV]) des réseaux entiers unimodulaires de rang 27 et 28 sans racines (éléments du réseau de norme 1 ou 2) .

Théorème 5.1.2 *Soit N une extension faiblement ramifiée de $\mathbb{Q}$ de degré 27. Si $(\mathcal{A}_N, \mathrm{Tr})$ est de minimum 3, alors $(\mathcal{A}_N, \mathrm{Tr})$ est le seul réseau unimodulaire de rang 27 de minimum 3 à 2664 vecteurs minimaux et à 3317760 automorphismes.*

Preuve. On consulte la table 4 de [BV] des réseaux entiers unimodulaires de rang 27 sans racines. Il y en a trois. $(\mathcal{A}_N, \mathrm{Tr})$ ne peut pas être le premier d'entre eux puisque le cardinal de son groupe d'automorphismes (7680) n'est pas divisible par 27. Le dernier a 1640 vecteurs de norme 3. Pour que $(\mathcal{A}_N, \mathrm{Tr})$ puisse lui être égal, il faut que l'ensemble de ces vecteurs soit stable sous l'action de G. Mais 1640 n'est pas divisible par 3, donc certains vecteurs minimaux doivent être fixés par G, c'est-à-dire provenir d'éléments de $\mathbb{Q}$. Si

$x \in \mathbb{Q}$ est l'un d'entre eux, alors $3 = \mathrm{Tr}_{N/\mathbb{Q}}(x^2) = 27x^2$ et donc $x = \pm 1/3$. Soit $\mathfrak{p}$ un idéal premier de N au-dessus de 3, on note $e = e(\mathfrak{p}/3)$ et on obtient $v_{\mathfrak{p}}(x) = -e$. Puisque $N/\mathbb{Q}$ est faiblement ramifiée, on tire de la formule de Hilbert que $v_{\mathfrak{p}}(\mathcal{A}_N) = 1 - e$, d'où l'on déduit que $x \notin \mathcal{A}_N$. Il s'ensuit que $(\mathcal{A}_N, \mathrm{Tr})$ ne peut pas être ce réseau. Par élimination, $(\mathcal{A}_N, \mathrm{Tr})$ est donc le deuxième réseau de la classification, qui est décrit dans le théorème. ∎

L'idée de prouver que ce réseau était le seul possible a été suggérée à l'auteur par J. Martinet.

5.2 Une autre famille d'extensions faiblement ramifiées

La famille considérée dans le paragraphe précédent n'est pas régulière (voir [Ei2] partie 6 pour une définition précise) : tous les corps de décomposition contiennent la sous-extension de $\mathbb{Q}(\zeta_9)$ de degré 3 et les extensions ne sont donc pas linéairement disjointes sur $\mathbb{Q}$. La famille que l'on étudie maintenant est régulière ; elle a été communiquée à l'auteur par Eichenlaub. On pose $u = 12t^2 - 30t + 109$ et $v = t^2 - 3t + 9$. On considère la famille de polynômes :

$$\begin{aligned} R_t(x) \;=\; & x^9 - 3^3 u\, x^7 - 2^1 3^3 (t-1) u\, x^6 + 2^5 3^4 v u\, x^5 + 2^4 3^4 (6t-13) v u\, x^4 \\ & - 2^4 3^3 (175t^2 - 495t + 1629) v u\, x^3 - 2^5 3^5 (33t - 103) v^2 u\, x^2 \\ & + 2^6 3^5 (7t^2 + 54t + 51) v^2 u\, x - 2^7 3^3 (3t^3 + 73t^2 - 75t + 1791) v^2 u \end{aligned}$$

Le corps de décomposition de $R_t(x)$ spécialisé en une valeur entière de t est galoisien sur $\mathbb{Q}$ de groupe de Galois G isomorphe à $C_9 \rtimes C_3$ pour une infinité de valeurs de t. Pour chaque valeur de t considérée dans la suite, on note R le corps de rupture de la spécialisation de R_t, D son corps de décomposition et $(\mathcal{A}_D, \mathrm{Tr})$ le G-réseau unimodulaire de dimension 27 obtenu en restreignant la forme trace à la racine carrée de la codifférente de D. Les résultats des calculs sont les suivants :

Proposition 5.2.1 *Pour toutes les valeurs de t considérées ci-dessous, D est une extension galoisienne faiblement ramifiée de $\mathbb{Q}$ de groupe de Galois G isomorphe à $C_9 \rtimes C_3$.*

(i) pour $t \in \{12, 21, 30\}$, $v_3(d_R) = 0$, $D/\mathbb{Q}$ est modérée et $(\mathcal{A}_D, \mathrm{Tr})$ est G-isométrique à $(\mathbb{Z}[G], q_G)$.

(ii) pour $t = 24$, $v_3(d_R) = 12$, le groupe de décomposition en 3 est abélien et $(\mathcal{A}_D, \mathrm{Tr})$ est G-isométrique à $(\mathbb{Z}[G], q_G)$.

(iii) pour $t \in \{9, 18, 27\}$, $v_3(d_R) = 12$, le groupe de décomposition en 3 est non abélien et $(\mathcal{A}_D, \mathrm{Tr})$ est le réseau de minimum 3 du théorème 5.1.2. Certains vecteurs minimaux de $(\mathcal{A}_D, \mathrm{Tr})$ engendrent des bases normales de $\mathcal{A}_D$.

(iv) pour $t \in \{15, 33\}$, $v_3(d_R) = 8$, le groupe de décomposition en 3 est abélien et $(\mathcal{A}_D, \mathrm{Tr})$ est un réseau de minimum 2 à 216 vecteurs minimaux et 3960

vecteurs de norme 3. *Aucun vecteur de norme* 2, 3 *ou* 4 *n'engendre de base normale de* $\mathcal{A}_D$, *certains vecteurs de norme* 5 *en engendrent.*

Au vu de ces résultats, il semble bien que le comportement de toutes les extensions de cette famille soit déterminé par la congruence de t modulo 27.

Remarque 5.2.2 Les exemples (iv) de la proposition ci-dessus montrent que l'isomorphisme de $\mathbb{Z}[G]$-modules du théorème 3 ne provient pas toujours d'une G-isométrie entre les réseaux.

5.3 Calcul dans des extensions modérées

On considère le polynôme paramétré par $t \in \mathbb{Z}$:

$$\begin{aligned} Q_t(X) &= X^7 - 7(t^2-t+2)X^5 + 14(t^2-t+2)^2X^3 - 7(t^2-t+2)^3X \\ &\quad -(2t-1)(t^2-t+2)(t^4-2t^3-16t^2+17t+11) \end{aligned}$$

On sait par le théorème 2.4.2 que le corps de décomposition M de Q_t spécialisé en une valeur entière de t est galoisien sur $\mathbb{Q}$ de groupe de Galois isomorphe à $C_7 \rtimes C_3$ et modéré pour une infinité de valeurs de t congrues à 25 modulo 49.

Les résultats des calculs sont :

Proposition 5.3.1 *Pour* $t \in \{25, 74, 123\}$, M *est une extension galoisienne de* $\mathbb{Q}$ *de groupe de Galois* G *isomorphe à* $C_7 \rtimes C_3$.

(i) Pour $t = 25$, $(\mathcal{A}_M, \mathrm{Tr})$ *est isométrique à* $(\mathbb{Z}[G], q_G)$.

(ii) Pour $t \in \{74, 123\}$, $(\mathcal{A}_M, \mathrm{Tr})$ *est le seul réseau unimodulaire de rang 21 de minimum 2 à 84 vecteurs minimaux ; $\mathcal{A}_M$ est un $\mathbb{Z}[G]$-module libre acceptant certains vecteurs de norme 3 de $(\mathcal{A}_M, \mathrm{Tr})$ comme base.*

Remarque 5.3.2 Pour $t = 25$, seul 2 a un groupe de décomposition non abélien ; pour $t = 74$ et $t = 123$, 2 et un autre premier (193 ou 67) ont pour groupe de décomposition le groupe $G \simeq C_7 \rtimes C_3$ tout entier.

On a donc des exemples d'extensions galoisiennes modérément ramifiées pour lesquelles le réseau associé à la racine carrée de la codifférente n'est pas isométrique à $(\mathbb{Z}[G], q_G)$ alors qu'il lui est stablement G-isométrique d'après le théorème de [ErT] rappelé dans l'introduction de ce chapitre (item 2).

5.4 L'algorithme utilisé

Les propositions des trois paragraphes précédents sont prouvées par le calcul à l'aide des logiciels Pari et Magma. On donne ici l'algorithme utilisé pour le calcul correspondant à $t = 5$ dans la proposition 5.1.1. La réduction à l'aide de `polredabs` (Pari) de la spécialisation de P_t en 5 est :

$$P_5(x) = x^9 - 21x^7 - 7x^6 + 126x^5 + 105x^4 - 189x^3 - 252x^2 - 63x + 7$$

Pour obtenir un polynôme Q_5 dont le corps de rupture soit égal au corps de décomposition D de P_5, on donne à Pari les instructions suivantes :

```
p5=x^9-21*x^7-7*x^6+126*x^5+105*x^4-189*x^3-252*x^2-63*x+7 ;
nf=nfinit(subst(p5,x,y)) ;
nffactor(nf,p5)
rnfequation(nf,%[5,1])
polredabs(%)
```

On obtient :

$$\begin{aligned} Q_5(x) = \; & x^{27} - 57x^{25} - 39x^{24} + 1353x^{23} + 1689x^{22} - 17265x^{21} - 30093x^{20} \\ & +129297x^{19} + 294266x^{18} - 572418x^{17} - 1755474x^{16} + 1324680x^{15} \\ & +6651036x^{14} - 305169x^{13} - 15987783x^{12} - 7092606x^{11} \\ & +23251944x^{10} + 20089453x^{9} - 17590917x^{8} - 25385334x^{7} \\ & +2912439x^{6} + 15074850x^{5} + 3688890x^{4} - 3218718x^{3} \\ & -1313379x^{2} + 197382x + 102871 \end{aligned}$$

De plus, le discriminant de $D/\mathbb{Q}$ est égal à $3^{48}7^{24}$ avec $e(3) = e(7) = 9$ et $f(3) = f(7) = 3$. On utilise maintenant le programme Magma avec les instructions suivantes :

```
Q :=RationalField() ; PR<x> :=PolynomialRing(Q) ;
P :=PR !(x^27 - 57*x^25 - 39*x^24 + (...) + 197382*x + 102871) ;
K :=NumberField([P]) ; OK :=MaximalOrder(K) ;
P3 :=Decomposition(OK,3)[1][1] ; P7 :=Decomposition(OK,7)[1][1] ;
AK :=P3^(-8)*P7^(-4) ;

BOK :=Basis(OK) ; BAK :=BasisMatrix(AK) ;
Gram :=MatrixAlgebra(Q,27) !0 ;
for i := 1 to 27 do
for j :=1 to 27 do
Gram[i][j] :=Trace(BOK[i]*BOK[j]) ;
end for ;
end for ;

GG :=BAK*Gram*Transpose(BAK) ;
LG,T :=LLLGram(GG) ;
L :=LatticeWithGram(LG) ;
```

On vérifie ensuite que le réseau `L` obtenu est unimodulaire (`Determinant(L)` donne 1), on calcule son minimum (`Minimum(L)`) qui vaut ici 3 et le nombre de vecteurs minimaux (`KissingNumber(L)`) qui vaut 2664 (comptés avec les opposés). Ceci montre la première partie du point (ii) de la proposition 5.1.1 pour $t = 5$.

On veut maintenant chercher parmi les vecteurs minimaux de `L` si certains engendrent des bases normales de la racine carrée de la codifférente sous l'action du groupe de Galois. L'instruction `S3 :=ShortestVectors(L)` donne accès à l'ensemble des vecteurs minimaux de `L` (modulo les opposés : `#S3` est égal à 1332). Il faut donc faire agir les éléments du groupe de Galois. Pour déterminer celui-ci explicitement, on revient à Pari et on utilise l'algorithme récemment implanté par Allombert ([A]). Les instructions sont :

```
gal=galoisinit(q5) ;
g1=galoispermtopol(gal,gal.gen[1]) ;
g2=galoispermtopol(gal,gal.gen[2]) ;
a1=Mod(g1,q5) ;a2=Mod(g2,q5) ;
A=matrix(27,27,i,j,0) ;B=A ;
y=Mod(z^0,q5) ;for(i=1,27,for(j=1,27,
                  A[i,j]=component(component(y,2),j)) ;y=y*a) ;
y=Mod(z^0,q5) ;for(i=1,27,for(j=1,27,
                  B[i,j]=component(component(y,2),j)) ;y=y*b) ;
write("matrices","A=",A,"B=",B)
```

Suivent quelques modifications pour mettre le fichier "matrices" au format Magma, puis :

```
load matrices ;
BO :=BasisMatrix(OK) ;
A :=BO*A*BO^(-1) ; B :=BO*B*BO^(-1) ;
A :=BAK*A*BAK^(-1) ; B :=BAK*B*BAK^(-1) ;
A :=T*A*T^(-1) ; B :=T*B*T^(-1) ;
Gal :=MatrixGroup<27,Q|[A,B]> ;

S3 :=ShortestVectors(L) ; SQ3 :=Seqset(S3) ;
phi, GGal :=OrbitAction(Gal,SQ3) ;
O :=Orbits(GGal) ;
SO :=[O[i] :i in [1..#O] | #O[i] eq 27] ;
```

```
for S in SO do
SS :=x@@phi : x in S ;
SubL :=sub<L|SS> ;
print Determinant(SubL) ;
end for ;
```

Pour chaque orbite de vecteur minimal sous l'action du groupe de Galois, le déterminant du sous-réseau de `L` engendré est affiché. Les bases normales de la racine carrée de la codifférente sont les vecteurs pour lesquels ce déterminant vaut 1 (il y en a dans ce cas). Lorsqu'il n'y en a pas (proposition 5.2.1 (iv), minimum 2), on fait le même processus avec l'ensemble des vecteurs de norme 3, puis 4, 5... Il faut alors modifier un peu la démarche pour éviter de saturer la mémoire (il y a 108 vecteurs de norme 2, 1980 de norme 3, 49275 de norme 4 et 1615680 de norme 5 modulo les opposés pour $t = 15$).

Bibliographie

[A] Allombert B., An efficient algorithm for the computation of Galois automorphisms, *to appear in Math. Comp.*

[BV] Bacher R., Venkov B., Réseaux entiers unimodulaires sans racines en dimensions 27 et 28, *Réseaux euclidiens, designs sphériques et formes modulaires*, 212–267, Monogr. Enseign. Math., **37**, *Enseignement Math., Genève*, 2001.

[BEr] Bachoc C., Erez B., Forme trace et ramification sauvage, *Proc. London Math. Soc.*, (3) **61**(1990), *no. 2*, 209–226.

[3BCO] Batut C., Belabas K., Bernardi D., Cohen H., Olivier M., *Users's guide to PARI-GP*, Université Bordeaux 1 (2000)[1].

[BoCa] Bosma W., Cannon J., *Handbook of Magma functions*, 1998.

[BuCh] Burns D., Chinburg T., Adams operations and integral Hermitian-Galois representations, *Amer. J. Math.*, **118**(1996), *no. 5*, 925–962.

[BMK] Butler G. and McKay J., The transitive groups of degree up to eleven, *Comm. Algebra*, **11**(1983), 863–911.

[B] Byott N.P., Integral Galois module structure of some Lubin-Tate extensions, *J. Number Theory*, **77** (1999), *no. 2*, 252–273.

[CNQ] Cassou-Noguès Ph., Queyrut J., Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées II, *Ann. Inst. Fourier (Grenoble)*, **32**(1982), *no. 1*, 7–27.

[CNT1] Cassou-Noguès Ph., Taylor M.J., Opérations d'Adams et groupes de classes d'algèbres de groupes, *J. Algebra*, **95**(1), 125–152 (1985).

[CNT2] Cassou-Noguès Ph., Taylor M.J., Galois module structure for wild extensions, in *Algebraic number theory and diophantine analysis, Proc. Conf. Graz 1998*, ed. Halter-Koch F. and Tichy R.F., de Gruyter, New York (2000), 69–91.

[Ch] Chinburg T., Exact sequences and Galois module structure, *Ann. of Math.* **121**(2) (1985), *no. 2*, 351–376.

[Coh] Cohen H., *Advanced topics in computational number theory*, Graduate texts in maths. **193**, Springer-Verlag, New York (2000).

[1] téléchargeable par `ftp ://megrez.math.u-bordeaux.fr/pub/pari`

[CP] Conner P. E., Perlis R., *A survey of trace forms of algebraic number fields*, Series in Pure Mathematics, **2**, World Scientific Publishing Co., Singapore (1984).

[CS] Conway J. H., Sloane N. J. A., *Sphere packings, lattices and groups*, third edition, Grundlehren der Mathematischen Wissenschaften, **290**, Springer-Verlag, New York (1999).

[Cou] Cougnard J., Un anneau d'entiers stablement libre et non libre, Experiment. Math., **3**(1994), *no. 2*, 129–136.

[CR1] Curtis C. W., Reiner I., *Methods of representation theory, Vol. I*, Wiley, New York (1990).

[CR2] Curtis C.W., Reiner I., *Methods of representation theory, Vol. II*, Wiley, New York (1994).

[Ei1] Eichenlaub Y., *Problèmes effectifs de théorie de Galois en degrés 8 à 11*, Thèse de Doctorat, Université Bordeaux 1 (1996).

[Ei2] Eichenlaub Y., Réalisation explicite des produits semi-directs à noyau abélien comme groupes de Galois, *prépublication*.

[ElM] Elder G.G., Madan M.L., Galois module structure of the integers in weakly ramified extensions, *Arch.Math. (Basel)* **64**(1995), *no. 2*, 117–120.

[Er1] Erez B., *Structure galoisienne et forme trace dans les corps de nombres*, Thèse de Doctorat, Université de Genève (1987).

[Er2] Erez B., A survey of recent work on the square root of the inverse different, Journées arithmétiques, Exp. Congr., Luminy (1989) *Astérisque* **198-200**, 133–152.

[Er3] Erez B., The Galois structure of the square root of the inverse different, *Math. Z.*, **208**(1991), 239–255.

[Er4] Erez B., *Galois modules in arithmetic*, en préparation.

[Er5] Erez B., Geometric trends in Galois module theory, in *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, 115–145, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[ErM] Erez B., Morales J., The Hermitian structure of rings of integers in odd degree abelian extensions, *J. Number Theory*, **40**(1992), *no. 1*, 92–104.

[ErT] Erez B., Taylor M. J., Hermitian modules in Galois extensions of number fields and Adams operations, *Ann. of Math.*, **135**(1992), *no. 2*, 271–296.

[F1] Fontaine J. M., Sur la décomposition des algèbres de groupes, *Ann. Sc. E.N.S. (4)*, **4** (1971), p. 121–180.

[F2] Fontaine J. M., Groupes de ramifications et représentations d'Artin, *Ann. Sc. E.N.S. (4)*, **4** (1971), p. 337–392.

[Fri] Fried M., On Hilbert's irreducibility theorem, *J. Number Theory*, **6** (1974), 211–231.

[Frö] Fröhlich A., *Galois module structure of algebraic integers*, Ergebnisse der Mathematik, 3. Folge, Bd. 1, Springer, Berlin (1983).

[Gi] Gillard R., Plongement d'une extension d'ordre p ou p^2 dans une surextension non abélienne d'ordre p^3, *J. reine und angew. Math.*, 268/269 (1974), p. 418–426.

[Gr] Greither C., Unramified Kummer extensions of prime power degree, *Manuscripta Math.*, **64**(1989), *no. 3*, 261–290.

[Ha] Hall M., *The theory of groups*, The Macmillan Cy., New York (1959).

[He] Hecke E., *Lectures on the theory of algebraic numbers*, Graduate texts in maths. **77**, Springer-Verlag, New York-Berlin (1981).

[HW1] Holland D., Wilson S. M. J., Fröhlich's and Chinburg's conjectures in the factorisability defect class group, *J. Reine Angew. Math.* **442**(1993), 1–17.

[HW2] Holland D., Wilson S. M. J., Factor equivalence of rings of integers and Chinburg's invariant in the defect class group, *J. London Math. Soc. (2)* **49**(1994), *no. 3*, 417–441.

[M1] Martinet J., Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre $2p$, *Ann. Inst. Fourier* **19**(1969), 1–80.

[M2] Martinet J., Modules sur l'algèbre du groupe quaternionien, *Ann. Sci. Ecole Norm. Sup. (4)* **4**(1971), 399–408.

[M3] Martinet J., Character theory and Artin L-functions, in *Algebraic number fields (L-functions and Galois properties)*, ed. Fröhlich A., Acad. Press, London, 1977, 1–87.

[MN] Massy R., Nguyen Quang Do T., Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3 : étude locale-globale, *J. reine und angew. Math.*, 291 (1977), p. 149–161.

[MD] Monier-Derviaux S., *Le problème de la descente galoisienne finie*, Thèse de Doctorat, Université de Valenciennes et du Hainaut Cambraisis (1997).

[Sa] Samuel P., *Théorie algébrique des nombres*, 2ème édition, Hermann, Paris (1971).

[Se1] Serre J.P., *Corps locaux*, 3ème édition, Hermann, Paris (1968).

[Se2] Serre J.P., Local class field theory, in *Algebraic number theory*, eds. Cassels J.W.S. and Fröhlich A., Acad. Press, London (1967), 128–161.

[Se3] Serre J.P., *Représentations linéaires des groupes finis*, 3ème édition, Hermann, Paris (1978).

[Tat1] Tate J.T., Fourier analysis in number fields and Hecke's zeta functions, in *Algebraic number theory*, eds. Cassels J.W.S. and Fröhlich A., Acad. Press, London (1967), 305–347.

[Tat2] Tate J.T., Local constants, in *Algebraic number fields (L-functions and Galois properties)*, ed. Fröhlich A., Acad. Press, London (1977), 89–131.

[Tay1] Taylor M.J., On Fröhlich's conjecture for rings of integers of tame extensions, *Invent. Math.*, **63**(1981), 41–79.

[Tay2] Taylor M.J., On the Galois module structure of rings of integers of wild abelian extensions, *J. London Math. Soc.*, (2) **52**(1995), 73–87.

[U] Ullom, S. V., The exponent of class groups, *J. Algebra*, **29**(1974), 124–132.

[Vö] Völklein, H., *Groups as Galois groups. An introduction*, Cambridge Studies in Advanced Mathematics, **53**, Cambridge University Press, Cambridge (1996).

[Vi1] Vinatier S., Structure galoisienne dans les extensions faiblement ramifiées de $\mathbb{Q}$, *J. Number Theory*, **91** (2001), *no. 1*, 126–152.

[Vi2] Vinatier S., Une famille infinie d'extensions faiblement ramifiées, *Math. Nachr.*, **243** (2002).

[W] Washington L.C., *Introduction to cyclotomic fields*, Graduate texts in maths. **83**, Springer-Verlag, New York (1982).

ARITHMÉTIQUE DES EXTENSIONS FAIBLEMENT RAMIFIÉES

Après les nombreux travaux effectués pour étudier la structure galoisienne de l'anneau d'entiers d'une extension modérée de corps de nombres, notamment par Fröhlich et Taylor, Erez s'est intéressé à celle de la racine carrée de la codifférente (le seul idéal autodual pour la forme trace). Il a montré que le cadre naturel pour cette étude est celui des extensions de degré impair faiblement ramifiées, c'est-à-dire pour lesquelles le second groupe de ramification est trivial en toute place. La présence de la ramification sauvage en certaines places pose de nouveaux problèmes, que l'on résoud dans cette thèse dans le cas où l'extension est absolue et abélienne aux places sauvages, grâce à une étude exhaustive des extensions locales, absolues, abéliennes et faiblement ramifiées. On s'intéresse aussi au cas non abélien aux places sauvages. Par ailleurs, on construit des exemples d'extensions absolues faiblement ramifiées de degré impair non abéliennes. Le calcul dans ces exemples du réseau unimodulaire obtenu en munissant la racine carrée de la codifférente de la forme trace permet de montrer qu'il n'est pas toujours isométrique au réseau unimodulaire standard.

Mots clés : structure galoisienne, extensions faiblement ramifiées, racine carrée de la codifférente, réseaux unimodulaires.

ARITHMETIC OF WEAKLY RAMIFIED EXTENSIONS

After numerous works dealing with the Galois structure of the ring of integers in tamely ramified extensions of number fields, achieved in particular by Fröhlich and Taylor, Erez started studying the Galois structure of the square root of the inverse different, which is the only self-dual ideal with respect to the trace form. In view of his results, it is natural for this study to suppose the extensions of odd degree and weakly ramified, i.e. the second ramification groups at all places are trivial. Having to deal with wildy ramified places brings new problems, which are solved in this thesis when the extension is also supposed absolute and abelian at wild places. This is made possible thanks to the complete description of local, absolute, abelian and weakly ramified extensions. Extensions which are not abelian at wild places are also considered. In addition, examples of weakly ramified extensions of odd degree which are not abelian are constructed. The calculation of the unimodular lattice obtained by equipping the square root of the inverse different of these extensions with the trace form shows that it's not always isometric to the standard unimodular lattice.

Key words : Galois module structure, weakly ramified extensions, square root of the inverse different, unimodular lattices.

MATHEMATIQUES PURES

Laboratoire A2X, UFR Math-Info de Bordeaux, 351 Cours de la Libération, 33405 Talence Cedex, France.