Versions effectives du théorème de Chebotarev

Alexandre Bailleul

Directeur de mémoire : Florent Jouve

Institut de Mathématiques de Bordeaux

Table des matières

Introduction

Ce document est mon mémoire de Master 2, que j'ai effectué à l'Université de Bordeaux en 2016/2017.

Le théorème de Chebotarev [1] est un théorème central de la théorie des nombres. À l'intersection des théories algébrique et analytique des nombres, c'est un résultat de répartition des nombres premiers (ou plus précisément des idéaux premiers d'un corps de nombres). Dans la lignée du théorème des nombres premiers, ainsi que du théorème des nombres premiers en progressions arithmétiques, il en est une vaste généralisation. On peut également le voir comme une généralisation d'un théorème de Frobenius [2] datant de 1880 pouvant être énoncé sous la forme suivante :

Si f est un polynôme unitaire de degré d à coefficients entiers, de groupe de Galois [3] G, alors la densité asymptotique des nombres premiers tels que $f \bmod p$ se décompose sous la forme d'un produit de n_1 polynômes irréductibles de degré 1, ..., n_r polynômes irréductibles de degré r, est égale à $\frac{|T|}{|G|}$, où T est l'ensemble des permutations de type $(n_1, \ldots, n_r)$ dans G (vu comme sous-groupe de $\mathfrak{S}_d$).

Traditionnellement on démontre le théorème de Chebotarev à l'aide du formalisme de la théorie du corps de classes. Cependant, ce n'était pas l'approche de Chebotarev (en 1922 cette théorie n'existait pas encore !), et ce n'est pas l'approche que l'on va adopter dans ce mémoire. En effet, les versions effectives de ce théorème que l'on souhaite obtenir nécessitent d'entreprendre une méthode très proche de la méthode classique de De La Vallée-Poussin [4] pour démontrer le théorème des nombres premiers.

Le théorème de Chebotarev a de nombreuses applications en théorie des nombres, et les versions effectives que nous avons en vue permettent d'obtenir des estimations non triviales du type « plus petit idéal premier (en norme) vérifiant une

1. Nikolai Grigorievich Chebotaryov (1894-1947)
2. Ferdinand Georg Frobenius (1849-1917)
3. Évariste Galois (1811-1832)
4. Charles-Jean Étienne Gustave Nicolas Le Vieux, Baron de la Vallée Poussin (1866-1962)

propriété ». Citons par exemple une borne sur le plus petit nombre premier dans une certaine classe résiduelle, résultat dans le même esprit que le fameux théorème de Linnik [5]. Nous aurons l'occasion de voir l'influence de certaines conjectures, notamment la conjecture d'Artin [6] sur les fonctions L, et l'hypothèse de Riemann [7] pour ces mêmes fonctions, sur la précision des résultats que l'on peut obtenir.

Je tiens à remercier Florent Jouve de m'avoir proposé ce sujet fascinant, à la fois moderne, et puisant ses sources dans des problèmes anciens, mélangeant les parties analytiques et algébriques de la théorie des nombres. Merci aussi à Léa Audureau–Guillo pour sa relecture attentive et son soutien lors de la rédaction de ce mémoire.

5. Yuri Vladimirovich Linnik (1915-1972)
6. Emil Artin (1898-1962)
7. Georg Friedrich Bernhard Riemann (1826-1866)

I Outils préliminaires

1) Corps de nombres et automorphismes de Frobenius

Dans cette partie, on introduit les objets qui permettent d'énoncer le théorème de Chebotarev, notamment la notion d'automorphisme de Frobenius.

Soit L/K une extension galoisienne de corps de nombres. On notera $\mathcal{O}_K$ et $\mathcal{O}_L$ les anneaux d'entiers de K et L respectivement. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, on peut associer la famille d'idéaux premiers de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, disons $\mathfrak{P}_1, \ldots, \mathfrak{P}_{g_\mathfrak{p}}$, c'est-à-dire les diviseurs premiers de $\mathfrak{p}\mathcal{O}_L$. On montre, par exemple à l'aide du théorème chinois, que le groupe de Galois $G := \mathrm{Gal}(L/K)$ permute transitivement les $\mathfrak{P}_i$. On en déduit le fait fondamental que les indices de ramifications $e(\mathfrak{P}_i/\mathfrak{p})$ sont tous égaux. Notons cette valeur commune $e_\mathfrak{p}$. De même, on montre que les $f(\mathfrak{P}_i/\mathfrak{p})$ sont tous les mêmes, et on note $f_\mathfrak{p}$ leur valeur commune. On obtient alors que

$$e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = [L : K]$$

grâce à la fameuse formule

$$\sum_{\substack{\mathfrak{P} \lhd \mathcal{O}_L \\ \mathfrak{P}|\mathfrak{p}}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = [L : K].$$

Soit maintenant $\mathfrak{p}$ un idéal premier (non nul) de $\mathcal{O}_K$ et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$ (ce que l'on notera désormais sans plus de précisions $\mathfrak{P} \mid \mathfrak{p}$). Notons $k_\mathfrak{P}$ le corps résiduel $\mathcal{O}_L/\mathfrak{P}$ et $k_\mathfrak{p}$ le corps $\mathcal{O}_K/\mathfrak{p}$ (rappelons que $\mathcal{O}_K$ et $\mathcal{O}_L$ sont des anneaux de Dedekind [8], et par conséquent leurs idéaux premiers non nuls sont maximaux).

Définition. Le **groupe de décomposition** associé à $\mathfrak{P}$ est

$$D_\mathfrak{P} = \{\sigma \in G, \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

8. Julius Wilhelm Richard Dedekind (1831-1916)

Autrement dit, $D_{\mathfrak{P}}$ est le stabilisateur de $\mathfrak{P}$ pour l'action de G sur les idéaux premiers de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$. Par la relation orbite-stabilisateur on obtient immédiatement que

$$|D_{\mathfrak{P}}| = \frac{|G|}{g_{\mathfrak{p}}} = e_{\mathfrak{p}} f_{\mathfrak{p}}.$$

Par définition de $D_{\mathfrak{P}}$, l'application

$$\begin{array}{rccc} & D_{\mathfrak{P}} & \longrightarrow & \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \\ \varphi_{\mathfrak{P}} : & \sigma & \longmapsto & \overline{\sigma} \end{array}$$

est bien définie, où $\overline{\sigma}$ désigne $x \bmod \mathfrak{P} \mapsto \sigma(x) \bmod \mathfrak{P}$. Il s'agit clairement d'un morphisme de groupes.

Définition. Le noyau de $\varphi_{\mathfrak{P}}$, noté $I_{\mathfrak{P}}$, est appelé le **groupe d'inertie** associé à $\mathfrak{P}$. On a

$$I_{\mathfrak{P}} = \{\sigma \in G, \forall x \in \mathcal{O}_L, \sigma(x) = x \bmod \mathfrak{P}\}.$$

On peut alors montrer que le morphisme $\varphi_{\mathfrak{P}}$ est surjectif. Comme

$$|\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})| = [k_{\mathfrak{P}} : k_{\mathfrak{p}}] = f_{\mathfrak{p}},$$

on en déduit que $|I_{\mathfrak{P}}| = e_{\mathfrak{p}}$. Autrement dit, $I_{\mathfrak{P}}$ mesure la ramification de $\mathfrak{p}$ dans L (le degré de ramification est le même pour tout premier au-dessus de $\mathfrak{p}$ dans $\mathcal{O}_L$).

Définition. On appelle **élément de Frobenius** associé à $\mathfrak{P}/\mathfrak{p}$ tout antécédent du morphisme de Frobenius, générateur de $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$. Un tel élément sera noté $\sigma_{\mathfrak{P}}$.

En général, $\sigma_{\mathfrak{P}}$ n'est bien défini que modulo $I_{\mathfrak{P}}$, mais en l'absence de ramification, c'est un élément de G vérifiant

$$\forall x \in \mathcal{O}_L, \sigma_{\mathfrak{P}}(x) = x^{|k_{\mathfrak{p}}|} \bmod \mathfrak{P}.$$

Ce sont ces éléments de Frobenius qui vont nous intéresser pour le théorème de Chebotarev

En utilisant de nouveau le fait qu'il n'y a qu'une seule orbite pour l'action de G sur les $\mathfrak{P} \mid \mathfrak{p}$, on trouve que les différents $D_{\mathfrak{P}}$, qui sont les stabilisateurs pour cette action, sont conjugués entre eux. On en déduit facilement que si $\mathfrak{p}$ est non ramifié dans L, les $\sigma_{\mathfrak{P}}$ pour $\mathfrak{P} \mid \mathfrak{p}$ forment une classe de conjugaison de G. On

notera cette classe de conjugaison $\sigma_{\mathfrak{p}}$. Si $\mathfrak{p}$ est ramifié dans L, les groupes d'inertie sont également conjugués entre eux, de sorte que $\sigma_{\mathfrak{p}} = \{\sigma_{\mathfrak{P}} I_{\mathfrak{P}}, \mathfrak{P} \mid \mathfrak{p}\}$ est également une classe de conjugaison de $D_{\mathfrak{P}}/I_{Pp}$.

Récapitulons quelques-unes des propriétés élémentaires de nos éléments de Frobenius :

À chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans L, on associe une classe de conjugaison $\sigma_{\mathfrak{p}}$ dont chaque élément σ est d'ordre $f_{\mathfrak{p}}$ et vérifie

$$\forall x \in \mathcal{O}_L, \sigma(x) = x^{|k_{\mathfrak{p}}|} \bmod \mathfrak{P}$$

pour un certain $\mathfrak{P} \mid \mathfrak{p}$.

Nous sommes désormais en mesure d'énoncer le théorème de Chebotarev :

Théorème (Chebotarev, 1922)**.** *Soit C une classe de conjugaison de G. Notons $\mathcal{P}$ l'ensemble des idéaux premiers de K non ramifiés dans L. Alors*

$$\lim_{x \to +\infty} \frac{|\{\mathfrak{p} \in \mathcal{P}, N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \sigma_{\mathfrak{p}} = C\}|}{|\{\mathfrak{p} \lhd \mathcal{O}_K, N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}|} = \frac{|C|}{|G|}.$$

Ce théorème énonce que les éléments de Frobenius associés aux idéaux premiers non ramifiés de $\mathcal{O}_K$ se répartissent bien dans les différentes classes de conjugaison de G.

Remarques.

i) On aurait pu énoncer le même résultat pour la limite du quotient

$$\frac{|\{\mathfrak{p} \in \mathcal{P}, N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \sigma_{\mathfrak{p}} = C\}|}{|\{\mathfrak{p} \lhd \mathcal{O}_K \text{ non ramifié}, N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}|}$$

car il n'y a qu'un nombre fini de premiers de K ramifiés dans L.

ii) Chebotarev n'a pas réellement démontré son théorème sous cette forme. Nous avons donné le résultat sous la forme d'une densité asymptotique, alors que Chebotarev avait démontré le résultat plus faible suivant :

$$\lim_{s \to 1} \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \text{non ramifié} \\ \sigma_{\mathfrak{p}} = C}} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})^s} = \frac{|C|}{|G|} \log\left(\frac{1}{s-1}\right) + O(1),$$

résultat sous une forme de densité de Dirichlet [9]. La version donnée ici est due à Artin.

9. Johann Peter Gustav Lejeune Dirichlet (1805-1859)

iii) Par le théorème des idéaux premiers, on a

$$|\{\mathfrak{p} \lhd \mathcal{O}_K, N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}| \underset{x\to+\infty}{\sim} \mathrm{Li}(x),$$

où Li est la fonction logarithme intégral :

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)} \underset{x\to+\infty}{\sim} \frac{x}{\log(x)}.$$

Ainsi, on peut reformuler le théorème de Chebotarev sous la forme

$$|\{\mathfrak{p} \in \mathcal{P}, N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \sigma_\mathfrak{p} = C\}| \underset{x\to+\infty}{\sim} \frac{|C|}{|G|}\mathrm{Li}(x).$$

Voyons désormais en quoi le théorème de Chebotarev est une généralisation des théorèmes des nombres premiers et des nombres premiers en progressions arithmétiques.

Prenons $K = L = \mathbb{Q}$. Alors les idéaux premiers de K correspondent aux nombres premiers, et le groupe de Galois sous-jacent est trivial. Par la dernière formulation, on trouve

$$|\{p \leq x\}| \underset{x\to+\infty}{\sim} \mathrm{Li}(x),$$

ce qui est exactement le théorème des nombres premiers.

Prenons maintenant $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta_m)$ où $m \geq 3$ est un entier et ζ_m est une racine primitive m-ième de l'unité. Rappelons que le groupe de Galois $\mathrm{Gal}(L/K)$ est alors constitué des automorphismes $\sigma_a : \zeta_m \mapsto \zeta_m^a$, où $a \in \mathbb{Z}$ est premier avec m. Cela définit bien un unique automorphisme de corps de $\mathbb{Q}(\zeta_m)$ car $(1, \zeta_m, \ldots, \zeta_m^{\varphi(m)})$ en est une $\mathbb{Q}$-base. On remarque que σ_a ne dépend que de la classe de a modulo m, et on obtient que $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. Ce groupe de Galois étant abélien, les classes de conjugaison sont réduites à des singletons, et les éléments de Frobenius sont des éléments de ce groupe. On vérifie alors facilement que l'élément de Frobenius associé à un nombre premier p est exactement l'automorphisme σ_a, où $p = a \bmod m$. Le théorème de Chebotarev nous donne alors

$$|\{p \leq x, p = a \bmod m\}| \underset{x\to+\infty}{\sim} \frac{1}{\varphi(m)}\mathrm{Li}(x),$$

ce qui constitue exactement la version forte du théorème des nombres premiers en progressions arithmétiques.

Signalons pour l'exemple l'application suivante : si D est un entier sans facteur carré, la densité des nombres premiers p tels que $\left(\frac{D}{p}\right) = 1$ est $\frac{1}{2}$, où $\left(\frac{\cdot}{p}\right)$ est le

symbole de Legendre modulo p. En effet, l'extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ est galoisienne de degré 2, et les nombres premiers p tels que $\left(\frac{D}{p}\right) = 1$ sont les nombres premiers p non ramifiés dans $\mathbb{Q}(\sqrt{D})$ tels que $D^{\frac{p-1}{2}} = 1 \bmod p$, c'est-à-dire ceux tels que $(\sqrt{D})^{|\mathbb{F}_p|} = \sqrt{D} \bmod p\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, c'est-à-dire ceux dont l'élément de Frobenius associé est trivial.

Finalement, pour justifier l'intérêt du théorème de Chebotarev dans l'étude de l'arithmétique des corps de nombres, signalons le théorème de Bauer [10] qui en est une conséquence :

Théorème (Bauer, 1903)**.** *Soit L/K une extension galoisienne de corps de nombres, et M/K une extension finie. Notons $P(L/K)$ l'ensemble des idéaux premiers $\mathfrak{p}$ de K admettant un diviseur premier $\mathfrak{P}$ dans L avec $f(\mathfrak{P}/\mathfrak{p}) = 1$, et $P(M/K)$ de manière similaire. Alors $P(M/K)$ est inclus, à un nombre fini d'exceptions près, dans $P(L/K)$ si et seulement si $L \subset M$.*

2) Représentations linéaires des groupes finis

Pour prouver le théorème de Chebotarev, nous aurons besoin de travailler avec des fonctions L d'Artin, qui sont définies grâce à des représentations linéaires de groupes de Galois. Les propriétés de ces fonctions découlent de quelques résultats célèbres sur les représentations linéaires des groupes finis, que nous allons présenter ici sans preuve. On pourra se référer à l'excellent livre de Serre [10] sur les représentations pour les démonstrations.

Dans toute cette partie, G désigne un groupe fini de neutre e.

Définition. Une **représentation linéaire** de G, ou **représentation**, est un morphisme $\rho : G \to GL(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie. Autrement dit, une représentation de G est une action linéaire sur un $\mathbb{C}$-espace vectoriel de dimension finie. On parlera parfois de (ρ, V) pour parler de la représentation associée. La dimension de V est appelée **rang** ou **degré** de ρ. On la notera $\deg(\rho)$.

Le **caractère** de ρ est l'application

$$\chi : \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \mathrm{tr}(\rho(g)) \end{array}.$$

Exemples.

10. Mihály Bauer (1874-1945)

i) La représentation triviale, ou représentation unité, est la représentation

$$\begin{array}{rccc} & G & \longrightarrow & \mathbb{C}^* \\ \mathbf{1}: & g & \longmapsto & 1 \end{array}.$$

Elle est de degré 1. Son caractère est souvent noté χ_0.

ii) Tout caractère de G, c'est-à-dire tout morphisme de groupes de G dans $\mathbb{C}^*$ correspond à une représentation de degré 1, et réciproquement. Elle est égale à son caractère. Ainsi la signature fournit une représentation du groupe $\mathfrak{S}_n$, ou encore le symbole de Jacobi fournit une représentation du groupe $\mathbb{F}_p^*$ pour tout nombre premier p.

iii) Soit X un ensemble fini sur lequel G agit, et V un $\mathbb{C}$-espace vectoriel dont une base est indexée par X. La représentation par permutations ρ associée à cette action est donnée par $\rho(g).e_x = e_{g.x}$ pour tout $g \in G$ et $x \in X$.

iv) La représentation régulière de G est la représentation par permutations associée à l'action de G sur lui-même par translation à gauche. Elle est de degré $|G|$ et de caractère $|G|\mathbf{1}_{\{e\}}$, où $\mathbf{1}_{\{e\}}$ désigne la fonction indicatrice de $\{e\}$.

v) L'application $\rho : D_n \to GL_2(\mathbb{C})$ définie par

$$\rho(r^k) = \begin{pmatrix} \mathrm{e}^{\frac{2i\pi k}{n}} & 0 \\ 0 & \mathrm{e}^{-\frac{2i\pi k}{n}} \end{pmatrix}$$

pour $0 \leq k \leq n-1$ et

$$\rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

étendue en un morphisme de groupes est une représentation de degré 2 du groupe diédral D_n.

L'ensemble des caractères de G est muni de quelques opérations utiles, que l'on résume ici pour référence :

a) Si χ_1 et χ_2 sont des caractères de G, associés aux représentations ρ_1 et ρ_2, alors $\chi_1 + \chi_2$ et $\chi_1\chi_2$ sont respectivement les caractères de la représentation somme directe $\rho_1 \oplus \rho_2$ et de la représentation tensorielle $\rho_1 \otimes \rho_2$ définies de manière évidente.

b) Si χ est un caractère de G, associé à la représentation (ρ, V), alors $\overline{\chi}$ est le caractère de la représentation duale de ρ, définie sur V^* par

$$f \mapsto (u \mapsto f(\rho(g^{-1})u).$$

Définition. On dit que deux représentations (ρ_1, V_1) et (ρ_2, V_2) de G sont **isomorphes** lorsqu'il existe un isomorphisme linéaire f entre V_1 et V_2 qui soit G-équivariant, c'est-à-dire tel que pour tout $g \in G, v \in V$,

$$f(\rho_1(g).v) = \rho_2(g).f(v).$$

Il est clair que les degrés de deux représentations isomorphes sont égaux, et, par la propriété d'invariance de la trace par changement de base, les caractères de deux telles représentations sont aussi égaux.

Définition. Une représentation (ρ, V) de G est dite **irréductible** si les seuls sous-espaces vectoriels de V qui sont stables pour l'action de G sont $\{0\}$ et V. Le caractère d'une telle représentation est appelé **caractère irréductible** de G. L'ensemble des caractères irréductibles de G est noté $\hat{G}$.

Un phénomène propre à la caractéristique zéro est le suivant :

Théorème (Maschke[11], 1898)**.** *Toute représentation de G est semi-simple, c'est-à-dire qu'elle peut s'écrire comme somme directe de représentations irréductibles.*

De plus, cette décomposition est essentiellement unique, en regroupant les représentations irréductibles qui sont isomorphes entre elles. C'est une méthode très utile pour étudier les représentations d'un groupe fini.

Exemple. Notons reg_G la représentation régulière de G. Alors son caractère χ vérifie

$$\chi = \sum_{\chi \in \hat{G}} \chi(e)\chi.$$

Les caractères sont des fonctions centrales sur G, c'est-à-dire qu'ils vérifient $\chi(ghg^{-1}) = \chi(h)$ pour tout $g, h \in G$. L'un des intérêts des caractères irréductibles est le suivant :

Proposition. *Les caractères irréductibles de G forment une base de l'espace des fonctions centrales de G. De plus, cette base est orthonormée pour le produit scalaire*

$$\langle \chi, \psi \rangle \mapsto \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}.$$

On en déduit :

11. Heinrich Maschke (1853-1908)

Corollaire. *Deux représentations de G ayant le même caractère sont isomorphes.*

Ainsi, comme leur nom l'indique, les caractères caractérisent leurs représentations. On pourra donc parler indifféremment d'un caractère ou d'une représentation dans la suite.

Passons maintenant aux représentations associées à des sous-groupes de G. Soit H un tel sous-groupe. On a bien évidemment un opérateur de restriction, qui à toute représentation de G associe une représentation de H. Mais l'on peut également construire des représentations du quotient G/H si H est distingué dans G.

Définition. Supposons que H est distingué dans G et soit (ρ, V) une représentation de G. La **représentation quotient** associée à ρ est la représentation du groupe G/H donnée par l'action de ρ sur V^H, le sous-espace des éléments de V invariants par H. Son caractère sera noté $\chi^\sharp$.

On vérifie facilement que pour tout $g \in G$,

$$\chi^\sharp(gH) = \frac{1}{|H|} \sum_{g' \in gH} \chi(g').$$

Une dernière construction bien plus utile va nous permettre de procéder en sens inverse : à partir d'une représentation de H, on va pouvoir construire une représentation de G.

Définition. Soit (ρ, W) une représentation de H. On construit la **représentation induite** de ρ à G, notée $\mathrm{Ind}_H^G \rho$, de la manière suivante :

Soit $(\sigma_i)_i$ un système fixé de représentants de G/H. On pose $V = \oplus_i W_i$, où pour tout i, $W_i = W$. Si $v \in W_i$, on définit, pour tout $h \in H$ et tout j, $(\sigma_j h).v = f_{i,j}(\rho(h).v)$, où $f_{i,j} : W_i \to W_k$ est l'isomorphisme correspondant à l'identité, avec k tel que $\sigma_j \sigma_i H = \sigma_k H$. Cette action, étendue par linéarité à V tout entier correspond à $\mathrm{Ind}_H^G \rho$.

De manière plus visuelle, la représentation induite est construire « par blocs ». On écrit tout élément de G sous la forme $\sigma_i h$ avec $h \in H$, on fait agir h localement sur l'espace W, puis on envoie les blocs W indexés par G/H les uns sur les autres, cette dernière étape étant déterminée par la structure du quotient G/H.

Remarques.

i) La représentation ainsi construite ne dépend pas, à isomorphisme près, du système de représentants de G/H choisi.

ii) De manière plus abstraite, on peut définir V par $\mathbb{C}[G] \otimes W$, où $\mathbb{C}[G]$ est l'algèbre du groupe G, c'est-à-dire l'ensemble des combinaisons linéaires formelles à coefficients dans $\mathbb{C}$ d'éléments de G, muni des opérations usuelles.

Exemple. Soit $\mathbf{1}$ le caractère unité du sous-groupe $\{e\}$ de G. Alors $\mathrm{Ind}_H^G \mathbf{1} = \mathrm{reg}_G$. En effet, l'espace W est ici une droite vectorielle, et le quotient $G/\{e\}$ s'identifie à G.

Proposition. *Soit ρ une représentation de H de caractère χ. Le caractère de $Ind_H^G \rho$ est*

$$Ind_H^G \chi : g \mapsto \frac{1}{|H|} \sum_{s \in G} \dot{\chi}(s^{-1} g s),$$

où $\dot{\chi}$ est le prolongement par zéro de χ à G tout entier.

Terminons cette partie par un théorème de Brauer [12] qui nous sera très utile pour obtenir des informations sur les fonctions L d'Artin en général.

Théorème (Brauer, 1946)**.** *Tout caractère de G est combinaison linéaire à coefficients entiers de caractères induits de caractères de degré* 1.

Remarques.

i) Ce théorème améliore d'une certaine manière un résultat précédent d'Artin, énonçant le fait que tout caractère de G est combinaison linéaire à coefficients rationnels de caractères induits de sous-groupes cycliques. Nous verrons dans la prochaine partie en quoi le théorème de Brauer est meilleur.

ii) Le théorème de Brauer est en fait légèrement plus précis. Les caractères de degré 1 en question sont des caractères de groupes dits élémentaires, c'est-à-dire produits directs d'un p-groupe et d'un groupe cyclique d'ordre premier à p, avec p un nombre premier.

3) Fonctions L d'Artin

Nous allons maintenant nous intéresser à la généralisation de la fonction ζ de Riemann qui nous permettra de démontrer le théorème de Chebotarev. Pour les preuves des énoncés, nous renvoyons à l'article de Snyder [12].

Fixons une extension galoisienne de corps de nombres L/K, de groupe de Galois G.

12. Richard Brauer (1901-1977)

Définition. Soit ρ une représentation de G, de caractère χ. Pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ et $s \in \mathbb{C}$, on définit le **facteur local d'Artin** en $\mathfrak{p}$ de la manière suivante :

— Si $\mathfrak{p}$ est non ramifié dans L, on pose

$$L_{\mathfrak{p}}(s, \chi, L/K) = \det(id - \rho(\sigma_{\mathfrak{p}})N(\mathfrak{p})^{-s})^{-1}.$$

— Si $\mathfrak{p}$ est ramifié dans L, on pose

$$L_{\mathfrak{p}}(s, \chi, L/K) = \det(id - \rho(\sigma_{\mathfrak{p}})N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{p}}})^{-1}$$

où $I_{\mathfrak{p}}$ désigne le groupe d'inertie de l'un des premiers de L au-dessus de $\mathfrak{p}$ et $V^{I_{\mathfrak{p}}}$ est le sous-espace de V constitué des éléments invariants par $I_{\mathfrak{p}}$.

Remarques.

i) Cette définition ne dépend pas du choix de l'élément de Frobenius associé à $\mathfrak{p}$ dans G car le déterminant, et donc le polynôme caractéristique, est invariant par conjugaison.

ii) De même la définition dans le cas ramifié a bien un sens en choisissant le même premier de L au-dessus de $\mathfrak{p}$ pour l'élément de Frobenius et pour le groupe d'inertie.

iii) Comme χ détermine ρ à conjugaison près, il n'y a pas d'ambigüité en notant ceci comme une fonction de χ.

Définition. Soit χ un caractère de G. La **fonction L d'Artin** associée à ce caractère est définie par

$$L(s, \chi, L/K) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \chi, L/K)$$

avec $s \in \mathbb{C}$.

Proposition. *Soit χ un caractère de G. Alors $s \mapsto L(s, \chi, L/K)$ est définie et holomorphe sur le demi-plan $\Omega = \{s \in \mathbb{C}, \mathfrak{Re}(s) > 1\}$.*

Démonstration. En effet, notons ρ la représentation associée à χ. Soient $n = \deg(\chi)$ et $\lambda_1, \ldots, \lambda_n$ les valeurs propres de $\rho(\sigma_{\mathfrak{p}})$. Alors pour tout idéal premier $\mathfrak{p}$ de K et pour tout $s \in \mathbb{C}$,

$$|\det(id - \rho(\sigma_{\mathfrak{p}})N(\mathfrak{p})^{-s})^{-1}| = \prod_{i=1}^{n} |1 - \lambda_i N(\mathfrak{p})^{-s}| \geq \prod_{i=1}^{n} (1 - N(\mathfrak{p})^{-\mathfrak{Re}(s)}),$$

car les λ_i sont d'ordre fini donc sont des racines de l'unité dans $\mathbb{C}$ et $|N(\mathfrak{p})^{-s}| = N(\mathfrak{p})^{-\mathfrak{Re}(s)}$. La convergence uniforme sur tout compact de Ω de la série de fonctions

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^{-s}}$$

donne le résultat. □

Exemples.

i) On a pour tout corps de nombres K et tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$,

$$L(s, \chi_0, K/K) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} = \zeta_K(s).$$

ii) On considère $L = \mathbb{Q}(\zeta_m)$ et $K = \mathbb{Q}$. Alors les caractères irréductibles du groupe de Galois $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ sont les caractères de Dirichlet modulo m et l'on a vu précédemment que l'élément de Frobenius correspondant au nombre premier $p = a \bmod m$ est $\zeta_m \mapsto \zeta_m^a$. Les premiers ramifiés étant exactement ceux divisant m, on obtient pour $\mathfrak{Re}(s) > 1$,

$$L(s, \chi, L/K) = \prod_{p \nmid m} (1 - \chi(p)p^{-s})^{-1} \times P = L(s, \chi) \times P,$$

où $L(., \chi)$ désigne la série L de Dirichlet traditionnelle, et P désigne le produit d'un nombre fini de facteurs locaux.

Plus généralement, si L/K est abélienne, la théorie du corps de classes, et plus précisément la loi de réciprocité d'Artin, permet d'identifier les caractères du groupe $\mathrm{Gal}(L/K)$ avec les caractères du groupe des classes généralisées $I_K(\mathfrak{f})/H_\mathfrak{f}$ associé au conducteur $\mathfrak{f}$ de l'extension L/K. Dans ce cadre, nos fonctions L d'Artin ne sont rien d'autre que des fonctions L de Hecke[13] associées à ces caractères. Or Hecke avait montré que ces fonctions L admettent un prolongement méromorphe à $\mathbb{C}$ avec pour unique pôle 1 si le caractère en question est trivial, et qu'elles vérifiait une équation fonctionnelle similaire à celle vérifiée par la fonction zêta de Riemann. Nous verrons plus loin comment ces résultats sont utilisés pour montrer des propriétés similaires pour les fonctions L d'Artin.

La proposition suivante résume les propriétés fondamentales des fonctions L d'Artin vis-à-vis des caractères. Elle se démontre en considérant chaque facteur local séparément.

Proposition. *Les fonctions L d'Artin vérifient les propriétés suivantes :*

i) Additivité : Si χ_1 et χ_2 sont des caractères de G alors pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$, $L(s, \chi_1 + \chi_2, L/K) = L(s, \chi_1, L/K)L(s, \chi_2, L/K)$.

ii) Inflation : Si H est un sous-groupe distingué, et χ est un caractère de G/H, alors pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$, $L(s, \chi, L^H/K) = L(s, \pi_H \circ \chi, L/K)$, où $\pi_H : G \twoheadrightarrow G/H$ est la projection dans le quotient.

13. Eric Hecke (1887-1947)

iii) Induction : Si $K \subset M \subset L$ avec $Gal(L/M) = H < G$ et χ est un caractère de H, on a pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$, $L(s, \chi, L/M) = L(s, Ind_H^G \chi, L/K)$.

C'est principalement la dernière propriété qui va nous intéresser. En effet, dans la preuve (inconditionnelle) du théorème de Chebotarev, on va vouloir se ramener au cas où le groupe de Galois est cyclique, ce que l'on pourra faire grâce à cette propriété d'induction.

Exemple. Pour $\mathfrak{Re}(s) > 1$, écrivons

$$\begin{aligned}
\zeta_L(s) &= L(s, \chi_0, L/L) \\
&= L(s, \mathrm{Ind}_{\{id_L\}}^G \chi_0, L/K) \\
&= L(s, \mathrm{reg}_G, L/K) \\
&= \prod_{\chi \in \hat{G}} L(s, \chi, L/K)^{\chi(1)} \\
&= \zeta_K(s) \prod_{\substack{\chi \in \hat{G} \\ \chi \neq \mathbf{1}}} L(s, \chi, L/K)^{\chi(1)}.
\end{aligned}$$

On voit ainsi apparaître un lien entre les fonctions zêta de Dedekind de nos deux corps de nombres. C'est en observant de tels liens entre des fonctions zêta de Dedekind qu'Artin en est venu à définir ses fonctions L.

Une autre conséquence de la propriété d'induction est la suivante :

Proposition. *Toute fonction L d'Artin admet un prolongement méromorphe à $\mathbb{C}$.*

Démonstration. Par le théorème de Brauer, on peut écrire tout caractère χ de G sous la forme

$$\chi = \sum_{i \in S} m_i \mathrm{Ind}_{H_i}^G \chi_i,$$

où $(H_i)_{i \in S}$ est une famille de sous-groupes élémentaires de G et les χ_i sont des caractères de degré 1. Ainsi, on a pour tout $s \in \mathbb{C}$ tel que $\mathfrak{Re}(s) > 1$,

$$L(s, \chi, L/K) = \prod_{i \in S} L(s, \chi_i, L/L^{H_i})^{m_i}.$$

Or les extensions L/L^{H_i} sont abéliennes. Les fonctions L apparaissant dans ce produit s'identifient donc à des fonctions L de Hecke, et admettent donc un prolongement méromorphe à $\mathbb{C}$. Les puissances étant des entiers relatifs, on obtient que notre fonction L est bien méromorphe sur $\mathbb{C}$. □

Remarque. Le théorème d'Artin cité en fin de partie précédente ne nous aurait pas permis d'obtenir un résultat aussi fort. En effet, on aurait eu des puissances rationnelles, ce qui ne préserve pas le caractère méromorphe des fonctions L de Hecke.

L'analogie avec les fonctions zêta de Dedekind va plus loin. Les fonctions L d'Artin vérifient une certaine équation fonctionnelle. Pour en parler, il faut compléter ces fonctions par un terme exponentiel.

Définition. On définit les fonctions $\Gamma_{\mathbb{R}}$ et $\Gamma_{\mathbb{C}}$ par

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)$$

et

$$\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s).$$

Si (χ, V) est un caractère de G, on définit le **facteur local** d'Artin associé à la valeur absolue archimédienne v de K par

$$L_v(s, \chi, L/K) = \begin{cases} \Gamma_{\mathbb{R}}(s)^{\dim V^{\mathcal{C}}}\Gamma_{\mathbb{R}}(s+1)^{\mathrm{codim} V^{\mathcal{C}}} \text{ si } v \text{ est réel} \\ \Gamma_{\mathbb{C}}(s)^{\chi(1)} \text{ si } v \text{ est complexe} \end{cases},$$

où $\mathcal{C}$ est le groupe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.
Enfin, on pose $A(\chi) = d_K^{\chi(1)} N_{K/\mathbb{Q}}(f_\chi)$, où d_K est le discriminant de K et f_χ est le **conducteur d'Artin** de χ (voir ci-dessous).

La **fonction L d'Artin complétée** est la fonction

$$\Lambda(s, \chi, L/K) = A(\chi)^{s/2} L(s, \chi, L/K) \prod_{v|\infty} L_v(s, \chi, L/K).$$

On ne donnera pas la définition précise du conducteur d'Artin d'un caractère de G, qui est relativement compliquée, et qui fait intervenir les sous-groupes de ramification supérieure de G. La seule propriété de ces conducteurs que nous utiliserons est la suivante.

Proposition (Relation conducteur-discriminant)**.** *On a la relation*

$$\prod_{\chi \in \hat{G}} A(\chi) = d_L,$$

où d_L désigne la discriminant de L.

Toutes ces définitions servent à donner une expression très simple de l'équation fonctionnelle satisfaite par nos fonctions L d'Artin. Les fonctions Λ jouent le rôle de la fonction Ξ pour la fonction ζ. L'équation fonctionnelle se démontre en se ramenant à des fonctions L de Hecke comme précédemment par le théorème de Brauer.

Théorème. *La fonction L d'Artin complétée associée au caractère χ de G vérifie*

$$\Lambda(s, \chi, L/K) = W(\chi)\Lambda(1 - s, \overline{\chi}, L/K)$$

pour tout $s \in \mathbb{C}$ où elle est définie, avec $W(\chi)$ est un nombre complexe de module 1.

4) Conjectures

La première conjecture qui aura une influence sur nos résultats est la suivante :

Conjecture (Artin)**.** *Soit L/K une extension galoisienne de corps de nombres et χ un caractère de Gal(L/K). Alors la fonction L d'Artin associée à χ est holomorphe sur $\mathbb{C} \setminus \{1\}$, et admet un pôle en* 1 *d'ordre la multiplicité du caractère unité dans χ.*

Cette conjecture nous permettra essentiellement d'éviter d'avoir à nous ramener au cas cyclique, ce qui fait nécessairement grossir les termes d'erreurs dans le théorème de Chebotarev. Dans la preuve inconditionnelle, nous aurons besoin de nous ramener à ce cas, pour lequel cette conjecture est un théorème grâce aux travaux de Hecke.

Remarque. De l'égalité

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

établie précédemment, on obtient, avec la conjecture d'Artin, que la fonction $\frac{\zeta_L}{\zeta_K}$ est une fonction entière, énoncé connu sous le nom de conjecture de Dedekind. On peut même voir que la conjecture d'Artin entraîne la conjecture de Dedekind dans le cas non galoisien en se ramenant à la clôture galoisienne de L/K. La conjecture de Dedekind a été démontrée dans le cas où L/K est galoisienne (théorème d'Aramata-Brauer) et dans le cas où $\tilde{L}/K$ est résoluble (théorème d'Uchida-Van Der Waall), où $\tilde{L}/K$ est la clôture galoisienne de L/K.

La seconde conjecture dont nous nous servirons est la généralisation de la fameuse hypothèse de Riemann :

Conjecture (Hypothèse de Riemann généralisée)**.** *Soit L/K une extension galoisienne de corps de nombres et χ un caractère de $Gal(L/K)$. Alors pour $0 \leq \mathfrak{Re}(s) \leq 1$, $L(s, \chi, L/K) = 0 \Rightarrow \mathfrak{Re}(s) = \frac{1}{2}$ et s est un zéro simple de cette fonction.*

L'utilisation de cette conjecture aura une énorme incidence sur le terme d'erreur du théorème de Chebotarev. Comme dans le cas usuel du théorème des nombres premiers, celle-ci fournit un terme d'erreur en x de l'ordre de $x^{1/2+\varepsilon}$ pour tout $\varepsilon > 0$.

II Versions effectives du théorème de Chebotarev (d'après Lagarias-Odlyzko-Serre)

La démonstration du théorème de Chebotarev que nous allons voir est tirée de l'article *Effective versions of the Chebotarev density theorem* [4] de Lagarias et Odlyzko, avec quelques améliorations de Serre [9].

1) Mise en place

Avant de débuter la preuve du théorème de Chebotarev, fixons tout d'abord quelques notations.

On s'intéresse ici à une extension finie galoisienne L/K de corps de nombres, de groupe de Galois G. On notera $n_K = [K : \mathbb{Q}]$, $n_L = [L : \mathbb{Q}]$ et $n_E = [E : \mathbb{Q}]$ pour toute extension intermédiaire $L/E/K$. De même, d_K, d_E et d_L désigneront respectivement les discriminants de K, E et L. Précisons que les dépendances des O et $\ll$ sera également en fonction de ces invariants. Ainsi nous obtiendrons un terme d'erreur plus précis qu'un simple équivalent, et nous verrons la dépendance de ces termes d'erreur en fonction des corps de nombres K et L.

Dans toute la suite, nous noterons N au lieu de $N_{K/\mathbb{Q}}$, la lettre $\mathfrak{p}$ désignera toujours un idéal premier de $\mathcal{O}_K$, et l'abréviation « n.r. » désignera « non ramifié dans L ». Si C est une classe de conjugaison de G, on pose

$$\pi_C(x) = \sum_{\substack{\mathfrak{p} \text{ n.r.} \\ \sigma_\mathfrak{p}=C \\ N(\mathfrak{p})\leq x}} 1$$

et

$$\psi_C(x) = \sum_{\substack{\mathfrak{p} \text{ n.r.}, m \\ \sigma_{\mathfrak{p}}=C \\ N(\mathfrak{p}^m)\leq x}} \log(N(\mathfrak{p})),$$

les généralisations naturelles des fonctions de compte des nombres premiers π et ψ.

L'idée de la démonstration est très proche de celle de De La Vallée-Poussin pour démontrer le théorème des nombres premiers. On écrit $\psi_C(x)$ sous la forme d'une intégrale sur un segment vertical d'une certaine fonction holomorphe F_C qui est une combinaison linéaire de dérivées logarithmiques de fonctions L d'Artin, plus un terme d'erreur R_1, que l'on estime facilement. On déplace ensuite le contour d'intégration vers la gauche, faisant apparaître un autre terme d'erreur R_2, de sorte que la nouvelle intégrale soit calculable en fonction des résidus de F_C. Une difficulté apparaît car on ne sait pas dire en général quels sont les pôles des fonctions L apparaissant dans F_C. Pour remédier à cela, on se ramène au cas abélien, et donc au cas de fonctions L de Hecke grâce aux propriétés d'induction des fonctions L d'Artin.

Le but est de donner une estimation relativement fine de $\psi_C(x)$ pour x grand, où la dépendance en les corps K et L apparaît clairement, puis d'en déduire le même genre d'estimation pour $\pi_C(x)$ par sommation par parties. Nous verrons en fin de partie comment on peut améliorer nos résultats si on suppose l'hypothèse de Riemann généralisée ou la conjecture d'Artin.

Définition. Pour χ caractère de G, $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, $\mathfrak{P} \mid \mathfrak{p}$ dans L et $m \in \mathbb{N}^*$, on pose

$$\chi_K(\mathfrak{p}^m) = \frac{1}{e_{\mathfrak{p}}} \sum_{\alpha \in I_{\mathfrak{P}}} \chi(\sigma_{\mathfrak{P}}^m \alpha).$$

Remarques.

i) Cette définition ne dépend pas du premier $\mathfrak{P}$ choisi au-dessus de $\mathfrak{p}$ car χ est une fonction centrale.

ii) Si $\mathfrak{p}$ est non ramifié dans L, on a $\chi_K(\mathfrak{p}^m) = \chi(\sigma_{\mathfrak{p}}^m)$, alors que si $\mathfrak{p}$ est ramifié dans L, $\chi_K(\mathfrak{p}^m) = \chi^\sharp(\sigma_{\mathfrak{P}}^m)$ selon les définitions de $I.2$).

Procédons maintenant à quelques réécritures. Tout d'abord, pour $\mathfrak{Re}(s) > 1$ et $\chi \in \hat{G}$, on a

$$-\frac{L'}{L}(s, \chi, L/K) = \sum_{\mathfrak{p}} \sum_{m=1}^{+\infty} \chi_K(\mathfrak{p}^m) \log(N(\mathfrak{p})) N(\mathfrak{p})^{-ms},$$

d'où en fixant $g \in C$ quelconque,

$$-\frac{|C|}{|G|}\sum_{\chi\in\hat{G}}\overline{\chi(g)}\frac{L'}{L}(s,\chi,L/K)=\frac{|C|}{|G|}\sum_{\mathfrak{p}}\sum_{m=1}^{+\infty}\left(\sum_{\chi\in\hat{G}}\overline{\chi(g)}\chi_K(\mathfrak{p}^m)\right)\log(N(\mathfrak{p}))N(\mathfrak{p})^{-ms}.$$

Par les relations d'orthogonalité, on obtient que si $\mathfrak{p}$ est non ramifié dans L,

$$\frac{|C|}{|G|}\sum_{\chi\in\hat{G}}\overline{\chi(g)}\chi_K(\mathfrak{p}^m)=\frac{|C|}{|G|}\sum_{\chi\in\hat{G}}\overline{\chi(g)}\chi(\sigma_{\mathfrak{p}}^m)=\begin{cases}1 \text{ si } \sigma_{\mathfrak{p}}^m\in C\\ 0 \text{ sinon}\end{cases},$$

tandis que pour $\mathfrak{p}$ ramifié, on a

$$\frac{|C|}{|G|}\sum_{\chi\in\hat{G}}\overline{\chi(g)}\chi_K(\mathfrak{p}^m)=\frac{1}{e_{\mathfrak{p}}}\sum_{\alpha\in I_{\mathfrak{P}}}\frac{|C|}{|G|}\sum_{\chi\in\hat{G}}\overline{\chi(g)}\chi(\sigma_{\mathfrak{P}}^m\alpha)$$

qui, pour les mêmes raisons d'orthogonalité et le fait que $|I_{\mathfrak{P}}|=e_{\mathfrak{p}}$, est borné en module par 1.

Posant

$$F_C(s)=-\frac{|C|}{|G|}\sum_{\chi\in\hat{G}}\overline{\chi(g)}\frac{L'}{L}(s,\chi,L/K)$$

et

$$\theta(\mathfrak{p}^m)=\frac{|C|}{|G|}\sum_{\chi\in\hat{G}}\overline{\chi(g)}\chi_K(\mathfrak{p}^m),$$

on obtient

$$F_C(s)=\sum_{\mathfrak{p}}\sum_{m=1}^{+\infty}\theta(\mathfrak{p}^m)\log(N(\mathfrak{p}))N(\mathfrak{p})^{-ms}$$

pour $\mathfrak{Re}(s)>1$.

La série de Dirichlet F_C a pour abscisse de convergence absolue $\sigma_a \leq 1$, on peut donc lui appliquer la formule de Perron avec terme d'erreur (voir [13] ou [2] par exemple). Ainsi, posant pour $\sigma_0, T > 1$ et $x \geq 2$,

$$I_C(x,T)=\frac{1}{2i\pi}\int_{\sigma_0+iT}^{\sigma_0+iT}F_C(s)\frac{x^s}{s}ds$$

et

$$R_0(x,T)=\sum_{\substack{\mathfrak{p},m\\ N(\mathfrak{p}^m)\neq x}}\left(\frac{x}{N(\mathfrak{p}^m)}\right)^{\sigma_0}\min\left(1,T^{-1}\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right|^{-1}\right)\log(N(\mathfrak{p})),$$

on obtient

$$\left| I_C(x,T) - \sum_{\substack{\mathfrak{p},m \\ N(\mathfrak{p}^m)\leq x}} \theta(\mathfrak{p}^m)\log(N(\mathfrak{p})) \right| \leq \sum_{\substack{\mathfrak{p},m \\ N(\mathfrak{p}^m)=x}} \left(\log(N(\mathfrak{p}))\sigma_0 T^{-1}\right) + R_0(x,T).$$

De plus, comme $\theta(\mathfrak{p}^m) = 1$ si $\mathfrak{p}$ est non ramifié dans L, on a aussi

$$\begin{aligned}\left| \psi_C(x) - \sum_{\substack{\mathfrak{p},m \\ N(\mathfrak{p}^m)\leq x}} \theta(\mathfrak{p}^m)\log(N(\mathfrak{p})) \right| &= \left| \sum_{\substack{\mathfrak{p} \text{ ramifié},m \\ N(\mathfrak{p}^m)\leq x}} \theta(\mathfrak{p}^m)\log(N(\mathfrak{p})) \right| \\ &\leq \sum_{\substack{\mathfrak{p} \text{ ramifié},m \\ N(\mathfrak{p}^m)\leq x}} \log(N(\mathfrak{p})) \\ &= \sum_{\mathfrak{p} \text{ ramifié}} \log(N(\mathfrak{p}))\left|\{m, N(\mathfrak{p}^m)\leq x\}\right|.\end{aligned}$$

Or $N(\mathfrak{p}^m) \leq x$ si et seulement si $m \leq \frac{\log x}{\log(N(\mathfrak{p}))}$, il y a donc au plus $\frac{\log x}{2}$ tels entiers m. On obtient donc

$$\begin{aligned}\left| \psi_C(x) - \sum_{\substack{\mathfrak{p},m \\ N(\mathfrak{p}^m)\leq x}} \theta(\mathfrak{p}^m)\log(N(\mathfrak{p})) \right| &\leq \frac{\log x}{2} \sum_{\mathfrak{p} \text{ ramifié}} \log(N(\mathfrak{p})) \\ &\leq \frac{\log x \log d_L}{2}\end{aligned}$$

car les premiers ramifiés de K divisent tous le discriminant de L.

De plus,

$$\sum_{\substack{\mathfrak{p},m \\ N(\mathfrak{p}^m)=x}} \log(N(\mathfrak{p})) \leq n_K \log x$$

car $N(\mathfrak{p}^m) = x$ ne peut se produire que si x est une puissance d'un nombre premier p tel que $\mathfrak{p} \mid p$. Pour un tel $\mathfrak{p}$, il ne peut y avoir qu'au plus un seul m tel que $N(\mathfrak{p}^m) = x$. Comme il y a au plus n_K premiers $\mathfrak{p}$ tels que $\mathfrak{p} \mid p$ (le cas d'égalité étant celui où p est totalement ramifié dans K), on trouve bien la majoration ci-dessus.

Rassemblant ces premières majorations, on trouve

$$\psi_C(x) = I_C(x,T) + R_1(x,T)$$

où

$$|R_1(x,T)| \leq \frac{\log x \log d_L}{2} + n_K \log x \sigma_0 T^{-1} + R_0(x,T).$$

À ce stade, on choisit $\sigma_0 = 1 + \frac{1}{\log(x)}$, de sorte que $x^{\sigma_0} = \mathrm{e}x$.

Pour estimer R_0, on le découpe en trois sommes

$$S_1 = \sum_{\substack{\mathfrak{p},m \\ N(\mathfrak{p}^m) \leq \frac{3}{4}x \text{ ou } N(\mathfrak{p}^m) \geq \frac{5}{4}x}} \left(\frac{x}{N(\mathfrak{p}^m)}\right)^{\sigma_0} \min\left(1, T^{-1}\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right|^{-1}\right) \log(N(\mathfrak{p})),$$

$$S_2 = \sum_{\substack{\mathfrak{p},m \\ 0 < |N(\mathfrak{p}^m) - x| \leq 1}} \left(\frac{x}{N(\mathfrak{p}^m)}\right)^{\sigma_0} \min\left(1, T^{-1}\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right|^{-1}\right) \log(N(\mathfrak{p}))$$

et

$$S_3 = R_0(x,T) - S_1 - S_2.$$

- **Majoration de S_1 :** Si $N(\mathfrak{p}^m) \leq \frac{3}{4}x$ ou $N(\mathfrak{p}^m) \geq \frac{5}{4}x$ alors

$$\begin{aligned}\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right| &\geq \log\left(\min\left(\frac{4}{3}, \frac{5}{4}\right)\right) \\ &= \log\left(\frac{5}{4}\right)\end{aligned}$$

de sorte que

$$\min\left(1, T^{-1}\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right|^{-1}\right) \leq \frac{1}{T\log\left(\frac{5}{4}\right)}$$

et donc

$$S_1 \leq \frac{\mathrm{e}x}{T\log\left(\frac{5}{4}\right)} \sum_{\mathfrak{p},m} \frac{\log(N(\mathfrak{p}))}{N(\mathfrak{p})^{m\sigma_0}} = \frac{\mathrm{e}x}{T\log\left(\frac{5}{4}\right)} \left(-\frac{\zeta_K'}{\zeta_K}(\sigma_0)\right).$$

Or, en réécrivant

$$-\frac{\zeta_K'}{\zeta_K}(\sigma_0) = \sum_{\mathfrak{p}} \frac{\log(N(\mathfrak{p}))}{N(\mathfrak{p})^{\sigma_0} - 1}$$

on peut faire le raisonnement suivant : si $N(\mathfrak{p}) = p^k$ pour un certain p premier et $k \geq 1$, alors

$$\begin{aligned}\frac{\log(N(\mathfrak{p}))}{N(\mathfrak{p})^{\sigma_0}-1} &= \frac{k\log p}{p^{k\sigma_0}-1}\\ &= \frac{k}{p^{(k-1)\sigma_0}+\cdots+1}\frac{\log p}{p^{\sigma_0}-1}\\ &\leq \frac{\log p}{p^{\sigma_0}-1}.\end{aligned}$$

Comme précédemment, pour chaque p premier, il y a au plus n_K premiers $\mathfrak{p} \mid p$ dans K. On en déduit donc que

$$-\frac{\zeta_K'}{\zeta_K}(\sigma_0) \leq n_K \sum_p \frac{\log p}{p^{\sigma_0}-1} = -n_K\frac{\zeta'}{\zeta}(\sigma_0) \ll \frac{n_K}{\sigma_0-1}$$

car ζ a un pôle simple en 1.

On obtient ainsi

$$S_1 \ll n_K x T^{-1}(\sigma_0-1)^{-1} = n_K x T^{-1}\log x.$$

- **Majoration de S_2 :** Comme il y a au plus deux entiers k tels que $|k-x| \leq 1$, et que $|N(\mathfrak{p}^m)-x| \leq 1$ entraîne $N(\mathfrak{p}^m) \geq x-1$ et $N(\mathfrak{p}) \leq x+1$, on obtient

$$S_2 \leq 2n_K \log(x+1)\left(\frac{x}{x-1}\right)^{\sigma_0} \ll n_K \log x.$$

- **Majoration de S_3 :** Finalement,

$$\begin{aligned}S_3 &= \sum_{\substack{\mathfrak{p},m\\ \frac{3}{4}x<N(\mathfrak{p}^m)<\frac{5}{4}x\\ |N(\mathfrak{p}^m)-x|>1}} \left(\frac{x}{N(\mathfrak{p}^m)}\right)^{\sigma_0} \min\left(1, T^{-1}\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right|^{-1}\right)\log(N(\mathfrak{p}))\\ &= \sum_{\substack{\mathfrak{p},m\\ 1<|N(\mathfrak{p}^m)-x|<\frac{x}{4}}} \left(\frac{x}{N(\mathfrak{p}^m)}\right)^{\sigma_0} \min\left(1, T^{-1}\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right|^{-1}\right)\log(N(\mathfrak{p})).\end{aligned}$$

Une étude de fonction donne l'inégalité $|\log y| \geq \frac{|y-1|}{2}$ pour $0 < y \leq 2$. On en déduit que pour $1 < |N(\mathfrak{p}^m)-x| < \frac{x}{4}$,

$$\left|\log\left(\frac{x}{N(\mathfrak{p}^m)}\right)\right|^{-1} \leq \frac{|x-N(\mathfrak{p}^m)|}{2N(\mathfrak{p}^m)} \leq \frac{x}{8N(\mathfrak{p}^m)}.$$

De plus, on a de nouveau $N(\mathfrak{p}^m) > x+1$ d'où

$$\left(\frac{x}{N(\mathfrak{p})}\right)^{\sigma_0} \ll 1,$$

tandis que $\log(N(\mathfrak{p})) \leq \log\left(\frac{5}{4}x\right) \ll \log(x)$.
On trouve donc

$$\begin{aligned} S_3 &\ll \frac{x\log x}{T} \sum_{\substack{\mathfrak{p},m \\ 1<|N(\mathfrak{p}^m)-x|<\frac{x}{4}}} \frac{1}{N(\mathfrak{p}^m)} \\ &= \frac{x\log x}{T} \sum_{\substack{k \\ 1<|k-x|<\frac{x}{4}}} \frac{1}{k} \left|\{(\mathfrak{p},m), N(\mathfrak{p}^m)=k\}\right| \\ &\ll n_K x(\log x)^2 T^{-1} \end{aligned}$$

par l'estimation classique de la série harmonique et le raisonnement précédent sur le nombre d'idéaux premiers au-dessus d'un nombre premier fixé.

On a donc finalement

$$R_0(x,T) \ll n_K \log x + n_K x(\log x)^2 T^{-1},$$

d'où

$$|R_1(x,T)| \ll \log x \log d_L + n_K \log x + n_K x(\log x)^2 T^{-1}.$$

Pour conclure cette partie, rassemblons ce que l'on a obtenu sous la forme d'une proposition :

Proposition. *Pour $x \geq 2$, $\sigma_0 = 1 + \frac{1}{\log x}$ et $T > 1$, on a*

$$\psi_C(x) = I_C(x,T) + R_1(x,T)$$

avec

$$I_C(x,T) = \frac{1}{2i\pi} \int_{\sigma_0+iT}^{\sigma_0+iT} F_C(s)\frac{x^s}{s} ds$$

et

$$|R_1(x,T)| \ll \log x \log d_L + n_K \log x + n_K x(\log x)^2 T^{-1}.$$

2) Réduction au cas cyclique

La prochaine étape est claire, estimer l'intégrale $I_C(x,T)$. Pour cela on l'écrit comme somme des intégrales faisant intervenir les $\frac{L'}{L}(s,\chi,L/K)$. Le problème de

cette méthode est que l'on connaît peu les propriétés analytiques de ces fonctions, notamment la présence d'éventuels pôles de partie réelle entre 0 et 1. Pour éviter ce problème, on emploie une astuce qui consiste à se ramener au cas cyclique (où l'on sait qu'il n'y a pas de tels pôles sauf éventuellement en 1). Pour faire cela, on va utiliser les propriétés d'induction des fonctions L d'Artin.

Notons $H = \langle g \rangle$ le sous-groupe de G engendré par g (rappellons que g est un élement quelconque de la classe de conjugaison C) et soit donc $E = L^H$ l'extension intermédiaire correspondante. On va montrer que l'on peut remplacer K par E dans la formule définissant la fonction F_C. La contrepartie de cette méthode est que l'on grossit les termes d'erreurs par rapport à ceux que l'on peut espérer avec la conjecture d'Artin (notamment en remplaçant n_K par $n_E \geq n_K$).

Proposition. *Pour $\mathfrak{Re}(s) > 1$, on a*

$$F_C(s) = -\frac{|C|}{|G|} \sum_{\chi \in \hat{H}} \overline{\chi(g)} \frac{L'}{L}(s, \chi, L/E).$$

Démonstration. Vu la définition de F_C, il suffit de montrer l'égalité suivante

$$\sum_{\chi \in \hat{H}} \overline{\chi(g)} \mathrm{Ind}_H^G \chi = \sum_{\chi \in \hat{G}} \overline{\chi(g)} \chi.$$

En effet, on obtiendra alors pour $\mathfrak{Re}(s) > 1$,

$$F_C(s) = -\frac{|C|}{|G|} \sum_{\chi \in \hat{H}} \overline{\chi(g)} \frac{L'}{L}(s, \mathrm{Ind}_H^G \chi, L/K) = -\frac{|C|}{|G|} \sum_{\chi \in \hat{H}} \overline{\chi(g)} \frac{L'}{L}(s, \chi, L/E).$$

Soit donc $f = \mathbf{1}_{\{g\}}$ l'indicatrice de $\{g\}$ dans H. Alors par linéarité de l'induction, on a

$$\mathrm{Ind}_H^G = h \mapsto \frac{1}{|H|} \sum_{s \in G} \dot{f}(s^{-1} h s)$$

où $\dot{f}$ est comme dans la partie I le prolongement de f à zéro hors de H. Or

$$\dot{f}(s^{-1} h s) = \begin{cases} 1 \text{ si } s^{-1} h s = g, \text{ i.e. si } h \in C \text{ et si } s = cx \text{ avec } c \in C_G(g) \text{ et } x^{-1} h x = g \\ 0 \text{ sinon} \end{cases},$$

avec $C_G(g)$ le centralisateur de g dans G.

On a donc

$$\mathrm{Ind}_H^G f = \frac{|C_G(g)|}{|H|} \mathbf{1}_C.$$

De plus, on a par les relations d'orthogonalité

$$f = \frac{1}{|H|} \sum_{\chi \in \hat{H}} \overline{\chi(g)} \chi,$$

tandis que

$$\frac{|C_G(g)|}{|H|} \mathbf{1}_C = \frac{|G|}{|C||H|} \mathbf{1}_C = \frac{1}{|H|} \sum_{\chi \in \hat{G}} \overline{\chi(g)} \chi,$$

ce qui donne exactement le résultat voulu. □

3) Estimation des zéros

Pour étudier l'intégrale de $I(x,T)$, il va nous falloir estimer les zéros des fonctions L associées à L/E. Pour cela, on va développer ces fonctions en produits portant sur leurs zéros grâce à la théorie de Hadamard [14].

On fixe désormais un caractère irréductible χ de $H = \mathrm{Gal}(L/E)$, et on notera

$$\delta(\chi) = \begin{cases} 1 \text{ si } \chi = \chi_0 \\ 0 \text{ sinon} \end{cases} .$$

Rappelons que dans la définition de la fonction L d'Artin complétée, il y a un terme exponentiel de la forme

$$\gamma_\chi(s) = \left(\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)\right)^{a(\chi)} \left(\pi^{-\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right)\right)^{b(\chi)}$$

où $a(\chi)$ et $b(\chi)$ sont des entiers naturels vérifiant $a(\chi) + b(\chi) = n_E$. En effet, χ étant irréductible et H étant abélien, χ est de degré 1 et donc ne contribue qu'à une puissance 1 pour chacun des n_E prolongements de $|.|$ à E.

Pour pouvoir appliquer le théorème de Hadamard à la fonction entière

$$f : s \mapsto (s(s-1))^{\delta(\chi)} \Lambda(s, \chi, L/E),$$

il nous faut montrer qu'elle est d'ordre fini, c'est-à-dire qu'il existe $C > 0$ tel que

$$f(s) = O(\mathrm{e}^{C|s|}).$$

14. Jacques Hadamard (1865-1963)

Par l'équation fonctionnelle, il suffit de le vérifier pour $\mathfrak{Re}(s) \geq \frac{1}{2}$. Il est bien connu que la fonction Γ est d'ordre au plus 1 (voir [2] ou [13] par exemple). Le terme $A(\chi)^{s/2}$ est clairement d'ordre 1, il nous reste donc à montrer que la fonction L associée à χ est également d'ordre 1. Or, comme L/E est cyclique, cette fonction n'est autre qu'une fonction L de Hecke, et le fait qu'elle soit d'ordre fini provient d'une représentation intégrale de cette fonction contenant une fonction θ de Jacobi généralisée (voir [8]). On conclut alors grâce au principe de Phragmen [15]-Lindelöf [16], car ces fonctions sont données comme des sommes de séries de Dirichlet sur le demi-plan

$$\{s \in \mathbb{C}, \mathfrak{Re}(s) > 1\}.$$

Théorème. *Il existe $B(\chi), B_1(\chi) \in \mathbb{C}$ tels que pour tout $s \in \mathbb{C}$,*

$$(s(s-1))^{\delta(\chi)}\Lambda(s,\chi,L/E) = \mathrm{e}^{B_1(\chi)+sB(\chi)} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) \mathrm{e}^{\frac{s}{\rho}},$$

où le produit porte sur les zéros de la fonction Λ.

Dans toute la suite, ρ désignera toujours un tel zéro. Prenant la dérivée logarithmique de ce produit, on trouve

$$\delta(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) + \frac{\Lambda'}{\Lambda}(s,\chi,L/E) = B(\chi) + \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right),$$

et donc en remplaçant Λ par sa définition, on obtient

$$\forall s \in \mathbb{C} \setminus \{0,1\}, \frac{L'}{L}(s,\chi,L/E) = B(\chi) + \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \delta(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) - \frac{\log A(\chi)}{2} - \frac{\gamma_\chi'}{\gamma_\chi}(s).$$

En suivant [7], on va montrer que l'on peut en quelque sorte se passer du terme $B(\chi)$.

Proposition. *On a*

$$\mathfrak{Re}(B(\chi)) = -\mathfrak{Re}\left(\sum_{\rho}\frac{1}{\rho}\right).$$

Démonstration. On va exploiter les différentes symétries de l'équation fonctionnelle. Tout d'abord, on a immédiatement grâce à la définition

$$\overline{\Lambda(s,\chi,L/E)} = \Lambda(\overline{s},\overline{\chi},L/E)$$

15. Lars Edvard Phragmén (1863–1937)
16. Ernst Leonard Lindelöf (1870-1946)

pour tout $s \in \mathbb{C} \setminus \{0,1\}$. Ainsi, pour de tels s, on a grâce à l'équation fonctionnelle

$$\overline{\frac{\Lambda'}{\Lambda}(s,\chi,L/E)} = \frac{\Lambda'}{\Lambda}(\overline{s},\overline{\chi},L/E) = -\frac{\Lambda'}{\Lambda}(1-\overline{s},\chi,L/E).$$

En particulier,

$$\mathfrak{Re}\frac{\Lambda'}{\Lambda}(1/2,\chi,L/E) = 0.$$

De plus, si ρ est un zéro de Λ alors $1-\overline{\rho}$ aussi pour les mêmes raisons. Par conséquent,

$$\mathfrak{Re}\left(\sum_{\rho}\frac{1}{1/2-\rho}\right) = 0$$

en regroupant

$$\frac{1}{1/2-\rho} + \frac{1}{1/2-\overline{\rho}} = \frac{1}{1/2-\rho} - \overline{\left(\frac{1}{1/2-\rho}\right)}.$$

En remplaçant s par $\frac{1}{2}$ dans la dérivée logarithmique de Λ, on trouve bien

$$\mathfrak{Re}\left(B(\chi) + \sum_{\rho}\frac{1}{\rho}\right) = 0.$$

□

On voit facilement que $A(\overline{\chi}) = A(\chi)$, $B(\overline{\chi}) = \overline{B(\chi)}$, $\delta(\overline{\chi}) = \delta(\chi)$ et $\gamma_\chi = \gamma_{\overline{\chi}}$ via les définitions dans la section I.3) et dans le produit de Hadamard. Ainsi

$$\frac{L'}{L}(s,\overline{\chi},L/E) = \overline{B(\chi)} + \sum_{\rho}\left(\frac{1}{s-\overline{\rho}} + \frac{1}{\overline{\rho}}\right) - \delta(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) - \frac{\log A(\chi)}{2} - \frac{\gamma_\chi'}{\gamma_\chi}(s),$$

et donc en sommant et en utilisant la proposition précédente, on trouve

Proposition. *Pour tout $s \in \mathbb{C} \setminus \{0,1\}$,*

$$\frac{L'}{L}(s,\chi,L/E) + \frac{L'}{L}(s,\overline{\chi},L/E) = \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}}\right) - 2\delta(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) - \log A(\chi) - 2\frac{\gamma_\chi'}{\gamma_\chi}(s).$$

Passons maintenant à quelques lemmes techniques. Dans toute la suite, les lettres σ et t désigneront respectivement la partie réelle et la partie imaginaire du complexe s, comme le veut l'usage.

Lemme 1. *Pour* $\mathfrak{Re}(s) > 1$,

$$\left|\frac{L'}{L}(s,\chi,L/E)\right| \ll \frac{n_E}{\sigma-1}.$$

Démonstration. On a déjà vu que

$$-\frac{L'}{L}(s,\chi,L/E) = \sum_{\mathfrak{p}}\sum_{m=1}^{+\infty}\chi_E(\mathfrak{p}^m)\log(N(\mathfrak{p}))N(\mathfrak{p})^{-ms}.$$

Or il est clair que

$$|\chi_E(\mathfrak{p}^m)| \leq 1$$

pour tout $\mathfrak{p}$ premier de K, donc

$$\left|\frac{L'}{L}(s,\chi,L/E)\right| \leq \sum_{\mathfrak{p}}\sum_{m=1}^{+\infty}\log(N(\mathfrak{p}))N(\mathfrak{p})^{-m\sigma} = -\frac{\zeta_E'}{\zeta_E}(\sigma) \ll \frac{n_E}{\sigma-1},$$

comme précédemment. □

Lemme 2. *Pour* $\mathfrak{Re}(s) > -\frac{1}{2}$ *et* $|s| \geq \frac{1}{8}$, *on a*

$$\left|\frac{\gamma_\chi'}{\gamma_\chi}(s)\right| \ll n_E\log(|s|+2).$$

Démonstration. La formule du produit donnant $\frac{1}{\Gamma}$ (voir [13]) nous donne

$$\left|\frac{\Gamma'}{\Gamma}(s)\right| \ll \log(|s|+2)$$

pour $|s| \geq \frac{1}{16}$ et $\mathfrak{Re}(s) > -\frac{1}{4}$.

Nos hypothèses sur s donnent bien

$$\begin{cases}\left|\frac{s}{2}\right| \geq \frac{1}{16}\\ \mathfrak{Re}\left(\frac{s}{2}\right) > -\frac{1}{4}\end{cases} \quad \text{et} \quad \begin{cases}\left|\frac{s+1}{2}\right| \geq \frac{1}{16}\\ \mathfrak{Re}\left(\frac{s+1}{2}\right) > -\frac{1}{4}\end{cases},$$

donc on a

$$\frac{\gamma_\chi'}{\gamma_\chi}(s) = a(\chi)\left(-\frac{\log\pi}{2}+\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right)\right)+b(\chi)\left(-\frac{\log\pi}{2}+\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+1}{2}\right)\right) \ll n_E\log(|s|+2)$$

car $a(\chi)+b(\chi) = n_E$. □

On peut finalement estimer le nombre de zéros de notre fonction L dans certains rectangles. On notera $n_\chi(t)$ le nombre de zéro de $s \mapsto L(s,\chi,L/E)$ de la forme $\rho = \beta + i\gamma$ avec $|\gamma - t| \leq 1$ et $0 < \beta < 1$.

Lemme 3. *On a*

$$n_\chi(t) \ll \log A(\chi) + n_E \log(|t|+2)$$

pour $t \in \mathbb{R}$.

Démonstration. L'égalité

$$\frac{L'}{L}(s,\chi,L/E)+\frac{L'}{L}(s,\overline{\chi},L/E) = \sum_\rho \left(\frac{1}{s-\rho}+\frac{1}{s-\overline{\rho}}\right) - 2\delta(\chi)\left(\frac{1}{s}+\frac{1}{s-1}\right) - \log A(\chi) - 2\frac{\gamma_\chi'}{\gamma_\chi}(s)$$

et les deux lemmes précédents nous donnent immédiatement que pour $s = 2+it$,

$$\sum_\rho \left(\frac{1}{s-\rho}+\frac{1}{s-\overline{\rho}}\right) \ll \log A(\chi) + n_E \log(|t|+2).$$

Mais pour $\mathfrak{Re}(s) = 2$, on a

$$\mathfrak{Re}\left(\frac{1}{s-\rho}\right) = \mathfrak{Re}\left(\frac{\overline{s}-\overline{\rho}}{|s-\rho|^2}\right) > 0$$

et de même

$$\mathfrak{Re}\left(\frac{1}{s-\overline{\rho}}\right) > 0$$

pour tout zéro ρ. On peut donc minorer

$$\begin{aligned}\sum_\rho \mathfrak{Re}\left(\frac{1}{s-\rho}+\frac{1}{s-\overline{\rho}}\right) &\geq \sum_{\substack{\rho \\ |\gamma-t|\leq 1}} \mathfrak{Re}\left(\frac{1}{s-\rho}+\frac{1}{s-\overline{\rho}}\right) \\ &= 2\sum_{\substack{\rho \\ |\gamma-t|\leq 1}} \frac{2-\beta}{(2-\beta)^2+(\gamma-t)^2} \\ &\geq 2\sum_{\substack{\rho \\ |\gamma-t|\leq 1}} \frac{1}{5} = \frac{2}{5} n_\chi(t),\end{aligned}$$

d'où le résultat annoncé. □

Grâce à cette estimation, on obtient les deux résultats suivants, qui nous serviront à la fin de la démonstration.

Lemme 4. *On a*

$$B(\chi) + \sum_{\substack{\rho \\ |\rho|<\varepsilon}} \frac{1}{\rho} \ll \varepsilon^{-1}(\log A(\chi) + n_E)$$

pour $0 < \varepsilon \leq 1$.

Démonstration. Comme précédemment, on prend $s = 2$ pour obtenir

$$\frac{L'}{L}(2, \chi, L/E) = B(\chi) + \sum_{\rho} \left(\frac{1}{2-\rho} + \frac{1}{\rho} \right) - \frac{3}{2}\delta(\chi) - \frac{\log A(\chi)}{2} - \frac{\gamma'_\chi}{\gamma_\chi}(2)$$

d'où

$$B(\chi) + \sum_{\rho} \left(\frac{1}{2-\rho} \right) \ll \log A(\chi) + n_E$$

car la partie imaginaire de s ne varie pas. On se débarrasse maintenant des « grands zéros » :

$$\left| \frac{1}{2-\rho} + \frac{1}{\rho} \right| = \frac{2}{|\rho(2-\rho)|} \leq \frac{2}{|\rho|^2}$$

pour tout zéro ρ, ce qui implique

$$\sum_{\substack{\rho \\ |\rho| \geq 1}} \left| \frac{1}{2-\rho} + \frac{1}{\rho} \right| \ll \sum_{j=1}^{+\infty} \frac{n_\chi(j)}{j^2} \ll \log A(\chi) + n_E.$$

De plus

$$\sum_{\substack{\rho \\ |\rho| < 1}} \left| \frac{1}{2-\rho} \right| \leq \sum_{\substack{\rho \\ |\rho| < 1}} 1 \leq n_\chi(0) \ll \log A(\chi) + n_E.$$

On obtient donc finalement pour $0 < \varepsilon \leq 1$,

$$\begin{aligned} B(\chi) + \sum_{\substack{\rho \\ |\rho| < \varepsilon}} \frac{1}{\rho} &\ll \sum_{\substack{\rho \\ \varepsilon < |\rho| \leq 1}} \frac{1}{|\rho|} + \log A(\chi) + n_E \\ &\leq \varepsilon^{-1} n_{\chi(0)} + \log A(\chi) + n_E \\ &\ll \varepsilon^{-1} (\log A(\chi) + n_E). \end{aligned}$$

□

Lemme 5. *On a*

$$\left| \frac{L'}{L}(s, \chi, L/E) + \frac{\delta(\chi)}{s-1} - \sum_{\substack{\rho \\ |\gamma - t| \leq 1}} \frac{1}{\rho} \right| \ll \log A(\chi) + n_E \log(|t| + 2)$$

pour $-\frac{1}{2} \leq \sigma \leq 3$ *et* $|s| \geq \frac{1}{8}$.

Démonstration. En soustrayant on a

$$\frac{L'}{L}(s,\chi,L/E)-\frac{L'}{L}(3+it,\chi,L/E)=\sum_{\rho}\left(\frac{1}{s-\rho}-\frac{1}{3+it-\rho}\right)-\frac{\gamma'_\chi}{\gamma_\chi}(s)+\frac{\gamma'_\chi}{\gamma_\chi}(3+it)$$
$$-\delta(\chi)\left(\frac{1}{s}+\frac{1}{s-1}-\frac{1}{3+it}-\frac{1}{2+it}\right).$$

En regroupant, on trouve donc

$$\left|\frac{L'}{L}(s,\chi,L/E)+\frac{\delta(\chi)}{s-1}-\sum_{\substack{\rho\\|\gamma-t|\leq 1}}\frac{1}{\rho}\right|\ll n_E\log(|t|+2)+\sum_{\substack{\rho\\|\gamma-t|>1}}\left|\frac{1}{s-\rho}-\frac{1}{3+it-\rho}\right|$$
$$+\sum_{\substack{\rho\\|\gamma-t|\leq 1}}\left|\frac{1}{3+it-\rho}\right|,$$

car la dérivée logarithmique de la fonction L en $3+it$ reste bornée d'après le lemme 1.

Or, pour tout zéro ρ, on a $|3+it-\rho|\geq 2$, donc

$$\sum_{\substack{\rho\\|\gamma-t|\leq 1}}\left|\frac{1}{3+it-\rho}\right|\leq n_\chi(t)\ll\log A(\chi)+n_E\log(|t|+2).$$

De plus, on a aussi

$$\left|\frac{1}{s-\rho}-\frac{1}{3+it-\rho}\right|=\frac{3-\sigma}{|s-\rho||3+it-\rho|}\leq\frac{7}{2|\rho|^2}.$$

En sommant sur les ρ tels que $|\gamma-t|>1$, on prend en compte $n_\chi(t+j)$ zéros dans le rectangle avec $|\gamma-t-j|\leq 1$, avec $j\in\mathbb{Z}\setminus\{-1,0,1\}$.

On a donc

$$\sum_{\substack{\rho\\|\gamma-t|>1}}\left|\frac{1}{s-\rho}-\frac{1}{3+it-\rho}\right|\ll\sum_{j=1}^{+\infty}\frac{n_\chi(t+j)+n_\chi(t-j)}{j^2}$$
$$\ll\log A(\chi)+n_E\sum_{j=1}^{+\infty}\frac{\log(|t+j|+2)+\log(|t-j|+2)}{j^2}$$
$$\ll\log A(\chi)+n_E\log(|t|+2)$$
$$+n_E\sum_{j=2}^{+\infty}\frac{\log(|t+j|+2)+\log(|t-j|+2)}{j^2}$$

Or, pour $j \geq 2$, on a

$$\begin{aligned}\log(|t|+2)+\log j &= \log(|tj|+j+j)\\ &\geq \log(|t|+j+2)\\ &\geq \log(|t+j|+2), \log(|t-j|+2).\end{aligned}$$

Par convergence de la série

$$\sum_j \frac{\log j}{j^2},$$

on obtient finalement

$$\sum_{\substack{\rho\\ |\gamma-t|>1}} \left|\frac{1}{s-\rho}-\frac{1}{3+it-\rho}\right| \ll \log A(\chi)+n_E\log(|t|+2).$$

□

4) Évaluation de l'intégrale

Rappelons que l'on cherche à évaluer

$$I_C(x,T) = -\frac{|C|}{|G|}\sum_{\chi\in\hat{H}}\overline{\chi(g)}\frac{1}{2i\pi}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{L'}{L}(s,\chi,L/E)\frac{x^s}{s}ds.$$

Pour tout $\chi \in \hat{H}$, notons

$$I_\chi(x,T) = \frac{1}{2i\pi}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{L'}{L}(s,\chi,L/E)\frac{x^s}{s}ds.$$

Nous allons utiliser le théorème des résidus pour calculer cette intégrale. Pour cela, on va l'écrire comme le bord droit d'un certain rectangle dont le bord gauche va « tendre infiniment vers la gauche ».

On pose donc $U = j+\frac{1}{2}$ avec $j \in \mathbb{N}$, $B_{T,U}$ le rectangle de sommets $\sigma_0 - iT, \sigma_0 + iT, -U+iT, -U-iT$ parcouru dans le sens direct et

$$I_\chi(x,T,U) = \frac{1}{2i\pi}\int_{B_{T,U}}\frac{L'}{L}(s,\chi,L/E)\frac{x^s}{s}ds.$$

Enfin, posons $R_\chi(x,T,U) = I_\chi(x,T,U) - I_\chi(x,T)$, que l'on découpe de la manière suivante :

$$V_\chi(x,T,U) = \frac{1}{2i\pi}\int_{-U+iT}^{-U-iT}\frac{L'}{L}(s,\chi,L/E)\frac{x^s}{s}ds = \frac{1}{2\pi}\int_T^{-T}\frac{L'}{L}(-U+it,\chi,L/E)\frac{x^{-U+it}}{-U+it}dt,$$

$$H_\chi(x,T,U)=\frac{1}{2i\pi}\int_{-U}^{-\frac14}\left(\frac{L'}{L}(\sigma-iT,\chi,L/E)\frac{x^{\sigma-iT}}{\sigma-iT}-\frac{L'}{L}(\sigma+iT,\chi,L/E)\frac{x^{\sigma+iT}}{\sigma+iT}\right)d\sigma$$

et

$$H^*_\chi(x,T,U) \text{ la même intégrale de } -\frac14 \text{ à } \sigma_0.$$

À l'aide des deux prochains lemmes, on va estimer $V_\chi(x,T,U)$ et $H_\chi(x,T,U)$, dont les domaines d'intégration sont hors de la bande critique.

Lemme 6. *On a*

$$\frac{\Gamma'}{\Gamma}(s)\ll\log(|s|+2)$$

pour s vérifiant $|s+k|\geq\frac18$ pour tout $k\in\mathbb{N}$.

Démonstration. On a déjà vu cette majoration pour $\mathfrak{Re}(s)\geq1$ dans le lemme 2. On va s'y ramener grâce à l'équation fonctionnelle de la fonction Γ. En effet, celle-ci se traduit par

$$\frac{\Gamma'}{\Gamma}(s+1)=\frac{\Gamma'}{\Gamma}(s)+\frac1s$$

pour $s\in\mathbb{C}\setminus\mathbb{Z}^-$, ce qui donne par récurrence

$$\frac{\Gamma'}{\Gamma}(s)=\frac{\Gamma'}{\Gamma}(s+m)-\sum_{k=0}^{m-1}\frac{1}{s+k}$$

pour tout $m\in\mathbb{N}^*$. En choisissant m tel que $1-m\leq\mathfrak{Re}(s)$, on a alors

$$\frac{\Gamma'}{\Gamma}(s+m)\ll\log(|s+m|+2),$$

tandis que

$$\sum_{k=0}^{m-1}\frac{1}{s+k}\ll\sum_{k=0}^{m-1}\frac{1}{\frac18+k}\ll\log m$$

grâce à la condition $|s+k|\geq\frac18$ pour tout $k\in\mathbb{N}$.

En prenant $m=\lfloor|s|+2\rfloor$ on obtient bien

$$\frac{\Gamma'}{\Gamma}(s)\ll\log(|s|+2).$$

□

Lemme 7. *Pour tout $\chi \in \hat{H}$, on a*

$$\frac{L'}{L}(s,\chi,L/E) \ll \log A(\chi) + n_E \log(|s|+2)$$

pour s vérifiant $\sigma \leq -\frac{1}{4}$ et $|s+k| \geq \frac{1}{4}$ pour tout $k \in \mathbb{N}$.

Démonstration. D'après l'équation fonctionnelle, on a

$$(s(s-1))^{\delta(\chi)} A(\chi)^{s/2} \gamma_\chi(s) L(s,\chi,L/E) = W(\chi)(s(s-1))^{\delta(\chi)} A(\chi)^{\frac{1-s}{2}} \gamma_\chi(1-s) L(1-s,\overline{\chi},L/E),$$

avec $W(\chi)$ de module 1.

En prenant les dérivées logarithmiques, on trouve

$$\frac{L'}{L}(s,\chi,L/E) = \frac{L'}{L}(1-s,\overline{\chi},L/E) - \log A(\chi) - \frac{\gamma_\chi'}{\gamma_\chi}(s) + \frac{\gamma_\chi'}{\gamma_\chi}(1-s) + \log W(\chi).$$

Or, si $\sigma \leq -\frac{1}{4}$, alors $1-\sigma \geq \frac{5}{4} > 1$ donc

$$\frac{L'}{L}(1-s,\overline{\chi},L/E) \ll -\frac{n_E}{\sigma} = O(1)$$

d'après le lemme 1, tandis que

$$\frac{\gamma_\chi'}{\gamma_\chi}(1-s) \ll n_E \log(|s|+2)$$

par le lemme 2.

De plus, le lemme 6 nous donne

$$\frac{\gamma_\chi'}{\gamma_\chi}(s) = a(\chi)\left(-\frac{\log\pi}{2} + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right)\right) + b(\chi)\left(-\frac{\log\pi}{2} + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+1}{2}\right)\right) \ll n_E \log(|s|+2)$$

car $\left|\frac{s}{2}+k\right| \geq \frac{1}{8}$ et $\left|\frac{s+1}{2}+k\right| \geq \frac{1}{8}$ pour tout $k \in \mathbb{N}$ par hypothèse sur s.

Rassemblant ces estimations, on obtient bien

$$\frac{L'}{L}(s,\chi,L/E) \ll \log A(\chi) + n_E \log(|s|+2).$$

□

• **Majoration de $V_\chi(x,T,U)$:** grâce à l'hypothèse sur U, on a $|s+k| \geq \frac{1}{4}$ pour tout $k \in \mathbb{N}$ si $\mathfrak{Re}(s) = -U$. Donc on a d'après le lemme 7

$$\begin{aligned} V_\chi(x,T,U) &= \frac{1}{2\pi}\int_T^{-T} \frac{L'}{L}(-U+it,\chi,L/E)\frac{x^{-U+it}}{-U+it}dt \\ &\ll \frac{x^{-U}}{U}\int_{-T}^{T}\left|\frac{L'}{L}(-U+it,\chi,L/E)\right|dt \\ &\ll \frac{x^{-U}}{U}T(\log A(\chi)+n_E\log(T+U)). \end{aligned}$$

• **Majoration de $H_\chi(x,T,U)$:** de la même manière, comme $T>1$,

$$\begin{aligned} H_\chi(x,T,U) &= \frac{1}{2i\pi}\int_{-U}^{-\frac{1}{4}}\left(\frac{L'}{L}(\sigma-iT,\chi,L/E)\frac{x^{\sigma-iT}}{\sigma-iT} - \frac{L'}{L}(\sigma+iT,\chi,L/E)\frac{x^{\sigma+iT}}{\sigma+iT}\right)d\sigma \\ &\ll \int_{-\infty}^{-\frac{1}{4}}\frac{x^\sigma}{T}(\log A(\chi)+n_E\log(|\sigma|+2)+n_E\log(T))d\sigma \\ &\ll \frac{x^{-1/4}}{T}(\log A(\chi)+n_E\log T). \end{aligned}$$

Maintenant, pour traiter le terme $H_\chi^*(x,T,U)$, on introduit la somme sur les zéros de notre fonction L. D'après le lemme 5

$$\left|\frac{L'}{L}(\sigma+iT,\chi,L/E) - \sum_{\substack{\rho \\ |\gamma-T|\leq 1}}\frac{1}{\rho}\right| \ll \log A(\chi)+n_E\log(|T|+2)$$

lorsque σ parcourt $[-1/4,\sigma_0]$, car alors $|\sigma+iT| \geq \frac{1}{8}$ et $-\frac{1}{2} \leq \sigma \leq 3$, tandis que le terme $\frac{\delta(\chi)}{\sigma+iT-1}$ reste borné. De même,

$$\left|\frac{L'}{L}(\sigma-iT,\chi,L/E) - \sum_{\substack{\rho \\ |\gamma+T|\leq 1}}\frac{1}{\rho}\right| \ll \log A(\chi)+n_E\log(|T|+2)$$

pour $\sigma \in [-1/4, \sigma_0]$. En intégrant la différence, on trouve

$$H^*_\chi(x,T,U) - \frac{1}{2i\pi}\int_{-1/4}^{\sigma_0}\left(\frac{x^{\sigma-iT}}{\sigma-iT}\sum_{\substack{\rho\\|\gamma+T|\le 1}}\frac{1}{\sigma-iT-\rho} - \frac{x^{\sigma+iT}}{\sigma+iT}\sum_{\substack{\rho\\|\gamma-T|\le 1}}\frac{1}{\sigma+iT-\rho}\right)d\sigma$$
$$\ll \int_{-1/4}^{\sigma_0}\frac{x^\sigma}{T}(\log A(\chi) + n_E\log T)d\sigma$$
$$= \frac{\mathrm{e}x - x^{-1/4}}{T\log x}(\log A(\chi) + n_E\log T)$$
$$\ll \frac{x}{T\log x}(\log A(\chi) + n_E\log T).$$

Il nous reste donc à majorer cette intégrale. Pour cela, il suffit de majorer les

$$\int_{-1/4}^{\sigma_0}\frac{x^{\sigma+it}}{(\sigma+it)(\sigma+it-\rho)}d\sigma$$

pour $t = \pm T$ et ρ zéro de L avec $|\gamma - t| \le 1$. À partir de maintenant on suppose que $|T| \ge 2$ et que T ne coïncide pas avec la partie imaginaire d'un zéro.

Lemme 8. *Pour $\rho = \beta + i\gamma$ avec $0 < \beta < 1$ et pour $|t| \ge 2$ avec $\gamma \ne t$, on a*

$$\int_{-1/4}^{\sigma_0}\frac{x^{\sigma+it}}{(\sigma+it)(\sigma+it-\rho)}d\sigma \ll |t|^{-1}x^{\sigma_0}(\sigma_0-\beta)^{-1}.$$

Démonstration. On suppose d'abord que $\gamma > t$. Alors par le théorème de Cauchy [17], on a

$$\int_R \frac{x^s}{s(s-\rho)}ds$$

où R est le rectangle de sommets $\sigma_0 + i(t-1), \sigma_0 + it, -\frac{1}{4} + it, -\frac{1}{4} + i(t-1)$ parcouru dans le sens direct.

Or sur les autres côtés, l'intégrande est majorée par

$$\frac{x^{\sigma_0}}{(|t|-1)(\sigma_0-\beta)}$$

et les côtés sont de longueur uniformément bornée. On en déduit le résultat. Si $\gamma < t$ il suffit de procéder de la même manière avec le rectangle de sommets $\sigma_0 + i(t+1), \sigma_0 + it, -\frac{1}{4} + it, -\frac{1}{4} + i(t+1)$ parcouru dans le sens direct. □

17. Augustin Louis Cauchy (1789-1857)

On obtient donc

$$\frac{1}{2i\pi}\int_{-1/4}^{\sigma_0}\left(\frac{x^{\sigma-iT}}{\sigma-iT}\sum_{\substack{\rho\\|\gamma+T|\leq 1}}\frac{1}{\sigma-iT-\rho}-\frac{x^{\sigma+iT}}{\sigma+iT}\sum_{\substack{\rho\\|\gamma-T|\leq 1}}\frac{1}{\sigma+iT-\rho}\right)d\sigma$$
$$\ll \frac{x^{\sigma_0}}{T}(\sigma_0-1)^{-1}(n_\chi(-T)+n_\chi(T))$$
$$\ll \frac{x\log x}{T}(\log A(\chi)+n_E\log T).$$

Finalement, cela donne

$$H_\chi^*(x,T,U)\ll \frac{x\log x}{T}(\log A(\chi)+n_E\log T),$$

puis

$$I_\chi(x,T)-I_\chi(x,T,U)\ll \frac{x\log x}{T}(\log A(\chi)+n_E\log T)+\frac{Tx^{-U}}{U}(\log A(\chi)+n_E\log(T+U)).$$

Appliquons désormais le théorème des résidus pour calculer $I_\chi(x,T,U)$. Pour cela, il nous faut déterminer les pôles de $\frac{L'}{L}$ à l'intérieur du rectangle $B_{T,U}$:

- Il y a un pôle simple en 1 (de résidu -1) si χ est le caractère unité, et pas de pôle sinon. Ce pôle fournit donc une contribution de $-x\delta(\chi)$.
- Les zéros non triviaux fournissent une contribution de

$$\sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho}.$$

- Enfin, il faut prendre en compte les zéros triviaux de L, que l'on trouve par l'équation fonctionnelle. Grâce à la formule

$$\frac{L'}{L}(s,\chi,L/E)=\frac{L'}{L}(1-s,\overline{\chi},L/E)-\log A(\chi)-\frac{\gamma_\chi'}{\gamma_\chi}(s)+\frac{\gamma_\chi'}{\gamma_\chi}(1-s)+\log W(\chi),$$

on voit que $\frac{L'}{L}$ admet des pôles simples de résidus $a(\chi)$ en les $-2m, m\in\mathbb{N}$ et des pôles simples de résidus $b(\chi)$ en les $-(2m-1), m\in\mathbb{N}^*$. Ainsi, hormis le pôle en 0, on trouve une contribution de

$$-b(\chi)\sum_{m=1}^{\lfloor\frac{U+1}{2}\rfloor}\frac{x^{-(2m-1)}}{2m-1}-a(\chi)\sum_{m=1}^{\lfloor\frac{U}{2}\rfloor}\frac{x^{-2m}}{2m}.$$

- Au voisinage de 0, on a
$$\frac{x^s}{s} = \frac{1}{s} + \log x + sh_1(s)$$
avec h_1 holomorphe au voisinage de 0. De plus
$$\frac{L'}{L}(s, \chi, L/E) = \frac{a(\chi) - \delta(\chi)}{s} + r(\chi) + sh_2(s)$$
avec h_2 holomorphe au voisinage de 0 et
$$r(\chi) = B(\chi) - \frac{1}{2}\log A(\chi) + \frac{n_E}{2}\log\pi + \delta(\chi) - \frac{a(\chi)}{2}\frac{\Gamma'}{\Gamma}(1) - \frac{b(\chi)}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}\right),$$
en effectuant un développement limité de $\frac{\Gamma'}{\Gamma}$ au voisinage de 0. En effet, on a
$$\frac{\Gamma'}{\Gamma}(z+1) - \frac{1}{z} = \frac{\Gamma'}{\Gamma}(z)$$
pour tout $z \in \mathbb{C} \setminus \mathbb{Z}^-$, et donc le résidu en 0 de $s \mapsto \frac{a(\chi)}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right)$ est $-a(\chi)$. Finalement le résidu en 0 de $s \mapsto \frac{L'}{L}(s, \chi, L/E)\frac{x^s}{s}$ est
$$r(\chi) + (a(\chi) - \delta(\chi))\log x.$$

On a donc finalement
$$I_\chi(x, T, U) = -\delta(\chi)x + \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} - b(\chi)\sum_{m=1}^{\lfloor\frac{U+1}{2}\rfloor} \frac{x^{-(2m-1)}}{2m-1} - a(\chi)\sum_{m=1}^{\lfloor\frac{U}{2}\rfloor} \frac{x^{-2m}}{2m} + r(\chi) + (a(\chi) - \delta(\chi))\log x.$$

En faisant tendre U vers $+\infty$ (tout en l'astreignant à être de la forme $j + \frac{1}{2}$ avec $j \in \mathbb{N}$). On trouve
$$\begin{aligned}
&I_\chi(x, T) + \delta(\chi)x - \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} + b(\chi)\sum_{m=1}^{+\infty} \frac{x^{-(2m-1)}}{2m-1} + a(\chi)\sum_{m=1}^{+\infty} \frac{x^{-2m}}{2m} - r(\chi) - (a(\chi) - \delta(\chi))\log x \\
&= I_\chi(x, T) + \delta(\chi)x - \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} + b(\chi)(-\log(1 - x^{-1}) + \frac{1}{2}\log(1 - x^{-2})) + a(\chi)(-\frac{1}{2}\log(1 - x^{-2})) \\
&\quad - r(\chi) - (a(\chi) - \delta(\chi))\log x \\
&\ll \frac{x\log x}{T}(\log A(\chi) + n_E \log T),
\end{aligned}$$
valable pour $x \geq 2$ et $|T| \geq 2$ avec T ne coïncidant pas avec la partie imaginaire d'un zéro de L.

Théorème. *Pour $x \geq 2$ et $|T| \geq 2$, on a*

$$\psi_C(x) - \frac{|C|}{|G|}x + S(x,T) \ll \frac{|C|}{|G|}\left(\frac{x\log x + T}{T}\log d_L + n_L \log x + \frac{n_L x \log x \log T}{T}\right) + \log x \log d_L + n_K x T^{-1}(\log x)^2,$$

où

$$S(x,T) = \frac{|C|}{|G|}\sum_{\chi\in\hat{H}} \overline{\chi(g)}\left(\sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{1}{\rho}\right).$$

Démonstration. Rappelons que

$$r(\chi) = B(\chi) - \frac{1}{2}\log A(\chi) + \frac{n_E}{2}\log\pi + \delta(\chi) - \frac{a(\chi)}{2}\frac{\Gamma'}{\Gamma}(1) - \frac{b(\chi)}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}\right).$$

On trouve donc grâce au lemme 4

$$r(\chi) - \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{1}{\rho} \ll \log A(\chi) + n_E.$$

Ainsi, si T n'est pas la partie imaginaire d'un zéro, on trouve

$$I_\chi(x,T) + \delta(\chi)x - \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{1}{\rho} \ll \log A(\chi) + n_E \log x + \frac{x\log x}{T}(\log A(\chi) + n_E \log T).$$

En sommant sur les $\chi \in \hat{H}$, on obtient

$$I_C(x,T) - \frac{|C|}{|G|}\sum_{\chi\in\hat{H}} \overline{\chi(g)}\left(\delta(\chi)x - \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{1}{\rho}\right)$$
$$\ll \frac{|C|}{|G|}\left(\sum_{\chi\in\hat{H}} \log A(\chi) + n_E \log x + \frac{x\log x}{T}(\log A(\chi) + n_E \log T)\right).$$

Or, par la relation conducteur-discriminant (donnée en fin de I.3)), on a

$$\sum_{\chi\in\hat{H}} \log A(\chi) = \log d_L$$

et

$$\sum_{\chi\in\hat{H}} n_E = n_E[L:E] = n_L.$$

Donc

$$I_C(x,T) - \frac{|C|}{|G|}\sum_{\chi\in\hat{H}}\overline{\chi(g)}\left(\delta(\chi)x - \sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho} - \sum_{\substack{\rho\\|\rho|<1/2}}\frac{1}{\rho}\right)$$
$$\ll \frac{|C|}{|G|}\left(\frac{x\log x+T}{T}\log d_L + n_L\log x + \frac{n_L x\log x\log T}{T}\right).$$

De plus, on sait que

$$\psi_C(x) = I_C(x,T) + R_1(x,T)$$

avec

$$R_1(x,T) \ll \log x\log d_L + n_K\log x + n_K x T^{-1}(\log x)^2.$$

On obtient donc la majoration annoncée tant que T n'est pas la partie imaginaire d'un zéro de l'une de nos fonctions L.

Pour de tels T, on considère la majoration obtenue en prenant $T+\varepsilon$ avec $\varepsilon > 0$ suffisamment petit (il n'y a pas d'accumulation de zéros). En faisant tendre ε vers 0, la seule discontinuité qui apparaît dans la majoration provient de la somme

$$\sum_{\chi\in\hat{H}}\overline{\chi(g)}\sum_{\substack{\rho\\|\gamma|<T+\varepsilon}}\frac{x^\rho}{\rho},$$

et celle-ci correspond à un saut borné par

$$\frac{x}{T}\sum_{\chi\in\hat{H}}(n_\chi(T)+n_\chi(-T)) \ll \frac{x}{T}\log d_L + \frac{xn_L}{T}\log T,$$

qui peut être absorbé dans le terme d'erreur. □

Ce dernier théorème est l'étape cruciale dans la démonstration du théorème de Chebotarev. Remarquons qu'en présence de l'hypothèse de Riemann généralisée, on pourrait d'ores et déjà obtenir une estimation très précise de $\psi_C(x)$. Nous y reviendrons en 7).

5) Région sans zéros

Dans le dernier théorème, on a encore le choix pour T. Pour optimiser ce choix, on va établir une région sans zéros de nos fonctions L. Or on sait que

$$\zeta_L(s) = \prod_{\chi\in\hat{H}} L(s,\chi,L/E),$$

on peut donc obtenir une telle région sans zéros à partir d'une région sans zéros pour ζ_L.

Lemme 9. *La fonction ζ_L ne s'annule pas en les $\rho = \beta + i\gamma$ avec*

$$|\gamma| \geq \frac{1}{1 + 4\log d_L}$$

et

$$\beta \geq 1 - c(\log d_L + n_L \log(|\gamma| + 2))^{-1},$$

où $c > 0$ est une constante effectivement calculable.

Démonstration. On utilise l'argument classique de De la Vallée-Poussin :

$$-\frac{\zeta_L'}{\zeta_L}(s) = \sum_{m=1}^{+\infty} \alpha(m) m^{-s}$$

pour $\mathfrak{Re}(s) > 1$, où $\alpha(m) \geq 0$ pour tout $m \in \mathbb{N}^*$.

On en déduit

$$\begin{aligned} &\mathfrak{Re}\left(-3\frac{\zeta_L'}{\zeta_L}(\sigma) - 4\frac{\zeta_L'}{\zeta_L}(\sigma + it) - \frac{\zeta_L'}{\zeta_L}(\sigma + 2it)\right) \\ &= \sum_{m=1}^{+\infty} \alpha(m) m^{-\sigma}(3 + 4\cos(t\log m) + \cos(2t\log m)) \geq 0 \end{aligned}$$

par l'identité

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

valable pour $\theta \in \mathbb{R}$.

On a de plus,

$$\zeta_L(s) = L(s, \chi_0, L/L),$$

et comme $\overline{\chi_0} = \chi_0$, on a par un lemme précédent

$$2\frac{\zeta_L'}{\zeta_L}(s) = \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}}\right) - \frac{2}{s} - \frac{2}{s-1} - \log d_L - 2\frac{\gamma_L'}{\gamma_L}(s)$$

pour $s \in \mathbb{C} \setminus \{0, 1\}$, avec $\gamma_L = \Gamma_{\mathbb{R}}^{r_1}\Gamma_{\mathbb{C}}^{r_2}$.

Comme

$$\frac{1}{\sigma-\rho} + \frac{1}{\sigma-\overline{\rho}} = 2\mathfrak{Re}((\sigma-\rho)^{-1}),$$

on a donc pour $\sigma > 1$,

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) \leq \frac{1}{\sigma-1} + \frac{1}{\sigma} + \frac{1}{2}\log d_L + \frac{\gamma_L'}{\gamma_L}(\sigma) - \sum_\rho \mathfrak{Re}((\sigma-\rho)^{-1}).$$

Or

$$\mathfrak{Re}((\sigma-\rho)^{-1}) = \frac{\sigma - \mathfrak{Re}(\rho)}{|\sigma-\rho|^2} > 0,$$

et l'absence de pôle de la fonction Γ sur le demi-plan $\{s \in \mathbb{C}, \mathfrak{Re}(s) > 0\}$ nous donnent donc

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) \leq \frac{1}{\sigma-1} + c_1 \log d_L + c_2 n_L$$

pour $2 \geq \sigma > 1$ et certaines constantes $c_1, c_2 > 0$.

Maintenant, si $\rho = \beta + i\gamma$ est un zéro non trivial de ζ_L avec $|\gamma| \geq \frac{1}{1+4\log d_L}$, alors en ignorant la somme qui est strictement positive, on trouve

$$\begin{aligned} -\mathfrak{Re}\frac{\zeta_L'}{\zeta_L}(\sigma+2i\gamma) &\leq \frac{1}{2}\log d_L + \mathfrak{Re}\left(\frac{1}{\sigma+2i\gamma-1} + \frac{1}{\sigma+2i\gamma}\right) + \mathfrak{Re}\frac{\gamma_L'}{\gamma_L}(\sigma+2i\gamma) \\ &\leq c_3 \log d_L + c_4 n_L \log(|\gamma|+2), \end{aligned}$$

et en ne gardant que la contribution de ρ dans la somme, on obtient

$$-\mathfrak{Re}\frac{\zeta_L'}{\zeta_L}(\sigma+i\gamma) \leq c_5 \log d_L + c_6 n_L \log(|\gamma|+2) - \frac{1}{\sigma-\beta}.$$

Rassemblant nos inégalités, on trouve que pour $2 \geq \sigma > 1$,

$$\frac{4}{\sigma-\beta} < \frac{3}{\sigma-1} + c_7(\log d_L + n_L \log(|\gamma|+2)).$$

Prenant $\sigma = 1 + (100c_7)^{-1}(\log d_L + n_L \log(|\gamma|+2))^{-1}$, on trouve

$$\frac{4}{\sigma-\beta} < 301 c_7(\log d_L + n_L \log(|\gamma|+2)),$$

soit

$$\begin{aligned} \beta &< \sigma - (1204 c_7(\log d_L + n_L \log(|\gamma|+2))^{-1} \\ &< 1 - c(\log d_L + n_L \log(|\gamma|+2))^{-1}. \end{aligned}$$

□

Lemme 10. *Si $n_L > 1$, ζ_L a au plus un zéro $\rho = \beta + i\gamma$ vérifiant $|\gamma| \leq (4 \log d_L)^{-1}$ et $\beta \geq 1 - (4 \log d_L)^{-1}$. Si ce zéro existe, il est simple et réel.*

Démonstration. On reprend la formule

$$\frac{\zeta_L'}{\zeta_L}(\sigma) = \frac{1}{2} \sum_{\rho} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}} \right) - \frac{1}{\sigma} - \frac{1}{\sigma - 1} - \frac{1}{2} \log d_L - \frac{\gamma_L'}{\gamma_L}(\sigma).$$

Pour $1 < \sigma \leq 2$, on obtient

$$\begin{aligned} \sum_{\rho} \frac{\sigma - \beta}{(\sigma - \beta)^2 + \gamma^2} &= \frac{1}{\sigma} + \frac{1}{\sigma - 1} + \frac{1}{2} \log d_L + \frac{\gamma_L'}{\gamma_L}(\sigma) + \frac{\zeta_L'}{\zeta_L}(\sigma) \\ &\leq \frac{1}{\sigma - 1} + \frac{1}{2} \log d_L \end{aligned}$$

car

$$\frac{\zeta_L'}{\zeta_L}(\sigma) \leq 0$$

et

$$\frac{1}{\sigma} + \frac{\gamma_L'}{\gamma_L}(\sigma) = \frac{1}{\sigma} - \frac{n_L}{2} \log \pi + \frac{r_1}{2} \frac{\Gamma'}{\Gamma} \left(\frac{\sigma}{2} \right) + \frac{r_2}{2} \frac{\Gamma'}{\Gamma} \left(\frac{\sigma + 1}{2} \right) < 0$$

pour $1 < \sigma \leq 1 + (\log 3)^{-1}$ (on peut vérifier cette inégalité numériquement par exemple).

Si $\rho = \beta + i\gamma$ est un zéro de ζ_L avec $\beta \geq 1 - (4 \log d_L)^{-1}$ et $|\gamma| \leq (4 \log d_L)^{-1}$, et supposons que $\gamma \neq 0$ ou bien que ρ est réel double, alors

$$2 \frac{\sigma - \beta}{(\sigma - \beta)^2 + \gamma^2} \leq \frac{1}{\sigma - 1} + \frac{1}{2} \log d_L$$

pour tout $\sigma \in]1, 2]$.

Mais pour $\sigma = 1 + (\log d_L)^{-1} \in]1, 2]$, on trouve alors

$$2 \frac{\sigma - \beta}{(\sigma - \beta)^2 + \gamma^2} \leq \frac{3}{2} \log d_L,$$

d'où

$$\frac{32}{17} \frac{1}{\sigma - \beta} < \frac{3}{2} \log d_L$$

car

$$|\gamma| \leq (4 \log d_L)^{-1} = \frac{1}{4}(\sigma - 1) < \frac{1}{4}(\sigma - \beta).$$

Ceci implique

$$\sigma - \beta > \frac{64}{51}(\log d_L)^{-1},$$

soit

$$\beta < 1 - (\frac{51}{13}\log d_L)^{-1} < 1 - (4\log d_L)^{-1},$$

une contradiction. □

On notera β_0 ce zéro exceptionnel, appelé zéro de Siegel [18].

6) Fin de la preuve

Théorème (Lagarias-Odlyzko, [4]). *Il existe une constante effectivement calculable $c > 0$ telle que, si $x \geq \exp(4n_L(\log d_L)^2)$, alors*

$$\psi_C(x) = \frac{|C|}{|G|}x - \frac{|C|}{|G|}\tilde{\chi}(g)\frac{x^{\beta_0}}{\beta_0} + R(x),$$

où $\tilde{\chi}$ est le caractère de H tel que $s \mapsto L(s, \chi, L/E)$ admette un zéro de Siegel en β_0, ce terme n'apparaissant pas si β_0 n'existe pas, et avec

$$|R(x)| \leq x\exp(-cn_L^{-1/2}(\log x)^{1/2}).$$

Démonstration. Si $\rho = \beta + i\gamma \neq \beta$ est un zéro non trivial de l'une des fonctions L précédemment traitées, avec $|\gamma| \leq T$, on a $|x^\rho| = x^\beta = xx^{\beta-1}$. Or si $|\gamma| \geq (1 + 4\log d_L)^{-1}$ alors

$$\begin{aligned}\beta - 1 &\leq -c(\log d_L + n_L\log(|\gamma| + 2))^{-1} \\ &\leq -c'(\log d_L + n_L\log T)^{-1} \\ &= -\frac{c'}{\log(d_L T^{n_L})}\end{aligned}$$

pour une autre constante $c' > 0$, et si $|\gamma| \leq (4\log d_L)^{-1}$ alors

$$\begin{aligned}\beta - 1 &\leq -(4\log d_L)^{-1} \\ &\leq -\frac{c''}{\log(d_L T^{n_L})}\end{aligned}$$

car $\rho \neq \beta_0$, pour une certaine constante $c'' > 0$ bien adaptée (on a $T \geq 2$).

18. Carl Ludwig Siegel (1896-1981)

Dans tous les cas, on obtient

$$|x^\rho| \leq x \exp\left(-c'' \frac{\log x}{\log(d_L T^{n_L})}\right).$$

De plus,

$$\begin{aligned}\sum_{\chi\in\hat{H}} \sum_{\substack{\rho \\ |\gamma|\leq T \\ |\rho|\geq 1/2}} \left|\frac{1}{\rho}\right| &\ll \sum_{\chi\in\hat{H}} \sum_{j=1}^{\lfloor T\rfloor+1} \frac{n_\chi(j)+n_\chi(-j)}{j} \\ &\ll \sum_{\chi\in\hat{H}} \sum_{j=1}^{\lfloor T\rfloor+1} \frac{2\log A(\chi)+2n_E\log(|j|+2)}{j} \\ &\ll \log T\log d_L + (\log T)^2 n_L = \log T \log(d_L T^{n_L}),\end{aligned}$$

et

$$\begin{aligned}\sum_{\chi\in\hat{H}} \sum_{\substack{\rho\neq 1-\beta_0 \\ |\rho|<1/2}} \left(\left|\frac{x^\rho}{\rho}\right| + \frac{1}{|\rho|}\right) &\ll x^{1/2} \sum_{\chi\in\hat{H}} \sum_{\substack{\rho\neq 1-\beta_0 \\ |\rho|<1/2}} \frac{1}{|\rho|} \\ &\leq x^{1/2} \sum_{\chi\in\hat{H}} \sum_{\substack{\rho\neq 1-\beta_0 \\ |\rho|<1/2}} (4\log d_L) \\ &\leq 4\log d_L x^{1/2} \sum_{\chi\in\hat{H}} n_\chi(0) \ll x^{1/2}(\log d_L)^2 + n_L \log d_L x^{1/2}.\end{aligned}$$

Or par un résultat classique de la théorie de Minkowski on a $n_L \ll \log d_L$ (si jamais $\log d_L = 0$ c'est que $L = \mathbb{Q}$ et cette somme est nulle car ζ n'a pas de zéros vérifiant $|\gamma| \leq 14$).

On a donc

$$\sum_{\chi\in\hat{H}} \sum_{\substack{\rho\neq 1-\beta_0 \\ |\rho|<1/2}} \left(\left|\frac{x^\rho}{\rho}\right| + \frac{1}{|\rho|}\right) \ll x^{1/2}(\log d_L)^2.$$

Enfin le dernier terme de la somme à majorer est

$$\frac{x^{1-\beta_0}}{1-\beta_0} - \frac{1}{1-\beta_0} = x^\sigma \log x \ll x^{1/2}\log x$$

pour un certain $\sigma \in [0, 1-\beta_0]$ par le théorème des accroissements finis.

On obtient ainsi

$$S(x,T)-\frac{|C|}{|G|}\tilde{\chi}(g)\frac{x^{\beta_0}}{\beta_0}=\frac{|C|}{|G|}\left(\sum_{\chi\in\hat{H}}\overline{\chi(g)}\left(\sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho}-\sum_{\substack{\rho\\|\rho|<1/2}}\frac{1}{\rho}\right)-\tilde{\chi}(g)\frac{x^{\beta_0}}{\beta_0}\right)$$
$$\ll\frac{|C|}{|G|}\left(x\exp\left(-c''\frac{\log x}{\log(d_LT^{n_L})}\right)\log T\log(d_LT^{n_L})+x^{1/2}(\log d_L)^2\right).$$

Ainsi,

$$\psi_C(x)-\frac{|C|}{|G|}x+\frac{|C|}{|G|}\tilde{\chi}(g)\frac{x^{\beta_0}}{\beta_0}\ll\frac{|C|}{|G|}\left(\frac{x\log x+T}{T}\log d_L+n_L\log x+\frac{n_Lx\log x\log T}{T}\right.$$
$$\left.+x^{1/2}(\log d_L)^2+x\exp\left(-c''\frac{\log x}{\log(d_LT^{n_L})}\right)\log T\log(d_LT^{n_L})\right)$$
$$+\log x\log d_L+n_KxT^{-1}(\log x)^2.$$

Prenant

$$T=\exp(n_L(\log x)^{1/2}-\log d_L)$$

on a $T\geq d_L\geq 2$ si $x\geq\exp(4n_L(\log d_L)^2)$, et on obtient finalement

$$\psi_C(x)-\frac{|C|}{|G|}x+\frac{|C|}{|G|}\tilde{\chi}(g)\frac{x^{\beta_0}}{\beta_0}\ll x\exp(-c''n_L^{-1/2}(\log x)^{1/2}).$$

□

Finalement, pour estimer $\pi_C(x)$, on procède par sommation par parties. Pour cela, introduisons la fonction sommatoire des $\log N(\mathfrak{p})$ pour $\sigma_{\mathfrak{p}}=C$:

$$\theta_C(x)=\sum_{\substack{\mathfrak{p}\\\sigma_{\mathfrak{p}}=C\\N(\mathfrak{p})\leq x}}\log N(\mathfrak{p}).$$

On a alors

$$|\psi_C(x)-\theta_C(x)|=\sum_{\substack{\mathfrak{p},m\geq 2\\\sigma_{\mathfrak{p}}=C\\N(\mathfrak{p}^m)\leq x}}\log N(\mathfrak{p})$$
$$\leq\log\sqrt{x}|\{\mathfrak{p},\exists m\geq 2,\sigma_{\mathfrak{p}}=C,N(\mathfrak{p}^m)\leq x\}|$$
$$\leq\pi_C(\sqrt{x})\log\sqrt{x}.$$

Or

$$\pi_C(x)=|\{\mathfrak{p},\sigma_{\mathfrak{p}}=C,N(\mathfrak{p})\leq x\}|\leq n_K\pi(x)=O\left(n_K\frac{x}{\log x}\right).$$

Donc

$$|\psi_C(x) - \theta_C(x)| \ll n_K x^{1/2}$$

et le théorème précédent est valable en remplaçant $\psi_C(x)$ par $\theta_C(x)$.

Posant

$$\theta_C(x) = \sum_{n \leq x} a_n \log n,$$

où $a_n = |\{\mathfrak{p}, \Sigma_{\mathfrak{p}} = C, N(\mathfrak{p}) = n\}|$, on trouve par sommation par parties

$$\begin{aligned} \pi_C(x) &= \sum_{n \leq x} a_n \log n \times \frac{1}{\log n} \\ &= \frac{\theta_C(x)}{\log x} + \int_2^x \frac{\theta_C(t)}{t(\log t)^2} dt. \end{aligned}$$

Mais

$$\int_2^x \frac{\theta_C(t)}{t(\log t)^2} dt \leq \int_2^{\sqrt{x}} \frac{\theta_C(t)}{t(\log 2)^2} dt + \int_{\sqrt{x}}^x \frac{\theta_C(x)}{t(\log \sqrt{x})^2} dt,$$

et de manière évidente,

$$\theta_C(x) \leq n_K \theta(x) \ll n_K x,$$

où θ est la traditionnelle fonction θ de Tchebychev [19]. On a donc

$$\int_2^x \frac{\theta_C(t)}{t(\log t)^2} dt \ll n_K x^{1/2} + \frac{x}{(\log x)^2}.$$

Grâce au théorème précédent, et à l'équivalent

$$\frac{x}{\log x} \underset{x \to +\infty}{\sim} \mathrm{Li}(x),$$

on obtient finalement notre version effective du théorème de Chebotarev :

Théorème (Chebotarev, version effective)**.** *Il existe des constantes effectivement calculables $c_1, c_2 > 0$ telles que si $x \geq \exp(4n_L(\log d_L)^2)$ alors*

$$\left| \pi_C(x) - \frac{|C|}{|G|} \mathrm{Li}(x) \right| \leq \frac{|C|}{|G|} \mathrm{Li}(x^{\beta_0}) + c_1 x \exp(-c_2 n_L^{-1/2} (\log x)^{1/2}).$$

Dans son article [14], Winckler a explicité des constantes admissibles dans le résultat de Lagarias-Odlyzko.

19. Pafnouti Lvovitch Tchebychev (1821-1894)

Théorème (Winckler, [14]). *Pour tout* $x \geq \exp(8n_L(\log(150867d_L^{44/5}))^2)$, *on a*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li}(x)\right| \leq \frac{|C|}{|G|}\operatorname{Li}(x^{\beta_0}) + C_0 x \exp\left(-\frac{1}{99}n_L^{-1/2}(\log x)^{1/2}\right),$$

avec $C_0 = 783846699796966$.

Signalons finalement une généralisation des résultats de Lagarias et Odlyzko due à Serre dans [9] :

Par linéarité, il est évident que le théorème se généralise à toute partie de G qui est union de classes de conjugaison. Plus généralement, pour toute fonction centrale f définie sur G, on peut définir

$$\pi_f(x) = \sum_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq x}} f(\sigma_{\mathfrak{p}}).$$

Le théorème de Chebotarev se transpose alors naturellement à π_f. En effet, $\pi_f(x)$ est égal à

$$\sum_{i=1}^{k} \lambda_i \pi_{C_i}(x),$$

où $C_1, \ldots, C_k$ sont les classes de conjugaison de G et λ_i est la valeur prise par f sur la classe C_i. Il n'y a plus qu'à remplacer la quantité $\frac{|C|}{|G|}$ par

$$\frac{1}{|G|}\sum_{g \in G} f(g) = \sum_{i=1}^{k} \lambda_i \frac{|C_i|}{|G|}.$$

7) Améliorations conditionnelles à GRH et la conjecture d'Artin

Le plus gros apport à nos estimations est l'utilisation de l'hypothèse de Riemann généralisée, qui affirme que les zéros non triviaux de nos fonctions L ont pour partie réelle 1/2. En fait, dans le cas qui nous intéresse, il suffit de supposer l'hypothèse de Riemann pour la fonction ζ_L.

Théorème (GRH). *Supposons que la fonction* ζ_L *vérifie l'hypothèse de Riemann, alors pour* $x \geq 2$,

$$\psi_C(x) - \frac{|C|}{|G|}x \ll \frac{|C|}{|G|}x^{1/2}\log x \log(d_L x^{n_L}) + \log x \log d_L.$$

Démonstration. Sous l'hypothèse de Riemann, le zéro de Siegel β_0 n'existe pas. Pour tout $\chi \in \hat{H}$, on obtient

$$\begin{aligned}\left|\sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} + \sum_{|\rho|<1/2} \frac{1}{\rho}\right| &\leq x^{1/2} \sum_{\substack{\rho \\ |\gamma|<T}} \frac{1}{|\rho|} \\ &\ll x^{1/2} \sum_{j=1}^{\lfloor T \rfloor} \frac{n_\chi(j)}{j} \\ &\ll x^{1/2} \log T(\log A(\chi) + n_E \log T).\end{aligned}$$

Ceci donne immédiatement

$$S(x,T) \ll \frac{|C|}{|G|} x^{1/2} \log T(\log d_L + n_L \log T).$$

Si on prend $T = x^{1/2} + 1$, on obtient

$$S(x,T) \ll \frac{|C|}{|G|} x^{1/2} \log(d_L x^{n_L}) \log x,$$

puis par la formule explicite,

$$\psi_C(x) - \frac{|C|}{|G|} x \ll \frac{|C|}{|G|} x^{1/2} \log x \log(d_L x^{n_L}) + \log x \log d_L.$$

□

Dans son article [9], Serre parvient à éliminer le terme $\log x \log d_L$ dans le terme d'erreur. En effet, celui-ci provient de l'estimation grossière

$$\sum_{\mathfrak{p} \text{ ramifié}} \log N(\mathfrak{p}) \leq \log d_L$$

au tout début de la preuve. On peut en fait améliorer cette majoration en étudiant plus précisément les degrés de ramification dans les corps locaux.

Proposition (Serre, [9] 1.3 Prop 5)**.** *On a*

$$\sum_{\mathfrak{p} \text{ } ramifié} \log N(\mathfrak{p}) \leq \frac{2}{|G|} \log d_L.$$

Ceci nous permet d'absorber le terme $\frac{2}{|G|} \log d_L$ dans le terme principal. On obtient donc finalement le théorème suivant.

Théorème (Chebotarev effectif sous GRH)**.** *Supposons que la fonction ζ_L vérifie l'hypothèse de Riemann, alors pour $x \geq 2$,*

$$\psi_C(x) - \frac{|C|}{|G|}x \ll \frac{|C|}{|G|}x^{1/2}\log x \log(d_L x^{n_L}).$$

Remarque. On peut même se passer de cette majoration et garder le terme

$$\sum_{\mathfrak{p} \text{ ramifié}} \log N(\mathfrak{p}) = \log M,$$

où M est le produit des premiers ramifiés de K. C'est ce que font [1] ou [7] par exemple.

La conjecture d'Artin, elle, permet de mener le raisonnement directement sur les fonctions L de l'extension L/K, sans avoir à passer par les fonctions L de Hecke. En effet, le développement en produit de Hadamard de

$$\Lambda(s, \chi, L/K)$$

ne fera pas intervenir de pôle que l'on ne sait pas contrôler. De plus, les majorations individuelles font intervenir la constante n_K plutôt que n_E, qui lui est supérieure. Mais au moment de sommer les estimations, on obtient dans tous les cas la quantité n_L. Il n'y a donc pas de gain significatif ici, hormis le fait de simplifier légèrement la preuve.

Remarque. Il faut tout de même parvenir à montrer que les fonctions L d'Artin (ou plus précisément les fonctions Λ) sont d'ordre 1. Ceci peut se faire en utilisant de nouveau le théorème de Brauer (en fin de I.2)).

Cependant, la conjecture d'Artin permet à Murty-Murty-Saradha de montrer la majoration légèrement plus précise suivante, grâce à l'inégalité de Cauchy-Schwarz [20] (voir [7]).

Théorème (Murty-Murty, [7])**.** *Supposons l'hypothèse de Riemann généralisée et la conjecture d'Artin. Alors pour toute réunion D de classes de conjugaison de G, on a*

$$\pi_D(x) - \frac{|D|}{|G|}\operatorname{Li}(x) \ll |D|^{1/2}x^{1/2}\log(d_L x^{n_L}).$$

Dans son article [1], Bellaïche propose une amélioration de cette méthode, en introduisant un invariant du groupe G, qui permet parfois d'obtenir des majorations plus fines. C'est ce que nous allons rapidement présenter dans la prochaine partie.

20. Hermann Amandus Schwarz (1843-1921)

III Améliorations dues à Bellaïche

1) Complexité de Littlewood

Dans toute cette partie, G désigne un groupe fini. Pour donner des versions plus précises du théorème de Chebotarev, Bellaïche introduit dans [1] la notion de complexité de Littlewood [21] d'une réunion de classes de conjugaison de G.

Définition. La **complexité de Littlewood** de la fonction centrale f est

$$\lambda(f) = \sum_{\chi \in \hat{G}} |\hat{f}(\chi)| \deg(\chi),$$

où $\hat{f}(\chi)$ est la composante de f selon χ dans la décomposition de f dans la base $\hat{G}$ de $\mathbb{C}^G$, ou de manière équivalente

$$\hat{f}(\chi) = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)}.$$

Si D est une réunion de classes de conjugaison de G, on notera $\lambda(D)$ pour $\lambda(\mathbf{1}_D)$.

Dans les énoncés du théorème de Chebotarev que nous verrons dans cette partie, nous aurons également besoin des quantités suivantes.

Définition. Si f est une fonction centrale sur G, on note sa valeur moyenne

$$\mu(f) = \frac{1}{|G|} \sum_{g \in G} f(g).$$

Soit maintenant D une réunion de classes de conjugaison de G. On définit alors

$$\varphi(D) = \inf_f \frac{\lambda(f)}{\mu(f)},$$

21. John Edensor Littlewood (1885-1977)

où la borne inférieure est prise sur les fonctions centrales f à valeurs réelles telles que $f(g) > 0 \Rightarrow g \in D$ et $\mu(f) > 0$.

La définition de la quantité $\varphi(f)$ est motivée par la remarque suivante. Si G est le groupe de Galois d'une extension L/K de corps de nombres, et f est une fonction centrale comme à la fin de la définition précédente, la positivité de $\pi_f(x)$ (voir la fin de II.6)) entraîne la positivité de $\pi_D(x)$. Le théorème de Chebotarev que l'on peut obtenir pour la fonction f entraîne ainsi une borne sur le premier $\mathfrak{p}$ (non ramifié) de K de plus petite norme tel que $\sigma_\mathfrak{p} \in D$. La borne inférieure est prise afin d'optimiser cette borne. Nous y reviendrons plus précisément dans la partie suivante. Notons déjà que cette notion n'est pas vide de sens grâce à la proposition suivante.

Proposition. *La borne inférieure définissant $\varphi(D)$ est atteinte par une fonction centrale f_D sur G, unique à multiplication par un réel strictement positif près. En particulier $\varphi(D) > 0$.*

Démonstration. Définissons l'ensemble E des fonctions centrales f à valeurs réelles telles que $f(g) > 0$ implique $g \in D$, $\mu(f) > 0$ et telles que

$$\sum_{g \in G} |f(g)| = 1,$$

c'est-à-dire de norme L^1 valant 1. Comme toute fonction centrale satisfaisant les conditions définissant $\varphi(D)$ a un unique multiple dans E, il suffit de montrer que la fonctionnelle

$$q : f \mapsto \frac{\lambda(f)}{\mu(f)}$$

admet un unique minimum sur E. On voit que E est un ensemble convexe, et que q est strictement convexe, ce qui assure l'unicité du minimum si celui-ci est atteint.

Soit $\varepsilon > 0$. Notons E_ε le sous-ensemble des éléments f de E tels que $\mu(f) \geq \varepsilon$. E_ε est compact car fermé dans la sphère unité de $\mathbb{C}^G$ pour la norme L^1, et le minimum de q sur E_ε est atteint. Or pour $f \in E \setminus E_\varepsilon$, on a

$$\frac{\lambda(f)}{\mu(f)} > \frac{\lambda(f)}{\varepsilon} \geq \frac{||f||_\infty}{\varepsilon} \geq \frac{1}{|G|\varepsilon},$$

où on a utilisé que

$$1 = ||f||_1 \leq |G| ||f||_\infty$$

et le fait que

$$||f||_\infty \leq \lambda(f),$$

ce qui se montre facilement en décomposant f dans la base $\hat{G}$. Ceci montre que le minimum de q sur E est celui sur E_ε pour ε suffisamment petit, qui est donc atteint.

Enfin on a

$$\varphi(D) = \frac{\lambda(f_D)}{\mu(f_D)} > 0.$$

□

Donnons enfin deux majorations de la complexité de Littlewood, qui correspondront respectivement aux versions de Lagarias-Odlyzko-Serre et de Murty-Murty-Saradha du théorème de Chebotarev.

Proposition. *Soit D une classe de conjugaison de G. Alors on a*

$$\lambda(D) \leq |D| \text{ (majoration triviale)}$$

et

$$\lambda(D) \leq |D|^{1/2} \text{ (majoration à la Cauchy-Schwarz).}$$

Démonstration. La première majoration découle bien évidemment de la première. On va montrer plus généralement que

$$\lambda(f) \leq ||f||_2 |G|^{1/2}$$

pour toute fonction centrale f sur G. La seconde majoration en découle en prenant $f = \mathbf{1}_D$.

Soit donc f une fonction centrale sur G. L'inégalité de Cauchy-Schwarz nous donne

$$\lambda(f) = \sum_{\chi \hat{G}} \hat{f}(\chi) \deg(\chi) \leq \left(\sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^2 \right)^{1/2} \left(\sum_{\chi \in \hat{G}} \deg(\chi)^2 \right)^{1/2}.$$

Or, l'égalité de Parseval nous donne que la première quantité est $||f||_2$, tandis qu'un résultat standard sur les représentations linéaires de G nous donne que la seconde vaut $|G|^{1/2}$. □

Pour plus de propriétés des fonctions λ et φ relativement au passage au quotient, à la restriction à un sous-groupe, à l'induction, ou encore à la précomposition par certaines bijections, et pour des exemples de calculs, on renvoie à [1].

2) Versions affinées du théorème de Chebotarev

On considère une extension galoisienne $L/\mathbb{Q}$ où L est un corps de nombres. On note $G = \mathrm{Gal}(L/\mathbb{Q})$ et f une fonction centrale sur G. Par support spectral de f, on entend l'ensemble des caractères irréductibles χ de G tels que $\langle f, \chi\rangle \neq 0$. Enfin on note M le produit des nombres premiers ramifiés dans L. Voici maintenant la version du théorème de Chebotarev utilisée par Bellaïche dans [1] :

Théorème (Chebotarev effectif selon Bellaïche)**.** *On suppose l'hypothèse de Riemann généralisée et la conjecture d'Artin pour les fonctions L associées aux représentations irréductibles dans le support spectral de f. Alors il existe une constante absolue $c > 0$ (qui ne dépend pas de L) telle que pour $x \geq 3$,*

$$|\pi_f(x) - \mu(f)\,\mathrm{Li}(x)| < cx^{1/2}\lambda(f)(\log x + \log M + \log|G|).$$

Dans le cas d'une réunion D de classes de conjugaison de G on obtient en particulier :

Corollaire. *On suppose l'hypothèse de Riemann généralisée et la conjecture d'Artin pour les fonctions L associées aux représentations irréductibles dans le support spectral de $\mathbf{1}_D$. Alors il existe une constante absolue $c > 0$ telle que pour $x \geq 3$,*

$$|\pi_D(x) - \frac{|D|}{|G|}\,\mathrm{Li}(x)| < cx^{1/2}\lambda(D)(\log x + \log M + \log|G|).$$

La preuve de cette version du théorème de Chebotarev est dans le même esprit que celle exposée en II. On commence par poser

$$\psi_f(x) = \sum_{p^m \leq x, p\nmid M} f(\sigma_p^m)\log p,$$

et on établit comme précédemment une formule explicite pour cette quantité, en utilisant les propriétés analytiques de nos fonctions L. En décomposant f sous la forme

$$f = \sum_{\chi\in\hat{G}} c_\chi \chi,$$

on voit qu'il suffit de montrer le théorème pour les $\chi \in \hat{G}$. En notant que

$$\mu(\chi) = \begin{cases} 1 \text{ si } \chi = \chi_0 \\ 0 \text{ sinon} \end{cases},$$

on montre alors que

$$|\psi_\chi(x) - \mu(\chi)x| < cx^{1/2}\log x \log(x^{\deg(\chi)}\mathfrak{f}_\chi),$$

où $\mathfrak{f}_\chi$ est comme en I.3) le conducteur d'Artin de χ. Or, on peut montrer que

$$\log f_\chi \leq 2\deg(\chi)(\log M + \log|G|),$$

ce qui donne

$$|\psi_\chi(x) - \mu(\chi)x| < c'x^{1/2}\log x\ \deg(\chi)(\log x + \log M + \log|G|).$$

En sommant et en se souvenant que

$$\lambda(f) = \sum_{\chi\in\hat{G}} |c_\chi|\deg(\chi),$$

on obtient

$$|\psi_f(x) - \mu(f)x| < c''x^{1/2}\lambda(f)\log x(\log x + \log M + \log|G|),$$

et finalement, par un argument de sommation par parties on obtient l'estimation voulue pour $\pi_f(x)$.

Remarque. En fait, on peut obtenir un résultat similaire pour n'importe quelle décomposition en combinaison linéaire de caractères, non nécessairement irréductibles, puisqu'on n'a pas utilisé l'irréductibilité des caractères ici. Ceci permet dans certains cas de se passer de la conjecture d'Artin si on sait la démontrer pour les fonctions L associées aux représentations en question.

Comme annoncé précédemment, on retrouve exactement nos versions précédentes du théorème de Chebotarev à l'aide des majorations données en III.1), sous les formes suivantes.

Corollaire (Lagarias-Odlyzko-Serre)**.** *On suppose l'hypothèse de Riemann généralisée et la conjecture d'Artin pour les fonctions L associées aux représentations irréductibles dans le support spectral de* $\mathbf{1}_D$*. Alors il existe une constante absolue* $c > 0$ *telle que pour* $x \geq 3$*,*

$$|\pi_D(x) - \frac{|D|}{|G|}\operatorname{Li}(x)| < cx^{1/2}|D|(\log x + \log M + \log|G|).$$

Corollaire (Murty-Murty-Saradha)**.** *On suppose l'hypothèse de Riemann généralisée et la conjecture d'Artin pour les fonctions L associées aux représentations irréductibles dans le support spectral de* $\mathbf{1}_D$*. Alors il existe une constante absolue* $c > 0$ *telle que pour* $x \geq 3$*,*

$$|\pi_D(x) - \frac{|D|}{|G|}\operatorname{Li}(x)| < cx^{1/2}|D|^{1/2}(\log x + \log M + \log|G|).$$

Remarque. Les termes d'erreur de nos versions précédentes du théorème de Chebotarev ont un terme logarithmique de la forme $\frac{\log(d_L)}{|G|} + \log x$. Mais on a vu que $\frac{\log d_L}{|G|}$ était comparable à $\log M$ (voir [9]). Ainsi ce terme logarithmique est meilleur d'un terme $\log |G|$, qui est cependant négligeable en pratique.

IV Applications des versions effectives du théorème de Chebotarev

1) Plus petit idéal premier dans un ensemble frobénien

L'utilisation la plus évidente du théorème de Chebotarev est de garantir l'existence d'une infinité de premiers non ramifiés dont les éléments de Frobenius forment une classe de conjugaison fixée à l'avance. Avec nos versions effectives de ce théorème, on peut donner une majoration de la plus petite norme d'un tel premier.

Proposition. *Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G et soit C une classe de conjugaison de G. Alors il existe un idéal premier $\mathfrak{p}$ de K non ramifié dans L tel que $\sigma_{\mathfrak{p}} = C$ et vérifiant*

$$N(\mathfrak{p}) \ll \exp(4n_L(\log d_L)^2).$$

Démonstration. Il suffit de chercher quand est-ce que $\pi_C(x) > 0$, et même plus simplement quand est-ce que $\psi_C(x) > 0$. Pour cela, il suffit de regarder quand est-ce que le terme $\frac{|C|}{|G|}x$ est strictement plus grand que le terme d'erreur.

Rappelons que l'inégalité que nous avons obtenu pour le théorème de Chebotarev est valable pour $x \geq \exp(4n_L(\log d_L)^2)$. Il suffit donc, pour de tels x, que

$$\frac{|C|}{|G|}x > \frac{|C|}{|G|}\frac{x^{\beta_0}}{\beta_0} + x\exp(-cn_L^{-1/2}(\log x)^{1/2}),$$

soit

$$\frac{x^{\beta_0-1}}{\beta_0} + \frac{|G|}{|C|}\exp(-cn_L^{-1/2}(\log x)^{1/2}) < 1.$$

Par exemple, dès que

$$\frac{x^{\beta_0-1}}{\beta_0} < \frac{1}{2}$$

et

$$\frac{|G|}{|C|}\exp(-cn_L^{-1/2}(\log x)^{1/2}) < \frac{1}{2},$$

c'est-à-dire

$$x > \left(\frac{2}{\beta_0}\right)^{1-\beta_0}$$

et

$$cn_L^{-1/2}(\log x)^{1/2} > \log\left(\frac{2|G|}{|C|}\right).$$

Comme β_0 ne s'approche jamais de 0 (rappelons que $\beta_0 \in [1-(4\log d_L)^{-1}, 1[$), seule la seconde inégalité nous intéresse. Celle-ci se réécrit encore

$$x > \exp\left(c^{-2}n_L\log^2\left(\frac{2|G|}{|C|}\right)\right).$$

Quitte à augmenter la constante c, on peut la supposer supérieure à 1, de sorte que x de l'ordre de $\exp(n_L^{1+\varepsilon})$, avec $\varepsilon > 0$ convient. Mais comme

$$\exp(n_L^{1+\varepsilon}) \leq \exp(4n_L(\log d_L)^2)$$

pour $\varepsilon > 0$ suffisamment petit, on obtient bien que le terme d'erreur est strictement inférieur au terme principal dès que l'inégalité est vérifiée, ce qui nous donne le résultat. □

Cette majoration n'est bien entendu pas du tout optimale, mais permet d'obtenir une première borne non triviale pour l'existence de premiers dont les Frobenius forment une certaine classe de conjugaison. En prenant le cas particulier $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta_m)$, où ζ_m est une racine primitive m-ième de l'unité dans $\mathbb{C}$, on obtient une version faible du théorème de Linnik.

Théorème. *Soient a et m des entiers premiers entre eux avec $1 \leq a \leq m$. Alors, le plus petit nombre premier p tel que $p = a \mod m$ vérifie*

$$p \ll \exp(4\varphi(m)(m\log m)^2).$$

Remarque. Le théorème de Linnik donne une estimation bien plus forte : le plus petit premier congru à a modulo m est $\ll m^L$, où L est une constante ne dépendant que de m, que l'on conjecture égale à 2 pour tout m.

Avec nos versions conditionnelles, on obtient la majoration plus forte suivante :

Proposition (Bellaïche, [1]). *Soit $L/\mathbb{Q}$ une extension galoisienne de groupe de Galois G, D une union de classes de conjugaison de G et M le produit des nombres premiers ramifiés dans L. Supposons vraies l'hypothèse de Riemann généralisée et la conjecture d'Artin pour les représentations irréductibles de G. Alors le plus petit nombre premier p tel que $\sigma_p \subset D$ vérifie*

$$p \ll \varphi(D)^2(\log M + \log |G|)^2$$

La preuve, que nous ne reproduisons pas ici, consiste à introduire la fonction auxiliaire

$$x \mapsto \sum_{p^k \leq x, p \nmid M} f_D(\sigma_p^k)(x - n),$$

où f_D est comme précédemment la fonction centrale réalisant le minimum dans la définition de $\varphi(D)$, et à utiliser les mêmes ingrédients que la preuve du théorème de Chebotarev pour estimer cette fonction, puis utiliser des estimations à la Tchebychev.

Pour les premiers en progressions arithmétiques, on trouve donc, en utilisant le fait que notre partie D est ici un singleton :

Théorème. *Soient a et m des entiers premiers entre eux avec $1 \leq a \leq m$. Supposons vraies l'hypothèse de Riemann généralisée pour les fonctions L de Dirichlet modulo m. Alors le plus petit nombre premier tel que $p = a \mod m$ vérifie*

$$p \ll \varphi(m)^2(\log \varphi(m) + \log rad(m))^2,$$

où $rad(m)$ est le produit des nombres premiers divisant m.

Une autre application directe du théorème de Chebotarev est l'étude des racines modulaires des polynômes irréductibles à coefficients entiers.

Soit donc f un élément de $\mathbb{Z}[X]$, irréductible, unitaire, et de degré n. L'extension $L/\mathbb{Q}$ est galoisienne, où L est le corps de décomposition de f sur $\mathbb{Q}$. On voit facilement que le nombre de racines de f modulo le nombre premier p est égal au nombre de points fixes de σ_p dans son action sur les racines de f dans L. En effet, les racines de f dans L sont en fait dans $\mathcal{O}_L$ puisque f est unitaire, et si α est une telle racine, $\sigma_p(\alpha) = \alpha^{|\mathcal{O}_L/\mathfrak{p}|} \mod \mathfrak{p}$, où $\mathfrak{p}$ est un premier de L au-dessus de p. Mais σ_p est trivial si et seulement si p est totalement ramifié dans L, et donc $|\mathcal{O}_L/\mathfrak{p}| = p$. En particulier on a

$$\alpha = \alpha^p \mod p,$$

ce qui veut exactement dire que $\alpha \bmod p \in \mathbb{F}_p$.

À l'aide du calcul explicite de la complexité de Littlewood de parties de $\mathfrak{S}_n$ de la forme « ensemble des permutations ayant k points fixes », et la proposition précédente, Bellaïche obtient alors (avec la majoration évidente $\log n! \leq n \log n$) :

Théorème (Bellaïche, [1]). *Soit M le produit des nombres premiers divisant le discriminant de f. En supposant l'hypothèse de Riemann généralisée et la conjecture d'Artin pour les représentations irréductibles de $Gal(L/\mathbb{Q})$ on a :*

i) Il existe un nombre premier $p \ll n^2(\log M + n \log n)^2$ ne divisant pas M tel que f admet au moins une racine modulo p.

ii) Il existe un nombre premier $p \ll n^4(\log M + n \log n)^2$ ne divisant pas M tel que f admet au moins deux racines modulo p.

iii) Il existe un nombre premier $p \ll n^4(\log M + n \log n)^2$ ne divisant pas M tel que f n'admet aucune racine modulo p.

Remarque. On aurait pu étudier un corps de rupture de f au lieu de son corps de décomposition. On aurait gagné sur le degré de l'extension étudiée, mais celle-ci n'a en général aucune raison d'être galoisienne. Notons qu'un résultat conditionnel proche de i) a été obtenu par Weinberger, Adleman et Odlyzko en utilisant le théorème des idéaux premiers dans un tel corps de rupture.

Donnons enfin en dernier exemple d'application directe du théorème de Chebotarev le résultat suivant :

Théorème (Bellaïche, [1]). *Soit P un polynôme unitaire irréductible à coefficients de degré n et soit M le produit des nombres premiers divisant le discriminant de P. En supposant l'hypothèse de Riemann généralisée et la conjecture d'Artin, s'il existe un nombre premier p ne divisant pas M tel que $P \bmod p$ est irréductible, alors il existe un tel nombre premier vérifiant*

$$p \ll 4^{n-1}(\log M + n \log n)^2.$$

2) Application aux courbes elliptiques

Pour conclure ce mémoire, on donne une dernière application du théorème de Chebotarev à l'étude des courbes elliptiques. Pour une introduction très complète aux courbes elliptiques, on recommande le livre [11] de Silverman. La conjecture de Koblitz est l'énoncé suivant :

Conjecture (Koblitz). *Soit E une courbe elliptique sur $\mathbb{Q}$ sans multiplication complexe et qui n'est isogène à aucune courbe elliptique possédant des $\mathbb{Q}$-points de torsion. Notons M le produit des nombres premiers de mauvaise réduction pour E. Alors*

$$|\{p \leq x, p \nmid M, |E(\mathbb{F}_p)| \text{ est premier}\}| \underset{x\to+\infty}{\sim} C_E \frac{x}{(\log x)^2},$$

où $C_E > 0$ est une constante ne dépendant que de E.

La conjecture prévoit même une formule pour C_E. Tout d'abord fixons quelques notations. Pour tout nombre premier ℓ, notons ρ_ℓ la représentation galoisienne

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

associée aux points de ℓ-torsion de E et G_ℓ son image. On fixe un entier $N \geq 1$ tel que l'image de $\prod_\ell \rho_\ell$ soit

$$\prod_{p\nmid N} G_\ell \times G_N,$$

où G_N est l'image de $\prod_{\ell\mid N} \rho$ dans $\prod_{\ell\mid N} \mathrm{GL}_2(\mathbb{F}_\ell)$. Enfin pour ℓ premier ne divisant pas N, on note D_ℓ l'ensemble des matrices de G_ℓ qui n'admettent pas 1 pour valeur propre, et D_N l'ensemble des matrices de G_N dont la réduction modulo tout $\ell \mid N$ n'admet pas 1 pour valeur propre. Alors la conjecture de Koblitz prévoit que

$$C_E = \frac{|D_N|}{|G_N| \prod_{\ell\mid N}\left(1-\frac{1}{\ell}\right)} \prod_{\ell\nmid N} \frac{|D_\ell|}{|G_\ell|\left(1-\frac{1}{\ell}\right)}.$$

Dans son article [1], Bellaïche s'intéresse également au cas d'une infinité d'extensions galoisiennes et obtient un résultat dans la direction de cette conjecture. Par une méthode de grand crible et sa version effective du théorème de Chebotarev, il obtient le résultat suivant.

Théorème (Bellaïche, [1]). *Soient $N \geq 1$ un entier sans facteurs carrés, Λ l'ensemble des nombres premiers ne divisant pas N et pour tout $\nu \in \Lambda$, $L_\nu/\mathbb{Q}$ une extension galoisienne finie de groupe de Galois G_ν, non ramifiée hors des nombres premiers divisant N, et D_ν une partie de G_ν stable par conjugaison. On pose*

$$\tilde{D} = \{p, p \nmid N, \forall \nu \in \Lambda, \sigma_{p,G_\nu} \subset D_\nu\}$$

et

$$\pi_D(x) = |\tilde{D} \cap [1, x]|.$$

On fait les hypothèses suivantes :

i) On a $\log |G_\ell| = O(\log \ell)$.

ii) Pour tout $\ell \in \Lambda$, $\ell - P \leq \frac{|G_\ell|}{|G_\ell \backslash D_\ell|} \leq \ell + P$, *où* $P > 0$ *est une constante.*

iii) Pour tout $\ell \in \Lambda$, $\lambda(D_\ell) \leq R\ell^\beta$, *où* $R > 0$ *et* $\beta \in [0, 1]$ *sont des constantes.*

iv) Pour tout sous-ensemble fini m *de* Λ *ne contenant pas* N, *l'application naturelle* $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_{\ell \in m} G_\ell$ *est surjective.*

Alors en posant C *définit comme ci-dessus, et en supposant l'hypothèse de Riemann généralisée et la conjecture d'Artin, on a*

$$\pi_D(x) < (4\beta + 4 + o(1))C\frac{x}{(\log x)^2}.$$

Il en déduit alors

Théorème (Bellaïche, [1])**.** *Sous l'hypothèse de Riemann généralisée et la conjecture d'Artin, on a*

$$|\{p \leq x, p \nmid M, |E(\mathbb{F}_p)| \text{ est premier}\}| < (8 + o(1))C_E\frac{x}{(\log x)^2}.$$

Bibliographie

[1] J. Bellaïche. *Théorème de Chebotarev et complexité de Littlewood*, volume 49. Annales Scientifiques de l'École Normale Supérieure, 2016.

[2] H. Davenport and H.L. Montgomery. *Multiplicative Number Theory*. Graduate Texts in Mathematics. Springer New York, 2000.

[3] H. Iwaniec and E. Kowalski. *Analytic Number Theory*. Number v. 53 in American Mathematical Society colloquium publications. American Mathematical Society, 2004.

[4] J. C. Lagarias and A. M. Odlyzko. *Effective versions of the Chebotarev density theorem*. Academic press, New York, 1977.

[5] H.W. Lenstra. *The Chebotarev Density Theorem*. 2010.

[6] H.W. Lenstra and P. Stevenhagen. *Chebotarev and his density theorem*, volume 18. Springer, 1996.

[7] M. R. Murty and V. K. Murty. *Non-Vanishing of L-Functions and Applications*. Progress in mathematics. Springer, 1997.

[8] J. Neukirch and N. Schappacher. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 1999.

[9] J.-P. Serre. *Quelques applications du théorème de densité de Chebotarev*. 1981.

[10] J.-P. Serre. *Représentations Linéaires des Groupes Finis*. Hermann, 1998.

[11] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[12] N. Snyder. *Artin's L-functions : A Historical Approach*. 2002.

[13] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*. Belin, 2015.

[14] B. Winckler. *Théorème de Chebotarev effectif*. arXiv preprint arXiv :1311.5715, 2013.