Le théorème de densité de Chebotarev

Gilles Felber

Projet de semestre

sous la supervision de

Professeur P. Michel et Docteur R. Moreira Nunes

Juin 2017

Section de Mathématiques
3e Année 2016–2017

Table des matières

1 Introduction

Le théorème de densité de Chebotarev décrit, dans le cadre d'une extension galoisienne de degré fini de corps de nombres L/K, la façon dont les idéaux premiers non-ramifiés de K se répartissent dans les différentes classes de conjugaison du groupe de Galois $Gal(L/K)$ via l'automorphisme de Frobenius ou symbole d'Artin. Il dit notamment que cette répartition est équitable par rapport aux cardinaux des classes de conjugaison. Un cas particulier de ce théorème qui ne sera pas démontré ici, est le théorème de la progression arithmétique de Dirichlet, qui décrit la répartition des nombres premier dans les suites arithmétiques, c'est-à-dire les nombres premiers modulo un entier, et qui est un corollaire du théorème de densité de Chebotarev dans le cas des extensions cyclotomiques. La preuve du théorème elle-même suit le même schéma que celle du théorème de Dirichlet, en remplaçant l'utilisation des fonctions L de Dirichlet par les fonctions L d'Artin.
Ce texte se compose de deux parties distinctes. La première partie se concentre durant les chapitres 2 à 4 sur la théorie des représentations linéaires de groupes finis et leurs caractères dans le but d'obtenir une base utile pour décrire les fonctions L associées à des caractères, notamment les fonctions L de Hecke et d'Artin, mais surtout, de démontrer le théorème de Brauer afin de pouvoir étendre les fonctions L d'Artin. Elle suit globalement la structure de Serre [1] en sautant certains chapitres.
La seconde partie commence par décrire les fonctions L de Hecke sans entrer dans la théorie des corps de classe, ce qui oblige à laisser certaines preuves sans démonstration. Elle introduit ensuite les fonctions L d'Artin et les étend dans un ouvert contenant le demi-plan complexe $\{s \in \mathbb{C} | Re(s) \geq 1\}$ à l'aide du théorème de Brauer. Finalement, les deux derniers chapitres démontrent la non-annulation des fonctions L d'Artin sur le demi-plan complexe $\{s \in \mathbb{C} | Re(s) \geq 1\}$ puis son application à la démonstration du théorème de densité de Chebotarev. Cette partie mixe les résultats et preuves de Triantafillou [2] pour les fonctions L de Hecke, de Neukirch [3] pour les fonctions L d'Artin et leur non-annulation et de Murty et Murty [4] pour la non-annulation des fonctions L de Hecke suivit d'une démonstration personnelle du théorème. Cette partie se base sur le cours Math-312 "Introduction à la théorie algébrique des nombres" donné au semestre d'automne 2016.

2 Représentations et caractères de groupes finis

Pour commencer, nous allons introduire les notions de représentations et de caractère d'un groupe fini, et démontrer quelques propriétés basiques à l'aide d'outils classique de théorie des groupes et d'algèbre linéaire.

Définition 2.1. Une *représentation linéaire* ρ d'un groupe fini G est un homomorphisme de groupe de G vers les automorphismes d'un K-espace vectoriel V :

$$\rho : G \to GL(V)$$

V est alors appelé un *espace de représentation* de G ou plus simplement une *représentation* de G.

Remarques.

1. Comme ρ est un homomorphisme, on a directement que $\rho(1) = 1$ et $\rho(s^{-1}) = \rho(s)^{-1}$
2. Dans tout ce qui suit, nous prendrons $K = \mathbb{C}$ et V de dimension finie sur $\mathbb{C}$, mais plusieurs résultats sur les représentations restent valables dans un corps algébriquement clos de caractéristique 0. Si V est de dimension n, on peut donc identifier $GL(V)$ à $GL_n(\mathbb{C})$, le groupe des matrices carrés $n \times n$ inversibles à coefficients complexes et on appelle n le *degré* de la représentation.
3. Pour alléger la notation, on notera parfois ρ_s à la place de $\rho(s)$.

Exemples.

1. La *représentation triviale* ou *représentation unité* est la représentation donnée par $\rho(s) = 1$ pour tout $s \in G$.
2. La *représentation régulière* est la représentation sur l'espace vectoriel $\mathbb{C}[G] := \{\sum_{s \in G} \lambda_s s | \lambda_s \in \mathbb{C}\}$ sur lequel G agit $\mathbb{C}$-linéairement par multiplication à gauche.
3. Toute représentation V d'un groupe G est équivalente à un $\mathbb{C}[G]$-module, en étendant par linéarité l'action de G sur V.

Définition 2.2. Deux représentations $\rho : G \to GL(V)$ et $\rho' : G \to GL(V')$ d'un groupe G sont *isomorphes* si il existe un isomorphisme d'espaces vectoriels $\tau : V \to V'$ tel que pour tout $s \in G$:

$$\tau \circ \rho(s) = \rho'(s) \circ \tau$$

Définition 2.3. Soient $\rho : G \to GL(V)$ une représentation de G et $W \subseteq V$ un sous-espace vectoriel. Si W est stable par G, autrement dit pour tout $x \in W$ et $s \in G$, $\rho_s(x) \in W$, alors W est une *sous-représentation* de V.

Théorème 2.1. *Soient $\rho : G \to GL(V)$ une représentation de G et $W \subseteq V$ une sous-représentation. Il existe alors un supplémentaire W' de W stable par G tel que $W \bigoplus W' = V$.*

Démonstration. Par l'algèbre linéaire, on sait que W possède un supplémentaire $\tilde{W}$ en tant qu'espace vectoriel et une projection $\tilde{\pi} : V \to W$ correspondant à ce supplémentaire. Posons

$$\pi = \frac{1}{g} \sum_{t \in G} \rho_t \tilde{\pi} \rho_t^{-1}.$$

Comme W est stable par ρ_t, l'image de π est contenue dans W. De plus, si $x \in W$ et $t \in G$, alors $\rho_t^{-1}(x)$ appartient à W donc $\rho_t \tilde{\pi} \rho_t^{-1}(x) = \rho_t \rho_t^{-1}(x) = x$ et $\pi(x) = x$, d'où π est une projection de V dans W. Cette projection définit un supplémentaire W' (son noyau) de W. De plus, on a pour tout $s \in G$

$$\rho_s \pi = \frac{1}{g} \sum_{t \in G} \rho_s \rho_t \tilde{\pi} \rho_t^{-1} = \frac{1}{g} \sum_{t \in G} \rho_{st} \tilde{\pi} \rho_{st}^{-1} \rho_s = \pi \rho_s.$$

Enfin, si $x \in W'$ et $s \in G$, alors $\pi(x) = 0$ et $\pi \rho_s(x) = \rho_s \pi(x) = 0$ donc $\rho_s(x) \in W'$ et W' est stable par G. □

Définition 2.4. Soit $\rho : G \to GL(V)$ une représentation de G. ρ est *irréductible* ou *simple* si $V \neq \{0\}$ et si aucun sous-espace vectoriel propre de V n'est stable par G, c'est-à-dire V ne possède pas de sous-représentation à part V et 0 ou encore, par le théorème 2.1, que $V = W \bigoplus W'$ implique que $V = W$ ou $V = W'$.

Théorème 2.2. *Toute représentation est somme directe d'un nombre fini de représentations irréductibles.*

Démonstration. Si V n'est pas irréductible, $V = W \bigoplus W'$ avec $V \neq W$ et $V \neq W'$ donc $\dim W < \dim V$ et $\dim W' < \dim V$ et le théorème s'en déduit par récurrence. □

Définition 2.5. Soient V_1 et V_2 deux espaces vectoriels. Le *produit tensoriel* de V_1 et V_2 est l'unique espace (à isomorphismes près) $V_1 \otimes V_2$ muni d'une application bilinéaire $V_1 \times V_2 \to V_1 \otimes V_2$, $(x_1, x_2) \mapsto x_1 x_2$ telle que, étant donné une base (e_i) de V_1 et une base (f_i) de V_2, l'image $(e_i f_j)$ des deux bases est une base de $V_1 \otimes V_2$.

Définition 2.6. Soient $\rho^1 : G \to GL(V_1)$ et $\rho^2 : G \to GL(V_2)$ deux représentations de G. Le produit tensoriel de ρ_1 et ρ_2 est la représentation

$$\rho^1 \otimes \rho^2 : G \to GL(V_1 \otimes V_2),\ s \mapsto \rho_s^1 \otimes \rho_s^2$$

Avec $\rho_s^1 \otimes \rho_s^2$ défini pour tout $x_1 \in V_1$, $x_2 \in V_2$ par $(\rho_s^1 \otimes \rho_s^2)(x_1 \otimes x_2) = \rho_s^1(x_1)\rho_s^2(x_2)$.

Définition 2.7. Le *caractère* χ d'une représentation $\rho : G \to GL(V)$ est la trace de cette représentation. Plus précisément, soit $s \in G$, on définit

$$\chi(s) := Tr(\rho(s))$$

C'est notamment la somme des valeurs propres (avec multiplicité) de $\rho(s)$. Un caractère *irréductible* est le caractère d'une représentation irréductible.

Exemple. Le caractère r_G de la représentation régulière ρ est donné par

$$r_G(s) = \begin{cases} g & \text{si } s = 1 \\ 0 & \text{sinon.} \end{cases}$$

où g est l'ordre de G.
En effet, dans la base donnée par les éléments de G, on a pour tout $t \in G$ que $\rho_s t = st$, et $st = t$ si et seulement si $s = 1$, donc la diagonale de ρ_s est nulle si $s \neq 1$.

Proposition 2.3. *Soit χ le caractère d'une représentation ρ de degré n. On a, pour tout $s, t \in G$:*

1. $\chi(1) = n$
2. $\chi(s^{-1}) = \overline{\chi(s)}$
3. $\chi(tst^{-1}) = \chi(s)$

Démonstration.

1. se déduit immédiatement du fait que $\rho(1) = 1$.
2. vient du fait que $\rho(s)$ est d'ordre fini divisant $|G|$. Donc ses valeurs propres $\lambda_1, \ldots, \lambda_n$ sont aussi d'ordre fini et donc de module 1. On a alors :
$$\chi(s^{-1}) = \sum \lambda_i^{-1} = \sum \overline{\lambda_i} = \overline{\sum \lambda_i} = \overline{\chi(s)}$$
3. découle de l'invariance de la trace par similitudes. □

Définition 2.8. Une application f sur G est *centrale* si elle invariante par conjugaison, c'est-à-dire pour tout $s, t \in G$

$$f(tst^{-1}) = f(s)$$

Ou encore

$$f(ts) = f(st)$$

Les caractères en sont un exemple.

Proposition 2.4. *Soient $\rho^1 : G \to GL(V_1)$ et $\rho^2 : G \to GL(V_2)$ deux représentations de G, χ_1 et χ_2 leurs caractères respectifs.*

1. *Le caractère de la somme directe $V_1 \oplus V_2$ est $\chi_1 + \chi_2$.*
2. *Le caractère du produit tensoriel $V_1 \otimes V_2$ est $\chi_1 \chi_2$.*

Démonstration. La première affirmation découle directement du fait que la matrice de $\rho_s^1 \oplus \rho_s^2$ est donnée par

$$\begin{pmatrix} M_s^1 & 0 \\ 0 & M_s^2 \end{pmatrix}$$

où M_s^1 et M_s^2 sont les matrices de ρ_s^1 et ρ_s^2 respectivement.
De même, pour la deuxième affirmation, les composantes de la matrice de $\rho_s^1 \otimes \rho_s^2$ est donnée par le produit des composantes des matrices de ρ_s^1 et ρ_s^2, d'où le résultat. □

Lemme 2.5 (de Schur). *Soient $\rho^1 : G \to GL(V_1)$ et $\rho^2 : G \to GL(V_2)$ deux représentations irréductibles de G, $f : V_1 \to V_2$ une application linéaire telle que $\rho^2 \circ f = f \circ \rho^1$. Alors :*

1. *Si ρ^1 n'est pas isomorphe à ρ^2, $f = 0$.*
2. *Si $V_1 = V_2$ et $\rho^1 = \rho^2$, f est une homothétie (un multiple scalaire de l'identité).*

Démonstration. Si $f = 0$, le lemme est trivial. Si $f \neq 0$, le noyau W_1 de f est une sous-représentation de V_1. Par irréductibilité de V_1, $W_1 = V_1$ ou $W_1 = 0$. Le premier cas implique $f = 0$, donc $W_1 = 0$ et f est injective. De la même façon, on a que l'image W_2 de f est égal à V_2, d'où f est surjective. Par définition, f est alors un isomorphisme de V_1 sur V_2 ce qui démontre le premier point.
Dans la situation de 2., si on prend une valeur propre $\lambda \in \mathbb{C}$ (il en existe une car $\mathbb{C}$ est algébriquement clos donc f est triangularisable), $f - \lambda id$ possède un noyau différent de zéro. Par ce qui précède, on a bien $\ker(f - \lambda id) = V_1$ et $f = \lambda id$. □

Corollaire 2.5.1. *Sous les hypothèses du lemme de Schur, soient $h : V_1 \to V_2$ linéaire, g l'ordre de G. Posons :*

$$\tilde{h} = \frac{1}{g} \sum_{t \in G} \rho^2(t^{-1}) h \rho^1(t)$$

Alors :

1. *Si ρ^1 et ρ^2 ne sont pas isomorphes, $\tilde{h} = 0$.*
2. *Si $V_1 = V_2$ et $\rho^1 = \rho^2$, $\tilde{h}$ est une homothétie de rapport $\frac{Tr(h)}{\dim(V_1)}$.*

Démonstration. $\tilde{h}$ satisfait les hypothèses du lemme de Schur. En effet, $\tilde{h}$ est évidemment linéaire et :

$$\rho^2(s^{-1})\tilde{h}\rho^1(s) = \frac{1}{g} \sum_{t \in G} \rho^2(s^{-1})\rho^2(t^{-1}) h \rho^1(t)\rho^1(s) = \frac{1}{g} \sum_{t \in G} \rho^2((ts)^{-1}) h \rho^1(ts) = \tilde{h}$$

Donc $\rho^2(s)\tilde{h} = \tilde{h}\rho^1(s)$ et par le lemme 2.5, on conclut dans le premier cas. Pour le deuxième, on sait que $\tilde{h}$ est une homothétie, i.e. un scalaire λ qu'il nous faut calculer. Mais

$$\dim(V_1)\lambda = Tr(\tilde{h}) = \frac{1}{g}\sum_{t\in G} Tr(\rho^2(t^{-1})h\rho^1(t)) = \frac{1}{g}\sum_{t\in G} Tr(h) = Tr(h),$$

d'où le résultat. □

On va réécrire le corollaire 2.5.1 sous forme matricielle. Supposons que ρ^1 *et* ρ^2 *sont données par les matrices :*

$$\rho^1(t) = (r_{i_1 j_1}(t))$$

$$\rho^2(t) = (r_{i_2 j_2}(t))$$

Corollaire 2.5.2. *Dans le premier cas, on a quels que soient* i_1, i_2, j_1, j_2 *:*

$$\frac{1}{g}\sum_{t\in G} r_{i_1 j_1}(t) r_{i_2 j_2}(t) = 0$$

Dans le second cas, on a :

$$\frac{1}{g}\sum_{t\in G} r_{i_1 j_1}(t) r_{i_2 j_2}(t) = \frac{1}{n}\delta_{i_1 i_2}\delta_{j_1 j_2}$$

Démonstration. Supposons h donné matriciellement par $h = (x_{j_1 i_2})$. En appliquant le corollaire 2.5.1, on trouve dans le premier cas $\tilde{h} = 0$ et dans le second cas $\tilde{h} = \frac{1}{n}Tr(h)$. Si on regarde cela comme une forme linéaire sur les $x_{j_1 i_1}$, dans le premier cas, elle est toujours nulle, ses coefficients sont donc nuls. De même pour le deuxième cas, $\tilde{h} = \lambda$ donc les coefficients sont bien $\frac{1}{n}\delta_{i_1 i_2}\delta_{j_1 j_2}$. □

Définitions 2.9. Soient $\phi, \psi : G \to \mathbb{C}$. On pose deux formes bilinéaires symétriques :

$$\langle \phi, \psi \rangle := \frac{1}{g}\sum_{t\in G} \phi(t)\psi(t^{-1})$$

$$(\phi, \psi) := \frac{1}{g}\sum_{t\in G} \phi(t)\overline{\psi(t)}$$

Ces applications sont clairement bilinéaires et symétriques. La deuxième est un produit scalaire et selon la proposition 2.3, les deux sont égales pour les caractères.

Théorème 2.6. *Les caractères irréductibles sont orthonormés pour le produit scalaire défini ci-dessus. C'est-à-dire si $\chi \neq \chi'$ sont des caractères irréductibles, alors :*

$$(\chi|\chi) = 1$$
$$(\chi|\chi') = 0$$

Démonstration. Soit ρ, ρ' des représentations irréductibles non-isomorphes de caractère χ respectivement χ', données sous forme matricielle par $\rho(t) = (r_{ij}(t))$ et $\rho'(t) = (r'_{ij}(t))$. En appliquant le corollaire 2.5.2, on trouve :

$$(\chi|\chi) = \frac{1}{g}\sum_{t\in G}\left(\sum_i r_{ii}(t)\right)\left(\sum_j \overline{r_{jj}(t)}\right) = \sum_{i,j}(r_{ii}, r_{jj}) = \sum_{i,j}\frac{\delta_{ij}}{n} = 1$$

Et de même :

$$(\chi|\chi') = \sum_{i,j}(r_{ii}, r'_{jj}) = 0$$

□

Théorème 2.7. *Soient $V = \bigoplus W_i$ une représentation de G décomposé en somme directe de représentations irréductibles et ϕ son caractère. Le nombre de W_i isomorphes à une représentation irréductible W de caractère χ vaut $(\phi|\chi)$.*

Démonstration. Par la proposition 2.4, si χ_i est le caractère de W_i, alors

$$\phi = \sum \chi_i$$

On en déduit :

$$(\phi|\chi) = \sum(\chi_i|\chi)$$

D'après le théorème 2.6, $(\chi_i|\chi) = 1$ si W_i et W sont isomorphes et 0 sinon. On en conclut le résultat. □

Corollaire 2.7.1. *Deux représentations de même caractère sont isomorphes.*

Démonstration. Le théorème précédent montre qu'elles contiennent toutes les deux le même nombre de fois chaque représentation irréductible. □

Corollaire 2.7.2. *Une représentation irréductible de caractère χ est contenu dans la représentation régulière un nombre de fois égal à son degré n.*

Démonstration. L'exemple 2.7 nous donne que :

$$(r_G, \chi) = \frac{1}{g}\sum_{t\in G} r_G(t)\chi(t^{-1}) = \frac{1}{g}g\chi(1^{-1}) = \chi(1) = n$$

□

Remarque. On peut ainsi ramener l'étude de représentations à celles de leurs caractères. De plus, on constate que toute représentation V de caractère ϕ est isomorphe à la somme directe

$$V = \sum m_i W_i$$

Où les W_i sont les représentations irréductibles et, si χ_i sont leurs caractères respectifs, $m_i = (\phi|\chi_i)$. De plus :

$$(\phi|\phi) = \sum m_i^2$$

On en déduit immédiatement le théorème suivant :

Théorème 2.8. *Soit ϕ le caractère d'une représentation V, $(\phi|\phi)$ est un entier positif et vaut 1 si et seulement V est irréductible.*

Théorème 2.9. *Les caractères irréductibles forment une base orthonormée de l'espace vectoriel des fonctions centrales.*

Démonstration. Le théorème 2.6 montre déjà que les caractères irréductibles forment un ensemble orthonormé. Il faut encore montrer qu'ils engendrent l'espace. Pour cela, montrons que seul 0 est orthogonal à tous les caractères irréductibles. Soit f orthogonale à tous les caractères irréductibles et définissons $\rho_f := \sum_{t\in G} f(t)\rho(t)$ où ρ est la représentation régulière. ρ_f est une application linéaire de $\mathbb{C}[G]$ dans lui-même. De plus :

$$\rho(s^{-1})\rho_f\rho(s) = \sum_{s\in G} f(t)\rho(s^{-1})\rho(t)\rho(s) = \sum_{t\in G} f(t)\rho(s^{-1}ts)$$

Posons $u = s^{-1}ts$. Comme f est centrale, on observe que :

$$\rho(s^{-1})\rho_f\rho(s) = \sum_{u\in G} f(sus^{-1})\rho(u) = \sum_{u\in G} f(u)\rho(u) = \rho_f$$

Et donc par le lemme de Schur, f est une homothétie. Son rapport est $\frac{1}{g}Tr(\rho_f)$ où g est la dimension de $\mathbb{C}[G]$, c'est à dire le cardinal de G. Or, la trace de ρ_f est donnée par

$$Tr(\rho_f) = \sum_{t\in G} f(t)Tr(\rho(t)) = \sum_{t\in G} f(t)\chi(t) = g(f|\chi)$$

Où χ est le caractère de la représentation régulière. Comme f est orthogonale à tous les caractères irréductibles, f est orthogonale à χ par linéarité. Donc $\rho_f = 0$ et alors

$$0 = \rho_f(1) = \sum_{t\in G} f(t)\rho(t)$$

Mais les $\rho(t)$ forment une base de $\mathbb{C}[G]$. On en déduit que $f(t) = 0$ pour tout $t \in G$, c'est-à-dire $f = 0$. □

Théorème 2.10. *Le nombre de représentations irréductibles (à isomorphismes près) est égal au nombre de classes de conjugaison de G.*

Démonstration. Une fonction est centrale si et seulement si elle est constante sur chaque classe de conjugaison. Elle est donc entièrement déterminée par ses valeurs sur chaque classe de conjugaison de G qui peuvent être choisies indépendamment les unes des autres, ce qui implique que la dimension de l'espace vectoriel des fonctions centrales est égal au nombre de classes de conjugaison de G. Le théorème précédent nous permet de conclure. □

3 Représentations induites

Dans ce chapitre, nous allons introduire le concept de représentation induite, qui permet de créer une représentation d'un groupe à partir d'une représentation d'un de ses sous-groupe, et démontrer quelques identités utiles pour la suite.

Définition 3.1. Soient G un groupe, $H \subseteq G$ un sous-groupe, $\rho : G \to GL(V)$ une représentation, $W \subseteq V$ une sous-représentation de ρ_H, la restriction de ρ à H, $\theta : H \to GL(W)$ cette représentation. Soit $s \in G$. Comme W est stable par H, l'espace vectoriel $\rho_s W$ ne dépend que de la classe à gauche sH de s. Pour une classe à gauche $\sigma \in G/H$, on peut donc définir l'espace $W_\sigma := \rho_s W$ pour n'importe quel $s \in \sigma$. La somme $\Sigma_{\sigma \in G/H} W_\sigma$ est stable par G. C'est donc une sous-représentation de V. La représentation ρ est *induite* par θ si

$$V = \bigoplus_{\sigma \in G/H} W_\sigma,$$

c'est-à-dire, V est égal à la somme des W_σ, $\sigma \in G/H$, et cette somme est directe. Si R est un système de représentants de G/H, alors la définition est équivalente à $V = \bigoplus_{r \in R} \rho_r W$. On notera $Ind_H^G(W) := V$ ou parfois simplement $Ind(W)$ la représentation induite. Le théorème suivant montre que cette notation est bien définie.

Théorème 3.1. *Soit $\theta : H \to W$ une représentation de H. Il existe une unique représentation linéaire $\rho : G \to V$ de G induite par θ à isomorphisme près.*

Démonstration. Sans perte de généralité, θ est irréductible, donc isomorphe à une sous-représentation de la représentation régulière de H selon le corollaire 2.7.2. De plus, il est immédiat que la représentation régulière de G est induite par celle de H. En restreignant à θ cette induction, on trouve l'espace $V := \sum_{r \in R} \theta_r W$ qui est stable par G et est donc la représentation recherchée. L'unicité découle directement de la définition.

□

Remarque. Comme toute représentation W de G est équivalente à un $\mathbb{C}[G]$-module, une façon plus naturelle de voir la représentation induite est d'étendre les scalaires de $\mathbb{C}[H]$ à $\mathbb{C}[G]$ à l'aide du produit tensoriel :

$$Ind_H^G(W) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$$

Une représentation V de G contenant W est alors induite par W si et seulement si l'injection $W \to V$ se prolonge en un isomorphisme $Ind_H^G(W) \to V$, ce qui montre l'existence et l'unicité de façon naturelle.

Définitions 3.2. Soient f une fonction centrale sur un sous-groupe H de G. h la cardinalité de H. La *fonction induite* par f sur G est

$$Ind_H^G(f)(s) := \frac{1}{h} \sum_{t\in G,\ t^{-1}st\in H} f(t^{-1}st)$$

que l'on notera parfois $Ind(f)$ pour alléger la notation.
Soit f' une fonction centrale sur G, on note

$$Res_H^G(f') := f'|_H$$

la restriction de f' à H, que l'on notera parfois aussi $Res(f')$.

Proposition 3.2. *1. $Ind(f)$ est une fonction centrale sur G*

2. *Si χ est le caractère d'une représentation W sur H, $Ind(\chi)$ est le caractère ψ de la représentation induite.*

Démonstration. Toute fonction centrale étant combinaison linéaire de caractères, et étant donné que l'opérateur d'induction est linéaire, 1. se déduit immédiatement de 2.
Soient R un ensemble de représentants des classes de G/H et $V = \bigoplus_{r\in R} \rho_r W$ la représentation induite. Pour $u \in G$ et $r \in R$, écrivons $ur = r_u t$, avec $r_u \in R$ et $t \in H$. Alors ρ_u permute les $\rho_r W$ et plus précisément $\rho_u \rho_r W = \rho_{r_u} W$. Ainsi, dans la matrice de ρ_u, les $r \in R$ tels que $r \neq r_u$ donnent des coefficients nuls dans la diagonale donc de trace nulle. On trouve donc :

$$\psi(u) = \sum_{r=r_u} Tr(\rho_u|_{\rho_r W})$$

Si $r = r_u$, alors $t = r^{-1}ur$ et $Tr(\rho_u|_{\rho_r W}) = Tr(\rho_{r^{-1}ur}|_{\rho_r W}) = Tr(\rho_t|_{\rho_r W}) = \chi(t)$. On en conclut que :

$$\psi(u) = \sum_{r=r_u} \chi(r^{-1}ur) = \sum_{r\in R,\ r^{-1}ur\in H} \chi(r^{-1}ur) = \frac{1}{h} \sum_{s\in G,\ s^{-1}us\in H} \chi(s^{-1}us)$$

□

Théorème 3.3 (Formule de réciprocité de Frobenius). *Soient $\langle\cdot,\cdot\rangle_H$ et $\langle\cdot,\cdot\rangle_G$ les formes bilinéaires définies en 2.9 de respectivement H et G, ψ une fonction centrale sur H et ϕ une fonction centrale sur G. Alors :*

$$\langle\psi, Res(\phi)\rangle_H = \langle Ind(\psi), \phi\rangle_G$$

Démonstration. Comme ϕ est centrale, elle est invariante par conjugaison. Par calcul direct, on obtient alors :

$$\langle Ind(\psi), \phi\rangle_G = \frac{1}{g}\sum_{s\in G}\left(\frac{1}{h}\sum_{t\in G,\ t^{-1}st\in H}\psi(t^{-1}st)\right)\phi(s^{-1})$$

$$= \frac{1}{gh}\sum_{s,t\in G,\ t^{-1}st\in H}\psi(t^{-1}st)\phi(t^{-1}s^{-1}t)$$

En posant $u = t^{-1}st$, on trouve :

$$\langle Ind(\psi), \phi\rangle_G = \frac{1}{gh}\sum_{u\in H} g\psi(u)\phi(u^{-1}) = \langle \psi, Res(\phi)\rangle_H$$

□

Proposition 3.4. *Soient ψ une fonction centrale sur H et ϕ une fonction centrale sur G. Alors :*

$$Ind(\psi Res(\phi)) = Ind(\psi)\phi$$

Démonstration. Par calcul direct, on obtient :

$$Ind(\psi Res(\phi))(s) = \frac{1}{h}\sum_{t\in G,\ t^{-1}st\in H}(\psi(t^{-1}st)\phi(t^{-1}st))$$

$$= \left(\frac{1}{h}\sum_{t\in G,\ t^{-1}st\in H} f(t^{-1}st)\right)\phi(s) = (Ind(\psi)\phi)(s)$$

□

Proposition 3.5. *Soient $K \subseteq H \subseteq G$ et W une représentation de K. Alors $Ind_H^G(Ind_K^H(W)) = Ind_K^G(W)$.*

Démonstration. Cela découle directement du fait que si R est un ensemble de représentants de H/K et S est un ensemble de représentants de G/H, alors SR est un ensemble de représentants de G/H, car alors :

$$Ind_H^G(Ind_K^H(W)) = \bigoplus_{s\in S}\rho_s\left(\bigoplus_{r\in R}\rho_r W\right) = \bigoplus_{s\in S,\ r\in R}\rho_{sr}W = Ind_K^G(W).$$

□

Proposition 3.6. *Soient G, $H \subseteq G$ un sous-groupe de G, K un sous-groupe normal de G contenu dans H et W une représentation de H/K. Alors H agit par projection sur W et G de la même façon sur $Ind_{H/K}^{G/K}(W)$ et*

$$Ind_H^G(W) = Ind_{H/K}^{G/K}(W)$$

en tant que représentations de G.

Démonstration. En effet, par le troisième théorème d'isomorphisme, $(G/K)/(H/K) \cong G/H$. Ainsi un ensemble de représentants R de G/H donne un ensemble de représentant $\{rK | r \in R\}$ de $(G/K)/(H/K)$. Alors :

$$Ind_H^G(W) = \bigoplus_{r \in R} \rho_r W = \bigoplus_{r \in R} \rho_{rK} W = Ind_{H/K}^{G/K}(W)$$

□

4 Théorème de Brauer

Le but de ce chapitre est de démontrer le théorème de Brauer, qui permet d'exprimer un caractère d'un groupe à partir de caractères de dimension un sur des sous-groupes de ce groupe et qui sera capital dans la prolongation analytique des fonctions L d'Artin.

Définition 4.1. Soient p un nombre premier, G un groupe fini, $x \in G$. x est un *p-élément* ou est *p-unipotent* si l'ordre de x est une puissance de p. x est un *p'-élément* ou est *p-régulier* si l'ordre de x est premier à p. En décomposant le groupe cyclique engendré par x en produit direct d'un groupe cyclique d'ordre une puissance de p et d'un groupe d'ordre premier à p, on voit que tout $x \in G$ se décompose en un produit $x = x_u x_r$ où x_u est p-unipotent et x_r est p-régulier, appelés respectivement la *p-composante* et la *p'-composante* de x.

Définition 4.2. Un *p-groupe* est un groupe d'ordre une puissance de p. Un groupe *p-élémentaire* est le produit d'un groupe cyclique d'ordre premier à p par un p-groupe. Un groupe est *élémentaire* s'il est p-élémentaire pour au moins un p.

Définition 4.3. Soient $x \in G$ un p'-élément, C le sous-groupe cyclique engendré par x et $P \subseteq Z(x)$ un p-sous-groupe de Sylow du centralisateur de x. $H := CP = C \times P$ est un sous-groupe p-élémentaire de G *associé* à x.

Définition 4.4. $R(G)$ est le sous-ensemble des fonctions centrales sur G composé de combinaisons $\mathbb{Z}$-linéaires de caractères.

Théorème 4.1. *Soient G un groupe fini, V_p le sous-groupe de $R(G)$ engendré par les caractères induits des sous-groupes p-élémentaires de G. L'indice de V_p dans $R(G)$ est fini et premier à p.*

V_p est l'image de l'homomorphisme

$$Ind : \bigoplus_{H \in X(p)} R(H) \to R(G)$$

où $X(p)$ est l'ensemble des sous-groupes p-élémentaires de G. C'est de plus un idéal par la proposition 3.4, il suffit donc, pour montrer le théorème, de montrer qu'un certain entier premier à p appartient à V_p.

Théorème 4.2. *Soit $g = p^n l$ l'ordre de G, avec $p \nmid l$. Alors $l \in V_p$.*

Soient μ_g une racine primitive g-ième de l'unité, $A = \mathbb{Q}[\mu_g]$ le corps cyclotomique engendré par cette racine. En prenant le produit tensoriel de l'identité sur A avec Ind, on définit une application A-linéaire

$$id_A \otimes Ind : \bigoplus_{H \in X(p)} A \otimes R(H) \to A \otimes R(G)$$

satisfaisant les propriétés suivantes :

Lemme 4.3. *L'image de $id_A \otimes Ind$ est $A \otimes V_p$ et $(A \otimes V_p) \cap R(G) = V_p$.*

Ainsi, il suffit de montrer que $l \in Im(id_A \otimes Ind)$, c'est à dire qu'il existe $a_H \in A$ et $f_H \in R(H)$ pour chaque $H \in X(p)$ tels que $l = \sum_{H \in X(p)} a_H Ind_H^G(f_H)$.

Définition 4.5. Soit C un groupe cyclique d'ordre c. On définit la fonction θ_C sur C par :

$$\theta_C(x) = \begin{cases} a & \text{si } x \text{ engendre } A \\ 0 & \text{sinon} \end{cases}$$

Proposition 4.4. *Soit G un groupe fini d'ordre g. Alors :*

$$g = \sum_{C \subseteq G} Ind_C^G(\theta_C)$$

La sommation étant sur l'ensemble des sous-groupes cycliques de G.

Démonstration. On a

$$Ind_C^G(x) = \frac{1}{a} \sum_{y \in G,\ yxy^{-1} \in C} \theta_C(yxy^{-1}) = \sum_{y \in G,\ yxy^{-1}\ engendre\ C} 1$$

Mais pour chaque $y \in G$, yxy^{-1} engendre un unique groupe cyclique. Ainsi :

$$\sum_{C \subseteq G} Ind_C^G(\theta_C) = \sum_{y \in G} 1 = g$$

□

Lemme 4.5. *Toute fonction centrale $f : G \to \mathbb{Z}$ à valeurs divisibles par g peut être écrite comme une combinaison A-linéaire de caractères induits par des caractères de sous-groupes cycliques de G.*

Démonstration. Puisque g divise toutes les valeurs de f, on peut écrire $f = g\chi$ où χ est une fonction centrale à valeurs entières. La proposition précédente nous permet d'écrire :

$$f = g\chi = \sum_{C \subseteq G} Ind_C^G(\theta_C)\chi = \sum_{c \subseteq G} Ind_C^G(\theta_C Res_C^G(\chi))$$

Il suffit de montrer que $\chi_C := \theta_C Res_C^G(\chi)$ est combinaison A-linéaire de caractères de C pour conclure. Mais comme les valeurs de χ_C sont divisibles par l'ordre de c, $(\chi_C, \psi) \in A$ pour tout caractère ψ de C, d'où le résultat. □

Lemme 4.6. *Soient $\chi \in A \otimes R(G)$ à valeurs dans $\mathbb{Z}$, $x \in G$ et x_r la p'-composante de x. Alors :*

$$\chi(x) \equiv \chi(x_r) \pmod{p}$$

Démonstration. Par le lemme précédent, on peut supposer que G est cyclique et engendré par x. Alors $\chi = \sum a_i\chi_i$ avec $a_i \in A$ et χ_i les caractères irréductibles de G, c'est-à-dire ceux de degré 1 puisque G est abélien. x_r étant une puissance de x, il existe une puissance q de p tel que $x^q = x_r^q$, d'où $\chi_i(x)^q = \chi_i(x_r)^q$. Ainsi :

$$\chi(x)^q \equiv (\sum a_i\chi(x))^q \equiv \sum a_i^q\chi_i(x)^q \equiv \sum a_i\chi_i(x_r)^q \equiv \chi(x_r)^q \pmod{pA}$$

Comme $pA \cap \mathbb{Z} = p\mathbb{Z}$ et que χ est à valeurs entières, on en déduit que $\chi(x)^q = \chi(x_r)^q \pmod p$. Comme q est une puissance de p, on peut conclure par le petit théorème de Fermat. □

Lemme 4.7. *Soient x un p'-élément de G, H un sous-groupe p-élémentaire de G associé à x. Alors il existe $\psi \in A \otimes R(H)$ à valeurs dans $\mathbb{Z}$ tel que $\psi' = Ind_H^G\psi$ vérifie :*

1. $\psi'(x) \not\equiv 0 \pmod p$
2. $\psi'(s) = 0$ *pour tout p'-élément $s \in G$ non-conjugué à x.*

Démonstration. Par définition $H = C \times P$ où C est le groupe cyclique engendré par x et $P \subseteq Z(x)$ est un p-sous-groupe de Sylow. Soient c l'ordre de C, p^a l'ordre de P, $\psi_C(x) : C \to \mathbb{Z}$ définie par $\psi_C(x) = c$ et $\psi_C(y) = 0$ sinon. Par le lemme 4.6, $\psi_C \in A \otimes R(C)$. On peut étendre ψ_C à H en posant $\psi(xy) = \psi_C(x)$ pour tout $x \in C$, $y \in P$. ψ est alors la fonction recherchée. En effet, si $s \in G$ est un p'-élément et $y \in G$, alors ysy^{-1} est un p'-élément. S'il appartient à H, il appartient donc à C. Ainsi, $\psi'(s) = 0$ si s n'est pas conjugué à x, ce qui montre le deuxième point. Calculons $\psi'(x)$:

$$\psi'(x) = \frac{1}{p^a} \sum_{yxy^{-1}=x} \psi(x) = \frac{|Z(x)|}{p^a}$$

Et alors $\psi'(x) \not\equiv 0 \pmod p$, puisque P est un p-sous-groupe de Sylow de $Z(x)$. □

Lemme 4.8. *Il existe $\psi \in A \otimes V_p$ à valeurs dans $\mathbb{Z}$ tel que $\psi(x) \not\equiv 0 \pmod p$ pour tout x dans G.*

Démonstration. Soient $(x_i)_{i\in I}$ un ensemble de représentants des classes p-régulières formé de p'-éléments et $(\psi_i)_{i\in I}$ l'ensemble des fonctions construites au lemme précédent par rapport à chaque x_i. $\psi := \sum_{i\in I}\psi_i$ convient. En effet, ψ appartient clairement à $A \otimes V_p$ et pour tout $x \in G$, sa p'-composante est conjuguée à un unique x_i. □

Preuve du théorème 4.2. Soit ψ comme au lemme précédent. Comme p ne divise pas les valeurs de ψ, le petit théorème de Fermat nous permet de dire que $\psi^{\phi(p^n)} \equiv 1$ où ϕ est l'indicatrice d'Euler et l'ordre de G est $g = p^n l$.

Ainsi, en posant $r := \phi(p^n) = p^{n-1}(p-1)$, la fonction $l(\psi^r - 1)$ est à valeurs divisibles par g. Le lemme 4.5 nous dit alors que cette fonction est dans $A \otimes V_p$. De plus, comme $A \otimes V_p$ est un idéal, $l\psi^r \in A \otimes V_p$. Par soustraction, on a bien que $l \in V_p$. □

Théorème 4.9. *Tout caractère de G est combinaison linéaire à coefficients entiers de caractères induits par des caractères de sous-groupes élémentaires.*

Démonstration. Il suffit de montrer que la somme $V = \sum_{p|g} V_p$ est égale à $R(G)$. Or, l'indice de V dans G divise celui de V_p pour chaque p. Il est donc premier à tous les nombres premier divisant g. La seule possibilité est que $[G : V_p] = 1$. □

Définition 4.6. Un groupe G est *nilpotent* s'il existe une suite d'extensions

$$\{1\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

telle que G_{i-1} est normal dans G et G_i/G_{i-1} est contenu dans le centre de G/G_{i-1} pour tout $i = 1, ..., n$.

Proposition 4.10. *Tout p-groupe G est nilpotent*

Démonstration. Considérons l'action de G sur lui-même par conjugaison. Le centre $Z(G)$ de G est l'ensemble des éléments fixés par l'action. $G \backslash Z(G)$ est réunion disjointes d'orbites non-triviales, c'est-à-dire d'orbite de cardinal une puissance non-nulle de p. On en déduit que :

$$|Z(G)| \equiv |G| \equiv 0 \pmod{p}.$$

D'où, si $G \neq \{1\}$, alors $Z(G) \neq \{1\}$. Et alors, $G/Z(G)$ est aussi un p-groupe de cardinal plus petit. Par récurrence, il est nilpotent et donc il existe une suite

$$Z(G)/Z(G) \subseteq G_1/Z(G) \subseteq ... \subseteq G/Z(G)$$

telle que $(G_i/Z(G))/(G_{i-1}/Z(G)) \cong G_i/G_{i-1}$ contenu dans le centre de $(G/Z(G))/(G_{i-1}/Z(G)) \cong G/G_{i-1}$. Donc la suite

$$\{1\} \subseteq Z(G) \subseteq G_1 \subseteq ... \subseteq G_n = G$$

convient. □

Lemme 4.11. *Soit G un groupe nilpotent non-commutatif. Il existe un sous-groupe commutatif normal dans G non-contenu dans son centre.*

Démonstration. Si on quotiente chaque groupe G_i de la suite d'extensions par $Z(G) \cap G_i$, on voit immédiatement que $G/Z(G)$ est aussi nilpotent. Soit $\overline{H}$ le premier sous-groupe non-trivial de la suite. Alors $\overline{H}$ est inclus dans le centre de $G/Z(G)$ et est donc commutatif. Comme il est fini, on peut l'écrire

comme un produit de sous-groupes cycliques. Ainsi, H est cyclique sans perte de généralité, en étendant la suite d'extension entre $\{1\}$ et H. Alors la pré-image A de H est le sous-groupe recherché. En effet, A n'est pas inclus dans $Z(G)$ par définition. De plus, si $xZ(G)$ génère H, alors pour tout $y \in A$, $y = x^r z$ avec $r \in \mathbb{N}$ et $z \in Z(G)$. On en conclut que si $y_1 = x^{r_1} z_1$ et $y_2 = x^{r_2} z_2$, alors comme z_1 et z_2 sont dans le centre de G, $y_1 y_2 = x^{r_1+r_2} z_1 z_2 = y_2 y_1$. Donc A est commutatif. □

Proposition 4.12. *Toute représentation irréductible $\rho : G \to V$ d'un groupe nilpotent G est monomiale, c'est-à-dire induite par une représentation de degré un d'un sous-groupe de G.*

Démonstration. Par récurrence sur l'ordre de G. Si G est commutatif, il n'y a rien à démontrer. Sinon, si ρ n'est pas injective, posons $K = \ker \rho$. Alors $\overline{\rho} : G/K \to V$ est injectif et par hypothèse de récurrence, il existe un sous-groupe H/K de G/K et une représentation W de degré un de H/K tels que $V = Ind_{H/K}^{G/K}(W)$. La proposition 3.6 nous permet de conclure. Si ρ est injective, par le lemme précédent, il existe un sous-groupe commutatif A normal dans G non-contenu dans le centre de G. Alors $\rho(A)$ n'est pas inclue dans le centre de $\rho(G)$ comme ρ est injective, donc il existe $a \in A$ tel que $\rho(a)$ n'est pas une homothétie.
Écrivons $V = \sum_i V_i$ la décomposition de la représentation ρ restreinte à A en représentations irréductibles. Comme A est commutatif, $\rho(a)$ restreint à V_i est une homothétie pour tout i. Mais $\rho(a)$ n'est pas une homothétie, il existe donc i et j tel que le rapport d'homothétie de $\rho(a)$ sur V_i et V_j n'est pas le même, c'est-à-dire V_i et V_j ne sont pas isomorphes. Soient V_{i_0} une des représentations et W la somme des V_i isomorphes à V_{i_0}. Soit H le sous-groupe de G des $s \in G$ tels que $\rho(s)W = W$. Alors $Ind_H^G(W) = V$. En effet, comme ρ est irréductible, G permute les V_i transitivement. De plus, si $gW = hW$, alors $gh^{-1}W = W$ donc $gh^{-1} \in H$ par définition. Comme $|H| < |G|$, on conclut à l'aide de l'hypothèse de récurrence et de la proposition 3.5. □

Théorème 4.13 (de Brauer). *Tout caractère de G est une $\mathbb{Z}$-combinaison linéaire de caractères monomiaux.*

Démonstration. Cela résulte directement de ce qui précède et du théorème 4.9, en utilisant le fait que tout caractère irréductible d'un groupe élémentaire est monomial, car ce groupe est nilpotent. □

5 Fonction zêta de Dedekind et fonction L de Hecke

Nous sommes à présent prêts pour introduire les fonctions L, en commençant par celles de Hecke, associées au caractère d'un quotient de groupes d'idéaux. Nous définirons la fonction zêta de Dedekind aussi, qui nous sera utile plus tard.
Soient K une extension de degré fini de $\mathbb{Q}$, $\mathcal{O}_K$ son anneau des entiers et N la norme sur les idéaux entiers de $\mathcal{O}_K$.

Définition 5.1. La fonction zêta de Dedekind pour le corps K est

$$\zeta_K(s) := \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

où la somme est sur l'ensemble des idéaux entiers de $\mathcal{O}_K$. Il est possible de l'écrire sous la forme d'un produit infini

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right),$$

où la somme est sur l'ensemble des idéaux premier de $\mathcal{O}_K$.

Définition 5.2. Soient $\mathfrak{m}$ un idéal de $\mathcal{O}_K$. $J(\mathfrak{m})$ est l'ensemble des idéaux fractionnaires de $\mathcal{O}_K$ premiers à $\mathfrak{m}$, c'est-à-dire si $\mathfrak{a} \in J(\mathfrak{m})$, alors $\mathfrak{a} + \mathfrak{m} = \mathcal{O}_K$. $P(\mathfrak{m})$ est le sous-ensemble des idéaux principaux $x\mathcal{O}_K$ tels que si $x = \frac{a}{b}$ avec $a, b \in \mathcal{O}_K$, alors $a \equiv b \pmod{\mathfrak{m}}$ et a et b sont premiers à $\mathfrak{m}$, et tels que x est totalement positif, c'est-à-dire que tous les plongements réels de x sont positifs. On note $G(\mathfrak{m}) := J(\mathfrak{m})/P(\mathfrak{m})$ qui est un corps fini.
Soit $\chi : G(\mathfrak{m}) \to \mathbb{C}$ un caractère de dimension un de $G(\mathfrak{m})$ étendu à l'ensemble J des idéaux entiers de $\mathcal{O}_K$ en posant $\chi(\mathfrak{a}) = 0$ si $\mathfrak{a} \notin J(\mathfrak{m})$. La fonction L de Hecke associée à $\mathfrak{m}$ et χ est

$$L(\mathfrak{m}, \chi, s) := \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

où $\mathfrak{a}$ parcourt les idéaux de $\mathcal{O}_K$. Dans la suite, on considérera toujours le même idéal $\mathfrak{m}$, on l'omettra donc dans la notation en posant $L(\chi, s) := L(\mathfrak{m}, \chi, s)$. χ étant totalement multiplicatif, il est possible d'écrire $L(\chi, s)$ sous la forme d'un produit infini sur les idéaux premiers de $\mathcal{O}_K$:

$$\prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)$$

Proposition 5.1. *Soient $(a_n) \subseteq \mathbb{C}$ une suite de nombres complexes de somme partielle A_n. S'il existe $0 \geq \sigma_0 < 1$ et $\rho \in \mathbb{C}$ tels que $A_n = \rho n + O(n^{\sigma_0})$, alors la fonction $f(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converge pour $Re(s) > \sigma_0$ avec un pôle en $s = 1$ de résidu ρ si $\rho \neq 0$.*

Démonstration. En posant $b_n = a_n - \rho$ et $g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$, on a que $f(s) = g(s) + \rho\zeta(s)$ donc sans perte de généralité, on peut supposer que $\rho = 0$. Dans ce cas, la fonction converge. En utilisant la formule de sommation d'Abel et en posant $s = \sigma + it$, on trouve :

$$\sum_{n \leq x} \frac{b_n}{n^s} = \frac{1}{x^s} \sum_{n \leq x} b_n + s \int_1^x \frac{\sum_{n \leq t} b_n}{t^{s+1}} ds \ll \frac{x^{\sigma_0}}{x^\sigma} + |s| \int_1^x \frac{x^{\sigma_0}}{t^{\sigma+1}} ds$$

$$\ll \frac{1}{x^{\sigma-\sigma_0}} + \frac{|s|}{x^{\sigma+2-\sigma_0}} - \frac{1}{\sigma + 2\sigma_0}$$

□

Proposition 5.2. *Il existe une constante dépendant uniquement de* $\mathfrak{m}$ *telle que pour chaque classe* $C \in G(\mathfrak{m})$*, le nombre d'idéaux de* $\mathcal{O}_K$ *dans* C *de norme plus petite ou égale à* n *vaut* $\rho n + O(n^{1-n_k^{-1}})$*, où* $n_k := [K : \mathbb{Q}]$.
La démonstration de cette proposition ne sera pas faite ici. Elle consiste principalement au calcul du volume fondamental d'un réseau.

Proposition 5.3. *La fonction L de Hecke s'étend de façon méromorphe sur* $Re(s) > 1 - n_k^{-1}$ *avec un unique pôle en* $s = 1$ *de résidu* $|G(\mathfrak{m})|\rho$ *si* $\chi = 1$.

Démonstration. En séparant la somme des coefficients selon les différentes classes de $G(\mathfrak{m})$, les relations d'orthogonalité des caractères ainsi que la proposition précédente nous donnent que :

$$\sum_{a \in J(\mathfrak{m}),\ N(\mathfrak{a}) \leq n} \chi(\mathfrak{a}) = \begin{cases} |G(\mathfrak{m})|\rho n + O(n^{1-n_k^{-1}}) & \text{si } \chi = 1 \\ O(n^{1-n_k^{-1}}) & \text{sinon} \end{cases}$$

La proposition 5.1 permet alors de conclure. □

Remarque. On en déduit que ζ_K est égal à la fonction L de Hecke pour le caractère trivial 1 à un nombre fini de facteurs près

$$\zeta_K(s) = L(\mathfrak{m}, 1, s) \prod_{\mathfrak{p} | \mathfrak{m}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right),$$

ce qui permet de conclure que ζ_K est holomorphe pour tout $Re(s) > 1 - n_K^{-1}$ excepté pour un pôle d'ordre 1 en $s = 1$.

6 Fonction L d'Artin

Ce chapitre introduit les fonctions L d'Artin puis les relient aux fonctions L de Hecke grâce au théorème de Brauer afin de les prolonger au-delà du demi-plan complexe $Re(s) \geq 1$.
Commençons par poser quelques notations valables pour les prochains chapitres. On fixe L/K une extension de degré fini de corps de nombres et galoisienne, c'est-à-dire normale et séparée, $G = G(L/K) := Hom_K(L, \mathbb{C})$ son groupe de Galois et $\mathcal{O}_L$ et $\mathcal{O}_K$ les anneaux des entiers de respectivement L et K munis de leur norme N sur leurs idéaux respectifs. On rappelle plusieurs notions de théorie algébrique des nombres et de théorie de Galois.

Définition 6.1. Soient $\mathfrak{p}$ un idéal premier de K et $\mathfrak{P}|\mathfrak{p}$ un idéal premier de L au-dessus de $\mathfrak{p}$, le *groupe de décomposition* $G_\mathfrak{P}$ de $\mathfrak{P}$ est son stabilisateur pour l'action de G, c'est-à-dire

$$G_\mathfrak{P} := \{\sigma \in G | \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

Soit $\sigma \in G_\mathfrak{P}$. Comme $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ et $\sigma(\mathfrak{p}) = \mathfrak{p}$, σ induit un isomorphisme

$$\overline{\sigma} : k_\mathfrak{P} \to k_\mathfrak{P}$$

sur le corps résiduel $k_\mathfrak{P} := \mathcal{O}_L/\mathfrak{P}$ fixant $k_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. $k_\mathfrak{P}$ est une extension galoisienne de $k_\mathfrak{p}$. On obtient un homomorphisme surjective

$$D_\mathfrak{P} \to Gal(k_\mathfrak{P}/k_\mathfrak{p}),$$

$$\sigma \to \overline{\sigma}$$

Le *groupe d'inertie* $I_\mathfrak{P}$ de $\mathfrak{P}$ est alors le noyau de cette application, c'est-à-dire :

$$I_\mathfrak{P} := \{\sigma \in G_\mathfrak{P} | \forall z \in \mathcal{O}_L \ \sigma(z) = z \pmod{\mathfrak{P}}\}$$

En particulier, si $\mathfrak{p}$ est non-ramifié, alors $I_\mathfrak{P}$ est trivial et l'homomorphisme est un isomorphisme. Soit φ l'automorphisme de Frobenius générant le groupe $Gal(k_\mathfrak{P}/k_\mathfrak{p})$, donné par $\varphi(z) := z^q$ où $q := N(\mathfrak{p})$. Le *Frobenius* $\varphi_\mathfrak{P} \in G_\mathfrak{P}/I_\mathfrak{P}$ en $\mathfrak{P}$ est la pré-image de l'automorphisme de Frobenius par l'isomorphisme (ou l'ensemble des pré-images si $\mathfrak{p}$ est ramifié). Les Frobenius au-dessus de $\mathfrak{p}$ sont tous conjugués. En particulier, si $\mathfrak{p}$ est non-ramifié, l'ensemble des Frobenius est une classe de conjugaison de G. Le *Frobenius* ou *symbole d'Artin* en $\mathfrak{p}$ est cette classe de conjugaison, notée souvent $\left(\frac{L/K}{\mathfrak{p}}\right)$ ou encore :

$$\varphi_\mathfrak{p} := \{\varphi_\mathfrak{P} : \mathfrak{P}|\mathfrak{p}\}$$

Définition 6.2. Soient $\rho : G \to GL(V)$ une représentation de G de caractère χ, $\mathfrak{p}$ un idéal de K et $\mathfrak{P}$ un idéal de L au-dessus de $\mathfrak{p}$. Le Frobenius $\varphi_{\mathfrak{P}}$ agit sur l'espace vectoriel $V^{I_{\mathfrak{P}}}$ des vecteurs fixés par le groupe d'inertie $\mathfrak{P}$. La *série L d'Artin* pour le caractère χ est le produit infini

$$L(L/K, \chi, s) := \prod_{\mathfrak{p}} \det\left(1 - \frac{\rho(\varphi_{\mathfrak{P}})}{N(\mathfrak{p})^s}; V^{I_{\mathfrak{P}}}\right)^{-1}$$

des polynômes caractéristiques des Frobenius en $\mathfrak{P}$ qu'on abrégera $L(\chi, s)$ lorsque l'extension considérée est claire et qu'il n'y a pas de confusion possible avec les fonctions L de Hecke. La série L d'Artin est bien définie car les Frobenius au-dessus de $\mathfrak{p}$ sont tous conjugués et donc possèdent le même polynôme caractéristique et le caractère χ de la représentation la définit à isomorphisme près. Par la suite, on omettra le ρ dans $\rho(\varphi_{\mathfrak{P}})$ pour alléger la notation.

Proposition 6.1. *Pour tout $\delta > 0$, la série L d'Artin $L(\chi, s)$ converge absolument et uniformément sur le demi-plan complexe $Re(s) > 1+\delta$, en particulier $L(\chi, s)$ y est holomorphe.*

Démonstration. Dans $\mathbb{C}$, il est possible de factoriser le polynôme caractéristique du Frobenius

$$\det\left(1 - \frac{\varphi_{\mathfrak{P}}}{N(\mathfrak{p})^s}; V^{I_{\mathfrak{P}}}\right) = \prod_i \left(1 - \frac{\alpha_i}{N(\mathfrak{p})^s}\right)$$

avec α_i des racines de l'unité. La série de Taylor du logarithme en 1 est :

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

En prenant formellement le logarithme du produit, on obtient

$$\log(L(\chi, s)) = \sum_p \sum_i \sum_{n=1}^{\infty} \frac{\alpha_i^n}{nN(\mathfrak{p})^{ns}}.$$

Comme $|\alpha_i| = 1$, que le nombre de racines est borné par $\dim(V)$, que $|N(\mathfrak{p})^s| = N(\mathfrak{p})^{\sigma} \geq p^{1+\delta}$ pour tout $s = \sigma + it$ tel que $\sigma \geq 1 + \delta$ et que le nombre d'idéaux $\mathfrak{p}|p$ au-dessus de p est borné par $n_K = [K : \mathbb{Q}]$, on trouve :

$$|\log(L(\chi, s))| \leq \sum_p \sum_{n=1}^{\infty} \frac{\dim(V) n_K}{np^{n(1+\delta)}} = \dim(V) n_K \log \zeta(1+\delta).$$

Ainsi le produit converge absolument et uniformément. □

Proposition 6.2.

1. *Pour le caractère de la représentation unité $\chi = 1$, on a :*

$$L(L/K, 1, s) = \zeta_K(s)$$

2. *Si χ_1 et χ_2 sont deux caractères de $G(L/K)$, alors :*

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

3. *Soient une plus grande extension galoisienne $L' \supset L \supset K$, χ un caractère de L/K et χ' le caractère obtenu via la représentation de $G(L'/K)$ par projection de $G(L'/K)$ sur $G(L/K)$. Alors :*

$$L(L'/K, \chi', s) = L(L/K, \chi, s)$$

Démonstration.

1. Dans ce cas, on a simplement $\rho(I_\mathfrak{P}) = \{1\}$ donc $V^{I_\mathfrak{P}} = \mathbb{C}$ et $\det(1 - \frac{1}{N(\mathfrak{p})^s}; \mathbb{C}) = 1 - N(\mathfrak{p})^{-s}$.
2. Si $\rho_1 : G \to V_1$ et $\rho_2 : G \to V_2$ sont deux représentations de $G(L/K)$ de caractères respectifs χ_1 et χ_2, alors la somme directe $\rho_1 \oplus \rho_2 : G \to V_1 \oplus V_2$ est une représentation de caractère $\chi_1 + \chi_2$ selon la proposition 2.4 et le polynôme caractéristique de $\varphi_\mathfrak{P}$ est alors le produit des deux polynômes caractéristiques, d'où le résultat :

$$\det(1 - \frac{\varphi_\mathfrak{P}}{N(\mathfrak{p})^s}; (V_1 \oplus V_2)^{I_\mathfrak{P}}) = \det(1 - \frac{\varphi_\mathfrak{P}}{N(\mathfrak{p})^s}; V_1^{I_\mathfrak{P}}) \det(1 - \frac{\varphi_\mathfrak{P}}{N(\mathfrak{p})^s}; V_2^{I_\mathfrak{P}})$$

3. Soit $\rho : Gal(L/K) \to V$ une représentation de caractère χ. La représentation ρ' de $Gal(L'/K)$ est la composition de ρ avec la projection $Gal(L'/K) \to Gal(L/K) \cong Gal(L'/K)/Gal(L'/L)$. Soient $\mathfrak{P}'|\mathfrak{P}|\mathfrak{p}$ des idéaux de $L'/L/K$ chacun l'un au-dessus de l'autre. La projection $Gal(L'/K) \to Gal(L/K)$ induit des projections $G_{\mathfrak{P}'} \to G_\mathfrak{P}$ et $I_{\mathfrak{P}'} \to I_\mathfrak{P}$ pour les groupes d'inertie et de ramification, ce qui induit une projection $G_{\mathfrak{P}'}/I_{\mathfrak{P}'} \to G_\mathfrak{P}/I_\mathfrak{P}$. On peut aussi voir cette projection comme celle du groupe résiduel, les extensions $k_{\mathfrak{P}'}/k_\mathfrak{P}/k_\mathfrak{p}$ étant galoisiennes.
Ainsi, par définition de ρ', $\rho'(I_{\mathfrak{P}'}) = \rho(I_\mathfrak{P})$ et donc $V^{I_{\mathfrak{P}'}} = V^{I_\mathfrak{P}}$ et $\rho'(\varphi_{\mathfrak{P}'}) = \rho(\varphi_\mathfrak{P})$. Le polynôme caractéristique est ainsi le même.

□

Théorème 6.3. *Soient $L \supset M \supset K$ une extension intermédiaire et χ un caractère de $G(L/M)$. Alors :*

$$L(L/M, \chi, s) = L(L/K, Ind(\chi), s)$$

Démonstration. Commençons par poser quelques notations.
Soient $G = G(L/K)$, $H = G(L/M) \subseteq G$ les groupes de Galois des extensions considérées. Soient $\mathfrak{p}$ un idéal premier de K, $\mathfrak{q}_1, ..., \mathfrak{q}_r$ tous les idéaux premiers au-dessus de $\mathfrak{p}$, $\mathfrak{P}_i$ un idéal au-dessus de $\mathfrak{q}_i$ pour chaque $i = 1, ..., r$. Soient encore G_i et I_i les groupes de décomposition et d'inertie de $\mathfrak{P}_i$ par rapport à $\mathfrak{p}$. Alors $H_i := G_i \cap H$ et $I_i' := I_i \cap H$ sont les groupes de décomposition et d'inertie de $\mathfrak{P}_i$ par rapport à $\mathfrak{q}_i$. Soit f_i le degré de $\mathfrak{q}_i$ par rapport à $\mathfrak{p}$. Comme les degrés de $\mathfrak{P}_i$ par rapport à $\mathfrak{q}_i$ et $\mathfrak{p}$ sont respectivement $[G_i : I_i]$ et $[H_i : I_i']$, les théorèmes d'isomorphisme nous donnent :

$$f_i := \frac{[G_i : I_i]}{[H_i : I_i']} = \frac{[G_i : I_i]}{[H_i I_i : I_i]} = [G_i : H_i I_i]$$

Et donc $N(\mathfrak{q}_i) = N(\mathfrak{p})^{f_i}$. Comme l'action de G est transitive sur les idéaux premiers au-dessus de $\mathfrak{p}$, pour chaque i, il existe $\tau_i \in G$ tel que $\tau_i \mathfrak{P}_i = \mathfrak{P}_1$. Et alors $G_i = \tau_i^{-1} G_1 \tau_i$ et $I_i = \tau_i^{-1} I_1 \tau_i$. Soient $\varphi_{\mathfrak{P}_1} \in G_1/I_1$ le Frobenius associé à $\mathfrak{P}_1$ par rapport à $\mathfrak{p}$ et $\varphi \in G_1$ un redressement de $\varphi_{\mathfrak{P}_1}$. Alors $\varphi_i := \tau_i^{-1} \varphi \tau_i \in G_i$ est envoyé sur le Frobenius $\varphi_{\mathfrak{P}_i} \in G_i/I_i$ de $\mathfrak{P}_i$ par rapport à $\mathfrak{p}$ et $\varphi_i^{f_i} \in H_i$ est projeté sur le Frobenius de $\mathfrak{P}_i$ par rapport à $\mathfrak{q}_i$. Soient $\rho : H \to GL(W)$ une représentation de H de caractère χ et $V = Ind_H^G(W)$ la représentation induite sur G. Pour démontrer le théorème, il suffit de montrer que le produit des facteurs de $L(L/M, \chi, s)$ pour $\mathfrak{q}_i, ..., \mathfrak{q}_r$ donne le facteur de $L(L/K, Ind(\chi), s)$ pour $\mathfrak{p}$ ou encore que

$$\det(1 - \varphi t; V^{I_1}) = \prod_{i=1}^{r} \det(1 - \varphi_i^{f_i} t^{f_i}; W^{I_i'})$$

avec le t^{f_i} venant de la valeur différente de la norme pour $\mathfrak{p}$ et $\mathfrak{q}_i$. On se réduit au cas $r = 1$ et $G_1 = G$. La conjugaison de φ_i par τ_i nous donne une application $\tau_i \varphi_i \tau_i^{-1} = \varphi$ agissant sur les éléments $\tau_i v$ de $\tau_i W$ tels que $\varphi_i(w) = w$ d'où $\tau_i \varphi_i \tau_i^{-1}(\tau_i w) = \tau_i w$. Il s'agit donc des éléments fixés par $\tau_i(I_i \cap H)\tau_i^{-1} = I_1 \cap \tau_i H \tau_i^{-1}$. La conjugaison ne changeant pas le polynôme caractéristique, on a

$$\det(1 - \varphi_i^{f_i} t^{f_i}; W^{I_i'}) = \det(1 - \varphi^{f_i} t^{f_i}; (\tau W)^{I_1 \cap \tau_i H \tau_i^{-1}})$$

et $f_i = [G_1 : (G_1 \cap \tau_i H \tau_i^{-1}) I_1]$. Prenons pour chaque i un système de représentants à gauche $\{\sigma_{ij}\}$ de $G_1/G_1 \cap \tau_i H \tau_i^{-1}$. Alors $\{\sigma_{ij}\tau_i\}$ est un système de représentants à gauche de G/H. En effet, si $\sigma \in G$, alors il existe i tel que $\sigma \mathfrak{P}_i = \mathfrak{P}_1$. Donc $\sigma \tau_i^{-1} \mathfrak{P}_1 = \mathfrak{P}_1$ et $\sigma \tau_i^{-1} \in G_i$. Il existe ainsi $h \in H$ tel que $\sigma \tau_i^{-1} = \sigma_{ij} \tau_i h \tau_i^{-1}$ et ainsi $\sigma = \sigma_{ij} \tau_i h$. Comme V est induit par W, on a par définition que :

$$V = \bigoplus_{i,j} \sigma_{ij} \tau_i W$$

Posons $V_i := \bigoplus_j \sigma_{ij}\tau_i W$. Cela définit une décomposition de $V = \bigoplus_i V_i$ en représentations de G_1 et donc :

$$\det(1-\varphi t; V^{I_1}) = \prod_{i=1}^{r} \det(1-\varphi t; V_i^{I_1})$$

Il suffit alors de démontrer :

$$\det(1-\varphi t; V_i^{I_1}) = \det(1-\varphi^{f_i} t^{f_i}; (\tau W)^{I_1 \cap \tau_i H \tau_i^{-1}})$$

On peut ainsi se réduire à la représentation de G_1. Simplifions la notation en remplaçant G_1 par G, I_1 par I, $G_1 \cap \tau_i H \tau_i^{-1}$ par H, f_i par $f = [G : HI]$, V_i par V et enfin $\tau_i W$ par W. Notons que $V = Ind_H^G(W)$ reste valable.
On peut même supposer $I = \{1\}$. En effet, posons $\overline{G} = G/I$ et $\overline{H} = H/(I \cap H)$, alors $V^I = Ind_{\overline{H}}^{\overline{G}}(W^{I \cap H})$ selon la proposition 3.6.
Dans cette situation, $I = \{1\}$ nous permet de conclure que φ génère G et $f = [G : H]$, ce qui implique que

$$V = \bigoplus_{i=0}^{f-1} \varphi^i W.$$

Matriciellement, si A est la matrice de φ^f par rapport à une base $w_1, ..., w_d$ de W, et E est la matrice unité $d \times d$, alors la matrice de φ par rapport à la base $\{\varphi^i w_j\}$ de V est

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & A \\ E & 0 & \cdots & 0 & 0 \\ 0 & E & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & E & 0 \end{pmatrix}$$

On en conclut que

$$\det(1-\varphi; V) = \det \begin{pmatrix} E & 0 & \cdots & 0 & -tA \\ -tE & E & \cdots & 0 & 0 \\ 0 & -tE & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -tE & E \end{pmatrix} \det(1-\varphi^f t^f; W)$$

tel que désiré. La dernière égalité étant obtenue en ajoutant la première ligne multipliée par t à la seconde, puis la deuxième ligne multipliée par t à la troisième et ainsi de suite. □

Corollaire 6.3.1.

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

Démonstration. En effet, le caractère induit par le caractère unité est le caractère régulier :

$$Ind(1) = \sum_{\chi} \chi(1)\chi = r_G$$

La proposition ci-dessus ainsi que le premier point de la proposition 6.2 permet alors de directement conclure, en isolant le caractère trivial. □

Théorème 6.4. *Soient L/K une extension abélienne, c'est-à-dire de groupe de Galois $G(L/K)$ abélien, $\rho : G(L/K) \to \mathbb{C}$ une représentation irréductible de degré 1 injective, et $\chi = \rho$ son caractère. Alors il existe un idéal $\mathfrak{m} \in I$ et un caractère $\tilde{\chi} : G(\mathfrak{m}) \to \mathbb{C}$ tels que les fonctions L d'Artin et de Hecke coïncident :*

$$L(L/K, \chi, s) = L(\mathfrak{m}, \tilde{\chi}, s)$$

Ce théorème est une reformulation de la loi de réciprocité d'Artin dans le cas des fonctions L. Il découle de la théorie des corps de classes et ne sera pas démontré ici.

Théorème 6.5. *La fonction L d'Artin admet un prolongement méromorphe à $\{s \in \mathbb{C} | Re(s) > 1 - n_k^{-1}\}$.*

Démonstration. La démonstration passe par trois cas :

1. Si $G(L/K)$ est abélien et χ est injectif, le théorème précédent permet de conclure.
2. Si $\chi : G(L/K) \to \mathbb{C}$ est une représentation irréductible de degré 1, alors par le premier théorème d'isomorphisme, χ se factorise en une représentation $\tilde{\chi} : G(L/K)/\ker\chi \to \mathbb{C}$ injective En posant M la sous-extension $L \supset M \supset K$ telle que $\ker\chi$ fixe M, le théorème fondamental de la théorie de Galois nous permet de conclure que $\ker\chi = G(L/M)$ et $G(L/K)/\ker\chi = G(M/K)$. Le point 3 de la proposition 6.2 nous permet de conclure que $L(L/K, \chi, s) = L(M/K, \tilde{\chi}, s)$. De plus, comme χ est une fonction centrale, on a que pour tout $g, h \in G$, $\chi(ghg^{-1}h^{-1}) = 1$, c'est-à-dire $\chi(gh) = \chi(hg)$ et donc $G/\ker\chi$ est abélien. Le point précédent permet de conclure.
3. Dans le cas général, le théorème de Brauer (4.13) nous dit que $\chi = \sum_{i=1}^{r} a_i Ind_{H_i}^G \chi_i$ avec $a_i \in \mathbb{Z}$ et $\chi_i : H_i \to \mathbb{C}$ des caractères de degrés 1 sur des sous-groupes H_i de G. Le point 2 de la proposition 6.2 et le théorème 6.3 permettent de déduire que :

$$L(L/K, \chi, s) = \prod_{i=1}^{r} L(K/M_i, \chi_i, s)^{a_i}$$

Le point précédent permet alors de conclure.

□

7 Non-annulation des fonctions L

Avant de démontrer le théorème de densité de Chebotarev, il nous faut, comme souvent avec les fonctions L, démontrer que les fonctions L d'Artin ne s'annulent pas sur la droite $Re(s) = 1$. Pour cela, nous commençons par étudier les fonctions L de Hecke, et avant tout, par démontrer une identité trigonométrique utile au théorème suivant.

Lemme 7.1. *Soient $\theta \in \mathbb{R}$ et $k \in \mathbb{N}^*$. Alors :*

$$2k + 1 + 2\sum_{j=1}^{2k}(2k + 1 - j)\cos(j\theta) = \left(1 + 2\sum_{j=1}^{k}\cos(j\theta)\right)^2$$

Démonstration. Procédons par récurrence. Si $k = 1$, l'identité trigonométrique $\cos(2\alpha) = 2\cos^2(\alpha) - 1$ nous donne :

$$3 + 4\cos(\theta) + 2\cos(2\theta) = 3 + 4\cos(\theta) + 4\cos^2(\theta) - 2 = (1 + 2\cos(\theta))^2$$

Si $k > 1$, supposons la formule vraie pour $k - 1$. On a :

$$\left(1 + 2\sum_{j=1}^{k}\cos(j\theta)\right)^2 = \left(1 + 2\sum_{j=1}^{k-1}\cos(j\theta)\right)^2 + 4(1+2\sum_{j=1}^{k-1}\cos(j\theta))\cos(k\theta) + 4\cos^2(k\theta)$$

$$= \left(2k - 1 + 2\sum_{j=1}^{2k-2}(2k - 1 - j)\cos(j\theta)\right) + 4\cos(k\theta) + 8\sum_{j=1}^{k-1}\cos(j\theta)\cos(k\theta) + 2\cos(2k\theta) + 2$$

L'identité trigonométrique $2\cos(\alpha)\cos(\beta) = \cos(\beta - \alpha) + \cos(\beta + \alpha)$ nous donne :

$$4\cos(k\theta) + 8\sum_{j=1}^{k-1}\cos(j\theta)\cos(k\theta) = 4\cos(k\theta) + 4\sum_{j=1}^{k-1}(\cos((k - j)\theta) + \cos((k + j)\theta))$$

$$= 4\sum_{j=1}^{2k-2}\cos(j\theta) + 4\cos((2k - 1)\theta)$$

D'où :

$$\left(1 + 2\sum_{j=1}^{k}\cos(j\theta)\right)^2 = 2k + 1 + 2\sum_{j=1}^{2k-2}(2k + 1 - j)\cos(j\theta) + 4\cos((2k - 1)\theta) + 2\cos(2k\theta)$$

$$= 2k + 1 + 2\sum_{j=1}^{2k}(2k + 1 - j)\cos(j\theta)$$

□

Théorème 7.2. *Soit $f : \mathbb{C} \to \mathbb{C}$ une fonction telle que :*

1. *f est holomorphe et non-nulle dans $Re(s) > 1$.*
2. *Sur la droite $Re(s) = 1$, f est holomorphe sauf en un unique pôle en $s = 1$ d'ordre $e \geq 0$.*
3. *$\log(f(s))$ peut être écrit comme une série de Dirichlet $\sum_{n=1}^{\infty} \frac{b_n}{n^s}$ avec $b_n \geq 0$ pour $Re(s) > 1$. Alors l'ordre des zéros de f sur la droite $Re(s) = 1$ est borné par $e/2$.*

Démonstration. Par l'absurde, supposons que f a un zéro d'ordre $k > e/2$ en $1 + it$ avec $t \in \mathbb{R}$. Alors $e \leq 2k - 1$. Posons :

$$g(s) = f(s)^{2k+1} \prod_{j=1}^{2k} f(s+ijt)^{2(2k+1-j)} = f(s)^{2k+1} f(s+it)^{4k} f(s+2it)^{4k-2} ... f(s+2kit)^2$$

Posons $\sigma = Re(s)$. Alors g est holomorphe pour $\sigma > 1$ et s'annule en s=1, car :

$$4k^2 - (2k+1)e \geq 4k^2 - (2k+1)(2k-1) = 1$$

Mais si $\sigma > 1$,

$$\log(g(s)) = (2k+1)\log(f(s)) + \sum_{j=1}^{2k} 2(2k+1-j)\log(f(s+ijt))$$

$$= \sum_{n=1}^{\infty} \frac{b_n}{n^s} \left(2k+1+2\sum_{j=1}^{2k} \frac{2k+1-j}{n^{ijt}} \right)$$

Posons $\theta := t\log(n)$. Alors :

$$Re(\log(g(\sigma))) = \log|g(\sigma)| = \sum_{n=1}^{\infty} \frac{b_n}{n^{\sigma}} \left(2k+1+2\sum_{j=1}^{2k+1} (2k+1-j)\cos(j\theta) \right)$$

Grâce au lemme 7.1, on trouve que $\log|g(\sigma)| \geq 0$ pour $\sigma > 1$ et donc $|g(\sigma)| \geq 1$ ce qui contredit le fait que g a un zéro en $s = 1$. □

Théorème 7.3. *Les fonctions L de Hecke $L(\chi, s)$ correspondant à des fonctions L d'Artin (via le théorème 6.4) ne s'annulent pas sur la droite $Re(s) = 1$.*

Démonstration. Soit

$$f(s) := \zeta_K(s) L(\chi, s) L(\overline{\chi}, s) L(\chi\overline{\chi}, s)$$

$$= \prod_{\mathfrak{p}} \left[\left(1 - \frac{1}{N(\mathfrak{p})^s}\right) \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right) \left(1 - \frac{\overline{\chi(\mathfrak{p})}}{N(\mathfrak{p})^s}\right) \left(1 - \frac{\chi(\mathfrak{p})\overline{\chi(\mathfrak{p})}}{N(\mathfrak{p})^s}\right) \right]^{-1}$$

En utilisant la série de Taylor de $\log(1-x)$, on trouve :

$$\log(f(s)) = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \left(\frac{1}{N(\mathfrak{p})^{ks}} + \frac{\chi(\mathfrak{p})^k}{N(\mathfrak{p})^{ks}} + \frac{\overline{\chi(\mathfrak{p})}^k}{N(\mathfrak{p})^{ks}} + \frac{\left(\chi(\mathfrak{p})\overline{\chi(\mathfrak{p})}\right)^k}{N(\mathfrak{p})^{ks}} \right)$$

$$= \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{|1+\chi(\mathfrak{p})^k|^2}{N(\mathfrak{p})^{ks}}$$

Le théorème 7.2 permet alors de conclure que $f(s) \neq 0$ sur $Re(s) = 1$, ce qui permet de conclure que $L(\chi, s) \neq 0$ si $s \neq 1$ car f y est holomorphe.
Pour s=1, le corollaire 6.3.1 nous dit que :

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

Si L/K est abélienne, alors les représentations irréductibles de $Gal(L/K)$ sont celles de degré un. La preuve du théorème 6.5 nous dit que ces fonctions L d'Artin coïncident avec des fonctions L de Hecke. Comme les fonctions L de Hecke n'ont pas de pôle et que ζ_L et ζ_K ont un pôle du même ordre, on en déduit que les fonctions L de Hecke ne peuvent s'annuler en $s = 1$. □

Théorème 7.4. *La fonction L d'Artin pour un caractère irréductible χ ne s'annule pas sur la droite $Re(s) = 1$. De plus, si χ n'est pas trivial, la fonction L d'Artin y est holomorphe.*

Démonstration. Si $\chi = 1$, $L(L/K, 1, s) = \zeta_K(s)$ qui est une fonction L de Hecke à un nombre fini de facteurs non-nuls près.
Si $\chi \neq 1$, le théorème de Brauer nous dit que $\chi = \sum_{i=1}^{r} a_i Ind_{H_i}^G \chi_i$. En prenant le produit scalaire avec 1, la formule de réciprocité de Frobenius (3.3) nous dit :

$$0 = (\chi, 1) = \sum_{i=1}^{r} a_i (Ind_{H_i}^G \chi_i, 1) = \sum_{i=1}^{r} a_i (\chi_i, 1|_H)$$

Ainsi, dans le produit

$$L(L/K, \chi, s) = \prod_{i=1}^{r} L(K/M_i \chi_i, s)^{a_i},$$

l'ensemble des pôles créés par la représentation unité des sous-groupes de G s'annule. En effet, chaque représentation χ_i crée un pôle d'ordre $(\chi_i, 1|_H)$ et il n'y a pas de zéro pour créer ou annuler des pôles. La fonction $L(L/K, \chi, s)$ est donc holomorphe et non-nulle sur la droite $Re(s) = 1$. □

8 Théorème de densité de Chebotarev

Dans ce chapitre, nous allons démontrer le théorème de densité de Chebotarev. Pour cela, nous allons utiliser la base de l'espace des fonctions centrales sur $G(L/K)$ donnée par les caractères, afin d'exprimer le problème en termes de fonctions L d'Artin dont on montrera d'abord que les termes correspondants aux caractères non-triviaux sont négligeables.

Définition 8.1. La *fonction de Van Mangoldt* $\Lambda : \mathbb{N} \to \mathbb{C}$ est définie par :

$$\Lambda(n) := \begin{cases} \log(p) & \text{si } n = p^k \text{ où } p \text{ est un nombre premier} \\ 0 & \text{sinon.} \end{cases}$$

Théorème 8.1 (Newman). *Soit $(a_n) \subseteq \mathbb{C}$ une suite de nombres complexes tels que $|a_n| = O(\Lambda(n))$ si $n \to \infty$. Alors la série*

$$f(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

converge sur $Re(s) > 1$. Si par ailleurs $f(s)$ admet un prolongement holomorphe sur un ouvert contenant le demi-plan $Re(s) \geq 1$ avec éventuellement un pôle d'ordre 1 en $s = 1$, alors il existe deux constantes R et L, avec R nulle si f est holomorphe en $s = 1$, telles que :

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = R \log(x) + L + o(1)$$

Ce théorème ne sera pas démontré ici.

Lemme 8.2. *Soit $\chi \neq 1$ un caractère irréductible du groupe de Galois $G = G(L/K)$. Alors*

$$\sum_{N(\mathfrak{p}) \leq x} \chi(\varphi_{\mathfrak{P}}) = R \log(x) + o\left(\frac{x}{\log(x)}\right),$$

où $\mathfrak{P}$ est un idéal au-dessus d'un idéal non-ramifié $\mathfrak{p}$ et R est la constante du théorème précédent, qui est nulle si χ n'est pas trivial.

Démonstration. Soit $L(\chi, s)$ la fonction L d'Artin associée à χ. Comme $L(\chi, s)$ ne s'annule pas dans un ouvert contenant $Re(s) \geq 1$, on peut écrire

$$\log(L(\chi, s)) = - \sum_{\mathfrak{p} \text{ non-ramifiés}} \log\left(\det\left(1 - \frac{\chi(\varphi_{\mathfrak{P}})}{N(\mathfrak{p})^s}\right)\right) + O(1)$$

$$= - \sum_{\mathfrak{p} \text{ non-ramifiés}} \sum_{i} \log\left(1 - \frac{\alpha_{\mathfrak{P},i}}{N(\mathfrak{p})^s}\right) + O(1),$$

où le $O(1)$ est dû aux idéaux ramifiés qui sont en nombre fini, et les $\alpha_{\mathfrak{P},i}$ sont les racines du polynôme caractéristique de $\varphi_{\mathfrak{P}}$, c'est-à-dire ses valeurs propres. En particulier, $\sum_i \alpha_{\mathfrak{P},i} = \chi(\varphi_{\mathfrak{P}})$ et même $\sum_i \alpha_{\mathfrak{P},i}^k = \chi(\varphi_{\mathfrak{P}}^k)$. Par la suite, toutes les sommes sur des idéaux premiers le seront sur les idéaux non-ramifiés, on ne le notera donc plus et on omettra aussi le $O(1)$. La dérivée du négatif du logarithme de la fonction L d'Artin (ou dérivée logarithmique) est alors :

$$-\frac{L'(\chi,s)}{L(\chi,s)} = \sum_{\mathfrak{p}} \sum_i \frac{\alpha_{\mathfrak{P},i} \log(N(\mathfrak{p}))N(\mathfrak{p})^{-s}}{1-\alpha_{\mathfrak{P},i}N(\mathfrak{p})^{-s}}$$

Comme $|\alpha_{\mathfrak{P},i}| = 1$, on peut développer les termes en série géométrique :

$$\frac{\alpha_{\mathfrak{P},i}N(\mathfrak{p})^{-s}}{1-\alpha_{\mathfrak{P},i}N(\mathfrak{p})^{-s}} = \sum_{k=1}^{\infty} \frac{\alpha_{\mathfrak{P},i}}{N(\mathfrak{p})^s}$$

Et on trouve donc :

$$\sum_{\mathfrak{p}} \sum_i \frac{\alpha_{\mathfrak{P},i} \log(N(\mathfrak{p}))N(\mathfrak{p})^{-s}}{1-\alpha_{\mathfrak{P},i}N(\mathfrak{p})^{-s}} = \sum_{\mathfrak{p}} \sum_i \sum_{k=1}^{\infty} \frac{\log(N(\mathfrak{p}))\alpha_{\mathfrak{P},i}^k}{N(\mathfrak{p})^{sk}} = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{\log(N(\mathfrak{p}))\chi(\varphi_{\mathfrak{P}}^k)}{N(\mathfrak{p})^{sk}}$$

On définit un analogue de la fonction de Van Mangoldt pour l'extension K par :

$$\Lambda(\mathfrak{a}) := \begin{cases} \log(N(\mathfrak{p})) & \text{si } \mathfrak{a} = \mathfrak{p}^k \text{ avec } \mathfrak{p} \text{ un idéal premier non-ramifié} \\ 0 & \text{sinon.} \end{cases}$$

On peut alors écrire, en utilisant la multiplicativité de la norme :

$$-\frac{L'(\chi,s)}{L(\chi,s)} = \sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})\chi(\varphi_{\mathfrak{a}})}{N(\mathfrak{a})^s}$$

Qui est bien définit en posant $\varphi_{\mathfrak{p}^k} := \varphi_{\mathfrak{P}}^k$ et $\chi(\varphi_{\mathfrak{a}}) = 0$ sinon, et qui est holomorphe avec un éventuel pôle en $s = 1$. Comme le nombre d'idéaux dont la norme est un entier donné est borné, le théorème de Newman (8.1) nous permet alors de conclure que :

$$\sum_{N(\mathfrak{a}) \leq x} \frac{\Lambda(\mathfrak{a})\chi(\varphi_{\mathfrak{a}})}{N(\mathfrak{a})} = R\log(x) + L' + o(1)$$

De plus :

$$\left| \sum_{N(\mathfrak{p})^k \leq x \ k \geq 2} \frac{\Lambda(\mathfrak{p}^k)\chi(\varphi_{\mathfrak{P}}^k)}{N(\mathfrak{p})^k} \right| \leq \sum_{\mathfrak{p}} \sum_{k=2}^{\infty} \frac{\log(N(\mathfrak{p}))\dim(V)}{N(\mathfrak{p})^k}$$

Le nombre d'idéaux premiers au-dessus de p est borné par $n_K = [K : \mathbb{Q}]$ et la norme de $\mathfrak{p}$ par p^{n_K}. Ainsi :

$$\left| \sum_{N(\mathfrak{p})^k \leq x \ k \geq 2} \frac{\Lambda(\mathfrak{p}^k)\chi(\varphi_{\mathfrak{P}}^k)}{N(\mathfrak{p})^k} \right| \leq \sum_{\mathfrak{p}} \frac{\log(N(\mathfrak{p}))\dim(V)}{N(\mathfrak{p})^2 - N(\mathfrak{p})} \leq \sum_{p} \frac{n_K^2 \log(p)\dim(V)}{p^2 - p}$$

qui converge. On a donc une autre constante L telle que :

$$\sum_{N(\mathfrak{P}) \leq x} \frac{\Lambda(\mathfrak{p})\chi(\varphi_{\mathfrak{P}})}{N(\mathfrak{a})} = R\log(x) + L + o(1)$$

Par la formule de sommation d'Abel, on trouve alors :

$$\sum_{N(\mathfrak{p}) \leq x} \Lambda(\mathfrak{p})\chi(\varphi_{\mathfrak{P}}) = x \sum_{N(\mathfrak{p}) \leq x} \frac{\Lambda(\mathfrak{p})\chi(\varphi_{\mathfrak{P}})}{N(\mathfrak{p})} - \int_1^x \sum_{N(\mathfrak{p}) \leq t} \Lambda(\mathfrak{p})\chi(\varphi_{\mathfrak{P}}) dt$$

$$= x\left(R\log(x) + L + o(1)\right) - \int_1^x \left(R\log(x) + L + o(1)\right) dt$$

$$= Rx\log(x) + Lxo(x) - Rx(\log(x) - 1) - Lx + o(1) = Rx + o(1)$$

En réutilisant la formule de sommation d'Abel, on en conclut :

$$\sum_{N(\mathfrak{p}) \leq x} \chi(\varphi_{\mathfrak{P}}) = \frac{1}{\log(x)} \sum_{N(\mathfrak{p}) \leq x} \Lambda(\mathfrak{p})\chi(\varphi_{\mathfrak{P}}) + \int_2^x \frac{\sum_{N(\mathfrak{p}) \leq t} \Lambda(\mathfrak{p})\chi(\varphi_{\mathfrak{P}})}{t\log^2(t)} dt$$

$$= R\frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right) + \int_2^x \frac{Rt + o(t)}{t\log^2(t)} dt = R\frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right).$$

En effet, si x est suffisamment grand, alors $o(t) \leq t$ pour tout $t \geq \sqrt{x}$ et :

$$\int_2^x \frac{Rt + o(t)}{t\log^2(t)} dt \leq \int_2^{\sqrt{x}} \frac{Rt + o(t)}{t\log^2(t)} dt + 2R\int_{\sqrt{x}}^x \frac{1}{\log^2(t)} dt$$

$$\leq O(\sqrt{x}) + (x - \sqrt{x})\frac{4}{\log^2(x)} = o\left(\frac{x}{\log(x)}\right)$$

□

Théorème 8.3 (de densité de Chebotarev). *Soient $L|K$ une extension galoisienne de corps de nombres de degré fini de groupe de Galois $G = Gal(L/K)$. Alors pour chaque classe de conjugaison $C := Ad(G)(\sigma)$, $\sigma \in G$, l'ensemble P_σ des idéaux premiers non-ramifiés pour lesquels $C = \varphi_{\mathfrak{p}}$ satisfait*

$$\#\{\mathfrak{p} \in P_\sigma | N(\mathfrak{p}) \leq x\} \sim \frac{|C|}{|G|}\pi_K(x)$$

si $x \to \infty$, où $\pi_L(x) := \#\{\mathfrak{p} | N(\mathfrak{p}) \leq x\}$.

Démonstration. Soit 1_C la fonction indicatrice de l'ensemble C, définie par :

$$1_C(t) = \begin{cases} 1 & \text{si } t \in C \\ 0 & \text{sinon.} \end{cases}$$

Comme C est une classe de conjugaison, 1_C est une fonction centrale. Si $c \in C$, le produit scalaire sur les caractères permet alors d'exprimer 1_C comme une combinaison $\mathbb{C}$-linéaire de caractères :

$$\#\{\mathfrak{p} \in P_\sigma | N(\mathfrak{p}) \leq x\} = \sum_{N(\mathfrak{p}) \leq x} 1_C(\varphi_\mathfrak{P}) = \sum_{N(\mathfrak{p}) \leq x} \sum_{\chi} (\chi, 1_C)\chi(\varphi_\mathfrak{P}).$$

Or si $\chi = 1$, alors

$$(1, 1_C) = \frac{|G|}{g} \sum_{t \in G} 1(t^{-1}) 1_C(t) = \frac{|C|}{|G|}.$$

Le lemme précédent nous permet de conclure que

$$\sum_{N(\mathfrak{p}) \leq x} \sum_{\chi \neq 1} (\chi, 1_C)\chi(\varphi_\mathfrak{P}) = o\left(\frac{x}{\log(x)}\right)$$

et, avec le caractère trivial,

$$\sum_{N(\mathfrak{p}) \leq x} 1(\varphi_\mathfrak{P}) = R\frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right)$$

On voit ainsi que la constante R est celle de l'estimation asymptotique de π_L par définition. On en conclut bien que :

$$\sum_{N(\mathfrak{p}) \leq x} 1_C(\varphi_\mathfrak{P}) = \frac{|C|}{|G|} \sum_{N(\mathfrak{p}) \leq x} 1(\varphi_\mathfrak{P}) + o\left(\frac{x}{\log(x)}\right) \sim \pi_K(x).$$

□

9 Conclusion

Ceci conclut la démonstration du théorème de densité de Chebotarev. Pour cela, nous avons commencé par décrire les bases la théorie des représentations linéaires de groupes finis, en particulier les représentations induites. Cela nous a permis de démontrer le théorème de Brauer, qui fut essentiel dans la suite pour relier les fonctions L de Hecke aux fonctions L d'Artin afin d'étendre ces dernières au delà du demi-plan complexe $Re(s) > 1$. La dernière étape avant de démontrer le théorème lui-même, fut de montrer que les fonctions L d'Artin ne s'annulaient pas sur la droite complexe $Re(s) = 1$. Grâce à cela, nous avons pu calculer la dérivée logarithmique de ces fonctions et en déduire leur poids dans l'estimation de la densité d'idéaux premiers non-ramifiés associés à une certaine classe de conjugaison du groupe de Galois. Enfin, nous avons pu conclure en calculant le poids de la fonction L d'Artin associée au caractère trivial, qui est la seule non-négligeable. A noter que le cheminement d'idées du dernier chapitre est très semblable à celui de la démonstration du théorème de la progression arithmétique de Dirichlet, à ceci près que les fonctions L considérées dans ce dernier sont celles de Dirichlet, qui sont associées aux caractères du groupe des unités d'un groupe cyclique fini.

Je remercie le professeur Philippe Michel et le docteur Ramon Moreira Nunes pour m'avoir proposé et suivi dans ce projet et ainsi m'avoir fait découvrir une partie de cette vaste théorie qu'est les fonctions L et plus généralement la théorie algébrique des nombres.

Références

[1] Jean-Pierre Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978.

[2] Nicholas George Triantafillou. The chebotarev density theorem, 2015.

[3] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *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.

[4] M. Ram Murty and V. Kumar Murty. *Non-vanishing of L-functions and applications*, volume 157 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1997.