HAL
open science

Aspects explicites des fonctions L et applications

Charlotte Euvrard

To cite this version:

Charlotte Euvrard. Aspects explicites des fonctions L et applications. Théorie des nombres [math.NT]. Université de Franche-Comté, 2016. Français. NNT : 2016BESA2074 . tel-01661548

HAL Id: tel-01661548

https://theses.hal.science/tel-01661548v1

Submitted on 12 Dec 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

École Doctorale Carnot-Pasteur

Thèse de Doctorat

présentée par

Charlotte Euvrard

pour obtenir le grade de
Docteur de Mathématiques de l'Université de Bourgogne Franche-Comté

Aspects explicites des fonctions L et applications

Thèse soutenue le 4 avril 2016, devant le jury composé de :

Bill Allombert	Ingénieur d'études	Université de Bordeaux	Examinateur
Cécile Armana	Maître de conférences	Université de Franche-Comté	Examinatrice
Christophe Delaunay	Professeur	Université de Franche-Comté	Directeur de thèse
Laurent Habsieger	Directeur de recherche	Université de Lyon	Président du jury
Stéphane Louboutin	Professeur	Université d'Aix-Marseille	Rapporteur
Christian Maire	Professeur	Université de Franche-Comté	Directeur de thèse
Olivier Robert	Maître de conférences	Université de Saint-Étienne	Rapporteur

Remerciements

Tout d'abord, je tiens à remercier mes directeurs de thèse, Christophe Delaunay et Christian Maire, sans qui je n'aurais pas pensé faire une thèse et surtout sans qui je n'aurais pas pu la terminer. Le travail en collaboration avec Christian m'a permis de découvrir un peu plus la recherche. Et surtout Christian m'a démontré, plus que ses qualités de directeur de thèse, son soutien infaillible. Je remercie également les membres de mon jury de thèse de m'avoir fait l'honneur d'accepter leurs rôles, à commencer par les rapporteurs qui ont subi le manuscrit : Stéphane Louboutin et Olivier Robert. Merci pour leurs commentaires et suggestions qui ont permis d'améliorer les résultats. Merci à Laurent Habsieger d'avoir accepté de présider le jury. Merci à Bill Allombert, je suis ravie d'être la première docteure à pouvoir le compter parmi son jury, j'en profite aussi pour le remercier pour toute la patience et l'aide qu'il m'a offertes dans l'utilisation de PARI/GP. Enfin, merci à Cécile Armana, qui était déjà présente à mes débuts, lors de ma soutenance de mémoire de M2. D'ailleurs, ce fut un plaisir de vivre ces années de thèse parmi l'équipe de théorie des nombres qui s'est assez régulièrement agrandie, notamment avec l'arrivée d'Agnès David, très bienveillante et particulièrement à l'écoute.

On retrouve ces qualités chez la plupart des membres du laboratoire de Mathématiques de Besançon, c'est ce qui fait qu'on s'y sent bien ! C'est agréable de voir le monde de la recherche avec un tel visage. Je pense particulièrement à Florence et Gilles Lancien qui m'ont toujours impressionnée par leurs innombrables qualités aussi bien humaines que professionnelles (quel bonheur d'avoir pu compter parmi leurs étudiants !). Louis Jeanjean a su m'écouter et me soutenir tout au long de ma thèse, particulièrement dans les moments difficiles, merci.

Je souhaite également remercier chaleureusement les documentalistes ainsi que les services administratif et informatique particulièrement efficaces grâce à Émilie et Odile, Catherines et Pascaline, Julien-Yves, Richard et Romain, remplacé maintenant par Christopher, que j'ai embêtés assez régulièrement mais qui ont toujours su répondre à mes demandes et même parfois les anticiper, un grand merci !

Ensuite, j'aimerais remercier l'ENSMM, en particulier Sylvie Cuche pour son efficacité en réponse à mes nombreuses demandes, et les membres du labo de Maths qui m'ont accueillie durant trois années et sans qui je n'aurais pas pu terminer ma thèse de cette façon : merci à Kamyar, Nathaël, Philippe, Rachid, Rémi et Satish avec qui j'ai partagé des TD et des surveillances. Et un merci tout particulier à Firmin qui m'a fait connaître l'ENSMM et qui depuis a rejoint de façon permanente ses rangs. Transition parfaite pour introduire les doctorants que j'ai eu grand plaisir à côtoyer durant cette période. D'abord, renommons Firmin, présent depuis la prépa agreg et avec qui j'ai partagé le bureau pendant deux ans, avec son humour légendaire, dont il a refilé le secret à deux co-bureaux d'exception toujours prêts à aider et écouter : Cyril (mon remplaçant officiel pour les BCPST, merci !) et Guillaume. Un sincère merci ! Merci également à mes co-bureaux Olga, Runlian et toutes les personnes qui sont passées pour de plus ou moins

longs séjours par le bureau 422. Je voudrais remercier Lucie, qui a réussi à se fondre parmi les doctorants, j'espère que son chemin pourra suivre les nôtres et qu'elle pourra garder la clé du bureau... Merci à la génération de docteurs au-dessus de la mienne. Ils étaient mes idoles, j'ai donc été plus que ravie de pouvoir les approcher, j'espère bien que nos liens ne s'effaceront pas de sitôt ! Je pense entre autres à Céline et Émilie qui sont devenues de très chères amies et qui ont su toujours être présentes, même lorsqu'elles ne l'étaient plus physiquement. Il y a aussi Guillaume avec qui j'ai fait mes premiers pas dans la recherche et avec les fonctions L d'Artin. Merci également à Alexis qui m'a souvent accompagnée dans les instants de pause... Et les générations en-dessous que j'ai eu grand plaisir à découvrir notamment Colin, Clément (compagnon de colles du mercredi), Johann, Marine (avec qui on a formé l'équipe de doctorantes de théorie des nombres et une partie de la "team penguin"), Michaël, Othman, Quentin. Et finissons par remercier ma génération, particulièrement celle de l'année de l'agreg avec Aude, François, Gilles, Michel et Thomas. Je souhaite à ceux qui ne sont pas encore docteurs de le devenir, merci à François de toujours penser à passer nous voir, même lorsque le temps lui manque. Je constate que cette année sera la dernière à la fac pour Aude, Michel et moi, une grande page se tourne... Nous avons vécu ensemble depuis le stress de l'agreg, ce n'est pas rien pour sceller des liens. Avec Aude, on va pouvoir fêter nos 10 ans dans le supérieur et dans la même classe, j'espère bien qu'on sera toujours aussi proches les 10 prochaines années, même si nos bureaux ne le seront sûrement pas autant... Merci pour tout ! Merci également d'avoir pu arbitrer la compétition des années de thèse entre Batiste et moi, merci à Batiste d'avoir été présent, plus ou moins directement.
Ensuite, j'aimerais remercier toutes les personnes rencontrées lors d'écoles d'été ou de conférences, à commencer par Arthur et Pierre, indissociables, merci à notre plus grand mécène pour la collection de cartes du bureau et merci pour la patience dont a fait preuve Pierre lors des ateliers PARI/GP. Continuons par un autre Bordelais de thèse : Bruno qui m'a fait l'honneur d'être présent à ma soutenance. Je remercie également Florent : grâce à ses mots fléchés, certains exposés sont passés beaucoup plus vite. Ensuite, je pense à la promesse que l'on s'était faite avec Alex et Coline : ce sera donc chose faite ! Un grand merci à Coline avec qui j'ai passé de très bons moments (pas forcément très studieux), merci de m'avoir soutenue et comprise.
Merci à ceux qui n'ont jamais cessé de chercher à comprendre ce en quoi pouvait consister mon travail : merci d'avoir toujours été présents à mes côtés malgré le manque d'explications. Merci à Camille, Lydie, Marion et Raphaëlle sur qui j'ai toujours pu compter, en particulier pour me remonter le moral et me redonner confiance. Merci également à Charline, Florian, Gwen, Micka et Pablo.
Un grand merci au soutien indéfectible de ma famille, même si je n'ai jamais su bien leur expliquer ma situation, ils m'ont toujours épaulée et réconfortée. Cette thèse leur doit donc beaucoup. Dorénavant, mon métier sera sûrement plus facile à décrire ! Je pense bien sûr à mes parents, ma sœur et mon frère qui ont été aux premières loges et ont réussi à me supporter, en espérant que les moments à venir soient encore meilleurs. Merci d'avoir été là et d'être toujours là. Merci aussi à Damien qui aura vite appris à me connaître. Merci également à mes grands-parents, chez qui j'ai passé une bonne partie de ma vie. Comme dirait mon grand-père, c'est en bonne partie grâce à eux que j'en suis arrivée là. Je n'oublie pas de remercier tout ceux qui ont contribué à cette réussite, en particulier mes tantes et oncles présents le jour J, sans eux, le pot n'aurait pas pu avoir autant de succès !
Merci également à tout ceux que j'ai oubliés mais qui ont compté...

Table des matières

Notations **v**

Introduction **1**

1 Fonctions L et fonctions L d'Artin **7**
1.1 Fonctions L . . . 7
1.1.1 Définitions et premières propriétés . . . 7
1.1.2 Convolution de Rankin-Selberg . . . 12
1.1.3 Conjectures . . . 14
1.2 Fonctions L d'Artin . . . 16
1.2.1 Définitions et propriétés . . . 16
1.2.2 Équation fonctionnelle . . . 21
1.2.3 Convolution de Rankin-Selberg . . . 25
1.2.4 Aspects explicites dans le cas $K = \mathbb{Q}$ . . . 27
1.2.4.1 Aspects explicites . . . 27
1.2.4.2 Exemple numérique sur la somme des zéros . . . 29
1.2.4.3 Corps quadratiques . . . 30

2 Majoration explicite pour déterminer une fonction L **35**
2.1 Théorème pour une fonction L générale . . . 35
2.2 Preuve du théorème 2.1.3 . . . 37
2.2.1 Formule explicite . . . 37
2.2.2 Conséquences du théorème 2.2.3 . . . 38
2.2.3 Fin de la preuve du théorème 2.1.3 . . . 40
2.2.4 Preuve du théorème 2.2.3 . . . 40
2.2.4.1 Préliminaires . . . 41
2.2.4.2 Majoration de l'intégrale des égalités (1) et (2) . . . 41
2.2.4.3 Majoration de $\sum \frac{1}{|\rho(\rho+1)|}$ sur les zéros de $L(s,f)$ . . . 44
2.2.4.4 Fin de la preuve du théorème 2.2.3 . . . 50
2.3 Majoration explicite pour déterminer une fonction L d'Artin . . . 51
2.3.1 Théorème . . . 51
2.3.2 Preuve du théorème 2.3.2 . . . 52
2.3.3 Aspects explicites entre coefficients et paramètres locaux d'une fonction L d'Artin . . . 59
2.4 Application aux fonctions L de formes modulaires primitives . . . 60
2.4.1 Définition . . . 60
2.4.2 Opérateurs de Hecke et formes primitives . . . 61
2.4.3 Fonctions L d'une forme modulaire primitive . . . 61
2.4.4 Théorème . . . 62

3 Séparation des caractères par le Frobenius **65**
3.1 Présentation du résultat 65
3.2 Preuve du théorème 3.1.1 67
3.3 Application aux polynômes 71
3.3.1 Cadre 71
3.3.2 Expression du Frobenius sous forme de cycles 72
3.3.3 Cas particulier : quand disc P est le discriminant d'un corps quadratique 74
3.3.4 Écriture du Frobenius séparant les caractères conjugués du groupe alterné 76
3.3.5 Comparaison avec la méthode de Bellaïche dans le cas du groupe symétrique 79
3.4 Sur les extensions non ramifiées d'un corps de nombres 81
3.4.1 Un exemple de base : le p-rang du groupe des classes 81
3.4.2 Caractères de degré $r > 1$ 83
3.4.3 Une variante : les extensions modérément ramifiées d'un corps de nombres 84
3.5 Expérimentations numériques avec le groupe A_n 87
3.5.1 Familles et expérimentations 87
3.5.1.1 Le groupe A_5 89
3.5.1.2 Le groupe A_7 91
3.5.1.3 Le groupe A_{13} 92
3.5.2 Sur une question diophantienne 94

A Programmes dans le cas $K = \mathbb{Q}$ **97**
A.1 Représentations 97
A.2 Frobenius 99
A.3 Coefficients d'une fonction L d'Artin 101
A.4 Paramètres locaux d'une fonction L d'Artin 102
A.5 Équation fonctionnelle 103
A.5.1 Conducteur 103
A.5.2 Le facteur gamma 105
A.5.3 Prolongement de la fonction L d'Artin 106

B Quelques propriétés et rappels **109**
B.1 Définitions et propriétés 109
B.1.1 Fonction gamma d'Euler 110
B.1.2 Transformée de Mellin 112
B.1.3 Automorphisme de Frobenius 112
B.2 Quelques propriétés des représentations 113
B.2.1 Caractère d'une représentation induite 114
B.2.2 Représentation régulière 114
B.2.3 Dual 116
B.2.4 Caractères des groupes alternés 117

Index **123**

Bibliographie **125**

Notations

$\lvert\,.\,\rvert$	cardinal
$\left(\frac{\cdot}{\cdot}\right)$	symbole de Kronecker
$\langle\chi_1,\chi_2\rangle$	produit scalaire entre les caractères χ_1 et χ_2
O (resp. $\ll$)	notation de Landau (resp. de Vinogradov) pour la domination
$\sim$	notation de Landau pour l'équivalence
$\lVert\phi\rVert_1$	$\int_{\mathbb{R}} \lvert\phi(x)\rvert \,\mathrm{d}x$
$\lVert\phi\rVert_\infty$	$\sup_{x\in\mathbb{R}} \lvert\phi(x)\rvert$
$\mathbf{1}_G$	caractère trivial du groupe G
$\alpha_{i,f}(p)$	paramètre locaux de la fonction L, $L(s,f)$, en p
C_i, c_i	constantes absolues
$[f]$	cycle de S_n de longueur f
$L,\ K$	corps de nombres
disc A	discriminant de A (un corps de nombres ou un polynôme)
A_n	groupe alterné de degré n
$\mathscr{C}$	classe de conjugaison
$d(f)$	degré de la fonction L $L(s,f)$
$d_p\mathrm{Cl}_K$	p-rang du groupe des classes de K
Cl_K	groupe des classes de K
e_G (ou simplement 1)	élément neutre du groupe G
$\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$	automorphisme de Frobenius de $\mathfrak{P}\vert\mathfrak{p}$
$\gamma_f(s)$	facteur gamma de la fonction L, $L(s,f)$
G	groupe de Galois de L/K
κ_j	j^e paramètre local à l'infini de la fonction L, $L(s,f)$
Λ_f	fonction de Von Mangoldt
$n(p)$	nombre de caractères abéliens non ramifiés d'ordre p de K
$\mathrm{N}(I)$	norme de l'idéal I
$\mathscr{O}_K$	anneau des entiers de K
p	nombre premier
$\mathscr{P}$	ensemble des nombres premiers sur $\mathbb{Z}$
$\mathfrak{P}\vert\mathfrak{p}$	idéal premier $\mathfrak{P}$ situé au-dessus de l'idéal premier $\mathfrak{p}$
$q(f)$	conducteur de la fonction L, $L(s,f)$
$r(f)$	ordre du pôle (ou du zéro) de la fonction L, $L(s,f)$, en $s=1$
S_n	groupe symétrique de degré n
$\sigma_{\mathfrak{p}}$	automorphisme de Frobenius d'un idéal premier au-dessus de $\mathfrak{p}$
ψ, χ	caractères
$\chi(\mathscr{C})$	représente $\chi(c)$ pour c dans la classe de conjugaison $\mathscr{C}$
ζ_K	fonction zêta de Dedekind du corps de nombres K
$\zeta=\zeta_{\mathbb{Q}}$	fonction zêta de Riemann

Introduction

On sait, depuis près de vingt-trois siècles, qu'il existe une infinité de nombres premiers. La preuve de ce résultat due à Euclide ne tient qu'en quelques lignes par un raisonnement par l'absurde : s'il n'y avait qu'un nombre fini de nombres premiers, leur produit additionné de 1 serait divisible par l'un d'eux donc 1 le serait aussi, d'où la contradiction. Ensuite, en 1837, une nouvelle étape a été franchie par Dirichlet avec le théorème de la progression arithmétique :

Théorème 1. *Pour tous les entiers naturels non nuls m et n premiers entre eux, il existe une infinité de nombres premiers de la forme $m + an$, où a est un entier positif.*

Sa démonstration, mêlant résultats algébriques et analytiques, est tout à fait innovante : elle associe à des caractères des produits eulériens infinis équivalents à des séries, appelées depuis fonctions L de Dirichlet. De là, naîtra une nouvelle branche des mathématiques : la théorie analytique des nombres.

Concernant la distribution asymptotique des nombres premiers, en 1896, Hadamard et de La Vallée Poussin ont démontré, indépendamment, le théorème suivant :

Théorème 2 (Théorème des nombres premiers)**.** *Le nombre $\pi(x)$ de nombres premiers inférieurs ou égaux à x est équivalent, au voisinage de l'infini, au quotient $x/\ln(x)$.*

La démonstration utilise des méthodes d'analyse complexe, en particulier la fonction zêta de Riemann. Celle-ci est définie par la série de Riemann $\sum_{n\geqslant 1} \frac{1}{n^s}$ convergeant absolument sur l'ensemble des complexes de partie réelle strictement supérieure à 1. Sur ce domaine, on peut l'écrire sous forme de produit eulérien, faisant alors apparaître les nombres premiers : $\zeta(s) = \prod_{p\in\mathscr{P}} \frac{1}{1-p^{-s}}$, où $\mathscr{P}$ désigne l'ensemble des nombres premiers.

Théorème 3. *La fonction $\Lambda(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$, définie pour les complexes s vérifiant $\mathrm{Re}(s) > 1$, se prolonge sur $\mathbb{C}$ en une fonction méromorphe avec seulement deux pôles, en $s = 0$ et $s = 1$, simples et vérifie l'équation fonctionnelle suivante : $\Lambda(s) = \Lambda(1-s)$.*

On peut déduire de ce théorème des résultats sur la fonction zêta de Riemann elle-même. En effet, on obtient immédiatement le prolongement de ζ en une fonction méromorphe possédant un pôle simple en $s = 1$, le pôle de Λ en $s = 0$ provenant du pôle de la fonction gamma d'Euler. On remarque que les autres pôles de $\Gamma\left(\frac{s}{2}\right)$, situés aux entiers pairs strictement négatifs, sont nécessairement compensés par des zéros de ζ : on les appelle les zéros triviaux de la fonction zêta de Riemann. De plus, la convergence du produit eulérien dans le demi-plan vertical ouvert $\mathrm{Re}(s) > 1$ entraîne que la fonction zêta de Riemann ne s'annule pas sur cette partie du plan complexe. L'équation fonctionnelle montre alors que $\zeta(s)$ ne s'annule pas en dehors des zéros triviaux pour des complexes de partie réelle strictement négative. Les zéros non triviaux de la fonction zêta de Riemann

se situent donc dans la bande $0 \leqslant \mathrm{Re}(s) \leqslant 1$. L'équation fonctionnelle permet également d'obtenir les valeurs de ζ aux entiers impairs négatifs à partir des valeurs aux entiers pairs positifs [1] : on connaît, depuis Euler, $\zeta(2) = \pi^2/6$ ou $\zeta(4) = \pi^4/90$. Plus généralement, Euler a démontré que les nombres $\zeta(2k)$ sont des multiples rationnels explicites de π^{2k}.

En 1859, Riemann conjecture un résultat concernant la localisation des zéros de $\zeta(s)$. À ce jour, bien que souvent admise, l'hypothèse de Riemann n'est toujours pas démontrée. En fait, la localisation des zéros reste un problème important en théorie des nombres.

Conjecture 4 (Hypothèse de Riemann)**.** *Les zéros non triviaux de $\zeta(s)$ ont tous une partie réelle égale à $1/2$.*

Il existe une généralisation de cette fonction aux corps de nombres : ce sont les fonctions zêta de Dedekind. La fonction zêta de Dedekind d'un corps de nombres K de degré $[K : \mathbb{Q}] = d = r_1 + 2r_2$, avec (r_1, r_2) la signature de K, est définie, dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$, par :

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \subset \mathscr{O}_K \\ \mathfrak{a} \neq 0}} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p} \text{ premier}} \frac{1}{1 - \mathrm{N}(\mathfrak{p})^{-s}},$$

la somme portant sur les idéaux entiers non nuls de $\mathscr{O}_K$ et le produit sur les idéaux entiers premiers de $\mathscr{O}_K$. De plus, elle se prolonge sur le plan complexe en une fonction méromorphe avec un seul pôle simple en $s = 1$. On retrouve également une fonction complétée

$$\Lambda(s) = |\mathrm{disc}\ K|^{s/2} \pi^{-ds/2} \Gamma\left(\frac{s}{2}\right)^{r_1+r_2} \Gamma\left(\frac{s+1}{2}\right)^{r_2} \zeta_K(s)$$

prolongeable méromorphiquement sur $\mathbb{C}$ avec deux pôles, en $s = 0$ et $s = 1$, simples et satisfaisant l'équation fonctionnelle $\Lambda(s) = \Lambda(1 - s)$.
La fonction zêta de Dedekind permet de distinguer des classes de corps de nombres. Par exemple, deux corps de nombres sont dits *arithmétiquement équivalents* si leur fonction zêta de Dedekind est égale. En particulier, des corps de nombres isomorphes sont arithmétiquement équivalents. De plus, il a été démontré (voir [Per77]) que le plus petit degré pour lequel on trouve des corps arithmétiquement équivalents non isomorphes est 7. On peut également citer la famille de corps non isomorphes arithmétiquement équivalents de degré 8 définie par $\mathbb{Q}(\theta)$ et $\mathbb{Q}(\sqrt{2}\theta)$, où θ est une racine réelle d'un polynôme $\mathbb{Q}$-irréductible de la forme $X^8 - \alpha \in \mathbb{Q}[X]$.
Malgré la brièveté de cette introduction à ces fonctions, nous constatons leur influence en mathématiques. Leur structure régie par certaines propriétés communes nous permet de classer ce genre de fonctions en une catégorie plus large appelée fonctions L.

Le premier chapitre est consacré à la définition précise des fonctions L générales ainsi que des fonctions L d'Artin. Nous en verrons leurs principales propriétés. Attention tout de même puisque malgré leur nom, les fonctions L d'Artin ne sont que conjecturalement des fonctions L. Détaillons un peu leur définition : les fonctions L d'Artin sont attachées à une extension galoisienne L/K et à une représentation (ρ, V) du groupe de Galois G associé, de caractère χ. Pour $\mathfrak{p}$ un idéal premier de K, on note $D_\mathfrak{p}$ le groupe de décomposition et $I_\mathfrak{p}$ le groupe d'inertie d'un idéal premier de $\mathscr{O}_L$ au-dessus de $\mathfrak{p}$ (la définition est indépendante

1. La façon moderne de voir les choses est plutôt d'utiliser l'équation fonctionnelle pour retrouver les valeurs de ζ aux entiers positifs pairs à partir de ses valeurs aux entiers négatifs impairs, comme ce qui est fait pour les fonctions L de Dirichlet, voir par exemple [Was97].

du choix de l'idéal dans $\mathscr{O}_L$). Soit $\sigma_{\mathfrak{p}}$ l'automorphisme de Frobenius engendrant $D_{\mathfrak{p}}/I_{\mathfrak{p}}$. On note $V^{I_{\mathfrak{p}}} = \{v \in V \,:\, \forall\, i \in I_{\mathfrak{p}},\ \rho(i)(v) = v\}$ le sous-espace vectoriel de V stable par $I_{\mathfrak{p}}$. Une fonction L d'Artin est définie dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$ par le produit suivant :

$$L(s, \chi, L/K) = \prod_{\mathfrak{p} \subset \mathscr{O}_K} \frac{1}{\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_{\mathfrak{p}}; V^{I_{\mathfrak{p}}})}.$$

Plus généralement, une fonction L, notée $L(s, f)$, est une série de Dirichlet possédant des propriétés particulières, dont une équation fonctionnelle. Il existe une généralisation de l'hypothèse de Riemann énonçant que les zéros d'une fonction L situés dans la bande $0 < \mathrm{Re}(s) < 1$ doivent être de partie réelle égale à $1/2$. Concernant les zéros situés sur les bords de la bande critique, nous énonçons la conjecture suivante, englobant l'hypothèse de Riemann.

Conjecture 5 (Grande Hypothèse de Riemann (GRH)). *À l'exception des éventuels zéros triviaux de partie réelle nulle, tous les zéros d'une fonction L situés dans la bande $0 \leqslant \mathrm{Re}(s) \leqslant 1$ sont situés sur la droite $\mathrm{Re}(s) = 1/2$.*

La définition des fonctions L fait intervenir des invariants, notamment ceux que l'on appelle les paramètres locaux en les nombres premiers. Ceux-ci, notés $\alpha_{i,f}(p)$, apparaissent dans l'écriture sous forme de produit eulérien dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$:

$$L(s, f) = \sum_{n \geqslant 1} a_f(n) n^{-s} = \prod_p \prod_{i=1}^{d(f)} (1 - \alpha_{i,f}(p) p^{-s})^{-1},$$

avec $a_f(1) = 1$, $a_f(n) \in \mathbb{C}$ et $\alpha_{i,f}(p) \in \mathbb{C}$. La première étape de cette thèse a été d'utiliser ces coefficients afin de distinguer deux fonctions L. En fait, un théorème de Henryk Iwaniec et Emmanuel Kowalski ([IK04], Theorem 5.22), repris ici dans le théorème 2.1.1, donne une majoration sur le nombre de paramètres locaux suffisants pour déterminer complètement une fonction L générale. Notons que différencier les paramètres locaux $\alpha_{i,f}(p)$ d'une fonction L n'est pas équivalent à différencier les coefficients $a_f(n)$ de la série de Dirichlet associée.

Théorème 6 ([IK04], Proposition 5.22). *Soit $L(s, f)$ et $L(s, g)$ deux fonctions L distinctes de même degré d. Supposons que $L(s, f \otimes \bar{f})$ et $L(s, f \otimes \bar{g})$ existent et que cette dernière soit entière. Supposons, de plus, que la conjecture 5 soit vraie pour ces deux fonctions L et que les paramètres locaux de $L(s, f \otimes \bar{f})$ et $L(s, f \otimes \bar{g})$ aux premiers divisant $q(f)q(g)$ soient de module inférieur à 1 (où $q(f)$, $q(g)$ désignent les conducteurs respectifs des fonctions $L(s, f)$ et $L(s, g)$). Alors il existe un nombre premier $p \leqslant C\,(d \ln \mathfrak{q}(f)\,\mathfrak{q}(g))^2$ ne divisant pas $q(f)q(g)$ tel que les paramètres locaux de $L(s, f)$ et $L(s, g)$ en p sont différents, avec C une constante absolue et $\mathfrak{q}(f)$, $\mathfrak{q}(g)$ les conducteurs analytiques respectifs des fonctions $L(s, f)$ et $L(s, g)$.*

L'objectif du deuxième chapitre est de rendre explicite cette constante. Ce travail a donné lieu à une publication dans le Journal de Théorie des Nombres de Bordeaux [Euv] dont un des résultats principaux est le suivant :

Théorème 7. *On note ϕ une fonction positive non nulle, $\mathscr{C}^\infty$ et à support compact dans $[1, 2]$. Dans le théorème 6, on peut prendre :*

$$C = \frac{51}{25\big(r(f \otimes \bar{f})\big)^2} \left(2D_{1,\phi} + 3D_{2,\phi} + \frac{754}{75} D_{0,\phi} r(f \otimes \bar{f}) + \frac{5}{2} D_{3,\phi} \omega'\big(q(f)q(g)\big) \right)^2,$$

où

$$\omega'(n) = \begin{cases} \frac{\omega(n)}{\ln n} & si\ n \geqslant 2 \\ 0 & si\ n = 1 \end{cases},$$

avec $\omega(n)$, définie sur $\mathbb{N}^*$, désignant la fonction additive dénombrant le nombre total des facteurs premiers de n,

$$\begin{aligned} D_{0,\phi} &:= \frac{C_{0,\phi}}{\|\phi\|_1} = \frac{1}{\|\phi\|_1} \int_1^2 |\phi''(x)| x^{3/2}\, \mathrm{d}x \\ D_{1,\phi} &:= \frac{C_{1,\phi}}{\|\phi\|_1} = \frac{1}{\|\phi\|_1} \int_1^2 \frac{\phi(x)}{x}\, \mathrm{d}x \\ D_{2,\phi} &:= \frac{C_{2,\phi}}{\|\phi\|_1} = \left(\frac{46}{4\pi} + \frac{27053}{500}\right) D_{0,\phi} \\ D_{3,\phi} &:= \frac{\|\phi\|_\infty}{\|\phi\|_1}. \end{aligned}$$

Avec un choix particulier pour la fonction ϕ, par exemple la fonction nulle en dehors de $]1,2[$ et définie par $\phi(x) = \exp\left(\frac{-0,3}{(x-1)(2-x)}\right)$ sinon, on trouve

$$C = 2 \cdot 10^8.$$

D'ailleurs, une question intéressante pourrait être de chercher une meilleure classe de fonctions afin d'obtenir une constante plus petite.

Lorsque les invariants des fonctions L admettent des propriétés spécifiques, il peut être intéressant d'adapter le raisonnement de la preuve à ces fonctions L et non pas simplement d'appliquer le résultat. C'est d'ailleurs ce que nous faisons pour les fonctions L d'Artin et les fonctions L de formes modulaires primitives.

Par exemple, le théorème suivant est vrai pour $C = 4,3 \cdot 10^7$.

Théorème 8. *Soit L/K une extension galoisienne de groupe de Galois G. Soient χ_1 et χ_2 deux caractères distincts de G de même degré d de représentation respective (ρ_1, V_1) et (ρ_2, V_2) dont le produit scalaire est nul. On suppose vraies la conjecture d'Artin et l'hypothèse de Riemann généralisée pour les deux fonctions L d'Artin $L(s, \chi_1 \otimes \bar{\chi}_i)$, $i = 1$ ou 2. Alors il existe un idéal premier $\mathfrak{p}$ de K, de norme inférieure ou égale à $C\left(d \ln \mathfrak{q}(\chi_1)\, \mathfrak{q}(\chi_2)\right)^2$, tel que les paramètres locaux de $L(s, \chi_1)$ et $L(s, \chi_2)$ en $\mathfrak{p}$ sont différents, avec*

$$C = \frac{51}{25}\left(\frac{(74 + \frac{289}{25}\langle \chi_1, \chi_1 \rangle) D_{0,\phi} + 2D_{1,\phi}}{\langle \chi_1, \chi_1 \rangle}\right)^2,$$

où ϕ est une fonction positive non nulle, $\mathscr{C}^\infty$, à support compact dans $[1,2]$ et les constantes $D_{0,\phi}$ et $D_{1,\phi}$ sont données dans le théorème 7 précédent.

Dans le cas des fonctions L d'Artin, les paramètres locaux correspondent aux valeurs propres des représentations en les Frobenius (aux problèmes des idéaux premiers ramifiés près). Connaître ces invariants pour une fonction L d'Artin a également permis l'écriture d'un programme avec le logiciel PARI/GP [PAR15] donnant les coefficients de sa série de Dirichlet. En fait, à partir d'un polynôme définissant une extension $L/\mathbb{Q}$ galoisienne, on peut d'abord connaître les différentes représentations du groupe de Galois associé

en faisant appel au logiciel GAP [GAP15]. Ensuite, comme nous le détaillons dans la partie 1.2.4, on calcule les valeurs propres de la représentation étudiée (en distinguant toutefois les premiers ramifiés des non ramifiés) en les automorphismes de Frobenius pour chaque nombre premier p. Puis il est possible de prolonger la fonction L. Les fonctions pour le calcul du conducteur et des facteurs gamma des fonctions L d'Artin ont d'ailleurs été écrites en C et intégrées à la version 2.9 de PARI/GP sous le nom $lfunartin$.

Par ailleurs, par définition dans le cas de fonction L d'Artin $L(s,\chi)$, la somme des paramètres locaux est égale à l'image du Frobenius par le caractère χ. Ainsi, séparer des caractères par les Frobenius revient à distinguer la somme des paramètres locaux associés aux fonctions L d'Artin de ces caractères. Ce sera l'objet du troisième chapitre qui est à mettre en lien avec le théorème de Chebotarev. En effet, celui-ci affirme que pour une extension galoisienne de corps de nombres L/K les automorphismes de Frobenius sont répartis dans l'ensemble des classes de conjugaison du groupe de Galois suivant une densité proportionnelle à leur taille. Par conséquent, en fixant une classe qui permet la séparation de deux caractères distincts du groupe de Galois en question, le théorème de Chebotarev apporte l'existence d'une infinité d'idéaux premiers $\mathfrak{p}$ pour lesquels les automorphismes de Frobenius $\sigma_{\mathfrak{p}}$ sont dans cette classe, et donc séparent ces caractères. L'effectivité permet de donner une borne supérieure sur la plus petite norme d'un tel idéal. Si, comme il est souvent coutume pour ces questions, nous nous plaçons dans le cadre où la conjecture d'Artin et l'hypothèse de Riemann généralisée aux fonctions L sont satisfaites, la borne donnée par le théorème de Chebotarev est alors, à une constante absolue près, en $\ln^2|\mathrm{disc}\ L|$ (on peut trouver ce résultat dans [MMS88], [IK04], [LO77] ou encore [Oes79]). En particulier, quand l'extension L/K est non ramifiée, la borne est en $|G|^2\ln^2|\mathrm{disc}\ K|$, où $|G|$ est l'ordre du groupe de Galois de l'extension L/K. La littérature pour ces questions est abondante ; citons Lagarias et Odlyzko [LO77], Lagarias, Montgomery et Odlyzko [LMO79], Serre [Ser81], Murty [MMS88], Osterlé [Oes79] ou plus récemment Iwaniec et Kowalski [IK04], Bellaïche [Bel], Winckler [Win13], Zaman [Zam15]...

Les résultats de ce chapitre ont été soumis à la publication, il s'agit d'un travail en collaboration avec Christian Maire. En particulier, nous démontrons le résultat suivant :

Proposition 9. *Soit K un corps de nombres de groupe de Galois absolu G_K non ramifié et soient χ et χ' deux caractères de G_K, de produit scalaire $\langle\chi,\chi'\rangle$ nul. En supposant vraies les conjectures d'Artin et de Riemann généralisée aux fonctions L d'Artin, il existe un idéal premier $\mathfrak{p}$ de K de norme inférieure à $C\chi(1)^4\ln^2|\mathrm{disc}\ K|$ tel que $\chi(\sigma_{\mathfrak{p}})\neq\chi'(\sigma_{\mathfrak{p}})$, où C est une constante absolue.*

En l'appliquant à des caractères particuliers du groupe alterné, les caractères conjugués, on obtient une borne sur un nombre premier p donnant l'écriture de la factorisation modulo p d'un polynôme répondant à certains critères.

Théorème 10. *Soit $P\in\mathbb{Z}[X]$ un polynôme de degré n, unitaire et $\mathbb{Q}$-irréductible. Supposons son discriminant égal au discriminant d'un corps quadratique. Sous la conjecture d'Artin et l'hypothèse de Riemann généralisée aux fonctions L d'Artin, on obtient :*

(i) Si n est impair, il existe un premier p plus petit que $C_1\ b(n)^4\ln^2|\mathrm{disc}\ P|$ tel que P soit irréductible dans $\mathbb{F}_p[X]$ avec

$$b(n)=\frac{(n-1)!}{2\left[\left(\frac{n-1}{2}\right)!\right]^2}\sim\frac{2^{n-\frac{3}{2}}}{\sqrt{\pi}\sqrt{n-1}}.$$

(ii) Si $n \equiv 0 (\mathrm{mod}\ 4)$, posons $m = 1 + n/4$. Alors il existe un nombre premier p plus petit que $C_2\ b(n)^4\ \ln^2 |\mathrm{disc}\ P|$ tel que $P (\mathrm{mod}\ p)$ se factorise sous la forme $Q_{2m-1}Q_{2m-3}$, où les polynômes Q_i sont des polynômes irréductibles de $\mathbb{F}_p[X]$ de degré i avec

$$b(n) = \frac{n!}{2(\frac{n}{2}+1)(\frac{n}{2}-1)[\frac{n}{2}(\frac{n}{4})!(\frac{n}{4}-1)!]^2} \sim \frac{2^{3/2}4^n}{n^{7/2}\pi^{3/2}}.$$

(iii) Supposons que l'entier n est un carré et écrivons $n = m^2$. Alors il existe un nombre premier p plus petit que $C_3\ b(n)^4\ \ln^2 |\mathrm{disc}\ P|$ tel que $P (\mathrm{mod}\ p)$ se factorise sous la forme $Q_1Q_3 \cdots Q_{2m-1}$, où les Q_i sont des polynômes irréductibles de $\mathbb{F}_p[X]$ de degré i avec

$$b(n) = \frac{n!}{2\prod_{r=1}^{m} \frac{(2m-r)!}{(m-r)!}} \sim \frac{\mathrm{e}^{m^2} m^{m^2+\frac{m}{2}+1}}{2^{\frac{3m^2+m+1}{2}} \pi^{\frac{m-1}{2}}}.$$

Les constantes C_1, C_2 et C_3 sont absolues.

Nous illustrerons également la proposition 9 par des calculs en étudiant l'évolution de la borne par rapport à la quantité $\ln^2 |\mathrm{disc}\ K|$. Pour cela, nous nous sommes concentrés sur des caractères non ramifiés irréductibles des groupes alternés A_5, A_7 et A_{13} au-dessus d'un corps quadratique K imaginaire ou réel. Pour ce faire, nous partons d'une famille de polynômes P_a de degré premier n (on prend $n = 5$, $n = 7$ et $n = 13$) paramétrés par un entier a dont on est assuré que le groupe de Galois est le groupe symétrique S_n. Par un bon choix de a, il en ressort une extension non ramifiée de $K := \mathbb{Q}(\sqrt{d_a})$ de groupe de Galois A_n, où d_a est le discriminant de P_a (pour nos familles on aura également $d_a = \mathrm{disc}\ K$). En faisant varier a, on obtient alors une famille d'extensions non ramifiées de corps quadratiques K de groupes de Galois A_n. Nous comparons la plus petite norme associée à un idéal premier dont le Frobenius sépare les caractères irréductibles de degré 3 pour A_5 (respectivement de degré 10 et 14 pour A_7) avec la borne en $\ln^2 |\mathrm{disc}\ K|$. Pour A_{13}, nous nous focalisons sur les caractères irréductibles conjugués venant d'un caractère irréductible de S_{13}.
Également, à la lumière des récents travaux de Pollack ([Pol13]), nous avons fait des simulations de la moyenne

$$\lim_{X\to\infty} \mu(P_a, \chi, \chi', X),$$

où

$$\mu(P_a, \chi, \chi', X) := \frac{\sum_{d_a \leqslant X} n(\chi, \chi')}{\sum_{d_a \leqslant X} 1},$$

et $n(\chi, \chi')$ est la plus petite norme associée à un idéal premier $\mathfrak{p}$ dont le Frobenius $\sigma_{\mathfrak{p}}$ sépare deux caractères χ et χ' irréductibles, non ramifiés et de même degré (ne dépendant pas de a) du corps $\mathbb{Q}(\sqrt{d_a})$ (associés aux polynômes P_a). Nos calculs semblent montrer que cette moyenne converge rapidement. La question du lien entre cette valeur de convergence et les caractères choisis se pose alors naturellement.

Chapitre 1

Fonctions L et fonctions L d'Artin

1.1 Fonctions L

Puisque nous traiterons tout au long de ce travail de fonctions L, nous reprenons proprement leur définition. Nous faisons le choix de les définir de la même façon que Henryk Iwaniec et Emmanuel Kowalski dans le chapitre 5 de [IK04]. D'autres auteurs, tels que Amir Akbary dans [Akb06], considèrent cette définition comme celle d'une classe de fonctions L, appelée classe Iwaniec-Kowalski. Dans la littérature, il existe d'autres familles axiomatiques de fonctions L, citons la classe de Selberg étudiée entre autres par Conrey et Ghosh dans [CG93], Kaczorowski et Perelli dans [KP99] ou encore [Per05]. Les fonctions L appartenant à cette classe doivent vérifier d'autres propriétés sur leurs coefficients. Malgré cette différence parmi les axiomes, plusieurs fonctions se retrouvent dans ces deux classes, notamment la fonction zêta de Riemann, les fonctions L de Dirichlet, les fonctions L de Hecke, ou conjecturalement les fonctions L d'Artin. Plus généralement, une fonction L de la classe Iwaniec-Kowalski n'ayant pas de pôle en $s = 0$ et satisfaisant la conjecture de Ramanujan-Petersson et sa version à l'infini appartient à la classe de Selberg (voir l'exercice 14 de [Akb06]).

1.1.1 Définitions et premières propriétés

Afin de définir les propriétés que doit satisfaire une fonction L (dans notre sens), nous avons besoin de quelques rappels généraux autour des séries de Dirichlet.

Quelques définitions préliminaires

Une série de Dirichlet, attachée à un "objet" arithmétique f, est une série de la forme $D(s, f) = \sum_{n\geqslant 1} a_f(n)n^{-s}$ où $s \in \mathbb{C}$ et $(a_f(n))_{n\in\mathbb{N}}$ est une suite de nombres complexes. Classiquement, on associe à $D(s, f)$ son abscisse de convergence absolue. Lorsque l'abscisse de convergence absolue d'une série de Dirichlet est un nombre positif, quitte à multiplier les coefficients $a_f(n)$ par une puissance de n, on peut supposer qu'elle vaut 1, c'est ce que nous ferons dans la suite. Remarquons que cette renormalisation n'affecte pas la propriété de multiplicativité des coefficients.

Lorsque $a_f(n)$ est une fonction multiplicative (c'est-à-dire $a_f(\prod_p p^{\alpha_p}) = \prod_p a_f(p^{\alpha_p})$), la

série de Dirichlet peut s'écrire en un produit eulérien, portant sur les nombres premiers :

$$D(s,f) = \prod_{p\geqslant 2}\Big(1+\sum_{k\geqslant 1}\frac{a_f(p^k)}{p^{ks}}\Big), \quad \mathrm{Re}(s)>1.$$

Le *dual* de la série $D(s,f)$ est la série de Dirichlet définie par $D(s,\bar{f}) = \overline{D(\bar{s},f)}$. On peut noter que $a_{\bar{f}}(n) = \overline{a_f(n)}$. Lorsque $D(s,\bar{f}) = D(s,f)$, on dit que $D(s,f)$ est *auto-duale*. Remarquons que dans ce cas la série de Dirichlet est à coefficients réels.

Nous aurons également besoin de la notion de facteur gamma : c'est une fonction, notée γ, faisant intervenir la fonction gamma d'Euler (voir la partie B.1.1 pour des détails sur cette fonction) qui s'écrit sous la forme :

$$\gamma(s) = \pi^{-ds/2}\prod_{j=1}^{d}\Gamma\left(\frac{s+\kappa_j}{2}\right),$$

où $d\in\mathbb{N}^*$ et $\kappa_j\in\mathbb{C}$.

Fonctions L

Une série de Dirichlet, $L(s,f)=\sum_{n\geqslant 1}a_f(n)n^{-s}$ d'abscisse de convergence absolue 1 telle que $a_f(1)=1$ et $a_f(n)\in\mathbb{C}$, est appelée *fonction L* si elle vérifie certaines propriétés que nous détaillons ici. De façon concise, elle doit pouvoir s'écrire sous forme de produit eulérien, posséder des invariants permettant de la compléter en une fonction méromorphe sur le plan complexe avec des pôles éventuels en $s=0$ et $s=1$ qui satisfait une équation fonctionnelle reliant les complexes s et $1-s$ et faisant apparaître l'objet dual de f.

Dans le demi-plan vertical ouvert non vide $\{s\ ;\ \mathrm{Re}(s)>1\}$, une fonction L s'écrit sous forme d'un produit eulérien du type :

$$L(s,f) = \prod_p\prod_{i=1}^{d(f)}(1-\alpha_{i,f}(p)p^{-s})^{-1},$$

avec $\alpha_{i,f}(p)\in\mathbb{C}$. L'entier $d(f)\geqslant 1$ (plus simplement noté d lorsque le contexte le permet) est le *degré* de la fonction L associée à f. On appelle *coefficients* les nombres complexes $a_f(n)$ et *paramètres locaux en un nombre premier* p les $\alpha_{i,f}(p)$, $1\leqslant i\leqslant d$. On demande qu'ils vérifient $|\alpha_{i,f}(p)|<p$ pour tout p (on se sert de cette condition par exemple afin d'obtenir le résultat de la proposition 1.1.3). La série de Dirichlet et le produit eulérien sont supposés absolument convergents dans le demi-plan ouvert vertical $\mathrm{Re}(s)>1$.

Remarque 1.1.1. L'existence du produit eulérien montre que la fonction $L(s,f)$ ne s'annule pas dans le demi-plan ouvert vertical $\mathrm{Re}(s)>1$.

Une fonction L possède un *facteur gamma*, noté γ_f, permettant à la *fonction L complétée* définie par

$$\Lambda(s,f) = q(f)^{s/2}\gamma_f(s)L(s,f) \quad \text{pour } \mathrm{Re}(s)>1,$$

d'admettre un prolongement méromorphe sur $\mathbb{C}$ avec des pôles éventuels en $s=0$ et $s=1$ et de satisfaire l'équation fonctionnelle

$$\Lambda(s,f) = \epsilon(f)\Lambda(1-s,\bar{f}), \tag{$\diamond$}$$

où $\epsilon(f)$, appelé signe de l'équation fonctionnelle[1], est de module 1. L'entier positif ou nul $q(f)$ est appelé le *conducteur*[2] de $L(s,f)$, il vérifie la propriété : lorsque p ne divise pas $q(f)$, $\alpha_{i,f}(p) \neq 0$ pour tout $1 \leqslant i \leqslant d$.
Le dual $L(s,\bar{f})$ est également une fonction L dont les invariants vérifient :

$$a_{\bar{f}}(n) = \overline{a_f(n)}, \quad \alpha_{i,\bar{f}}(p) = \overline{\alpha_{i,f}(p)}, \quad \gamma_{\bar{f}}(s) = \gamma_f(s), \quad q(\bar{f}) = q(f) \quad \text{et} \quad \epsilon(\bar{f}) = \overline{\epsilon(f)}.$$

Remarquons alors l'égalité reliant la fonction L complétée avec celle de son dual :

$$\Lambda(s,\bar{f}) = \overline{\Lambda(\bar{s},f)}.$$

Pour avoir une fonction L, on demande également à ce que le facteur gamma s'écrive

$$\gamma_f(s) = \pi^{-ds/2} \prod_{j=1}^{d} \Gamma\left(\frac{s+\kappa_j}{2}\right)$$

et vérifie $\mathrm{Re}(\kappa_j) > -1$ et que chacun des complexes κ_j soit ou un réel ou un nombre complexe dont le conjugué apparaît également dans le facteur gamma. Ils sont appelés *les paramètres locaux de $L(s,f)$ à l'infini*. Ces paramètres κ_j ne sont pas nécessairement deux à deux distincts et lorsqu'il s'agit d'un complexe non réel, le conjugué $\bar{\kappa}_j$ apparaît avec la même multiplicité. En ajoutant à ces conditions les propriétés de la fonction gamma d'Euler (voir la partie B.1.1), on en déduit que le facteur gamma n'a pas de zéro sur $\mathbb{C}$ et pas de pôle pour $\mathrm{Re}(s) \geqslant 1$. Ses pôles se situent en $s = -2n - \kappa_j$ avec $n \in \mathbb{N}$.

Lemme 1.1.2. *Soit*

$$\gamma_f(s) = \pi^{-ds/2} \prod_{j=1}^{d} \Gamma\left(\frac{s+\kappa_j}{2}\right),$$

où pour chaque j on a $\mathrm{Re}(\kappa_j) > -1$ et κ_j et son conjugué apparaissent avec la même multiplicité. Posons $A_j(t) = \frac{\frac{1}{2}+it+\kappa_j}{2}$. Alors, pour $s = 1/2 + it$ de partie réelle $1/2$ on a

$$\frac{\gamma_f'}{\gamma_f}(s) + \frac{\gamma_f'}{\gamma_f}(1-s) = -d\ln\pi + \sum_{j=1}^{d} \mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(A_j(t))\right).$$

<u>Preuve</u>
Par dérivation logarithmique, on a

$$\frac{\gamma_f'}{\gamma_f}(s) = -\frac{d\ln\pi}{2} + \frac{1}{2}\sum_{j=1}^{d} \frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa_j}{2}\right) = -\frac{d\ln\pi}{2} + \frac{1}{2}\sum_{j=1}^{d} \frac{\Gamma'}{\Gamma}\left(\frac{s+\overline{\kappa_j}}{2}\right),$$

la seconde égalité venant du fait que κ_j et son conjugué apparaissent avec la même multiplicité. Puisque $(\Gamma'/\Gamma)(\bar{s}) = \overline{(\Gamma'/\Gamma)(s)}$ et puisque pour $s = 1/2 + it$ de partie réelle $1/2$, on a $(1 - s + \overline{\kappa_j})/2 = (\bar{s} + \overline{\kappa_j})/2 = \overline{(s+\kappa_j)/2}$, on obtient $(\gamma_f'/\gamma_f)(1-s) = \overline{(\gamma_f'/\gamma_f)(s)}$, d'où le résultat. □

1. En général, il ne correspond pas à un signe au sens classique, c'est une traduction de l'anglais "root number".
2. La notion de conducteur provient de la géométrie arithmétique et se calcule souvent dans ce cadre-là.

Le théorème 2.1 de l'article [CG93] de Conrey et Ghosh donne l'unicité du facteur gamma ainsi que du conducteur associés à une fonction L.
Notons que par définition, la fonction L complétée est une fonction holomorphe dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$ et $(s(1-s))^{r(f)}\Lambda(s,f)$ est une fonction entière d'ordre 1, où $r(f)$ (ou plus simplement r s'il n'y a pas de confusion possible) est l'ordre du pôle ou du zéro de $\Lambda(s,f)$ en $s=1$ (si $\Lambda(s,f)$ a un pôle en $s=1$, $r(f)>0$; si la fonction $\Lambda(s,f)$ a un zéro en $s=1$, $r(f)<0$; sinon, $r(f)=0$).

Exemples

La fonction zêta de Dedekind d'un corps de nombres K de degré $[K:\mathbb{Q}] = d = r_1 + 2r_2$, avec (r_1, r_2) la signature de K, est une fonction L auto-duale. En effet, elle est définie, dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$, par :

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a}\subset\mathscr{O}_K \\ \mathfrak{a}\neq 0}} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p} \text{ premier}} \frac{1}{1-\mathrm{N}(\mathfrak{p})^{-s}},$$

la somme portant sur les idéaux entiers non nuls de $\mathscr{O}_K$ et le produit sur les idéaux entiers premiers de $\mathscr{O}_K$. De plus, elle se prolonge sur le plan complexe en une fonction méromorphe avec un seul pôle simple en $s=1$. En posant

$$\gamma(s) = \pi^{-ds/2}\Gamma\left(\frac{s}{2}\right)^{r_1+r_2}\Gamma\left(\frac{s+1}{2}\right)^{r_2}$$

et le conducteur $q = |\mathrm{disc}\ K|$, on sait que la fonction complétée $\Lambda(s) = q^{s/2}\gamma(s)\zeta_K(s)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$ avec deux pôles, en $s=1$ et $s=0$, simples et vérifie l'équation fonctionnelle $\Lambda(s) = \Lambda(1-s)$.

On peut en déduire le cas particulier $K = \mathbb{Q}$ ($r_1 = 1$ et $r_2 = 0$) de la fonction zêta de Riemann $\zeta(s)$ qui est donc également une fonction L.

Les fonctions L de Dirichlet satisfont également tous les points de notre définition.

Par ailleurs, citons la fonction zêta de Shintani qui est un exemple de série de Dirichlet n'appartenant pas à la classe de fonctions L étudiées. On pourra notamment se référer à l'article [Tho14] de Frank Thorne dans lequel il démontre que cette fonction ne peut même pas s'exprimer comme une somme finie de produits eulériens.

Premières propriétés

Dans cette partie, nous définissons les outils, notamment le conducteur analytique, dont nous aurons besoin pour la suite ainsi que quelques propriétés.
D'abord, on peut déduire de l'équation fonctionnelle que :

1. l'entier $r(f)$ est égal à l'ordre du pôle ou du zéro de $\Lambda(s,f)$ en $s=0$. Et puisque $\gamma_f(s)$ n'a ni zéro ni pôle pour $\mathrm{Re}(s) \geqslant 1$, $r(f)$ est également l'ordre du pôle ou du zéro de $L(s,f)$ en $s=1$. De plus, on a $r(\bar{f}) = r(f)$;
2. pour une fonction L auto-duale, on obtient $\epsilon(f)^2 = 1$ donc $\epsilon(f) = \pm 1$. Dans ce cas, le nom de signe de l'équation fonctionnelle prend tout son sens ;
3. puisque la fonction $\Lambda(s,f) = q(f)^{s/2}\gamma_f(s)L(s,f)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$ avec des pôles éventuels en $s=0$ et $s=1$, les pôles de la

fonction $\gamma_f(s)$ en $s \neq 0$ sont compensés par des zéros de la fonction $L(s,f)$: ce sont les *zéros triviaux*. Ils se situent aux points $-2n-\kappa_j \neq 0$ pour $n \in \mathbb{N}$. Les autres zéros de $L(s,f)$, appelés *zéros non triviaux*, sont situés dans la zone critique $0 \leqslant \mathrm{Re}(s) \leqslant 1$: mis à part éventuellement 0, ce sont exactement les zéros de $\Lambda(s,f)$. Notons que les éventuels pôles de $L(s,f)$ sont situés en $s=0$ et $s=1$;

4. Remarquons que si $L(s,f)$ n'a pas de pôle en $s=1$ alors $r(f) \leqslant 0$ donc $\Lambda(s,f)$ n'a également pas de pôle en $s=0$ (dans ce cas, $L(s,f)$ non plus) donc l'éventuel pôle de $\gamma_f(s)$ en $s=0$ est compensé par un zéro de $L(s,f)$. En particulier, cela démontre l'équivalence entre l'analyticité de $L(s,f)$ et celle de $\Lambda(s,f)$;
5. si ρ est un zéro non trivial de $L(s,f)$ alors, d'après la définition du dual de $L(s,f)$, $\bar{\rho}$ est un zéro de $L(s,\bar{f})$ et donc $\Lambda(\bar{\rho},\bar{f})=0$. Ainsi $\Lambda(1-\bar{\rho},f)=0$, on en déduit que $1-\bar{\rho}$ est un zéro de $L(s,f)$. Si ρ est un zéro trivial de $L(s,f)$ alors $\rho=-2n-\kappa_j \neq 0$ et donc $\bar{\rho}=-2n-\overline{\kappa_j}$. Par propriété des paramètres κ_j, $\bar{\rho}$ est également un zéro trivial.

Définition/Proposition 1.1.3. On note Λ_f la fonction de Von Mangoldt associée à la fonction $L(s,f)$:

$$\Lambda_f(n) = \begin{cases} \displaystyle\sum_{i=1}^{d} \alpha_{i,f}(p)^k \ln(p) & \text{si } n=p^k \text{ avec } p \text{ un nombre premier} \\ 0 & \text{sinon} \end{cases},$$

de telle sorte que, dans le demi-plan ouvert vertical $\mathrm{Re}(s)>1$,

$$-\frac{L'}{L}(s,f) = \sum_{n\geqslant 1} \Lambda_f(n) n^{-s}.$$

Remarque 1.1.4. Rappelons que toute fonction holomorphe f ne s'annulant pas sur un ouvert simplement connexe admet une détermination holomorphe du logarithme, notée g, vérifiant l'égalité $g'=f'/f$.
Par ailleurs, en notant $\ln(z)$ la détermination principale du logarithme, si $|z|<1$ (on a donc bien $1-z \notin \mathbb{R}_-$) alors :

$$-\ln(1-z) = \sum_{k=1}^{+\infty} \frac{z^k}{k}.$$

<u>Preuve de la proposition 1.1.3</u>
Dans le demi-plan ouvert vertical $\mathrm{Re}(s)>1$, puisque $|\alpha_{i,f}(p)|<p$, on a : $|\alpha_{i,f}(p)/p^s|<1$. La fonction

$$-\sum_p \sum_{i=1}^{d} \ln(1-\alpha_{i,f}(p)p^{-s}) = \sum_p \sum_{i=1}^{d} \sum_{k\geqslant 1} \frac{\alpha_{i,f}(p)^k}{k} p^{-ks}$$

étant clairement une détermination holomorphe du logarithme de $L(s,f)$ sur le demi-plan ouvert vertical $\mathrm{Re}(s)>1$, on obtient par dérivation :

$$\frac{L'}{L}(s,f) = -\sum_p \sum_{i=1}^{d} \sum_{k\geqslant 1} \frac{\alpha_{i,f}(p)^k \ln p}{p^{ks}},$$

d'où le résultat. □

Définition 1.1.5. On définit le *conducteur analytique* de $L(s,f)$ par :

$$\mathfrak{q}(s,f) = q(f)\mathfrak{q}_\infty(s,f),$$

où

$$\mathfrak{q}_\infty(s,f) = \prod_{j=1}^{d} \left(|s+\kappa_j|+3\right).$$

Remarque 1.1.6. On note simplement $\mathfrak{q}(f)$ pour $\mathfrak{q}(0,f) = q(f)\prod_{j=1}^{d}(|\kappa_j|+3)$.

Propriétés 1.1.7. *Remarquons quelques propriétés vérifiées par le conducteur :*

1. *on a* $\mathfrak{q}_\infty(s,f) \leqslant \mathfrak{q}(s,f)$ *;*
2. *le conducteur analytique en* 0 *peut être minoré de la façon suivante :* $\mathfrak{q}(f) \geqslant 3^d q(f)$ *;*
3. *on en déduit une majoration du degré :* $d \leqslant \ln \mathfrak{q}(f)$ *;*
4. *pour le conducteur analytique, on a :* $\mathfrak{q}(s,f) \leqslant \mathfrak{q}(f)\left(|s|+3\right)^d$ *;*
5. *sous la conjecture généralisée de Selberg (autrement dit, si les paramètres locaux à l'infini d'une fonction* L *sont dans* $\mathbb{R}^+$*),* $\mathfrak{q}(f) \leqslant \mathfrak{q}(s,f)$*, pour* $s \in \mathbb{C}$ *tel que* $\mathrm{Re}(s) \geqslant 0$.

PREUVE
Les trois premiers points sont évidents. Pour la quatrième propriété, on minore le terme de droite :

$$\begin{aligned}
\mathfrak{q}(f)\left(|s|+3\right)^d &= q(f)\prod_{j=1}^{d}\left(|s\kappa_j| + 3\left(|s|+|\kappa_j|+3\right)\right) \\
&\geqslant q(f)\prod_{j=1}^{d} 3\left(|s|+|\kappa_j|+3\right) \text{ car } |s\kappa_j| \geqslant 0 \\
&\geqslant 3^d\mathfrak{q}(s,f) \geqslant \mathfrak{q}(s,f).
\end{aligned}$$

Enfin, pour la dernière égalité, puisque $\mathrm{Re}(s) \geqslant 0$ et pour tout j, $\kappa_j \geqslant 0$, $|s+\kappa_j| \geqslant \kappa_j$ pour tout j. Ainsi,

$$\mathfrak{q}(f) = q(f)\prod_{j=1}^{d}(|\kappa_j|+3) \leqslant q(f)\prod_{j=1}^{d}(|s+\kappa_j|+3) = \mathfrak{q}(s,f).$$

□

1.1.2 Convolution de Rankin-Selberg

Nous aurons également besoin d'autres outils tels que la convolution de Rankin-Selberg dont nous devrons souvent admettre l'existence.
La définition suivante de la convolution de Rankin-Selberg de deux fonctions L est tirée de celle donnée par H. Iwaniec et E. Kowalski dans [IK04] page 97.

Définition 1.1.8. Soit $L(s,f)$ et $L(s,g)$ deux fonctions L de degrés respectifs d et e dont les paramètres locaux à l'infini sont respectivement $(\kappa_i)_{1\leqslant i\leqslant d}$ et $(\nu_j)_{1\leqslant j\leqslant e}$ et les paramètres locaux $(\alpha_{i,f}(p))_{1\leqslant i\leqslant d}$ et $(\beta_{j,g}(p))_{1\leqslant j\leqslant e}$. On dit que f et g ont une convolution de Rankin-Selberg s'il existe une fonction L, $L(s,f\otimes g)$, vérifiant :

— la fonction $L(s,f\otimes g)$ est une fontion L de degré de avec :

$$L(s,f\otimes g)=\prod_{p\nmid q(f)q(g)} L_p(s,f\otimes g)\prod_{p\mid q(f)q(g)} H_p(p^{-s}),$$

où $L_p(s,f\otimes g)=\prod_{i,j}(1-\alpha_{i,f}(p)\beta_{j,g}(p)p^{-s})^{-1}$ et $H_p(p^{-s})=\prod_{j=1}^{de}(1-\gamma_j(p)p^{-s})^{-1}$, avec $|\gamma_j(p)|<p$;

— le facteur gamma de $L(s,f\otimes g)$ est donné par

$$\gamma_{f\otimes g}(s)=\pi^{-des/2}\prod_{i,j}\Gamma\left(\frac{s+\mu_{i,j}}{2}\right),$$

avec $\mathrm{Re}(\mu_{i,j})\leqslant \mathrm{Re}(\kappa_i+\nu_j)$ et $|\mu_{i,j}|\leqslant|\kappa_i|+|\nu_j|$;

— le conducteur $q(f\otimes g)$ divise $q(f)^e q(g)^d$;

— la fonction $L(s,f\otimes\bar{f})$ a un pôle en $s=1$;

— sauf si l'une des fonctions $L(s,f)$ ou $L(s,g)$ peut se factoriser en un produit de fonctions L, la fonction $L(s,f\otimes g)$ est entière si $g\neq\bar{f}$.

Cette dernière propriété nous permettra de définir la convolution de Rankin-Selberg pour des fonctions L d'Artin associées à des caractères pas forcément irréductibles.

Propriétés 1.1.9. *Remarquons les propriétés suivantes :*

1. *si $L(s,f\otimes f)$ ou $L(s,f\otimes\bar{f})$ existe alors : $|\alpha_i(p)|<\sqrt{p}$ pour $p\nmid q(f)$ et $\mathrm{Re}(\kappa_j)>-1/2$;*
2. *le conducteur analytique vérifie $\mathfrak{q}(s,f\otimes g)\leqslant\mathfrak{q}(f)^e\mathfrak{q}(g)^d(|s|+3)^{de}$;*
3. *en 0, on a : $\mathfrak{q}(f\otimes g)\leqslant\mathfrak{q}(f)^e\mathfrak{q}(g)^d$.*

<u>Preuve</u>

D'abord, si $L(s,f\otimes f)$ (respectivement $L(s,f\otimes\bar{f})$) existe alors c'est une fonction L donc les paramètres locaux en p vérifient $|\alpha_{i,f\otimes f}(p)|<p$ (respectivement $|\alpha_{i,f\otimes\bar{f}}(p)|<p$). Or, lorsque $p\nmid q(f)$, on peut trouver des indices i et j tels que $\alpha_{j,f\otimes f}(p)=\alpha_{i,f}(p)^2$ (respectivement $\alpha_{j,f\otimes\bar{f}}(p)=\alpha_{i,f}(p)\overline{\alpha_{i,f}(p)}$) donc $|\alpha_{i,f}(p)|^2<p$. De plus, dans ces cas, $\mathrm{Re}(\mu_{i,i})\leqslant 2\mathrm{Re}(\kappa_i)$ (puisque $\gamma_f(s)=\gamma_{\bar{f}}(s)$) et puisqu'on a supposé $\mathrm{Re}(\kappa_j)>-1$ pour des fonctions L, on doit avoir $\mathrm{Re}(\kappa_i)>-1/2$. Ensuite, en utilisant $q(f\otimes g)\mid q(f)^e q(g)^d$ et $|\mu_{i,j}|\leqslant|\kappa_i|+|\nu_j|$ (vraies par définition), on a :

$$\begin{aligned}\mathfrak{q}(s,f\otimes g)&=q(f\otimes g)\prod_{i,j}(|s+\mu_{i,j}|+3)\\&\leqslant q(f)^e q(g)^d\prod_{i=1}^{d}\prod_{j=1}^{e}(|s|+3)(|\kappa_i|+3)(|\nu_j|+3)\\&\leqslant q(f)^e q(g)^d(|s|+3)^{de}\prod_{i=1}^{d}(|\kappa_i|+3)^e\prod_{j=1}^{e}(|\nu_j|+3)^d\\&\leqslant\mathfrak{q}(f)^e\mathfrak{q}(g)^d(|s|+3)^{de}.\end{aligned}$$

Enfin, pour le dernier point, on obtient de la même façon :

$$\begin{aligned}
\mathfrak{q}(f\otimes g) &= q(f\otimes g)\prod_{i,j}(|\mu_{i,j}|+3)\\
&\leqslant q(f)^e q(g)^d \prod_{i=1}^{d}\prod_{j=1}^{e}(|\kappa_i|+3)(|\nu_j|+3)\\
&\leqslant q(f)^e q(g)^d \left(\prod_{i=1}^{d}(|\kappa_i|+3)\right)^e \left(\prod_{j=1}^{e}(|\nu_j|+3)\right)^d\\
&\leqslant \left(q(f)\prod_{i=1}^{d}(|\kappa_j|+3)\right)^e \left(q(g)\prod_{j=1}^{e}(|\nu_j|+3)\right)^d\\
&\leqslant \mathfrak{q}(f)^e\mathfrak{q}(g)^d. \qquad \square
\end{aligned}$$

1.1.3 Conjectures

Dans la suite, nous supposerons vraies certaines conjectures classiques que nous énonçons ici. Commençons par l'hypothèse de Riemann propre aux fonctions L. Celle-ci concerne les zéros d'une fonction L et nous la supposerons vraie quasi systématiquement, bien qu'aucun exemple de fonction L la satisfaisant ne soit connu. Cependant, on connaît des résultats sur des régions sans zéro : par exemple, pour une fonction L, $L(s,f)$, de degré d dont les convolutions de Rankin-Selberg $L(s,f\otimes f)$ et $L(s,f\otimes\bar{f})$ existent et vérifient $L(s,f\otimes f)$ est entière si $f\neq\bar{f}$ tandis que $L(s,f\otimes\bar{f})$ a un pôle simple en $s=1$, en supposant, de plus, que les paramètres locaux de $L(s,f)$ aux premiers p divisant le conducteur vérifient $|\alpha_{i,f}(p)|^2\leqslant p/2$, le théorème 5.10 de [IK04] démontre l'existence d'une constante absolue $c>0$ telle que $L(\sigma+it,f)$ ne s'annule pas dans la région du plan complexe définie par $\sigma\geqslant 1-\frac{c}{d^4\ln(\mathfrak{q}(f)(|t|+3))}$, sauf pour une fonction auto-duale qui peut avoir un zéro réel strictement inférieur à 1.

Conjecture 1.1.10 (*Hypothèse de Riemann généralisée*)**.** *Soit $L(s,f)$ une fonction L. Alors tous les zéros de $L(s,f)$ situés dans la bande critique $0<\mathrm{Re}(s)<1$ sont sur la droite $\mathrm{Re}(s)=1/2$.*

Intéressons-nous maintenant aux zéros ρ situés sur les bords de la bande critique.
Puisque $\mathrm{Re}(-2n-\kappa_j)<1$ pour tout $n\in\mathbb{N}$, aucune fonction L ne possède de zéro trivial de partie réelle 1. D'autre part, nous verrons que les exemples de fonctions L étudiés ne possèdent pas de zéros non triviaux de partie réelle 1. Dans la suite, on supposera donc souvent qu'une fonction L n'a pas de zéro de partie réelle égale à 1. Notons qu'en supposant cette hypothèse vraie, les zéros de partie réelle nulle d'une fonction L sont des zéros triviaux (sinon l'équation fonctionnelle donne $\Lambda(it,f)=0=\Lambda(1+it,f)$) et il y en a donc au plus d, le degré de la fonction L. En particulier, les zéros de la fonction complétée $\Lambda(s,f)$ se situent dans la bande $0<\mathrm{Re}(s)<1$ et sont nécessairement des zéros de la fonction $L(s,f)$.

Dans un cas particulier, le théorème 35 de [Akb06] démontre qu'une fonction L n'a effectivement pas de zéro de partie réelle 1.

THÉORÈME 1.1.11 (Rankin (1939), Ogg (1969))**.** *Soit $L(s,f)$ une fonction L entière telle que $L(s,f\otimes\bar{f})$ existe et a un pôle simple en $s=1$. Alors la fonction L n'a pas de zéro de partie réelle égale à 1.*

Remarquons que si la fonction $L(s, f \otimes \bar{f})$ a un pôle d'ordre strictement supérieur à 1 en $s = 1$, on peut souvent écrire la fonction $L(s, f)$ sous forme d'un produit de fonctions L et donc appliquer le théorème à chacune d'entre elles.

Illustrons cela sur l'exemple des fonctions L d'Artin (définies dans la section suivante). Pour un caractère irréductible ψ non trivial du groupe de Galois d'une extension L/K, sous la conjecture d'Artin, d'après la proposition 1.2.26, la fonction L d'Artin $L(s, \psi, L/K)$ satisfait bien le critère du théorème précédent. Ainsi, $L(1 + it, \psi, L/K) \neq 0$ pour tout $t \in \mathbb{R}$. Il en est de même pour la fonction zêta de Dedekind ζ_K (voir, par exemple, le théorème 5.33 de [IK04]). Et pour les fonctions L d'Artin associées à un caractère χ quelconque, on utilise la décomposition du caractère en somme de caractères irréductibles : $\chi = n_0\mathbf{1} + \sum_i n_i\psi_i$ avec $n_i \in \mathbb{N}$ et ψ_i irréductibles. On peut donc écrire

$$L(s, \chi, L/K) = \zeta_K(s)^{n_0} \prod_i L(s, \psi_i, L/K)^{n_i}.$$

On en déduit alors que $L(1 + it, \chi, L/K) \neq 0$ pour tout $t \in \mathbb{R}$.

En ajoutant l'hypothèse de Riemann généralisée à l'hypothèse que nous faisons sur les zéros de partie réelle 1, nous obtenons la conjecture suivante que nous appellerons Grande Hypothèse de Riemann (GRH) :

Conjecture 1.1.12 (Grande Hypothèse de Riemann (GRH)). *À l'exception des éventuels zéros triviaux de partie réelle nulle, tous les zéros d'une fonction L situés dans la bande $0 \leqslant \mathrm{Re}(s) \leqslant 1$ sont situés sur la droite $\mathrm{Re}(s) = 1/2$.*

Ensuite, les conjectures suivantes concernent les paramètres et coefficients d'une fonction L. Dans le chapitre suivant, pour distinguer deux fonctions L d'Artin à partir de leurs paramètres locaux, nous aurons besoin de certaines versions de ces conjectures.

Conjecture 1.1.13 (*Conjecture de Ramanujan-Petersson*). *Soit $L(s, f)$ une fonction L. Alors, pour tout $i \in [\![1, d]\!]$, pour les premiers p ne divisant pas $q(f)$, on a $|\alpha_{i,f}(p)| = 1$ et sinon $|\alpha_{i,f}(p)| \leqslant 1$.*

Remarque 1.1.14. Pour une fonction L satisfaisant la conjecture de Ramanujan-Petersson, on a : $|a_f(n)| \leqslant \tau_d(n)$, où $\tau_d(n)$ représente le nombre de façons d'écrire l'entier n sous forme d'un produit de d nombres naturels.

Conjecture 1.1.15 (*Conjecture de Ramanujan-Petersson à l'infini* ou *conjecture généralisée de Selberg*). *Soit $L(s, f)$ une fonction L. Alors, pour tout $j \in [\![1, d]\!]$, $\mathrm{Re}(\kappa_j) \geqslant 0$.*

Remarque 1.1.16. Dans ce cas, le facteur gamma n'a pas de pôle sur l'ensemble des complexes vérifiant $\mathrm{Re}(s) > 0$.

Il n'est pas difficile de trouver des exemples de fonctions L satisfaisant ces deux dernières conjectures. Par exemple, la fonction zêta de Dedekind d'un corps de nombres K les illustre : en effet, ses paramètres locaux en un idéal premier valent 1 et ceux à l'infini sont 0 et 1.

1.2 Fonctions L d'Artin

Ce chapitre est consacré au cas particulier des fonctions L d'Artin. Celles-ci sont associées à des corps de nombres galoisiens et à une représentation du groupe de Galois correspondant. On peut les voir comme une généralisation de la fonction zêta de Dedekind, au sens de la propriété 1.2.7. En fait, ce ne sont que conjecturalement (voir la conjecture d'Artin 1.2.10) des fonctions L au sens où nous les avons définies dans la partie précédente : en effet, l'équation fonctionnelle ne traite pas de la position des pôles éventuels de la fonction complétée. En revanche, les fonctions L d'Artin vérifient la conjecture de Ramanujan-Petersson à l'infini (conjecture 1.1.15) et possèdent une convolution de Rankin-Selberg (voir partie 1.2.3) correspondant à la fonction L d'Artin associée au produit tensoriel des représentations. Après avoir énoncé les propriétés des fonctions L d'Artin, nous nous intéresserons au cas où le corps de base est simplement $\mathbb{Q}$ pour expliciter les invariants.

1.2.1 Définitions et propriétés

Soit L/K une extension galoisienne de groupe de Galois G, (ρ, V) une représentation de G de caractère χ. Pour $\mathfrak{p}$ un idéal premier de K, on note $D_\mathfrak{p}$ le groupe de décomposition et $I_\mathfrak{p}$ le groupe d'inertie d'un idéal premier $\mathfrak{P}$ de $\mathscr{O}_L$ au-dessus de $\mathfrak{p}$. Soit $\sigma_\mathfrak{p} = \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ l'automorphisme de Frobenius engendrant $D_\mathfrak{p}/I_\mathfrak{p}$ (voir partie B.1.3 pour plus de précisions). On note $V^{I_\mathfrak{p}} = \{v \in V \,:\, \forall\, i \in I_\mathfrak{p},\ \rho(i)(v) = v\}$ le sous-espace vectoriel de V stable par $I_\mathfrak{p}$.

On note $\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_\mathfrak{p}; V^{I_\mathfrak{p}})$ le déterminant défini de la façon suivante :

- lorsque $\mathfrak{p}$ est non ramifié, $\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_\mathfrak{p}; V^{I_\mathfrak{p}}) = \det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\rho(\sigma_\mathfrak{p}))$;
- si $\mathfrak{p}$ est ramifié :
  - soit $V^{I_\mathfrak{p}} = \{0\}$ et alors $\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_\mathfrak{p}; V^{I_\mathfrak{p}}) = 1$;
  - soit $V^{I_\mathfrak{p}} \neq \{0\}$, dans ce cas on note $\tilde{\rho}$ la représentation induite par (ρ, V) (voir, par exemple, l'exercice 7.1 de [Ser77], [Neu99] page 521 ou encore [Sny02] page 44). Ainsi, $(\tilde{\rho}, V^{I_\mathfrak{p}})$ est une représentation de $D_\mathfrak{p}/I_\mathfrak{p}$ de caractère associé $\tilde{\chi}$ tel que $\tilde{\chi}(\bar{\sigma}) = \dfrac{1}{|I_\mathfrak{p}|}\displaystyle\sum_{e \in I_\mathfrak{p}} \chi(e\sigma)$ avec σ un antécédent de $\bar{\sigma}$ dans $D_\mathfrak{p}$ ([Mar77b] page 11). (Dans la suite, nous utiliserons souvent la notation χ au sens abusif de $\tilde{\chi}$.) Ainsi, dans ce cas, $\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_\mathfrak{p}; V^{I_\mathfrak{p}}) = \det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\tilde{\rho}(\sigma_\mathfrak{p}))$.

  Sinon, en notant $\varphi_\mathfrak{p}$ un représentant de $\sigma_\mathfrak{p}$ dans $D_\mathfrak{p}$, on a $\rho(\varphi_\mathfrak{p}) \in \mathrm{GL}(V^{I_\mathfrak{p}})$ (en effet, puisque $I_\mathfrak{p}$ est distingué dans $D_\mathfrak{p}$, pour tout $i \in I_\mathfrak{p}$, il existe $i' \in I_\mathfrak{p}$ tel que $i\varphi_\mathfrak{p} = \varphi_\mathfrak{p} i'$ d'où $\rho(i)(\rho(\varphi_\mathfrak{p})(v)) = \rho(\varphi_\mathfrak{p})(v)$ pour $v \in V^{I_\mathfrak{p}}$) donc le déterminant correspond au déterminant de la matrice $\rho(\varphi_\mathfrak{p})$ valant 0 en dehors de $V^{I_\mathfrak{p}}$ et ne dépend pas du choix du relèvement. C'est en utilisant cette deuxième façon de voir le déterminant que nous pourrons utiliser le logiciel de calcul PARI/GP ([PAR15]) pour trouver les paramètres locaux.

Remarque 1.2.1. La proposition B.2.7 permet de retrouver

$$\tilde{\chi}(\bar{1}) = \frac{1}{|I_\mathfrak{p}|}\sum_{e \in I_\mathfrak{p}} \chi(e) = \dim V^{I_\mathfrak{p}}.$$

Pour tout $s \in \mathbb{C}$, on peut montrer que $\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_\mathfrak{p}; V^{I_\mathfrak{p}})$ ne dépend ni du choix d'un idéal premier de $\mathscr{O}_L$ au-dessus de $\mathfrak{p}$ ni de la représentation choisie isomorphe à (ρ, V).

Bien que ce ne soit pas une fonction L au sens de la définition donnée dans la partie 1.1.1 (l'analyticité n'étant pas vérifiée comme nous le verrons plus tard), nous appelons *fonction L d'Artin* la série de Dirichlet définie dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$ par :

$$L(s, \chi, L/K) = \prod_{\mathfrak{p} \subset \mathscr{O}_K} \frac{1}{\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_{\mathfrak{p}}; V^{I_{\mathfrak{p}}})}.$$

Lorsqu'il n'y pas de confusion possible, nous noterons simplement $L(s, \chi)$.

Remarque 1.2.2. D'après son écriture, une fonction L d'Artin ne s'annule pas pour des complexes de partie réelle strictement supérieure à 1.

Définition 1.2.3. Pour une fonction L d'Artin, $L(s, \chi, L/K)$, dont la représentation (ρ, V) associée au caractère χ est de degré d et $(\widetilde{\rho}, V^{I_{\mathfrak{p}}})$ de degré $d_{\mathfrak{p}}$, on note $\alpha_{i,\rho}(\mathfrak{p})$ (ou $\alpha_{i,\chi}(\mathfrak{p})$ selon le contexte), $1 \leqslant i \leqslant d$, les valeurs propres de $\widetilde{\rho}(\sigma_{\mathfrak{p}})$ avec la convention $\alpha_{i,\rho}(\mathfrak{p}) = 0$ si $d_{\mathfrak{p}} < i \leqslant d$. Les complexes $\{\alpha_{i,\rho}(\mathfrak{p})\}_{1 \leqslant i \leqslant d}$ sont les *paramètres locaux en* $\mathfrak{p}$ de $L(s, \chi)$.

Remarque 1.2.4. En particulier, $|\alpha_{i,\rho}(\mathfrak{p})| = 1$ pour tout $1 \leqslant i \leqslant d_{\mathfrak{p}}$. En effet, $\sigma_{\mathfrak{p}}$ appartenant à un groupe fini, les valeurs propres de $\widetilde{\rho}(\sigma_{\mathfrak{p}})$ sont des racines de l'unité.
D'autre part, d'après leur définition pour des fonctions L d'Artin, les paramètres locaux vérifient : $\chi(\sigma_{\mathfrak{p}}^k) = \sum_{i=1}^{d} \alpha_{i,\rho}(\mathfrak{p})^k$.
Les paramètres locaux en les idéaux premiers apparaissent dans l'écriture sous forme de produit eulérien d'une fonction L d'Artin.

Proposition 1.2.5. *Soit $L(s, \chi, L/K)$ une fonction L d'Artin et d le degré de la représentation (ρ, V) associée au caractère χ. Alors :*

$$L(s, \chi, L/K) = \prod_{\mathfrak{p} \subset \mathscr{O}_K} \prod_{i=1}^{d} \left(1 - \alpha_{i,\rho}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}\right)^{-1} = \sum_{n \geqslant 1} a_\chi(n) n^{-s},$$

le produit portant sur les idéaux premiers non nuls de K.

<u>Preuve</u>
Par définition des valeurs propres, pour tout idéal premier $\mathfrak{p}$, on a :

$$\det(X\mathrm{Id} - \widetilde{\rho}(\sigma_{\mathfrak{p}})) = \prod_{i=1}^{d_{\mathfrak{p}}} (X - \alpha_{i,\rho}(\mathfrak{p})).$$

D'où

$$\begin{aligned}
\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_{\mathfrak{p}}; V^{I_{\mathfrak{p}}}) &= \det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\tilde{\rho}(\sigma_{\mathfrak{p}})) \\
&= \mathrm{N}(\mathfrak{p})^{-d_{\mathfrak{p}}s} \det(\mathrm{N}(\mathfrak{p})^{s}\mathrm{Id} - \tilde{\rho}(\sigma_{\mathfrak{p}})) \\
&= \mathrm{N}(\mathfrak{p})^{-d_{\mathfrak{p}}s} \prod_{i=1}^{d_{\mathfrak{p}}} (\mathrm{N}(\mathfrak{p})^{s} - \alpha_{i,\rho}(\mathfrak{p})) \\
&= \prod_{i=1}^{d_{\mathfrak{p}}} (1 - \alpha_{i,\rho}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}) \\
&= \prod_{i=1}^{d} \left(1 - \alpha_{i,\rho}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}\right).
\end{aligned}$$

□

On définit la fonction de Von Mangoldt Λ_χ associée à une fonction L d'Artin de la façon suivante :

Définition/Proposition 1.2.6. Avec les notations précédentes, dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$, on a :

$$-\frac{L'}{L}(s,\chi) = \sum_{n\geqslant 1} \Lambda_\chi(n) n^{-s},$$

avec $\Lambda_\chi(n) = \sum_{\substack{\mathfrak{p},k \\ n=\mathrm{N}(\mathfrak{p})^k}} \sum_{i=1}^{d} \alpha_{i,\rho}(\mathfrak{p})^k \ln \mathrm{N}(\mathfrak{p})$. En particulier, $\Lambda_\chi(n) = 0$ si n n'est pas une puissance d'un nombre premier.

PREUVE

On procède de la même façon que pour la proposition 1.1.3 (ici $|\alpha_{i,\rho}(\mathfrak{p})| \leqslant 1$) :

$$-\sum_{\mathfrak{p}} \sum_{i=1}^{d} \ln(1-\alpha_{i,\rho}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}) = \sum_{\mathfrak{p}} \sum_{i=1}^{d} \sum_{k\geqslant 1} \frac{\alpha_{i,\rho}(\mathfrak{p})^k \mathrm{N}(\mathfrak{p})^{-ks}}{k}$$

est une détermination holomorphe du logarithme de $L(s,f)$ ($\ln(z)$ désignant la détermination principale du logarithme). En dérivant, on obtient donc :

$$\frac{L'}{L}(s,\chi) = -\sum_{\mathfrak{p}} \sum_{i=1}^{d} \sum_{k\geqslant 1} \frac{\alpha_{i,\rho}(\mathfrak{p})^k \ln \mathrm{N}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})^{ks}},$$

d'où le résultat. □

Propriétés 1.2.7.

1. *En évaluant la fonction L en la représentation triviale du groupe G, on obtient :*

$$L(s, \mathbf{1}_G, L/K) = \zeta_K(s),$$

   où ζ_K est la fonction zêta de Dedekind de K.

2. *Si χ_1, χ_2 sont deux caractères de G associés aux représentations (ρ_1, V_1) et (ρ_2, V_2) alors :*

$$L(s, \chi_1+\chi_2, L/K) = L(s,\chi_1, L/K) L(s, \chi_2, L/K),$$

   où $\chi_1+\chi_2$ correspond au caractère associé à la somme directe des représentations $V_1 \oplus V_2$.

3. *Soit $L/M/K$ une tour d'extensions galoisiennes et ψ un caractère de $H = \mathrm{Gal}(L/M)$. On note $\mathrm{Ind}_H^G \psi$ le caractère induit sur $G = \mathrm{Gal}(L/K)$ par ψ. Alors*

$$L(s,\psi, L/L^H) = L(s, \mathrm{Ind}_H^G \psi, L/K).$$

PREUVE

1. On est dans le cas particulier $\chi = \mathbf{1}_G$ donc $\dim(V) = \chi(1) = 1$ et $V^{\mathrm{I}_p} = V$. Ainsi $\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\sigma_{\mathfrak{p}}; V^{I_{\mathfrak{p}}}) = 1 - \mathrm{N}(\mathfrak{p})^{-s}$.

2. On pose (ρ_1, V_1) et (ρ_2, V_2) les représentations de G associées respectivement à χ_1 et χ_2. Alors $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ est une représentation de caractère $\chi_1 + \chi_2$. Et $(V_1 \oplus V_2)^{\mathrm{I}_p} = V_1^{\mathrm{I}_p} \oplus V_2^{\mathrm{I}_p}$ donc

$$\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}(\rho_1 \oplus \rho_2)(\sigma_\mathfrak{p}), (V_1 \oplus V_2)^{\mathrm{I}_p}) = \det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\rho_1(\sigma_\mathfrak{p}), V_1^{\mathrm{I}_p}) \times \det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\rho_2(\sigma_\mathfrak{p}), V_2^{\mathrm{I}_p}).$$

3. On pourra se référer à [Neu99] page 522 ou [Sny02] pages 60 et 73. □

On peut relier les fonctions zêta de Dedekind de L et de K en faisant intervenir des fonctions L d'Artin. D'ailleurs, le point de départ des recherches d'Artin sur les fonctions L a été de prouver que le quotient $(\zeta_L/\zeta_K)(s)$ est une fonction entière pour une extension galoisienne L/K. Ce résultat est appelé théorème d'Aramata-Brauer, on pourra en trouver une preuve dans [MM97] (Theorem 3.1). La propriété plus générale énonçant que $(\zeta_L/\zeta_K)(s)$ est une fonction entière pour toute extension L/K reste un problème ouvert connu sous la nom de conjecture de Dedekind. On pourra se référer au paragraphe 4 du chapitre 2 de [MM97] pour en savoir davantage sur les résultats connus, notamment dus à Uchida et Van der Wall.

Corollaire 1.2.8. *On a :*

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq \mathbf{1}_G} L(s, \chi, L/K)^{\chi(1)},$$

où le produit porte sur les caractères non triviaux irréductibles de $G = \mathrm{Gal}(L/K)$.

<u>Preuve</u>
Notons $H = \{e\} = \mathrm{Gal}(L/L)$. On utilise les différents résultats de la proposition précédente et l'écriture de la représentation régulière sous forme de caractères (voir le corollaire B.2.5) :

$$\begin{aligned}
\zeta_L(s) &= L(s, \mathbf{1}_{\{e\}}, L/L) \\
&= L(s, \mathbf{1}_{\{e\}}, L/L^{\{e\}}) \\
&= L(s, \mathrm{Ind}_{\{e\}}^G \mathbf{1}_{\{e\}}, L/K) \\
&= L\left(s, \sum_\chi \chi(1)\chi, L/K\right) \\
&= \prod_\chi L\left(s, \chi, L/K\right)^{\chi(1)} \\
&= L(s, 1_G, L/K) \prod_{\chi \neq \mathbf{1}_G} L(s, \chi, L/K)^{\chi(1)} \\
&= \zeta_K(s) \prod_{\chi \neq \mathbf{1}_G} L(s, \chi, L/K)^{\chi(1)}.
\end{aligned}$$

□

Ceci nous permet d'en déduire une propriété vérifiée par des corps arithmétiquement équivalents, c'est-à-dire des corps ayant la même fonction zêta de Dedekind.

Propriété 1.2.9. *Soit K, K' deux corps arithmétiquement équivalents et $d \in \mathbb{Z}$ tel que $\sqrt{d}$ n'appartienne ni à K ni à K'. Alors $L(s,\chi,K(\sqrt{d})/K) = L(s,\chi,K'(\sqrt{d})/K')$ où χ est le caractère non trivial du groupe de Galois associé aux extensions quadratiques $K(\sqrt{d})/K$ ou $K'(\sqrt{d})/K'$.*

PREUVE
Puisque K et K' sont arithmétiquement équivalents, on a $\zeta_K(s) = \zeta_{K'}(s)$. De plus, sous ces hypothèses, d'après le théorème 4.2 de [Van08] par exemple, on sait que les corps $K(\sqrt{d})$ et $K'(\sqrt{d})$ sont également arithmétiquement équivalents, autrement dit $\zeta_{K(\sqrt{d})}(s) = \zeta_{K'(\sqrt{d})}(s)$. En appliquant le corollaire 1.2.8 précédent aux corps $K(\sqrt{d})$ et $K'(\sqrt{d})$, on a :

$$\zeta_K(s)L(s,\chi,K(\sqrt{d})/K) = \zeta_{K'}(s)L(s,\chi,K'(\sqrt{d})/K').$$

D'où le résultat. □

Le théorème de Brauer (chapitre 2, page 29 de [Ser67]) permet d'écrire tout caractère de G comme combinaison linéaire à coefficients entiers de caractères induits par des caractères de degré 1 : soit χ caractère de G, il existe des sous-groupes H_i de G, des caractères ψ_i de H_i de degré 1 et des entiers $m_i \in \mathbb{Z}$ tels que $\chi = \sum_i m_i \mathrm{Ind}_{H_i}^G \psi_i$.

En utilisant les propriétés précédentes, on a : $L(s,\chi,L/K) = \prod_i L(s,\psi_i,L/L^{H_i})^{m_i}$.

Pour un caractère non trivial ψ de dimension 1, $L(s,\psi,L/K)$ se prolonge analytiquement sur $\mathbb{C}$ (on l'identifie à une fonction L de Hecke). Pour le caractère trivial, on sait que $L(s,\mathbf{1}_G,L/K) = \zeta_K(s)$ admet un prolongement sur $\mathbb{C}$ en une fonction méromorphe avec un pôle simple en $s=1$. Ainsi, nous pouvons montrer que $L(s,\chi,L/K)$ admet un prolongement méromorphe sur $\mathbb{C}$.

Dans la suite de ce travail, nous nous placerons souvent dans le cadre où la conjecture suivante est vraie.

Conjecture 1.2.10 (Conjecture d'Artin)**.** *Toute fonction L d'Artin $L(s,\chi,L/K)$ se prolonge en une fonction holomorphe sur $\mathbb{C}$ sauf éventuellement en $s=1$ où il y a un pôle d'ordre égal au nombre de fois où intervient le caractère trivial dans la décomposition de χ.*
Ou encore, de façon équivalente, la fonction L d'Artin $L(s,\chi,L/K)$ (ou sa fonction complétée $\Lambda(s,\chi,L/K)$, voir partie suivante pour une définition) se prolonge en une fonction entière pour un caractère χ irréductible et non trivial.

Remarque 1.2.11. L'équivalence provient de la connaissance de la fonction zêta de Dedekind : elle se prolonge sur $\mathbb{C}$ en une fonction méromorphe avec un pôle simple en $s=1$. En effet, en décomposant une représentation (ρ,V) de G de caractère χ en somme de représentations irréductibles, on peut écrire $\chi = \sum_{i=1}^r n_i\chi_i$ avec $n_i \in \mathbb{N}$ et χ_i les caractères irréductibles de G, χ_1 étant le caractère trivial. On a alors :

$$L(s,\chi,L/K) = \prod_{i=1}^r L(s,\chi_i)^{n_i} = \zeta_K(s)^{n_1}\prod_{i=2}^r L(s,\chi_i)^{n_i}.$$

Remarques 1.2.12. La conjecture est vraie pour des caractères de degré 1, les fonctions L d'Artin correspondant alors aux fonctions L de Hecke.

Rappelons que sous la conjecture d'Artin, nous avons démontré (voir partie 1.1.3) que les fonctions L d'Artin n'ont pas de zéro de partie réelle égale à 1 : l'hypothèse GRH (conjecture 1.1.12) est donc équivalente à l'hypothèse de Riemann généralisée.

1.2.2 Équation fonctionnelle

On complète la fonction L d'Artin par des facteurs gamma correspondant aux places infinies de K. Commençons par définir l'idéal appelé conducteur d'Artin. Pour cela, nous devons d'abord définir $f_{\mathfrak{p}}(\chi)$.

Définition 1.2.13. Soit χ un caractère de $G = \mathrm{Gal}(L/K)$ et $\mathfrak{p}$ un idéal premier de K. Soit $\mathscr{P}$ un idéal premier de L au-dessus de $\mathfrak{p}$. On note v_L la valuation de L normalisée. Pour $i \geqslant 0$, on appelle $G_i = \{\sigma \in G \,|\, \forall x \in \mathscr{O}_L,\ v_L(\sigma(x) - x) \geqslant i+1\}$ le i-ème groupe de ramification de $\mathscr{P}$ au-dessus de $\mathfrak{p}$, G_0 étant le groupe d'inertie. On obtient la suite décroissante suivante : $I_{\mathfrak{p}} = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$.
On définit le nombre rationnel suivant, qui ne dépend pas du choix de $\mathscr{P}$ au-dessus de $\mathfrak{p}$:

$$f_{\mathfrak{p}}(\chi) = \sum_{i=0}^{+\infty} \frac{|G_i|}{|G_0|} \mathrm{codim} V^{G_i}.$$

Propriétés 1.2.14. *Pour tout caractère χ de G :*

1. *le nombre $f_{\mathfrak{p}}(\chi)$ est un entier naturel ;*
2. *si $\mathfrak{p}$ est non ramifié dans L/K, $f_{\mathfrak{p}}(\chi) = 0$;*
3. *pour le caractère trivial, $f_{\mathfrak{p}}(\mathbf{1}_G) = 0$ pour tout idéal $\mathfrak{p}$.*

<u>Preuve</u>
Pour le point 1, on pourra se référer à [Neu99] page 527-533 ou [Sny02].
Le point 2. est évident en remarquant qu'il n'y a, dans ce cas, qu'un seul groupe dans la suite : $G_0 = \{1\}$.
Pour le caractère trivial, $V^{G_i} = V$, d'où le résultat. □

Définition 1.2.15 (Conducteur d'Artin)**.** Le *conducteur d'Artin* associé au caractère χ est l'idéal $f(\chi)$ de K défini par :

$$f(\chi) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{f_{\mathfrak{p}}(\chi)}.$$

Propriété 1.2.16. *Si $\mathfrak{p}$ est non ramifié dans L/K alors, pour tout caractère χ de G, $\mathfrak{p} \nmid f(\chi)$.*

Définissons le facteur gamma aux places infinies approprié aux fonctions L d'Artin.

Définition 1.2.17. Soit d le degré de la représentation associée à χ. On définit γ_χ comme le produit suivant sur les places infinies de K :

$$\gamma_\chi(s) = \prod_{v \text{ complexes}} \left(\pi^{-s-1/2}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\right)^d$$
$$\times \prod_{v \text{ réelles}} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{\dim V_v^+} \left(\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)\right)^{\dim V_v^-}$$

où V_v^+, V_v^- sont définis pour une place infinie v réelle de la façon suivante : à chaque place w de L au-dessus de v, on fait correspondre un groupe de décomposition défini par $G(w) = \{g \in G \mid \rho(g)(w) = w\}$ d'ordre 1 ou 2. Le générateur σ_w de $G(w)$ est défini à conjugaison près par v (σ_w correspond à la conjugaison complexe s'il est d'ordre 2). On décompose V en somme directe $V = V_v^+ \oplus V_v^-$ où V_v^+ (respectivement V_v^-) correspond à la valeur propre $+1$ (respectivement -1) de $\rho(\sigma_w)$: $V_v^+ = \{x \in V \mid \rho(\sigma_w)(x) = x\}$ et $V_v^- = \{x \in V \mid \rho(\sigma_w)(x) = -x\}$. En fait, $\dim V_v^+ = \dim V^{<\sigma_w>} = \frac{1}{2}(d + \chi(\sigma_w))$ (voir la proposition B.2.7) et donc $\dim V_v^- = \frac{1}{2}(d - \chi(\sigma_w))$ (puisque $\dim V_v^- = \dim V - \dim V_v^+$).

Remarque 1.2.18. On peut aussi écrire :

$$\gamma_\chi(s) = \prod_{v \text{ complexes}} \pi^{-sd-\frac{d}{2}} \left(\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\right)^d$$
$$\times \prod_{v \text{ réelles}} \pi^{-\frac{sd}{2}+\frac{\chi(\sigma_w)-d}{4}} \left(\Gamma\left(\frac{s}{2}\right)\right)^{\dim V_v^+} \left(\Gamma\left(\frac{s+1}{2}\right)\right)^{\dim V_v^-}.$$

THÉORÈME 1.2.19 (Équation fonctionnelle)**.** *Soit $\Lambda(s,\chi)$ la fonction L complétée définie par $\Lambda(s,\chi) = q(\chi)^{s/2}\gamma_\chi(s)L(s,\chi,L/K)$ dans le demi-plan ouvert vertical $\mathrm{Re}(s) > 1$, où le conducteur $q(\chi)$ de $\Lambda(s,\chi)$ correspond à $q(\chi) = |\mathrm{disc}\ K|^{\chi(1)}\mathrm{N}_{K/\mathbb{Q}}(f(\chi))$. Alors $\Lambda(s,\chi)$ admet un prolongement méromorphe sur $\mathbb{C}$ et vérifie l'équation fonctionnelle*

$$\Lambda(1-s,\chi) = W(\chi)\Lambda\left(s,\overline{\chi}\right),$$

où $W(\chi)$ est de module 1 et $\overline{\chi}$ le caractère de la représentation duale de V.

Remarque 1.2.20. D'après la proposition B.2.12, le caractère $\overline{\chi}$ est simplement le conjugué complexe de χ.

Remarques 1.2.21. De la même façon que dans le cas de fonctions L génériques, nous déduisons de l'équation fonctionnelle des propriétés sur le comportement de la fonction L d'Artin.
Par définition, la fonction L complétée n'a ni pôle ni zéro pour les complexes de partie réelle strictement supérieure à 1. L'équation fonctionnelle nous permet d'en déduire qu'il en est de même pour les complexes de partie réelle strictement inférieure à 0. On constate que les pôles de partie réelle strictement négative du prolongement du facteur gamma doivent être compensés par des zéros de la fonction L d'Artin : les zéros triviaux de $L(s,\chi)$ sont donc situés en $s = -2m \neq 0$ et/ou (selon l'écriture du facteur gamma) $s = -2m-1$ pour $m \in \mathbb{N}$. Ainsi, les seuls pôles et zéros que la fonction complétée peut avoir se situent dans la bande $0 \leqslant \mathrm{Re}(s) \leqslant 1$. Et comme le facteur gamma a seulement un pôle éventuel en $s = 0$ (et pas de zéro) dans cette partie du plan complexe, la fonction L complétée a donc les mêmes pôles et zéros que sa fonction L d'Artin associée sur la partie du plan complexe $\mathrm{Re}(s) > 0$.
Comme nous l'avons déjà remarqué dans la partie définissant les fonctions L générales, l'équation fonctionnelle donne l'égalité entre l'ordre du pôle de $\Lambda(s,\chi)$ en $s = 1$ et en $s = 0$. Celui-ci correspond également à l'ordre du pôle de $L(s,\chi)$ en $s = 1$.

Notons que sous la conjecture d'Artin, la fonction L complétée est méromorphe avec des pôles en $s = 0$ et $s = 1$ d'ordre égal au nombre de fois où intervient le caractère trivial dans la décomposition de χ en caractères irréductibles. En particulier, on a équivalence entre l'analyticité des fonctions $L(s,\chi)$ et $\Lambda(s,\chi)$. Dans le cas où la fonction L d'Artin

est entière, elle possède éventuellement un zéro en $s = 0$ (compensant le pôle potentiel du facteur gamma).

Conjecturalement, les fonctions L d'Artin se retrouvent donc bien dans le cadre des fonction L.

Propriété 1.2.22. *Si $p \mid q(\chi) = |\text{disc } K|^{\chi(1)} \mathrm{N}_{K/\mathbb{Q}}(f(\chi))$ alors p est ramifié dans $L/\mathbb{Q}$.*

<u>Preuve</u>
En effet, $p \mid q(\chi)$ implique deux cas : soit p divise le discriminant de K et donc p est ramifié dans $K/\mathbb{Q}$, a fortiori dans $L/\mathbb{Q}$; soit p divise la norme de $f(\chi)$ et alors il existe un idéal premier $\mathfrak{p}$ de K au-dessus de p tel que $f_{\mathfrak{p}}(\chi) \neq 0$ d'où $\mathfrak{p}$ est ramifié dans L/K. $\square$

Notons que la réciproque est fausse. En effet, prenons l'exemple où L est le corps de décomposition du polynôme $x^3 - 2$ et $K = \mathbb{Q}$. Alors le groupe de Galois de $L/\mathbb{Q}$ est isomorphe au groupe diédral d'ordre 6. Il possède donc deux représentations de degré 1 et une de degré 2. Intéressons-nous à la représentation (χ, V) de degré 1 non triviale : elle est triviale sur le sous-groupe $\mathbb{Z}/3\mathbb{Z}$. Les seuls premiers ramifiés sont 2 et 3. On peut calculer (en utilisant le logiciel PARI/GP ([PAR15]) par exemple) que le degré de ramification de 2 vaut 3 donc le groupe d'inertie I_2 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Ainsi, $V^{G_0} = V^{I_2} = V$. De plus, G_1 est trivial d'après le corollaire 4.6.5 de [MR04] donc $f_2(\chi) = 0$ et 2 ne divise pas $f(\chi) = q(\chi)$.

Propriété 1.2.23. *On a $q(\overline{\chi}) = q(\chi)$ et $\gamma_{\overline{\chi}}(s) = \gamma_{\chi}(s)$.*

<u>Preuve</u>
Les notations utilisées dans cette démonstration sont celles de la partie B.2.3.
Par définition, $q(\overline{\chi}) = |\text{disc } K|^{\overline{\chi}(1)} \mathrm{N}(f(\overline{\chi}))$. Puisque $\overline{\chi}(1) = \dim(V^*) = \dim V = \chi(1)$, il reste à montrer que $f(\overline{\chi}) = f(\chi)$.
Rappelons que : $f(\overline{\chi}) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{f_{\mathfrak{p}}(\overline{\chi})}$ avec $f_{\mathfrak{p}}(\overline{\chi}) = \sum_{i=0}^{+\infty} \frac{|G_i|}{|G_0|} \text{codim}\,(V^*)^{G_i}$.
Puisque $\text{codim}\,(V^*)^{G_i} = \dim V^* - \dim\,(V^*)^{G_i} = \dim V - \dim\,(V^*)^{G_i}$, il nous faut montrer que $\dim\,(V^*)^{G_i} = \dim\,(V)^{G_i}$. Rappelons $(V^*)^{G_i} = \{f \in V^* \,:\, \forall\, g \in G_i,\, \overline{\rho}(g)(f) = f\}$.
Pour tout i, on peut décomposer V sous la forme $V^{G_i} \oplus W$. Soit $(e_1, \ldots, e_n)$ une base adaptée de V telle que $(e_1, \ldots, e_m)$ $(m \leqslant n)$ soit une base de V^{G_i}. Soit $(e_1^*, \ldots, e_n^*)$ la base de V^* associée. De cette façon, pour tout $g \in G_i$, pour $i \in [\![1, m]\!]$, $\rho(g)(e_i) = e_i$ et pour $i \in [\![m+1, n]\!]$, $\rho(g)(e_i) \in \text{Vect}(e_{m+1}, \cdots, e_n)$. En effet, supposons par l'absurde qu'il existe $i \in [\![m+1, n]\!]$ tel que $\rho(g)(e_i) = \sum_{k=1}^{n} \alpha_k e_k$. En composant par $\rho(g^{-1})$, on obtient :
$e_i = \sum_{k=1}^{m} \alpha_k e_k + \sum_{k=m+1}^{n} \alpha_k \rho(g^{-1})(e_k)$ donc $\alpha_k = 0$ pour $k \in [\![1, m]\!]$.
D'une part, en restreignant à V^{G_i} les éléments de $(V^*)^{G_i}$, on obtient des éléments de $(V^{G_i})^*$. Donc $\dim(V^*)^{G_i} \leqslant \dim(V^{G_i})^*$.
D'autre part, pour tout $i \in [\![1, m]\!]$, on prolonge l'élément e_i^* de la base de $(V^{G_i})^*$ en posant $e_i^*(e_j) = 0$ pour $j \in [\![m+1, n]\!]$. Il reste à vérifier que $e_i^* \in (V^*)^{G_i}$: soit $j \in [\![1, n]\!]$

et $g \in G_i$,

$$\begin{aligned}
\overline{\rho}(g)(e_i^*)(e_j) &= e_i^*(\rho(g^{-1})e_j) \\
&= \begin{cases} e_i^*(e_j) & \text{si } j \in [\![1,m]\!] \\ e_i^*\left(\sum_{k=m+1}^{n} \alpha_k e_k\right) & \text{si } j \in [\![m+1,n]\!] \end{cases} \\
&= \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases} \\
&= e_i^*(e_j)
\end{aligned}$$

donc $\overline{\rho}(g)(e_i^*) = e_i^*$.
Par ailleurs, concernant le facteur gamma, on a

$$\begin{aligned}
\gamma_{\overline{\chi}}(s) = &\prod_{v \text{ complexes}} \left(\pi^{-s-1/2}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\right)^{\chi(1)} \\
&\times \prod_{v \text{ réelles}} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{\dim(V^*)_v^+} \left(\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)\right)^{\dim(V^*)_v^-},
\end{aligned}$$

où $\dim(V^*)_v^+ = \frac{1}{2}\left(\overline{\chi(1)} + \overline{\chi(\sigma_w)}\right)$ et $\dim(V^*)_v^- = \frac{1}{2}\left(\overline{\chi(1)} - \overline{\chi(\sigma_w)}\right)$, par définition de $\overline{\chi}$. Et puisque $\overline{\chi}(1) \in \mathbb{N}^*$, on obtient $\overline{\chi(1)} = \chi(1)$. Par ailleurs, $\overline{\chi(\sigma_w)} = \chi(\sigma_w^{-1}) = \mathrm{tr}(\rho(\sigma_w)^{-1})$ et $\rho(\sigma_w)^{-1} = \rho(\sigma_w)$ car σ_w est d'ordre 2, donc $\overline{\chi(\sigma_w)} = \chi(\sigma_w)$.
Ainsi, $\dim(V^*)_v^+ = \dim V_v^+$ et $\dim(V^*)_v^- = \dim V_v^-$ donc $\gamma_{\overline{\chi}}(s) = \gamma_\chi(s)$. □

Propriété 1.2.24. *D'après l'équation fonctionnelle $\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\overline{\chi})$ et la propriété précédente, on peut écrire*

$$\gamma_\chi(s) = \left[\pi^{-sd}\left(\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\right)^d\right]^{r_2} \times \left[\pi^{-sd/2}\prod_{j=1}^{d}\Gamma\left(\frac{s+\lambda_j}{2}\right)\right]^{r_1}$$

où $\lambda_j \in \{0,1\}$ et (r_1,r_2) est la signature du corps de nombres K : r_1 (respectivement r_2) représente le nombre de places réelles (respectivement complexes) donc $r_1+2r_2 = [K:\mathbb{Q}]$. Autrement dit,

$$\gamma_\chi(s) = \pi^{-sd[K:\mathbb{Q}]/2}\prod_{j=1}^{d[K:\mathbb{Q}]}\Gamma\left(\frac{s+\kappa_j}{2}\right),$$

avec $\kappa_j \in \{0,1\}$. Les fonctions L d'Artin vérifient donc la conjecture de Ramanujan-Petersson à l'infini.

Remarque 1.2.25. Notons que le degré sur K de la fonction L d'Artin $L(s,\chi,L/K)$ correspond au degré de la représentation ρ, noté $\deg(\rho)$ tandis que son degré sur $\mathbb{Q}$ est $\deg(\rho)[K:\mathbb{Q}]$. En particulier, on a la majoration : $\chi(1)[K:\mathbb{Q}] \leqslant \ln \mathfrak{q}(\chi)$.

1.2.3 Convolution de Rankin-Selberg

Dans le cadre de fonctions L d'Artin, la convolution de Rankin-Selberg correspond au produit tensoriel des représentations associées. Cependant, pour garder une cohérence avec la définition générale, nous gardons la même notation pour la convolution entre deux caractères.
Pour deux fonctions L d'Artin $L(s, \chi_{V_1})$ et $L(s, \chi_{V_2})$ de représentations associées (ρ_{V_1}, V_1) et (ρ_{V_2}, V_2), la convolution de Rankin-Selberg correspond à la fonction L d'Artin

$$L(s, \chi_{V_1} \otimes \chi_{V_2}) = L(s, \chi_{V_1 \otimes V_2}) = L(s, \chi_{V_1}\chi_{V_2}).$$

Plus précisément, si on écrit les fonctions sous la forme

$$L(s, \chi_{V_1}) = \prod_{\mathfrak{p} \subset \mathscr{O}_K} \prod_{i=1}^{d} \left(1 - \frac{\alpha_{i,\rho_1}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1} \text{ et } L(s, \chi_{V_2}) = \prod_{\mathfrak{p} \subset \mathscr{O}_K} \prod_{j=1}^{e} \left(1 - \frac{\beta_{j,\rho_2}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1}$$

alors $L(s, \chi_{V_1} \otimes \chi_{V_2}) = \prod_{\mathfrak{p} \subset \mathscr{O}_K} \prod_{i=1}^{d} \prod_{j=1}^{e} \left(1 - \alpha_{i,\rho_1}(\mathfrak{p})\beta_{j,\rho_2}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}\right)^{-1}$.

Proposition 1.2.26. *Sous la conjecture d'Artin, avec les notations précédentes, lorsque les caractères χ_{V_1} et χ_{V_2} sont irréductibles, la fonction L d'Artin $L(s, \chi_{V_1} \otimes \chi_{V_2})$ se prolonge analytiquement sur $\mathbb{C}$ sauf en $s = 1$ où elle possède un pôle simple si et seulement si V_2 est isomorphe à V_1^* si et seulement si $\chi_{V_2} = \overline{\chi_{V_1}}$.*

Preuve
Vérifions que la représentation triviale apparaît dans la décomposition de $V_1 \otimes V_2$ si et seulement si ρ_{V_1} est isomorphe à $\rho_{V_2^*}$. Nous cherchons donc à montrer que $\langle \chi_{V_1 \otimes V_2}, \mathbf{1}_G \rangle = 1$ si $V_2 \simeq V_1^*$ et 0 sinon. Grâce à la proposition B.2.12, on a :

$$\langle \chi_{V_1 \otimes V_2}, \mathbf{1}_G \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{V_1}(g)\chi_{V_2}(g) = \frac{1}{|G|} \sum_{g \in G} \chi_{V_2}(g)\overline{\chi_{V_1^*}(g)} = \langle \chi_{V_2}, \chi_{V_1^*} \rangle.$$

La proposition B.2.1 permet alors de conclure :

$$\langle \chi_{V_1 \otimes V_2}, \mathbf{1}_G \rangle = \begin{cases} 1 & \text{si } V_2 \simeq V_1^* \\ 0 & \text{sinon} \end{cases}.$$

□

Remarque 1.2.27. Notons que sous la conjecture d'Artin, pour des caractères χ et χ' quelconques, on a l'égalité $r(\chi \otimes \overline{\chi'}) = \langle \chi, \chi' \rangle$.

Propriétés 1.2.28. *Les résultats énoncés sur la convolution de Rankin-Selberg dans un cadre général sont encore valables pour les fonctions L d'Artin :*

$$f(\chi_{V_1} \otimes \chi_{V_2}) \mid f(\chi_{V_1})^e f(\chi_{V_2})^d$$
$$q(\chi_{V_1} \otimes \chi_{V_2}) \mid q(\chi_{V_1})^e q(\chi_{V_2})^d$$
$$\mathfrak{q}(s, \chi_{V_1} \otimes \chi_{V_2}) \leqslant \mathfrak{q}(s, \chi_{V_1})^e \mathfrak{q}(s, \chi_{V_2})^d.$$

PREUVE

Par définition et puisque $\deg(\chi_{V_1} \otimes \chi_{V_2}) = \deg(\chi_{V_1})\deg(\chi_{V_2})$, on a :

$$q(\chi_{V_1} \otimes \chi_{V_2}) = |\text{disc } K|^{\deg(\chi_{V_1}\otimes\chi_{V_2})}\mathrm{N}_{K/\mathbb{Q}}(f(\chi_{V_1} \otimes \chi_{V_2})) = |\text{disc } K|^{de}\mathrm{N}_{K/\mathbb{Q}}(f(\chi_{V_1} \otimes \chi_{V_2})).$$

Montrons que $\mathrm{N}_{K/\mathbb{Q}}(f(\chi_{V_1\otimes V_2})) \mid \mathrm{N}^e_{K/\mathbb{Q}}(f(\chi_{V_1}))\mathrm{N}^d_{K/\mathbb{Q}}(f(\chi_{V_2}))$.
La définition d'un conducteur d'Artin donne :

$$f(\chi_{V_1} \otimes \chi_{V_2}) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\sum_{i=0}^{\infty} \operatorname{codim}(V_1\otimes V_2)^{G_i} \frac{|G_i|}{|G_0|}}.$$

En utilisant $\begin{array}{ll} \rho_{V_1\otimes V_2} : \mathrm{Gal}(L/K) & \to \mathrm{GL}(V_1 \otimes V_2) \\ \sigma & \mapsto \rho_{V_1\otimes V_2}(\sigma) : x_1x_2 \mapsto \rho_{V_1}(\sigma)(x_1)\rho_{V_2}(\sigma)(x_2) \end{array}$, on a :

$$\begin{aligned}(V_1 \otimes V_2)^{G_i} &= \left\{x_1x_2 \in V_1 \otimes V_2 \,|\, \forall\, g \in G_i,\ (\rho_{V_1\otimes V_2})(g)(x_1x_2) = x_1x_2\right\} \\ &= \{x_1x_2 \in V_1 \otimes V_2 \,|\, \forall\, g \in G_i,\ \rho_{V_1}(g)(x_1)\rho_{V_2}(g)(x_2) = x_1x_2\} \\ &= V_1^{G_i} \otimes V_2^{G_i}.\end{aligned}$$

En notant $d = \dim V_1$, $e = \dim V_2$, $s = \dim V_1^{G_i} \leqslant d$ et $t = \dim V_2^{G_i} \leqslant e$, on obtient alors :

$$\begin{aligned}\operatorname{codim}(V_1 \otimes V_2)^{G_i} &= \dim V_1 \otimes V_2 - \dim(V_1 \otimes V_2)^{G_i} = \dim V_1 \otimes V_2 - \dim V_1^{G_i} \dim V_2^{G_i} \\ &= de - st \\ \operatorname{codim} V_1^{G_i} &= \dim V_1 - \dim V_1^{G_i} \\ &= d - s \\ \operatorname{codim} V_2^{G_i} &= \dim V_2 - \dim V_2^{G_i} \\ &= e - t.\end{aligned}$$

Puisque $e + t \leqslant 2e$ et que :

$$\begin{aligned} e + t \leqslant 2e &\Leftrightarrow (e + t)(d - s) \leqslant 2e(d - s) \\ &\Leftrightarrow (e + t)(d - s) + se - dt \leqslant 2ed - 2es + se - dt \\ &\Leftrightarrow de - st \leqslant ed - se + ed - dt \\ &\Leftrightarrow de - st \leqslant e(d - s) + d(e - t) \\ &\Leftrightarrow \operatorname{codim}(V_1 \otimes V_2)^{G_i} \leqslant e \operatorname{codim} V_1^{G_i} + d \operatorname{codim} V_2^{G_i},\end{aligned}$$

on a :

$$\begin{aligned} f(\chi_{V_1} \otimes \chi_{V_2}) &= \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\sum_{i=0}^{\infty} \operatorname{codim}(V_1\otimes V_2)^{G_i} \frac{|G_i|}{|G_0|}} \mid \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\sum_{i=0}^{\infty} (e \operatorname{codim} V_1^{G_i} + d \operatorname{codim} V_2^{G_i}) \frac{|G_i|}{|G_0|}} \\ &\mid \left(\prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\sum_{i=0}^{\infty} \operatorname{codim} V_1^{G_i} \frac{|G_i|}{|G_0|}}\right)^e \left(\prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\sum_{i=0}^{\infty} \operatorname{codim} V_2^{G_i}) \frac{|G_i|}{|G_0|}}\right)^d \\ &\mid f(\chi_{V_1})^e f(\chi_{V_2})^d \end{aligned}$$

donc

$$\mathrm{N}_{K/\mathbb{Q}}(f(\chi_{V_1} \otimes \chi_{V_2})) \mid \mathrm{N}^e_{K/\mathbb{Q}}(f(\chi_{V_1}))\mathrm{N}^d_{K/\mathbb{Q}}(f(\chi_{V_2})).$$

Finalement,

$$q(\chi_{V_1} \otimes \chi_{V_2}) \mid |\text{disc } K|^{de} \mathrm{N}^e_{K/\mathbb{Q}}(f(\chi_{V_1}))\mathrm{N}^d_{K/\mathbb{Q}}(f(\chi_{V_2})) \mid q(\chi_{V_1})^e q(\chi_{V_2})^d.$$

En notant κ_i (respectivement μ_j ; ν_k) les paramètres locaux à l'infini de la fonction L d'Artin $L(s, \chi_{V_1} \otimes \chi_{V_2})$ (respectivement $L(s, \chi_{V_1})$; $L(s, \chi_{V_2})$), on en déduit :

$$\begin{aligned}
\mathfrak{q}(s, \chi_{V_1} \otimes \chi_{V_2}) &= q(\chi_{V_1 \otimes V_2}) \prod_{i=1}^{de[K:\mathbb{Q}]} \big(|s + \kappa_i| + 3\big) \\
&\leqslant q(\chi_{V_1})^e q(\chi_{V_2})^d \big(|s| + 4\big)^{de[K:\mathbb{Q}]} && \text{car } \kappa_i \in \{0, 1\} \\
&\leqslant q(\chi_{V_1})^e q(\chi_{V_2})^d \big((|s| + 3)^2\big)^{de[K:\mathbb{Q}]} && \text{car } |s| + 4 \leqslant 6|s| + 9 \leqslant |s|^2 + 6|s| + 9 \\
&\leqslant q(\chi_{V_1})^e q(\chi_{V_2})^d \prod_{i=1}^{d[K:\mathbb{Q}]} \big(|s + \mu_i| + 3\big)^e \prod_{i=1}^{e[K:\mathbb{Q}]} \big(|s + \nu_i| + 3\big)^d \\
&\leqslant \Big(q(\chi_{V_1}) \prod_{i=1}^{d[K:\mathbb{Q}]} \big(|s + \mu_i| + 3\big)\Big)^e \Big(q(\chi_{V_2}) \prod_{i=1}^{e[K:\mathbb{Q}]} \big(|s + \nu_i| + 3\big)\Big)^d \\
&= \mathfrak{q}(s, \chi_{V_1})^e \mathfrak{q}(s, \chi_{V_2})^d.
\end{aligned}$$

□

Remarque 1.2.29. Notons que dans la preuve nous avons en fait démontré :

$$f_{\mathfrak{p}}(\chi_{V_1} \otimes \chi_{V_2}) \leqslant e f_{\mathfrak{p}}(\chi_{V_1}) + d f_{\mathfrak{p}}(\chi_{V_2}),$$

pour tout idéal premier $\mathfrak{p}$ de K.

1.2.4 Aspects explicites dans le cas $K = \mathbb{Q}$

Dans le cas où le corps de base est $\mathbb{Q}$, en gardant les mêmes notations, la fonction L d'Artin s'écrit comme un produit sur les nombres premiers :

$$L(s, \chi, L/\mathbb{Q}) = \sum_{n \geqslant 1} \frac{a_\chi(n)}{n^s} = \prod_{p \in \mathbb{Z}} \frac{1}{\det(\mathrm{Id} - p^{-s}\sigma_p; V^{I_p})} = \prod_{p \in \mathbb{Z}} \prod_{i=1}^{d} \big(1 - \alpha_{i,\rho}(p) p^{-s}\big)^{-1}.$$

1.2.4.1 Aspects explicites

Nous utilisons le logiciel PARI/GP ([PAR15]) pour créer un programme donnant les coefficients de la série de Dirichlet ou les paramètres locaux d'une fonction L d'Artin. Les détails de ce programme sont donnés dans le chapitre annexe A.

Soit P un polynôme à coefficients rationnels définissant un corps de nombres L galoisien au-dessus de $\mathbb{Q}$. On note $G = \mathrm{Gal}(L/\mathbb{Q})$ et ρ la représentation du groupe G, de caractère χ, pour laquelle nous cherchons la fonction L d'Artin $L(s, \chi, L/K)$.

Intéressons-nous concrètement, sur un exemple, à trouver les paramètres locaux d'une fonction L d'Artin. Soit P le polynôme $\mathbb{Q}$-irréductible de degré 12, $P = x^{12} - 24x^{10} + 120x^8 - 206x^6 + 120x^4 - 24x^2 + 1$ (trouvé dans la base des polynômes galoisiens de PARI/GP), définissant un corps de nombres dont le groupe de Galois est le groupe diédral d'ordre 12.

En général, la fonction *galoisinit* calcule le groupe de Galois associé à un polynôme $\mathbb{Q}$-irréductible de degré inférieur à 36 et la fonction *galoisexport* permet d'obtenir la structure du groupe de Galois adaptée à GAP ([GAP15]). Ensuite, grâce à la commande $IrreducibleRepresentations$, GAP renvoie l'image des générateurs du groupe par les différentes représentations.

Si on connaît le déterminant définissant le produit eulérien de la fonction L d'Artin alors, à travers la fonction *direuler*, PARI/GP nous renvoie les coefficients de la série de Dirichlet attachée, autrement dit les coefficients $a_\chi(n)$.
Nous cherchons donc à calculer ce déterminant. En notant φ_p un représentant dans D_p du Frobenius σ_p engendrant D_p/I_p, on a $\rho(\varphi_p) \in \mathrm{GL}(V^{I_p})$ donc le déterminant de la définition $\det(\mathrm{Id} - p^{-s}\sigma_p; V^{I_p})$ correspond au déterminant de la matrice $\rho(\varphi_p)$ valant 0 en dehors de V^{I_p}.
Lorsque le nombre premier p est non ramifié, autrement dit lorsqu'il ne divise pas le discriminant du corps de nombres considéré, $V^{I_p} = V$. Dans ce cas, il nous suffit de trouver le Frobenius. Celui-ci est donné dans PARI/GP par $idealfrobenius$.
Dans notre exemple, les premiers ramifiés sont 2, 3 et 31 (on peut les trouver en utilisant $factor(nfinit(P).disc)$).
Pour le premier 7 non ramifié, on obtient $\sigma_7(x) = -\frac{11}{8}x^{11} + \frac{65}{2}x^9 - \frac{613}{4}x^7 + \frac{1833}{8}x^5 - 89x^3 + \frac{41}{4}x$ (en utilisant *galoispermtopol* pour obtenir cette écriture) ou bien, vu comme une permutation des racines, $\sigma_7 = (1, 10, 11, 12, 3, 2)(4, 8, 6, 9, 5, 7)$. Cette dernière écriture permet d'utiliser GAP pour obtenir l'image du Frobenius par la représentation : par exemple, pour la 5e représentation (au sens de GAP),

$$\rho_5(\sigma_7) = \begin{pmatrix} \mathrm{e}^{\frac{2i\pi}{3}} & 0 \\ 0 & \mathrm{e}^{\frac{4i\pi}{3}} \end{pmatrix}.$$

Pour un nombre premier ramifié, on revient à la définition de l'automorphisme de Frobenius et, en utilisant le programme $frobram$ (voir partie A.2 pour les détails), on a : $\sigma_2(x) = \frac{-3}{2}x^{11} + \frac{71}{2}x^9 - \frac{1345}{8}x^7 + 252x^5 - 92x^3 + \frac{11}{8}x$ ou $\sigma_2 = (1, 7)(2, 4)(3, 8)(5, 10)(6, 12)(9, 11)$. D'où

$$\rho_5(\sigma_2) = \begin{pmatrix} 0 & \mathrm{e}^{\frac{2i\pi}{3}} \\ \mathrm{e}^{\frac{4i\pi}{3}} & 0 \end{pmatrix}.$$

De même, $\sigma_3 = \mathrm{Id}$ et $\sigma_{31} = \sigma_2$. Ensuite, on doit connaître

$$V^{I_p} = \{v = (v_1, v_2) \in \mathbb{C}^2 \ : \ \forall\, \mathrm{i} \in I_p,\ \rho_5(\mathrm{i})(v) = v\}$$

afin de restreindre la matrice.
Notons i_p^j le j^e générateur du groupe I_p. Le groupe d'inertie est donné par la commande *idealramgroups* dans PARI/GP :

$$\begin{aligned} I_2 &= \mathrm{Vect}((1, 12)(2, 11)(3, 10)(4, 9)(5, 8)(6, 7)) \\ I_3 &= \mathrm{Vect}((1, 11, 3)(2, 10, 12)(4, 6, 5)(7, 8, 9), (1, 9)(2, 5)(3, 7)(4, 12)(6, 10)(8, 11)) \\ I_{31} &= \mathrm{Vect}((1, 6)(2, 9)(3, 5)(4, 11)(7, 12)(8, 10)) \end{aligned}$$

et $\rho_5(\mathrm{i}_2^1) = \mathrm{Id}$, $\rho_5(\mathrm{i}_3^1) = \begin{pmatrix} \mathrm{e}^{\frac{4i\pi}{3}} & 0 \\ 0 & \mathrm{e}^{\frac{2i\pi}{3}} \end{pmatrix}$, $\rho_5(\mathrm{i}_3^2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\rho_5(\mathrm{i}_{31}^1) = \begin{pmatrix} 0 & \mathrm{e}^{\frac{2i\pi}{3}} \\ \mathrm{e}^{\frac{4i\pi}{3}} & 0 \end{pmatrix}$.

On en déduit donc $V^{I_2} = V = \mathbb{C}^2$, $V^{I_3} = \{(0,0)\}$ et $V^{I_{31}} = \mathrm{Vect}((1, \mathrm{e}^{\frac{4i\pi}{3}}))$. Ainsi, on obtient $\det(\mathrm{Id} - X\sigma_2; V^{I_2}) = \det(\mathrm{Id} - X\rho_5(\sigma_2)) = 1 - X^2$, $\det(\mathrm{Id} - X\sigma_3; V^{I_3}) = 1$ et $\det(\mathrm{Id} - X\sigma_{31}; V^{I_{31}}) = \det(\mathrm{Id} - X \begin{pmatrix} 1 & 0 \\ \mathrm{e}^{\frac{4i\pi}{3}} & 0 \end{pmatrix}) = 1 - X$.
On a donc maintenant toutes les informations nécessaires pour obtenir les paramètres locaux de la fonction L d'Artin ou les coefficients : on cherche les racines du déterminant pour obtenir les valeurs propres donc les paramètres locaux et on utilise *direuler* pour obtenir les coefficients de la série de Dirichlet associée au produit eulérien. Par exemple, ici, les 40 premiers coefficients obtenus par le programme sont les suivants :

```
[1, 0, 0, 1, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, 0, 1, -1, 0, -1, 0,

          0, 0, -1, 0, 1, 0, 0, -1, -1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

On remarque que ce ne sont que des réels appartenant à $\{-1, 0, 1\}$ mais si nous allons plus loin, on trouve des coefficients égaux à 2 (par exemple le 53e).

Regardons également quelques paramètres locaux : en $p = 2$, on trouve $\alpha_{1,\rho_5}(2) = -1$ et $\alpha_{2,\rho_5}(2) = 1$; en 3, on a égalité $\alpha_{1,\rho_5}(3) = \alpha_{2,\rho_5}(3) = 0$; $\alpha_{1,\rho_5}(7) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ et $\alpha_{2,\rho_5}(7) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$; $\alpha_{1,\rho_5}(31) = 0$ et $\alpha_{2,\rho_5}(31) = 1$. Ils correspondent bien à ce que nous avons trouvé précédemment.
La proposition 2.3.13 donne le lien entre les coefficients et les paramètres locaux d'une fonction L d'Artin.

Les programmes transcrits dans la partie annexe A généralisent cette méthode à un polynôme quelconque.
De plus, en utilisant les coefficients obtenus et le paquet *ComputeL* créé par Dokchitser [Dok], mis à jour par Pascal Molin, on peut prolonger la fonction L d'Artin (voir partie A.5) et ainsi obtenir les différentes valeurs de $L(s, \chi)$. La partie suivante se sert de cela.
Notons également que Tim et Vladimir Dokchitser, dans l'article [DD10], donnent un critère explicite pour identifier la classe de conjugaison d'un automorphisme de Frobenius et ont permis d'implémenter les fonctions L d'Artin dans Magma ([BCP97]).

1.2.4.2 Exemple numérique sur la somme des zéros

À l'aide du programme que l'on vient de présenter, sous la conjecture d'Artin, on peut obtenir des exemples de calculs du type

$$\sum_{\substack{\rho=\frac{1}{2}+it \\ \text{zéro de } L(s,\chi) \\ |t|\leqslant L}} \frac{1}{|\rho(\rho+1)|}.$$

Ce résultat est utile, notamment puisque nous avons besoin d'en connaître une majoration lorsque l'on veut obtenir une borne pour distinguer deux fonctions L d'Artin, comme nous le verrons dans le chapitre suivant.
Par exemple, toujours en utilisant le logiciel PARI/GP [PAR15], pour le corps défini par le polynôme $\mathbb{Q}$-irréductible $P = x^8 - 4x^7 - 8x^6 + 24x^5 + 30x^4 - 16x^3 - 20x^2 + 2$ et un caractère χ réel de degré 1, on a :

$$\sum_{\substack{\rho=\frac{1}{2}+it \\ \text{zéro de } L(s,\chi)}} \frac{1}{|\rho(\rho+1)|} = \sum_{\substack{\rho=\frac{1}{2}+it \\ \text{zéro de } L(s,\chi) \\ 0\leqslant|t|\leqslant 50}} \frac{1}{|\rho(\rho+1)|} + \sum_{\substack{\rho=\frac{1}{2}+it \\ \text{zéro de } L(s,\chi) \\ 50<|t|}} \frac{1}{|\rho(\rho+1)|}$$
$$\leqslant 0,50 + 0,48 \leqslant 0,98.$$

La première somme est obtenue par le programme : une fois qu'on a prolongé la fonction L d'Artin, on cherche graphiquement (à l'aide de la fonction *solve*) les parties imaginaires des zéros de la fonction. Maintenant, dans la version 2.9 de PARI/GP, on peut utiliser la fonction *lfunzeros* pour obtenir les zéros. La deuxième somme provient de l'application numérique de la remarque 2.3.10 avec $\ell = 50$ et le conducteur vaut ici 28.
En utilisant le théorème 2.3.9, on obtient $\displaystyle\sum_{\substack{\rho=\frac{1}{2}+it \\ \text{zéro de } L(s,\chi)}} \frac{1}{|\rho(\rho+1)|} \leqslant 42$, c'est loin d'être une majoration optimale. La différence entre le résultat théorique et le calcul exact vient principalement des zéros de petite partie imaginaire. Par exemple, en enlevant les zéros de partie imaginaire plus petite que 2,5 (on sait qu'il n'y en a pas), on obtient :

$$\sum_{\substack{\rho=\frac{1}{2}+it \\ |t|\geqslant 2,5}} \frac{1}{|\rho(\rho+1)|} \leqslant 9.$$

1.2.4.3 Corps quadratiques

Pour des corps quadratiques, nous pouvons exprimer explicitement les coefficients et paramètres de la fonction L d'Artin. Les résultats du chapitre suivant nous permettent d'obtenir une borne sur le plus petit non résidu quadratique.

Définition 1.2.30. On note $\left(\frac{a}{p}\right)$ le *symbole de Kronecker* égal au symbole de Legendre pour un entier $a \in \mathbb{Z}$ et un premier $p > 2$:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \\ 1 & \text{si } a \equiv x^2 \bmod p \text{ admet une solution non nulle} \\ -1 & \text{si } a \equiv x^2 \bmod p \text{ n'a pas de solution} \end{cases}$$

et avec la règle suivante pour $p = 2$:

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{si } 2 \mid a \\ 1 & \text{si } a \equiv \pm 1 \bmod 8 \\ -1 & \text{si } a \equiv \pm 3 \bmod 8 \end{cases}.$$

On étend cette définition à un entier positif n impair avec le *symbole de Jacobi* : si $n = \displaystyle\prod_{i=1}^{k} p_i^{\alpha_i}$ est la décomposition de n en facteurs premiers alors

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}.$$

Pour $n \in \mathbb{N}^*$, on dit que a est un *résidu quadratique modulo* n s'il existe $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \equiv x^2$ modulo n. Remarquons que tout entier est un résidu quadratique modulo 2 et que pour un nombre premier $p > 2$, a est un résidu quadratique modulo p est équivalent à $\left(\frac{a}{p}\right) = 1$.

Proposition 1.2.31. *Soit $L = \mathbb{Q}(\sqrt{m})$, m un entier sans facteurs carrés. Intéressons-nous à la fonction L d'Artin associée à la représentation ρ non triviale du groupe de Galois de $L/\mathbb{Q}$, de caractère χ. On a :*

$$L(s, \chi, \mathbb{Q}(\sqrt{m})/\mathbb{Q}) = \begin{cases} \displaystyle\prod_{p \in \mathscr{P}} \frac{1}{1 - \left(\frac{m}{p}\right) p^{-s}} & \text{si } m \equiv 1 \bmod 4 \\ \displaystyle\prod_{p \in \mathscr{P} \setminus \{2\}} \frac{1}{1 - \left(\frac{m}{p}\right) p^{-s}} & \text{si } m \equiv 2 \text{ ou } 3 \bmod 4 \end{cases},$$

où $\left(\frac{a}{p}\right)$ désigne le symbole de Kronecker entre a et p.

<u>Preuve</u>
On note $P(x) = x^2 - m$ le polynôme associé à l'extension L. Le groupe de Galois G associé à $L/\mathbb{Q}$ est d'ordre 2, il contient l'identité et l'application σ qui envoie $\sqrt{m}$ sur $-\sqrt{m}$. Les nombres premiers ramifiés sont les premiers divisant le discriminant de L. On rappelle que le discriminant de L vaut m si m est congru à 1 modulo 4 et $4m$ si m est congru à 2 ou 3 modulo 4. Lorsque m est congru à 1 ou 2 modulo 4, ils correspondent donc exactement aux premiers divisant l'entier m. Alors que si m est congru à 3 modulo 4, les premiers ramifiés sont 2 et les premiers divisant l'entier m.
Intéressons-nous à la fonction L d'Artin associée à la représentation ρ non triviale : on a $\rho(e_G) = 1$ et $\rho(\sigma) = -1$.
Pour p un premier ramifié, on a $|I_p| = 2$ (puisque c'est l'indice de ramification) donc $I_p = G$ et alors $V^{I_p} = \{0\}$. Ainsi $\det(\mathrm{Id} - p^{-s}\sigma_p; V^{I_p}) = 1$.
Pour un premier p non ramifié, $D_p =< \sigma_p >$ donc pour déterminer $1 - p^{-s}\rho(\sigma_p)$, il suffit de connaître D_p. Ceci revient à trouver le degré résiduel associé au premier p. Pour ce faire, mettons à part le cas $p = 2$ et utilisons la factorisation de P modulo p (on peut utiliser cette méthode puisque $p \nmid \operatorname{disc} L$) et le symbole de Legendre :

$$\begin{aligned} \overline{P} &= x^2 - \overline{m} \mod p \\ &= \begin{cases} (x-n)(x+n) & \text{si } m \equiv n^2 \bmod p \\ x^2 - \overline{m} & \text{si } m \text{ n'est pas un carré modulo } p \end{cases} \\ &= \begin{cases} (x-n)(x+n) & \text{si } \left(\frac{m}{p}\right) = 1 \\ x^2 - \overline{m} & \text{si } \left(\frac{m}{p}\right) = -1 \end{cases}. \end{aligned}$$

Dans le cas $p = 2$ lorsque 2 n'est pas ramifié, c'est-à-dire lorsque $m \equiv 1 \bmod 4$, on utilise le polynôme minimal de $\frac{\sqrt{m}+1}{2}$: $Q(x) = x^2 - x + \frac{1-m}{4} \in \mathbb{Z}[x]$. Et modulo 2, sa réduction donne $x(x + \overline{1})$ si $m \equiv 1 \bmod 8$ et $x^2 + x + \overline{1}$, qui est $\mathbb{Q}$-irréductible, si $m \equiv 5 \bmod 8$.
Le degré d'inertie vaut donc 1 lorsque $\left(\frac{m}{p}\right) = 1$ (ici, c'est le symbole de Kronecker qu'on utilise) et 2 sinon. Dans le premier cas, cela signifie que $D_p = \{e_G\}$ donc on a l'égalité $1 - p^{-s}\rho(\sigma_p) = 1 - p^{-s}$, sinon $D_p = G$ donc $\sigma_p = \sigma$ et $1 - p^{-s}\rho(\sigma_p) = 1 + p^{-s}$. D'où le résultat. □

PROPOSITION 1.2.32. *Pour un nombre m congru à 1 modulo 4 sans facteurs carrés, si on suppose vraies l'hypothèse de Riemann généralisée et la conjecture d'Artin alors le plus petit nombre premier p tel que $\left(\frac{m}{p}\right) = -1$ est majoré par $4,4 \cdot 10^7 \ln^2(12m)$. Notons qu'un tel p est nécessairement un non résidu quadratique modulo m.*

On peut comparer cette borne à celle donnée par [Ank52] en $\ln^2(m)$ pour un nombre premier m ou encore Bach démontre que le plus petit non résidu quadratique est inférieur à $2\ln^2(m)$ pour tout entier m sous l'hypothèse de Riemann (théorème 2 dans [Bac90]). Notons que la constante $4,4 \cdot 10^7$ obtenue ci-dessus provient du théorème 2.3.2 qui s'applique à une fonction L d'Artin générale, on ne peut donc pas espérer "rivaliser" avec la constante donnée par Bach. D'autre part, un théorème dû à Chowla (voir par exemple [Ank52]) montre qu'il y a une infinité de nombres premiers p pour lesquels le plus petit non résidu quadratique modulo p est $\gg \ln p$.

Afin de démontrer cette proposition, on commence par le lemme suivant.

Lemme 1.2.33. *Dans l'extension quadratique $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ avec m sans facteurs carrés, le conducteur associé au caractère χ non trivial du groupe de Galois associé vaut :*

$$q(\chi) = \begin{cases} \text{disc } \mathbb{Q}(\sqrt{m}) & \textit{si } m \equiv 1 \textit{ ou } 3 \bmod 4 \\ 2m & \textit{si } m \equiv 2 \bmod 4. \end{cases}$$

PREUVE

Ici, on a $q(\chi) = f(\chi) = \prod_p p^{f_p(\chi)}$. Pour obtenir le conducteur analytique, il faut connaître les groupes de ramification pour les premiers p ramifiés. On a déjà rappelé que lorsque m est congru à 1 ou 2 modulo 4, ils correspondent exactement aux premiers divisant l'entier m. Alors que si m est congru à 3 modulo 4, les premiers ramifiés sont 2 et les premiers divisant l'entier m.

Soit p un nombre premier ramifié. On sait que $G_0 = I_p = G$ (puisque $I_p \subset G$ et $|I_p| = 2$) donc $V^{G_0} = \{0\}$. Et ensuite, le corollaire 4.6.5 de [MR04] nous permet de conclure que G_1 est trivial pour $p \neq 2$ donc $V^{G_1} = V$. Si $p = 2$ est ramifié, on a G_1 non trivial donc $G_1 = G$. Ensuite, on utilise le fait que $G_1/G_2 = G/G_2$ est un groupe abélien d'exposant 2 (voir [Neu99] page 177), autrement dit G/G_2 est isomorphe à G, on en déduit que G_2 est trivial d'où $V^{G_2} = V$. En résumé,

$$f_p(\chi) = \begin{cases} 0 & \text{si } p \text{ n'est pas ramifié} \\ 1 & \text{si } p \text{ est ramifié et } p \neq 2 \\ 2 & \text{si } p = 2 \text{ est ramifié} \end{cases}$$

donc

$$q(\chi) = \begin{cases} m & \text{si } m \equiv 1 \bmod 4 \\ 2m & \text{si } m \equiv 2 \bmod 4 \\ 4m & \text{si } m \equiv 3 \bmod 4 \end{cases} = \begin{cases} \text{disc } \mathbb{Q}(\sqrt{m}) & \text{si } m \equiv 1 \text{ ou } 3 \bmod 4 \\ \frac{\text{disc } \mathbb{Q}(\sqrt{m})}{2} & \text{si } m \equiv 2 \bmod 4. \end{cases}$$

□

PREUVE DE LA PROPOSITION 1.2.32

On se place dans l'extension quadratique $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ et on applique le corollaire 2.3.1 aux deux caractères de degré 1 du groupe de Galois G associé. Posons $\chi_1 = \mathbf{1}$ le caractère trivial et $\chi_2 = \chi$ le caractère irréductible non trivial. Alors, d'après les propriétés d'une fonction L d'Artin, $L(s, \chi_1) = \zeta(s) = \prod_p (1 - p^{-s})^{-1}$ et on trouve l'écriture de $L(s, \chi)$ dans la proposition 1.2.31 précédente.

Afin d'appliquer le corollaire 2.3.1, on a besoin de connaître les conducteurs. Pour le caractère trivial, d'après le résultat 1.2.14, on sait que $q(\mathbf{1}) = f(\mathbf{1})\mathrm{disc}\ \mathbb{Q} = 1$. De plus, d'après la définition 1.2.17, l'espace vectoriel V^+ est de dimension 1 (ici, il n'y a qu'une seule place infinie réelle) et donc le paramètre local à l'infini vaut 0. Ainsi, $\mathfrak{q}(\mathbf{1}) = \mathfrak{q}_\infty(\mathbf{1}) = 3$. Concernant χ_2, puisque $m \equiv 1 \bmod 4$, le lemme 1.2.33 précédent donne $q(\chi) = m$ et donc $\mathfrak{q}(\chi) \leqslant 4m$ (selon la valeur du paramètre local à l'infini).

Finalement, en appliquant le corollaire 2.3.1, on sait qu'il existe un nombre premier ne divisant pas m tel que $\left(\frac{m}{p}\right) \neq 1$ vérifiant $p \leqslant C \ln^2(12m)$ où la constante C peut être écrite sous la forme $C = \frac{51}{25}\left(86D_{0,\phi} + 2D_{1,\phi} + \frac{5}{2}D_{3,\phi}\omega\big(q(\chi_1)q(\chi_2)\big)/\ln\big(q(\chi_1)q(\chi_2)\big)\right)^2$, $\omega(n)$ désigne la fonction additive dénombrant le nombre total des facteurs premiers de n et ϕ est une fonction positive non nulle, $\mathscr{C}^\infty$ à support compact dans $[1,2]$. En faisant un choix pour la fonction ϕ, par exemple, $\phi(x) = \exp\left(\frac{-0,3}{(x-1)(2-x)}\right)$ sur $]1,2[$ et nulle ailleurs, et puisque $\frac{\omega(m)}{\ln m} \leqslant 1,5$ on obtient $C \leqslant 4,4 \cdot 10^7$.
Par ailleurs, puisque $p \nmid m$, $\left(\frac{m}{p}\right) \neq 1$ est équivalent à $\left(\frac{m}{p}\right) = -1$.
Le dernier point vient du fait qu'en supposant $p \neq 2$, on a $\left(\frac{m}{p}\right) = (-1)^{\frac{p-1}{2}\frac{m-1}{2}}\left(\frac{p}{m}\right)$ (voir [Coh07a] page 36), d'où $-1 = \left(\frac{m}{p}\right) = \left(\frac{p}{m}\right)$ car m est congru à 1 modulo 4. Et par décomposition de m en facteurs premiers $m = \prod_i q_i$ (les puissances valent 1 puisqu'on a supposé m sans facteurs carrés), on obtient l'existence d'un nombre premier q_0 divisant m tel que $-1 = \left(\frac{p}{q_0}\right)$. Ainsi, p n'est pas un carré modulo q_0 donc p ne peut pas être un carré modulo m. □

Remarque 1.2.34. Notons que dans le cas $m \equiv 3 \bmod 4$, l'entier -1 n'est pas un résidu quadratique modulo m (puisque les carrés sont congrus à 0 ou 1 modulo 4).

Chapitre 2

Majoration explicite du nombre de paramètres locaux suffisants pour déterminer une fonction L

On cherche à connaître le nombre de paramètres locaux suffisants pour déterminer une fonction L. Un théorème de [IK04] (ici c'est le théorème 2.1.1) répond à cette question, sous certaines conditions, en permettant de distinguer deux fonctions L générales en considérant leurs paramètres locaux pour tous les premiers jusqu'à une certaine borne théorique. Nous explicitons ce théorème dans le cadre général de fonctions L : le résultat est donné dans le théorème 2.1.2. Ensuite, nous adaptons ce théorème aux fonctions L d'Artin et de formes modulaires primitives. Nous verrons que, dans ce cas, la borne peut être améliorée grâce à la connaissance des invariants. La partie essentielle de ce chapitre fait l'objet d'une publication au Journal de Théorie des Nombres de Bordeaux et se trouve dans l'article [Euv].

2.1 Théorème pour une fonction L générale

Le résultat suivant est dû à H. Iwaniec et E. Kowalski :

Théorème 2.1.1 ([IK04], Proposition 5.22)**.** *Soit $L(s,f)$ et $L(s,g)$ deux fonctions L distinctes de même degré d. Supposons que $L(s,f\otimes\bar{f})$ et $L(s,f\otimes\bar{g})$ existent et que cette dernière soit entière. Supposons, de plus, que GRH soit vraie pour ces deux fonctions L et que les paramètres locaux de $L(s,f\otimes\bar{f})$ et $L(s,f\otimes\bar{g})$ aux premiers divisant $q(f)q(g)$ soient de module inférieur à 1. Alors il existe un nombre premier $p\leqslant C\left(d\ln\mathfrak{q}(f)\,\mathfrak{q}(g)\right)^2$ ne divisant pas $q(f)q(g)$ tel que les paramètres locaux de $L(s,f)$ et $L(s,g)$ en p sont différents, avec C une constante absolue.*

Remarquons que l'ordre du pôle n'apparaît pas dans la preuve donnée dans [IK04]. Notons également que dans la preuve que nous donnons, nous n'avons pas besoin de supposer l'égalité des facteurs gamma. La condition sur le module des paramètres locaux peut être remplacée par l'hypothèse plus forte de Ramanujan-Petersson.

Nous avons rendu explicite cette constante C :

Théorème 2.1.2. *Le théorème 2.1.1 est vérifié avec :*

$$C = 2\cdot 10^8.$$

PREUVE

Cette constante a été obtenue grâce à la version plus précise donnée par le théorème 2.1.3 suivant en utilisant une fonction ϕ particulière choisie dans la classe des fonctions $\phi_{D,a,b}$, $D > 0$ et $1 \leqslant a < b \leqslant 2$, définies par $\phi_{D,a,b}(x) = \exp\left(\frac{-D}{(x-a)(b-x)}\right)$ sur $]1,2[$ et nulles ailleurs. Dans cette classe, une recherche rapide des meilleurs constantes D, a et b montre que le choix $D = 3/10$, $a = 1$ et $b = 2$ n'est pas loin d'être optimal et donne :

$$\|\phi\|_1 \geqslant 0,17 \ ; \ D_{0,\phi} \leqslant 53,5 \ ; \ D_{1,\phi} \leqslant 0,68 \ ; \ D_{2,\phi} \leqslant 3085 \ \text{ et } \ D_{3,\phi} \leqslant 1,75.$$

Par ailleurs, dans le théorème 2.1.3, quitte à majorer 1 par $r(f \otimes \bar{f})$, on peut négliger l'ordre du pôle. □

THÉORÈME 2.1.3. *On note ϕ une fonction positive non nulle, $\mathscr{C}^\infty$ à support compact dans $[1,2]$. Dans le théorème 2.1.1, on peut prendre :*

$$C = \frac{51}{25\big(r(f\otimes\bar{f})\big)^2}\left(2D_{1,\phi}+3D_{2,\phi}+\frac{754}{75}D_{0,\phi}r(f\otimes\bar{f})+\frac{5}{2}D_{3,\phi}\omega'\big(q(f)q(g)\big)\right)^2,$$

où

$$\omega'(n) = \begin{cases} \frac{\omega(n)}{\ln n} & si\ n \geqslant 2 \\ 0 & si\ n = 1 \end{cases},$$

avec $\omega(n)$, définie sur $\mathbb{N}^*$, désignant la fonction additive dénombrant le nombre total des facteurs premiers de n,

$$\begin{aligned} D_{0,\phi} &:= \frac{C_{0,\phi}}{\|\phi\|_1} = \frac{1}{\|\phi\|_1}\int_1^2 |\phi''(x)|x^{3/2}\,\mathrm{d}x \\ D_{1,\phi} &:= \frac{C_{1,\phi}}{\|\phi\|_1} = \frac{1}{\|\phi\|_1}\int_1^2 \frac{\phi(x)}{x}\,\mathrm{d}x \\ D_{2,\phi} &:= \frac{C_{2,\phi}}{\|\phi\|_1} = \Big(\frac{46}{4\pi}+\frac{27053}{500}\Big)D_{0,\phi} \\ D_{3,\phi} &:= \frac{\|\phi\|_\infty}{\|\phi\|_1}. \end{aligned}$$

Remarques 2.1.4. Une étude classique de $\omega(n)$ (voir par exemple [Rob83] page 380) permet d'obtenir une borne pour $n \geqslant 3$:

$$\omega'(n) \leqslant \frac{1,38402}{\ln(\ln n)}.$$

En fait, $\omega'(n) \leqslant 3/2$ pour $n \geqslant 1$ (on utilise la majoration précédente pour $n \geqslant 13$).
Notons que l'on peut majorer $C_{0,\phi}$ et $C_{1,\phi}$ en faisant intervenir des normes infinies :

$$\begin{aligned} D_{0,\phi} &\leqslant \frac{\|\phi''\|_\infty}{\|\phi\|_1}\frac{2(2^{5/2}-1)}{5} \\ D_{1,\phi} &\leqslant \frac{\|\phi\|_\infty}{\|\phi\|_1}\ln 2. \end{aligned}$$

2.2 Preuve du théorème 2.1.3

Considérons deux fonctions L distinctes, $L(s,f)$ et $L(s,g)$, de même degré d telles que $L(s,f\otimes\bar{f})$ et $L(s,f\otimes\bar{g})$ existent. On note ϕ une fonction positive non nulle, $\mathscr{C}^\infty$ à support compact dans $[1,2]$. On définit le réel $X\geqslant 1$ de façon à ce que les paramètres locaux de $L(s,f)$ et $L(s,g)$ coïncident pour tous les nombres premiers p inférieurs ou égaux à $2X$ ne divisant pas $q(f)q(g)$. Nous cherchons à majorer X.
Par hypothèse, $L(s,f\otimes\bar{f})$ est méromorphe avec un pôle d'ordre $r(f\otimes\bar{f})\geqslant 1$ en $s=1$ et la fonction $L(s,f\otimes\bar{g})$ est entière.

Dans toute la suite, la lettre h sera utilisée pour remplacer f ou g lorsque le résultat est indépendant de la fonction considérée.

La propriété suivante est une conséquence de la définition du réel X.

Propriété 2.2.1. *Si les paramètres locaux de $L(s,f)$ et $L(s,g)$ coïncident pour tous les nombres premiers $p\leqslant 2X$ ne divisant pas $q(f)q(g)$ alors $\Lambda_{f\otimes\bar{f}}(n)=\Lambda_{f\otimes\bar{g}}(n)$ pour tout entier $n\leqslant 2X$ premier à $q(f)q(g)$.*

<u>Preuve</u>
La définition 1.1.8 de la convolution de Rankin-Selberg, ainsi que la définition de la fonction duale, permettent d'écrire : pour $i\in[\![1,d^2]\!]$, il existe j et $k\in[\![1,d]\!]$ tels que $\alpha_{i,f\otimes\bar{h}}(p)=\alpha_{j,f}(p)\alpha_{k,\bar{h}}(p)=\alpha_{j,f}(p)\overline{\alpha_{k,h}(p)}$ pour $p\nmid q(f)q(\bar{h})=q(f)q(h)$. Ici, on suppose $\alpha_{k,f}(p)=\alpha_{k,g}(p)$ pour $p\leqslant 2X$ ne divisant pas $q(f)q(g)$ donc $\alpha_{i,f\otimes\bar{f}}(p)=\alpha_{i,f\otimes\bar{g}}(p)$ pour $p\leqslant 2X$ tels que $p\nmid q(f)q(g)$. D'après la définition 1.1.3, on a :

$$\Lambda_{f\otimes\bar{h}}(n)=\begin{cases}\displaystyle\sum_{i=1}^{d^2}\alpha_{i,f\otimes\bar{h}}(p)^\ell\ln p & \text{si } n=p^\ell\\ 0 & \text{sinon}\end{cases}.$$

Pour $n\leqslant 2X$ vérifiant $(n,q(f)q(g))=1$, deux cas se présentent :
• soit n n'est pas une puissance d'un nombre premier, alors $\Lambda_{f\otimes\bar{f}}(n)=0=\Lambda_{f\otimes\bar{g}}(n)$;
• soit $n=p^\ell$, alors $p\leqslant 2X$ et $(n,q(f)q(g))=1$ revient à dire que p ne divise pas $q(f)q(g)$, on a donc $\Lambda_{f\otimes\bar{f}}(n)=\sum_{i=1}^{d^2}\alpha_{i,f\otimes\bar{f}}(p)^\ell\ln p=\sum_{i=1}^{d^2}\alpha_{i,f\otimes\bar{g}}(p)^\ell\ln p=\Lambda_{f\otimes\bar{g}}(n)$. □

2.2.1 Formule explicite

On adapte la formule explicite donnée dans le théorème 5.11 de [IK04] afin d'obtenir le résultat suivant :

Théorème 2.2.2 (Formule explicite). *Soit ϕ une fonction positive non nulle, $\mathscr{C}^\infty$ à support compact dans $[1,2]$ et $\hat{\phi}(s)=\int_1^2\phi(x)x^{s-1}\,\mathrm{d}x$ sa transformée de Mellin. Soit $L(s,f)$ une fonction L. Alors on a :*

$$\sum_{n\leqslant 2X}\Lambda_f(n)\phi\left(\frac{n}{X}\right)=\frac{1}{2i\pi}\int_{\frac12-i\infty}^{\frac12+i\infty}\left(\frac{\gamma_f'}{\gamma_f}(s)+\frac{\gamma_f'}{\gamma_f}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s$$
$$+\|\phi\|_1 r(f)X-\sum_{\substack{\rho\text{ zéro de}\\ L(s,f)}}X^\rho\hat{\phi}(\rho),$$

où $\|\phi\|_1=\int_1^2\phi(x)\,\mathrm{d}x>0$, $r(f)$ correspond à l'ordre du pôle de $L(s,f)$ en $s=1$ et la somme porte sur les zéros, comptés avec multiplicité, de $L(s,f)$ dans la bande critique $0\leqslant\mathrm{Re}(\rho)\leqslant 1$.

On utilise cette formule explicite pour obtenir les majorations suivantes que nous démontrerons dans la partie 2.2.4.

THÉORÈME 2.2.3. *En supposant GRH vérifiée pour les deux fonctions $L(s, f \otimes \bar{f})$ et $L(s, f \otimes \bar{g})$, on a :*

$$\begin{aligned}\Big|\sum_n \Lambda_{f\otimes\bar{f}}(n)\phi\left(\frac{n}{X}\right) - r(f\otimes\bar{f})\,\|\phi\|_1 X\Big| &\leqslant C_{1,\phi}d(f\otimes\bar{f}) \\ &\quad + C_{2,\phi}\ln\mathfrak{q}(f\otimes\bar{f})\sqrt{X} + \frac{754}{75}C_{0,\phi}r(f\otimes\bar{f})\sqrt{X} \\ \Big|\sum_n \Lambda_{f\otimes\bar{g}}(n)\phi\left(\frac{n}{X}\right)\Big| &\leqslant C_{1,\phi}d(f\otimes\bar{g}) + C_{2,\phi}\ln\mathfrak{q}(f\otimes\bar{g})\sqrt{X},\end{aligned}$$

où $C_{0,\phi}$, $C_{1,\phi}$ et $C_{2,\phi}$ sont données au théorème 2.1.3.

Ce sont $C_{0,\phi}$, $C_{1,\phi}$ et $C_{2,\phi}$ qui nous permettront finalement de démontrer le théorème 2.1.3, en notant que $d(f\otimes\bar{f}) = d(f\otimes\bar{g}) = d^2$.

2.2.2 Conséquences du théorème 2.2.3

Dans cette partie, en admettant le théorème 2.2.3 démontré dans la partie 2.2.4, nous obtenons une majoration de $\sqrt{X}$ qui nous permet de démontrer le théorème 2.1.3.
D'abord, nous simplifions l'énoncé du théorème 2.2.3 avec les notations :

$$\begin{aligned}M &= r(f\otimes\bar{f})\,\|\phi\|_1 X \\ E_1 &= C_{1,\phi}d(f\otimes\bar{f}) + C_{2,\phi}\sqrt{X}\ln\mathfrak{q}(f\otimes\bar{f}) + \frac{754}{75}C_{0,\phi}\sqrt{X}r(f\otimes\bar{f}) \\ E_2 &= C_{1,\phi}d(f\otimes\bar{g}) + C_{2,\phi}\sqrt{X}\ln\mathfrak{q}(f\otimes\bar{g}) \\ a(h) &= \sum_n \Lambda_{f\otimes\bar{h}}(n)\phi\left(\frac{n}{X}\right).\end{aligned}$$

Nous avons donc : $|M - a(f)| \leqslant E_1$ et $|a(g)| \leqslant E_2$.
Pour majorer X, on cherche donc à majorer M. L'inégalité triangulaire donnant :

$$0 \leqslant M \leqslant |M - a(f)| + |a(f) - a(g)| + |a(g)| \leqslant E_1 + E_2 + |a(f) - a(g)|,$$

il reste alors à majorer la différence $|a(f) - a(g)|$.

Lemme 2.2.4. *En supposant que les paramètres locaux des fonctions L, $L(s, f\otimes\bar{f})$ et $L(s, f\otimes\bar{g})$, aux premiers divisant $q(f)q(g)$ sont de module inférieur à 1, on a :*

$$\left|\sum_n \Lambda_{f\otimes\bar{f}}(n)\phi\left(\frac{n}{X}\right) - \sum_n \Lambda_{f\otimes\bar{g}}(n)\phi\left(\frac{n}{X}\right)\right| \leqslant 2\,\|\phi\|_\infty\, d^2 \ln\big(q(f)q(g)\big)\ln(2X)\omega'\big(q(f)q(g)\big),$$

où $\omega'(n)$ est donné au théorème 2.1.3.

<u>PREUVE</u>

L'égalité suivante résulte de la propriété 2.2.1 :

$$\begin{aligned}
&\left|\sum_n \Lambda_{f\otimes\bar{f}}(n)\phi\left(\frac{n}{X}\right) - \sum_n \Lambda_{f\otimes\bar{g}}(n)\phi\left(\frac{n}{X}\right)\right| \\
&\quad = \left|\sum_{\substack{n\leqslant 2X\\(n,q(f)q(g))\neq 1}} \Lambda_{f\otimes\bar{f}}(n)\phi\left(\frac{n}{X}\right) - \sum_{\substack{n\leqslant 2X\\(n,q(f)q(g))\neq 1}} \Lambda_{f\otimes\bar{g}}(n)\phi\left(\frac{n}{X}\right)\right| \\
&\quad \leqslant \|\phi\|_\infty \sum_{\substack{n\leqslant 2X\\(n,q(f)q(g))\neq 1}} \left(\left|\Lambda_{f\otimes\bar{f}}(n)\right| + \left|\Lambda_{f\otimes\bar{g}}(n)\right|\right). \qquad (2.1)
\end{aligned}$$

Pour $n \leqslant 2X$ vérifiant $(n, q(f)q(g)) \neq 1$, on a :

$$\begin{aligned}
\left|\Lambda_{f\otimes\bar{h}}(n)\right| &\leqslant \begin{cases} \displaystyle\sum_{j=1}^{d^2} |\alpha_{j,f\otimes\bar{h}}|^k \ln(p) & \text{si } n = p^k \\ 0 & \text{sinon} \end{cases} \\
&\leqslant \begin{cases} d^2\ln(p) & \text{si } n = p^k \\ 0 & \text{sinon} \end{cases} \left(\begin{array}{l}\text{d'après l'hypothèse sur les paramètres} \\ \text{locaux en } p \mid q(f)q(g)\end{array}\right)
\end{aligned}$$

donc

$$\begin{aligned}
\sum_{\substack{n\leqslant 2X\\(n,q(f)q(g))\neq 1}} \left(\left|\Lambda_{f\otimes\bar{f}}(n)\right| + \left|\Lambda_{f\otimes\bar{g}}(n)\right|\right) &\leqslant 2d^2 \sum_{p\mid q(f)q(g)} \ln(p) \sum_{\substack{k\in\mathbb{N}\\p^k\leqslant 2X}} 1 \\
&\leqslant 2d^2 \sum_{p\mid q(f)q(g)} \ln(p)\ \mathrm{card}\left\{k\in\mathbb{N} : p^k \leqslant 2X\right\} \\
&\leqslant 2d^2 \sum_{p\mid q(f)q(g)} \ln(p)\frac{\ln(2X)}{\ln p} \\
&\leqslant 2d^2 \ln(2X)\omega\big(q(f)q(g)\big),
\end{aligned}$$

d'où le résultat souhaité avec l'inégalité (2.1). □

On en déduit alors le résultat suivant :

Proposition 2.2.5. *Avec les notations précédentes et en supposant vraie GRH pour les fonctions $L(s, f\otimes\bar{f})$ et $L(s, f\otimes\bar{g})$ et que les paramètres locaux de $L(s, f\otimes\bar{f})$ et $L(s, f\otimes\bar{g})$ aux premiers divisant $q(f)q(g)$ sont de module inférieur à 1, on a :*

$$\begin{aligned}
\sqrt{X} \leqslant \frac{1}{r(f\otimes\bar{f})\,\|\phi\|_1}\Bigg(&C_{2,\phi}\big(\ln\mathfrak{q}(f\otimes\bar{f}) + \ln\mathfrak{q}(f\otimes\bar{g})\big) + \frac{754}{75}C_{0,\phi}r(f\otimes\bar{f}) \\
&+ 2d^2\Big(\frac{\ln(2X)}{\sqrt{X}}\ln\big(q(f)q(g)\big)\,\|\phi\|_\infty\,\omega'\big(q(f)q(g)\big) + C_{1,\phi}\Big)\Bigg),
\end{aligned}$$

où $C_{0,\phi}$, $C_{1,\phi}$, $C_{2,\phi}$ et $\omega'(n)$ sont définis au théorème 2.1.3.

2.2.3 Fin de la preuve du théorème 2.1.3

À l'aide du résultat précédent et des majorations suivantes $q(h) \leqslant \mathfrak{q}(h)$, $\mathfrak{q}(f\otimes\bar{f}) \leqslant \mathfrak{q}(f)^{2d}$, $\mathfrak{q}(f\otimes\bar{g}) \leqslant (\mathfrak{q}(f)\mathfrak{q}(g))^d$ et $d \leqslant \ln\big(\mathfrak{q}(f)\mathfrak{q}(g)\big)$, on obtient :

$$\begin{aligned}\sqrt{X} &\leqslant \frac{d\ln\big(\mathfrak{q}(f)\mathfrak{q}(g)\big)}{r(f\otimes\bar{f})\,\|\phi\|_1}\left(3C_{2,\phi}+\frac{754}{75}C_{0,\phi}r(f\otimes\bar{f})+2\Big(d\frac{\ln(2X)}{\sqrt{X}}\,\|\phi\|_\infty\,\omega'\big(q(f)q(g)\big)+C_{1,\phi}\Big)\right)\\ &\leqslant \frac{d\ln\big(\mathfrak{q}(f)\mathfrak{q}(g)\big)}{r(f\otimes\bar{f})}\left(3D_{2,\phi}+\frac{754}{75}D_{0,\phi}r(f\otimes\bar{f})+2\Big(d\frac{\ln(2X)}{\sqrt{X}}D_{3,\phi}\omega'\big(q(f)q(g)\big)+D_{1,\phi}\Big)\right)\end{aligned}$$

Deux cas se présentent alors :
- si $\sqrt{X} \leqslant d\ln(\mathfrak{q}(f)\mathfrak{q}(g))$, nous avons le résultat avec $C=1$;
- sinon $X \geqslant d^2\ln^2(\mathfrak{q}(f)\mathfrak{q}(g)) \geqslant 4$ (car $\mathfrak{q}(h) \geqslant 3$). Puisque la fonction $y \mapsto \frac{\ln(2y)}{\sqrt{y}}$ est décroissante pour $y \geqslant 4$ et $d \leqslant \frac{1}{2}\ln(\mathfrak{q}(f)\mathfrak{q}(g))$ (en effet, d'après les propriétés 1.1.7, $\mathfrak{q}(f)\mathfrak{q}(g) \geqslant 3^{2d}q(f)q(g) \geqslant \mathrm{e}^{2d}$), on a :

$$\frac{\ln(2X)}{\sqrt{X}} \leqslant \frac{\ln\big(2d^2\ln^2(\mathfrak{q}(f)\mathfrak{q}(g))\big)}{d\ln(\mathfrak{q}(f)\mathfrak{q}(g))} \leqslant \frac{4\ln\big(2^{-1/4}\ln(\mathfrak{q}(f)\mathfrak{q}(g))\big)}{d\ln(\mathfrak{q}(f)\mathfrak{q}(g))} \leqslant \frac{4\cdot 2^{-1/4}\cdot\mathrm{e}^{-1}}{d} \leqslant \frac{5}{4d},$$

car pour tout $y>0$, on a $\frac{\ln\left(2^{-1/4}y\right)}{y} \leqslant 2^{-1/4}\mathrm{e}^{-1}$. Ainsi,

$$\sqrt{X} \leqslant \frac{d\ln(\mathfrak{q}(f)\mathfrak{q}(g))}{r(f\otimes\bar{f})}\left(3D_{2,\phi}+2D_{1,\phi}+\frac{754}{75}D_{0,\phi}r(f\otimes\bar{f})+\frac{5}{2}D_{3,\phi}\omega'\big(q(f)q(g)\big)\right).$$

2.2.4 Preuve du théorème 2.2.3

Nous cherchons à majorer chaque terme de la formule explicite du théorème 2.2.2 appliquée aux fonctions $L(s,f\otimes\bar{f})$ et $L(s,f\otimes\bar{g})$:

$$\begin{aligned}\sum_{n\leqslant 2X}\Lambda_{f\otimes\bar{f}}(n)\phi\left(\frac{n}{X}\right) &= r(f\otimes\bar{f})\,\|\phi\|_1\,X - \sum_{\substack{\rho \text{ zéro de}\\ L(f\otimes\bar{f},s)}} X^\rho\hat{\phi}(\rho)\\ &+\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma'_{f\otimes\bar{f}}}{\gamma_{f\otimes\bar{f}}}(s)+\frac{\gamma'_{f\otimes\bar{f}}}{\gamma_{f\otimes\bar{f}}}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s\end{aligned} \tag{1}$$

et puisque $L(s,f\otimes\bar{g})$ n'a pas de pôle en $s=1$, autrement dit $r(f\otimes\bar{g})=0$, on obtient :

$$\begin{aligned}\sum_{n\leqslant 2X}\Lambda_{f\otimes\bar{g}}(n)\phi\left(\frac{n}{X}\right) &= -\sum_{\substack{\rho \text{ zéro de}\\ L(f\otimes\bar{g},s)}} X^\rho\hat{\phi}(\rho)\\ &+\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma'_{f\otimes\bar{g}}}{\gamma_{f\otimes\bar{g}}}(s)+\frac{\gamma'_{f\otimes\bar{g}}}{\gamma_{f\otimes\bar{g}}}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s,\end{aligned} \tag{2}$$

où la somme porte sur les zéros ρ de $L(s,f\otimes\bar{h})$ tels que $0\leqslant \mathrm{Re}(\rho)\leqslant 1$.

Les fonctions $L(s,f\otimes\bar{f})$ et $L(s,f\otimes\bar{g})$ sont des fonctions L (voir la définition de la partie 1.1.2), nous pouvons donc énoncer les propriétés dans le cadre de fonctions L génériques. Dans les paragraphes 2.2.4.1 à 2.2.4.4, nous n'utiliserons que les propriétés générales pour les invariants des fonctions L, notamment pour les paramètres κ_j. Ainsi, nous notons $L(s,f)$ une fonction L générique que nous spécifierons en $L(s,f\otimes\bar{f})$ et $L(s,f\otimes\bar{g})$ quand cela sera nécessaire pour notre étude.

2.2.4.1 Préliminaires

Les résultats suivants nous seront utiles dans les différentes majorations à considérer.

Lemme 2.2.6. *Pour $s = \sigma + it \in \mathbb{C}\backslash\mathbb{R}_-$, on a :*

$$\left|\hat{\phi}(s)\right| \leqslant \frac{C_\phi(\sigma)}{|s(s+1)|} \text{ avec } C_\phi(\sigma) := \int_1^2 |\phi''(x)| x^{\sigma+1}\,\mathrm{d}x.$$

<u>Preuve</u>
En effet, en exprimant $\hat{\phi}$ en fonction de ϕ'' grâce à une double intégration par parties, on a :

$$\begin{aligned}
\hat{\phi}(s) &= \int_1^2 \phi(x) x^{s-1}\,\mathrm{d}x \\
&= \left[\phi(x)\frac{x^s}{s}\right]_1^2 - \frac{1}{s}\int_1^2 \phi'(x)x^s\,\mathrm{d}x = -\frac{1}{s}\int_1^2 \phi'(x)x^s\,\mathrm{d}x \\
&= -\frac{1}{s}\left(\left[\phi'(x)\frac{x^{s+1}}{s+1}\right]_1^2 - \frac{1}{s+1}\int_1^2 \phi''(x)x^{s+1}\,\mathrm{d}x\right) \\
&= \frac{1}{s(s+1)}\int_1^2 \phi''(x)x^{s+1}\,\mathrm{d}x.
\end{aligned}$$

□

Nous aurons besoin de contrôler $|(\Gamma'/\Gamma)(s)|$. Pour cela, rappelons le résultat suivant démontré dans la partie B.1.1.

Lemme 2.2.7. *Pour $s \in \mathbb{C}\backslash\mathbb{R}_-$, on a, $B_2(y) = y^2 - y + \frac{1}{6}$ désignant le 2e polynôme de Bernoulli :*

$$\frac{\Gamma'(s)}{\Gamma(s)} = -\frac{1}{s} + \ln(1+s) - \frac{1}{2}\frac{1}{1+s} - \frac{1}{12}\frac{1}{(1+s)^2} + \int_1^{+\infty} B_2(\{t\})\frac{1}{(t+s)^3}\,\mathrm{d}t. \qquad (\dagger)$$

De plus, pour $s \in \mathbb{C}\backslash\mathbb{R}_-$ tel que $\mathrm{Re}(s) \geqslant -1$, on obtient la majoration :

$$\left|\frac{\Gamma'}{\Gamma}(s)\right| \leqslant \frac{\pi}{2} + \frac{1}{12}\frac{1}{(\mathrm{Re}(s)+1)^2} + \frac{1}{|s|} + \frac{1}{2}\frac{1}{|1+s|} + \frac{1}{12}\frac{1}{|1+s|^2} + \ln(|1+s|).$$

2.2.4.2 Majoration de l'intégrale des égalités (1) et (2)

Les résultats précédents nous permettent d'obtenir la majoration souhaitée :

Proposition 2.2.8. *Pour une fonction L quelconque, notée $L(s,f)$, de degré $d = d(f)$, vérifiant les propriétés énoncées dans la section 1.1.1, on a :*

$$\left|\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma_f'}{\gamma_f}(s) + \frac{\gamma_f'}{\gamma_f}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s\right| \leqslant \frac{C_{0,\phi}}{4\pi}\left(39d(f) + 7\ln\mathfrak{q}(f)\right)\sqrt{X},$$

où

$$C_{0,\phi} = \int_1^2 |\phi''(x)| x^{3/2}\,\mathrm{d}x.$$

PREUVE
Nous devons borner en module

$$I = \frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma_f'}{\gamma_f}(s)+\frac{\gamma_f'}{\gamma_f}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s.$$

D'après le lemme 1.1.2, en gardant la notation $A_j(t) = (1/2 + it + \kappa_j)/2$, on obtient :

$$I = \frac{-d\ln\pi}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}X^s\hat{\phi}(s)\,\mathrm{d}s + \frac{1}{2i\pi}\sum_{j=1}^{d}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(A_j(t))\right)X^s\hat{\phi}(s)\,\mathrm{d}s.$$

Puis, en utilisant la transformée inverse de Mellin (voir partie B.1.2, applicable grâce aux bonnes propriétés de la fonction ϕ), on a :

$$I = -d\ln\pi\phi\left(\frac{1}{X}\right) + \frac{\sqrt{X}}{2i\pi}\sum_{j=1}^{d}\int_{-\infty}^{+\infty}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(A_j(t))\right)X^{it}\hat{\phi}\left(\frac{1}{2}+it\right)\,\mathrm{d}t$$

Enfin, puisque ϕ est à support compact dans $[1,2]$ (et $X \geqslant 2$) et d'après le lemme 2.2.6, on obtient :

$$|I| \leqslant \frac{C_{0,\phi}\sqrt{X}}{2\pi}\sum_{j=1}^{d}\int_{\mathbb{R}}\left|\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(A_j(t))\right)\right|\frac{\mathrm{d}t}{\left|\frac{1}{2}+it\right|\left|\frac{3}{2}+it\right|} \quad \text{où } C_{0,\phi} = \int_1^2|\phi''(x)|x^{3/2}\,\mathrm{d}x.$$

Distinguons différents cas [1] :
• Pour les indices j tels que $\mathrm{Re}(\kappa_j) > -1/2$, $A_j(t) \in \mathbb{C}\backslash\mathbb{R}_-$ pour tout $t \in \mathbb{R}$, on peut donc utiliser l'égalité (†) du lemme 2.2.7, on a alors :

$$\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}(A_j(t))\right| \leqslant \frac{\mathrm{Re}\ A_j(t)}{|A_j(t)|^2} + \ln|1+A_j(t)| + \frac{1}{2|1+A_j(t)|} + \frac{1}{12|1+A_j(t)|^2} + \frac{1}{6}\int_1^{+\infty}\frac{\mathrm{d}x}{(x+\mathrm{Re}\ A_j(t))^3}.$$

De plus, on a :

$$|1+A_j(t)| \geqslant \mathrm{Re}(1+A_j(t)) = \frac{5+2\mathrm{Re}\ \kappa_j}{4} \geqslant 1$$

$$\text{et} \qquad \int_1^{+\infty}\frac{\mathrm{d}x}{(x+\mathrm{Re}\ A_j(t))^3} \leqslant \int_1^{+\infty}\frac{\mathrm{d}x}{x^3} = \frac{1}{2}$$

donc :

$$\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}(A_j(t))\right| \leqslant \frac{\mathrm{Re}\ A_j(t)}{|A_j(t)|^2} + \ln|1+A_j(t)| + \frac{1}{2} + \frac{1}{12} + \frac{1}{12}.$$

• Pour les indices j tels que $-1 < \mathrm{Re}(\kappa_j) \leqslant -1/2$, on utilise la formule $\Gamma(z+1) = z\Gamma(z)$ pour obtenir :

$$\frac{\Gamma'}{\Gamma}(z) = \frac{\Gamma'}{\Gamma}(1+z) - \frac{1}{z}.$$

1. Le problème est également traité de la sorte dans [OS11]. Remarquons que dans la classe de Selberg, la situation est plus simple puisque les parties réelles des paramètres locaux sont supposées positives, voir par exemple [KP99].

Ainsi, on peut majorer : $\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}\left(A_j(t)\right)\right| \leqslant \left|\mathrm{Re}\frac{\Gamma'}{\Gamma}\left(1+A_j(t)\right)\right| + \frac{|\mathrm{Re}A_j(t)|}{|A_j(t)|^2}$.
On peut alors appliquer l'égalité (†) du lemme 2.2.7 à $1+A_j(t) \in \mathbb{C}\backslash\mathbb{R}_-$:

$$\begin{aligned}\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}\left(A_j(t)\right)\right| \leqslant \frac{\mathrm{Re}\ (1+A_j(t))}{|1+A_j(t)|^2} + \ln|2+A_j(t)| + \frac{1}{2|2+A_j(t)|} + \frac{1}{12|2+A_j(t)|^2} \\ + \frac{1}{6}\int_1^{+\infty}\frac{\mathrm{d}x}{(x+1+\mathrm{Re}\ A_j(t))^3} + \frac{|\mathrm{Re}\ A_j(t)|}{|A_j(t)|^2}.\end{aligned}$$

Puisque $\frac{\mathrm{Re}(1+A_j(t))}{|1+A_j(t)|^2} \leqslant \frac{1}{|1+A_j(t)|}$, $|2+A_j(t)| \geqslant 7/4$, $|1+A_j(t)| \geqslant 3/4$ et

$$\int_1^{+\infty}\frac{\mathrm{d}x}{(x+1+\mathrm{Re}\ A_j(t))^3} \leqslant \int_1^{+\infty}\frac{\mathrm{d}x}{(x+\frac{3}{4})^3} = \frac{8}{49},$$

on a :

$$\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}\left(A_j(t)\right)\right| \leqslant \ln|2+A_j(t)| + \frac{82}{49} + \frac{|\mathrm{Re}\ A_j(t)|}{|A_j(t)|^2}.$$

Ainsi, dans toutes les situations, nous pouvons majorer de la façon suivante :

$$\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}\left(A_j(t)\right)\right| \leqslant \ln|2+A_j(t)| + \frac{82}{49} + \frac{|\mathrm{Re}\ A_j(t)|}{|A_j(t)|^2}.$$

Grâce à cette inégalité, on a :

$$\begin{aligned}\sum_{j=1}^{d}\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}\left(A_j(t)\right)\right| &\leqslant d\frac{82}{49} + \ln\Big(\prod_{j=1}^{d}|2+A_j(t)|\Big) + \sum_{j=1}^{d}\frac{|\mathrm{Re}\ A_j(t)|}{|A_j(t)|^2} \\ &\leqslant d\frac{82}{49} + \ln\Big(\prod_{j=1}^{d}(2+|s+\kappa_j|)\Big) + \sum_{j=1}^{d}\frac{|\mathrm{Re}\ A_j(t)|}{|A_j(t)|^2} \\ &\leqslant d\frac{82}{49} + \ln\mathfrak{q}_\infty(s,f) + \sum_{j=1}^{d}\frac{|\mathrm{Re}\ A_j(t)|}{|A_j(t)|^2}.\end{aligned}$$

Notons que le cas $\mathrm{Re}(\kappa_j) = -1/2$ donne $\mathrm{Re}\ A_j(t) = 0$.
Ensuite, en utilisant la fonction arctangente, on obtient la majoration suivante :

$$\begin{aligned}\int_{\mathbb{R}}\frac{|\mathrm{Re}\ A_j(t)|}{|A_j(t)|^2}\frac{\mathrm{d}t}{\left|\frac{1}{2}+it\right|\left|\frac{3}{2}+it\right|} &\leqslant \frac{4^2}{3}\int_{\mathbb{R}}\frac{|1+2\mathrm{Re}\ \kappa_j|}{(1+2\mathrm{Re}\ \kappa_j)^2+4(t+\mathrm{Im}\ \kappa_j)^2}\mathrm{d}t \\ &\leqslant \frac{16}{3}\frac{1}{|1+2\mathrm{Re}\ \kappa_j|}\int_{\mathbb{R}}\frac{1}{1+\left(\frac{2(t+\mathrm{Im}\ \kappa_j)}{|1+2\mathrm{Re}\ \kappa_j|}\right)^2}\mathrm{d}t \\ &\leqslant \frac{16}{3}\frac{\pi}{2} = \frac{8\pi}{3}.\end{aligned}$$

Finalement, en majorant $\mathfrak{q}_\infty(s,f)$ par $\mathfrak{q}(f)(|s|+3)^d$ (voir la proposition 1.1.7), on obtient :

$$\begin{aligned}
&\left|\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma_f'}{\gamma_f}(s)+\frac{\gamma_f'}{\gamma_f}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s\right| \\
&\quad\leqslant \frac{C_{0,\phi}\sqrt{X}}{2\pi}\left(\frac{8\pi}{3}d+\int_{\mathbb{R}}\frac{d\left(\frac{82}{49}+\ln(\sqrt{\frac{1}{4}+t^2}+3)\right)+\ln\mathfrak{q}(f)}{\sqrt{\frac{1}{4}+t^2}\sqrt{\frac{9}{4}+t^2}}\,\mathrm{d}t\right) \\
&\quad\leqslant \frac{C_{0,\phi}\sqrt{X}}{2\pi}\left(\frac{39}{2}d+\frac{5}{2}\ln\mathfrak{q}(f)\right) \qquad \text{avec } C_{0,\phi}=\int_1^2|\phi''(x)|x^{3/2}\,\mathrm{d}x.
\end{aligned}$$

□

2.2.4.3 Majoration de la somme $\sum \frac{1}{|\rho(\rho+1)|}$ sur les zéros de $L(s,f)$

Soit $L(s,f)$ une fonction L quelconque vérifiant les propriétés énoncées dans la section 1.1.1 et la conjecture GRH. On cherche à majorer

$$\left|\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0\leqslant \mathrm{Re}(\rho)\leqslant 1}} X^\rho\hat{\phi}(\rho)\right|.$$

La conjecture GRH (incluant l'hypothèse de Riemann) permet d'écrire :

$$\left|\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0\leqslant \mathrm{Re}(\rho)\leqslant 1}} X^\rho\hat{\phi}(\rho)\right| \leqslant \sqrt{X}\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ \mathrm{Re}(\rho)=1/2}}|\hat{\phi}(\rho)|+\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ \mathrm{Re}(\rho)=0}}|\hat{\phi}(\rho)|.$$

Pour ρ de partie réelle nulle, puisque ϕ est une fonction positive à support compact dans $[1,2]$, on a :

$$|\hat{\phi}(\rho)| \leqslant \int_1^2 |x^{\rho-1}\phi(x)|\,\mathrm{d}x = \int_1^2 \frac{\phi(x)}{x}\,\mathrm{d}x =: C_{1,\phi}.$$

D'après GRH, il existe au plus $d(f)$ zéros ρ vérifiant $\mathrm{Re}(\rho)=0$ donc

$$\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ \mathrm{Re}(\rho)=0}}|\hat{\phi}(\rho)| \leqslant C_{1,\phi}d(f).$$

D'autre part, d'après le lemme 2.2.6, on peut écrire :

$$\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ \mathrm{Re}(\rho)=1/2}}|\hat{\phi}(\rho)| \leqslant C_{0,\phi}\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ \mathrm{Re}(\rho)=1/2}}\frac{1}{|\rho(\rho+1)|},$$

ainsi,

$$\left|\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0\leqslant \mathrm{Re}(\rho)\leqslant 1}} X^\rho\hat{\phi}(\rho)\right| \leqslant C_{0,\phi}\sqrt{X}\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ \mathrm{Re}(\rho)=1/2}}\frac{1}{|\rho(\rho+1)|}+C_{1,\phi}d(f),$$

avec $C_{0,\phi}=\int_1^2|\phi''(x)|x^{3/2}\,\mathrm{d}x$ et $C_{1,\phi}=\int_1^2\frac{\phi(x)}{x}\,\mathrm{d}x$.

Nous cherchons alors à majorer la somme $\displaystyle\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ \mathrm{Re}(\rho)=1/2}} \frac{1}{|\rho(\rho+1)|}$. Pour cela, nous avons besoin de résultats préliminaires.

On rappelle que si $L(s,f)$ est une fonction L alors $(s(1-s))^{r(f)}\Lambda(s,f)$ est une fonction entière d'ordre 1 ne s'annulant ni en 0 ni en 1, il existe donc des constantes $a=a(f)$ et $b=b(f)$ telles que

$$(s(1-s))^{r(f)}\Lambda(s,f) = \mathrm{e}^{a+bs}\prod_{\rho\neq 0,1}\left(1-\frac{s}{\rho}\right)\mathrm{e}^{s/\rho},$$

où ρ varie parmi les zéros de $\Lambda(s,f)$ différents de 0 et 1. Notons que sous GRH, la fonction $\Lambda(s,f)$ n'a pas de zéro en 0 et 1. Ensuite, on a

$$-\frac{L'}{L}(s,f) = \frac{1}{2}\ln q(f) + \frac{\gamma_f'}{\gamma_f}(s) - b + \frac{r(f)}{s} + \frac{r(f)}{s-1} - \sum_{\rho\neq 0,1}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right), \qquad (\star)$$

les deux expressions étant normalement convergentes dans les sous-ensembles compacts qui ne contiennent ni pôle ni zéro. La constante $b(f)$ vérifie

$$\mathrm{Re}(b(f)) = -\sum_{\rho\neq 0,1}\mathrm{Re}(\rho^{-1}), \qquad (\star\star)$$

où ρ varie parmi les zéros de $\Lambda(s,f)$ différents de 0 et 1.

Pour T et ℓ des réels positifs, on note $m_\ell(T,f)$ le nombre de zéros de $\Lambda(s,f)$, $\rho = 1/2+it$, tels que $|t-T|\leqslant \ell$ pour une fonction L quelconque vérifiant les propriétés énoncées dans la section 1.1.1. La proposition suivante est une version explicite d'une propriété connue des fonctions L majorant ce réel, on pourra se référer par exemple à la proposition 5.7 de [IK04]. Dans la suite, nous aurons à considérer $\ell = 1/2$.

Proposition 2.2.9. *Sous GRH pour une fonction $L(s,f)$ quelconque, on a :*

$$m_{\frac{1}{2}}(T,f) \leqslant \frac{13}{5}\left(\frac{56}{25}d(f) + \frac{1}{2}\ln q(f) + \frac{1}{2}\ln \mathfrak{q}_\infty(3+iT,f) + \frac{5}{6}r(f)\right).$$

Preuve

Nous adaptons donc la preuve de [IK04] afin de garder les termes plus précis. On pose $s_0 = \sigma + iT$ avec $\sigma > 2$. En passant à la partie réelle dans l'égalité $(\star)$, on obtient :

$$\begin{aligned}-\mathrm{Re}\frac{L'}{L}(s_0,f) = \frac{1}{2}\ln q(f) + \mathrm{Re}\frac{\gamma_f'}{\gamma_f}(s_0) - \mathrm{Re}\ b + r(f)\mathrm{Re}\left(\frac{1}{s_0}+\frac{1}{s_0-1}\right)\\ - \sum_{\substack{\rho \text{ zéro de}\\ \Lambda(s,f)}}\left(\mathrm{Re}\frac{1}{s_0-\rho} + \mathrm{Re}\frac{1}{\rho}\right),\end{aligned}$$

avec ρ variant parmi les zéros de $\Lambda(s,f)$ différents de 0 et 1. On a donc

$$\begin{aligned}\sum_{\substack{\rho \text{ zéro de}\\ \Lambda(s,f)}}\mathrm{Re}\frac{1}{s_0-\rho} &= \mathrm{Re}\frac{L'}{L}(s_0,f) + \frac{1}{2}\ln q(f) + \mathrm{Re}\frac{\gamma_f'}{\gamma_f}(s_0)\\ &\quad + r(f)\left(\frac{\sigma}{\sigma^2+T^2} + \frac{\sigma-1}{(\sigma-1)^2+T^2}\right) - \left(\mathrm{Re}\ b + \sum_{\substack{\rho \text{ zéro de}\\ \Lambda(s,f)}}\mathrm{Re}\frac{1}{\rho}\right).\end{aligned}$$

Grâce à l'égalité ($\star\star$) ci-dessus et puisque $T^2 \geqslant 0$, on en déduit :

$$\sum_{\substack{\rho \text{ zéro de} \\ \Lambda(s,f)}} \mathrm{Re}\frac{1}{s_0-\rho} \leqslant \left|-\frac{L'}{L}(s_0,f)\right| + \frac{1}{2}\ln q(f) + \left|\frac{\gamma_f'}{\gamma_f}(s_0)\right| + r(f)\frac{2\sigma-1}{\sigma(\sigma-1)}.$$

D'abord, puisque $-\dfrac{L'}{L}(s,f) = \displaystyle\sum_{n\geqslant 1}\Lambda_f(n)n^{-s}$ et

$$\begin{aligned}
|\Lambda_f(n)| &\leqslant \begin{cases} \displaystyle\sum_{i=1}^{d}|\alpha_i^k(p)|\ln(p) & \text{si } n=p^k \\ 0 & \text{sinon} \end{cases} \\
&\leqslant \begin{cases} dp^k\ln(p) & \text{si } n=p^k \\ 0 & \text{sinon} \end{cases} \qquad \text{(par définition, } |\alpha_i(p)|<p) \\
&\leqslant \quad dn\Lambda(n),
\end{aligned}$$

$\Lambda(n)$ désignant la fonction "classique" de Von Mangoldt, on a :

$$\left|-\frac{L'}{L}(s_0,f)\right| \leqslant \sum_{n\geqslant 1}\frac{|\Lambda_f(n)|}{|n^{s_0}|} = \sum_{n\geqslant 1}\frac{|\Lambda_f(n)|}{n^{\sigma}} \leqslant d\sum_{n\geqslant 1}\frac{\Lambda(n)}{n^{\sigma-1}}.$$

Ensuite, puisque $\mathrm{Re}(s_0) > 2$ et $\mathrm{Re}(\kappa_j) > -1$, $\mathrm{Re}\left(\frac{s_0+\kappa_j}{2}\right) > 1/2$, on peut donc appliquer le lemme 2.2.7 :

$$\begin{aligned}
&\left|\frac{\gamma_f'}{\gamma_f}(s_0)\right| \leqslant \frac{d}{2}\ln\pi + \frac{1}{2}\sum_{j=1}^{d}\left|\frac{\Gamma'\left(\frac{s_0+\kappa_j}{2}\right)}{\Gamma\left(\frac{s_0+\kappa_j}{2}\right)}\right| \\
&\leqslant \frac{d}{2}\left(\ln\pi+\frac{\pi}{2}\right) + \frac{1}{2}\sum_{j=1}^{d}\frac{1}{12}\frac{4}{(\mathrm{Re}(s_0+\kappa_j)+2)^2} \\
&\qquad + \frac{1}{2}\sum_{j=1}^{d}\left(\frac{2}{|s_0+\kappa_j|} + \frac{1}{|2+s_0+\kappa_j|} + \frac{1}{3|2+s_0+\kappa_j|^2} + \ln\left(\left|1+\frac{s_0+\kappa_j}{2}\right|\right)\right) \\
&\leqslant \frac{d}{2}\left(\ln\left(\frac{\pi}{2}\right) + \frac{\pi}{2} + \frac{1}{3(\sigma+1)^2} + \frac{2}{\sigma-1} + \frac{1}{\sigma+1} + \frac{1}{3(\sigma+1)^2}\right) \\
&\qquad + \frac{1}{2}\ln\left(\prod_{j=1}^{d}|2+s_0+\kappa_j|\right) \\
&\leqslant \frac{d}{2}\left(\ln\left(\frac{\pi}{2}\right) + \frac{\pi}{2} + \frac{2}{\sigma-1} + \frac{1}{\sigma+1} + \frac{2}{3(\sigma+1)^2}\right) + \frac{1}{2}\ln\mathfrak{q}_\infty(s_0,f).
\end{aligned}$$

En supposant vraie GRH pour $L(s,f)$, on peut écrire :

$$\sum_{\substack{\rho \text{ zéro de} \\ \Lambda(s,f)}} \mathrm{Re}\frac{1}{s_0-\rho} \geqslant \sum_{\substack{\rho=\frac{1}{2}+it \\ |t-T|\leqslant\ell}} \frac{\sigma-\frac{1}{2}}{\left(\sigma-\frac{1}{2}\right)^2+\ell^2} = \frac{\sigma-\frac{1}{2}}{\left(\sigma-\frac{1}{2}\right)^2+\ell^2}m_\ell(T,f).$$

Ainsi,

$$m_\ell(T,f) \leqslant \frac{\left(\sigma-\frac{1}{2}\right)^2+\ell^2}{\sigma-\frac{1}{2}}\left(\frac{d}{2}\left(\ln\left(\frac{\pi}{2}\right)+\frac{\pi}{2}+\frac{2}{\sigma-1}+\frac{1}{\sigma+1}+\frac{2}{3(\sigma+1)^2}\right)\right.$$
$$\left.+\frac{1}{2}\ln\mathfrak{q}_\infty(\sigma+iT,f)+d\sum_{n\geqslant 1}\frac{\Lambda(n)}{n^{\sigma-1}}+\frac{1}{2}\ln q(f)+r(f)\frac{2\sigma-1}{\sigma(\sigma-1)}\right).$$

Grâce à une comparaison numérique, on s'aperçoit que $\sigma=3$ est un bon candidat pour obtenir une majoration quasiment optimale de $m_{\frac{1}{2}}(T,f)$.
Dans ce cas,

$$m_{\frac{1}{2}}(T,f) \leqslant \frac{13}{5}\left(\frac{56}{25}d+\frac{1}{2}\ln q(f)+\frac{1}{2}\ln\mathfrak{q}_\infty(3+iT,f)+\frac{5}{6}r(f)\right).$$

□

Nous pouvons maintenant démontrer le théorème suivant :

Théorème 2.2.10. *En supposant vraie GRH pour la fonction $L(s,f)$, on a :*

$$\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{|\rho(\rho+1)|} \leqslant C(d(f),\mathfrak{q}(f),q(f),r(f)),$$

où

$$C(d,\mathfrak{q},q,r) = \frac{13}{5}\left(\frac{1617}{100}d+\frac{58}{25}\left(\ln\mathfrak{q}+\ln q+\frac{5}{3}r\right)\right).$$

Remarque 2.2.11. En utilisant la majoration $d(f)\leqslant \ln\mathfrak{q}(f)$ des propriétés 1.1.7 et $\ln q(f)\leqslant \ln\mathfrak{q}(f)$, on peut majorer $C(d(f),\mathfrak{q}(f),q(f),r(f))$ par :

$$\frac{27053}{500}\ln\mathfrak{q}(f)+\frac{754}{75}r(f).$$

Preuve
Puisqu'on suppose l'hypothèse de Riemann généralisée vérifiée pour $L(s,f)$, un zéro ρ de $L(s,f)$ situé dans la bande $0<\mathrm{Re}(\rho)<1$ peut s'écrire sous la forme $\rho=1/2+it$. Le nombre de zéros triviaux est inférieur au degré $d(f)$ de la fonction $L(s,f)$ donc :

$$\begin{aligned}\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{|\rho(\rho+1)|} &\leqslant \sum_{\substack{\rho \text{ zéro de } \Lambda(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{|\rho(\rho+1)|} + \sum_{\substack{\rho \text{ zéro trivial de } L(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{\sqrt{\frac{9}{16}+\frac{5}{2}t^2+t^4}}\\ &\leqslant \sum_{\substack{\rho \text{ zéro de } \Lambda(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{|\rho(\rho+1)|} + \frac{4}{3}\sum_{\substack{\rho \text{ zéro trivial de } L(s,f)\\ 0<\mathrm{Re}(\rho)<1}} 1\\ &\leqslant \sum_{\substack{\rho \text{ zéro de } \Lambda(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{|\rho(\rho+1)|} + \frac{4}{3}\,d(f).\end{aligned}$$

Par ailleurs, on obtient :

$$\begin{aligned}
\sum_{\substack{\rho \text{ zéro de } \Lambda(s,f)\\ \rho=1/2+it}} \frac{1}{|\rho(\rho+1)|} &\leqslant \sum_{n\in\mathbb{Z}} \sum_{\substack{\rho=1/2+it\\ |n-t|\leqslant 1/2}} \frac{1}{\sqrt{\frac{9}{16}+\frac{5}{2}t^2+t^4}} \\
&\leqslant \sum_{n=-\infty}^{-1} \sum_{\substack{\rho=1/2+it\\ |n-t|\leqslant 1/2}} \frac{1}{\sqrt{\frac{9}{16}+\frac{5}{2}t^2+t^4}} + \sum_{n=1}^{+\infty} \sum_{\substack{\rho=1/2+it\\ |n-t|\leqslant 1/2}} \frac{1}{\sqrt{\frac{9}{16}+\frac{5}{2}t^2+t^4}} \\
&\quad + \sum_{\substack{\rho=1/2+it\\ |t|\leqslant 1/2}} \frac{1}{\sqrt{\frac{9}{16}+\frac{5}{2}t^2+t^4}} \\
&\leqslant \sum_{n=-\infty}^{-1} \frac{m_{\frac{1}{2}}(n,f)}{\sqrt{n^4+2n^3+4n^2+3n+\frac{5}{4}}} + \sum_{n=1}^{+\infty} \frac{m_{\frac{1}{2}}(n,f)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}} \\
&\quad + \frac{4}{3} m_{\frac{1}{2}}(0,f).
\end{aligned}$$

En utilisant la proposition 2.2.9, on a :

$$\begin{aligned}
\sum_{\substack{\rho \text{ zéro de } \Lambda(s,f)\\ \rho=1/2+it}} \frac{1}{|\rho(\rho+1)|} &\leqslant \frac{13}{5}\Bigg(\sum_{n=-\infty}^{-1} \frac{\frac{56}{25}d(f)+\frac{1}{2}\ln q(f)+\frac{1}{2}\ln \mathfrak{q}_\infty(3+in,f)+\frac{5}{6}r(f)}{\sqrt{n^4+2n^3+4n^2+3n+\frac{5}{4}}} \\
&\quad + \sum_{n=1}^{+\infty} \frac{\frac{56}{25}d(f)+\frac{1}{2}\ln q(f)+\frac{1}{2}\ln \mathfrak{q}_\infty(3+in,f)+\frac{5}{6}r(f)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}} \\
&\quad + \frac{4}{3}\big(\frac{56}{25}d(f)+\frac{1}{2}\ln q(f)+\frac{1}{2}\ln \mathfrak{q}_\infty(3,f)+\frac{5}{6}r(f)\big)\Bigg) \\
&\leqslant \frac{13}{5}\Bigg(d(f)\big(\frac{112}{25}A(1)+\frac{224}{75}\big)+\ln q(f)\big(A(1)+\frac{2}{3}\big)+\frac{2}{3}\ln \mathfrak{q}_\infty(3,f) \\
&\quad + \frac{5}{3}r(f)\big(A(1)+\frac{2}{3}\big)+\frac{1}{2}\sum_{n=-\infty}^{-1} \frac{\ln \mathfrak{q}_\infty(3+in,f)}{\sqrt{n^4+2n^3+4n^2+3n+\frac{5}{4}}} \\
&\quad + \frac{1}{2}\sum_{n=1}^{+\infty} \frac{\ln \mathfrak{q}_\infty(3+in,f)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}}\Bigg).
\end{aligned}$$

où on a défini $A(\ell) := \displaystyle\sum_{n=\ell}^{+\infty} \frac{1}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}}$.

On majore $\mathfrak{q}_\infty(3+in,f)$ et $\mathfrak{q}_\infty(3-in,f)$ par $\mathfrak{q}(f)(|3+in|+3)^{d(f)}$, ainsi

$$\ln \mathfrak{q}_\infty(3\pm in,f) \leqslant \ln \mathfrak{q}(f) + d(f)\ln(|3+in|+3).$$

D'où,

$$\begin{aligned}\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{|\rho(\rho+1)|} \leqslant \frac{13}{5}\Bigg(d(f)\Bigg(\frac{112}{25}A(1)+\frac{224}{75}+\frac{4}{3}+\frac{2}{3}\ln 6 \\ +\sum_{n=1}^{+\infty}\frac{\ln\left(|3+in|+3\right)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}}\Bigg) \\ +\ln\mathfrak{q}(f)A(1)+\frac{2}{3}\ln\mathfrak{q}(f) \\ +\ln q(f)\big(A(1)+\frac{2}{3}\big)+\frac{5}{3}r(f)\big(A(1)+\frac{2}{3}\big)\Bigg) \\ \leqslant \frac{13}{5}\left(\frac{1617}{100}d(f)+\frac{58}{25}\left(\ln\mathfrak{q}(f)+\ln q(f)+\frac{5}{3}r(f)\right)\right).\end{aligned}$$

□

Remarque 2.2.12. En excluant les premiers zéros, par exemple les zéros de partie imaginaire dont la valeur absolue est inférieure à un réel ℓ, on obtient :

$$\begin{aligned}\sum_{\substack{\rho \text{ zéro de } \Lambda(s,f)\\ |t|\geqslant\ell}} \frac{1}{|\rho(\rho+1)|} &\leqslant 2\sum_{n=\ell}^{+\infty}\frac{m_{\frac{1}{2}}(n,f)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}} \\ &\leqslant \sum_{n=\ell}^{+\infty}\frac{1}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}}\Bigg(\frac{13}{5}\big(\ln\mathfrak{q}(f)+\ln q(f)\big)+\frac{13}{3}r(f) \\ &\quad+\left(\frac{1456}{125}+\frac{13}{5}\ln\big(|3+in|+3\big)\right)d(f)\Bigg).\end{aligned}$$

Ceci peut nous permettre de faire des calculs explicites, voir par exemple le résultat numérique sur les zéros dans la partie traitant des fonctions L d'Artin.

Remarque 2.2.13. En procédant de la même façon, en supposant vraie l'hypothèse de Riemann généralisée pour la fonction $L(s,f)$, on peut avoir la majoration suivante :

$$\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0<\mathrm{Re}(\rho)<1}} \frac{1}{|\rho|^2} \leqslant A(d(f),\mathfrak{q}(f),q(f),r(f)),$$

où

$$A(d,\mathfrak{q},q,r)=\frac{13}{5}\left(d\left(\frac{112}{25}\pi\tanh\left(\frac{\pi}{2}\right)+\frac{221}{10}\right)+\big(\ln\mathfrak{q}+\ln q+\frac{5}{3}r\big)\big(\pi\tanh\left(\frac{\pi}{2}\right)+2\big)\right),$$

avec $\displaystyle\sum_{n=1}^{+\infty}\frac{1}{n^2-n+\frac{1}{2}}=\pi\tanh\left(\frac{\pi}{2}\right)$ démontrée dans la propriété B.1.1.

Corollaire 2.2.14. *Avec le même paramètre que dans le théorème précédent, on a, sous GRH pour $L(s,f)$:*

$$\left|\sum_{\substack{\rho \text{ zéro de } L(s,f)\\ 0\leqslant \mathrm{Re}(\rho)\leqslant 1}} X^{\rho}\hat{\phi}(\rho)\right| \leqslant \sqrt{X}C_{0,\phi}C(d(f),\mathfrak{q}(f),q(f),r(f)) + d(f)C_{1,\phi},$$

avec $C_{0,\phi} = \int_1^2 |\phi''(x)|x^{3/2}\,\mathrm{d}x$ *et* $C_{1,\phi} = \int_1^2 \frac{\phi(x)}{x}\,\mathrm{d}x$.

2.2.4.4 Fin de la preuve du théorème 2.2.3

En reportant dans les inégalités (1) et (2) page 40 les résultats de la proposition 2.2.8 et du corollaire 2.2.14 en prenant soin de remplacer $d(f)$ par $d(f\otimes\bar{f})$ ou $d(f\otimes\bar{g})$ (qui valent $d(f)^2$ puisque $d(f)=d(g)$), on obtient :

$$\begin{aligned}
&\Big|\sum_n \Lambda_{f\otimes\bar{f}}(n)\phi\left(\frac{n}{X}\right) - r(f\otimes\bar{f})\,\|\phi\|_1 X\Big| \\
&\qquad\leqslant C_{1,\phi}d(f\otimes\bar{f}) + C_{0,\phi}\sqrt{X}\Bigg(\frac{39d(f\otimes\bar{f})+7\ln\mathfrak{q}(f\otimes\bar{f})}{4\pi} \\
&\qquad\qquad + C(d(f\otimes\bar{f}),\mathfrak{q}(f\otimes\bar{f}),q(f\otimes\bar{f}),r(f\otimes\bar{f}))\Bigg) \\
&\Big|\sum_n \Lambda_{f\otimes\bar{g}}(n)\phi\left(\frac{n}{X}\right)\Big| \leqslant C_{1,\phi}d(f\otimes\bar{g}) \\
&\qquad + C_{0,\phi}\sqrt{X}\left(\frac{39d(f\otimes\bar{g})+7\ln\mathfrak{q}(f\otimes\bar{g})}{4\pi} + C(d(f\otimes\bar{g}),\mathfrak{q}(f\otimes\bar{g}),q(f\otimes\bar{g}),0)\right),
\end{aligned}$$

où

$$C_{0,\phi} = \int_1^2 |\phi''(x)|x^{3/2}\,\mathrm{d}x \;\;;\;\; C_{1,\phi} = \int_1^2 \frac{\phi(x)}{x}\,\mathrm{d}x$$

et

$$C(d,\mathfrak{q},q,r) = \frac{13}{5}\left(\frac{1617}{100}d + \frac{58}{25}\left(\ln\mathfrak{q} + \ln q + \frac{5}{3}r\right)\right).$$

En utilisant la majoration $d(f)\leqslant \ln\mathfrak{q}(f)$ et la remarque 2.2.11, on obtient :

$$\begin{aligned}
&\Big|\sum_n \Lambda_{f\otimes\bar{f}}(n)\phi\left(\frac{n}{X}\right) - r(f\otimes\bar{f})\,\|\phi\|_1 X\Big| \leqslant C_{1,\phi}d(f\otimes\bar{f}) \\
&\qquad + C_{2,\phi}\sqrt{X}\ln\mathfrak{q}(f\otimes\bar{f}) + \frac{754}{75}C_{0,\phi}\sqrt{X}r(f\otimes\bar{f}) \\
&\Big|\sum_n \Lambda_{f\otimes\bar{g}}(n)\phi\left(\frac{n}{X}\right)\Big| \leqslant C_{1,\phi}d(f\otimes\bar{g}) + C_{2,\phi}\sqrt{X}\ln\mathfrak{q}(f\otimes\bar{g}),
\end{aligned}$$

avec

$$C_{2,\phi} := \Big(\frac{46}{4\pi} + \frac{27053}{500}\Big)C_{0,\phi}.$$

2.3 Majoration explicite du nombre de paramètres locaux suffisants pour déterminer une fonction L d'Artin

Dans ce cas, on se place sur une extension galoisienne L/K de corps de nombres. Nous devrons donc ajuster les preuves, notamment en remplaçant les nombres premiers par des idéaux premiers ou encore le degré d des représentations par le degré $d[K:\mathbb{Q}]$ des fonctions L d'Artin sur $\mathbb{Q}$.

2.3.1 Théorème

L'adaptation du théorème 2.1.3 permet d'obtenir le résultat qui suit. Remarquons que la remarque 1.2.4 permet de supprimer l'hypothèse sur les paramètres locaux. De même, sous la conjecture d'Artin, nous avons démontré (voir partie 1.1.3) que les fonctions L d'Artin ne possèdent pas de zéro de partie réelle 1 : l'hypothèse de Riemann généralisée remplace GRH (conjecture 1.1.12).

Corollaire 2.3.1. *Soit L/K une extension galoisienne de groupe de Galois G. Soient χ_1 et χ_2 deux caractères irréductibles distincts de G, de même degré d, de représentation respective (ρ_1, V_1) et (ρ_2, V_2). On suppose vraies la conjecture d'Artin et l'hypothèse de Riemann généralisée pour les deux fonctions L d'Artin $L(s, \chi_1 \otimes \bar{\chi}_i)$, $i = 1$ ou 2. Alors il existe un idéal premier $\mathfrak{p}$ de K, de norme $\mathrm{N}(\mathfrak{p}) = p^f$ inférieure ou égale à $C\left(d[K:\mathbb{Q}] \ln \mathfrak{q}\left(\chi_1\right) \mathfrak{q}\left(\chi_2\right)\right)^2$ avec p ne divisant pas $q(\chi_1)q(\chi_2)$, tel que les paramètres locaux de $L(s, \chi_1)$ et $L(s, \chi_2)$ en $\mathfrak{p}$ sont différents, avec*

$$C = \frac{51}{25}\left(86 D_{0,\phi} + 2 D_{1,\phi} + \frac{5}{2} D_{3,\phi} \omega'\big(q(\chi_1)q(\chi_2)\big)\right)^2,$$

où ϕ est une fonction positive non nulle, $\mathscr{C}^\infty$, à support compact dans $[1,2]$,

$$D_{0,\phi} = \frac{1}{\|\phi\|_1} \int_1^2 |\phi''(x)| x^{3/2} \,\mathrm{d}x \,;\; D_{1,\phi} = \frac{1}{\|\phi\|_1} \int_1^2 \frac{\phi(x)}{x} \,\mathrm{d}x \text{ et } D_{3,\phi} = \frac{\|\phi\|_\infty}{\|\phi\|_1}.$$

Rappelons que pour tout $n \in \mathbb{N}^*$, $\omega'(n) \leqslant 3/2$ où ω' est définie par :

$$\omega'(n) = \begin{cases} \frac{\omega(n)}{\ln n} & \text{si } n \geqslant 2 \\ 0 & \text{si } n = 1 \end{cases},$$

la fonction $\omega(n)$, définie sur $\mathbb{N}^*$, désignant la fonction additive dénombrant le nombre total des facteurs premiers de n.

Ici, on connaît la convolution de Rankin-Selberg de deux caractères, ceci nous permet de ne pas avoir besoin de la condition de divisibilité du nombre premier (comme le montre la propriété 2.3.6) et on obtient le théorème suivant.

Théorème 2.3.2. *Soit L/K une extension galoisienne de groupe de Galois G. Soient χ_1 et χ_2 deux caractères irréductibles distincts de G, de même degré d, de représentation respective (ρ_1, V_1) et (ρ_2, V_2). On suppose vraies la conjecture d'Artin et l'hypothèse de Riemann généralisée pour les deux fonctions L d'Artin $L(s, \chi_1 \otimes \bar{\chi}_i)$, $i = 1$ ou 2. Alors il*

existe un idéal premier $\mathfrak{p}$ *de* K*, de norme inférieure ou égale à* $C\left(d\ln\mathfrak{q}\left(\chi_1\right)\mathfrak{q}\left(\chi_2\right)\right)^2$*, tel que les paramètres locaux de* $L(s,\chi_1)$ *et* $L(s,\chi_2)$ *en* $\mathfrak{p}$ *sont différents, avec*

$$C=\frac{51}{25}\left(86D_{0,\phi}+2D_{1,\phi}\right)^2,$$

où ϕ *est une fonction positive non nulle,* $\mathscr{C}^\infty$*, à support compact dans* $[1,2]$*,*

$$D_{0,\phi} \;=\; \frac{1}{\|\phi\|_1}\int_1^2 |\phi''(x)|x^{3/2}\,\mathrm{d}x \text{ et } D_{1,\phi}=\frac{1}{\|\phi\|_1}\int_1^2 \frac{\phi(x)}{x}\,\mathrm{d}x.$$

Remarque 2.3.3. En perdant cette condition de divisibilité, le degré du corps de nombres $[K:\mathbb{Q}]$ n'apparaît plus et donc nous obtenons une meilleure borne, bien que la constante C ne soit pas nettement améliorée.

Donnons également une version pour des caractères pas nécessairement irréductibles dont le produit scalaire est nul.

THÉORÈME 2.3.4. *Soit* L/K *une extension galoisienne de groupe de Galois* G*. Soient* χ_1 *et* χ_2 *deux caractères distincts de* G*, de même degré* d*, de représentation respective* (ρ_1,V_1) *et* (ρ_2,V_2) *dont le produit scalaire est nul. On suppose vraies la conjecture d'Artin et l'hypothèse de Riemann généralisée pour les deux fonctions* L *d'Artin* $L(s,\chi_1\otimes\bar{\chi}_i)$*,* $i=1$ *ou 2. Alors il existe un idéal premier* $\mathfrak{p}$ *de* K*, de norme inférieure ou égale à* $C\left(d\ln\mathfrak{q}\left(\chi_1\right)\mathfrak{q}\left(\chi_2\right)\right)^2$*, tel que les paramètres locaux de* $L(s,\chi_1)$ *et* $L(s,\chi_2)$ *en* $\mathfrak{p}$ *sont différents, avec*

$$C=\frac{51}{25}\left(\frac{(74+\frac{289}{25}\langle\chi_1,\chi_1\rangle)D_{0,\phi}+2D_{1,\phi}}{\langle\chi_1,\chi_1\rangle}\right)^2,$$

où ϕ *est une fonction positive non nulle,* $\mathscr{C}^\infty$*, à support compact dans* $[1,2]$ *et les constantes* $D_{0,\phi}$ *et* $D_{1,\phi}$ *sont données dans le théorème 2.3.2 précédent.*

Corollaire 2.3.5. *Les théorèmes 2.3.2 et 2.3.4 précédents sont vrais pour* $C=4,3\cdot 10^7$*.*

PREUVE
On effectue les calculs de la constante C avec la fonction ϕ, trouvée dans la preuve du théorème 2.1.2, définie par $\phi(x)=\exp\left(\frac{-0,3}{(x-1)(2-x)}\right)$ sur $]1,2[$ et nulle ailleurs, pour laquelle on obtient

$$D_{0,\phi}\leqslant 53,5 \;\text{ et }\; D_{1,\phi}\leqslant 0,68.$$

□

2.3.2 Preuve du théorème 2.3.2

Plaçons-nous dans le contexte du théorème : soit L/K une extension galoisienne de groupe de Galois G, soient χ_1 et χ_2 deux caractères irréductibles distincts de G, de même degré d, de représentations respectives (ρ_1,V_1) et (ρ_2,V_2).
Dans le cas des fonctions L d'Artin, on remplace le degré d par $d[K:\mathbb{Q}]$ et d^2 par $d^2[K:\mathbb{Q}]$ dans les résultats de la partie 2.2. De la même façon, on suppose que les paramètres locaux de $L(s,\chi_1)$ et $L(s,\chi_2)$ coïncident pour tous les idéaux premiers $\mathfrak{p}$ de K de norme inférieure ou égale à $2X$. On cherche à majorer X. De plus, grâce aux informations supplémentaires connues ($\kappa_i\in\{0,1\}$ ou encore la convolution de Rankin-Selberg), on a des résultats plus précis.

Propriété 2.3.6. *Si les paramètres locaux de $L(s,\chi_1)$ et $L(s,\chi_2)$ coïncident pour tous les idéaux premiers $\mathfrak{p}$ de K de norme inférieure ou égale à $2X$, on a $\Lambda_{\chi_1\otimes\bar{\chi_1}}(n) = \Lambda_{\chi_1\otimes\bar{\chi_2}}(n)$ pour tout entier $n \leqslant 2X$.*

Preuve
Soit a valant 1 ou 2. La définition de la convolution de Rankin-Selberg donnée dans la partie 1.2.3 et la définition de la fonction duale, permettent d'écrire : pour tout $i \in [\![1, d^2]\!]$, il existe j et $k \in [\![1, d]\!]$ tels que $\alpha_{i,\chi_1\otimes\bar{\chi}_a}(\mathfrak{p}) = \alpha_{j,\chi_1}(\mathfrak{p})\alpha_{k,\bar{\chi}_a}(\mathfrak{p}) = \alpha_{j,\chi_1}(\mathfrak{p})\overline{\alpha_{k,\chi_a}(\mathfrak{p})}$. Ici, on suppose $\alpha_{k,\chi_1}(\mathfrak{p}) = \alpha_{k,\chi_2}(\mathfrak{p})$ pour un idéal premier $\mathfrak{p}$ de K de norme inférieure ou égale à $2X$ donc $\alpha_{i,\chi_1\otimes\bar{\chi}_1}(\mathfrak{p}) = \alpha_{i,\chi_1\otimes\bar{\chi}_2}(\mathfrak{p})$ pour $\mathfrak{p}$ tel que $\mathrm{N}(\mathfrak{p}) \leqslant 2X$. D'après la définition 1.2.6, on a :

$$\Lambda_{\chi_1\otimes\bar{\chi}_a}(n) = \sum_{\substack{\mathfrak{p},\ell \\ n=\mathrm{N}(\mathfrak{p})^\ell}} \sum_{i=1}^{d^2} \alpha_{i,\chi_1\otimes\bar{\chi}_a}(\mathfrak{p})^\ell \ln \mathrm{N}(\mathfrak{p})$$

d'où le résultat. □

On reprend la démarche de la partie 2.2 mais puisque, pour tout $n \in \mathbb{N}$,

$$\sum_n \Lambda_{\chi_1\otimes\overline{\chi_1}}(n)\phi\left(\frac{n}{X}\right) = \sum_n \Lambda_{\chi_1\otimes\overline{\chi_2}}(n)\phi\left(\frac{n}{X}\right),$$

il nous reste juste à majorer les deux termes $\left|\sum_n \Lambda_{\chi_1\otimes\overline{\chi_1}}(n)\phi\left(\frac{n}{X}\right) - r(\chi_1\otimes\overline{\chi_1})\,\|\phi\|_1 X\right|$ et $\left|\sum_n \Lambda_{\chi_1\otimes\overline{\chi_2}}(n)\phi\left(\frac{n}{X}\right)\right|$ (car $r(\chi_1\otimes\overline{\chi_2}) = \langle\chi_1,\chi_2\rangle = 0$ d'après l'hypothèse et la remarque 1.2.27) : c'est ce qui est fait dans le théorème 2.3.12. Pour obtenir ces résultats, nous avons besoin des majorations données par les propositions suivantes.

Proposition 2.3.7. *On a :*

$$\left|\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma_\chi'}{\gamma_\chi}(s) + \frac{\gamma_\chi'}{\gamma_\chi}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s\right| \leqslant \frac{57C_{0,\phi}}{20}d[K:\mathbb{Q}]\sqrt{X},$$

où $C_{0,\phi} = \int_1^2 |\phi''(x)|x^{3/2}\,\mathrm{d}x$.

Preuve
On reprend la preuve de la proposition 2.2.8 en utilisant le lemme 1.1.2 avec

$$\gamma_\chi(s) = \pi^{-sd[K:\mathbb{Q}]/2}\prod_{j=1}^{d[K:\mathbb{Q}]}\Gamma\left(\frac{s+\kappa_j}{2}\right),$$

où $\kappa_j \in \{0,1\}$ (voir la propriété 1.2.24). Le degré d est donc ici remplacé par le degré de la fonction L d'Artin sur $\mathbb{Q}$ qui vaut $d[K:\mathbb{Q}]$. On note $A_j(t)$ le complexe $\frac{1/2+it+\kappa_j}{2} = \frac{s+\kappa_j}{2}$ et on a :

$$\begin{aligned}&\left|\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma_f'}{\gamma_f}(s) + \frac{\gamma_f'}{\gamma_f}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s\right| \\ &\leqslant \frac{C_{0,\phi}\sqrt{X}}{2\pi}\sum_{j=1}^{d[K:\mathbb{Q}]}\int_{\mathbb{R}}\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}(A_j(t))\right|\frac{\mathrm{d}t}{\left|\frac{1}{2}+it\right|\left|\frac{3}{2}+it\right|} \quad \text{où } C_{0,\phi} = \int_1^2 |\phi''(x)|x^{3/2}\,\mathrm{d}x.\end{aligned}$$

Grâce à l'égalité (†) du lemme 2.2.7, on a :

$$\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}(A_j(t))\right| \leqslant \frac{1}{|A_j(t)|} + \ln|1+A_j(t)| + \frac{1}{2|1+A_j(t)|} + \frac{1}{12|1+A_j(t)|^2} + \frac{1}{6}\int_1^{+\infty}\frac{\mathrm{d}x}{(x+\mathrm{Re}A_j(t))^3}$$

Puisque $\kappa_j = 0$ ou 1, on a :

$$|A_j(t)| \geqslant \mathrm{Re}(A_j(t)) \geqslant \frac{1}{4}$$
$$|1+A_j(t)| \geqslant \mathrm{Re}(1+A_j(t)) \geqslant \frac{5}{4}$$
$$x + \mathrm{Re}A_j(t) \geqslant x + \frac{1}{4}$$

d'où

$$\begin{aligned}\sum_{j=1}^{d[K:\mathbb{Q}]}\left|\mathrm{Re}\frac{\Gamma'}{\Gamma}(A_j(t))\right| &\leqslant d[K:\mathbb{Q}]\left(4+\frac{1}{2}\frac{4}{5}+\frac{1}{12}\left(\frac{4}{5}\right)^2+\frac{1}{6}\frac{1}{2}\frac{1}{\left(1+\frac{1}{4}\right)^2}\right)+\ln\prod_{j=1}^{d[K:\mathbb{Q}]}|1+A_j(t)| \\ &= \frac{338}{75}d[K:\mathbb{Q}] + \ln\Big(\prod_{j=1}^{d[K:\mathbb{Q}]}|2+s+\kappa_j|\Big) - d[K:\mathbb{Q}]\ln 2 \\ &\leqslant d[K:\mathbb{Q}]\left(\frac{338}{75} - \ln 2 + \ln|3+s|\right).\end{aligned}$$

Ainsi,

$$\begin{aligned}&\left|\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma_f'}{\gamma_f}(s)+\frac{\gamma_f'}{\gamma_f}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s\right| \\ &\leqslant \frac{C_{0,\phi}\sqrt{X}}{2\pi}d[K:\mathbb{Q}]\int_{\mathbb{R}}\frac{\frac{338}{75}-\ln 2+\ln\sqrt{\frac{49}{4}+t^2}}{\sqrt{\frac{1}{4}+t^2}\sqrt{\frac{9}{4}+t^2}}\,\mathrm{d}t \\ &\leqslant \frac{57C_{0,\phi}}{20}d[K:\mathbb{Q}]\sqrt{X}.\end{aligned}$$

□

La proposition suivante remplace la proposition 2.2.9 du cadre général. Nous avons pu utiliser le fait que les paramètres locaux aux premiers d'une fonction L d'Artin sont toujours de module inférieur à 1 (voir la remarque 1.2.4).

PROPOSITION 2.3.8. *Soit $m_\ell(T,\chi)$ le nombre de zéros $\rho = 1/2+it$ de $\Lambda(s,\chi)$ tels que $|t-T| \leqslant \ell$. Si l'hypothèse de Riemann est vraie pour la fonction L d'Artin $L(s,\chi)$, on a :*

$$m_{\frac{1}{2}}(T,\chi) \leqslant \frac{5}{3}\left(\frac{14}{5}d(\chi)[K:\mathbb{Q}] + \frac{1}{2}\ln q(\chi) + \frac{d(\chi)[K:\mathbb{Q}]}{2}\ln\sqrt{25+T^2} + \frac{3}{2}r(\chi)\right).$$

<u>Preuve</u>
De la même façon que dans la preuve de la proposition 2.2.9, pour $s_0 = \sigma + iT$, on a :

$$\sum_{\substack{\rho \text{ zéro de} \\ \Lambda(s,\chi)}} \mathrm{Re}\frac{1}{s_0-\rho} \leqslant \left|-\frac{L'}{L}(s_0,\chi)\right| + \frac{1}{2}\ln q(\chi) + \left|\frac{\gamma'_\chi}{\gamma_\chi}(s_0)\right| + r(\chi)\frac{2\sigma-1}{\sigma(\sigma-1)}.$$

Dans ce cas, connaissant $\kappa_j \in \{0,1\}$, le complexe $(s+\kappa_j)/2 \notin \mathbb{R}_-$ pour $\mathrm{Re}(s) > -1$, et plus seulement pour $\mathrm{Re}(s) > 1$. De plus, l'information sur le module des paramètres locaux permet de majorer la fonction Λ_χ de la façon suivante : si $n = p^\ell$ (rappelons que si tel n'est pas le cas, $\Lambda_\chi(n) = 0$), avec p un nombre premier, nous notons $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ les g idéaux premiers de $\mathscr{O}_K$ au-dessus de p, e_j et f_j les indices de ramification et degrés résiduels correspondants et k_j les entiers vérifiant $\mathrm{N}(\mathfrak{p}_j)^{k_j} = n$ et $k_j = 0$ dans le cas où n ne peut pas s'écrire sous cette forme. Alors

$$\begin{aligned}
|\Lambda_\chi(n)| = |\sum_{\substack{\mathfrak{p},k \\ n=\mathrm{N}(\mathfrak{p})^k}} \sum_{i=1}^{d} \alpha_{i,\rho}(\mathfrak{p})^k \ln \mathrm{N}(\mathfrak{p})| &\leqslant \sum_{j=1}^{g}\sum_{i=1}^{d} |\alpha_{i,\rho}(\mathfrak{p}_j)^{k_j}| \ln \mathrm{N}(\mathfrak{p}_j) \\
&\leqslant d\sum_{j=1}^{g} \ln \mathrm{N}(\mathfrak{p}_j) = d\ln p \sum_{j=1}^{g} f_j \leqslant d \ln p \sum_{j=1}^{g} e_j f_j = d\ln p[K:\mathbb{Q}] \\
&\leqslant d[K:\mathbb{Q}]\Lambda(n)
\end{aligned}$$

donc on obtient :

$$\begin{aligned}
\left|-\frac{L'}{L}(s_0,\chi)\right| &\leqslant \sum_{n\geqslant 1} \frac{|\Lambda_\chi(n)|}{|n^{s_0}|} = \sum_{n\geqslant 1} \frac{|\Lambda_\chi(n)|}{n^{\mathrm{Re}(s_0)}} \\
&\leqslant d[K:\mathbb{Q}] \sum_{n\geqslant 1} \frac{\Lambda(n)}{n^{\mathrm{Re}(s_0)}}
\end{aligned}$$

qui est une série convergente dès que $\mathrm{Re}(s_0) > 1$.
On peut donc poser $s_0 = \sigma + iT$ avec $\sigma > 1$. Puisque $\mathrm{Re}\left(\frac{s_0+\kappa_j}{2}\right) > 1/2$ ($\kappa_j \in \{0,1\}$), nous sommes dans les conditions d'application du lemme 2.2.7 :

$$\begin{aligned}
&\left|\frac{\gamma'_\chi}{\gamma_\chi}(s_0)\right| \leqslant \frac{d[K:\mathbb{Q}]}{2}\ln\pi + \frac{1}{2}\sum_{j=1}^{d[K:\mathbb{Q}]} \left|\frac{\Gamma'\left(\frac{s_0+\kappa_j}{2}\right)}{\Gamma\left(\frac{s_0+\kappa_j}{2}\right)}\right| \\
&\leqslant \frac{d[K:\mathbb{Q}]}{2}\left(\ln\pi + \frac{\pi}{2}\right) + \frac{1}{2}\sum_{j=1}^{d[K:\mathbb{Q}]} \frac{1}{12}\frac{4}{(2+\sigma+\kappa_j)^2} \\
&\quad + \frac{1}{2}\sum_{j=1}^{d[K:\mathbb{Q}]}\left(\frac{2}{|s_0+\kappa_j|} + \frac{1}{|2+s_0+\kappa_j|} + \frac{1}{3|2+s_0+\kappa_j|^2} + \ln\left(\left|1+\frac{s_0+\kappa_j}{2}\right|\right)\right) \\
&\leqslant \frac{d[K:\mathbb{Q}]}{2}\left(\ln\left(\frac{\pi}{2}\right) + \frac{\pi}{2} + \frac{1}{3(\sigma+2)^2} + \frac{2}{\sigma} + \frac{1}{\sigma+2} + \frac{1}{3(\sigma+2)^2}\right) + \frac{1}{2}\ln\left(\prod_{j=1}^{d[K:\mathbb{Q}]} |2+s_0+\kappa_j|\right) \\
&\leqslant \frac{d[K:\mathbb{Q}]}{2}\left(\ln\left(\frac{\pi}{2}\right) + \frac{\pi}{2} + \frac{2}{\sigma} + \frac{1}{\sigma+2} + \frac{2}{3(\sigma+2)^2} + \ln(|3+s_0|)\right).
\end{aligned}$$

Dans la dernière inégalité, plutôt que de majorer le dernier terme par $\ln \mathfrak{q}_\infty(s,\chi)/2$, nous majorons simplement κ_j par 1, cela nous donne une meilleure borne.
En supposant vraie l'hypothèse de Riemann généralisée pour $L(s,\chi)$, on a :

$$\sum_{\substack{\rho \text{ zéro de} \\ \Lambda(s,\chi)}} \mathrm{Re}\frac{1}{s_0-\rho} \geqslant \sum_{\substack{\rho=1/2+it \\ |t-T|\leqslant \ell}} \frac{\sigma-1/2}{(\sigma-1/2)^2+\ell^2} = \frac{\sigma-1/2}{(\sigma-1/2)^2+\ell^2} m_\ell(T,\chi).$$

D'où

$$m_\ell(T,\chi) \leqslant \frac{(\sigma-1/2)^2+\ell^2}{\sigma-1/2}\Bigg(\frac{1}{2}\ln q(\chi) + r(\chi)\frac{2\sigma-1}{\sigma(\sigma-1)}$$
$$+\frac{d[K:\mathbb{Q}]}{2}\Big(\ln\Big(\frac{\pi}{2}\Big)+\frac{\pi}{2}+\frac{2}{\sigma}+\frac{1}{\sigma+2}+\frac{2}{3(\sigma+2)^2}+2\sum_{n\geqslant 1}\frac{\Lambda(n)}{n^\sigma}+\ln\sqrt{(3+\sigma)^2+T^2}\Big)\Bigg).$$

Dans la suite, nous aurons à considérer $\ell = 1/2$. Grâce à une comparaison numérique, on s'aperçoit que $\sigma = 2$ est un bon candidat pour obtenir une majoration quasiment optimale de $m_{\frac{1}{2}}(T,\chi)$. Dans ce cas,

$$m_{\frac{1}{2}}(T,\chi) \leqslant \frac{5}{3}\left(\frac{14}{5}d[K:\mathbb{Q}] + \frac{1}{2}\ln q(\chi) + \frac{d[K:\mathbb{Q}]}{2}\ln\sqrt{25+T^2} + \frac{3}{2}r(\chi)\right).$$

□

Dans le cas de fonctions L d'Artin, comme nous l'avons déjà noté dans les remarques 1.2.21, les zéros ρ de $L(s,\chi)$ vérifiant $0 < \mathrm{Re}(\rho) < 1$ sont exactement les zéros non triviaux de $L(s,\chi)$, autrement dit les zéros de $\Lambda(s,\chi)$.

THÉORÈME 2.3.9. *En supposant vraie l'hypothèse de Riemann généralisée pour $L(s,\chi)$, on majore la somme sur les zéros non triviaux de $L(s,\chi)$ par :*

$$\sum_{\rho=1/2+it}\frac{1}{|\rho(\rho+1)|} \leqslant \frac{2831}{100}\chi(1)[K:\mathbb{Q}] + \frac{193}{50}\ln q(\chi) + \frac{289}{25}r(\chi).$$

PREUVE

On reprend la preuve du théorème 2.2.10 en majorant κ_j par 1 et en utilisant la borne précédente pour $m_{\frac{1}{2}}(T,\chi)$:

$$\sum_{\substack{\rho \text{ zéro de} \\ \Lambda(s,\chi)}}\frac{1}{|\rho(\rho+1)|} \leqslant \frac{5}{3}\Bigg(d[K:\mathbb{Q}]\Bigg(\frac{28}{5}A(1)+\frac{56}{15}+\sum_{n=1}^{+\infty}\frac{\ln\left(\sqrt{25+n^2}\right)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}}+\frac{2}{3}\ln 5\Bigg)$$
$$+\ln q(\chi)\big(A(1)+\frac{2}{3}\big)+3r(\chi)\big(A(1)+\frac{2}{3}\big)\Bigg)$$
$$\leqslant \frac{2831}{100}d[K:\mathbb{Q}]+\frac{193}{50}\ln q(\chi)+\frac{289}{25}r(\chi).$$

□

Remarque 2.3.10. Comme dans le cas général, nous pouvons obtenir un résultat en excluant les petits zéros :

$$\sum_{\substack{\rho=1/2+it\\|t|\geqslant\ell}}\frac{1}{|\rho(\rho+1)|}\leqslant 2\sum_{n=\ell}^{+\infty}\frac{m_{\frac{1}{2}}(n,\chi)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}}$$
$$\leqslant\sum_{n=\ell}^{+\infty}\frac{d[K:\mathbb{Q}]\big(\frac{28}{3}+\frac{5}{3}\ln(\sqrt{25+n^2})\big)+\frac{5}{3}\ln q(\chi)+5r(\chi)}{\sqrt{n^4-2n^3+4n^2-3n+\frac{5}{4}}}$$

Par exemple, pour $\ell=10$, nous pouvons apprécier la précision gagnée :

$$\sum_{\substack{\rho=1/2+it\\|t|\geqslant 10}}\frac{1}{|\rho(\rho+1)|}\leqslant\frac{41}{25}d[K:\mathbb{Q}]+\frac{19}{100}\ln q(\chi)+\frac{14}{25}r(\chi).$$

Remarque 2.3.11. Comme pour le cas général, en procédant de la même façon que précédemment, en supposant vraie l'hypothèse de Riemann généralisée pour $L(s,\chi)$, nous obtenons :

$$\sum_{\rho=1/2+it}\frac{1}{|\rho|^2}\leqslant 60\chi(1)[K:\mathbb{Q}]+\frac{17}{2}\ln q(\chi)+25r(\chi).$$

Finalement, nous obtenons une version plus précise du théorème 2.2.3 pour des fonctions L d'Artin :

Théorème 2.3.12. *Si les conjectures de Riemann et d'Artin sont vérifiées pour les fonctions $L(s,\chi_1\otimes\chi_i)$ ($i=1$ ou 2) et si $\langle\chi_1,\chi_2\rangle=0$, on a :*

$$\left|\sum_{n\leqslant 2X}\Lambda_{\chi_1\otimes\overline{\chi_1}}(n)\phi\left(\frac{n}{X}\right)-r(\chi_1\otimes\overline{\chi_1})\,\|\phi\|_1\,X\right|\leqslant C_{1,\phi}d^2[K:\mathbb{Q}]$$
$$+C_{0,\phi}\sqrt{X}\Big(\frac{779}{25}d^2[K:\mathbb{Q}]+\frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_1})+\frac{289}{25}r(\chi_1\otimes\overline{\chi_1})\Big)$$
$$\left|\sum_{n\leqslant 2X}\Lambda_{\chi_1\otimes\overline{\chi_2}}(n)\phi\left(\frac{n}{X}\right)\right|\leqslant C_{1,\phi}d^2[K:\mathbb{Q}]+C_{0,\phi}\sqrt{X}\Big(\frac{779}{25}d^2[K:\mathbb{Q}]+\frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_2})\Big),$$

où $C_{0,\phi}=\int_1^2|\phi''(x)|x^{3/2}\,\mathrm{d}x$ et $C_{1,\phi}=\int_1^2\frac{\phi(x)}{x}\,\mathrm{d}x$.

<u>Preuve</u>

On reprend la preuve de la proposition 2.2.3 de la partie 2.2.4.4 en utilisant cette fois l'inégalité de la proposition 2.3.7 :

$$\left|\frac{1}{2i\pi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\left(\frac{\gamma'_{\chi_1\otimes\bar{\chi}_i}}{\gamma_{\chi_1\otimes\bar{\chi}_i}}(s)+\frac{\gamma'_{\chi_1\otimes\bar{\chi}_i i}}{\gamma_{\chi\otimes\bar{\chi}_i}}(1-s)\right)X^s\hat{\phi}(s)\,\mathrm{d}s\right|\leqslant\frac{57C_{0,\phi}}{20}d^2[K:\mathbb{Q}]\sqrt{X}.$$

Sous la conjecture d'Artin, pour des caractères de produit scalaire nul, on a $r(\chi_1\otimes\overline{\chi_2})=0$ (voir remarque 1.2.27), le théorème 2.3.9 donne donc :

$$\sum_{\substack{\rho\text{ zéro de}\\\Lambda(s,\chi_1\otimes\overline{\chi_1})}}\frac{1}{|\rho|^2}\leqslant\frac{2831}{100}d^2[K:\mathbb{Q}]+\frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_1})+\frac{289}{25}r(\chi_1\otimes\overline{\chi_1})$$
$$\text{et}\quad\sum_{\substack{\rho\text{ zéro de}\\\Lambda(s,\chi_1\otimes\overline{\chi_2})}}\frac{1}{|\rho|^2}\leqslant\frac{2831}{100}d^2[K:\mathbb{Q}]+\frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_2}).$$

On sait qu'une fonction L d'Artin ne possède pas de zéro de partie réelle 1, elle peut donc avoir au plus $d[K:\mathbb{Q}]$ zéros de partie réelle nulle, correspondant aux éventuels pôles du facteur gamma (ce serait en fait des réels nuls). Ainsi, on obtient :

$$\begin{aligned}|\sum_{\substack{\rho \text{ zéro de } L(s,\chi)\\ 0\leqslant \mathrm{Re}(\rho)\leqslant 1}} X^\rho \hat{\phi}(\rho)| &\leqslant |\sum_{\substack{\rho \text{ zéro de } L(s,\chi)\\ 0<\mathrm{Re}(\rho)<1}} X^\rho \hat{\phi}(\rho)| + |\sum_{\substack{\rho \text{ zéro de } L(s,\chi)\\ \mathrm{Re}(\rho)=0}} X^\rho \hat{\phi}(\rho)| \\ &\leqslant C_{0,\phi}\sqrt{X} \sum_{\substack{\rho \text{ zéro de } L(s,\chi)\\ \mathrm{Re}(\rho)=\frac{1}{2}}} \frac{1}{|\rho(\rho+1)|} + C_{1,\phi}\chi(1)[K:\mathbb{Q}].\end{aligned}$$

D'après (1) et (2) page 40, on a alors :

$$\begin{aligned}\left|\sum_{n\leqslant 2X} \Lambda_{\chi_1\otimes\overline{\chi_1}}(n)\phi\left(\frac{n}{X}\right) - r(\chi_1\otimes\overline{\chi_1})\,\|\phi\|_1 X\right| &\leqslant \frac{57C_{0,\phi}}{20}\sqrt{X}d^2[K:\mathbb{Q}] + C_{1,\phi}d^2[K:\mathbb{Q}] \\ &\quad + C_{0,\phi}\sqrt{X}\Big(\frac{2831}{100}d^2[K:\mathbb{Q}] + \frac{193}{50}\ln q(\chi_1\otimes\bar{\chi_1}) + \frac{289}{25}r(\chi_1\otimes\overline{\chi_1})\Big) \\ &\leqslant C_{1,\phi}d^2[K:\mathbb{Q}] + C_{0,\phi}\sqrt{X}\Big(\frac{779}{25}d^2[K:\mathbb{Q}] + \frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_1}) + \frac{289}{25}r(\chi_1\otimes\overline{\chi_1})\Big) \\ \left|\sum_{n\leqslant 2X} \Lambda_{\chi_1\otimes\overline{\chi_2}}(n)\phi\left(\frac{n}{X}\right)\right| &\leqslant \frac{57C_{0,\phi}}{20}\sqrt{X}d^2[K:\mathbb{Q}] + C_{1,\phi}d^2[K:\mathbb{Q}] \\ &\quad + C_{0,\phi}\sqrt{X}\Big(\frac{2831}{100}d^2[K:\mathbb{Q}] + \frac{193}{50}\ln q(\chi_1\otimes\bar{\chi_2})\Big) \\ &\leqslant C_{1,\phi}d^2[K:\mathbb{Q}] + C_{0,\phi}\sqrt{X}\Big(\frac{779}{25}d^2[K:\mathbb{Q}] + \frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_2})\Big).\end{aligned}$$

□

On peut donc reprendre le résultat de la proposition 2.2.5 en utilisant les propriétés suivantes des conducteurs : $d^2[K:\mathbb{Q}] \leqslant \ln \mathfrak{q}(\chi_1\otimes\bar{\chi}_2)$ (voir remarque 1.2.25) et $q(\chi_1\otimes\overline{\chi_i}) \leqslant (q(\chi_1)q(\chi_i))^d$ (propriétés 1.2.28), on obtient finalement :

$$\begin{aligned}r(\chi_1\otimes\overline{\chi_1})\|\phi\|_1 X &\leqslant \left|\sum_{n\leqslant 2X} \Lambda_{\chi_1\otimes\overline{\chi_1}}(n)\phi\left(\frac{n}{X}\right) - r(\chi_1\otimes\overline{\chi_1})\,\|\phi\|_1 X\right| \\ &\quad + \left|\sum_{n\leqslant 2X} \Lambda_{\chi_1\otimes\overline{\chi_1}}(n)\phi\left(\frac{n}{X}\right)\right| \\ &\leqslant \left|\sum_{n\leqslant 2X} \Lambda_{\chi_1\otimes\overline{\chi_1}}(n)\phi\left(\frac{n}{X}\right) - r(\chi_1\otimes\overline{\chi_1})\,\|\phi\|_1 X\right| \\ &\quad + \left|\sum_{n\leqslant 2X} \Lambda_{\chi_1\otimes\overline{\chi_2}}(n)\phi\left(\frac{n}{X}\right)\right| \\ &\leqslant 2C_{1,\phi}d^2[K:\mathbb{Q}] + C_{0,\phi}\sqrt{X}\Big(\frac{1558}{25}d^2[K:\mathbb{Q}] \\ &\quad + \frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_1}) + \frac{193}{50}\ln q(\chi_1\otimes\overline{\chi_2}) + \frac{289}{25}r(\chi_1\otimes\overline{\chi_1})\Big) \\ &\leqslant 2C_{1,\phi}d^2[K:\mathbb{Q}] + (74 + \frac{289}{25}r(\chi_1\otimes\overline{\chi_1}))C_{0,\phi}\sqrt{X}d\ln(\mathfrak{q}(\chi_1)\mathfrak{q}(\chi_2)).\end{aligned}$$

D'où

$$\sqrt{X} \leqslant d\ln(\mathfrak{q}(\chi_1)\mathfrak{q}(\chi_2))\frac{(74+\frac{289}{25}r(\chi_1\otimes\overline{\chi_1}))C_{0,\phi}+2C_{1,\phi}}{r(\chi_1\otimes\overline{\chi_1})\,\|\phi\|_1}.$$

Le théorème 2.3.4 tel qu'il est écrit s'obtient à l'aide de la remarque suivante (remarque 1.2.27) : $r(\chi_1\otimes\overline{\chi_1}) = \langle\chi_1,\chi_1\rangle$.

2.3.3 Aspects explicites entre coefficients et paramètres locaux d'une fonction L d'Artin

Nous pouvons remarquer que dans le cas général, pour deux caractères χ et χ', l'égalité entre les coefficients $a_\chi(p)$ et $a_{\chi'}(p)$ des séries de Dirichlet des fonctions L d'Artin $L(s,\chi,L/K)$ et $L(s,\chi',L/K)$ n'impliquent pas l'égalité des paramètres locaux en p. D'ailleurs, lorsque $K=\mathbb{Q}$, nous donnons des contre-exemples. Cependant, la proposition suivante permet de relier les paramètres locaux en p d'une fonction L d'Artin avec les coefficients de sa série de Dirichlet en les puissances de p :

Proposition 2.3.13. *Si $K=\mathbb{Q}$, on a $a_\chi(p^j) = h_j(\alpha_{1,\rho}(p),\dots,\alpha_{d,\rho}(p))$ pour p un nombre premier, avec h_j le polynôme symétrique complètement homogène de degré j.*

Remarque 2.3.14. Notons que $\chi(\sigma_p) = \sum_{i=1}^{d}\alpha_{i,\rho}(p) = a_\chi(p)$.

On en déduit :

Corollaire 2.3.15. *Dans le cas où $K=\mathbb{Q}$, si les paramètres locaux en p de χ sont différents de ceux de χ', il existe au moins un entier $j\in[\![1,d]\!]$ tel que $a_\chi(p^j)\neq a_{\chi'}(p^j)$.*

Les coefficients d'une fonction L d'Artin en certaines puissances d'un nombre premier peuvent donc être égaux même si leurs paramètres locaux sont différents. Illustrons ce résultat par des exemples numériques obtenus grâce aux programmes évoqués dans la partie 1.2.4.1.

Si L est le corps de nombres défini par le polynôme irréductible $P = x^{12}-24x^{10}+120x^8-206x^6+120x^4-24x^2+1$ et χ_1, χ_2 les caractères irréductibles de degré 2 du groupe $\mathrm{Gal}(L/\mathbb{Q})$, les coefficients $a_{\chi_1}(2)=a_{\chi_2}(2)=0$ mais les paramètres locaux en 2 sont différents : $\alpha_{1,\chi_1}(2)=\alpha_{2,\chi_1}(2)=0$ et $\alpha_{1,\chi_2}(2)=-1$ ($\alpha_{2,\chi_2}(2)=1$). Dans ce cas, d'après le corollaire 2.3.15, les coefficients $a_{\chi_1}(2^2)$ et $a_{\chi_2}(2^2)$ sont forcément différents. Dans cet exemple, $a_{\chi_1}(4)=1$ tandis que $a_{\chi_2}(4)=0$.
Deux représentations χ_1 et χ_2 de degré 2 du polynôme $\mathbb{Q}$-irréductible défini par $P = x^{32}+40x^{28}+204x^{24}+728x^{20}+1190x^{16}+728x^{12}+204x^8+40x^4+1$ ont des paramètres locaux en 3 différents : $\{-1,1\}\neq\{-i,i\}$. Mais les premiers coefficients distincts sont les neuvièmes : $a_{\chi_1}(3^2)=-1\neq 1=a_{\chi_2}(3^2)$.
Il existe un polynôme P de degré 27 dont les représentations χ_1 et χ_2 de degré 3 ont des paramètres locaux en 2 différents mais les premiers coefficients qui diffèrent sont $a_{\chi_1}(2^3)$ et $a_{\chi_2}(2^3)$.
Pour les caractères de degré 4 du groupe de Galois associé à $P = x^{40}-25x^{30}+620x^{20}-125x^{10}+25$ $\mathbb{Q}$-irréductible, les paramètres locaux sont différents en $p=3$ (car pour une des deux représentations le sous-espace vectoriel V^{I_3} est trivial) mais les premiers coefficients différents sont en $n=11$. Les coefficients provenant des paramètres locaux de $p=3$ sont seulement différents en $n=3^4=81$.

2.4 Application aux fonctions L de formes modulaires primitives

Pour cette partie, les références sont [Ber13] et [Rou09]. On commence par rappeler la définition ainsi que les principales propriétés des formes modulaires primitives. Puis on illustre le théorème 2.1.3 dans ce cas.

2.4.1 Définition

Soit $\mathbb{H}$ le demi-plan de Poincaré et $SL_2(\mathbb{Z})$ l'ensemble des matrices 2×2 d'entiers dont le déterminant vaut 1. Ce groupe agit sur $\mathbb{H}$ par homographie : pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et $z \in \mathbb{H}$, l'action est définie par :

$$\gamma \cdot z = \frac{az+b}{cz+d}.$$

Pour tout $N \in \mathbb{N}$, le sous-groupe de congruence de $SL_2(\mathbb{Z})$ est défini par :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ N \text{ divise } c \right\}.$$

Définition 2.4.1. Soit $k \geqslant 2$ un entier pair et $N \geqslant 1$ un entier positif. On appelle forme modulaire de poids k, de niveau N et de caractère trivial toute fonction holomorphe sur $\mathbb{H}$ vérifiant la relation suivante :

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. De plus, on dit que f est parabolique si la fonction définie par $z \mapsto (\mathrm{Im}(z))^{k/2} f(z)$ est bornée sur $\mathbb{H}$.

Notons $S_k(N)$ l'espace des formes paraboliques de poids k, de niveau N et de caractère trivial. Il s'agit d'un espace vectoriel de dimension finie sur lequel on définit un produit hermitien, appelé produit scalaire de Petersson :

$$\langle f, g \rangle = \int_{\mathscr{D}_0(N)} f(z)\overline{g(z)} y^k \frac{\mathrm{d}x\mathrm{d}y}{y^2} \text{ avec } z = x + iy$$

et où $\mathscr{D}_0(N)$ désigne un domaine fondamental de $\Gamma_0(N)$.

Pour tous entiers positifs N' et $d \neq 1$ tels que $N' \mid N$ et $d \mid \frac{N}{N'}$ et toute forme $f \in S_k(N')$, on peut vérifier que la fonction $z \mapsto f(dz)$ est une forme parabolique de poids k, de niveau N et de caractère trivial. L'espace

$$S_k^a(N) = \mathrm{Vect}\left\{ z \mapsto f(dz)\ ;\ N' \mid N,\ d \mid \frac{N}{N'},\ f \in S_k(N') \right\}$$

s'appelle l'espace des formes anciennes de niveau N. L'espace des formes nouvelles par rapport à N, noté $S_k^n(N)$, est l'orthogonal de $S_k^a(N)$ dans $S_k(N)$.

2.4.2 Opérateurs de Hecke et formes primitives

Définition 2.4.2. Pour tout entier $n \geqslant 1$, on définit le n^e opérateur de Hecke par :

$$\begin{aligned} T_n : S_k(N) &\to S_k(N) \\ f &\mapsto \frac{1}{n} \sum_{\substack{ad=n \\ (d,N)=1}} a^k \sum_{b=0}^{d-1} f\left(\frac{az+b}{d}\right). \end{aligned}$$

Propriétés 2.4.3. *Les opérateurs de Hecke vérifient les propriétés suivantes :*

1. *pour $m, n \geqslant 1$, $T_m T_n = \sum_{\substack{d|(m,n) \\ (d,N)=1}} d^{k-1} T_{mn/d^2}$. En particulier, les opérateurs de Hecke commutent deux à deux et si m et n sont premiers entre eux : $T_m T_n = T_{mn}$;*
2. *pour $(n, N) = 1$, T_n est un opérateur auto-adjoint de $S_k(N)$, autrement dit : pour tous $f, g \in S_k(N)$,*
$$\langle T_n f, g\rangle = \langle f, T_n g\rangle \ ;$$
3. *les sous-espaces $S_k^a(N)$ et $S_k^n(N)$ sont stables par rapport aux opérateurs T_n avec $(n, N) = 1$.*

Définition 2.4.4. Soit $k \geqslant 2$ un entier pair et $N \in \mathbb{N}$ un entier. Les fonctions propres de tous les opérateurs de Hecke T_n dans l'espace $S_k^n(N)$ s'appellent formes primitives de poids k, de niveau N et de caractère trivial.
L'ensemble de ces formes, noté $H_k^*(N)$, est une base de $S_k^n(N)$.

Proposition 2.4.5. *Toute forme primitive $f \in H_k^*(N)$ admet un développement de Fourier de la forme :*

$$f(z) = \sum_{n \geqslant 1} \lambda_f(n) n^{(k-1)/2} \mathrm{e}^{2\pi i n z},$$

où $\lambda_f(n)$ est le n^e coefficient de Fourier de f normalisé.

2.4.3 Fonctions L d'une forme modulaire primitive

On pourra se référer à [Ogg69], [Li75] ou [Li79].

Définition 2.4.6. Pour f une forme primitive de poids k, de niveau N et de caractère trivial, la fonction L associée est définie, pour $s \in \mathbb{C}$ de partie réelle supérieure à 1, par :

$$L(s, f) = \sum_{n \geqslant 1} \frac{\lambda_f(n)}{n^s}$$

où $\lambda_f(n)$ est le n^e coefficient de Fourier de f normalisé.

Les travaux de M. Eichler, G. Shimura, Y. Ihara et P. Deligne (voir par exemple [KMV02]) permettent d'énoncer le résultat suivant :

Proposition 2.4.7. *Soit χ_0 le caractère de Dirichlet principal modulo N. On désigne par $\alpha_f^{(1)}(p)$ et $\alpha_f^{(2)}(p)$ les racines complexes de l'équation $X^2 - \lambda_f(p)X + \chi_0(p) = 0$. Alors*

$$L(s, f) = \prod_p \left(1 - \frac{\lambda_f(p)}{p^s} + \frac{\chi_0(p)}{p^{2s}}\right)^{-1} = \prod_p \left(1 - \frac{\alpha_f^{(1)}(p)}{p^s}\right)^{-1} \left(1 - \frac{\alpha_f^{(2)}(p)}{p^s}\right)^{-1}.$$

De plus, une telle fonction L vérifie la conjecture de Ramanujan-Petersson, autrement dit, $|\alpha_f^{(1)}(p)|$, $|\alpha_f^{(2)}(p)| \leqslant 1$.

THÉORÈME 2.4.8 (Équation fonctionnelle). *La fonction $L(s,f)$ est auto-duale de degré 2 et sa fonction L complétée*

$$\Lambda(s,f) = \left(\frac{\sqrt{N}}{\pi}\right)^s \Gamma\left(\frac{s+\frac{k-1}{2}}{2}\right)\Gamma\left(\frac{s+\frac{k+1}{2}}{2}\right)L(s,f)$$

se prolonge analytiquement sur $\mathbb{C}$ et vérifie l'équation fonctionnelle :

$$\Lambda(s,f) = \epsilon(f)\Lambda(1-s,f)$$

où $\epsilon(f) = \pm 1$.

Remarque 2.4.9. En comparant avec la définition donnée pour une fonction L générale (voir paragraphe 1.1.1), on retrouve les invariants associés : le conducteur correspond au niveau N, les paramètres locaux en un nombre premier p sont les racines $\alpha_f^{(1)}(p)$ et $\alpha_f^{(2)}(p)$ et les paramètres locaux à l'infini correspondent aux réels $\frac{k-1}{2}$ et $\frac{k+1}{2}$.

PROPOSITION 2.4.10 (Convolution de Rankin-Selberg, [IK04] pages 132-133 ou encore [KMV02] page 135). *Pour deux formes primitives f et g de poids respectifs k_f et k_g vérifiant $k_f \leqslant k_g$, la convolution de Rankin-Selberg $L(s, f\otimes g)$ est de degré 4 et s'écrit :*

$$L(s,f\otimes g) = \prod_p \prod_{i=1}^{2}\prod_{j=1}^{2}\left(1-\frac{\alpha_f^{(i)}(p)\alpha_g^{(j)}(p)}{p^s}\right)^{-1}.$$

De plus, elle a un pôle simple en $s=1$ si $g=f$ et est entière sinon et son facteur gamma est donné par :

$$\gamma_{f\otimes g}(s) = \pi^{-2s}\Gamma\left(\frac{s+\frac{k_g-k_f}{2}}{2}\right)\Gamma\left(\frac{s+\frac{k_g+k_f}{2}}{2}\right)\Gamma\left(\frac{s+\frac{k_g-k_f}{2}+1}{2}\right)\Gamma\left(\frac{s+\frac{k_g+k_f}{2}-1}{2}\right).$$

Remarque 2.4.11. La proposition 2.4.7 permet de déduire de la proposition précédente que les paramètres locaux en un nombre premier d'une convolution de Rankin-Selberg sont de module inférieur à 1.

2.4.4 Théorème

Le résultat suivant est l'application du théorème 2.1.3 aux formes modulaires primitives holomorphes sur $\Gamma_0(N)$. Dans ce cas, afin de conserver la propriété du produit de convolution de Rankin-Selberg $q(f\otimes g) \mid (q(f)q(g))^2$, on suppose les niveaux sans facteurs carrés et premiers entre eux, ainsi $q(f\otimes g) = ppcm(N_f,N_g)^2 = (N_fN_g)^2$, on pourra se référer à [KMV02], [Ogg69] (Theorem 6), [Li75] (Theorem 10) ou [Li79].
De plus, il n'existe pas de zéro de partie réelle égale à 1 (voir par exemple le théorème 5.44 de [IK04]) : GRH est donc simplement remplacée par l'hypothèse de Riemann généralisée.

Corollaire 2.4.12. *Soit $L(s,f)$ et $L(s,g)$ deux fonctions L associées à des formes primitives holomorphes f et g de poids k_f et k_g, de niveau N_f et N_g sans facteurs carrés et premiers entre eux. Supposons que l'hypothèse de Riemann généralisée soit vraie pour les deux fonctions $L(s,f\otimes f)$ et $L(s,f\otimes g)$. Alors, pour $N=\max(N_f,N_g)$ et $k=\max(k_f,k_g)$, il existe un nombre premier p ne divisant pas N_fN_g et $p \leqslant 16\ C\ln^2\left(N\left(3+\frac{k+1}{2}\right)^2\right)$, tel que les paramètres locaux de $L(s,f)$ et $L(s,g)$ en p sont différents, avec C une constante absolue.*

Corollaire 2.4.13. *La constante C du corollaire précédent est la même que celle du théorème 2.1.3.*

Grâce à la connaissance des paramètres locaux de la convolution de Rankin-Selberg, on peut procéder de la même manière que dans le cas des fonctions L d'Artin pour obtenir le théorème suivant qui permet une légère amélioration de la constante, indépendamment de la divisibilité des conducteurs par le nombre premier.

Théorème 2.4.14. *Soit $L(s,f)$ et $L(s,g)$ deux fonctions L associées à des formes primitives holomorphes f et g de poids k_f et k_g, de niveau N_f et N_g sans facteurs carrés et premiers entre eux. Supposons que l'hypothèse de Riemann généralisée soit vraie pour les deux fonctions $L(s,f\otimes f)$ et $L(s,f\otimes g)$. Alors, pour $N=\max(N_f,N_g)$ et $k=\max(k_f,k_g)$, il existe un nombre premier $p\leqslant 8C\ln^2\left(N\left(3+\frac{k+1}{2}\right)^2\right)$, tel que les paramètres locaux de $L(s,f)$ et $L(s,g)$ en p sont différents, avec*

$$C=\frac{51}{25}\left(2D_{1,\phi}+3D_{2,\phi}+\frac{754}{75}D_{0,\phi}\right)^2,$$

où

$$\begin{aligned}
D_{0,\phi}&=\frac{1}{\|\phi\|_1}\int_1^2|\phi''(x)|x^{3/2}\,\mathrm{d}x\\
D_{1,\phi}&=\frac{1}{\|\phi\|_1}\int_1^2\frac{\phi(x)}{x}\,\mathrm{d}x\\
D_{2,\phi}&=D_{0,\phi}\left(\frac{46}{4\pi}+\frac{27053}{500}\right).
\end{aligned}$$

Corollaire 2.4.15. *Le corollaire 2.4.12 et le théorème 2.4.14 précédents sont vérifiés avec $C=2\cdot 10^8$.*

Remarque 2.4.16. Dans l'appendice de [CG14], Sam Chow et Alexandru Ghitza donnent des exemples de bornes : une forme nouvelle de poids 38 et de niveau 3 est déterminée par ses 2 premiers coefficients, ce qui est bien meilleur que la borne, de l'ordre de 10^{11}, obtenue ici. Cependant, la borne donnée par le théorème 2.4.14 est en $\ln^2(Nk^2)$, ce qui est asymptotiquement meilleur que d'autres résultats inconditionnels déjà connus. Notamment, on sait que (voir par exemple [CG14]) pour f et g deux formes nouvelles sur $\Gamma_0(N)$, distinctes, de poids k et de niveau N, il existe n tel que $\lambda_f(n)\neq\lambda_g(n)$ et $n\leqslant\frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)]=\dfrac{Nk}{12}\displaystyle\prod_{p|N}\left(1+\frac{1}{p}\right)$.

Chapitre 3

Séparation des caractères par le Frobenius

Ce chapitre repose essentiellement sur un travail en collaboration avec Christian Maire qui a été soumis à la publication. Il est consacré à la question de la séparation de deux caractères du groupe de Galois absolu d'un corps de nombres K par le Frobenius d'un idéal premier $\mathfrak{p}$ de $\mathscr{O}_K$. Nous commençons par (re)donner une borne pour la norme $\mathrm{N}(\mathfrak{p})$ de $\mathfrak{p}$ en fonction des conducteurs et des degrés des représentations associées. Nous illustrons ensuite ce résultat par deux applications : (i) à la recherche d'un nombre premier p pour lequel $P(\mathrm{mod}\ p)$ admet un certain type de factorisation dans $\mathbb{F}_p[X]$, où $P \in \mathbb{Z}[X]$ est $\mathbb{Q}$-irréductible unitaire et de discriminant égal au discriminant d'un corps quadratique ; (ii) au nombre maximum de certaines extensions modérément ramifiées de groupe de Galois A_n (au-dessus d'un corps de nombres K). Enfin, nous réalisons des expérimentations à la séparation de caractères non ramifiés du groupe alterné A_n (pour $n = 5, 7$ et 13) au-dessus de corps quadratiques réels et imaginaires, ceci à travers des familles de trinômes. On termine par une observation sur les solutions d'une équation diophantienne en relation avec des travaux de Rémond [Rém10] et de Bugeaud [Bug97].

3.1 Présentation du résultat

Le principal résultat du chapitre est présenté ci-dessous, il sera démontré dans la partie suivante.

Théorème 3.1.1. *Soit K un corps de nombres de groupe de Galois absolu G_K et soient χ et χ' deux caractères de G_K, de produit scalaire nul. En supposant vraies les conjectures d'Artin et de Riemann généralisée aux fonctions L d'Artin, il existe un idéal premier $\mathfrak{p}$ de K de norme plus petite que*

$$\frac{4}{\langle \chi, \chi \rangle^2}\Big[c_1\chi(1)\chi'(1)[K:\mathbb{Q}] + c_2\Big(\ln q(\chi \otimes \overline{\chi'}) + \ln q(\chi \otimes \overline{\chi})\Big) + c_3\langle \chi, \chi \rangle\Big]^2$$

tel que $\chi(\sigma_{\mathfrak{p}}) \neq \chi'(\sigma_{\mathfrak{p}})$, où $\sigma_{\mathfrak{p}}$ désigne l'automorphisme de Frobenius associé à l'idéal premier $\mathfrak{p}$ et où les c_i sont des constantes réelles, indépendantes du corps et des caractères.

Remarque 3.1.2. Quand l'idéal premier $\mathfrak{p}$ est ramifié, $\chi(\sigma_{\mathfrak{p}})$ correspond à la "moyenne" du Frobenius au sens de la définition donnée dans la partie 1.2.1. Le choix de l'idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ n'a pas d'influence ici puisque les différents automorphismes de Frobenius sont conjugués et donc les caractères sont égaux.

Le résultat présenté ici semble préciser un récent travail de Rouse et Thorne dans lequel les auteurs donnent une borne pour la séparation des ensembles des valeurs propres de deux représentations irréductibles (proposition 4.1 de [RT14]). Mais une lecture attentive de la preuve de leur résultat montre qu'en fait la borne donnée permet de séparer les caractères irréductibles en jeu. En effet, ceci est "caché" dans l'inégalité (4.6) : celle-ci provient de la différence entre les fonctions $\Lambda_{\chi\otimes\overline{\chi}}(n)$ et $\Lambda_{\chi\otimes\overline{\chi'}}(n)$, minorée par le théorème 2.3.12 et majorée en utilisant la définition 1.2.6 introduisant les paramètres locaux. Avec les notations introduites ici dans le paragraphe 3.2, par les résultats de l'article [RT14], on trouve la différence $|\psi_1(x,\chi\otimes\overline{\chi})-\psi_1(x,\chi\otimes\overline{\chi'})|$, ce qui permet alors de minorer $|\theta_1(x,\chi\otimes\overline{\chi})-\theta_1(x,\chi\otimes\overline{\chi'})|$ donc d'obtenir x tel que $\theta_1(x,\chi\otimes\overline{\chi})\neq\theta_1(x,\chi\otimes\overline{\chi'})$.

Ici nous présentons une preuve légèrement différente (dans l'esprit de [LO77]) en nous efforçant d'éviter les majorations trop brutales, ce qui donne quelques situations nous semblant intéressantes (voir la section 3.4.3).

Donnons un corollaire à ce théorème dans le cas où les caractères sont de même degré. On note M le produit $\prod_{p\in P(L/K)} p$, où $P(L/K)$ est l'ensemble des nombres premiers $p\in\mathbb{Z}$ tels qu'il existe un idéal premier $\mathfrak{p}$ de K ramifié dans L qui soit au-dessus de p. Remarquons que $M\leqslant|\text{disc } L|$.

Corollaire 3.1.3. *Sous les conditions du théorème 3.1.1 en notant $d=\chi(1)=\chi'(1)$ et $G=\mathrm{Gal}(L/K)$, la borne devient à une constante près :*

$$\begin{cases} d^4\ln^2|\text{disc } K|\ln^2(M|G|) & \textit{si } K\neq\mathbb{Q} \textit{ et } P(L/K)\neq\emptyset \\ d^4\ln^2|\text{disc } K| & \textit{si } K\neq\mathbb{Q} \textit{ et } P(L/K)=\emptyset \\ d^4\ln^2(M|G|) & \textit{si } K=\mathbb{Q} \textit{ et } P(L/K)\neq\emptyset \\ d^4 & \textit{sinon.} \end{cases}$$

<u>PREUVE</u>
Étudions le premier cas lorsque $K\neq\mathbb{Q}$ et $P(L/K)\neq\emptyset$.
D'après la définition du conducteur, on a : $q(\chi\otimes\chi')=|\text{disc } K|^{d^2}\mathrm{N}(f(\chi\otimes\chi'))$. La propriété 1.2.28 concernant le conducteur d'Artin de la convolution de deux caractères permet d'obtenir $\ln q(\chi\otimes\chi')\leqslant d^2\ln|\text{disc } K|+d\big(\ln\mathrm{N}(f(\chi))+\ln\mathrm{N}(f(\chi'))\big)$. On utilise ensuite la proposition 2.5 de [MMS88] pour majorer indifféremment $\ln\mathrm{N}(f(\chi))$ et $\ln\mathrm{N}(f(\chi'))$ par $2d[K:\mathbb{Q}]\ln(M|G|)$.
Alors $\ln q(\chi\otimes\chi')\leqslant(1+4c_0)d^2\ln|\text{disc } K|\ln(M|G|)$ en utilisant $[K:\mathbb{Q}]\leqslant c_0\ln|\text{disc } K|$ puisque $K\neq\mathbb{Q}$ (voir par exemple [Odl77] ou [Odl90]).
La borne du théorème 3.1.1 devient donc

$$\frac{1}{\langle\chi,\chi\rangle^2}\Big(c_1d^2[K:\mathbb{Q}]+2(1+4c_0)c_2d^2\ln|\text{disc } K|\ln(M|G|)+c_3\langle\chi,\chi\rangle\Big)^2 \leqslant c_4\Big(d^2\ln|\text{disc } K|\ln(M|G|)\Big)^2.$$

Notons que si $P(L/K)=\emptyset$, autrement dit lorsque l'extension L/K est non ramifiée, $\mathrm{N}(f(\chi))=\mathrm{N}(f(\chi'))=1$. □

En ajoutant des conditions sur les conducteurs, une majoration des quantités en jeu permet de retrouver le résultat suivant :

Corollaire 3.1.4 ([RT14], Proposition 4.1)**.** *Sous les conditions du théorème 3.1.1 avec $\chi(1)=\chi'(1)=d$ et $q=\max(q(\chi),q(\chi'))$ avec $\ln q>d[K:\mathbb{Q}]$, les paramètres locaux, $\{\alpha_{i,\rho}(\mathfrak{p})\}_i$, en $\mathfrak{p}$ de $L(s,\chi)$ sont différents de ceux de $L(s,\chi')$ pour un idéal premier $\mathfrak{p}$ de norme plus petite que $c_5d^2\ln^2 q$, c_5 étant une constante réelle absolue.*

PREUVE
En effet, en utilisant les propriétés des conducteurs, on obtient :

$$q(\chi \otimes \overline{\chi}) = q(\chi \otimes \overline{\chi'}) \leqslant \Big(q(\chi)q(\chi')\Big)^d \leqslant q^{2d}$$

et le résultat découle de 3.1.1. □

Remarque 3.1.5. On peut rendre explicite la constante c_5 du résultat de Rouse et Thorne en utilisant le théorème 2.3.2. Alors :

$$c_5 = 4(1+2\ln 2)^2 \frac{51}{25}\left(86D_{0,\phi} + 2D_{1,\phi}\right)^2,$$

où ϕ est une fonction positive non nulle, $\mathscr{C}^\infty$, à support compact dans $[1,2]$,

$$D_{0,\phi} = \frac{1}{\|\phi\|_1}\int_1^2 |\phi''(x)|x^{3/2}\,\mathrm{d}x \text{ et } D_{1,\phi} = \frac{1}{\|\phi\|_1}\int_1^2 \frac{\phi(x)}{x}\,\mathrm{d}x.$$

Avec la fonction ϕ définie par $\phi(x) = \exp\left(\frac{-0,3}{(x-1)(2-x)}\right)$ sur $]1,2[$ et nulle ailleurs, on obtient :

$$c_5 \leqslant 9,8 \times 10^8.$$

3.2 Preuve du théorème 3.1.1

Soit (ρ, V) une représentation continue (complexe) de G_K de degré r et de caractère χ. Nous nous plaçons dans le cadre de fonctions L d'Artin. Par un argument topologique, on rappelle que le noyau $\mathrm{Ker}(\rho)$ est un sous-groupe ouvert de G_K et donc que l'image $\mathrm{Im}(\rho)$ de ρ est finie. Soit le corps de nombres $L = \overline{K}^{\mathrm{Ker}(\rho)}$; posons $G = \mathrm{Gal}(L/K)$. La représentation ρ se factorise à travers G.

Nous nous inspirons de l'article de Lagarias et Odlyzko [LO77], de Bellaïche [Bel] et du livre de Iwaniec et Kowalski [IK04].

Pour $x \in \mathbb{R}$, $x \geqslant 2$, et un caractère χ de G_K, posons :

$$\theta_1(x,\chi) = \sum_{\substack{\mathfrak{p} \\ \mathrm{N}(\mathfrak{p}) \leqslant x}} \sum_{i=1}^{d} \alpha_{i,\rho}(\mathfrak{p})(x - \mathrm{N}(\mathfrak{p}))\ln \mathrm{N}(\mathfrak{p}),$$

$$\psi_1(x,\chi) = \sum_{n \leqslant x} \Lambda_\chi(n)(x-n).$$

Comme dans la preuve du théorème 3 de [Bel], nous allons comparer ces deux fonctions.

Remarque 3.2.1. Le fait d'utiliser la fonction f définie par :

$$f :]0,+\infty[\to \mathbb{C}$$
$$t \mapsto \begin{cases} x-t & \text{si } t \leqslant x \\ 0 & \text{sinon} \end{cases}$$

plutôt que la fonction indicatrice sur l'ensemble des réels inférieurs à x (à la manière de [LO77]) va faire apparaître $\displaystyle\sum_\rho \frac{x^{1+\rho}}{\rho(\rho+1)}$ dont on connaît déjà une majoration (c'est le résultat du théorème 2.3.9), contrairement à $\displaystyle\sum_\rho \frac{x^\rho}{\rho}$.

Soit la fonction $\chi \mapsto r(\chi) = \langle \chi, \chi \rangle$ qui donne le nombre de fois où la représentation triviale intervient dans la décomposition de $\rho_{|L}$ en représentations irréductibles.

Lemme 3.2.2 ([Bel], lemme 6)**.** *Soit χ un caractère de G_K. En supposant que $L(s,\chi)$ satisfait l'hypothèse de Riemann et la conjecture d'Artin, la fonction $\psi_1(x,\chi)$ vérifie :*

$$\left|\psi_1(x,\chi) - \frac{1}{2}r(\chi)x^2\right| \leqslant c_6 x^{3/2}\big(\ln q(\chi) + \chi(1)[K:\mathbb{Q}] + r(\chi)\big).$$

<u>PREUVE</u>
L'utilisation de la transformée de Mellin dans l'égalité de la proposition 1.2.6, $-\dfrac{L'}{L}(s,\chi) = \displaystyle\sum_{n\geqslant 1} \Lambda_\chi(n) n^{-s}$, permet d'obtenir pour $x \in \mathbb{R}$, $x \geqslant 2$:

$$\psi_1(x,\chi) = \frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty} -\frac{L'}{L}(s,\chi)\,\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s.$$

En effet, on applique le résultat énoncé dans la proposition B.1.11 à la fonction f définie par :

$$\begin{aligned} f\ :\ ]0,+\infty[&\to \mathbb{C} \\ t &\mapsto \begin{cases} x-t & \text{si } t \leqslant x \\ 0 & \text{sinon} \end{cases} \end{aligned}$$

Rappelons (voir l'égalité ($\star$) page 45) l'existence d'une constante $b(\chi)$ telle que, sous la conjecture d'Artin, on a :

$$-\frac{L'}{L}(s,\chi) = \frac{1}{2}\ln q(\chi) + \frac{\gamma_\chi'}{\gamma_\chi}(s) - b(\chi) + \frac{r(\chi)}{s} + \frac{r(\chi)}{s-1} - \sum_{\rho\neq 0,1}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right),$$

où ρ varie parmi les zéros, différents de 0 et 1, de la fonction complétée $\Lambda(s,\chi)$.
La preuve suit celle due à Lagarias et Odlyzko dans [LO77] (ou encore [Win13]). On commence par appliquer le théorème de Cauchy en déplaçant la droite d'intégration vers la gauche (à l'infini). À la limite, sur les "trois" bords introduits, seule l'intégrale sur la droite initiale est non nulle. Ainsi $\psi_1(x,\chi)$ est la somme des résidus de $-\dfrac{L'}{L}(s,\chi)\dfrac{x^{s+1}}{s(s+1)}$ sur le demi-plan $\mathrm{Re}(s) \leqslant 2$.
Il reste alors à déterminer les résidus en jeu.
D'abord, il y a le pôle en $s = 1$ de la fonction $(L'/L)(s,\chi)$ d'ordre $r(\chi)$ dont le résidu vaut -1 qui donne donc ici $-r(\chi)x^2/2$.
Ensuite, à chaque zéro ρ de $\Lambda(s,\chi)$, $(L'/L)(s,\chi)$ a un pôle d'ordre 1, de résidu 1, cela donne donc une contribution en $\sum_\rho \frac{x^{1+\rho}}{\rho(\rho+1)}$. Sous l'hypothèse de Riemann, $\mathrm{Re}(\rho) = 1/2$. D'autre part, d'après le théorème 2.3.9, il vient :

$$\left|\sum_\rho \frac{x^{1+\rho}}{\rho(\rho+1)}\right| \leqslant x^{3/2}\sum_{\rho=1/2+it}\frac{1}{|\rho(\rho+1)|} \leqslant Cx^{3/2}(d[K:\mathbb{Q}] + \ln q(\chi) + r(\chi)).$$

La fonction $(L'/L)(s,\chi)$ possède également des pôles d'ordre 1 aux zéros triviaux et éventuellement en 0 (correspondant aux pôles de γ_χ) situés en $s = -2m-1$ et en $s = -2m$

pour $m \in \mathbb{N}$. En écrivant γ_χ sous la forme $\gamma_\chi(s) = \pi^{-sd[K:\mathbb{Q}]/2}\Gamma\left(\frac{s+1}{2}\right)^{\alpha[K:\mathbb{Q}]}\Gamma\left(\frac{s}{2}\right)^{\beta[K:\mathbb{Q}]}$, où $\alpha + \beta = d = \chi(1)$, on obtient pour les résidus des zéros triviaux la majoration :

$$\alpha[K:\mathbb{Q}]\sum_{m=1}^{+\infty}\frac{x^{-2m}}{2m(2m+1)} + \beta[K:\mathbb{Q}]\sum_{m=1}^{+\infty}\frac{x^{1-2m}}{2m(2m-1)} \leqslant xd[K:\mathbb{Q}]\ln 2.$$

Les résidus restants sont ceux en $s = 0$ et $s = -1$. La formule $\frac{\Gamma'}{\Gamma}(s) = \frac{\Gamma'}{\Gamma}(s+1) - \frac{1}{s}$ et les développements en séries de Laurent montrent qu'il existe des fonctions f_1 et g_1 analytiques en $s = 0$ ($g_1(s)$ dépend de χ) telles que :

$$\frac{x^{s+1}}{s(s+1)} = \frac{x}{s} + x\ln x - x + sf_1(s)$$

et

$$\frac{L'}{L}(s,\chi) = \frac{\beta[K:\mathbb{Q}] - r(\chi)}{s} + A(\chi) + sg_1(s),$$

avec

$$A(\chi) = b(\chi) - \frac{1}{2}\ln q(\chi) + \frac{d[K:\mathbb{Q}]}{2}\ln\pi + r(\chi) - \frac{\alpha[K:\mathbb{Q}]}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}\right) - \frac{\beta[K:\mathbb{Q}]}{2}\frac{\Gamma'}{\Gamma}(1).$$

Ainsi,

$$\mathrm{Res}(\frac{L'}{L}(s,\chi),0) = xA(\chi) + x(\ln x - 1)(\beta[K:\mathbb{Q}] - r(\chi)).$$

En $s = -1$, il existe des fonctions f_2 et g_2 analytiques en $s = -1$ ($g_2(s)$ dépend de χ) vérifiant :

$$\frac{x^{s+1}}{s(s+1)} = \frac{-1}{s+1} - 1 - \ln x + (s+1)f_2(s)$$

et

$$\frac{L'}{L}(s,\chi) = \frac{\alpha[K:\mathbb{Q}]}{s+1} + B(\chi) + (s+1)g_2(s),$$

avec

$$\begin{aligned} B(\chi) = b(\chi) &- \frac{1}{2}\ln q(\chi) + \frac{d[K:\mathbb{Q}]}{2}\ln\pi + \frac{3}{2}r(\chi) \\ &- \frac{\beta[K:\mathbb{Q}]}{2}\left(\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}\right) + 2\right) - \frac{\alpha[K:\mathbb{Q}]}{2}\frac{\Gamma'}{\Gamma}(1) + \sum_{\rho\neq 0,1}\frac{1}{\rho(\rho+1)}. \end{aligned}$$

D'où

$$\mathrm{Res}(\frac{L'}{L}(s,\chi),-1) = -B(\chi) - (\ln x + 1)\alpha[K:\mathbb{Q}].$$

On peut majorer ces derniers résidus par :

$$Cx\ln x\Big(d[K:\mathbb{Q}] + \ln q(\chi) + r(\chi)\Big)$$

notamment en utilisant la majoration de $b(\chi)$ donnée dans [Win13] page 12.
Finalement, puisque sur $\mathbb{R}_+^*$, $\ln x \leqslant \frac{1}{\alpha}\mathrm{e}^{-1}x^\alpha$ pour tout $\alpha \in \mathbb{R}_+^*$, on obtient :

$$|\psi_1(x,\chi) - \frac{1}{2}r(\chi)x^2| \leqslant c_6 x^{3/2}\Big(d[K:\mathbb{Q}] + \ln q(\chi) + r(\chi)\Big).$$

□

PROPOSITION 3.2.3. *Soit χ un caractère de G_K. Alors, en supposant vraie l'hypothèse de Riemann généralisée et la conjecture d'Artin pour $L(s,\chi)$, il vient :*

$$\left|\theta_1(x,\chi) - \frac{1}{2}r(\chi)x^2\right| \leqslant x^{3/2}\Big(c_7\chi(1)[K:\mathbb{Q}] + c_8 \ln q(\chi) + c_9 r(\chi)\Big).$$

PREUVE

Commençons par estimer la différence entre θ_1 et ψ_1 :

$$\begin{aligned}
|\theta_1(x,\chi) - \psi_1(x,\chi)| &= \Big|\sum_{\substack{\mathfrak{p},k\geqslant 2\\ \mathrm{N}(\mathfrak{p})^k\leqslant x}} \sum_{i=1}^{d} \alpha_{i,\rho}(\mathfrak{p})^k (x - \mathrm{N}(\mathfrak{p})^k)\ln \mathrm{N}(\mathfrak{p})\Big| \\
&\leqslant x \sum_{\substack{\mathfrak{p},k\geqslant 2\\ \mathrm{N}(\mathfrak{p})^k\leqslant x}} \sum_{i=1}^{d} |\alpha_{i,\rho}(\mathfrak{p})|^k \ln \mathrm{N}(\mathfrak{p}) \\
&\leqslant dx \sum_{\substack{\mathfrak{p},k\geqslant 2\\ \mathrm{N}(\mathfrak{p})^k\leqslant x}} \ln \mathrm{N}(\mathfrak{p}) \qquad \text{car } |\alpha_{i,\rho}(\mathfrak{p})| \leqslant 1 \\
&\leqslant dx \sum_{k\geqslant 2} \sum_{\substack{\mathfrak{p}\\ \mathrm{N}(\mathfrak{p})\leqslant x^{1/k}}} \ln \mathrm{N}(\mathfrak{p}).
\end{aligned}$$

Notons $\mathfrak{p}_1,\cdots,\mathfrak{p}_g$ les g idéaux premiers de $\mathscr{O}_K$ au-dessus d'un nombre premier p et f_i leur degré résiduel respectif. Alors

$$\begin{aligned}
|\theta_1(x,\chi) - \psi_1(x,\chi)| &\leqslant dx \sum_{k\geqslant 2} \sum_{p\leqslant x^{1/k}} \sum_{i=1}^{g} \ln \mathrm{N}(\mathfrak{p}_i) \\
&\leqslant dx \sum_{k\geqslant 2} \sum_{p\leqslant x^{1/k}} \ln p \sum_{i=1}^{g} f_i \\
&\leqslant dx[K:\mathbb{Q}] \sum_{k\geqslant 2} \sum_{p\leqslant x^{1/k}} \ln p \\
&\leqslant dx[K:\mathbb{Q}] \sum_{2\leqslant k\leqslant \frac{\ln x}{\ln 2}} \sum_{p\leqslant x^{1/k}} \ln p \text{ (pour les entiers } k \text{ supérieurs : } x^{1/k} < 2)
\end{aligned}$$

En découpant l'intervalle de sommation, il vient :

$$|\theta_1(x,\chi) - \psi_1(x,\chi)| \leqslant xd[K:\mathbb{Q}]\Big(\Delta(2) + \cdots + \Delta(m)\Big),$$

où

$$\Delta(i) = \sum_{p\leqslant x^{1/i}} \ln p\ ,$$

et où $m = \lfloor \ln x/\ln 2\rfloor$.

Il est ensuite bien connu (voir par exemple [Ten95], corollaire 8.1) que

$$\sum_{p\leqslant x} \ln p \leqslant c_{10}x$$

et ainsi $\Delta(i) \leqslant c_{10}x^{1/i}$. On obtient alors :

$$\begin{aligned}|\theta_1(x,\chi)-\psi_1(x,\chi)| &\leqslant c_{10}xd[K:\mathbb{Q}]\Big(x^{1/2}+(m-1)\Delta(3)\Big)\\ &\leqslant c_{10}xd[K:\mathbb{Q}]\Big(x^{1/2}+x^{1/3}\ln x\Big)\\ &\leqslant 2c_{10}x^{3/2}d[K:\mathbb{Q}].\end{aligned}$$

Finalement, grâce au lemme 3.2.2, on peut conclure :

$$\begin{aligned}\left|\theta_1(x,\chi)-\tfrac{1}{2}r(\chi)x^2\right| &\leqslant |\theta_1(x,\chi)-\psi_1(x,\chi)|+\left|\psi_1(x,\chi)-\tfrac{1}{2}r(\chi)x^2\right|\\ &\leqslant 2c_{10}x^{3/2}d[K:\mathbb{Q}]+c_6x^{3/2}\Big(d[K:\mathbb{Q}]+\ln q(\chi)+r(\chi)\Big)\\ &\leqslant x^{3/2}\Big(c_7d[K:\mathbb{Q}]+c_8\ln q(\chi)+c_9r(\chi)\Big).\end{aligned}$$

avec $c_7 = 2c_{10}+c_6$, $c_8 = c_9 = c_6$. □

<u>Preuve du théorème 3.1.1</u>
La preuve repose sur le fait bien connu suivant : pour deux caractères distincts χ et χ' de produit scalaire nul, il vient $r(\chi\otimes\overline{\chi'}) = 0$ et $r(\chi\otimes\overline{\chi}) = r \geqslant 1$. On applique ensuite la proposition 3.2.3 aux caractères $\chi\otimes\overline{\chi'}$ et $\chi\otimes\overline{\chi}$ pour obtenir, pour tout $x\in\mathbb{R}_+$:

$$\begin{aligned}&\left|\theta_1(x,\chi\otimes\overline{\chi'})\right| \leqslant x^{3/2}\Big[c_7\chi(1)\chi'(1)[K:\mathbb{Q}]+c_8\ln q(\chi\otimes\overline{\chi'})\Big]\\ &\left|\theta_1(x,\chi\otimes\overline{\chi})-\frac{1}{2}rx^2\right| \leqslant x^{3/2}\Big[c_7\chi(1)\chi'(1)[K:\mathbb{Q}]+c_8\ln q(\chi\otimes\overline{\chi})+c_9r\Big].\end{aligned}$$

Il reste à montrer l'existence d'un réel x tel que $\theta_1(x,\chi\otimes\overline{\chi'}) \neq \theta_1(x,\chi\otimes\overline{\chi})$; on aura alors bien l'existence d'un idéal premier $\mathfrak{p}$ de K de norme plus petite que x tel que $\sum_{i=1}^d \alpha_{i,\rho\otimes\overline{\rho'}}(\mathfrak{p}) \neq \sum_{j=1}^d \alpha_{j,\rho\otimes\overline{\rho}}(\mathfrak{p})$, autrement dit vérifiant $(\chi\otimes\overline{\chi'})(\sigma_\mathfrak{p}) \neq (\chi\otimes\overline{\chi})(\sigma_\mathfrak{p})$, c'est-à-dire $\chi'(\sigma_\mathfrak{p}) \neq \chi(\sigma_\mathfrak{p})$.
Notons

$$Z_1 = c_7\chi(1)\chi'(1)[K:\mathbb{Q}]+c_8\ln q(\chi\otimes\overline{\chi'})$$

et

$$Z_2 = c_7\chi(1)\chi'(1)[K:\mathbb{Q}]+c_8\ln q(\chi\otimes\overline{\chi})+c_9r.$$

Choisissons x_0 assez grand tel que $r^2x_0 > 4(Z_1+Z_2)^2$ (ainsi $\frac{1}{2}r\sqrt{x_0} > Z_1+Z_2$ donc $\frac{1}{2}r\sqrt{x_0}-Z_1 > Z_2$). Supposons $\theta_1(x_0,\chi\otimes\overline{\chi'}) = \theta_1(x_0,\chi\otimes\overline{\chi}) = A$. Alors on a : $|A| \leqslant x_0^{3/2}Z_1$ et $|A-\frac{1}{2}rx_0^2| \leqslant x_0^{3/2}Z_2$ donc $\frac{1}{2}rx_0^2 - A \geqslant \frac{1}{2}rx_0^2 - x_0^{3/2}Z_1 = x_0^{3/2}(\frac{1}{2}r\sqrt{x_0}-Z_1) > x_0^{3/2}Z_2$, d'où la contradiction. Ainsi, $\theta_1(x_0,\chi\otimes\overline{\chi'}) \neq \theta_1(x_0,\chi\otimes\overline{\chi})$. □

3.3 Application aux polynômes

Commençons par fixer un cadre pour cette partie.

3.3.1 Cadre

Soit $P\in\mathbb{Z}[X]$ un polynôme unitaire et $\mathbb{Q}$-irréductible et soit M un corps de rupture de P de clôture galoisienne L (autrement dit, L est le corps de décomposition de P). Supposons que $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_n$; soit $K/\mathbb{Q}$ l'unique sous-extension quadratique de $L/\mathbb{Q}$, en fait $K = \mathbb{Q}(\sqrt{\mathrm{disc}\ P})$ et le groupe de Galois de L/K est isomorphe au groupe alterné A_n.

Soit p un nombre premier non ramifié dans L/K ; notons par $\mathfrak{P}$ un idéal de L au-dessus de p et posons $\mathfrak{p} = \mathscr{O}_K \cap \mathfrak{P}$. Remarquons que deux cas se distinguent : soit p est ramifié et alors le degré de ramification $e(\mathfrak{P}/p) = e(\mathfrak{p}/p) = 2$ (puisque p est non ramifié dans L/K) ; soit p est non ramifié. On note $\sigma_p = \mathrm{Frob}(\mathfrak{P}/p)$ (au sens de la définition donnée dans la partie B.1.3) et $\sigma_{\mathfrak{p}} = \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$.
Soit $p\mathscr{O}_M = \mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{p}_{s+1}^2 \cdots \mathfrak{p}_g^2$ la décomposition de p dans M avec e_i et f_i les indices de ramification et degrés résiduels associés. Remarquons l'égalité : $\sum_{i=1}^{g} e_i f_i = \deg(P)$.
Lorsque $\mathscr{O}_M = \mathbb{Z}[\theta]$, avec θ une racine de P dans $\overline{\mathbb{Q}}$, de façon équivalente, on peut écrire $P = Q_{f_1}^{e_1} \cdots Q_{f_g}^{e_g} \in \mathbb{F}_p[X]$ où les polynômes Q_{f_i} sont des polynômes $\mathbb{Q}$-irréductibles de degré f_i et premiers entre eux. De plus, on a la correspondance $P = P_1 \cdots P_g \in \mathbb{Q}_p[X]$ avec $\deg P_i = e_i f_i$ (voir [Hal97], théorème 3 page 14).

3.3.2 Expression du Frobenius sous forme de cycles

Localisons le problème en nous plaçant dans $\mathbb{Q}_p$. On prolonge la valuation p-adique par rapport à l'idéal $\mathfrak{P}$. On complète le corps de nombres L par rapport à la valuation obtenue pour obtenir $L_{\mathfrak{P}}$. Si l'on note $(\alpha_j^{(i)})_j$ les racines de P_i dans $\overline{\mathbb{Q}_p}$ (d'où $P_i = \mathrm{Irr}(\alpha_j^{(i)}, \mathbb{Q}_p)$), alors $L_{\mathfrak{P}}$ correspond à l'extension $\mathbb{Q}_p(\alpha_1^{(1)}, \ldots, \alpha_{e_1 f_1}^{(1)}, \ldots, \alpha_1^{(m)}, \ldots, \alpha_{e_m f_m}^{(m)})$ de $\mathbb{Q}_p$. De la même façon, on note $K_{\mathfrak{p}} = \mathbb{Q}_p(\sqrt{\mathrm{disc}\ P})$. L'extension galoisienne $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est une extension non ramifiée de groupe de Galois isomorphe à un sous-groupe de A_n : en effet, $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ est isomorphe au groupe de décomposition de $\mathfrak{P}/\mathfrak{p}$ dans l'extension L/K (de groupe de Galois isomorphe à A_n) car $\mathfrak{p}$ est non ramifié dans cette extension, autrement dit $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) =< \sigma_{\mathfrak{p}} >$.

THÉORÈME 3.3.1. *Lorsque $p\mathscr{O}_M = \mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{p}_{s+1}^2 \cdots \mathfrak{p}_g^2$ avec f_i les degrés résiduels associés, on a :*

- *lorsque p est non ramifié dans $K/\mathbb{Q}$, le Frobenius $\sigma_{\mathfrak{p}}$ s'écrit $([f_1] \cdots [f_g])^{f(\mathfrak{p}/p)}$, où $f(\mathfrak{p}/p)$ représente le degré résiduel de $\mathfrak{p} \subset \mathscr{O}_K$ au-dessus de p et $[f_i]$ correspond à un f_i-cycle ;*
- *lorsque p est ramifié dans $K/\mathbb{Q}$, $\sigma_{\mathfrak{p}}$ peut s'écrire $[f_1'] \cdots [f_t']$ avec $f_i' = f_i$ ou $2f_i$ correspondant aux degrés résiduels de la décomposition de p dans $\mathscr{O}_{M(\sqrt{\mathrm{disc}\ P})}$.*

<u>PREUVE</u>

Précisons donc la décomposition en produit de cycles de $\sigma_{\mathfrak{p}}$.

Premier cas : le premier p est non ramifié dans $K/\mathbb{Q}$.
Partons d'une racine $\alpha_1^{(1)}$ de P_1 : puisque p est non ramifié dans $K/\mathbb{Q}$, il est non ramifié dans $L/\mathbb{Q}$ et donc $[\mathbb{Q}_p(\alpha_1^{(1)}) : \mathbb{Q}_p] = e(\mathfrak{q}/p)f(\mathfrak{q}/p) = f(\mathfrak{q}/p) = f_1 = \deg(P_1)$, où $\mathfrak{q}$ représente un idéal premier de $\mathbb{Q}_p(\alpha_1^{(1)})$ au-dessus de p. Ainsi, les corps de rupture et de décomposition sont égaux : $\mathbb{Q}_p(\alpha_1^{(1)}) = \mathbb{Q}_p(\alpha_1^{(1)}, \cdots, \alpha_{f_1}^{(1)})$. L'extension $\mathbb{Q}_p(\alpha_1^{(1)})/\mathbb{Q}_p$ étant cyclique (puisque toute extension non ramifiée de $\mathbb{Q}_p$ est contenue dans une extension cyclique), son groupe de Galois est engendré par un cycle de longueur $f_1 = \deg(P_1)$. Maintenant, connaître le groupe de Galois de $L_{\mathfrak{P}}/\mathbb{Q}_p$ c'est connaître son action sur les différentes racines de P. Comme l'action de $\mathrm{Gal}(L/\mathbb{Q})$ sur $\alpha_1^{(i)}$ s'exprime comme un cycle de longueur f_i (car le groupe de Galois agit sur les racines de chaque polynôme irréductible) et que les différents cycles provenant des racines de P sont à supports disjoints, le groupe de Galois de $L_{\mathfrak{P}}/\mathbb{Q}_p$ est engendré par un produit de f_i-cycles à supports disjoints que nous notons σ. La conclusion dépend alors de l'extension $\mathbb{Q}_p(\sqrt{\mathrm{disc}\ P})/\mathbb{Q}_p$: si l'extension n'est pas triviale, le groupe $\mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p(\sqrt{\mathrm{disc}\ P}))$ est engendré par σ^2 (seul

$$\begin{tikzcd}
 & \mathbb{Q}_p(\sqrt{\operatorname{disc} P}, \alpha_1^{(1)}) \arrow[dr, dash] & \\
\mathbb{Q}_p(\sqrt{\operatorname{disc} P}) \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{Q}_p^{\text{n.r.}} \arrow[dl, dash, bend left] \\
 & \mathbb{Q}_p(\alpha_1^{(1)}) \arrow[ur, dash] \arrow[dr, dash] & \\
 & \mathbb{Q}_p \arrow[ur, dash, bend left] \arrow[uur, dash, bend right, "\text{cycl. non ram.}"'] &
\end{tikzcd}$$

élément de degré $f_1 f_2 \cdots f_g/2$ dans le groupe cyclique) ; sinon, le groupe de Galois de $L_{\mathfrak{P}}/\mathbb{Q}_p(\sqrt{\operatorname{disc} P})$ est le même que celui de $L_{\mathfrak{P}}/\mathbb{Q}_p$, il est donc engendré par σ.
En résumé, le Frobenius de $\mathfrak{p}$ dans $\operatorname{Gal}(L/K)$ s'écrit sous la forme $([f_1] \cdots [f_g])^{f(\mathfrak{p}/p)}$ puisque $[\mathbb{Q}_p(\sqrt{\operatorname{disc} P}) : \mathbb{Q}_p] = f(\mathfrak{p}/p)$.

Second cas : le premier p est ramifié dans $K/\mathbb{Q}$.
Il vient la tour d'extensions $\mathbb{Q}_p \subset K_{\mathfrak{p}} \subset L_{\mathfrak{P}}$ où $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est une extension non ramifiée de degré $f = f(\mathfrak{P}/\mathfrak{p})$ (en effet, $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$, voir par exemple [Hal97] page 13 ou [Ser68], chapitre II, §3 théorème 1) et $K_{\mathfrak{p}}/\mathbb{Q}_p$ est ramifiée. Par unicité d'une extension cyclique non ramifiée, le corps $L_{\mathfrak{P}}$ s'obtient par le compositum de $K_{\mathfrak{p}}/\mathbb{Q}_p$ avec une extension non ramifiée de $L_{\mathfrak{P}}/\mathbb{Q}_p$ (donc cyclique) de degré $f = \operatorname{ppcm}(f_i, i = 1, \cdots, g)$ et ainsi $\operatorname{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/f\mathbb{Z}$. En particulier, $\operatorname{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ agit trivialement sur $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) =< \sigma_{\mathfrak{p}} >$.
Comme p est non ramifié dans L/K, il vient la décomposition $p\mathscr{O}_M = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s\mathfrak{p}_{s+1}^2 \ldots \mathfrak{p}_g^2$, où chaque premier $\mathfrak{p}_i$ est de degré résiduel f_i. Pour $1 \leqslant i \leqslant s$, le groupe de Galois de P_i est simplement un cycle de longueur f_i. Pour $s+1 \leqslant i \leqslant g$: si $\mathbb{Q}_p(\sqrt{\operatorname{disc} P}) \not\subseteq \mathbb{Q}_p(\alpha_1^{(i)})$ alors $\deg(\operatorname{Irr}(\alpha_1^{(i)}, \mathbb{Q}_p(\sqrt{\operatorname{disc} P}))) = [\mathbb{Q}_p(\alpha_1^{(i)}, \sqrt{\operatorname{disc} P}) : \mathbb{Q}_p(\sqrt{\operatorname{disc} P})] = [\mathbb{Q}_p(\alpha_1^{(i)}) : \mathbb{Q}_p]$ et $[\mathbb{Q}_p(\alpha_1^{(i)}) : \mathbb{Q}_p] = \deg P_i = 2f_i$ d'où le polynôme P_i reste irréductible sur $\mathbb{Q}_p(\sqrt{\operatorname{disc} P})$ et donc le groupe de Galois de l'extension $\mathbb{Q}_p(\alpha_1^{(i)}, \sqrt{\operatorname{disc} P})/\mathbb{Q}_p(\sqrt{\operatorname{disc} P})$ est engendré par un $(2f_i)$-cycle.

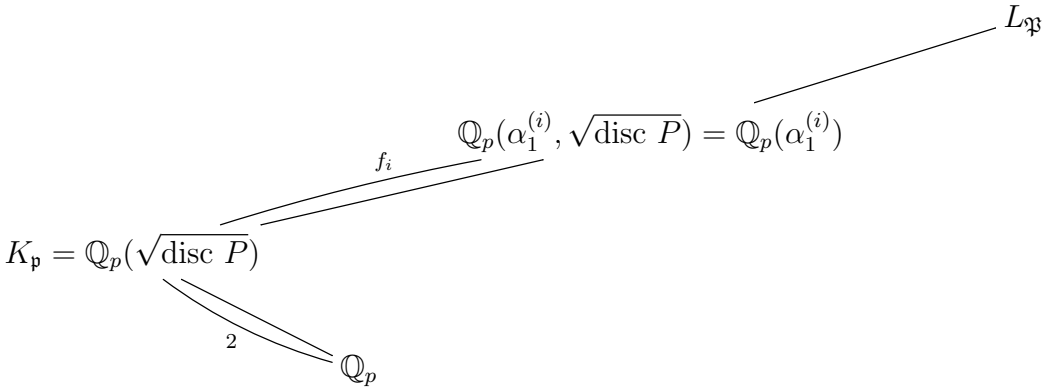
$$\begin{tikzcd}
 & \mathbb{Q}_p(\alpha_1^{(i)}, \sqrt{\operatorname{disc} P}) \\
K_{\mathfrak{p}} = \mathbb{Q}_p(\sqrt{\operatorname{disc} P}) \arrow[ur, dash, bend left, "2f_i"] \arrow[ur, dash, bend right] \arrow[dr, dash] & \\
 & \mathbb{Q}_p(\alpha_1^{(i)}) \\
 & \mathbb{Q}_p \arrow[u, dash, bend left, "2f_i"] \arrow[u, dash, bend right]
\end{tikzcd}$$

Cas $\mathbb{Q}_p(\sqrt{\operatorname{disc} P}) \not\subseteq \mathbb{Q}_p(\alpha_1^{(i)})$

Dans le cas où $\mathbb{Q}_p(\sqrt{\text{disc } P}) \subseteq \mathbb{Q}_p(\alpha_1^{(i)})$, on a :

$$\begin{aligned}\deg(\mathrm{Irr}(\alpha_1^{(i)}, \mathbb{Q}_p(\sqrt{\text{disc } P}))) &= [\mathbb{Q}_p(\alpha_1^{(i)}, \sqrt{\text{disc } P}) : \mathbb{Q}_p(\sqrt{\text{disc } P})] \\ &= \frac{[\mathbb{Q}_p(\alpha_1^{(i)}, \sqrt{\text{disc } P}) : \mathbb{Q}_p]}{[\mathbb{Q}_p(\sqrt{\text{disc } P}) : \mathbb{Q}_p]} = \frac{[\mathbb{Q}_p(\alpha_1^{(i)}) : \mathbb{Q}_p]}{2} = f_i.\end{aligned}$$

Le polynôme P_i se décompose donc en un produit de deux polynômes de degré f_i sur $\mathbb{Q}_p(\sqrt{\text{disc } P})$ et le groupe de Galois de l'extension $\mathbb{Q}_p(\alpha_1^{(i)}, \sqrt{\text{disc } P})/\mathbb{Q}_p(\sqrt{\text{disc } P})$ est engendré par un produit de deux f_i-cycles.



Cas $\mathbb{Q}_p(\sqrt{\text{disc } P}) \subseteq \mathbb{Q}_p(\alpha_1^{(i)})$

Notons que toutes ces informations peuvent se lire dans le corps $M(\sqrt{\text{disc } P})$. En effet, puisque l'extension $L/\mathbb{Q}(\sqrt{\text{disc } P})$ est non ramifiée, le degré de ramification dans l'extension $L/\mathbb{Q}$ est égal à celui dans $\mathbb{Q}(\sqrt{\text{disc } P})/\mathbb{Q}$ qui vaut 2 (car galoisien). De même, ce degré revient au degré de ramification de $M(\sqrt{\text{disc } P})/\mathbb{Q}$ donc la décomposition de p dans $\mathscr{O}_{M(\sqrt{\text{disc } P})}$ s'écrit : $p\mathscr{O}_{M(\sqrt{\text{disc } P})} = \mathfrak{q}_1^2 \dots \mathfrak{q}_t^2$, avec $f_i' = f_i$ pour $1 \leqslant i \leqslant s$ et $f_i' = f_i$ ou $2f_i$ pour $s+1 \leqslant i \leqslant g$. Alors le cas où $f_i' = f_i$ correspond à un polynôme de $\mathscr{O}_M$ se décomposant en un produit de deux polynômes dans $\mathscr{O}_{M(\sqrt{\text{disc } P})}$ tandis que $f_i' = 2f_i$ correspond au cas où le polynôme P_i reste premier dans $\mathscr{O}_{M(\sqrt{\text{disc } P})}$. Comme nous l'avons vu, chaque idéal premier $\mathfrak{p}_i$ correspond au polynôme P_i, les degrés résiduels de p dans $\mathscr{O}_{M(\sqrt{\text{disc } P})}$ nous donnent donc l'information cherchée. □

3.3.3 Cas particulier : quand disc P est le discriminant d'un corps quadratique

Nous allons préciser le cas où p est ramifié dans $K/\mathbb{Q}$ quand le discriminant du polynôme considéré est celui d'un corps quadratique. Commençons par rappeler le résultat suivant de Kondo qui nous ramène dans le contexte de la partie précédente. Notons que dans le théorème suivant, le corps K est égal à $\mathbb{Q}(\sqrt{\text{disc } P})$.

THÉORÈME 3.3.2 ([Kon95], Theorem 1)**.** *Si le discriminant d'un polynôme P de degré n sur $\mathbb{Q}$ est le discriminant d'un corps quadratique K, alors le groupe de Galois de la clôture galoisienne $L/\mathbb{Q}$ de P est isomorphe au groupe symétrique S_n et l'extension L/K est non ramifiée de groupe de Galois isomorphe à A_n.*

La preuve utilise le fait que le groupe de Galois de $L/\mathbb{Q}$ est un sous-groupe primitif de S_n qui contient une transposition : c'est donc le groupe S_n.

Nous avons ensuite besoin du lemme suivant :

Lemme 3.3.3. *Partons d'un polynôme $P \in \mathbb{Z}[X]$ $\mathbb{Q}$-irréductible unitaire dont le discriminant est le discriminant d'un corps quadratique. Soit $M = \mathbb{Q}(\theta)$ un corps de rupture de P, ici θ est une racine de P dans $\overline{\mathbb{Q}}$. Alors $\mathscr{O}_M = \mathbb{Z}[\theta]$.*

Preuve
Puisque disc P est le discriminant d'un corps quadratique, il s'écrit avec d un entier sans facteurs carrés : disc $P = d$ avec $d \equiv 1 (\mathrm{mod}\ 4)$ ou $4d$ avec $d \equiv 2$ ou $3 (\mathrm{mod}\ 4)$. D'autre part, il existe $a \in \mathbb{N}^*$ tel que disc $P = a^2$disc M. On en déduit alors $a = 1$ ou $a = 2$. Par ailleurs, on sait que disc $M \equiv 0, 1 (\mathrm{mod}\ 4)$ (c'est le critère de Stickelberger, voir par exemple [Lan94] ou [Nar74] page 59). Ainsi, $a = 1$ et donc disc M = disc P, d'où le résultat. □

Rappelons maintenant le lemme bien connu suivant (voir par exemple le théorème 2 de [Kon95]).

Lemme 3.3.4. *Pour un polynôme $P \in \mathbb{Z}[X]$ $\mathbb{Q}$-irréductible unitaire dont le discriminant est le discriminant d'un corps quadratique, lorsque le premier p divise* disc P *il vient $p\mathscr{O}_M = \mathfrak{p}_1 \cdots \mathfrak{p}_{g-1}\mathfrak{p}_g^2$ avec $f_g = 1$. Ou de façon équivalente, par la décomposition des idéaux puisque $\mathscr{O}_M = \mathbb{Z}[\theta]$, sur $\mathbb{F}_p$ le polynôme P se factorise de la manière suivante :*

$$P = Q_{f_1} \cdots Q_{f_{g-1}} (X - x_0)^2 \ \in \mathbb{F}_p[X],$$

où les polynômes Q_{f_i} sont des polynômes $\mathbb{Q}$-irréductibles de degré f_i et premiers entre eux.

Proposition 3.3.5. *Soit $P \in \mathbb{Z}[X]$ un polynôme $\mathbb{Q}$-irréductible unitaire dont le discriminant est le discriminant d'un corps quadratique et p un premier ramifié de degrés résiduels $(f_i)_{1 \leqslant i \leqslant g}$ dans $\mathscr{O}_M$. Le Frobenius $\sigma_{\mathfrak{p}}$ dans* $\mathrm{Gal}(L/K)$ *est soit (conjugué à) $\vartheta = [f_1] \cdots [f_{g-1}]$, soit le produit $\vartheta \cdot \tau$, où τ est une transposition à support disjoint de ϑ, le choix se faisant selon la signature de la permutation ϑ. Avec α une racine du polynôme P_g de degré 2 apparaissant dans la décomposition de P dans $\overline{\mathbb{Q}_p}$, on a : $\mathbb{Q}_p(\sqrt{\mathrm{disc}\ P}) = \mathbb{Q}_p(\alpha)$ si et seulement si $\varepsilon(\vartheta) = +1$.*

Preuve
Soit p un premier ramifié. D'après le lemme 3.3.4, $p\mathscr{O}_{M(\sqrt{\mathrm{disc}\ P})} = \mathfrak{q}_1^2 \ldots \mathfrak{q}_t^2$ ($t = g$ ou $g+1$) avec $f'_i = f_i$ pour $1 \leqslant i \leqslant g-1$ et $f'_g = 1$ ou 2. D'après le paragraphe 3.3.2, si l'on note par ϑ le produit de f_i-cycles à supports disjoints, $i = 1, \cdots, g-1$, alors le Frobenius $\sigma_{\mathfrak{p}}$ dans $\mathrm{Gal}(L/K)$ est soit (conjugué à) ϑ, soit le produit $\vartheta \cdot \tau$, où τ est une transposition à support disjoint de ϑ. Par ailleurs, en utilisant $\mathscr{O}_M \simeq \mathbb{Z}[X]/(P)$, on écrit $P = P_1 \cdots P_g$ dans $\mathbb{Q}_p[X]$ avec $\deg P_i = e_i f_i$, autrement dit $\deg P_i = f_i$ pour $1 \leqslant i \leqslant g-1$ et $\deg P_g = 2$. Soit α une racine de P_g dans $\overline{\mathbb{Q}_p}$. Comme nous l'avons vu dans la preuve du théorème 3.3.1, pour obtenir l'écriture du Frobenius, nous devons savoir si $\mathbb{Q}_p(\sqrt{\mathrm{disc}\ P})$ correspond à l'extension $\mathbb{Q}_p(\alpha)$ ou non. À ce niveau, utilisons la globalité de la situation : $\sigma_{\mathfrak{p}} \in A_n$ donc la signature $\varepsilon(\vartheta)$ de l'élément ϑ permet de conclure. □

Exemple 3.3.6. Soit le polynôme $P = X^{11} + X + 123$ de discriminant disc $P = -\ell$ avec $\ell = 22613649218372985685884825021253 9$ un nombre premier. Ainsi, la factorisation de $P \in \mathbb{F}_\ell[X]$ donne la décomposition de $\ell\mathscr{O}_M$. Ici, $P = (Q_1^{(1)})^2\ Q_1^{(2)}\ Q_1^{(3)}\ Q_7 \in \mathbb{F}_\ell[X]$, où les polynômes $Q_1^{(i)}$ sont des polynômes de degré 1 et où Q_7 est un polynôme $\mathbb{Q}$-irréductible de degré 7. La permutation ϑ est donc un 7-cycle et $\mathbb{Q}_\ell(\sqrt{\mathrm{disc}\ P}) = \mathbb{Q}_\ell(\alpha)$, où α est une racine de P dans $\overline{\mathbb{Q}_\ell}$ (selon les notations précédentes).

Notons alors que le groupe de décomposition de ℓ dans $L/\mathbb{Q}$ est cyclique, isomorphe à $\mathbb{Z}/14\mathbb{Z}$. Les autres premiers sont non ramifiés, leurs groupes de décomposition sont donc cycliques. Cet exemple donne une réponse pour S_{11} à la *Question arithmétique* de Bubbolini et Sonn, §1 de [BS15]. Nous retrouvons le même phénomène pour le groupe S_{19} avec le polynôme $P = X^{19} + X + 191$.

Exemple 3.3.7. Soit le polynôme $P = X^5 + X + 5$ de discriminant disc $P = 3 \cdot 651\ 127$. Sur $\mathbb{F}_3$, la factorisation de P est de la forme $(X - x_0)^2 Q_3$; ainsi $\varepsilon(\vartheta) = +1$.
Sur $\mathbb{F}_{651\ 127}$, la factorisation de P est de la forme $(X - x_0)^2 Q_1 Q_2$; ainsi $\varepsilon(\vartheta) = -1$. Pour ce second nombre premier $\ell = 651\ 127$, on remarque que le groupe de décomposition de ℓ dans $L/\mathbb{Q}$ est isomorphe au groupe de Klein (voir preuve du théorème 3.3.1 dans le cas ramifié).

3.3.4 Écriture du Frobenius séparant les caractères conjugués du groupe alterné

Si nous regardons tout spécialement la restriction au groupe alterné A_n des caractères irréductibles auto-conjugués du groupe symétrique S_n (voir la partie B.2.4 pour la définition), on obtient les résultats suivants :

PROPOSITION 3.3.8. *Lorsque le discriminant du polynôme P est le discriminant d'un corps quadratique, si $\sigma_{\mathfrak{p}}$, $\mathfrak{p}|p$, sépare un couple de caractères conjugués (χ, χ') alors le premier p est décomposé dans $K = \mathbb{Q}(\sqrt{\text{disc } P})/\mathbb{Q}$; en particulier, p n'est pas ramifié. De plus, lorsque p est décomposé, la factorisation de $P \in \mathbb{F}_p[X]$ s'écrit*

$$P = P_{f_1} \cdots P_{f_g} (\text{mod } p),$$

où les polynômes $P_{f_i} \in \mathbb{F}_p[X]$ sont irréductibles (distincts) de degré f_i si et seulement si le Frobenius $\sigma_{\mathfrak{p}}$ (dans A_n) est en produit de f_i-cycles à supports disjoints.

PREUVE
L'hypothèse sur le discriminant de P permet de nous placer dans le cadre fixé.
Ensuite, d'après la proposition B.2.20, le Frobenius $\sigma_{\mathfrak{p}}$ séparant un couple de caractères conjugués appartient à une classe de conjugaison de S_n qui se décompose dans A_n. Or, dans la situation locale du cas où le premier p est ramifié de la preuve du théorème 3.3.1, nous avons vu que $\text{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ agit trivialement sur $\text{Gal}(L_{\mathfrak{P}}/K_p) =< \sigma_{\mathfrak{p}} >$. En retournant à la situation globale, cela indique donc que la classe de conjugaison de $\sigma_{\mathfrak{p}} \in A_n$ est stable par la conjugaison de toute transposition et donc que cette classe ne provient pas d'une classe de S_n qui se décompose dans A_n. Il reste alors le cas p non ramifié. Pour deux idéaux premiers $\mathfrak{P}_1$ et $\mathfrak{P}_2$ de L au-dessus de p (on sait qu'il existe $\tau \in S_n$ tel que $\tau(\mathfrak{P}_1) = \mathfrak{P}_2$), les Frobenius $\text{Frob}(\mathfrak{P}_i/p)$ sont conjugués dans S_n (d'après la propriété 2. des propriétés B.1.14). Or :

- si p est inerte dans $K/\mathbb{Q}$, il n'y a qu'un seul idéal premier $\mathfrak{p}$ de $\mathscr{O}_K$ au-dessus de p, les Frobenius $\text{Frob}(\mathfrak{P}_i/p)$ sont finalement conjugués dans A_n (puisque les idéaux premiers $\mathfrak{P}_i$ le sont).
- si p est décomposé (autrement dit p n'est ni ramifié ni inerte), il y a alors deux idéaux premiers $\mathfrak{p}_1$ et $\mathfrak{p}_2$ dans K au-dessus de p. En notant $(\mathfrak{P}_i^j)_j$ les différents idéaux premiers de L au-dessus de $\mathfrak{p}_i$, $i = 1$ ou 2, on a : $\text{Frob}(\mathfrak{P}_i^j/p) = \text{Frob}(\mathfrak{P}_i^j/\mathfrak{p}_i)$, d'après la propriété 3. des propriétés B.1.14. Il existe $\sigma \in S_n \backslash A_n$ tel que : $\sigma(\mathfrak{P}_1^j) = \mathfrak{P}_2^k$. Ainsi, grâce à 2. des propriétés B.1.14, il vient :

$$\text{Frob}(\mathfrak{P}_2^k/\mathfrak{p}_2) = \text{Frob}(\mathfrak{P}_2^k/p) = \sigma \text{Frob}(\mathfrak{P}_1^j/p)\sigma^{-1} = \sigma \text{Frob}(\mathfrak{P}_1^j/\mathfrak{p}_1)\sigma^{-1}.$$

Par conséquent, le nombre premier p est décomposé dans $K/\mathbb{Q}$.
L'équivalence se déduit ensuite du théorème 3.3.1 avec $f(\mathfrak{p}/p) = 1$. □

Proposition 3.3.9. *Soit* T *le diagramme de Young symétrique associé aux caractères conjugués* χ_{T} *et* χ'_{T} *et* $\mathscr{C}_{\mathrm{T}} = [q_1]\cdots[q_k]$ *sa classe associée. On note* $\sigma_{\mathfrak{p}} = [f_1]\cdots[f_g]$ *le Frobenius d'un idéal premier* $\mathfrak{p}$ *de* K *au-dessus de* p*. Alors le Frobenius* $\sigma_{\mathfrak{p}}$ *sépare les caractères* χ_{T} *et* χ'_{T} *si et seulement si la famille des* f_i *est égale à la famille des* q_i*. En particulier, les entiers* f_i *sont impairs et deux à deux distincts.*

Preuve
Supposons que le Frobenius $\sigma_{\mathfrak{p}} = [f_1]\cdots[f_g]$ sépare les caractères χ_{T} et χ'_{T}. D'après la proposition B.2.20, on sait que le Frobenius correspond à l'une des classes de conjugaison $\mathscr{C}_T^{(1)}$ ou $\mathscr{C}_T^{(2)}$. Toutes deux se décrivant avec la même décomposition en cycles que $\mathscr{C}_T$, on a donc égalité des familles f_i et q_i.
Réciproquement, si $\{f_i\}_i = \{q_j\}_j$ alors $\sigma_{\mathfrak{p}} \in A_n$ est une des classes de conjugaison $\mathscr{C}_T^{(1)}$ ou $\mathscr{C}_T^{(2)}$ donc il sépare les caractères χ_T et χ'_T.
La dernière remarque provient de la propriété B.2.18 rappelant la forme d'une telle classe de conjugaison. □

Théorème 3.3.10. *Soit* $P \in \mathbb{Z}[X]$ *un polynôme unitaire,* $\mathbb{Q}$*-irréductible de degré* n*. Supposons que le discriminant de* P *est égal au discriminant d'un corps quadratique. L'automorphisme de Frobenius* $\sigma_{\mathfrak{p}}$*,* $\mathfrak{p}|p$*, sépare un couple de caractères conjugués* (χ, χ') *de classe associée* $\mathscr{C} = [q_1]\cdots[q_k]$ *si et seulement si la factorisation de* $P \in \mathbb{F}_p[X]$ *s'écrit* $P = P_{q_1}\cdots P_{q_g} (\mathrm{mod}\ p)$*, où les polynômes* $P_{q_i} \in \mathbb{F}_p[X]$ *sont irréductibles (distincts) de degré* q_i *impairs, deux à deux distincts.*

Preuve
Le sens direct provient du résultat des propositions 3.3.8 et 3.3.9 : si $\sigma_{\mathfrak{p}}$, $\mathfrak{p}|p$, sépare un couple de caractères conjugués (χ, χ') de classe associée $\mathscr{C} = [q_1]\cdots[q_k]$ (les q_i sont impairs, distincts deux à deux par la propriété B.2.18) alors $\sigma_{\mathfrak{p}} = [q_1]\cdots[q_g]$ d'après la proposition 3.3.9 précédente et d'après la proposition 3.3.8, on a la factorisation du polynôme modulo p.
Réciproquement, supposons $P = P_{q_1}\cdots P_{q_g} (\mathrm{mod}\ p)$ avec les degrés q_i impairs, deux à deux distincts. On cherche à montrer que le Frobenius $\sigma_{\mathfrak{p}}$ s'écrit sous la forme $[q_1]\cdots[q_k]$. Puisque $\mathscr{O}_M = \mathbb{Z}[\theta]$, on sait qu'on a : $p\mathscr{O}_M = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$ avec les degrés résiduels $f_i = q_i$. Par identification des degrés des polynômes, la somme des q_i vaut n. Par ailleurs, on sait que $n = \sum_{i=1}^g e_i f_i = \sum_{i=1}^g e_i q_i$. On en déduit donc $e_i = 1$ et $f_i = q_i$. Ainsi, p est non ramifié dans $M/\mathbb{Q}$, en particulier il n'est pas ramifié dans $K/\mathbb{Q}$. D'après le théorème 3.3.1 et puisque $f_i = q_i$, le Frobenius s'écrit $\sigma_{\mathfrak{p}} = [q_1]\cdots[q_k]$ ou $([q_1]\cdots[q_k])^2$. Par imparité des q_i, on en déduit $\sigma_{\mathfrak{p}} = [q_1]\cdots[q_k]$. □

Corollaire 3.3.11. *Soit* $P \in \mathbb{Z}[X]$ *un polynôme de degré* n*, unitaire et* $\mathbb{Q}$*-irréductible. supposons son discriminant égal au discriminant d'un corps quadratique. Sous la conjecture d'Artin et l'hypothèse de Riemann généralisée aux fonctions* L *d'Artin, on obtient :*

(i) Si $n = 2m+1$ *est impair, il existe un premier* p *plus petit que* $C_1\ b(n)^4 \ln^2 |\mathrm{disc}\ P|$ *tel que* P *soit irréductible dans* $\mathbb{F}_p[X]$ *avec*

$$b(n) = \frac{1}{2}\binom{2m}{m} \sim \frac{2^{n-\frac{3}{2}}}{\sqrt{\pi}\sqrt{n-1}}.$$

(ii) Si $n \equiv 0 \pmod 4$, posons $m = 1 + n/4$. Alors il existe un nombre premier p plus petit que $C_2\ b(n)^4\ \ln^2|\mathrm{disc}\ P|$ tel que $P \pmod p$ se factorise sous la forme $Q_{2m-1}Q_{2m-3}$, où les polynômes Q_i sont des polynômes irréductibles de $\mathbb{F}_p[X]$ de degré i avec

$$b(n) = \frac{n!}{2(\frac{n}{2}+1)(\frac{n}{2}-1)[\frac{n}{2}(\frac{n}{4})!(\frac{n}{4}-1)!]^2} \sim \frac{2^{\frac{3}{2}}4^n}{n^{\frac{7}{2}}\pi^{\frac{3}{2}}}.$$

(iii) Supposons que l'entier n est un carré et écrivons $n = m^2$. Alors il existe un nombre premier p plus petit que $C_3\ b(n)^4\ \ln^2|\mathrm{disc}\ P|$ tel que $P \pmod p$ se factorise sous la forme $Q_1Q_3\cdots Q_{2m-1}$, où les Q_i sont des polynômes irréductibles de $\mathbb{F}_p[X]$ de degré i avec

$$b(n) = \frac{n!}{2\prod_{r=1}^{m}\frac{(2m-r)!}{(m-r)!}} \sim \frac{\mathrm{e}^{m^2}m^{m^2+\frac{m}{2}+1}}{2^{\frac{3m^2+m+1}{2}}\pi^{\frac{m-1}{2}}}.$$

Ici les constantes C_1, C_2 et C_3 sont absolues.

PREUVE

Notons par L le corps de décomposition de P ; soit $K = \mathbb{Q}(\sqrt{\mathrm{disc}\ P})$. L'extension L/K est une extension non ramifiée de groupe de Galois isomorphe à A_n (cf. théorème 3.3.2). Soit $\mathscr{C}$ la classe de conjugaison des éléments de S_n dont la décomposition (en cycles à support disjoint) s'écrit sous la forme d'un n-cycle (respectivement d'un produit d'un $(2m-1)$-cycle et d'un $(2m-3)$-cycle ; d'un produit $[1][3]\cdots[2m-1]$). Dans A_n, cette classe $\mathscr{C}$ se décompose en deux classes de conjugaisons $\mathscr{C}_1$ et $\mathscr{C}_2$. À cette classe $\mathscr{C}$, on peut associer un caractère irréductible φ de S_n dont la restriction à A_n est la somme de deux caractères conjugués irréductibles χ_1 et χ_2. Les caractères χ_1 et χ_2 sont de même degré $b(n) = \frac{c(n)}{2}$. Ici on se trouve dans la deuxième situation du corollaire 3.1.3, celui-ci nous donne donc l'existence d'un idéal premier $\mathfrak{p}$ de K de norme inférieure à $Cb(n)^4\ln^2|\mathrm{disc}\ P|$ ($\mathrm{disc}\ P = \mathrm{disc}\ K$) vérifiant $\chi_1(\sigma_\mathfrak{p}) \neq \chi_2(\sigma_\mathfrak{p})$. Le théorème 3.3.10 précédent permet alors d'obtenir le résultat en notant que $\mathrm{N}(\mathfrak{p}) = p$ puisque p est décomposé.

On trouve les degrés $b(n)$ en utilisant la formule des équerres, rappelée dans la proposition B.2.16. Afin d'obtenir les équivalents respectifs, on utilise la formule de Stirling.

Plus précisément, le point (i) correspond au diagramme de Young associé à la partition $n = ((n+1)/2, 1, \cdots, 1)$, la classe de conjugaison associée étant la classe des n-cycles. On calcule $c(n) = \frac{n!}{n\left[\left(\frac{n-1}{2}\right)!\right]^2} = \frac{(n-1)!}{\left[\left(\frac{n-1}{2}\right)!\right]^2} \sim \frac{2^{n-\frac{1}{2}}}{\sqrt{\pi}\sqrt{n-1}}$. Notons également que la proportion de nombres premiers p dont le Frobenius appartient à la classe d'un n-cycle (ce qui revient à la proportion de n-cycles) est égale à $\dfrac{(n-1)!/2}{n!/2} = \dfrac{1}{n}$. En effet, dans S_n, le cardinal de la classe de conjugaison d'un n-cycle vaut $(n-1)!$ donc dans A_n, $(n-1)!/2$.

Le point (ii) correspond à la représentation irréductible dont le diagramme de Young a pour partition $n = (n/4+1, n/4+1, 2, \cdots, 2)$ associé à la classe $\mathscr{C}_T = [\frac{n}{2}+1][\frac{n}{2}-1]$. Nous trouvons

$$c(n) = \frac{n!}{(\frac{n}{2}+1)(\frac{n}{2}-1)[\frac{n}{2}(\frac{n}{4})!(\frac{n}{4}-1)!]^2} \sim \frac{2^{\frac{5}{2}}4^n}{n^{\frac{7}{2}}\pi^{\frac{3}{2}}}.$$

Le point (iii) correspond au diagramme de Young symétrique de partition $n = (m, m, ..., m)$ associé à la classe $\mathscr{C}_T = [2m-1][2m-3]\cdots[1]$. On obtient :

$$c(n) = \frac{n!}{\prod_{r=1}^{m}\frac{(2m-r)!}{(m-r)!}} \sim \frac{\mathrm{e}^{m^2}m^{m^2+\frac{m}{2}+1}}{2^{\frac{3m^2+m-1}{2}}\pi^{\frac{m-1}{2}}}.$$

□

3.3.5 Comparaison avec la méthode de Bellaïche dans le cas du groupe symétrique

Discutons brièvement de la "qualité" des bornes obtenues. Tout d'abord, une application "classique" du théorème de Chebotarev donne une borne en $O\Big(\big(n!\big)^2 \ln^2 |\text{disc } P|\Big)$ (d'autres bornes sont données dans [Bel], [MM97] ou [Mur94] : $n(n!)^2 \ln n$ et $nn! \ln n$). Ensuite, pour un polynôme P de degré impair n, notre méthode s'applique et donne une borne en $O\left(\dfrac{4^{2n}}{n^2} \ln^2 |\text{disc } P|\right)$ garantissant l'existence d'un premier p avec $P(\text{mod } p)$ irréductible sur $\mathbb{F}_p[X]$ (voir (i) du corollaire 3.3.11). Dans un récent travail, Bellaïche ([Bel], théorème 17) donne une borne en $O\big(4^n(\ln \text{disc } P + n \ln n)^2\big)$ pour tout P polynôme irréductible à coefficients dans $\mathbb{Z}$. Dans cette partie, nous nous efforçons de comparer les deux approches. Avec un minutieux travail, il est probable que la méthode de Bellaïche apporte une très bonne borne pour la situation (ii) du corollaire 3.3.11 (en $\mathscr{O}(2^n)$?) ; par contre, le point (iii) est nettement plus compliqué... c'est le cas extrême ; ici la borne que l'on obtient est légèrement meilleure que $(m^2!)^2$:

$$\frac{b(n)}{(n!)^2} \sim \frac{\mathrm{e}^{3m^2}}{m^{3m^2-\frac{m}{2}+1} 2^{\frac{3m^2+m+3}{2}} \pi^{\frac{m+1}{2}}} \ll \frac{1}{n^n},$$

ou encore

$$b(n) = O\left(\frac{(n!)^2}{n^n}\right).$$

Revenons sur la borne donnée par Bellaïche (dans [Bel]) dans le contexte des groupes S_n. Dans cet article, pour des histoires de notations, il ne considère que des extensions dont le corps de base est $\mathbb{Q}$.

Théorème 3.3.12 ([Bel], théorème 3). *Soit $L/\mathbb{Q}$ une extension galoisienne de groupe de Galois G isomorphe au groupe S_n que l'on suppose non ramifiée en dehors de l'ensemble Σ. Soit $\mathscr{C}$ une classe de conjugaison de S_n. Sous les conjectures d'Artin et de Riemann généralisée aux fonctions L d'Artin, le plus petit nombre premier p non ramifié tel que le Frobenius $\sigma_p \in \mathscr{C}$ vérifie*

$$p \leqslant c_{11} \varphi(\mathscr{C})^2 \ln^2(M|G|),$$

où $M = \prod_{\ell \in \Sigma} \ell$. Ici

$$\varphi(\mathscr{C}) = \sum_{\chi \in \mathrm{Irr}(G)} |\chi(\mathscr{C})| \chi(1),$$

$\mathrm{Irr}(G)$ *désignant l'ensemble des caractères irréductibles de G et $\chi(\mathscr{C})$ un abus de notation pour $\chi(c)$, $c \in \mathscr{C}$.*

On utilise les notations introduites par Bellaïche, $\mathbb{I}_{\mathscr{C}}$ désigne la fonction indicatrice de $\mathscr{C}$: $\varphi_G(\mathscr{C}) \leqslant \frac{\lambda(\mathbb{I}_{\mathscr{C}})}{\mu(\mathbb{I}_{\mathscr{C}})} = \lambda(\mathbb{I}_{\mathscr{C}}) \frac{|G|}{|\mathscr{C}|}$ et $\lambda(\mathbb{I}_{\mathscr{C}}) = \sum_{\chi \in \mathrm{Irr}(G)} |\langle \chi, \mathbb{I}_{\mathscr{C}} \rangle| \chi(1) = \frac{|\mathscr{C}|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} |\chi(\mathscr{C})| \chi(1)$.

Remarque 3.3.13. En adaptant la preuve de Joël Bellaïche lorsqu'il y a une extension intermédiaire L/K non ramifiée, on trouve la borne :

$$p \leqslant c_{11} \varphi(\mathscr{C})^2 \ln^2 |\text{disc } K|.$$

En effet, en reprenant le fil de sa preuve, on doit majorer $q(\chi) = f(\chi) = \prod_{p\in\mathbb{Z}} p^{f_p(\chi)}$. On sait que $f_p(\chi) = 0$ lorsque p est non ramifié dans $L/\mathbb{Q}$, ici ceci revient à p non ramifié dans $K/\mathbb{Q}$, autrement dit p ne divise pas le discriminant de K. Finalement, $q(\chi) \leqslant |\text{disc } K|^{\max_{p|\text{disc}K} f_p(\chi)}$.
D'après la preuve de la proposition 2.5 de [MMS88], on a :

$$f_p(\chi) \leqslant \frac{2\chi(1)(e(\mathfrak{p}/p)-1)}{e(\mathfrak{p}/p)} + 2\chi(1)v_p(e(\mathfrak{p}/p)) \leqslant 2\chi(1) + 2\chi(1)v_p(e(\mathfrak{p}/p)).$$

D'où

$$\begin{aligned} f(\chi) &= \prod_{p|\text{disc } K} p^{2\chi(1)}(\prod_p p^{v_p(e(\mathfrak{p}/p))})^{2\chi(1)} \leqslant |\text{disc } K|^{2\chi(1)} e(\mathfrak{p}/p)^{2\chi(1)} \\ &\leqslant (|\text{disc } K|[K:\mathbb{Q}])^{2\chi(1)} \leqslant (c_0|\text{disc } K|)^{4\chi(1)} \end{aligned}$$

car $[K:\mathbb{Q}] \leqslant c_0 \ln|\text{disc } K|$.
Dans la preuve de Bellaïche, on majore $\ln q(\chi)$ par $C\chi(1)\ln|\text{disc } K|$, on remplace donc $\ln(M|G|)$ par $\ln|\text{disc } K|$ d'où le résultat.
Lorsque K est un corps quadratique, notons que $q(\chi) \leqslant |2 \text{ disc } K|^{2\chi(1)}$.

Soit $P \in \mathbb{Z}[X]$ un polynôme $\mathbb{Q}$-irréductible unitaire dont le discriminant est celui d'un corps quadratique K. Alors on sait que le groupe de Galois de $L/\mathbb{Q}$, L étant le corps de décomposition de P, est isomorphe à S_n et L/K est non ramifiée de groupe de Galois A_n. Soit $\mathscr{C}$ une classe de conjugaison de S_n dont la restriction à A_n se décompose en deux classes de conjugaison $\mathscr{C}^{(1)}$ et $\mathscr{C}^{(2)}$. Pour p non ramifié dans $K/\mathbb{Q}$ et $\mathfrak{p}$ un idéal premier de K au-dessus de p, $\sigma_p \in \mathscr{C}$ est équivalent à $\sigma_\mathfrak{p} \in \mathscr{C}^{(1)}$ ou $\mathscr{C}^{(2)}$, ou encore $\sigma_\mathfrak{p}$ sépare les deux caractères conjugués associés à $\mathscr{C}$ du groupe alterné A_n. En effet, la propriété B.1.14 nous permet d'écrire $\sigma_p = \sigma_\mathfrak{p}$ ou $\sigma_p^2 = \sigma_\mathfrak{p}$ et l'écriture des classes de conjugaison considérées sous forme de cycles de longueur impaire donne le résultat.
Ainsi, on peut reformuler le corollaire 3.1.3 sous la forme suivante.
Le plus petit nombre premier p non ramifié dans $L/\mathbb{Q}$ tel que le Frobenius σ_p soit dans une classe de conjugaison $\mathscr{C}$ de A_n provenant d'une classe de S_n se décomposant en deux vérifie $p \leqslant C\left(\frac{\chi_\mathrm{T}(1)}{2}\right)^4 \ln^2|\text{disc } K|$, où χ_T est le caractère irréductible associé à $\mathscr{C}$ de diagramme de Young symétrique T.
On en arrive à la comparaison des quantités $\displaystyle\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathscr{C})|\chi(1) = \sum_{\lambda \text{ partition de } S_n} |\chi_\lambda(\mathscr{C})|\chi_\lambda(1)$ et $\left(\dfrac{\chi_\mathrm{T}(1)}{2}\right)^2$.
Donnons quelques exemples.

Exemple 3.3.14. Pour n impair, prenons le diagramme de Young T associé à la partition $(\frac{n+1}{2}, 1, \cdots, 1)$. Comme nous l'avons vu dans le point (i) du corollaire 3.3.11, dans ce cas, $\left(\dfrac{\chi_\mathrm{T}(1)}{2}\right)^2 \sim \dfrac{2^{2n-3}}{\pi(n-1)}$.
D'un autre côté, en notant $\mathscr{C}_T$ la classe de conjugaison associée aux cycles de longueur n, on a $\displaystyle\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathscr{C}_\mathrm{T})|\chi(1) = 2^{n-1}$. En effet, en utilisant la règle de Murnaghan-Nakayama (voir proposition B.2.23), pour λ une partition de S_n, on trouve

$$\chi_\lambda(\mathscr{C}_\mathrm{T}) = \begin{cases} \pm 1 & \text{si } \lambda = (k, 1, \cdots, 1),\ k \in [\![1, n]\!] \\ 0 & \text{sinon} \end{cases}$$

donc

$$\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathscr{C}_{\mathrm{T}})|\chi(1) = \sum_{\substack{\lambda_k=(k,1,\cdots,1)\\ \text{partition de } S_n}} \chi_{\lambda_k}(1) = \sum_{k=1}^{n} \frac{n!}{n(k-1)!(n-k)!} = \sum_{k=1}^{n} \binom{n-1}{k-1} = 2^{n-1}.$$

Exemple 3.3.15. Pour n pair, prenons le diagramme de Young symétrique T de partition $(\frac{n}{2}, 2, 1, \cdots, 1)$; ici $\mathscr{C}_T = [n-1][1]$.
On obtient

$$\chi_T(1) = \frac{4(n-2)!}{n\left((\frac{n}{2}-2)!\right)^2} \sim \frac{n^{\frac{1}{2}}2^{n-\frac{3}{2}}}{\sqrt{\pi}}$$

d'où $\left(\frac{\chi_{\mathrm{T}}(1)}{2}\right)^2 \sim \frac{n2^{2n-5}}{\pi}$. D'un autre côté, avec les calculs de l'exemple B.2.26, on trouve :

$$\begin{aligned}\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathscr{C})|\chi(1) &= |\chi_{(1,\cdots,1)}(\mathscr{C})|\chi_{(1,\cdots,1)}(1) + |\chi_{(n)}(\mathscr{C})|\chi_{(n)}(1)\\ &\quad + \sum_{k=2}^{n-2} |\chi_{(k,2,1\cdots,1)}(\mathscr{C})|\chi_{(k,2,1\cdots,1)}(1)\\ &= 2 + \sum_{k=2}^{n-2} \frac{n!}{(n-1)k(n-k)(k-2)!(n-k-2)!}\\ &= n2^{n-2} - 2^n + 2^2.\end{aligned}$$

Exemple 3.3.16. Considérons le groupe S_9 et le diagramme de Young associé à la partition $\lambda = (3,3,3)$. C'est un tableau symétrique dont la classe de conjugaison $\mathscr{C}$ associée a pour décomposition [5][3][1]. Le caractère χ_{T} est de degré 42 donc $\left(\frac{\chi_{\mathrm{T}}(1)}{2}\right)^2 = 441$. À l'aide de Magma ([BCP97]), on calcule $\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathscr{C})|\chi(1) = 1\,284$.

Question : Pour certains diagrammes de Young symétriques, le comportement asymptotique de la quantité introduite par Bellaiche est meilleur. Est-ce que c'est vrai pour tous les diagrammes symétriques ?

3.4 Sur les extensions non ramifiées d'un corps de nombres

3.4.1 Un exemple de base : le p-rang du groupe des classes

La version effective du théorème de Chebotarev et un argument élémentaire de dénombrement permettent de donner une borne supérieure pour le nombre $n(p)$ de caractères abéliens non ramifiés d'ordre p de K et ainsi de majorer le p-rang $d_p\mathrm{Cl}_K$ du groupe des classes Cl_K de K. Cette méthode ne donne pas la meilleure borne mais, néanmoins, d'une part, conjecturalement, le résultat obtenu pour le p-rang n'est pas si mauvais que cela et puis d'autre part, elle a le mérite de s'étendre à d'autres situations, ce que nous ferons à la fin de cette section (en s'inspirant de [RT14]).
Posons $N = \mathrm{card}\{\mathfrak{p} \subset \mathscr{O}_K \mid \mathrm{N}(\mathfrak{p}) \leqslant X\}$. Le théorème des nombres premiers donne l'existence d'une constante c_{12} telle que

$$N \leqslant c_{12}[K:\mathbb{Q}]\frac{X}{\ln X}.$$

Précisons la méthode utilisée. Soit l'entier X qui, pour tout couple (χ, χ') de caractères distincts de degré 1 non ramifiés et d'ordre p, assure l'existence d'un premier $\mathfrak{p}$ de K tel que $\mathrm{N}(\mathfrak{p}) \leqslant X$ et tel que $\chi(\sigma_\mathfrak{p}) \neq \chi'(\sigma_\mathfrak{p})$. Notons que quand $\sigma_\mathfrak{p}$ varie, les valeurs de $\chi(\sigma_\mathfrak{p})$ et de $\chi'(\sigma_\mathfrak{p})$ se trouvent dans un ensemble de cardinal p. Les caractères χ de degré 1 et d'ordre p sont donc déterminés par les valeurs $\chi(\sigma_\mathfrak{p})$, avec $\mathrm{N}(\mathfrak{p}) \leqslant X$, autrement dit l'ensemble $(\chi(\sigma_{\mathfrak{p}_1}), \cdots, \chi(\sigma_{\mathfrak{p}_N}))$, où $\mathfrak{p}_i$ est le i^e idéal premier de norme plus petite que X, définit entièrement le caractère χ. Il y a donc au plus p^N caractères de ce type.
En conclusion, il vient :

$$\ln(n(p)) \leqslant c_{12} \ln(p)[K : \mathbb{Q}] \frac{X}{\ln(X)}. \tag{3}$$

Rappelons le résultat du corollaire 3.1.3 :

PROPOSITION 3.4.1. *Soient χ et χ' deux caractères non ramifiés distincts de K de degré 1 et d'ordre p. Alors, sous les conjectures d'Artin et l'hypothèse de Riemann généralisée aux fonctions L d'Artin, il existe un premier $\mathfrak{p}$ de K de norme $\mathrm{N}(\mathfrak{p}) \leqslant c_4 \ln^2 |\mathrm{disc}\ K|$ tel que $\chi(\sigma_\mathfrak{p}) \neq \chi'(\sigma_\mathfrak{p})$.*

En conclusion, on obtient :

Corollaire 3.4.2. *Pour tout corps de nombres K,*

$$d_p \mathrm{Cl}_K = \frac{1}{\ln(p)} \ln(n(p)) \leqslant c_{12}[K : \mathbb{Q}] \frac{c_4 \ln^2 |\mathrm{disc}\ K|}{\ln c_4 + 2 \ln \ln |\mathrm{disc}\ K|}.$$

PREUVE
Dans ce cadre, $[L : K] = |G| = p^{d_p \mathrm{Cl}_K}$. Comme G est abélien, en utilisant les degrés des représentations $|G| = \sum_{i=1}^{n(p)} 1^2 = n(p)$, on obtient $d_p \mathrm{Cl}_K = \frac{\ln(n(p))}{\ln p}$. On en déduit le résultat en utilisant l'inégalité (3) avec $X = c_4 \ln^2 |\mathrm{disc}\ K|$ dû à la proposition 3.4.1. □

Rappelons alors à ce niveau la question suivante :
Question : [[Ser81], §2.5] A-t-on $\mathrm{N}(\mathfrak{p}) \ll_\varepsilon \ln^{1+\varepsilon} |\mathrm{disc}\ L|$?

Dans le cadre du p-rang du groupe des classes, cette question est à rapprocher de l'inégalité facile du théorème de Brauer-Siegel (voir par exemple le lemme 2 du chapitre XVI de [Lan94] page 322) qui aboutit au résultat suivant :

THÉORÈME 3.4.3. *Pour tout corps de nombres, on a :* $d_p \mathrm{Cl}_K \leqslant c_{12} \frac{1}{\ln p} \ln |\mathrm{disc}\ K|$.

PREUVE
On note Cl_K le groupe des classes d'idéaux de K et $h_K = |\mathrm{Cl}_K|$ le nombre de classes de K. On peut définir le p-rang $d_p \mathrm{Cl}_K$ de la façon suivante : $d_p \mathrm{Cl}_K = \dim_{\mathbb{F}_p} \mathrm{Cl}_K / p\mathrm{Cl}_K$. D'où $d_p \mathrm{Cl}_K \leqslant \frac{\ln h_K}{\ln p}$. La majoration du lemme 2 du chapitre XVI de [Lan94] nous permet d'écrire $\ln h_K \leqslant C \ln |\mathrm{disc}\ K|$ d'où le résultat. □

Remarque 3.4.4. En particulier à K fixé, le théorème de Brauer-Siegel indique bien que $d_p \mathrm{Cl}_K = 0$ pour p assez grand. Ce qui n'est pas le cas de l'inégalité du corollaire 3.4.2.

Remarque 3.4.5. Par deux approches différentes, la théorie analytique des nombres apporte deux estimations pour $d_p \mathrm{Cl}_K$. La première peut être adaptée à tout groupe simple $\mathscr{S}$ (ce sera l'objet de la section à venir). Quant à la seconde, elle découle de la formule analytique du nombre de classes et est donc propre au groupe des classes.

Pour tenter d'être complet, citons également les travaux plus récents de Ellenberg-Venkatesh [EV06], [EV07] et de Ellenberg [Ell08], pour une approche utilisant la géométrie des nombres.

3.4.2 Caractères de degré $r > 1$

Étant donné un groupe simple $\mathscr{S}$ fixé, une question naturelle consiste à chercher un résultat sur le modèle du p-rang du groupe des classes.

Fixons donc un groupe simple $\mathscr{S}$ et soit χ un caractère non trivial de $\mathscr{S}$ (de plus petit degré $r > 1$). Notons $k(\mathscr{S})$ le nombre de classes de conjugaison de $\mathscr{S}$, $e(\mathscr{S})$ le nombre de représentations irréductibles de $\mathscr{S}$ de degré 1 et soit $a(\chi)$ le nombre de valeurs prises par χ. Commençons par la première estimation suivante pour $a(\chi)$.

Lemme 3.4.6. *On a :* $a(\chi) \leqslant k(\mathscr{S}) \leqslant e(\mathscr{S}) + \dfrac{|\mathscr{S}| - e(\mathscr{S})}{r^2} \leqslant e(\mathscr{S}) + \dfrac{|\mathscr{S}| - 1}{r^2}$.

<u>Preuve</u>
Cela provient tout simplement de la formule $\sum_{\psi} \psi(1)^2 = |\mathscr{S}|$, la somme portant sur les caractères irréductibles de $\mathscr{S}$ et du fait que le nombre de représentations irréductibles d'un groupe fini est égal à son nombre de classes de conjugaison. □

Rappelons maintenant le résultat de Collins qui précise le théorème de Jordan sur les sous-groupes simples de $\mathrm{Gl}_n(\mathbb{C})$.

Théorème 3.4.7 ([Col07], Theorem A). *Soit $\mathscr{S} \hookrightarrow \mathrm{Gl}_n(\mathbb{C})$ un groupe simple. Alors dès que $n \geqslant 71$, on a $|\mathscr{S}| \leqslant (n+1)!$.*

En d'autres termes, ce résultat donne une borne inférieure asymptotique (suivant $|\mathscr{S}|$) sur le degré minimal r des représentations non triviales des groupes simples. Associée au lemme 3.4.6, on obtient (pour $r \geqslant 71$)

$$a(\chi) \ll \frac{(r+1)!}{r^2}.$$

Cette inégalité est à comparer avec l'exemple B.2.25.

Revenons au contexte arithmétique. Soit un entier $k \geqslant 1$. Supposons que le corps de nombres K admette une extension galoisienne non ramifiée de groupe de Galois G vérifiant $G \simeq \overbrace{\mathscr{S} \times \cdots \times \mathscr{S}}^{k}$. Alors $\hat{G} \simeq \prod_{i=1}^{k} \hat{\mathscr{S}}$, isomorphisme en un sens évident. Considérons ensuite les caractères irréductibles de G de la forme $\varphi_i = \mathbf{1} \otimes \cdots \otimes \mathbf{1} \otimes \chi \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1}$, où l'on rappelle que χ est un caractère non trivial de degré r (que l'on peut supposer minimal) et où $\mathbf{1}$ est le caractère trivial. Les caractères φ_i sont irréductibles de degré r et ils prennent les mêmes valeurs que le caractère χ.
Soient alors $i \neq j$. Par le corollaire 3.1.3, sous la conjecture d'Artin et l'hypothèse de Riemann généralisée aux fonctions L d'Artin, on sait qu'il existe un idéal premier $\mathfrak{p}$ de norme plus petite que

$$X = c_4 r^4 \ln^2 |\mathrm{disc}\ K|$$

tel que $\varphi_i(\sigma_{\mathfrak{p}}) \neq \varphi_j(\sigma_{\mathfrak{p}})$. En d'autres termes, le premier $\mathfrak{p}$ sépare les caractères φ_i et φ_j. Rappelons la définition $N = \mathrm{card}\{\mathfrak{p} \subset \mathscr{O}_K \mid \mathrm{N}(\mathfrak{p}) \leqslant X\}$.

La famille $(\varphi_j(\sigma_{\mathfrak{p}_1}), \ldots, \varphi_j(\sigma_{\mathfrak{p}_N}))$, où $\mathfrak{p}_i$ est le i^e idéal premier de norme plus petite que X, est donc représentative d'un caractère φ_j. D'autre part, pour chaque $i \in [\![1, N]\!]$ et tout entier $j \in \{1, \cdots, k\}$, la quantité $\varphi_j(\sigma_{\mathfrak{p}_i})$ peut prendre au maximum $a(\chi)$ valeurs différentes. Ainsi, on obtient :

$$k \leqslant a(\chi)^N.$$

Souvenons-nous ensuite que $N \leqslant c_{12}[K : \mathbb{Q}]\dfrac{X}{\ln X}$, pour obtenir :

PROPOSITION 3.4.8. *Avec les notations précédentes et sous la conjecture d'Artin et l'hypothèse de Riemann généralisée aux fonctions L d'Artin, il vient :*

$$\begin{aligned}\ln(k) &\leqslant c_4 c_{12} \ln a(\chi)[K : \mathbb{Q}]\frac{r^4 \ln^2 |\text{disc } K|}{\ln c_4 + 4\ln r + 2\ln\ln|\text{disc } K|}\\ &\leqslant c_4 c_{12}\frac{\ln a(\chi)}{\ln r} r^4 [K : \mathbb{Q}] \ln^2 |\text{disc } K|.\end{aligned}$$

J. Rouse et F. Thorne, dans [RT14], donnent l'inégalité $\ln(k) \ll r^5[K : \mathbb{Q}] \ln^2 |\text{disc } K|$ faisant donc apparaître une puissance r^5.

Revenons à l'estimation issue de l'inégalité donnée par Collins : pour r assez grand, $\ln a(\chi) \ll r \ln r$, ce qui redonne le résultat de Rouse et Thorne. Mais comme le montre le cas du groupe alterné, cette majoration peut être nettement améliorée :

Exemple 3.4.9. Dans le cas du groupe alterné $\mathscr{S} = A_n$, il vient $a(\chi) \leqslant 2r + 3$ (voir partie B.2.22 page 119) et ainsi la borne de la proposition 3.4.8 est en r^4. Plus précisément, si l'on prend le diagramme de Young T de partition $\lambda = (n-1, 1)$ alors le caractère χ_{T} associé est de degré $n-1$ (pour $n \geq 7$, c'est le caractère non trivial de plus petit degré) et $a(\chi_T) = O(n)$. Ainsi on obtient ici : $\ln(k) \ll_K n^4$.

Remarque 3.4.10. Lorsque $r = 1$, le corollaire 3.4.2 s'obtient avec une approche légèrement différente. En effet, soit le groupe simple $\mathscr{S} = \mathbb{Z}/p\mathbb{Z}$. On considère les caractères φ_i de la forme $\chi_1 \otimes \cdots \otimes \chi_k$, où les caractères χ_i sont de degré 1. Ces caractères sont de degré $1^k = 1$. La borne du corollaire 3.1.3 n'est pas impactée et cette démarche apporte alors $(p-1)^k$ caractères d'ordre p.

3.4.3 Une variante : les extensions modérément ramifiées d'un corps de nombres

Dans la section précédente, comme les représentations en jeu sont non ramifiées, les conducteurs sont réduits à leurs plus simples expressions. Dans cette partie, nous reprenons ces calculs pour des situations où les conducteurs de produit tensoriel se simplifient. Commençons par une remarque.

Remarque 3.4.11. Soit ρ une représentation de caractère χ. L'ensemble des valeurs prises par $\chi(\sigma_{\mathfrak{p}})$, quand $\mathfrak{p}$ varie, peut différer de l'ensemble des valeurs du caractère χ : cette différence provient des places ramifiées et de la définition de $\chi(\sigma_{\mathfrak{p}})$ dans ce cas particulier (voir partie 1.2.1). Par contre, on a de façon évidente

$$|\{\chi(\sigma_{\mathfrak{p}}),\ \mathfrak{p} \subset \mathscr{O}_K\}| \leqslant a(\chi) + |\Sigma|,$$

où Σ est l'ensemble des premiers $\mathfrak{p}$ ramifiés (à travers χ).

Définition 3.4.12. Soit A une matrice carrée de taille $r \times r$ à coefficients complexes. Si A est d'ordre 2, on définit la *signature* de A comme étant le couple (r_+, r_-), où r_+ (respectivement r_-) est le nombre de valeurs propres de A égales à $+1$ (respectivement à -1) : $r_+ + r_- = r$.

Soit $\rho : G_K \to \mathrm{Gl}_r(\mathbb{C})$ une représentation continue de caractère χ. Pour $\tau \in G_K$ tel que $\rho(\tau)$ est d'ordre 2, la signature de τ (relativement à ρ) est la signature de $\rho(\tau)$. Remarquons alors que $\rho(\tau)$ et $\rho^{-1}(\tau) = \overline{\rho}(\tau)$ ont même signature.

A présent, on s'intéresse aux représentations ρ (ou aux caractères χ) peu ramifiées dans le sens suivant :

Définition 3.4.13. Une représentation ρ est dite *peu ramifiée* si lorsqu'elle est ramifiée en un idéal $\mathfrak{p}$ alors le groupe d'inertie de $\mathfrak{p}$ se factorise à travers un élément $\tau_\mathfrak{p}$ d'ordre 2, autrement dit, $I_\mathfrak{p} =< \tau_\mathfrak{p} >$.
Dans ce cas, si (r_+, r_-) est la signature de $\rho(\tau_\mathfrak{p})$, on dit que la représentation ρ est de $\mathfrak{p}$-*signature* (r_+, r_-).

Remarque 3.4.14. Notons que pour une représentation peu ramifiée, si $\mathfrak{p}$ est au-dessus d'un premier impair, la ramification en $\mathfrak{p}$ est alors modérée.

Lemme 3.4.15. *Soit $\mathfrak{p}$ un premier impair. Soient ρ et ρ' deux représentations (de caractères χ et χ') peu ramifiées en $\mathfrak{p}$ ayant pour conducteur local : $f_\mathfrak{p}(\chi) = k$ et $f_\mathfrak{p}(\chi') = k'$. Alors*

$$f_\mathfrak{p}(\chi \otimes \chi') = k'(r-k) + k(r'-k'),$$

où r (respectivement r') est le degré de ρ (respectivement de ρ').

<u>Preuve</u>
Partons de ρ. Comme la ramification est modérée, il vient $\rho(G_{i,\mathfrak{p}}) = \{1\}$ pour $i \geqslant 1$, où $G_{i,\mathfrak{p}}$ désigne le i^e groupe de ramification d'un idéal $\mathscr{P}$ au-dessus de $\mathfrak{p}$. L'action de $G_{0,\mathfrak{p}}$ se factorise sur V à travers $\rho(\tau_\mathfrak{p})$ et la codimension de $V^{G_{0,\mathfrak{p}}}$ est exactement le nombre de valeurs propres de ρ valant -1. En effet, puisque $\tau_\mathfrak{p}$ est d'ordre 2, $\rho(\tau_\mathfrak{p})$ est diagonalisable (il possède un polynôme annulateur X^2-1 scindé à racines simples) avec r_+ 1 et r_- (-1) sur sa diagonale. D'où $V^{I_\mathfrak{p}} = \{v \in V \ : \ \rho(\tau_\mathfrak{p})(v) = v\}$ est le sous-espace vectoriel engendré par $r_+ = r - r_-$ vecteurs. Ainsi, $k = f_\mathfrak{p}(\chi) = \mathrm{codim} V^{I_\mathfrak{p}} = r_-$.
Ici ρ et ρ' sont de $\mathfrak{p}$-signatures $(r-k, k)$ et $(r'-k', k')$, et alors $\rho \otimes \rho'$ est une représentation de $\mathfrak{p}$-signature $\big(kk' + (r-k)(r'-k'), k(r'-k') + k'(r-k)\big)$, d'où le résultat. □

Les situations intéressantes pour nous sont celles où la borne brutale (voir remarque 1.2.29) $f_\mathfrak{p}(\chi \otimes \chi') \leqslant r' f_\mathfrak{p}(\chi) + r f_\mathfrak{p}(\chi')$ est très mauvaise. Typiquement, supposons $r = r'$ puis que les représentations ρ et ρ' sont de même $\mathfrak{p}$-signature $(0, r)$, ce qui revient à avoir $f_\mathfrak{p}(\chi) = f_\mathfrak{p}(\chi') = r$. Alors, d'après le lemme 3.4.15 précédent, $f_\mathfrak{p}(\chi \otimes \chi') = 0$.

Notons par $\mathscr{N}(\mathfrak{p}^k)$ le nombre de caractères de degré r non ramifiés en dehors de $\mathfrak{p}$, peu ramifiés en $\mathfrak{p}$ avec pour conducteur k. En appliquant la stratégie de la section précédente (ou bien le corollaire suivant le démontre dans un cadre plus général), on obtient

$$\ln(\mathscr{N}(\mathfrak{p}^r)) \ll r^5 [K : \mathbb{Q}] \ln^2 |\mathrm{disc}\ K|.$$

Cette non dépendance en $\mathfrak{p}$ n'est pas surprenante : en effet, comme les représentations en jeu sont de $\mathfrak{p}$-conducteur r, cela signifie que $\rho(\tau_\mathfrak{p}) = -I_r$, où I_r est la matrice identité. Donc $\rho(\tau_\mathfrak{p})$ est dans le centre de $\mathrm{Im}(\rho)$: le corps $L := \overline{K}^{\mathrm{Ker}(\rho)}$ est une extension quadratique

totalement et modérément ramifiée d'une extension non ramifiée de L_0/K. La théorie du corps de classes indique que, étant donnée L_0, l'extension L/L_0 est unique.
Il faut donc aller un peu plus loin pour trouver une illustration non triviale.

Corollaire 3.4.16. *Dans les conditions précédentes et sous la conjecture d'Artin et l'hypothèse de Riemann généralisée aux fonctions L d'Artin,*

$$\ln \mathscr{N}(\mathfrak{p}^k) \ll r[K:\mathbb{Q}]\Big(r^2 \ln|\text{disc } K| + 2k(r-k)\ln \mathrm{N}(\mathfrak{p})\Big)^2.$$

PREUVE
D'après le théorème 3.1.1, il existe un idéal premier $\mathfrak{q}$ de l'anneau $\mathscr{O}_K$ de norme inférieure à $X = \frac{4}{\langle\chi,\chi\rangle^2}(c_1 r^2[K:\mathbb{Q}]+c_2(\ln q(\chi\otimes\overline{\chi'})+\ln q(\chi\otimes\overline{\chi'}))+c_3\langle\chi,\chi\rangle))^2$ tel que $\chi(\sigma_\mathfrak{q}) \neq \chi'(\sigma_\mathfrak{q})$, où χ et χ' sont deux caractères de degré r non ramifiés en dehors de $\mathfrak{p}$, peu ramifiés en $\mathfrak{p}$ de conducteur k. Les valeurs des caractères en les différents Frobenius $\sigma_{\mathfrak{p}_i}$, $1 \leqslant i \leqslant N$ ($N = \text{card}\{\mathfrak{p} \subset \mathscr{O}_K \mid \mathrm{N}(\mathfrak{p}) \leqslant X\}$), sont donc représentatives d'un tel caractère. Ainsi, $\mathscr{N}(\mathfrak{p}^k) \leqslant a(\chi)^N$.
Par ailleurs, en utilisant le lemme 3.4.15, on obtient : $q(\chi\otimes\overline{\chi'}) = |\text{disc } K|^{r^2}\mathrm{N}(f(\chi\otimes\overline{\chi'})) = |\text{disc } K|^{r^2}\mathrm{N}(\mathfrak{p}^{2k(r-k)})$ d'où $X \leqslant C(r^2\ln|\text{disc } K| + 2k(r-k)\ln\mathrm{N}(\mathfrak{p}))^2$.
Ainsi, $\ln\mathscr{N}(\mathfrak{p}^k) \leqslant N\ln(a(\chi)) \leqslant C[K:\mathbb{Q}]\frac{X}{\ln X}\ln(a(\chi))$. On obtient le résultat en utilisant la majoration pour r assez grand $\ln a(\chi) \leqslant r\ln r$ (le nombre de valeurs prises par un caractère pouvant être majoré par $(r+1)!/r^2$). □

Retournons de nouveau vers les groupes alternés A_n, pour $n \geq 7$.

Définition 3.4.17. Un élément $\tau \in S_n$ est dit de *longueur* k si τ est le produit de k transpositions (à supports disjoints).

On remarque que tout élément d'ordre 2 de A_n est le produit de k transpositions pour un certain entier pair k.

Soit $\mathfrak{p}$ un idéal premier impair de K. Pour $n \geqslant 7$, notons par $\mathscr{N}(A_n,\mathfrak{p},k)$ le nombre d'extensions du corps K de groupe de Galois isomorphe à A_n non ramifiées en dehors de $\mathfrak{p}$ et dont le groupe d'inertie en $\mathfrak{p}$ est de longueur k (l'entier k est donc pair). Une synthèse de nos précédents résultats et discussions nous permet d'obtenir le corollaire suivant :

Corollaire 3.4.18. *Sous les conditions précédentes, il vient*

$$\ln\mathscr{N}(A_n,\mathfrak{p},k) \ll [K:\mathbb{Q}]\Big((n-1)^2\ln|\text{disc } K| + 2k(n-1-k)\ln\mathrm{N}(\mathfrak{p})\Big)^2.$$

PREUVE
On sait (proposition B.2.27) qu'il existe une unique représentation irréductible non triviale de A_n de degré inférieur à n : elle est de degré $n-1$, notons-la ρ et χ son caractère. Ainsi, le nombre $\mathscr{N}(A_n,\mathfrak{p},k)$ d'extensions du corps K de groupe de Galois isomorphes à A_n non ramifiées en dehors de $\mathfrak{p}$ et dont le groupe d'inertie en $\mathfrak{p}$ est de longueur k correspond au nombre de représentations irréductibles de degré $n-1$ dans le groupe $G \simeq \overbrace{A_n \times \cdots \times A_n}^{\mathscr{N}(A_n,\mathfrak{p},k)}$ avec A_n non ramifiées en dehors de $\mathfrak{p}$ et dont le groupe d'inertie en $\mathfrak{p}$ est de longueur k, engendré par un élément $\tau_\mathfrak{p}$. Les caractères associés sont de la forme : $\mathbf{1}\otimes\cdots\otimes\mathbf{1}\otimes\chi\otimes\mathbf{1}\otimes\cdots\otimes\mathbf{1}$ (remarquons que les caractères et les représentations prennent les mêmes valeurs que χ et ρ).

Notons que, par hypothèse, la représentation considérée est peu ramifiée.
Par ailleurs, ici $\tau_{\mathfrak{p}}$ étant de longueur k, il vient $\chi(\tau_{\mathfrak{p}}) = n-1-2k$, d'après l'exemple B.2.25. Comme $\chi(\tau_{\mathfrak{p}})$ est la somme de $+1$ et de -1, on a facilement que $\rho(\tau_{\mathfrak{p}})$ est de signature $(n-k-1, k)$. D'où le conducteur d'Artin $f(\chi) = \mathrm{N}(\mathfrak{p})^k$.
En procédant de la même façon que dans la preuve du corollaire 3.4.16, en utilisant cette fois la majoration $a(\chi) \leqslant 2(n-1)+3$ donnée dans la propriété B.2.22, on obtient le résultat. □

Le gain ici se fait sur le terme devant $\ln \mathrm{N}(\mathfrak{p})$. En particulier, si n est pair, pour $k = n-2$, on passe de $2(n-1)(n-2)$ à $2(n-2)$. À noter ici que l'extension L/K correspondante de groupe de Galois A_n est de discriminant relatif disc $L/K = \mathfrak{p}^{\frac{n!}{4}}$ et de discriminant absolu $\left(\mathrm{N}(\mathfrak{p})^{\frac{1}{2}} \text{disc } K\right)^{\frac{n!}{2}}$.

Remarque 3.4.19. Il est possible de reprendre ces deux derniers corollaires en prenant un ensemble Σ de premiers ramifiés non nécessairement réduit à un élément. Typiquement soit $\mathscr{N}(\Sigma, k)$ le nombre de caractères de degré r non ramifiés en dehors de Σ, peu ramifiés en $\mathfrak{p} \in \Sigma$ avec pour conducteur local k. Regardons l'évolution de $\mathscr{N}(\Sigma, k)$ suivant Σ, plus précisément suivant la remarque 3.4.11. Quand la quantité $|\Sigma|$ est bornée, les inégalités des corollaires 3.4.16 et 3.4.18 restent valables. Par contre, si on cherche à connaître l'évolution suivant la croissance de $|\Sigma|$, il vient la borne

$$\ln\big(a(\chi)+|\Sigma|\big)\frac{\left(r^2 \ln|\text{disc } K| + 2k(r-k)\sum_{\mathfrak{p}\in\Sigma}\ln \mathrm{N}(\mathfrak{p})\right)^2}{\ln|\Sigma|} \ll_{K,r,k} \Big(\sum_{\mathfrak{p}\in\Sigma}\ln \mathrm{N}(\mathfrak{p})\Big)^2.$$

3.5 Expérimentations numériques avec le groupe A_n

Nous allons nous placer dans le contexte des extensions non ramifiées de groupe de Galois le groupe alterné A_n pour tester la borne du corollaire 3.1.3 : déterminer le premier de plus petite norme dont le Frobenius sépare des caractères irréductibles de même degré. Une borne est donnée en fonction du carré du logarithme du discriminant du corps de base et des puissances quatrièmes des degrés des représentations. Rappelons que par la théorie du corps de classes, les extensions abéliennes sont liées au groupe des classes (et leurs caractères irréductibles sont de degré 1). Pour les extensions non ramifiées de groupes de Galois simples (donc non abéliens), il n'y a plus la théorie du corps de classes.

3.5.1 Familles et expérimentations

Nos calculs vont se faire dans des familles de trinômes irréductibles de $\mathbb{Q}[X]$ de la forme : $P = X^n + uX + v$, avec $u, v \in \mathbb{Q}$. De telles familles ont été étudiées par de nombreux auteurs (Yamamoto [Yam70] ou Uchida [Uch70]). Rappelons le critère de Uchida :

Théorème 3.5.1 ([Uch70], Theorem 1). *Soit $P = X^n + uX + v \in \mathbb{Q}[X]$ un polynôme $\mathbb{Q}$-irréductible de corps des racines L. Si n est un nombre premier et si $((n-1)u, nv) = 1$, alors le groupe de Galois de P est isomorphe au groupe S_n et l'extension $L/\mathbb{Q}(\sqrt{\text{disc } P})$ est non ramifiée.*

Soient $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ les racines de P. Notons $M = \mathbb{Q}(\alpha_1)$ un corps de rupture de P, $L = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ le corps de décomposition de P et disc $P := \prod_{i<j}(\alpha_i - \alpha_j)^2$ le discriminant de P. Posons $K = \mathbb{Q}(\sqrt{\text{disc } P})$. Pour un tel trinôme $P = X^n + uX + v$, $u, v \in \mathbb{Q}$,

un calcul classique (voir [Sam67] page 49 ou [Uch70]) montre que :

$$\text{disc } P = (-1)^{\frac{n(n-1)}{2}}\Big(n^n v^{n-1} + (-1)^{n-1}(n-1)^{n-1}u^n\Big).$$

PROPOSITION 3.5.2. *Le discriminant d du polynôme $P = X^n + uX + v \in \mathbb{Q}[X]$, n impair, vérifie les propriétés suivantes :*

(i) $d \equiv 0$ *ou* $1 \pmod 4$ *et* $d \equiv 0 \pmod 4$ *si et seulement si v est pair ;*

(ii) lorsque $n \geqslant 5$, d est le discriminant d'un corps quadratique si et seulement s'il est sans facteurs carrés ; dans ce cas, $((n-1)u, nv) = 1$. En particulier, v est impair.

PREUVE

(i) Dans le cas où $n = 2k+1$ est un nombre premier supérieur à 2, le discriminant vaut $d = (-1)^{k(2k+1)}\Big((2k+1)^{2k+1}v^{2k} + (2k)^{2k}u^{2k+1}\Big)$ d'où $d \equiv (-1)^k(2k+1)^{2k+1}v^{2k} \bmod 4$ (car $(2k)^{2k} = 4^k k^{2k} \equiv 0 \bmod 4$). D'autre part, en distinguant les cas k pair ou impair, on obtient $(-1)^k(2k+1)^{2k+1} \equiv 1 \pmod 4$ et $v^{2k} \equiv 1 \bmod 4 \Leftrightarrow v$ est impair.

(ii) Supposons que d est le discriminant du corps quadratique $\mathbb{Q}(\sqrt{m})$ avec m sans facteurs carrés. Alors soit $d = m \equiv 1 \pmod 4$ soit $d = 4m$ lorsque $m \equiv 2$ ou $3 \bmod 4$. Or d'après l'écriture de d, si 4 divise d alors 16 divise d donc ce dernier cas ne peut pas arriver. On peut donc écrire d sans facteurs carrés.

Réciproquement, si d est sans facteurs carrés alors $d \equiv 1 \bmod 4$ (puisque 4 ne peut pas diviser d), d est donc le discriminant du corps quadratique $\mathbb{Q}(\sqrt{d})$.

Notons b le pgcd $((n-1)u, nv)$. Par définition, il existe des entiers c_1 et c_2 tels que $(n-1)u = c_1 b$ et $nv = c_2 b$ avec $(c_1, c_2) = 1$. On peut alors écrire, en notant $n = 2k+1$, $d = (-1)^{\frac{n(n-1)}{2}} b^{2k}(nc_2^{n-1} + (-1)^{n-1}uc_1^{n-1})$. Ainsi, $((n-1)u, nv) = 1$ (sinon d possède un facteur carré non trivial). □

Lorsque les caractères du groupe alterné considérés sont des caractères conjugués, on utilise le théorème 3.3.10 qui nous donne un critère (en étudiant l'irréductibilité du polynôme modulo les nombres premiers) pour obtenir le premier nombre premier pour lequel le Frobenius sépare les caractères.

Nous nous concentrons sur des familles de trinômes P_a de degré n à un seul paramètre, pour $n = 5, 7$ et 13, dont les groupes de Galois sous-jacents sont isomorphes à S_n. Ici, a est un paramètre qui va varier dans l'ensemble des nombres naturels $\mathbb{N}$. Pour un tel entier a, le groupe de Galois de L/K est isomorphe à A_n et si par exemple le discriminant $d_a = \text{disc } P_a$ est sans facteurs carrés, alors L/K est non ramifiée (d'après la proposition 3.5.2 et le théorème 3.3.2). Nous ressortons ensuite deux caractères χ et χ' de même degré (typiquement des caractères conjugués) et nous cherchons donc la plus petite norme $n(\chi, \chi')$ associée à un idéal premier $\mathfrak{p}$ dont le Frobenius sépare les caractères étudiés.

Nous déterminerons également pour X assez grand la quantité

$$\mu(P_a, \chi, \chi', X) := \frac{\displaystyle\sum_{d_a \leqslant X} n(\chi, \chi')}{\displaystyle\sum_{d_a \leqslant X} 1}.$$

À travers nos exemples, cette proportion semble se stabiliser assez vite. Une question naturelle se pose alors au sujet du lien entre cette valeur de convergence et les caractères choisis.

Un point clef pour cette étude est de bien nous assurer que ces familles de polynômes sont "exhaustives" en vérifiant que celles-ci contiennent une sous-famille de paramètres $(a_k)_k$ telle que : (i) le polynôme P_{a_k} est $\mathbb{Q}$-irréductible ; (ii) le groupe de Galois du corps des racines de P_{a_k} est S_n ; (iii) la quantité $n(\chi, \chi')$ peut être aussi grande que possible.

Nos expérimentations consistent à faire varier a entre 1 et 300 000 pour le groupe alterné A_{13} (jusqu'à 500 000 pour les groupes alternés A_5 et A_7). À chaque valeur de a permettant au polynôme P_a de satisfaire les conditions du théorème 3.5.1, nous calculons le discriminant d_a ainsi que la norme du plus petit premier dont le Frobenius sépare les caractères χ et χ'. Pour des raisons de lisibilité, nous nous limitons à l'affichage de la plus grande norme lorsque a varie entre n et $n + 100$.
Le deuxième graphique obtenu correspond à l'évolution de $\mu(P_a, \chi, \chi', x)$ lorsque x varie entre 1 et 300 000 pour le groupe alterné A_{13} (jusqu'à 500 000 pour les groupes alternés A_5 et A_7). Pour les mêmes raisons, nous utilisons un point par tranche de 1 000.

3.5.1.1 Le groupe A_5

Commençons par le polynôme $P_a = X^5 + X + a$ de discriminant $d_a = 5^5a^4 + 4^4$. On s'intéresse aux paramètres a pour lesquels P_a est $\mathbb{Q}$-irréductible et d_a est le discriminant d'un corps quadratique. Alors, comme nous l'avons vu dans la proposition 3.5.2, nécessairement a est impair et la condition sur d_a est équivalente au fait que d_a est sans facteurs carrés. Si tel est le cas, on se retrouve dans le cadre du théorème 3.5.1 donc le groupe de Galois sous-jacent est S_5, il fournit ainsi une extension non ramifiée L_a/K_a de groupe de Galois A_5 au-dessus du corps quadratique réel $K_a = \mathbb{Q}(\sqrt{d_a})$.
Dans le groupe A_5, il y a cinq classes de conjugaison $\mathscr{C}_1 = (1)$, $\mathscr{C}_2 = (123)$, $\mathscr{C}_3 = (12)(34)$, $\mathscr{C}_4 = (12345)$ et $\mathscr{C}_5 = (21345)$ et deux caractères irréductibles conjugués χ et χ' de degré 3 provenant d'un caractère irréductible de S_5 de degré 6 dont la classe associée est celle des 5-cycles.

On cherche le premier $\mathfrak{p} \subset \mathscr{O}_K$ de plus petite norme pour lequel les caractères χ et χ' de degré 3 de $\mathrm{Gal}(L_a/K_a) \simeq A_5$ sont différents en le Frobenius $\sigma_{\mathfrak{p}}$. Cela équivaut à déterminer le plus petit nombre premier p pour lequel $P_a \in \mathbb{F}_p[X]$ est irréductible (voir théorème 3.3.10).
Testons l'exhaustivité de la famille. Soient $p_1 = 2, \ldots, p_k$ les k premiers nombres premiers et soit $a_k = -2 - p_2 \cdots p_k$. La factorisation de P_{a_k} dans $\mathbb{F}_7[X]$ indique que P_{a_k} est irréductible sur $\mathbb{Q}$: les polynômes irréductibles sur $\mathbb{Z}/p\mathbb{Z}$ sont irréductibles sur $\mathbb{Z}$ et la factorisation modulo 2 permet d'affirmer qu'il n'y a pas de racine dans $\mathbb{Z}$. Par le résultat de Uchida (théorème 3.5.1), l'extension sous-jacente est de groupe de Galois S_5 puisque 2 ne divise pas a_k. D'autre part pour $i = 2, \ldots, k$, il vient $P_{a_k}(1) \equiv 0 \pmod{p_i}$ et on peut vérifier que P_{a_k} est également réductible dans $\mathbb{F}_2[X]$. Par conséquent, le plus petit premier p dont le Frobenius sépare les caractères χ et χ' est plus grand que p_{k+1} :

$$n(\chi, \chi') \geqslant p_{k+1}.$$

Comme $\ln |d_{a_k}| \sim_{k\to\infty} C \cdot \ln p_1 \cdots p_k \sim_k C \cdot p_k$, la borne de séparation des caractères χ et χ' donnée par le corollaire 3.1.3 est alors en p_k^2 (à une constante près). Ceci est donc à comparer avec le premier de plus petite norme qui sépare χ et χ', de norme au moins p_{k+1}.
Notons à ce niveau que, sous l'hypothèse de Riemann généralisée, $p_{k+1} \leqslant p_k + p_k^{\frac{1}{2}+\varepsilon}$ (voir [Nic69]).

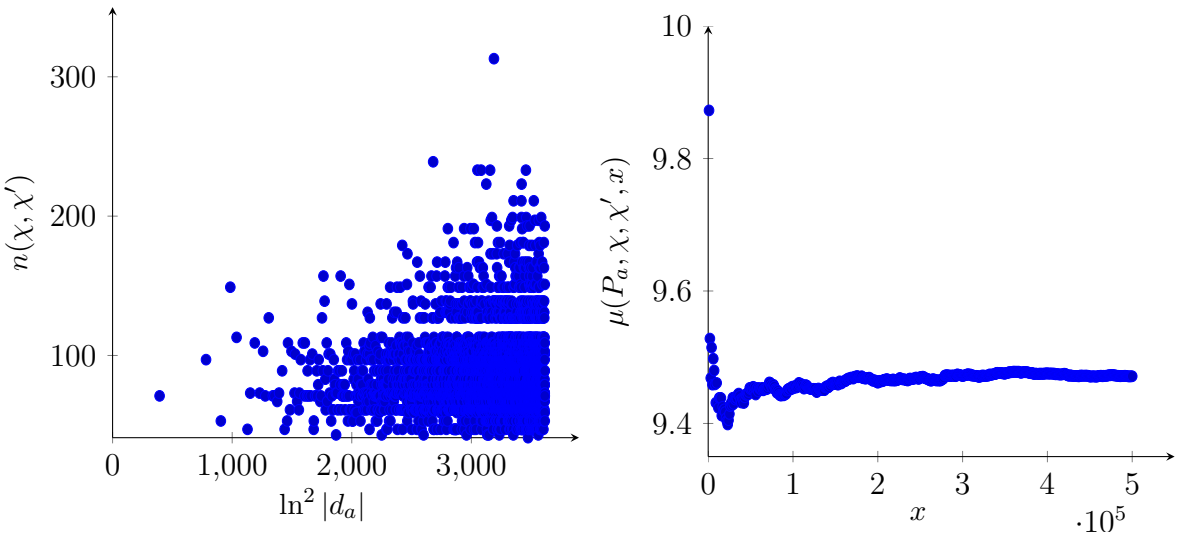


FIGURE 3.1 – Pour les caractères de degré 3 de A_5 définis par $P_a = X^5 + X + a$

Le plus grand nombre premier obtenu dans les 183 962 corps quadratiques étudiés est 313 pour le polynôme $X^5 + X + 180\ 895$ de discriminant $3 \cdot 7 \cdot 43 \cdot 3705685202388396493027$ qu'on peut approcher par $3,4 \cdot 10^{24}$.

De la même façon, considérons la famille de polynômes $P_a = X^5 - aX + 1$ avec a tel que P_a est $\mathbb{Q}$-irréductible et tel que d_a est sans facteurs carrés. Ici $d_a = 5^5 - 4^4 a^5$ et les corps quadratiques $K = \mathbb{Q}(\sqrt{d_a})$ sont imaginaires.
En posant $a_k = 2 + p_2 \dots p_k$, la famille de polynômes P_{a_k} vérifie bien les conditions d'exhaustivité voulues : comme a_k est premier à 5 (condition nécessaire pour que d_a soit sans facteurs carrés), le groupe de Galois sous-jacent est S_5 ; la réduction dans $\mathbb{F}_5$ donne l'irréductibilité ; comme pour le cas précédent, $P_{a_k}(1) \equiv 0 \pmod{p_i}$ pour $i = 2, \dots, k$ et ainsi le plus petit premier p dont le Frobenius sépare les caractères χ et χ' associés aux 5-cycles est plus grand que p_{k+1}.
Quand $1 \leqslant a \leqslant 500\ 000$, nous obtenons une famille de 341 266 corps à étudier. Le plus grand nombre premier obtenu est 331 pour le polynôme $X^5 - 153\ 032X + 1$, de discriminant $-3 \cdot 2129 \cdot 336398708600765077320084 1 \approx -2,2 \cdot 10^{28}$.

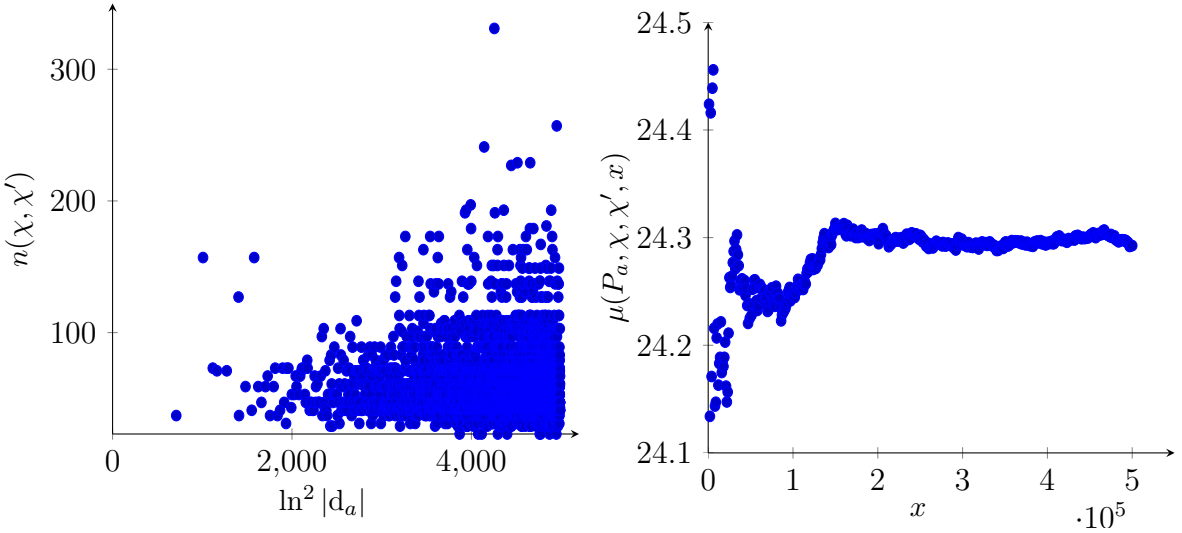


FIGURE 3.2 – Pour les caractères de degré 3 de A_5 définis par $P_a = X^5 - aX + 1$

3.5.1.2 Le groupe A_7

Dans A_7, il y a deux caractères irréductibles de degré 10 et deux caractères irréductibles de degré 14.

Les caractères de degré 10. Comme pour les caractères irréductibles de degré 3 de A_5, les deux caractères irréductibles de degré 10 sont conjugués et proviennent d'un même caractère irréductible de S_7. Ils sont séparés par le Frobenius $\sigma_{\mathfrak{p}}$ lorsque celui-ci est un 7-cycle, ce qui équivaut au fait que $P \in \mathbb{F}_p[X]$ est irréductible.
Pour $1 \leqslant a \leqslant 500\,000$, considérons les polynômes irréductibles $P_a = X^7 - 2X + a$ dont les discriminants sont sans facteurs carrés (cela implique $(a, 6) = 1$) : on obtient une famille de 150 072 corps.
En posant $a_k = 1 + p_1 \dots p_k$, le polynôme P_{a_k} vérifie bien les conditions d'exhaustivité. En effet, P_{a_k} se réduit modulo 3 en $X(X^6 + X^5 + X^4 + X^3 + X^2 + X + 2)$, le polynôme $X^6 + X^5 + X^4 + X^3 + X^2 + X + 2$ étant irréductible dans $\mathbb{F}_3$, il y a deux possibilités : soit P_{a_k} est $\mathbb{Q}$-irréductible soit il se décompose en deux polynômes, l'un de degré 1 et l'autre de degré 6. Or on peut montrer que le polynôme P_{a_k} n'a pas de racine dans $\mathbb{Q}$: s'il en avait une, notons-la m, alors m serait dans $\mathbb{Z}$ et diviserait a_k ; en utilisant la réduction modulo 3 et le fait que $a_k \equiv m \equiv 1 \bmod 3$, on arrive à une contradiction. Le résultat de Uchida montre que le groupe sous-jacent est S_7 (puisque 6 ne divise pas a_k) et comme $P_{a_k}(1) \equiv 0 \pmod{p_i}$ pour $i = 1, \dots, k$, on obtient bien que le plus petit nombre premier pour lequel P_{a_k} est irréductible dans $\mathbb{F}_p$ est supérieur à p_{k+1}.
Dans la liste obtenue, on note que le plus grand nombre premier obtenu est 461 pour le polynôme $X^7 - 2X + 432\,131$ de discriminant $-5 \cdot 11 \cdot 199 \cdot 26796293 \cdot 138350621 \cdot 132162187786326150319 \approx 5,4 \cdot 10^{40}$.

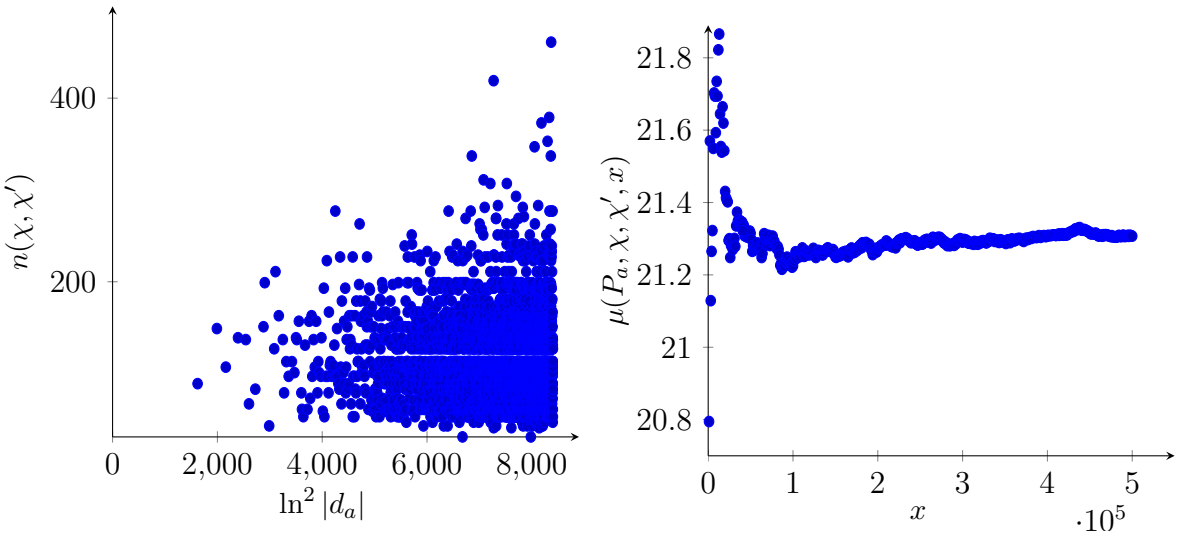


FIGURE 3.3 – Pour les caractères de degré 10 de A_7 définis par $P_a = X^7 - 2X + a$

Les caractères de degré 14. Les deux caractères irréductibles de degré 14 proviennent des partitions $(4, 3)$ et $(5, 2)$, ils ne sont pas conjugués. Les caractères χ et χ' ont les mêmes polynômes caractéristiques pour 6 classes de conjugaison mais n'ont pas les mêmes pour 3 classes (donc pas les mêmes valeurs propres) ni la même trace : ce sont les classes où intervient au moins un 3-cycle (il y a donc les 3-cycles, les produits de deux 3-cycles

et le produit d'un 3-cycle avec deux transpositions). Ainsi, le Frobenius $\sigma_{\mathfrak{p}}$ sépare les caractères de degré 14 si et seulement si il est dans une classe contenant un 3-cycle.
Utilisons nos observations du paragraphe 3.3.2.
Si p est non ramifié, $\sigma_{\mathfrak{p}}$ contient un 3-cycle si et seulement si 3 divise f_i pour un certain entier i : en effet, $\sigma_{\mathfrak{p}} = [f_1]\cdots[f_g]$ ou $\sigma_{\mathfrak{p}} = ([f_1]\cdots[f_g])^2$ et un 6-cycle au carré se décompose en un produit de deux 3-cycles. Ceci peut se lire dans la factorisation de P dans $\mathbb{F}_p[X]$: puisque $\mathscr{O}_M \simeq \mathbb{Z}[X]/(P)$ (M un corps de rupture de P), on obtient que $\sigma_{\mathfrak{p}}$ contient un 3-cycle si et seulement si $P \in \mathbb{F}_p[X]$ contient un facteur irréductible de degré 3 ou 6.
Si p est ramifié, d'après le lemme 3.3.4 et la proposition 3.3.5, $\sigma_{\mathfrak{p}}$ contient un 3-cycle si et seulement si $P \in \mathbb{F}_p[X]$ contient un facteur irréductible de degré 3.

En conclusion, le Frobenius $\sigma_{\mathfrak{p}}$, avec $\mathfrak{p} \mid p$, sépare les caractères de degré 14 si et seulement si la factorisation de $P \in \mathbb{F}_p[X]$ contient un facteur irréductible de degré 3 ou 6 (sous la condition sur disc P).
Soit la famille $P_a = X^7 - X + a$. En posant $a_k = p_3 \dots p_k$, le polynôme P_{a_k} vérifie bien les conditions voulues : P_{a_k} est irréductible modulo 2 ; comme pour $3 \leqslant i \leqslant k$, $P_{a_k} \equiv X^7 - X \equiv X(X-1)(X+1)(X^2-X+1)(X^2+X+1) \bmod p_i$, le plus petit nombre premier pour lequel on peut trouver un 3-cycle ou un 6-cycle est supérieur à p_{k+1} (pour p_2, on utilise les réductions modulo 3 avec $a_k \equiv 1$ ou $2 \bmod 3$). D'après le théorème 3.5.1, l'extension sous-jacente est de groupe de Galois S_7 puisque 6 ne divise pas a_k.

Sur les 162 866 corps étudiés, la plus grande norme de nombre premier obtenue est $83^2 = 6\ 889$ pour le polynôme $X^7 - X + 254\ 005$, de discriminant $-29 \cdot 47 \cdot 337 \cdot 481519763744768140611173622940549 \approx 2,3 \cdot 10^{39}$.

Notons que les sauts apparaissant dans le graphique correspondant sont dus au fait que la norme des idéaux premiers peut valoir le carré d'un nombre premier, celui-ci pouvant se ramifier.

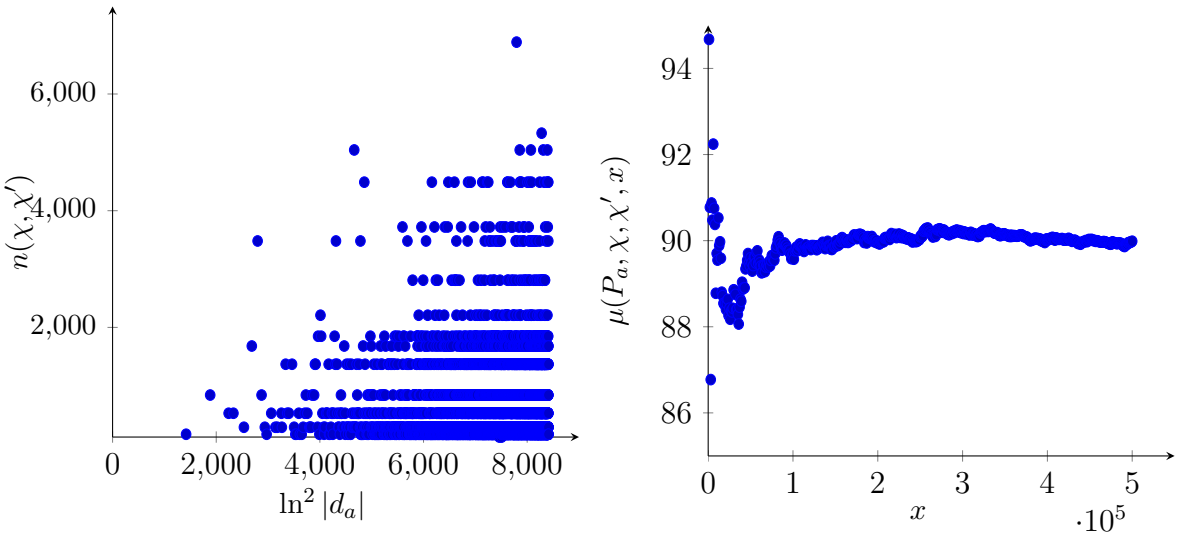


FIGURE 3.4 – Pour les caractères de degré 14 de A_7 définis par $P_a = X^7 - X + a$

3.5.1.3 Le groupe A_{13}

Il y a 3 couples de caractères irréductibles provenant de tableaux de Young symétriques :

— un couple de caractères de degré 462 séparés par les cycles de longueur 13 et donc par les Frobenius des premiers p pour lesquels P est irréductible dans $\mathbb{F}_p[X]$;
— un couple de caractères de degré 4 290 séparés par les Frobenius des premiers p pour lesquels $P = Q_7Q_5Q_1 \in \mathbb{F}_p[X]$, où les polynômes Q_i sont irréductibles de degré i ;
— un couple de caractères de degré 8 008 séparés par les Frobenius des premiers p pour lesquels $P = Q_9Q_3Q_1 \in \mathbb{F}_p[X]$, où les polynômes Q_i sont irréductibles de degré i.

Soit $P_a = X^{13} + X + a$. En prenant $a_k = -2 + p_2 \cdots p_k$, 12 et $13a_k$ sont premiers entre eux donc le résultat de Uchida indique que le groupe de Galois sous-jacent est S_{13}. De plus, le polynôme P_{a_k} vérifie la condition d'exhaustivité pour les caractères de degré 462 : les réductions modulo 2 et 43 donnent l'irréductibilité. Comme $P_{a_k}(1) \equiv 0 \bmod p_i$ pour $i = 2, \ldots, k$, le plus petit nombre premier pour lequel P_{a_k} est irréductible dans $\mathbb{F}_p$ est bien supérieur à p_{k+1}.
Soit $(a_k)_k$ la famille de paramètres définis par $a_k \equiv 0 \bmod p_3p_5 \cdots p_k$ et $a_k \equiv 1 \bmod 7$. On a toujours 12 et $13a_k$ premiers entre eux donc le groupe de Galois sous-jacent est S_{13}. De plus, la factorisation modulo 2 de P_{a_k} permet d'en déduire qu'il n'a pas de racine dans $\mathbb{Z}$, si on combine cette information avec sa factorisation modulo 7, on obtient l'irréductibilité de P_{a_k}. La factorisation modulo p_i, pour $i \geqslant 5$, $P_{a_k} \equiv X^{13} + X = X(X^4+1)(X^8-X^4+1)$ montre qu'il ne peut apparaître ni de 9-cycle ni de produit d'un 5-cycle avec un 7-cycle. Cette famille passe le test d'exhaustivité pour les caractères de degré 4 290 et 8 008.

Nous nous intéressons donc aux polynômes $P_a = X^{13} + X + a$, $\mathbb{Q}$-irréductibles, pour lesquels les discriminants sont sans facteurs carrés. Cela représente 84 374 corps.

Pour les caractères de degré 462, le plus grand nombre premier obtenu est 929 pour le polynôme $X^{13} + X + 247\,285$.

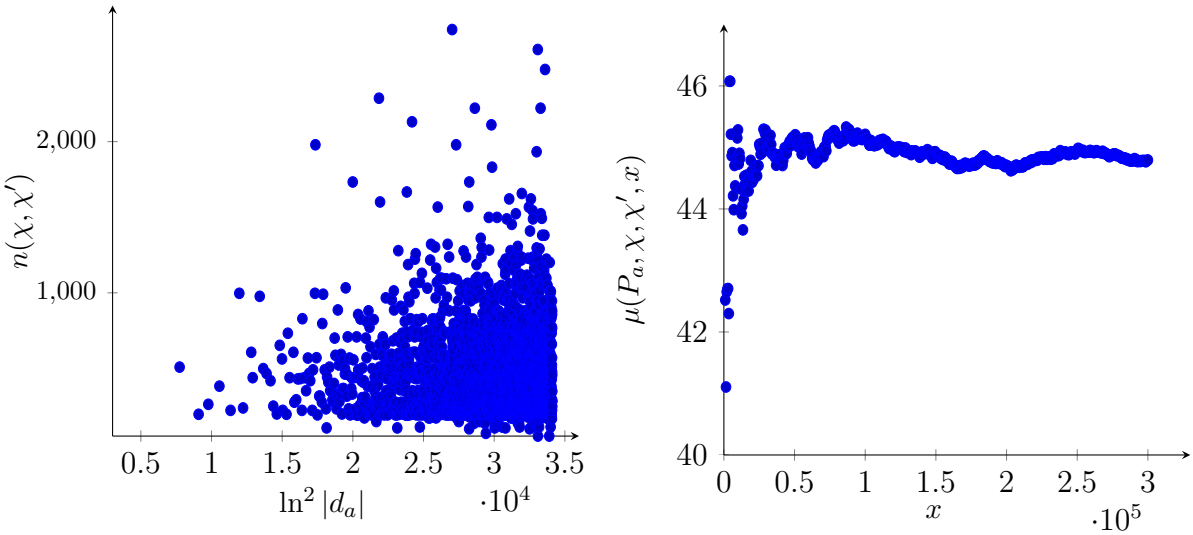


FIGURE 3.5 – Pour les caractères de degré 462 de A_{13} définis par $P_a = X^{13} + X + a$

Pour la séparation des caractères de degré 4 290, le plus grand nombre premier obtenu est 2 741 pour le polynôme $X^{13} + X + 55\,355$.
Pour les caractères de degré 8 008, le plus grand nombre premier obtenu est 1993 pour le polynôme $X^{13} + X + 54\,983$.

Remarque 3.5.3. Pour le groupe A_{13}, regardons la variation de la borne du corollaire 3.1.3 en fonction du degré r lorsque $\ln|\text{disc } K|$ varie "peu", en lisant en parallèle et

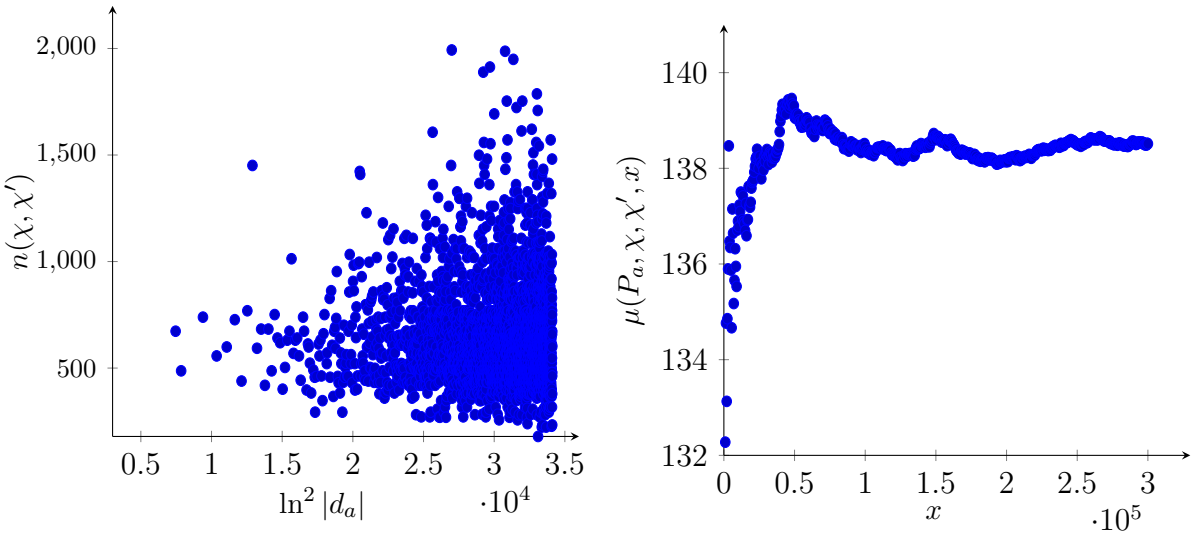


FIGURE 3.6 – Pour les caractères de degré 4290 de A_{13} définis par $P_a = X^{13} + X + a$

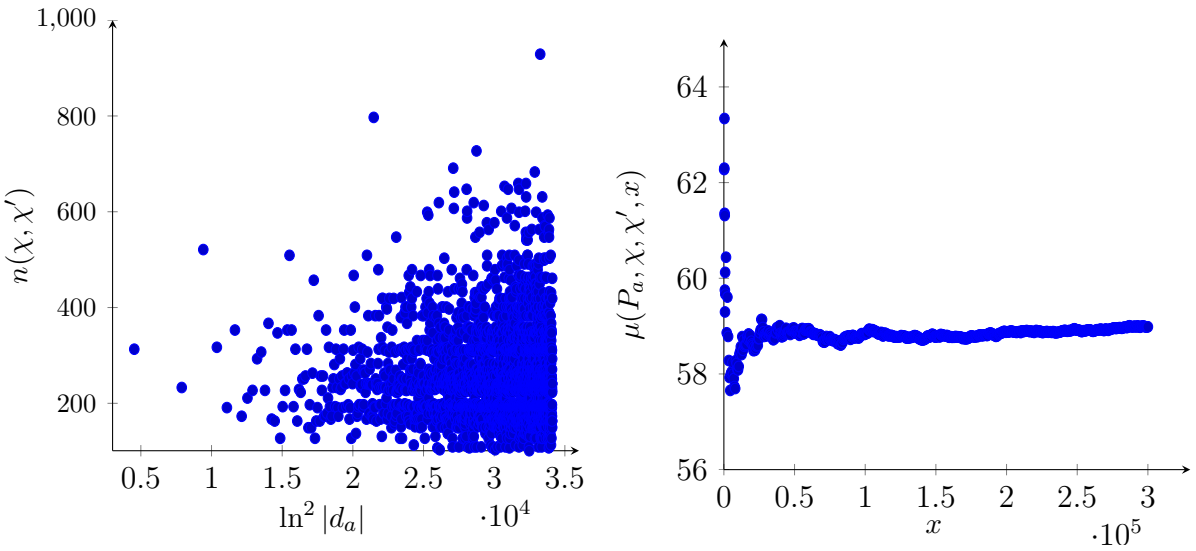


FIGURE 3.7 – Pour les caractères de degré 8008 de A_{13} définis par $P_a = X^{13} + X + a$

"verticalement" les trois diagrammes. Par exemple, le ratio entre $r = 8\ 008$ et $r = 462$ est de 52 ; le carré de ce ratio, voire la puissance 4e de ce ratio, est alors à comparer aux axes des ordonnées des graphes associés aux caractères en question.

3.5.2 Sur une question diophantienne

Pour finir, revenons à la famille de polynômes de la forme $P_a = X^n - aX + 1$ de discriminant $d_a = n^n - (n-1)^{n-1}a^n$. Si l'on s'assure que le polynôme P_a est $\mathbb{Q}$-irréductible, que $n \geqslant 5$ est premier (pour simplifier, on peut prendre $n = 5$) et que $(a, n) = 1$, alors le résultat de Uchida [Uch70] évoqué précédemment, indique que le corps de décomposition de P_a est une extension non ramifiée de groupe de Galois A_n au-dessus de $\mathbb{Q}(\sqrt{d_a})$.

Soit $d < 0$ un entier négatif sans facteurs carrés et soit le corps quadratique $K = \mathbb{Q}(\sqrt{d})$. Intéressons-nous à la problématique suivante : quand a varie, connaître le nombre de fois où il apparaît une extension non ramifiée au-dessus de K de groupe de Galois A_n, le tout donné par un polynôme P_a. Ou encore, d'après le résultat de Uchida, déterminer les entiers a tels $d_a = db^2$, où b est un entier. On tombe ainsi sur l'équation diophantienne

(hyperelliptique) suivante :

$$n^n - (n-1)^{n-1}X^n = dY^2 \tag{3.1}$$

et à ses solutions entières. C'est une équation de genre $g = \frac{(n-1)}{2} > 1$. D'après les travaux de Siegel, on sait que l'équation (3.1) n'a qu'un nombre fini de solutions entières. Se posent alors deux questions : (a) quel est le nombre de solutions ? ; (b) quelle est la taille des solutions ?

Commençons par regarder la question du nombre de solutions. Le résultat principal de Rémond dans [Rém10] sur l'effectivité du résulat de Siegel montre pour notre situation que le nombre M de couples entiers (X, Y) solutions de (3.1) est au plus $\exp\left(5^{n^4} n \ln n \ln(n \ln n)\right)$ et ainsi

$$\ln M \ll 5^{n^4} n \ln n.$$

Supposons à présent que l'entier $n = \ell$ est un nombre premier. Si le polynôme P_a est $\mathbb{Q}$-irréductible, il donne lieu alors à une extension non ramifiée de groupe de Galois A_n au-dessus du corps $\mathbb{Q}(\sqrt{d_a})$. D'autre part, d'après l'exemple 3.4.9, si $\mathscr{N}(A_n)$ désigne le nombre d'extensions non ramifiées linéairement indépendantes de K de groupe de Galois A_n, alors

$$\ln \mathscr{N}(A_n) \ll n^4.$$

Les quantités M et $\mathscr{N}(A_n)$ donnent chacune à leur façon une borne sur le nombre d'extensions de groupe de Galois A_n non ramifiées données par la famille des polynômes $(P_a)_a$ au-dessus d'un corps quadratique K fixé.
À ce stade, on peut voir apparaître plusieurs questions. Typiquement : (i) Peut-on abaisser la borne de Rémond dans notre contexte ? (ii) Soient $a \neq a'$ tels que $d_a = d_{a'} b^2$. Les corps de décomposition associés aux polynômes P_a et $P_{a'}$ peuvent-ils être identiques ?

Une autre direction serait la problématique de la taille des solutions de l'équation (3.1), c'est-à-dire la question de l'effectivité de la méthode Baker. Notre référence pour cette question est le travail [Bug97] de Bugeaud.
Trouver une borne sur la hauteur des solutions entières de l'équation de départ (3.1) revient à trouver une borne sur la hauteur des solutions de l'équation

$$\alpha X^n = -Y^2 + \beta, \tag{3.2}$$

où $\alpha = d(n-1)^{n-1}$ et $\beta = dn^n$.
En appliquant alors le théorème 2 de [Bug97], on trouve que si (x, y) est solution de (3.2), alors

$$|y| \ll \exp\left((4\beta)^{10n} \alpha^{4n} (\ln 4\alpha\beta)^{8n}\right),$$

ce qui grossièrement donne

$$\ln |y| \ll n^{(10+\varepsilon)n^2}.$$

En pratique les formes linéaires montrent pour certaines équations toute leur puissance et la question suivante doit être lue dans ce cadre :
Question : Est-il possible de baisser significativement la borne sur $|y|$?
Concrètement, prenons $n = 5$. Etant donné d (pas trop grand), trouver toutes les solutions entières de l'équation (3.1) (en particulier quand celle-ci en a au moins une) ?

Annexe A

Programmes dans le cas $K = \mathbb{Q}$

Dans le cas où le corps de base est $\mathbb{Q}$, en gardant les mêmes notations, la fonction L d'Artin s'écrit comme un produit sur les nombres premiers :

$$L(s,\chi,L/\mathbb{Q}) = \sum_{n\geqslant 1} \frac{a_\chi(n)}{n^s} = \prod_{p\in\mathbb{Z}} \frac{1}{\det(\mathrm{Id} - p^{-s}\sigma_p; V^{I_p})} = \prod_{p\in\mathbb{Z}}\prod_{i=1}^{d} \left(1-\alpha_{i,\rho}(p)p^{-s}\right)^{-1}.$$

En notant φ_p un représentant dans D_p du Frobenius σ_p engendrant D_p/I_p, on obtient $\rho(\varphi_p) \in \mathrm{GL}(V^{I_p})$ donc le déterminant correspond au déterminant de la restriction de la matrice $\rho(\varphi_p)$ à V^{I_p}.
Soit P un polynôme à coefficients rationnels définissant un corps de nombres L galoisien au-dessus de $\mathbb{Q}$. On note $G = \mathrm{Gal}(L/\mathbb{Q})$. On note ρ_r la r^e (au sens de GAP) représentation du groupe G.
Pour simplifier les notations, a désigne une racine primitive n^e de l'unité, on la définit comme une racine du polynôme cyclotomique de degré n. Elle apparaît sous la forme de $E(n)$ dans GAP.
Notons $\mathscr{B}$ la base de $\mathbb{C}^{\deg\rho_r}$ dans laquelle est donnée la représentation.

A.1 Représentations

Dans GAP, le programme suivant permet d'obtenir l'image de tous les éléments d'un groupe G par la n^e représentation de G. Dans ce cas, chaque élément du groupe est déterminé par l'image de 1.

```
Rep := function(G,n)
  local R, gens;
  gens:= GeneratorsOfGroup(G);
  R := IrreducibleRepresentations(G);
  PrintTo("representation.g","{\n");
  AppendTo("representation.g",List(AsList(G),g->[1^g,Image(R[n],g)]));
  AppendTo("representation.g","}\n");
end;
Read("group.g"); Rep(G,n);
```

En faisant appel à cette fonction, le premier programme ci-dessous retourne l'image de chaque élément de G par la r^e représentation ρ_r dans PARI/GP. La seconde fonction permet d'obtenir pour chaque élément g du groupe, le déterminant de la matrice $\mathrm{Id}-\rho_r(g)$. Et la troisième combine ces deux résultats en donnant ces vecteurs l'un à la suite de l'autre.

```
install(group_elts,GL)
install(group_order,lG)


justerep(P,r)=
{
  X='X;
  my(G,R);
  G=galoisinit(P);
  local(n=poldegree(P));
  system("rm -f group.g representation.g");
  write1("group.g","G:=");
  write1("group.g",galoisexport(G));
  write("group.g",Str("; n:=",r,";"));
  system("gap -q -n Rep.g </dev/null");
  local(z = Mod('a,polcyclo(n,'a)));
  local(E=k->z^(n/k));
  R=read("representation.g");
  return(R);
}

fun(P,r)=
{
  X='X;
  my(G,M,V,R);
  G=galoisinit(P);
  local(n=poldegree(P));
  system("rm -f group.g representation.g");
  write1("group.g","G:=");
  write1("group.g",galoisexport(G));
  write("group.g",Str("; n:=",r,";"));
  system("gap -q -n Rep.g </dev/null");
  local(z = Mod('a,polcyclo(n,'a)));
  local(E=k->z^(n/k));
  R=read("representation.g");
  V=vector(n,i,
    M = Mat(apply(x->x~,R[i][2]))~;
    [R[i][1],matdet(1-X*M)]);
  return(V);
}
```

```
funandR(P,r)=
{
  X='X;
  my(G,M,V,R);
  G=galoisinit(P);
  local(n=poldegree(P));
  system("rm -f group.g representation.g");
  write1("group.g","G:=");
  write1("group.g",galoisexport(G));
  write("group.g",Str("; n:=",r,";"));
  system("gap -q -n Rep.g </dev/null");
  local(z = Mod('a,polcyclo(n,'a)));
  local(E=k->z^(n/k));
  R=read("representation.g");
  V=vector(n,i,
    M = Mat(apply(x->x~,R[i][2]))~;
    [R[i][1],matdet(1-X*M)]);
  return([V,R]);
}
```

A.2 Frobenius

Les éléments de G sont représentés par des permutations de l'ensemble E des racines p-adiques du polynôme P (où p est totalement décomposé).
Le premier nombre d'une permutation de G correspond à l'image de la première racine, elle détermine en fait complètement l'élément de G.
Pour les premiers non ramifiés dans L, la commande $idealfrobenius$ renvoie le Frobenius comme un élément de G exprimé sous forme de permutation. Les programmes suivants permettent d'obtenir le même résultat pour les premiers ramifiés. Rappelons la définition d'un Frobenius σ_p d'un nombre premier p non ramifié : $\sigma_p(x) \equiv x^p \pmod{\mathfrak{p}}$ pour tout $x \in \mathscr{O}_L$, où $\mathfrak{p}$ est un idéal premier de L au-dessus de p. Dans le cas d'un premier ramifié, on utilise cette définition afin de trouver φ_p, un antécédent du générateur σ_p du quotient D_p/I_p. Ici, le résultat est indépendant du choix de $\mathfrak{p}$. L'idée est alors de tester chaque élément du groupe G. Dès lors qu'un élément vérifie cette égalité pour tous les éléments de la base de l'anneau $\mathscr{O}_L$, on le définit comme le Frobenius de p.
La première fonction ci-dessous donne, pour les K premiers nombres premiers, l'expression de leur Frobenius sous forme d'un vecteur correspondant aux puissances des générateurs de G. En utilisant ce résultat, le second programme nous permet d'obtenir le Frobenius du premier p sous forme de permutation.

```
isfrob2(P,K)=
{
  my(d,N,G,A,r,v,B,m,M,u,H,o,V,z,Q,s,j,pr,qr);
  N=nfinit(P);
```

```
  G=galoisinit(P);
  d=poldegree(P);
  A=G.gen;
  r=length(A);
  v=primes(K);
  B=N.zk;
  m=length(B);
  o=G.orders;
  M=vector(K);
  forvec(u=vector(r,k,[0,o[k]-1]),
     Q=Vecsmall(vector(d,i,i));
     for(s=1,r,Q=Q*A[s]^u[s]);
     H=galoispermtopol(G,Q);
     for(i=1,K,
          pr=idealprimedec(N,v[i])[1];
          qr=nfmodprinit(N,pr);
      if(M[i]==0,
               j=1;
               while(nfeltreducemodpr(N,nfgaloisapply(N,H,B[j]),qr)==
                   nfeltreducemodpr(N,nfeltpowmodpr(N,B[j],v[i],qr),qr)
                    &j<m
               ,j=j+1);
      if(j=m &
          nfeltreducemodpr(N,nfgaloisapply(N,H,B[j]),qr)==
          nfeltreducemodpr(N,nfeltpowmodpr(N,B[j],v[i],qr)
          ,qr)
     ,M[i]=[v[i],vector(r,c,u[c])]))));
  return(M);
}


frobram(P,p)=
{
  my(i,Z,A,r,Q,G,N);
  N=nfinit(P);
  G=galoisinit(P);
  A=G.gen;
  r=length(A);
  i=primepi(p);
  Z=isfrob2(P,i)[i][2];
  Q=Vecsmall(vector(poldegree(P),i,i));
  for(s=1,r,Q=Q*A[s]^Z[s]);
  return(Q);
}
```

A.3 Coefficients d'une fonction L d'Artin

Afin d'obtenir les coefficients d'une fonction L d'Artin, nous devons calculer le déterminant $\det(\mathrm{Id} - p^{-s}\sigma_p; V^{I_p})$. Rappelons que dans le cas de premiers non ramifiés, $\det(\mathrm{Id} - p^{-s}\sigma_p; V^{I_p}) = \det(\mathrm{Id} - p^{-s}\rho(\sigma_p))$ alors que dans le cas de premiers ramifiés, on utilise la restriction de la matrice $\rho(\varphi_p)$ à V^{I_p}, où φ_p correspond à un antécédent de σ_p dans D_p. Nous devons d'abord calculer V^{I_p} afin de vérifier s'il est réduit à $\{0\}$ ou non. On peut écrire $V^{I_p} = \bigcap_{i \in I_p} \mathrm{Ker}(\rho_r(i) - \mathrm{Id})$. Dans les programmes suivants, cet espace vectoriel est donné par $z = (z_1, \cdots, z_k)$, base de V^{I_p} exprimée dans $\mathscr{B}$. Notons $\mathscr{B}'$ une base de $\mathbb{C}^{\deg \rho_r}$ complétée à partir des vecteurs $(z_1, \cdots, z_k)$ de V^{I_p} et $\delta_{V^{I_p}}$ la fonction correspondant à l'identité sur V^{I_p} et nulle ailleurs.

La fonction suivante donne le déterminant $\det(\mathrm{Id} - p^{-s}\sigma_p; V^{I_p}) = \det(\mathrm{Id} - p^{-s}\rho_{r|V^{I_p}}(\varphi_p))$. En effet, après avoir déterminé V^{I_p}, le cas où il correspond à l'espace vectoriel nul est mis à part. Puis l'opération $z \times 1/z$ ($1/z$ correspond à l'inverse à gauche de z) permet d'obtenir la matrice de $\delta_{V^{I_p}}$ dans les bases $\mathscr{B}'$ et $\mathscr{B}$. La matrice S représente $\rho(\varphi_p)$ dans la base $\mathscr{B}$. Ainsi le produit $Sz \times 1/z$ donne bien la matrice de $\rho(\varphi_p)$ restreinte à V^{I_p}.

```
ram(P,p,r)=
{
  my(Q,S,a,z,c,G,N,R);
  X='X;
  N=nfinit(P); G=galoisinit(N); R=justerep(P,r);
  Q=frobram(P,p);
  S=Mat(apply(x->x~,R[Q[1]][2]))~;
  pr=idealprimedec(N,p);
  J=idealramgroups(N,G,pr[1])[2][1];j=length(J);a=vector(j);
  for(i=1,j,
    a[i]=matker(Mat(apply(x->x~,R[J[i][1]][2]))~-1));
  if(j>1,
    z=a[1];
    for(i=2,j,
      if(z==a[i],
        z=a[i],
        z=matintersect(z,a[i])))
   ,z=Mat(a[1]));
  if(length(z)==0,
    c=1
   ,c=(matdet(1-Mat((S*z/z)*X))^(-1)));
  return(c);
}
```

Pour obtenir, les coefficients de la fonction L d'Artin, il suffit maintenant d'appliquer la fonction *direuler* en différenciant les premiers ramifiés des non ramifiés.

```
artin(P,r,U)=
{
  my(N,G,V,pr,frob);
  N=nfinit(P);
```

```
  G=galoisinit(P);
  V=fun(P,r);
  direuler(p=2,U,
    if(N.disc%p==0,
      ram(P,p,r)
     ,pr=idealprimedec(N,p);
      frob=idealfrobenius(N,G,pr[1]);
      V[frob[1]][2]^-1))
}
```

A.4 Paramètres locaux d'une fonction L d'Artin

Nous avons vu que les paramètres locaux d'une fonction L d'Artin correspondent aux valeurs propres de la matrice $\rho(\varphi_p)_{|V^{I_p}}$. Puisque nous avons la matrice représentant $\rho(\varphi_p)_{|V^{I_p}}$ (donnée par $S \times z \times 1/z$ dans les programmes), il ne reste plus qu'à calculer ses valeurs propres. La première fonction suivante renvoie les valeurs propres associées à la r^e représentation de G et le nombre premier p. La dernière fonction donne les valeurs propres, de la r^e représentation, pour les U premiers nombres premiers.

```
valprop(P,p,r)=
{
  my(n,Q,S,b,z,c,G,N,H,pr,frob,y,J,j,R);
  X='X;
  N=nfinit(P); n=poldegree(P);
  G=galoisinit(N);
  R=justerep(P,r);
  H=vector(n,i,
     M = Mat(apply(x->x~,R[i][2]))~;
     [R[i][1],M]);
  pr=idealprimedec(N,p);
  y=polroots(polcyclo(poldegree(P),'x))[1];
  if(N.disc%p==0,
      Q=frobram(P,p);
      S=H[Q[1]][2];
      J=idealramgroups(N,G,pr[1])[2][1];
      j=length(J);
      b=vector(j);
      for(i=1,j,b[i]=matker(H[J[i][1]][2]-1));
      if(j>1,
         z=b[1];
         for(i=2,j,
            if(z==b[i],
              z=b[i]
             ,z=matintersect(z,b[i])))
         ,z=Mat(b[1]));
      if(z==[;],
          c=0
```

```
          ,if(polroots(matdet(X-substpol(lift(Mat(S*z/z)),'a,y)))==[]~,
             c=matdet(X-substpol(lift(Mat(S*z/z)),'a,y))
            ,c=polroots(matdet(X-substpol(lift(Mat(S*z/z)),'a,y)))))
    ,frob=idealfrobenius(N,G,pr[1]);
    if(polroots(matdet(X- substpol(lift(H[frob[1]][2]),'a,y)))==[]~,
       c=matdet(X- substpol(lift(H[frob[1]][2]),'a,y))
      ,c=polroots(matdet(X-substpol(lift(H[frob[1]][2]),'a,y)))));
return(c);
}


artinvp(P,r,U)=
{
  my(s,v,t);
  t=primes(U);
  v=vector(U,i,[t[i],valprop(P,t[i],r)]);
  return(v);
}
```

A.5 Équation fonctionnelle

Afin de compléter la fonction L d'Artin, nous utilisons le paquet *ComputeL* de Tim Dokchitser (voir [Dok]) mis à jour par Pascal Molin. Pour cela, il nous faut donner le conducteur ainsi que le nombre de 0 et de 1 intervenant dans le facteur gamma.
Maintenant, les fonctions pour le calcul du conducteur et des facteurs gamma des fonctions L d'Artin ont été portés en C et intégrés à la fonction $lfunartin$ de PARI/GP dans la version 2.9.

A.5.1 Conducteur

Dans ce cas, le conducteur est : $q(\chi_r) = \prod_p p^{f_p(\chi_r)}$, avec $f_p(\chi_r) = \sum_{i=0}^{+\infty} \frac{|G_i|}{|G_0|} \mathrm{codim} V^{G_i}$, où pour $i \geqslant 0$, $G_i = \{\sigma \in G \,|\, \forall x \in \mathscr{O}_L,\, v_L(\sigma(x) - x) \geqslant i+1\}$ est le i-ème groupe de ramification d'un idéal premier de L au-dessus de p, G_0 étant le groupe d'inertie. On obtient la suite décroissante finie suivante : $I_p = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$.
D'abord, nous aurons besoin d'utiliser les librairies sur les groupes. Ensuite, la fonction *idealramgroups* retourne les différents groupes de ramification, en donnant leurs générateurs, toujours exprimés sous forme de permutation. La fonction suivante renvoie donc un vecteur v dont les coordonnées sont les quotients : $v[i] = \frac{|G_{i-1}|}{|G_0|}$ pour $i \in [\![1, n+1]\!]$.

```
install(group_elts,GL)
install(group_order,lG)

ordr(P,p)=
{
  my(N,G,pr,J,l,z,u,U,m,o);
  N=nfinit(P);
  G=galoisinit(P);
```

```
  pr=idealprimedec(N,p)[1];
  J=idealramgroups(N,G,pr);
  l=length(J)-1;
  if(l>0,
    z=vector(l);
    M=vector(l);
    for(i=1,l,M[i]=group_order(J[i+1]));
    for(n=1,l,z[n]=M[n]/M[1]));
  return(z);
}
```

Pour obtenir les codimensions des espaces vectoriels V^{G_i}, on exprime V^{G_i} sous la forme $\bigcap_{g_i \in G_i} \mathrm{Ker}(\rho_r(g_i) - \mathrm{Id})$.

```
codime(P,p,r,i)=
{
  my(Q,d,z,c,G,N,V,pr,J,j,v);
  N=nfinit(P);
  G=galoisinit(P);
  [V,R]=funandR(P,r);
  d=poldegree(V[1][2]);
  pr=idealprimedec(N,p);
  J=idealramgroups(N,G,pr[1])[i+1][1];
  j=length(J);
  v=vector(j);
  for(l=1,j,
     v[l]=matker(substpol(simplify(lift(Mat(apply(x->x~,R[J[l][1]][2]))~)),
     'a,polroots(polcyclo(poldegree(P),'x))[1])-1));
  if(j>1,
    z=abs(matintersect(v[1],v[2]))
   ,z=Mat(v[1]));
  if(j>2,
    for(k=3,j,z=abs(matintersect(z,v[k])))
    ,z);
  c=d-length(z);
  return(c);
}
```

La fonction suivante correspond à l'entier $f_p(\chi_r)$.

```
puiss(P,p,r)=
{
  my(N,z,m,v,pr,J,G);
  N=nfinit(P);
  G=galoisinit(P);
  z=ordr(P,p);
  m=length(z);
  v=vector(m);
  pr=idealprimedec(N,p);
```

```
  J=idealramgroups(N,G,pr[1]);
  for(i=1,m,v[i]=z[i]*codime(P,p,r,i));
  sum(i=1,m,v[i])
}
```

Finalement, pour obtenir le conducteur d'Artin, il reste à faire le produit des premiers p ramifiés (pour les premiers non ramifiés, $f_p(\chi_r) = 0$) élevés à la puissance $f_p(\chi_r)$.

```
cond(P,r)=
{
  my(s,V);
  V=vecextract(factor(nfinit(P).disc),"..","..1");
  if(V[1,1]==-1,V=vecextract(V,"2..",".."));
  v=matsize(V)[1];
  s=1;
  for(i=1,v,s=s*V[i,1]^puiss(P,V[i,1],r));
  return(s);
}
```

A.5.2 Le facteur gamma

Dans ce cas particulier, il n'y a qu'une seule place infinie et elle est réelle donc le facteur gamma est : $\gamma_\chi(s) = \pi^{-\frac{sd}{2}}\Gamma\left(\frac{s}{2}\right)^{n^+}\Gamma\left(\frac{s+1}{2}\right)^{n^-}$. Il faut trouver les dimensions des espaces vectoriels V^- et V^+ définis de la façon suivante : à chaque place w de L au-dessus de la place réelle infinie, correspond un groupe de décomposition $G(w)$ de générateur σ_w d'ordre 1 ou 2, $G(w) = \{g \in G \mid \rho(g)(w) = w\}$. On décompose V en somme directe $V = V^+ \oplus V^-$ et $n^+ = \dim V^+ = \frac{1}{2}(d + \chi_r(\sigma_w))$ donc $n^- = \dim V_v^- = \frac{1}{2}(d - \chi_r(\sigma_w))$.

Dans la pratique, on cherche σ_w sous forme de conjugaison complexe. La première fonction ci-dessous permet d'obtenir l'image du premier élément de l'ensemble E par la conjugaison complexe vue comme permutation. A partir de ce résultat, la deuxième renvoie les entiers $\frac{1}{2}(d + \chi_r(\sigma_w))$ et $\frac{1}{2}(d - \chi_r(\sigma_w))$ en calculant la trace de cet élément. Et la dernière retourne le vecteur constitué de n^+ 0 et de n^- 1.

```
conjcomp(P)=
{
  my(V,N,G,A,r,d,B,S,a,s,C,res);
  N=nfinit(P);
  G=galoisinit(P);
  A=G.group;
  r=length(A);
  d=poldegree(P);
  B=vector(r);
  a=polroots(P)[1];
  for(k=1,r,if(A[k]^2==Vecsmall(vector(d,i,i)),B[k]=A[k]));
  S=[];
  for(k=1,r,if(B[k]<>0 &
  abs(substpol(lift(nfgaloisapply(N,galoispermtopol(G,B[k]),x)),x,a)
        -conj(a))<10^-10,S=concat(S,B[k])));
```

```
  s=length(S);
  C=vector(s);
  for(k=1,s,C[k]=S[k][1]);
  res=vecmin(C);
  return(res);
}


dimconj(P,r)=
{
  my(V,R,a,v,n1,n2,t);
  [V,R]=funandR(P,r);
  v=poldegree(V[1][2]);
  a=conjcomp(P);
  t=trace(Mat(apply(x->x~,R[a][2])));
  n1=(v+t)/2;
  n2=(v-t)/2;
  return([n1,n2]);
}


gammaforcomputeL(P,r)=
{
  my(a,n,n1,n2,V,F,f);
  a=conjcomp(P);
  F=fun(P,r);
  f=poldegree(F[1][2]);
  if(a==0,
    V=vector(f)
   ,n1=dimconj(P,r)[1];
    n2=dimconj(P,r)[2];
    V=vector(n1+n2);
    for(k=n1+1,n1+n2,V[k]=1));
return(V);
}
```

A.5.3 Prolongement de la fonction L d'Artin

Le programme créé par Dokchitser, appliqué ici aux fonctions L d'Artin, permet en particulier d'obtenir les valeurs de la fonction $L(s,\chi)$ et $W(\chi)$, le signe de l'équation fonctionnelle. Pour cela, on lui fournit les coefficients de la fonction (ici c'est la fonction $artin(P,r,U)$ qui permet d'avoir les U premiers coefficients associés à la r^e représentation), le conducteur et le vecteur constitué des paramètres locaux à l'infini.

Voilà, comment procéder en pratique, après avoir chargé le programme de Dokchitser :

```
b=substpol(lift(artin(P,r,U)),'a,polroots(polcyclo(poldegree(P),'x))[1]);
c(l)=lift(b[l]);
gammaV=gammaforcomputeL(P,r);
conductor=cond(P,r);
```

```
\\ajouter Lpoles    = [1]; Lresidues = [-1];pour r=1
weight=1;
sgn= X;
initLdata("c(k)",,"conj(c(k))");
sgneq = Vec(checkfeq());
sgn   = -sgneq[2]/sgneq[1]
```

Le signe de l'équation fonctionnelle est donné par *sgn*. Et on obtient la valeur $L(s_0, \chi_r)$ simplement en demandant $L(s_0)$.

Annexe B

Quelques propriétés et rappels

B.1 Définitions et propriétés

Commençons par la propriété suivante permettant de donner un résultat exact à une série.

Propriété B.1.1. *On a* $\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^2 - n + \frac{1}{2}} = \pi \tanh\left(\frac{\pi}{2}\right)$.

<u>Preuve</u>
En utilisant les termes pairs et impairs, on obtient :

$$\begin{aligned}\sum_{n=1}^{+\infty} \frac{1}{n^2 - n + \frac{1}{2}} &= 4\sum_{p=1}^{+\infty} \frac{1}{(2p-1)^2 + 1} \\ &= 4\Big(\sum_{n=1}^{+\infty} \frac{1}{n^2+1} - \frac{1}{4}\sum_{p=1}^{+\infty} \frac{1}{p^2 + \frac{1}{4}}\Big).\end{aligned}$$

La formule (1) de la proposition 9.6.24 de [Coh07b] donne l'égalité suivante vérifiée pour tout $x \notin \mathbb{Z}$: $\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^2 - x^2} = \frac{1 - (\pi x)\mathrm{cotan}(\pi x)}{2x^2}$. On en déduit donc :

$$\begin{aligned}\sum_{n=1}^{+\infty} \frac{1}{n^2 - n + \frac{1}{2}} &= 4\Big(\frac{1 - (\pi i)\mathrm{cotan}(\pi i)}{-2} - \frac{1}{4} \times \frac{1 - (\pi \frac{i}{2})\mathrm{cotan}(\pi \frac{i}{2})}{-\frac{1}{2}}\Big) \\ &= 2(\pi i)\mathrm{cotan}(\pi i) - (\pi i)\mathrm{cotan}(\pi \frac{i}{2}) \\ &= 2\pi i \frac{1 - \tan^2 \frac{\pi i}{2}}{2\tan \frac{\pi i}{2}} - \pi i \frac{1}{\tan \frac{\pi i}{2}} \\ &= -i\pi \tan \frac{\pi i}{2} \\ &= \pi \tanh \frac{\pi}{2} \quad \text{car } \tan ix = i \tanh x.\end{aligned}$$

□

B.1.1 Fonction gamma d'Euler

Définition B.1.2. La fonction gamma d'Euler est définie, pour $\mathrm{Re}(s) > 0$, par :

$$\Gamma(s) = \int_0^{+\infty} \mathrm{e}^{-t} t^{s-1} \, \mathrm{d}t.$$

Proposition B.1.3. *La fonction Γ se prolonge à tout le plan complexe en une fonction méromorphe dont les pôles sont simples et situés aux entiers négatifs. Le résidu de la fonction Γ en $s = -n$, $n \in \mathbb{N}$, est $(-1)^n/n!$. Pour tout $s \in \mathbb{C} \backslash -\mathbb{N}$, on a :*

$$\Gamma(s+1) = s\Gamma(s).$$

Proposition B.1.4 (Formule de Weierstrass)**.** *Pour tout $s \in \mathbb{C}$, on a :*

$$\frac{1}{\Gamma(s)} = s\mathrm{e}^{\gamma s} \prod_{n=1}^{+\infty} \left(1 + \frac{s}{n}\right) \mathrm{e}^{-\frac{s}{n}},$$

où $\gamma = \lim_{N \to +\infty} \sum_{n=1}^{N} \left[\frac{1}{n} - \ln\left(1 + \frac{1}{n}\right)\right]$ *est la constante d'Euler.*

Corollaire B.1.5. *La fonction $\Gamma(s)$ ne possède pas de zéro et on a : $\Gamma(\bar{s}) = \overline{\Gamma(s)}$ pour tout $s \in \mathbb{C}$.*

Proposition B.1.6. *Pour $s \in \mathbb{C} \backslash \mathbb{R}_-$, on a, $B_2(y) = y^2 - y + \frac{1}{6}$ désignant le 2e polynôme de Bernoulli :*

$$\frac{\Gamma'(s)}{\Gamma(s)} = -\frac{1}{s} + \ln(1+s) - \frac{1}{2}\frac{1}{1+s} - \frac{1}{12}\frac{1}{(1+s)^2} + \int_1^{+\infty} B_2(\{t\}) \frac{1}{(t+s)^3} \, \mathrm{d}t. \qquad (\dagger)$$

De plus, pour $s \in \mathbb{C} \backslash \mathbb{R}_-$ tel que $\mathrm{Re}(s) \geqslant -1$, on obtient la majoration :

$$\left|\frac{\Gamma'}{\Gamma}(s)\right| \leqslant \frac{\pi}{2} + \frac{1}{12}\frac{1}{(\mathrm{Re}(s)+1)^2} + \frac{1}{|s|} + \frac{1}{2}\frac{1}{|1+s|} + \frac{1}{12}\frac{1}{|1+s|^2} + \ln(|1+s|).$$

Pour démontrer cette proposition, énonçons d'abord le résultat suivant :

Lemme B.1.7. *Soit $N \in \mathbb{N}^*$ et $s \in \mathbb{C} \backslash \mathbb{R}_-$. En désignant par B_2 le deuxième polynôme de Bernoulli et $\{x\}$ la partie fractionnaire du réel x (en fait : $\{x\} = x - \lfloor x \rfloor$), on a la relation suivante :*

$$\sum_{n=1}^{N} \frac{1}{n+s} = \frac{-1}{12(N+s)^2} + \frac{1}{12(1+s)^2} + \frac{1}{2(N+s)} + \frac{1}{2(1+s)}$$
$$+ \ln(N+s) - \ln(1+s) + \int_1^N B_2(\{t\})(t+s)^{-3} \, \mathrm{d}t$$

<u>Preuve</u>

Nous commençons par montrer la relation suivante pour une fonction f de classe $\mathscr{C}^2$ sur $]0, +\infty[$:

$$\int_1^N B_2(\{t\}) f''(t) \, \mathrm{d}t = \frac{f'(N) - f'(1)}{6} - 2\sum_{n=1}^{N} f(n) + f(N) + f(1) + 2\int_1^N f(t) \, \mathrm{d}t.$$

Alors, en l'appliquant à la fonction f définie par $f(t) = \frac{1}{2(t+s)}$, on obtient le résultat. Pour démontrer cette égalité, on décompose l'intégrale sous forme de la somme :

$$\int_1^N B_2(\{t\})f''(t)\ \mathrm{d}t = \sum_{n=1}^{N-1} \int_n^{n+1} B_2(\{t\})f''(t)\ \mathrm{d}t$$

puis sur chaque sous-intégrale, on utilise deux intégrations par parties :

$$\begin{aligned}\int_n^{n+1} B_2(\{t\})f''(t)\ \mathrm{d}t &= \int_0^1 B_2(t)f''(n+t)\ \mathrm{d}t \\ &= \frac{f'(n+1)-f'(n)}{6} + f(n+1) - f(n) - 2\int_0^1 tf'(n+t)\ \mathrm{d}t \\ &= \frac{f'(n+1)-f'(n)}{6} - (f(n+1)+f(n)) + 2\int_n^{n+1} f(t)\ \mathrm{d}t.\end{aligned}$$

Puis par sommation, on obtient bien ce que l'on veut. □

<u>Preuve de la proposition B.1.6</u>

Par la formule de Weierstrass rappelée dans la proposition B.1.4, pour tout $s \in \mathbb{C}$, on a :

$$\frac{1}{\Gamma(s)} = s\mathrm{e}^{\gamma s} \prod_{n=1}^{+\infty} \left(1 + \frac{s}{n}\right) \mathrm{e}^{-s/n},$$

où γ est la constante d'Euler.

Alors, ln désignant la détermination principale du logarithme, il existe $m(s) \in \mathbb{Z}$ tel que

$$\ln(\Gamma(s)) + 2i\pi m(s) = -\ln(s) - \gamma s + \lim_{N\to+\infty} \sum_{n=1}^{N} \left(\frac{s}{n} - \ln\left(1+\frac{s}{n}\right)\right).$$

D'où

$$\frac{\Gamma'}{\Gamma}(s) = -\frac{1}{s} - \gamma + \lim_{N\to+\infty} \sum_{n=1}^{N} \left(\frac{1}{n} - \frac{1}{n+s}\right).$$

Et par définition de la constante d'Euler γ, on obtient :

$$\begin{aligned}\frac{\Gamma'}{\Gamma}(s) &= -\frac{1}{s} + \lim_{N\to+\infty} \sum_{n=1}^{N} \left(\ln\left(\frac{n+1}{n}\right) - \frac{1}{n+s}\right) \\ &= -\frac{1}{s} + \lim_{N\to+\infty} \left(\ln(N+1) - \sum_{n=1}^{N} \frac{1}{n+s}\right).\end{aligned}$$

En utilisant l'égalité du lemme B.1.7 précédent, on a :

$$\frac{\Gamma'(s)}{\Gamma(s)} = -\frac{1}{s} + \ln(1+s) - \frac{1}{2}\frac{1}{1+s} - \frac{1}{12}\frac{1}{(1+s)^2} + \int_1^{+\infty} B_2(\{t\})\frac{1}{(t+s)^3}\ \mathrm{d}t. \qquad (\dagger)$$

Ensuite, pour l'inégalité, rappelons que $|\ln(1+s)| = \left|\ln|1+s| + i\arcsin\left(\frac{b}{\sqrt{a^2+b^2}}\right)\right|$ pour un complexe $1+s = a+ib$ vérifiant $a \geqslant 0$. Dans ce cas, on peut majorer $|\ln(1+s)|$

par $\ln(|1+s|)+\frac{\pi}{2}$. La condition supplémentaire $\mathrm{Re}(s)\geqslant -1$ nous permet d'utiliser cette majoration. De plus, avec l'inégalité $|t+s|^3\geqslant(\mathrm{Re}(s)+t)^3$, on obtient :

$$\begin{aligned}\left|\frac{\Gamma'(s)}{\Gamma(s)}\right| &\leqslant \frac{1}{|s|}+|\ln(1+s)|+\frac{1}{2}\frac{1}{|1+s|}+\frac{1}{12}\frac{1}{|1+s|^2}+\int_1^{+\infty}|B_2(\{t\})|\frac{1}{|t+s|^3}\,\mathrm{d}t\\ &\leqslant \frac{1}{|s|}+\ln(|1+s|)+\frac{\pi}{2}+\frac{1}{2}\frac{1}{|1+s|}+\frac{1}{12}\frac{1}{|1+s|^2}+\frac{1}{6}\int_1^{+\infty}\frac{\mathrm{d}t}{(\mathrm{Re}(s)+t)^3}.\end{aligned}$$

Ainsi pour $s\in\mathbb{C}\backslash\mathbb{R}_-$ tel que $\mathrm{Re}(s)\geqslant -1$,

$$\left|\frac{\Gamma'(s)}{\Gamma(s)}\right|\leqslant\frac{\pi}{2}+\frac{1}{12}\frac{1}{(\mathrm{Re}(s)+1)^2}+\frac{1}{|s|}+\frac{1}{2}\frac{1}{|1+s|}+\frac{1}{12}\frac{1}{|1+s|^2}+\ln(|1+s|).$$

□

B.1.2 Transformée de Mellin

Nous admettrons les résultats suivants que nous pouvons retrouver, par exemple, dans [God02] pages 108-109.

Définition B.1.8. La transformation de Mellin fait correspondre à une fonction f, définie sur $]0,+\infty[$, la fonction analytique $\hat{f}(s)$ suivante : pour $s\in\mathbb{C}$,

$$\hat{f}(s)=\int_0^{+\infty}x^{s-1}f(x)\,\mathrm{d}x.$$

La convergence de cette intégrale dépend uniquement de $\mathrm{Re}(s)=\sigma$. Il est clair que $\hat{f}$ est définie dans une bande du plan complexe de la forme $\mathrm{Re}(s)\in I$, où I est un intervalle. On l'appelle bande de définition de la fonction $\hat{f}$.

Proposition B.1.9. *La fonction $\hat{f}$ est holomorphe à l'intérieur de sa bande de définition et est bornée dans toute bande verticale fermée et de largeur finie où elle est définie.*

Remarque B.1.10. Pour une fonction f bornée et intégrable sur $]0,+\infty[$, la bande de définition de la fonction $\hat{f}$ est au minimum $0<\mathrm{Re}(s)<1$.

Définition/Proposition B.1.11. Pour une fonction f continue sur $]0,+\infty[$ telle que $\hat{f}$ est absolument convergente pour $\mathrm{Re}(s)=c$ et l'intégrale $\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}x^{-s}\hat{f}(s)\,\mathrm{d}s$ est absolument convergente alors :

$$f(x)=\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}x^{-s}\hat{f}(s)\,\mathrm{d}s.$$

B.1.3 Automorphisme de Frobenius

Soit L/K une extension galoisienne de groupe de Galois G et soit $\mathfrak{p}$ un idéal premier de $\mathscr{O}_K$. Notons $\mathfrak{P}$ un idéal de $\mathscr{O}_L$ au-dessus de $\mathfrak{p}$, $D_{\mathfrak{P}/\mathfrak{p}}$ le groupe de décomposition et $I_{\mathfrak{P}/\mathfrak{p}}$ le groupe d'inertie de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$.

Proposition B.1.12 ([Sam67], §6.2). *Le morphisme naturel*

$$\begin{array}{rcl} \mathrm{red} : D_{\mathfrak{P}/\mathfrak{p}} & \to & \mathrm{Gal}\left(\frac{\mathscr{O}_L}{\mathfrak{P}}/\frac{\mathscr{O}_K}{\mathfrak{p}}\right) \\ \sigma & \mapsto & \bar{\sigma} \end{array}$$

est surjectif de noyau $I_{\mathfrak{P}/\mathfrak{p}}$. On obtient donc un isomorphisme entre les groupes $D_{\mathfrak{P}/\mathfrak{p}}/I_{\mathfrak{P}/\mathfrak{p}}$ et $\mathrm{Gal}\left(\frac{\mathscr{O}_L}{\mathfrak{P}}/\frac{\mathscr{O}_K}{\mathfrak{p}}\right)$.

Proposition B.1.13. *Le groupe* $\mathrm{Gal}\left(\frac{\mathscr{O}_L}{\mathfrak{P}}/\frac{\mathscr{O}_K}{\mathfrak{p}}\right)$ *est cyclique, engendré par un générateur privilégié vérifiant $x \mapsto x^{\mathrm{N}(\mathfrak{p})}$.*

Il existe alors un unique élément $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ du groupe quotient $D_{\mathfrak{P}/\mathfrak{p}}/I_{\mathfrak{P}/\mathfrak{p}}$ dont l'image dans $\mathrm{Gal}\left(\frac{\mathscr{O}_L}{\mathfrak{P}}/\frac{\mathscr{O}_K}{\mathfrak{p}}\right)$ est ce générateur. C'est cet élément $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ que nous appelons *automorphisme de Frobenius*. Notons que $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ est un générateur du groupe $D_{\mathfrak{P}/\mathfrak{p}}/I_{\mathfrak{P}/\mathfrak{p}}$.

Lorsque $\mathfrak{p}$ est non ramifié dans L/K, $|I_{\mathfrak{P}/\mathfrak{p}}| = 1$ et donc $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \in D_{\mathfrak{P}/\mathfrak{p}}$ est bien défini. Dans la définition des fonctions L d'Artin, nous devrons néanmoins parler de Frobenius pour un idéal premier $\mathfrak{p}$ ramifié. Dans ce cas, la définition ne pose pas de problème puisqu'il est associé à une représentation $(\tilde{\rho}, V^{I_{\mathfrak{P}/\mathfrak{p}}})$ du groupe $D_{\mathfrak{P}/\mathfrak{p}}/I_{\mathfrak{P}/\mathfrak{p}}$.
Notons que lorsque l'on choisit un autre idéal premier $\mathfrak{P}'$ dans L au-dessus de $\mathfrak{p}$ alors les automorphismes de Frobenius $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ et $\mathrm{Frob}(\mathfrak{P}'/\mathfrak{p})$ sont conjugués ([Neu99] page 518 ou Kowalski dans [BCdS+03] page 9).

Propriétés B.1.14 ([Sam67], §6.3 ou [Mar77a] page 108). *Lorsque $\mathfrak{p}$ est non ramifié, on a les propriétés suivantes :*

1. *l'automorphisme de Frobenius est caractérisé par les deux propriétés suivantes :*

$$\left\{ \begin{array}{ll} \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})(\mathfrak{P}) & = \mathfrak{P} \\ \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})(x) & \equiv x^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{P}} \text{ pour tout } x \in \mathscr{O}_L \end{array} \right. ;$$

2. *pour tout élément $\tau \in G$,* $\mathrm{Frob}(\tau(\mathfrak{P})/\mathfrak{p}) = \tau \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})\tau^{-1}$;
3. *si M est un corps de nombres tel que $K \subset M \subset L$ est une tour d'extensions, on a :* $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}_M) = \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})^f$ *où $\mathfrak{p}_M = \mathfrak{P} \cap \mathscr{O}_M$ et f est le degré résiduel de $\mathfrak{p}_M$ au-dessus de $\mathfrak{p}$.*

B.2 Quelques propriétés des représentations

Donnons une référence principale concernant les représentations : [Ser67].

Pour deux caractères, χ et χ', d'un groupe G, $\langle \chi, \chi' \rangle = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \chi(g)\overline{\chi'(g)}$ est un produit scalaire hermitien.
Toute représentation V d'un groupe G, de caractère χ, est isomorphe à une somme directe $V = m_1 V_1 \oplus \cdots \oplus m_r V_r$, où V_i est une représentation irréductible de G et $m_i \in \mathbb{N}$. En notant χ_i le caractère associé à V_i, on a : $\chi = \displaystyle\sum_{i=1}^{r} m_i \chi_i$. Pour V' une représentation irréductible de caractère φ, $\langle \chi, \varphi \rangle = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \chi(g)\overline{\varphi(g)}$ représente le nombre de fois où V' apparaît parmi les V_i, à isomorphisme près.

Proposition B.2.1. *Soit (V_1, ρ_1) et (V_2, ρ_2) deux représentations irréductibles de G. Alors*

$$\langle \chi_{V_1}, \chi_{V_2} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{V_1}(g) \overline{\chi_{V_2}(g)} = \begin{cases} 1 & \text{si } V_1 \simeq V_2 \\ 0 & \text{sinon} \end{cases}.$$

B.2.1 Caractère d'une représentation induite

Pour ce paragraphe et le suivant, nous avons utilisé [MM97].

Soit H un sous-groupe de G et ψ un caractère de H. On note $g_1, \ldots, g_s$ les représentants du quotient G/H, autrement dit $s = [G : H]$ et $G = \cup_i g_i H$. On étend ψ à G en utilisant $\widetilde{\psi}$ défini par $\widetilde{\psi}(g) = \begin{cases} \psi(g) & \text{si } g \in H \\ 0 & \text{sinon} \end{cases}$.

Définition/Proposition B.2.2. On définit le caractère $\mathrm{Ind}_H^G \psi$ induit par ψ dans G de la façon suivante :

$$(\mathrm{Ind}_H^G \psi)(g) := \sum_{i=1}^{s} \widetilde{\psi}(g_i^{-1} g g_i) = \frac{1}{|H|} \sum_{t \in G} \widetilde{\psi}(t^{-1} g t).$$

<u>Preuve</u>
Pour $t \in G$, il existe $i \in [\![1, s]\!]$ et $h \in H$ tel que $t = g_i h$. Il y a équivalence entre $t^{-1} g t \in H$ et $g_i^{-1} g g_i \in H$ donc $\widetilde{\psi}(t^{-1} g t) = \widetilde{\psi}(g_i^{-1} g g_i)$. Ensuite, on écrit :

$$\sum_{t \in G} \widetilde{\psi}(t^{-1} g t) = \sum_{\substack{t \in G \\ t = g_i h}} \widetilde{\psi}(h g_i^{-1} g g_i h) = \sum_{i=1}^{s} \sum_{h \in H} \widetilde{\psi}(g_i^{-1} g g_i).$$

□

B.2.2 Représentation régulière

Définition B.2.3. Soit g l'ordre d'un groupe G. Pour un $\mathbb{C}$-espace vectoriel V de dimension g, de base $(w_g)_{g \in G}$, on définit la représentation régulière reg_G de G par :

$$\begin{aligned} \mathrm{reg}_G : G &\to \mathrm{GL}(V) \\ \sigma &\mapsto (w_g \mapsto w_{\sigma g}). \end{aligned}$$

Proposition B.2.4. *Son caractère r_G est donné par : $r_G(\sigma) = \begin{cases} |G| & \text{si } \sigma = e_G \\ 0 & \text{sinon} \end{cases}$. En particulier, le degré de la représentation régulière est g.*

Corollaire B.2.5. *On peut également écrire r_G en utilisant tous les caractères irréductibles de G :*

$$r_G = \sum_{\chi} \chi(e_G) \chi$$

ou encore

$$r_G = \mathrm{Ind}_{\{e_G\}}^G \mathbf{1}_{\{e_G\}}.$$

PREUVE
Par définition du caractère induit, $(\mathrm{Ind}_{\{e_G\}}^G \mathbf{1}_{\{e_G\}})(g) = \sum_{t\in G} \widetilde{\mathbf{1}}_{\{e_G\}}(t^{-1}gt)$ et

$$\widetilde{\mathbf{1}}_{\{e_G\}}(t^{-1}gt) = \begin{cases} 1 & \text{si } t^{-1}gt = e_G \\ 0 & \text{sinon} \end{cases} = \begin{cases} 1 & \text{si } g = e_G \\ 0 & \text{sinon} \end{cases}$$

donc $(\mathrm{Ind}_{\{e_G\}}^G \mathbf{1}_{\{e_G\}})(g) = \begin{cases} |G| & \text{si } g = e_G \\ 0 & \text{sinon} \end{cases}$.
Pour justifier l'écriture du caractère de la représentation régulière en fonction de tous les caractères irréductibles de G, on utilise la décomposition d'un caractère en somme de caractères irréductibles : $r_G = \sum_\chi a_\chi \chi$ avec $a_\chi = \langle \chi, r_G \rangle$. Et on peut calculer

$$\langle \chi, r_G \rangle = \frac{1}{|G|} \sum_{g\in G} \chi(g)\overline{r_G(g)} = \chi(e_G).$$

□

Corollaire B.2.6. *Les degrés des différents caractères irréductibles d'un groupe G vérifient la relation : $\sum_\chi \chi(e_G)^2 = |G|$.*

PREUVE
On applique la première égalité du corollaire B.2.5 en e_G. □

PROPOSITION B.2.7. *Pour une représentation (ρ, V) de G de caractère associé χ et H un sous-groupe de G, on a* $\dim V^H = \dfrac{1}{|H|} \displaystyle\sum_{h\in H} \chi(h)$.

Afin de démontrer cette proposition, nous avons besoin du lemme suivant :

Lemme B.2.8. *Soit (ρ, V) une représentation de G et H un sous-groupe de G. L'application q définie de V dans V par : $q(v) = \dfrac{1}{|H|} \displaystyle\sum_{h\in H} \rho(h)(v)$ correspond à la projection de V dans V^H.*

PREUVE
L'application q étant clairement linéaire, on doit montrer que q est idempotente et que son image est le groupe V^H.
D'abord, montrons que $q(v) \in V^H$ pour tout $v \in V$: cela revient à prouver que $\rho(h')q(v) = q(v)$ pour $h' \in H$. Puisque

$$\begin{aligned} \rho(h')q(v) &= \frac{1}{|H|} \sum_{h\in H} \rho(h'h)(v) \\ &= \frac{1}{|H|} \sum_{h''\in H} \rho(h'')(v) \\ &= q(v), \end{aligned}$$

on a bien $q(v)$ invariant sous H.
Maintenant, démontrons que $q \circ q = q$: pour $v \in V$,

$$\begin{aligned}
q \circ q(v) &= \frac{1}{|H|} \sum_{h \in H} q(\rho(h)(v)) \\
&= \frac{1}{|H|} \sum_{h \in H} \frac{1}{|H|} \sum_{h' \in H} \rho(h')(\rho(h)(v)) \\
&= \frac{1}{|H|^2} \sum_{h \in H} \sum_{h' \in H} \rho(h'h)(v) \\
&= \frac{1}{|H|^2} \sum_{h \in H} \sum_{h'' \in H} \rho(h'')(v) \\
&= \frac{|H|}{|H|^2} \sum_{h'' \in H} \rho(h'')(v) \\
&= q(v).
\end{aligned}$$

□

<u>Preuve</u>
En utilisant l'application q introduite dans le lemme B.2.8, q est une projection de V dans V^H donc $\dim V^H = \mathrm{tr}(q)$.
D'où $\dim V^H = \dfrac{1}{|H|} \displaystyle\sum_{h \in H} \mathrm{tr}(\rho(h)) = \dfrac{1}{|H|} \displaystyle\sum_{h \in H} \chi(h)$. □

B.2.3 Dual

On pourra se référer à [Sny02] aux pages 44-45.

Dans ce paragraphe, (ρ_1, V_1) et (ρ_2, V_2) sont deux représentations d'un groupe G. L'espace vectoriel des applications linéaires de V_1 dans V_2 sera noté $\mathrm{Hom}(V_1, V_2)$.

Définition B.2.9. Pour un espace vectoriel V, on appelle *espace vectoriel dual* de V l'espace vectoriel $\mathrm{Hom}(V_1, \mathbb{C})$, noté V^*.

Dans la suite, on notera $(\rho, \mathrm{Hom}(V_1, V_2))$ et $(\overline{\rho}, V^*)$ les représentations définies de la façon suivante :

Définition B.2.10. On munit l'espace $\mathrm{Hom}(V_1, V_2)$ d'une représentation ρ de G définie, pour $g \in G$ et $f \in \mathrm{Hom}(V_1, V_2)$, par :

$$\rho(g)(f) = \rho_2(g) \circ f \circ \rho_1(g)^{-1}.$$

Remarque B.2.11. En appliquant cette définition au cas de la représentation triviale $(1, V_2)$, on obtient la représentation duale $(\overline{\rho}, V^*)$ définie par : $(\overline{\rho}(g)(f))(v) = f(\rho(g^{-1})(v))$ pour tout $g \in G$, $v \in V$ et $f \in V^*$.

Proposition B.2.12. *Si χ est le caractère associé à la représentation (ρ, V) alors le caractère $\overline{\chi}$ associé à la représentation duale $(\overline{\rho}, V^*)$ correspond au conjugué complexe de χ.*

<u>Preuve</u>

Soit $g \in G$ et $\rho(g) = \begin{pmatrix} \alpha_1 & \star & \cdots & \cdots & \star \\ 0 & \alpha_2 & \star & \cdots & \star \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & \star \\ 0 & \cdots & \cdots & 0 & \alpha_d \end{pmatrix}$ dans une base $(e_1, \ldots, e_d)$ de V.

Puisque $|\alpha_i| = 1$ pour tout $i \in [\![1, d]\!]$ et que $\rho(g^{-1})\rho(g) = I_d$,

$\rho(g^{-1}) = \begin{pmatrix} \overline{\alpha_1} & \star & \cdots & \cdots & \star \\ 0 & \overline{\alpha_2} & \star & \cdots & \star \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & \star \\ 0 & \cdots & \cdots & 0 & \overline{\alpha_d} \end{pmatrix}$, autrement dit $\rho(g^{-1})(e_j) = \overline{\alpha_j} e_j + \sum_{k=1}^{j-1} \lambda_k^j e_k$.

Comme $(\overline{\rho}(g)(e_i^*))(e_j) = e_i^*(\rho(g^{-1})e_j)$ pour tout i, $j \in [\![1, d]\!]$, on obtient

$$\overline{\rho}(g)(e_i^*)(e_j) = \begin{cases} \lambda_i^j & \text{si } i < j \\ \overline{\alpha_i} & \text{si } i = j \\ 0 & \text{si } i > j \end{cases},$$

c'est-à-dire $\overline{\rho}(g)(e_i^*) = \overline{\alpha_i} e_i^* + \sum_{k=i+1}^{d} a_k e_k^*$.

Ainsi $\mathrm{Mat}_{(e_1^*, \ldots, e_d^*)} \overline{\rho}(g) = \begin{pmatrix} \overline{\alpha_1} & 0 & \cdots & \cdots & 0 \\ \star & \overline{\alpha_2} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \star & \ddots & \ddots & 0 \\ \star & \cdots & \cdots & \star & \overline{\alpha_d} \end{pmatrix}$ donc $\chi_{\overline{\rho}}(g) = \overline{\alpha_1 + \cdots + \alpha_d} = \overline{\chi_\rho(g)}$.

□

B.2.4 Caractères des groupes alternés

Partons du groupe symétrique S_n.

Propriété B.2.13 ([Ser67], théorème 7 I-20)**.** *Le nombre de représentations irréductibles d'un groupe G, à isomorphisme près, est égal au nombre de classes de conjugaison de G.*

Puisque les classes de conjugaison du groupe symétrique S_n sont déterminées par la longueur des cycles dans la décomposition en cycles à support disjoint, on en déduit que le nombre de représentations irréductibles de S_n correspond au nombre de partitions de l'entier n. Puisqu'ils représentent les partitions, intéressons-nous alors aux diagrammes de Young.

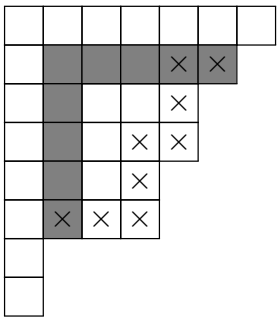
Définitions B.2.14.

1. Un *diagramme de Young* est une collection finie de cases, ou cellules, organisée en lignes alignées à gauche, avec la propriété que les longueurs des lignes décroissent au sens large. La suite des longueurs des lignes donne une partition λ de l'entier n qui est le nombre total de cases du diagramme.
2. La (i, j)-*équerre* d'un diagramme de Young est composée de la case située en position (i, j) et de toutes les cellules à droite et en-dessous. Sa *longueur*, notée $h(i, j)$, est le nombre de cellules composant l'équerre.

3. Une *équerre tordue*[1] est une partie connexe du bord d'un diagramme de Young qui peut être supprimée tout en laissant un diagramme de Young.

Propriété B.2.15. *Il y a une correspondance bijective naturelle entre les équerres et les équerres tordues de même longueur.*

<u>Preuve</u>
En effet, une équerre tordue reliant la i^e ligne à la j^e colonne correspond à la (i,j)-équerre comme l'illustre l'exemple suivant :



□

Proposition B.2.16 (Formule des équerres)**.** *Pour une partition λ de n, la dimension de la représentation associée dans S_n est donnée par :*

$$\dim V_\lambda = \frac{n!}{\prod_{i,j} h(i,j)},$$

où le produit porte sur toutes les cases du diagramme de Young associé à λ.

Pour cette partie, nous nous référons à [FH91], lecture 5.
Soit ρ une représentation irréductible de S_n. Alors sa restriction à A_n est : soit irréductible soit la somme directe de deux représentations irréductibles de même degré. Le résultat suivant donne plus d'informations sur cette restriction :

Théorème B.2.17 ([FH91], Proposition 5.1)**.** *Soit ρ une représentation irréductible de S_n. La représentation $\varphi = \rho_{|A_n}$ est irréductible si et seulement si l'une des conditions équivalentes suivantes est vérifiée :*

(i) le diagramme de Young associé à ρ n'est pas symétrique (on dit alors que ρ n'est pas auto-conjuguée) ;

(ii) $\rho \not\cong \rho \otimes \rho_0$, où ρ_0 est la représentation non triviale du quotient S_n/A_n.

Par ailleurs, quand la représentation φ se décompose en somme de deux représentations irréductibles conjuguées φ_1 et φ_2, les représentations de A_n obtenues sont conjuguées, autrement dit, $\varphi_2 := \varphi_1 \circ f_t$, où t est une transposition quelconque et où f_t est la conjugaison par t.

Rappelons que toute représentation irréductible de A_n s'obtient de cette façon, c'est-à-dire en regardant la restriction à A_n d'une représentation irréductible de S_n.

1. traduction libre pour le mot anglais *skew-hook*

Propriété B.2.18. *Une classe de conjugaison $\mathscr{C}$ de S_n se décompose en deux classes de conjugaison de A_n si et seulement si $\mathscr{C}$ est la classe de conjugaison d'un élément dont la décomposition en cycles ne fait apparaître que des cycles de longueurs impaires et toutes différentes.*

Proposition B.2.19. *Les classes de conjugaison de S_n se décomposant en deux classes de conjugaison de A_n sont en correspondance bijective avec les diagrammes de Young symétriques.*

Preuve

Partons d'une classe de conjugaison $\mathscr{C}$ de S_n qui se scinde en deux classes de conjugaison de A_n. Alors $\mathscr{C} = [q_1]\cdots[q_k]$, où $[q_i]$ désigne un q_i-cycle (les supports sont disjoints) ; en particulier les entiers q_i sont impairs, d'après la propriété B.2.18. Le diagramme de Young de la représentation ρ s'obtient simplement en imbriquant les crochets symétriques de taille $q_1, \cdots, q_k$.

Réciproquement, partons d'un diagramme T de Young symétrique associé à la partition $\lambda = (\lambda_1, \cdots, \lambda_k)$, $\lambda_1 \geq \cdots \geq \lambda_k$. Ce tableau donne une représentation irréductible ρ_{T} de S_n de caractère θ_{T} dont la restriction à A_n se décompose en somme de deux caractères irréductibles χ_{T} et χ'_{T} de A_n (d'après le théorème B.2.17). Notons Γ_i, $i = 1\cdots, k$, les crochets symétriques du diagramme de Young T puis posons $q_i = |\Gamma_i|$ le cardinal de Γ_i. On peut noter que $q_i = 2(\lambda_i - i) + 1$ et que k est le plus grand entier vérifiant $\lambda_k - k \geq 0$. À ce tableau symétrique T, on associe la classe de conjugaison $\mathscr{C}_{\mathrm{T}}$ dont la décomposition des éléments s'écrit comme le produit de q_i-cyles, $i = 1, \cdots, k$ (à supports disjoints). Comme les éléments q_i sont impairs et distincts (il est immédiat que $q_i > q_{i-1}$), la classe de conjugaison $\mathscr{C}_{\mathrm{T}}$ se scinde en deux classes de conjugaison $\mathscr{C}_{\mathrm{T}}^{(1)}$ et $\mathscr{C}_{\mathrm{T}}^{(2)}$ de A_n. □

Lorsque le diagramme de Young T est symétrique, résumons dans la proposition suivante la particularité du lien entre une représentation irréductible ρ_{T} du groupe S_n et $\mathscr{C}_{\mathrm{T}}$ la classe de conjugaison associée se décomposant en deux classes de conjugaison $\mathscr{C}_T^{(1)}$ et $\mathscr{C}_T^{(2)}$ dans A_n.

Proposition B.2.20.
1) Pour tout caractère irréductible θ de A_n différent de χ_{T} et χ'_{T}, il vient

$$\theta(\mathscr{C}_T^{(1)}) = \theta(\mathscr{C}_T^{(2)});$$

2) Pour toute classe de conjugaison $\mathscr{C}'$ de A_n différente de $\mathscr{C}_T^{(i)}$, $i = 1, 2$, il vient

$$\chi_{\mathrm{T}}(\mathscr{C}') = \chi'_{\mathrm{T}}(\mathscr{C}').$$

De plus, $\chi_{\mathrm{T}}(\mathscr{C}_T^{(1)}) = \chi'_{\mathrm{T}}(\mathscr{C}_T^{(2)}) \neq \chi_{\mathrm{T}}(\mathscr{C}_T^{(2)}) = \chi'_{\mathrm{T}}(\mathscr{C}_T^{(1)})$.

Ainsi, les seules classes de conjugaison séparant les caractères χ_{T} et χ'_{T} sont les classes $\mathscr{C}_T^{(i)}$ qui se décomposent en cycles de la même façon que $\mathscr{C}_{\mathrm{T}}$.

Passons à des rappels sur les valeurs des caractères irréductibles de A_n.

Définition B.2.21. On note $a(\chi)$ le nombre de valeurs prises par un caractère χ irréductible de A_n : $a(\chi) = |\{\chi(s),\ s \in A_n\}|$.

Propriété B.2.22. *Pour tout caractère χ du groupe alterné A_n, $a(\chi) \leqslant 2\chi(1) + 3$.*

<u>Preuve</u>
Rappelons que les caractères de S_n sont à valeurs entières. Si ρ est une représentation irréductible de S_n non auto-conjuguée, la restriction φ de ρ au groupe alterné A_n est irréductible. Notons par χ son caractère et par d son degré. Alors, comme pour tout $s \in A_n$, $|\chi(s)| \leqslant d$ (se rappeler que χ est de degré d et que les valeurs propres de la représentation associée sont des racines de l'unité) et que les valeurs de χ sont entières, il vient $a(\chi) \leqslant 2d+1$.
Si maintenant ρ est auto-conjuguée, alors la restriction φ de ρ à A_n se décompose en somme de deux représentations irréductibles conjuguées φ_1 et φ_2, de caractères respectifs χ_1 et χ_2. On rappelle que $\varphi_2 := \varphi_1 \circ f_t$, où t est une transposition quelconque et où f_t est la conjugaison par t. Ainsi, si c est une classe de conjugaison non décomposée d'un élément s de A_n, *i.e.* $f_t(c) = c$ donc $\varphi_1(c) = \varphi_2(c)$, on obtient $\varphi_i(c) = \frac{1}{2}\rho(c)$ et par conséquent les caractères $2 \cdot \chi_i$ des représentations $\varphi_i \oplus \varphi_i$ prennent, sur ces classes, leurs valeurs dans l'ensemble $a(\chi)$, χ étant le caractère de ρ. Il en est de même pour les classes de conjugaison c décomposées non associées à ρ : la proposition B.2.20 montre que $\chi_1(c) = \chi_2(c)$. Pour les deux dernières classes, *i.e.* les classes décomposées associées à ρ, ces valeurs sortent de l'ensemble $a(\chi)$. En conclusion il vient $a(\chi_i) \leqslant 2d+3$. □

Proposition B.2.23 (Règle de Murnaghan-Nakayama)**.** *Soit λ une partition de n et $g = [m]h \in S_n$ avec $[m]$ un m-cycle et h une permutation de S_{n-m}. Alors la règle de Murnaghan-Nakayama donne une méthode de calcul du caractère associé à la partition :*

$$\chi_\lambda(g) = \sum_\mu (-1)^{r(\mu)} \chi_\mu(h),$$

où la somme porte sur toutes les partitions μ de S_{n-m} obtenues en enlevant une équerre tordue de longueur m à λ, et pour $r(\mu)$, on ôte 1 au nombre de lignes de cette équerre tordue.

Remarque B.2.24. Avec les notations précédentes, si λ n'a pas d'équerre de longueur m alors $\chi_\lambda(g) = 0$.

Exemple B.2.25. Soit $\lambda = (n-1, 1)$ une partition de n de représentation irréductible associée ρ. La représentation ρ est de degré $n-1$ et sa restriction à A_n est encore irréductible. Notons par χ_λ le caractère de ρ. Le diagramme de Young, complété avec les longueurs des équerres, est le suivant :

n	$n-2$	$\cdots$	$\cdots$	2	1
1					

donc, d'après la proposition B.2.16, la dimension de la représentation associée vaut :

$$\chi_\lambda(1) = \frac{n!}{n(n-2)!} = n-1.$$

Pour $1 \leqslant k \leqslant n-2$, si $\mathscr{C}_k$ est la classe de conjugaison des cycles de longueur $(n-k)$, la règle de Murnaghan-Nakayama indique que $\chi_\lambda(\mathscr{C}_k) = k-1$, ce qui donne une minoration en $O(n)$ pour $a(\chi)$.
Si on s'intéresse à la classe de conjugaison $\mathscr{C}$ des produits de 2 transpositions, on obtient $\chi_\lambda(\mathscr{C}) = n-5$ pour $n \geqslant 4$. Plus généralement on obtient que le caractère d'un produit de k transpositions (pour $k \leqslant \frac{n-1}{2}$) est $n-2k-1$.

Détaillons le cas où $\mathscr{C}_k$ est la classe de conjugaison des cycles de longueur $n-k$, où $1 \leqslant k \leqslant n-2$: on applique la règle de Murnaghan-Nakayama avec $m = n-k$ et $h = 1 \in S_k$.

$$\chi_\lambda(\mathscr{C}_k) = \sum_\mu (-1)^{r(\mu)} \chi_\mu(1),$$

où μ est une partition de S_k obtenue en ôtant une équerre tordue de longueur $n-k$ au diagramme de Young de λ. Puisque $2 \leqslant n-k \leqslant n-1$, pour chaque entier k, il n'existe qu'une seule équerre tordue de longueur $n-k$ et il correspond à la ligne de longueur $n-k$ d'où $r(\mu) = 1-1 = 0$. Le μ associé est alors :

k	$k-2$	$\cdots$	2	1
1				

donc $\chi_\mu(1) = \dim V_\mu = \frac{k!}{k(k-2)!} = (k-1)$. Ainsi, $\chi_\lambda(\mathscr{C}_k) = k-1$.

Exemple B.2.26. Prenons n pair et soit $\mathscr{C}$ la classe de conjugaison des cycles de longueur $(n-1)$. Soit χ_{T} un caractère irréductible de diagramme de Young T. La règle de Murnaghan-Nakayma indique ici que

$$\chi_{\mathrm{T}}(\mathscr{C}) = \begin{cases} 1 & \text{si} \quad \mathrm{T} = (1, \cdots, 1) \ \text{ ou } \mathrm{T} = (n) \\ (-1)^{n-k-1} & \text{si} \quad \mathrm{T} = (k, 2, 1, \cdots, 1) \\ 0 & \text{sinon} \end{cases}.$$

Proposition B.2.27 ([FH91], exercice 5.5)**.** *Pour $n \geqslant 7$, la seule représentation irréductible non triviale de A_n de dimension inférieure à n est une représentation de degré $n-1$.*

Index

$\left(\frac{a}{p}\right)$, symbole de Kronecker, 30

Arithmétiquement équivalents, corps, 2
Auto-conjuguée, représentation, 118
Auto-duale, fonction, 8
Automorphisme de Frobenius, 113

Coefficient d'une fonction L, 8
Conducteur
  $q(f)$, 9
  $q(\chi)$, 22
  analytique, $\mathfrak{q}(f)$, 12
  d'Artin, $f(\chi)$, 21
Conjecture
  de Ramanujan-Petersson, 15
    à l'infini, 15
  généralisée de Selberg, 15

Degré d'une fonction L, 8
Diagramme de Young, 117
Dual, 8

Équerre, 117
  tordue, 118
Espace vectoriel dual, 116

$f(\chi)$, conducteur d'Artin, 21
Facteur gamma d'une fonction L, γ_f, 8
Fonction L, 8
  complétée, 8
  d'Artin, 17

γ_f, facteur gamma d'une fonction L, 8
Grande Hypothèse de Riemann (GRH), 15

Hypothèse de Riemann généralisée, 14

Longueur
  d'une équerre, 117
  d'une permutation, 86

$\mathfrak{p}$-signature d'une représentation, 85
Paramètres locaux
  à l'infini, 9
  d'une fonction L d'Artin, 17
  en un nombre premier, 8
Peu ramifiée, représentation, 85

$q(f)$, conducteur, 9
$\mathfrak{q}(f)$, conducteur analytique, 12

$r(f)$, 10
Résidu quadratique modulo n, 31
Règle de Murnaghan-Nakayama, 120

Signature d'une matrice, 85
Symbole de
  Jacobi, $\left(\frac{a}{n}\right)$, 30
  Kronecker, $\left(\frac{a}{p}\right)$, 30

$\omega(n)$, 36

Zéros
  non triviaux, 11
  triviaux, 11

Bibliographie

[Akb06] Amir Akbary : Lectures on classical analytic theory of L-functions. Institute for Research in Fundamental Sciences, Iran, 2006. `http://www.cs.uleth.ca/~akbary/publications.html`.

[Ank52] Nesmith Cornett Ankeny : The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[Bac90] Eric Bach : Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[BCdS+03] D. Bump, J. W. Cogdell, E. de Shalit, D. Gaitsgory, E. Kowalski et S. S. Kudla : *An introduction to the Langlands program.* Birkhäuser Boston, Inc., Boston, MA, 2003. Lectures presented at the Hebrew University of Jerusalem, Jerusalem, March 12–16, 2001, Edited by Joseph Bernstein and Stephen Gelbart.

[BCP97] Wieb Bosma, John Cannon et Catherine Playoust : The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bel] Joël Bellaïche : Théorème de Chebotarev et complexité de Littlewood. *Ann. Sci. Éc. Norm. Supér.*, à paraître.

[Ber13] Damien Bernard : *Statistiques des zéros non-triviaux de fonctions L de formes modulaires.* Thèse de doctorat, Université Blaise Pascal, 2013.

[BS15] Daniela Bubboloni et Jack Sonn : Intersective S_n polynomials with few irreducible factors. *ArXiv e-prints*, juillet 2015.

[Bug97] Yann Bugeaud : Bounds for the solutions of superelliptic equations. *Compositio Math.*, 107(2):187–219, 1997.

[CG93] John Brian Conrey et Amit Ghosh : On the Selberg class of Dirichlet series : small degrees. *Duke Math. J.*, 72(3):673–693, 1993.

[CG14] Sam Chow et Alexandru Ghitza : Distinguishing newforms. *preprint*, 2014.

[Coh07a] Henri Cohen : *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 de *Graduate Texts in Mathematics.* Springer, New York, 2007.

[Coh07b] Henri Cohen : *Number theory. Vol. II. Analytic and modern tools*, volume 240 de *Graduate Texts in Mathematics.* Springer, New York, 2007.

[Col07] Michael J. Collins : On Jordan's theorem for complex linear groups. *J. Group Theory*, 10(4):411–423, 2007.

[DD10] T. Dokchitser et V. Dokchitser : Identifying Frobenius elements in Galois groups. *ArXiv e-prints*, septembre 2010.

[Dok] Tim DOKCHITSER : ComputeL - Computing special values of L-functions. `http://www.maths.bris.ac.uk/~matyd/computel/`.

[Ell08] Jordan S. ELLENBERG : Points of low height on $\mathbb{P}^1$ over number fields and bounds for torsion in class groups. *In Computational arithmetic geometry*, volume 463 de *Contemp. Math.*, pages 45–48. Amer. Math. Soc., Providence, RI, 2008.

[Euv] Charlotte EUVRARD : Majoration explicite sur le nombre de coefficients suffisants pour déterminer une fonction L. *J. Théor. Nombres Bordeaux*, à paraître.

[EV06] Jordan S. ELLENBERG et Akshay VENKATESH : The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.

[EV07] Jordan S. ELLENBERG et Akshay VENKATESH : Reflection principles and bounds for class group torsion. *Int. Math. Res. Not. IMRN*, (1):Art. ID rnm002, 18, 2007.

[FH91] William FULTON et Joe HARRIS : *Representation theory*, volume 129 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[GAP15] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.9*, 2015. Disponible à l'adresse `http://www.gap-system.org`.

[God02] Roger GODEMENT : *Analyse mathématique. III.* Springer-Verlag, Berlin, 2002. Fonctions analytiques, différentielles et variétés, surfaces de Riemann. [Analytic functions, differentials and manifolds, Riemann surfaces].

[Hal97] Emmanuel HALLOUIN : Parcours initiatique à travers la théorie des valuations. *Prépublication de l'Université de Poitiers*, 1997.

[IK04] Henryk IWANIEC et Emmanuel KOWALSKI : *Analytic number theory*, volume 53 de *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[KMV02] Emmanuel KOWALSKI, Philippe MICHEL et Jeffrey VANDERKAM : Rankin-Selberg L-functions in the level aspect. *Duke Math. J.*, 114(1):123–191, 2002.

[Kon95] Takeshi KONDO : Algebraic number fields with the discriminant equal to that of a quadratic number field. *J. Math. Soc. Japan*, 47(1):31–36, 1995.

[KP99] Jerzy KACZOROWSKI et Alberto PERELLI : On the structure of the Selberg class. I. $0 \leq d \leq 1$. *Acta Math.*, 182(2):207–241, 1999.

[Lan94] Serge LANG : *Algebraic number theory*, volume 110 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1994.

[Li75] Wen Ch'ing Winnie LI : Newforms and functional equations. *Math. Ann.*, 212:285–315, 1975.

[Li79] Wen Ch'ing Winnie LI : L-series of Rankin type and their functional equations. *Math. Ann.*, 244(2):135–166, 1979.

[LMO79] Jeffrey C. LAGARIAS, Hugh L. MONTGOMERY et Andrew M. ODLYZKO : A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[LO77] Jeffrey C. Lagarias et Andrew M. Odlyzko : Effective versions of the Chebotarev density theorem. *In Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[Mar77a] Daniel A. Marcus : *Number fields.* Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[Mar77b] Jacques Martinet : Character theory and Artin L-functions. *In Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 1–87. Academic Press, London, 1977.

[MM97] M. Ram Murty et V. Kumar Murty : *Non-vanishing of L-functions and applications*, volume 157 de *Progress in Mathematics.* Birkhäuser Verlag, Basel, 1997.

[MMS88] M. Ram Murty, V. Kumar Murty et N. Saradha : Modular forms and the Chebotarev density theorem. *Amer. J. Math.*, 110(2):253–281, 1988.

[MR04] Pascal Molin et Sylvain Rairat : Le théorème de Kronecker-Weber. Mémoire sous la direction de Gaëtan Chenevrier, 2004.

[Mur94] V. Kumar Murty : The least prime which does not split completely. *Forum Math.*, 6(5):555–565, 1994.

[Nar74] Władysław Narkiewicz : *Elementary and analytic theory of algebraic numbers.* PWN—Polish Scientific Publishers, Warsaw, 1974. Monografie Matematyczne, Tom 57.

[Neu99] Jürgen Neukirch : *Algebraic number theory*, volume 322 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Nic69] Jean-Louis Nicolas : Répartition des nombres premiers. *In Séminaire Delange-Pisot-Poitou, tome 9 : 1967-1968, Théorie des nombres, Fasc. 2, Exp. No. G6, 4p.* Secrétariat Mathématique, Paris, 1969.

[Odl77] Andrew M. Odlyzko : On conductors and discriminants. *In Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 377–407. Academic Press, London, 1977.

[Odl90] Andrew M. Odlyzko : Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)*, 2(1):119–141, 1990.

[Oes79] Joseph Oesterlé : Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée. *Astérisque*, (61):165–167, 1979.

[Ogg69] Andrew P. Ogg : On a convolution of L-series. *Invent. Math.*, 7:297–312, 1969.

[OS11] Almasa Odžak et Lejla Smajlović : On asymptotic behavior of generalized Li coefficients in the Selberg class. *J. Number Theory*, 131(3):519–535, 2011.

[PAR15] The PARI Group, Bordeaux. *PARI/GP version* `2.7.5`, 2015. Disponible à l'adresse `http://pari.math.u-bordeaux.fr/`.

[Per77] Robert Perlis : On the equation $\zeta_K(s) = \zeta_{K'}(s)$. *J. Number Theory*, 9(3):342–360, 1977.

[Per05] Alberto PERELLI : A survey of the Selberg class of L-functions. I. *Milan J. Math.*, 73:19–52, 2005.

[Pol13] Paul POLLACK : The smallest inert prime in a cyclic number field of prime degree. *Math. Res. Lett.*, 20(1):163–179, 2013.

[Rém10] Gaël RÉMOND : Nombre de points rationnels des courbes. *Proc. Lond. Math. Soc. (3)*, 101(3):759–794, 2010.

[Rob83] Guy ROBIN : Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arith.*, 42(4):367–389, 1983.

[Rou09] Djamel ROUYMI : *Formules de trace en niveau primaire et non annulation de valeurs centrales de fonctions L automorphes.* Thèse de doctorat, Université Henri Poincaré, 2009.

[RT14] Jeremy ROUSE et Frank THORNE : On the existence of large degree Galois representations for fields of small discriminant. *Pacific J. Math.*, 271(1):243–256, 2014.

[Sam67] Pierre SAMUEL : *Théorie algébrique des nombres.* Hermann, Paris, 1967.

[Ser67] Jean-Pierre SERRE : *Représentations linéaires des groupes finis.* Hermann, Paris, 1967.

[Ser68] Jean-Pierre SERRE : *Corps locaux.* Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser77] Jean-Pierre SERRE : *Linear representations of finite groups.* Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Ser81] Jean-Pierre SERRE : Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Sny02] Noah SNYDER : *Artin's L-functions : A Historical Approach.* Thèse de doctorat, Harvard University, 2002.

[Ten95] Gérald TENENBAUM : *Introduction à la théorie analytique et probabiliste des nombres*, volume 1 de *Cours Spécialisés [Specialized Courses].* Société Mathématique de France, Paris, second édition, 1995.

[Tho14] Frank THORNE : Shintani's zeta function is not a finite sum of Euler products. *Proc. Amer. Math. Soc.*, 142(6):1943–1952, 2014.

[Uch70] Kôji UCHIDA : Unramified extensions of quadratic number fields. II. *Tôhoku Math. J. (2)*, 22:220–224, 1970.

[Van08] Lotte VAN DER ZALM : Arithmetically equivalent fields. Master thesis under supervision of Gunther Cornellissen, 2008.

[Was97] Lawrence C. WASHINGTON : *Introduction to cyclotomic fields*, volume 83 de *Graduate Texts in Mathematics.* Springer-Verlag, New York, second édition, 1997.

[Win13] Bruno WINCKLER : Théorème de Chebotarev effectif. *ArXiv e-prints*, novembre 2013.

[Yam70] Yoshihiko YAMAMOTO : On unramified Galois extensions of quadratic number fields. *Osaka J. Math.*, 7:57–76, 1970.

[Zam15] Asif ZAMAN : Bounding the least prime ideal in the Chebotarev Density Theorem. *ArXiv e-prints*, août 2015.