FONCTIONS L ET ÉQUIRÉPARTITION

JULES MAS, LÉO GRATIEN

Mémoire de première année, sous la direction de Gaëtan Chenevier

Table des matières

1. Introduction

Ce mémoire, sous la direction de Gaëtan Chenevier, a secrètement la motivation de la recherche de la *dialectique* que A. Lautman illustre dans son *Essai sur les notions de structure et d'existence en mathématiques* :

> *C'est un problème fondamental pour la philosophie mathématique que d'établir une théorie des rapports du continu et du discontinu, de l'arithmétique et de l'analyse.*

L'équirépartition en théorie des nombres existe sous de nombreuses formes. Le but de notre travail a été d'étudier des phénomènes arithmétiques à partir de l'étude analytique de fonctions de plus en plus sophistiquées.

Nous étudierons dans un premier temps le théorème de la progression arithmétique de Dirichlet, grâce aux fonctions L associées.

Théorème 1.1 (Dirichlet)**.** *Pour n, m entiers premiers entre eux, la densité des nombres premiers de la forme $n + km$ est non nulle est vaut $1/\varphi(m)$.*

Puis une autre forme d'équirépartition plus géométrique, portant sur la décomposition de p premier en somme de deux carrés, nécessitera de nouveaux outils analytiques. Nous démontrerons le théorème de Hecke suivant. Soit p un nombre premier congru à 1 modulo 4, p admet dans $\mathbf{Z}[i]$ une décomposition unique de la forme $p = \pi\bar{\pi}$ et $\arg \pi \in \left[0, \frac{\pi}{4}\right[$.

Théorème 1.2 (Hecke)**.** *La suite des arguments de π notée (θ_p) est équirépartie dans $\left[0, \frac{\pi}{4}\right[$.* [1]

Enfin, la dernière partie de notre travail portera à généraliser le premier théorème à certaines extensions algébriques de $\mathbf{Q}$. La démonstration du théorème de Chebotarev nécessite la (longue) théorie du corps de classes, à laquelle nous avons préférer substituer des tentatives plus directes et claires : conjecture d'Artin et extension abélienne.

Nous avons parlé ci-dessus de *densité* sans être plus clair. Il existe plusieurs notions, dont les *densité naturelle* et *analytique*, définies en première section. Pour le cadre de nos démonstrations, nous nous limitons à la seconde bien qu'étant doté de quelques outils supplémentaires (dans l'appendice au premier chapitre de [Ser94a], J.-P. Serre utilise le théorème taubérien de Wiener–Ikehara) tous nos résultats se transposent à la densité naturelle.

1. Pour une définition précise de l'équirépartition que nous utiliserons, voir le théorème 3.1

2. Théorème de Dirichlet

2.1. Définitions et rappels.

Pour $t \in \mathbf{R}$, on note Ω_t le demi-plan ouvert $\{z \in \mathbf{C},\ \mathrm{Re}\, z > t\}$ et $\mathbf{P}$ l'ensemble des nombres premiers. Rappelons que la *fonction zêta de Riemann* est définie sur Ω_1 par $\zeta(s) = \sum_{n\in\mathbf{N}^*} n^{-s}$ et on a l'identité d'Euler

$$\forall s \in \Omega_1, \quad \sum_{n\in\mathbf{N}^*} \frac{1}{n^s} = \prod_{p\in\mathbf{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

où le produit est ici absolument convergent sur Ω_1. La *densité analytique* d'un ensemble $\mathcal{A} \subset \mathbf{P}$ se définit par $\mathrm{d}(\mathcal{A}) = \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{A}} \frac{1}{p^s}}{\sum_{p\in\mathbf{P}} \frac{1}{p^s}}$ lorque cette limite existe. Cette notion apparaîtra assez naturellement (elle diffère cependant de la *densité naturelle*, prendre par exemple l'ensemble des nombres premiers de premier chiffre 1 [Ser94a]). On rappelle les faits connus suivants, découlant du pôle simple de ζ en $s = 1$.

Proposition 2.1. Soit $f(s) = \sum_{p\in\mathbf{P}} \frac{1}{p^s}$ holomorphe sur Ω_1. On a l'équivalent $f(s) \sim \ln(\frac{1}{s-1})$ quand s réel tend vers 1^+. La densité analytique de $\mathcal{A}$ se reformule donc

$$\mathrm{d}(\mathcal{A}) = \lim_{s\to 1^+} \frac{-1}{\ln(s-1)} \sum_{p\in\mathcal{A}} \frac{1}{p^s}.$$

lorsque cette limite existe.

Soient a, m deux entiers fixés dans la suite, avec $(a, m) = 1$. On mesure la densité de $\mathbf{P}_a$, ensemble des nombres premiers congrus à a modulo m, en comparant le comportement asymptotique de $f_a(s) = \sum_{p\in P_a} \frac{1}{p^s}$ quand s tend vers 1^+ à celui de $f(s)$.

2.2. Caractères et prolongement des $L(s, \chi)$.

On introduit les *caractères de Dirichlet*, prolongement périodique à $\mathbf{N}$ d'un caractère χ de $(\mathbf{Z}/m\mathbf{Z})^\times$ nul sur les entiers non premier à m. La fonction obtenue est encore notée χ et multiplicative. À un tel caractère χ nous lui associons sa *fonction L de Dirichlet* sur Ω_1 via $L(s, \chi) = \sum_{n\in\mathbf{N}^*} \frac{\chi(n)}{n^s}$.

Nous utiliserons de manière cruciale le fait que les caractères forment une base orthonormale des fonctions de $(\mathbf{Z}/m\mathbf{Z})^\times$ dans $\mathbf{C}$ pour le produit scalaire $\langle f, g\rangle = \frac{1}{\varphi(m)} \sum_{a\in(\mathbf{Z}/m\mathbf{Z})^\times} f(a)\overline{g(a)}$.

Lemme 2.2. Soit $f : (\mathbf{Z}/m\mathbf{Z})^\times \to \mathbf{C}$. Alors $f = \sum_\chi \langle f, \chi\rangle\chi$. En particulier, $\mathbf{1}_{\mathbf{P}_a} = \frac{1}{\varphi(m)} \sum_\chi \overline{\chi(a)}\chi$.

D'après le lemme, on décompose $f_a(s) = \frac{1}{\varphi(m)} \sum_\chi \overline{\chi(a)} f_\chi(s)$ avec $f_\chi(s) = \sum_{p\in\mathbf{P}} \frac{\chi(p)}{p^s}$. L'étude de $\mathbf{1}_{\mathbf{P}_a}$ se ramène donc à la quantification des contributions des f_χ au voisinage de 1. En fait, seul $f_{\mathbf{1}}$ ne sera pas négligeable.

De manière analogue à la fonction ζ, la multiplicativité des caractères de Dirichlet donne pour tout $s \in \Omega_1$:

$$L(s, \chi) = \prod_{p\in\mathbf{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

où le produit est ici absolument convergent.

Une transformation d'Abel et le fait que $\left(\sum_{k=1}^{n}\chi(k)\right)_n$ est bornée (et nulle si $m|n$) montre que $L(s,\chi)$ se prolonge holomorphiquement à Ω_0 si χ n'est pas trivial. $L(s,\chi=1)$ correspond, à un nombre fini de facteurs près, à la fonction ζ de Riemann. Elle se prolonge donc en une fonction holomorphe sur $\Omega_0\backslash\{1\}$ avec un pôle simple en $s=1$.

2.3. **Démonstration du théorème.**

On définit $\zeta_m(s)=\prod_\chi L(s,\chi)$ la fonction zêta sur $(\mathbf{Z}/m\mathbf{Z})^\times$, avec χ les caractères de $(\mathbf{Z}/m\mathbf{Z})^\times$. Sa force vient en parti, comme nous le verrons en section 4, du fait que c'est la fonction zêta de Dedekind du m-ième corps cyclotomique. Nous allons montrer que ζ_m a un unique pôle simple en $s=1$. Cela impliquera directement la non-annulation des $L(1,\chi)$, pour $\chi\neq\mathbf{1}$. La démarche suivante suit Serre [Ser94b] :

Proposition 2.3. Pour p premier ne divisant pas m, on note $f(p)$ l'ordre de p modulo m, et $g(p)=\varphi(m)/f(p)$. On a :

$$\zeta_m(s)=\prod_{p\nmid m}\left(1-\frac{1}{p^{f(p)s}}\right)^{-g(p)} \tag{1}$$

Preuve. On a : $\zeta_m(s)=\prod_\chi L(s,\chi)=\prod_\chi\prod_{p\in\mathbf{P}}(1-\frac{\chi(p)}{p^s})^{-1}=\prod_{p\in\mathbf{P}}\prod_\chi(1-\frac{\chi(p)}{p^s})$ où l'intervertion est possible par absolue convergence du produit sur Ω_1. Pour $p\nmid m$, on introduit le produit $F_p=\prod_\chi\left(1-\frac{\chi(p)}{p^s}\right)$. Chaque $\chi(p)$ est une racine $f(p)$-ième de l'unité qui y apparaît $g(p)$ fois. Ainsi,

$$F_p=\left(1-\frac{1}{p^{f(p)s}}\right)^{-g(p)}$$

en vertu de la relation algébrique $\prod_{w\in\mathbf{U}_{f(p)}}(1-wT)=1-T^{f(p)}$. On obtient ainsi le résultat, les facteurs pour p divisant m valant 1. □

On peut conclure avec le

Théorème 2.4. *La fonction ζ_m est à coefficients entiers positifs, et admet un pôle simple en $s=1$. Ainsi, $L(1,\chi)$ est non nul si χ est non trivial.*

Preuve. À un facteur multiplicatif près, $L(s,\mathbf{1})=\prod_{p\nmid m}\left(1-\frac{1}{p^s}\right)^{-1}$ est la fonction zêta de Riemann et se prolonge sur Ω_0 en une fonction méromorphe avec 1 comme unique pôle, qui est de multiplicité un. Nous avons également prolongé les $L(s,\chi)$ en remarque du lemme 2.2 à Ω_0 de manière holomorphe. Supposons par l'absurde qu'il existe $\chi\neq\mathbf{1}$, $L(1,\chi)=0$. Alors $\zeta_m(s)$ serait holomorphe en $s=1$ et ainsi sur Ω_0. Or, l'égalité de la proposition 2.3 montre que $\zeta_m(s)$ est une série à coefficients positifs. Par le théorème de Landau, on en déduit que la série associée converge sur Ω_0. Ainsi le p-ième terme de (1) s'écrit

$$\left(1-\frac{1}{p^{f(p)s}}\right)^{-g(p)}=\left(\sum_{k\geq0}p^{-kf(p)s}\right)^{g(p)}\geq\sum_{k\geq0}p^{-k\varphi(m)s}.$$

Or en $s = \frac{1}{\varphi(m)} \in \Omega_0$, la série $\sum_{k\geq 0} p^{-k\varphi(m)s}$ diverge, c'est une contradiction. □

Il reste à contrôler les f_χ pour $\chi \neq \mathbf{1}$ pour conclure avec la décomposition que nous avions obtenue au lemme 2.2. Pour éviter de contrôler la bonne définition du logarithme de $L(s,\chi)$ sur Ω_0, on *définit* la fonction $\ln L(s,\chi)$ par la formule $\sum_{n,p} \frac{\chi(p)^n}{np^{ns}}$ de sorte que $\exp(\ln L(s,\chi)) = L(s,\chi)$.

La décomposition $\ln L(s,\chi) = f_\chi(s) + F_\chi(s)$ pour $s \in \Omega_1$ nous ramène aux fonctions L. En effet, comme $L(1,\chi) \neq 0$, la fonction $\ln L(s,\chi)$ est bien définie et holomorphe au voisinage de 1. De plus F_χ est somme d'une série normalement convergente de fonctions holomorphes sur $\Omega_{\frac{1}{2}}$. Ainsi, f_χ est bornée au voisinage de 1.

En combinant la propriété précédente et

$$f_a(s) = \frac{1}{\varphi(m)} \sum_\chi \overline{\chi(a)} f_\chi(s) = \frac{1}{\varphi(m)} f_{\mathbf{1}} + \frac{1}{\varphi(m)} \sum_{\chi \neq \mathbf{1}} \overline{\chi(a)} f_\chi(s),$$

on en déduit le théorème de Dirichlet version analytique :

$$\boxed{\mathrm{d}(\mathbf{P}_a) = \lim_{s \to 1^+} \frac{f_a(s)}{f(s)} = \frac{1}{\varphi(m)}.}$$

3. Vers le théorème de Hecke

Comme dans l'introduction, on rappelle que pour un nombre premier p congru à 1 modulo 4, p admet dans $\mathbf{Z}[i]$ une décomposition de la forme $p = \pi\bar{\pi}$, on choisit celle d'argument $\pi = \sqrt{p}e^{i\theta_p}$, $\theta_p \in \left[0, \frac{\pi}{4}\right[$. Le but de cette section est de démontrer le théorème suivant.

Théorème 3.1 (Hecke)**.** *La suite des (θ_p) pour $p \equiv 1 \pmod 4$ est équirépartie dans $\left[0, \frac{\pi}{4}\right[$. Plus précisément, pour toute $f \in \mathcal{C}(\mathbf{S}^1, \mathbf{R})$ invariante par D_8, on a*

$$\frac{\sum_{p\equiv 1\ (4)} \frac{f(e^{i\theta_p})}{p^s}}{\sum_{p\equiv 1\ (4)} \frac{1}{p^s}} \xrightarrow[s\to 1^+]{} \frac{4}{\pi}\int_0^{\frac{\pi}{4}} f(e^{i\theta})\mathrm{d}\theta.$$

Remarque. Il est assez naturel de s'intéresser aux fonctions du cercle continues et invariantes sous l'action de D_8. En effet, pour un nombre premier p congru à 1 modulo 4 donné, l'angle θ_p peut être défini de 8 façons différentes comme l'argument de $a+ib$ avec $p = a^2+b^2$. L'ensemble des définitions possibles de $e^{i\theta_p}$ constituent une orbite de $\mathbf{S}^1$ sous l'action de D_8.

3.1. Fonctions L_m de Hecke : équation fonctionnelle et prolongements.

On introduit pour $m \in 4\mathbf{N}^*$, la fonction $L_m(s) = \sum_{z\in\mathbf{Z}[i]-\{0\}} \frac{z^m}{|z|^{2s+m}}$. Celle-ci est holomorphe sur $\Omega_1 = \{s \in \mathbf{C} \,|\, \mathrm{Re}(s) > 1\}$; notre but est son étude pour l'équirépartition des (θ_p). Le lecteur pourra observer l'équation (3) pour se convaincre de la pertinence de telles fonctions L.

On obtient dans un premier temps le prolongement à Ω_0, puis grâce à des outils plus avancé une équation fonctionnelle définissant L_m à $\mathbf{C}$ entier.

Définissons la *fonction thêta* sur $\mathbf{R}_+^*$ par $\theta_m^*(t) = \sum_{z\in\mathbf{Z}[i]} z^m e^{-\pi|z|^2 t}$. Notons que si $m = 0$, on retrouve $\theta^2(t)$ le carré de la fonction thêta de Jacobi. La proposition suivante sert à justifier son corollaire, à savoir la bonne définition de la transformée de Mellin de θ_m^*.

Définition 1. Soit f dans l'espace de Schwartz de $\mathbf{R}_+$, noté $\mathscr{S}(\mathbf{R}_+)$. On définit sa *transformée de Mellin* par $\mathcal{M}(f)(s) = \int_{t\geq 0} f(t)t^s \frac{\mathrm{d}t}{t}$. En particulier $\Gamma(s) = \mathcal{M}(e^{-t})(s)$.

Proposition 3.2. Si $m \geq 1$, il existe $T > 0$ et $C, \alpha > 0$ tels que $|\theta_m^*(t)| \leq C\exp(-\alpha t)$ pour $t > T$ et $|\theta_m^*(t)| \leq \frac{C\exp(-\frac{\alpha}{t})}{t^m\sqrt{t}}$ pour $0 < t \leq \frac{1}{T}$.

Preuve. On a

$$|\theta_m^*(t)| \leq \sum_{z\in\mathbf{Z}[i]} |z|^m e^{-\pi|z|^2 t} = \sum_{n=1}^{+\infty} \sum_{k^2+l^2=n^2} n^m e^{-\pi n^2 t} \leq \sum_{n=1}^{+\infty} (2n+1)^2 n^m e^{-\pi n t}$$
$$\leq 9\sum_{n=1}^{+\infty} n^{m+2} e^{-\pi n t}$$
.

Or il existe $T>0$ tel que pour tout $t\geq T$, $-\pi nt+(m+2)\log(n) \leq -\frac{\pi nt}{2}$ car $(\frac{\log(n)}{n})_n$ est bornée. Alors pour tout $t\geq T$, $|\theta_m^*| \leq 9\sum_{n=1}^{+\infty} e^{-\frac{\pi nt}{2}} = 9\frac{e^{-\frac{\pi t}{2}}}{1-e^{\frac{-\pi t}{2}}} \leq 9\frac{e^{-\frac{\pi t}{2}}}{1-e^{\frac{-\pi T}{2}}}$. $C = \frac{9}{1-e^{\frac{-\pi T}{2}}}$ et $\alpha = -\frac{\pi}{2}$ conviennent. On obtient l'autre inégalité via l'équation fonctionnelle. □

Corollaire 3.3. Si $m\geq 1$, $\mathcal{M}(\theta_m^*)(s)$ converge pour tout $s\in\mathbf{C}$ et définit une fonction holomorphe sur $\mathbf{C}$.

Preuve. Par décroissance exponentielle de θ_m^* à l'infini et en 0, on obtient que cette intégrale à paramètre converge et définit une fonction entière par théorème d'holomorphie sous l'intégrale. □

On suppose d'abord $m\geq 1$. Alors pour $s\in\Omega_{m/2+1}$, l'inversion est licite par convergence uniforme sur $\mathbf{R}$:

$$\begin{aligned}
\mathcal{M}(\theta_m^*)(s) &= \int_0^{+\infty} \sum_{z\in\mathbf{Z}[i]} z^m e^{-\pi|z|^2 t} t^s \frac{\mathrm{d}t}{t} \\
&= \sum_{z\in\mathbf{Z}[i]} z^m \int_0^{+\infty} e^{-\pi|z|^2 t} t^s \frac{\mathrm{d}t}{t} \\
&= \pi^{-s} \sum_{z\in\mathbf{Z}[i]} \frac{z^m}{|z|^{2s}} \int_0^{+\infty} e^{-t} t^s \frac{\mathrm{d}t}{t} \\
&= \pi^{-s}\Gamma(s) L_m\left(s-\frac{m}{2}\right),
\end{aligned}$$

soit

$$\mathcal{M}(\theta_m^*)(s) = \pi^{-s}\Gamma(s) L_m\left(s-\frac{m}{2}\right). \tag{2}$$

Corollaire 3.4. Soit $s\in\Omega_0$, compte tenu du prolongement holomorphe de Γ à $\mathbf{C}-\mathbf{Z}_-$ sans zéro, la quantité $\mathcal{M}(\theta_m^*)(s+m/2)\pi^{s+m/2}/\Gamma(s+m/2)$ est bien définie par le corollaire précédent 3.3. Cela prolonge $L_m(s)$ au demi-plan $\Omega_0 = \{s\,;\,\mathrm{Re}(s)>0\}$.

3.2. Équirépartition des θ_p pour p premier.

On s'intéresse maintenant aux conséquences arithmétiques des propriétés de L_m. L'analogue du *critère de Weyl* pour la densité naturelle (qui s'intéresse aux $n\mapsto \frac{1}{n}\sum_{k\leq n} e^{im\theta_p}$ pour tout $m>0$) est l'étude des $\sum_p \frac{\cos(m\theta_p)}{p^s}$, ce que nous faisons en 3.2.2.

Pour cela, on rappelle que $\mathbf{Z}[i]$ est (euclidien donc) principal, donc factoriel. On peut anticiper et remarquer que $\mathbf{Z}[i]$ est l'anneau des entiers du corps quadratique $\mathbf{Q}(i)$. On notera génériquement π un élément irréductible de $\mathbf{Z}[i]$. Soit encore $L_m(s) = \sum_{z\in\mathbf{Z}[i]-\{0\}} \frac{z^m}{|z|^{2s+m}}$.

La structure de $\mathbf{Z}[i]$ nous invite à généraliser l'identité d'Euler à L_m, ce qui est fait dans le lemme 3.6. On détermine donc les irréductibles de $\mathbf{Z}[i]$:

Lemme 3.5 (Irréductibles des entiers de Gauss)**.** Les irréductibles de l'anneau $\mathbf{Z}[i]$ sont, modulo les 4 associés :

i. $1+i$, de norme 2,
ii. les nombres premiers congrus à 3 modulo 4,
iii. les π tels que $|\pi|^2 = p$ soit un nombre premier congru à 1 modulo 4. Il y en a deux (conjugués) pour chaque tel nombre premier.

Preuve. Soit π un irréductible de $\mathbf{Z}[i]$ et $n = N(\pi) = \pi\overline{\pi} \in \mathbf{N}_{\geq 2}$ sa norme. Par principalité de $\mathbf{Z}[i]$, π est aussi premier donc divise l'un des facteurs premiers p de n. (On peut donc écrire $p = \pi a$ ce qui implique $N(\pi)|p^2$, puis $N(\pi) \in \{p, p^2\}$.)

— Si $p \equiv 3 \pmod 4$, p n'est pas la somme de deux carrés donc p est irréductible et π et p sont associés.
— Si $p \equiv 1 \pmod 4$, alors -1 est un carré modulo p donc il existe un entier m tel que p divise $m^2+1 = (m+i)(m-i)$. Si p était irréductible, il serait premier et p diviserait $m+i$ ou $m-i$ ce qui est absurde car aucun de ces deux éléments n'appartient à $p\mathbf{Z}[i]$. Écrivons alors $p = \pi a$ avec $N(a) > 1$. De $p^2 = N(\pi)N(a)$ on tire $N(a) = N(\pi) = p$. Donc a est égal ou conjugué à π, et le premier cas est exclu. On conclut en remarquant que π et $\overline{\pi}$ ne sont pas associés.
— Si $p = 2$, il est clair que π vaut $1 \pm i$. □

Proposition 3.6. Soit $s \in \Omega_1$ et m définit comme plus haut. On a la formule produit portant sur les irréductibles :

$$\forall s \in \Omega_1,\ L_m(s) = \prod_{\pi} \left(1 - \frac{\pi^m}{|\pi|^{2s+m}}\right)^{-1} \tag{3}$$

où le produit est absolument convergent.

3.2.1. *Comportement de L_m au voisinage de* 1.

On aperçoit donc comment faire apparaître la quantité qui nous intéresse, les $\cos(m\theta_p)$. Deux choix s'offrent à nous : la dérivée logarithmique de L_m ou son logarithme. À la différence de la première section, on adopte la seconde approche en définissant son logarithme – ce qui nous évite une construction plus pénible.

La formule (3) nous invite à poser lorsque $s > 1$:

$$\ln(L_m(s)) = 2 \sum_{\substack{p\equiv 1(4)\\ \pi\overline{\pi}=p}} \frac{\cos(m\theta_p)}{p^s} + R(s) \tag{4}$$

avec

$$\left\{\begin{array}{rcl} R(s) & = & \ln(\varepsilon(s)) - \sum_{p\equiv 3(4)} \ln\left(1-\frac{1}{p^{2s}}\right) + 2\sum_{p\equiv 1(4)}\sum_{k\geq 2}\frac{\cos(mk\theta_p)}{p^{ks}}, \\ \varepsilon(s) & = & \left(1-\frac{(1+i)^m}{2^{s+m/2}}\right)^{-1}\left(1-\frac{(1-i)^m}{2^{s+m/2}}\right)^{-1} \end{array}\right.$$

Lemme 3.7. L'exponentielle de $\ln L_m(s)$ est par construction $L_m(s)$ et le reste $R(s)$ reste borné quand s tend vers 1.

Preuve.

— Montrons d'abord la propriété sur l'exponentielle de $\ln L_m(s)$. En utilisant la caractérisation des irréductibles précédente, on a d'une part, par interversion des facteurs possible par convergence absolue du produit,

$$L_m(s) = \varepsilon(s)\prod_{\substack{p\equiv 1(4)\\ \pi\overline{\pi}=p}}\left(1-\frac{\pi^m}{p^{s+m/2}}\right)^{-1}\left(1-\frac{\overline{\pi}^m}{p^{s+m/2}}\right)^{-1}\prod_{p\equiv 3 \pmod 4}\left(1-\frac{1}{p^{2s}}\right)^{-1}.$$

D'autre part,

$$\ln\, L_m(s) = \sum_{\substack{p\equiv 1(4)\\ \pi\overline{\pi}=p}}\sum_{k\geq 1}\frac{\pi^{mk}+\overline{\pi}^{mk}}{p^{k(s+\frac{m}{2})}} + Q(s) = -\sum_{\substack{p\equiv 1(4)\\ \pi\overline{\pi}=p}}\ln\left(1-\frac{\pi^m}{p^{s+\frac{m}{2}}}\right)\left(1-\frac{\overline{\pi}^m}{p^{s+\frac{m}{2}}}\right)+Q(s)$$

avec $Q(s) = \ln(\varepsilon(s)) - \sum_{p\equiv 3(4)}\ln\left(1-\frac{1}{p^{2s}}\right)$. Donc :

$$\exp(\ln\, L_m(s)) = \prod_{\pi}\left(1-\frac{\pi^m}{|\pi|^{2s+m}}\right)^{-1}.$$

— Soit $s\in\Omega_1$. Il est immédiat de remarquer que les termes $\ln\,\varepsilon(s)$, et $\sum_{p\equiv 3(4)}\ln\left(1-\frac{1}{p^{2s}}\right)$ converge en $s=1$. Reste le deuxième terme qui est partie réelle de $I = 2\sum_{p\equiv 1(4)}\sum_{k\geq 2} e^{imk\theta_p}p^{ks}$, majorée par

$$|I| \leq 2\sum_{p\equiv 1(4)}\frac{1}{p^{2s}}\frac{1}{1-p^{-s}} \leq \frac{2}{1-2^{-s}}\sum_{p\equiv 1(4)}\frac{1}{p^{2s}},$$

et cette quantité converge en $s=1$. D'où $R(s)$ bornée au voisinage de 1.

□

3.2.2. *Démonstration du théorème de Hecke.*

Reprenons l'équation 4. Pour démontrer le théorème sur la base des cos, il nous reste à montrer qu'un contrôle de $\ln\, L_m$ est possible en 1. On montre plus précisément le caractère borné de $\ln\, L_m$. On adapte pour cela l'astuce de Hadamard–La Vallée-Poussin du théorème des nombres premiers [2] dans la :

2. Elle ne nous a pas été utile dans la section 1 car l'étude plus intrinsèque de la fonction zêta ζ_m contenait la difficulté de la proposition qui suit.

Proposition 3.8. Soit s dans $s > 1$, alors

$$|L_m(s)|^4 |L_{2m}(s)||L_0(s)|^3 \geq 1. \tag{5}$$

En particulier,

$$L_m(1) \neq 0 \quad \text{pour} \quad m \geq 1.$$

Preuve. On utilise l'inégalité $\forall \theta \in \mathbf{R}$, $4\cos(\theta) + \cos(2\theta) + 3 = 2(\cos(\theta) + 1)^2 \geq 0$ et $Q(s) \geq 0$ pour avoir

$$\ln(L_m(s)) \geq 2 \sum_{\substack{p \equiv 1(4) \\ \pi\overline{\pi} = p}} \sum_{k=1}^{+\infty} \frac{\cos(mk\theta_p)}{p^{ks}}.$$

Puis, pour $m \geq 1$, le prolongement entier de L_{2m} montre qu'elle est holomorphe en $s = 1$. De plus $L_0(s) = \sum_{(n,m)\neq(0,0)} \frac{1}{(n^2+m^2)^s}$ admet un pôle simple en $s = 1$ [3].

Supposons par l'absurde que $L_m(1) = 0$. Le produit de gauche dans l'équation 5 à au moins un zéro en 1 de multiplicité au moins $4 - 0 - 3 = 1$, ce qui est contradictoire. □

Remarque. Notons que notre méthode rompt avec celle empreintée dans le cas des fonctions L de Dirichlet. Former une « fonction zêta de Hecke sur $\mathbf{Q}[i]$ » est, cette fois, bien moins évident. Celle contiendrait en autre le produit $\prod_m L_m(s)$, fonction qui n'a pas de raison d'être définie d'abord et de posséder des bonnes propriétés ensuite.

Ainsi, $\ln(L_m(s))$ reste borné quand s réel tend vers 1 si $m \geq 1$. D'où le résultat annoncé plus haut :

Proposition 3.9. Si $m \geq 1$,

$$-\frac{2}{\ln(s-1)} \sum_{\substack{p \equiv 1(4) \\ \pi\overline{\pi} = p}} \frac{\cos(m\theta_p)}{p^s} \longrightarrow 0$$

quand s réel tend vers 1^+. Si $m = 0$, cette quantité tend vers 1. Rappelons l'énoncé du théorème de Hecke, que l'on peut enfin démontrer.

Théorème 3.10. *Soit $f : \mathbb{S}^1 \longrightarrow \mathbf{R}$ continue et invariante par l'action de D_8. Alors :*

$$-\frac{2}{\ln(s-1)} \sum_{p \equiv 1\,(4)} \frac{f(e^{i\theta_p})}{p^s} \longrightarrow \frac{4}{\pi} \int_0^{\frac{\pi}{4}} f(e^{i\theta}) \mathrm{d}\theta$$

quand s réel tend vers 1^+. En ce sens, les θ_p sont équirépartis dans $[0, \frac{\pi}{4}[$.

Preuve. On procède en deux temps.

3. Pour le voir, on peut par exemple approcher $\sum_m \frac{1}{n^2+m^2}$ par $\int_0^{+\infty} \frac{1}{(n^2+x^2)^s} \mathrm{d}x = \frac{1}{n^{2s-1}} \int_0^{+\infty} \frac{1}{(1+u^2)^s} \mathrm{d}u$ et conclure par le théorème de convergence dominée et l'existence d'un pôle simple à la fonction ζ en 1.

— Montrons déjà le résultat pour les $f(z) = \sum_{k=-n}^{n} a_k z^k$. Remarquons que f est paire donc $a_k = a_{-k}$; f est invariante par rotation d'angle $\frac{\pi}{4}$, donc $a_k = a_k e^{i\frac{k\pi}{4}}$, d'où $a_k = 0$ dès que 8 ne divise pas k. On a :

$$-\frac{2}{\ln(s-1)} \sum_{p\equiv 1\,(4)} \frac{f(e^{i\theta_p})}{p^s} = a_0 \frac{-2}{\ln(s-1)} \sum_{p\equiv 1\,(4)} \frac{1}{p^s} + \sum_{1\leq 8k\leq n} 2a_{8k} \frac{-2}{\ln(s-1)} \sum_{p\equiv 1\,(4)} \frac{\cos(8k\theta_p)}{p^s} \longrightarrow a_0$$

quand s tend vers 1. Par ailleurs,

$$\int_0^{\frac{\pi}{4}} f(e^{i\theta}) \mathrm{d}\theta = \frac{\pi}{4} a_0.$$

— Soit maintenant une fonction f telle que dans l'énoncé et $\epsilon > 0$. Par densité des polynômes trigonométriques, il existe g une fonction de $\mathbb{S}^1$ dans $\mathbf{C}$ de la forme $g(z) = \sum_{k=-n}^{n} a_k z^k$ telle que $||f - g||_\infty \leq \epsilon$. En notant $I(f) = \frac{4}{\pi} \int_0^{\frac{\pi}{4}} f(e^{i\theta}) \mathrm{d}\theta$ et $H_f(s) = \frac{-2}{\ln(s-1)} \sum_{p\equiv 1\,(4)} \frac{f(e^{i\theta_p})}{p^s}$:

$$\begin{aligned} |H_f(s) - I(f)| &\leq |H_f(s) - H_g(s)| + |H_g(s) - I(g)| + |I(f) - I(g)| \\ &\leq H_{|f-g|}(s) + |H_g(s) - I(g)| + I(|f-g|) \\ &\leq \epsilon \frac{2}{|\ln(s-1)|} \sum_{p\equiv 1\,(4)} \frac{1}{p^s} + |H_g(s) - I(g)| + \epsilon \\ &\underset{s\to 1}{\longrightarrow} 2\epsilon. \end{aligned}$$

Le théorème de Hecke s'en déduit :

$$\boxed{\frac{-2}{\ln(s-1)} \sum_{p\equiv 1\,(4)} \frac{f(e^{i\theta_p})}{p^s} \underset{s\to 1}{\longrightarrow} \frac{4}{\pi} \int_0^{\frac{\pi}{4}} f(e^{i\theta}) \mathrm{d}\theta.}$$

3.3. Équation fonctionnelle des L_m.

Non-nécessaire à l'étude des (θ_p), cette sous-section permet le prolongement de nos fonctions L_m à $\mathbf{C}$. On s'intéresse aux fonctions θ_m^* définies plus haut.

Proposition 3.11 (Formule de Poisson)**.** Soit $\Lambda \subset \mathbf{C}$ un réseau et $f \in \mathscr{S}(\mathbf{C})$. Alors on a la *formule de Poisson dans* $\mathbf{C}$:

$$\sum_{\omega\in\Lambda} f(\omega) = \frac{1}{\mathrm{Vol}\,(\Lambda)} \sum_{\omega\in\Lambda^*} \widehat{f}(\omega) \tag{6}$$

où $\widehat{f}$ est la *transformée de Fourier* de f donnée par

$$\forall z \in \mathbf{C}, \quad \widehat{f}(z) = \int_{\mathbf{C}} f(\omega) e^{2i\pi z\cdot\omega} \mathrm{d}\omega,$$

et le *réseau dual* Λ^* l'ensemble $\{\omega \in \mathbf{C} \text{ tel que } \omega \cdot \Lambda \subset \mathbf{Z}\}$.

Preuve. Soient X un domaine fondamental de Λ et $f \in \mathscr{S}(\mathbf{C})$. La fonction $F(z) = \sum_{\omega\in\Lambda} f(z+\omega)$ est somme d'une série qui converge absolument sur $\mathbf{C}$ par hypothèse. De plus, F est ω-périodique pour tout $\omega \in X$ de sorte que F peut être vu comme une fonction de $\mathbf{C}/\Lambda$.

En particulier, F est $\mathcal{C}^1$ donc somme de sa série de Fourier en tout point. Or si $\omega_0 \in \Lambda^*$:

$$\begin{aligned} c_{\omega_0}(F) = \int_{\mathbf{C}/\Lambda} e^{-2i\pi\omega_0\cdot z} F(z)\mathrm{d}z = & \int_{\mathbf{C}/\Lambda} e^{-2i\pi\omega_0\cdot z}\left(\sum_{\omega\in\Lambda} f(z+\omega)\right)\mathrm{d}z \\ = & \sum_{\omega\in\Lambda}\int_{\omega+X} e^{-2i\pi\omega_0\cdot z} f(z)\mathrm{d}z \\ = & \frac{1}{\mathrm{Vol}\,(\Lambda)}\widehat{F}(\omega_0), \end{aligned}$$

où l'interversion série-intégrale est justifiée par convergence uniforme sur $\mathbf{C}/\Lambda$. D'où la formule de Poisson en évaluant F en 0. □

L'équation suivante, qui découle de la formule de Poisson, nous permettra de déterminer une relation sur $L_m(s)$.

Corollaire 3.12. Pour tout $t > 0$, on a l'équation fonctionnelle

$$\theta_m^*(t) = \frac{1}{t^m\sqrt{t}}\theta_m^*\left(\frac{1}{t}\right). \tag{7}$$

Preuve. En effet, partons du fait connu que la fonction $g : z \in \mathbf{C} \mapsto e^{-\pi|z|^2} \in \mathbf{C}$ est sa propre transformée de Fourier : $\forall z \in \mathbf{C},\quad e^{-\pi|z|^2} = \int_{\mathbf{C}} e^{2i\pi z\cdot u} e^{-\pi|u|^2}\mathrm{d}u$. Après dérivation (au sens défini dans la note de bas de page) selon la variable z^* m fois [4] :

$$\forall z \in \mathbf{C},\ (-\pi z)^m e^{-\pi|z|^2} = \int_{\mathbf{C}} (i\pi u)^m e^{2i\pi z\cdot u} e^{-\pi|u|^2}\mathrm{d}u,$$

et la parité de m permet de conclure : $g_m : z \in \mathbf{C} \mapsto z^m e^{-\pi|z|^2} \in \mathbf{C}$ est aussi sa propre transformée de Fourier. L'équation fonctionnelle sur θ_m^* est alors juste un corollaire de l'équation de Poisson avec $\Lambda = \Lambda^* = \mathbf{Z}[i]$ de volume 1. □

Reprenons l'équation (2) reliant θ_m^* à L_m :

$$\xi_m(s) := \mathcal{M}(\theta_m^*)(s) = \pi^{-s} L_m(s - m/2)\Gamma(s).$$

Pour $s \in \mathbf{C}$ et $m > 0$, on rappelle $\mathcal{M}(\theta^*)(s) = \displaystyle\int_0^{+\infty} \theta^*(t) t^s \frac{\mathrm{d}t}{t}$ et on note $I_0 = \int_0^1 \theta^*(t) t^s \frac{\mathrm{d}t}{t}$. Le changement de variable $t \to \frac{1}{u}$ donne $I_0 = \int_1^{+\infty} \theta^*(t) t^{m+\frac{1}{2}-s} \frac{\mathrm{d}t}{t}$. Ainsi,

$$\mathcal{M}(\theta^*)(s) = \int_1^{+\infty} \left(t^{m+1/2-s} + t^s\right)\theta^*(t)\frac{\mathrm{d}t}{t}. \tag{8}$$

Cela amène :

$$\boxed{\xi_m(s) = \xi_m(m + 1/2 - s) \quad \text{pour tout } s \in \mathbf{C}} \tag{9}$$

4. On rappelle, comme vu en cours d'Analyse Complexe, que $\frac{\partial}{\partial z^*} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right)$.

Remarque. — On peut obtenir une équation symétrique selon $s \to 1-s$ avec la fonction $\widehat{\xi}_m(s) := \xi_m((m+1/2)s)$.)

— Nous proposons une méthode bien moins avancée pour obtenir l'analycité de L_m en 1 en appendice. La méthode précédente reste d'un grand intérêt pour des fonctions L plus générale.

— Dans la dernière partie du mémoire, nous illustrons un corollaire de la *conjecture d'Artin* qui énonce que beaucoup de fonction L sont en fait entière sur $\mathbf{C}$, et le seul moyen d'obtenir ce genre de résultat reste l'approche fonctionnelle.

Il reste à s'intéresser au cas $m = 0$, qui se traite similairement avec $\theta_m^* - 1$ (le terme $z = 0$ n'est plus annulé dans la définition de θ_m^* !).

4. Préliminaire au théorème de Chebotarev

Essayons de généraliser le résultat de Dirichlet. On reformule ce dernier : plaçons nous dans l'extension (abélienne) cyclotomique n-ième de $\mathbf{Q}$, c'est à dire dans $\mathbf{Q}(e^{\frac{2i\pi}{n}})$. Pour $p \in \mathbf{P}$, l'idéal principal $\mathfrak{p} = (p)$ contient p et — d'après les résultats qui suivent sur les *anneaux de Dedekind* — se décompose en idéaux premiers de l'anneau des entiers. Pour presque tout p, nous verrons que ce dernier ne se ramifie pas (c'est le cas si et seulement si $p|n$).

Soit $\sigma \in G = \mathrm{Gal}(\mathbf{Q}(e^{2i\pi/n})/\mathbf{Q})$. Nous le prouverons dans un cadre plus général, G est isomorphe aux inversibles de $\mathbf{Z}/n\mathbf{Z}$. On associe à $\mathfrak{p}$ un élément $\left(\frac{\mathbf{K}/\mathbf{Q}}{\mathfrak{p}}\right)$ de G, dit *élément de Frobenius*, tel que pour α entier,

$$\left(\frac{\mathbf{K}/\mathbf{Q}}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}.$$

Le théorème de Dirichlet affirme qu'étant fixé $k \in (\mathbf{Z}/n\mathbf{Z})^*$, la *densité de Dirichlet* de l'ensemble $\{p \in \mathbf{P},\ \left(\frac{\mathbf{K}/\mathbf{Q}}{\mathfrak{p}}\right) = k\}$ est égale à $\frac{1}{\varphi(n)}$. On généralise cela à toute extension $\mathbf{K}/\mathbf{Q}$ galoisienne finie.

4.1. Théorie algébrique des nombres.

On suppose connu la théorie de Galois élémentaire, jusqu'à la correspondance d'Artin. Rappelons qu'une extension finie de $\mathbf{K}$ est *galoisienne* si elle est

(1) *normale*, c'est à dire stable par éléments conjugués ;
(2) *séparable*, c'est à dire $P \wedge P' = 1$ pour tout polynôme minimal sur $\mathbf{K}$ (ce qui est toujours vérifié si car $\mathbf{K} = 0$, ou si $\mathbf{K} = \mathbf{F}_{p^l}$ parfait).

On a le :

Théorème 4.1 (de l'élément primitif)**.** *Soit $\mathbf{L}/\mathbf{K}$ une extension finie de corps, avec $\mathbf{K}$ de caractéristique nulle. Alors $\mathbf{L}$ est monogène.*

Preuve. Puisque l'extension est séparable, on choisit n morphismes distincts de $\mathbf{L}$ dans $\overline{\mathbf{K}}$ une clôture algébrique [5]. Soit $V_{i,j}$ le sous $\mathbf{K}$-ev des $x \in \mathbf{L}$ ayant même image par les i et j-ème morphismes. Alors l'union finie de tels sous-espaces est distincte de $\mathbf{L}$, un élément α n'étant dans aucun $V_{i,j}$ a donc un polynôme minimal sur $\mathbf{K}$ de degré n. D'où $\mathbf{L} = \mathbf{K}(\alpha)$. □

Définition 2. Soit $x \in \mathbf{L}$ une extension galoisienne sur $\mathbf{K}$. On peut regarder le morphisme de $\mathbf{K}$-espace vectoriel $m_x : y \mapsto xy$. Sa trace et son déterminant fournissent deux éléments de $\mathbf{K}$, notés $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(x)$ et $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(x)$.

Si on note $x_1, \ldots, x_n$ (c'est à dire les $\sigma(x), \sigma \in G$) les conjugués de x (inclu) dans une clôture algébrique de $\mathbf{K}$, alors $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(x) = x_1 + \ldots + x_n$ et $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(x) = x_1 \cdots x_n$.

5. Le théorème de Steinitz nous assure l'existence est l'unicité, à isomorphisme près, de cette clôture. Cependant, le choix de cet isomorphisme n'est pas unique !

4.1.1. *Discriminant.*

Définition 3. Soit $\alpha = (\alpha_1, \dots, \alpha_n)$ une famille de $\mathbf{L}/\mathbf{K}$, posons $\Delta(\alpha) = \det(\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha_i\alpha_j))$. Cette quantité est appelée *discriminant* de α dans $\mathbf{L}$.

Proposition 4.2. Soit $\mathbf{L}/\mathbf{K}$ une extension galoisienne finie comme ci-dessus. Soit α une base de $\mathbf{L}$. Alors

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Preuve. Il suffit de noter que $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha_i\alpha_j) = \sum_{\sigma\in G}\sigma(\alpha_i\alpha_j)$ de sorte que

$$\Delta(\alpha_1, \dots, \alpha_n) = \det\left(\sum_{\sigma\in G}\sigma(\alpha_i)\sigma(\alpha_j)\right) = \det\left(\sigma_k(\alpha_i)\right)\cdot\det\left(\sigma_k(\alpha_j)\right),$$

ce qui conclut. □

4.2. **Anneau de Dedekind.**

Dans toute cette section 4.2, $\mathbf{K}$ est un corps de nombres de degré n. L'anneau $\mathfrak{O}$ des entiers de $\mathbf{K}$ n'est pas nécessairement factoriel, mais nous allons montrer que c'est un *anneau de Dedekind*, c'est à dire

i. C'est un anneau intègre,

ii. noethérien [6] et intégralement clos dans son corps de fractions,

iii. plus fortement : tout idéal premier non nul est maximal.

On le note $\mathfrak{O}$ dans cette partie.

4.2.1. *Propriétés arithmétiques des anneaux de Dedekind.*

Lemme 4.3. $\mathfrak{O}$ est un $\mathbf{Z}$-module libre de rang n. Autrement dit, il existe une base $\alpha_1, \dots, \alpha_n \in \mathfrak{O}$ de $\mathbf{K}/\mathbf{Q}$ telle que $\mathfrak{O} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$.

Preuve. Soit $\beta_1, \dots, \beta_n$ une base de $\mathbf{K}/\mathbf{Q}$. β_i satisfait une équation du type $a_0\beta^n + \cdots + a_n = 0$ avec $a_i \in \mathbf{Z}$ et a_0 non nul (qui dépendent de $i \in [\![1, n]\!]$). En multipliant par a_0^{n-1}, on voit que $a_0\beta_i$ est entier sur $\mathbf{K}$. Notons $b_i = a_0$ et $b = b_1 \dots b_n$. Alors $b\beta_1, \dots, b\beta_n$ sont tous dans $\mathfrak{O}$ et forment une base de $\mathbf{K}/\mathbf{Q}$. Prenons maintenant une telle base $\alpha_1, \dots, \alpha_n$ telle que $|\Delta(\alpha_1, \dots, \alpha_n)|$ soit minimal (possible car le discriminant d'une base dans $\mathfrak{O}$ est un entier strictement positif).

Soit α entier. On écrit $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n$ avec les $\gamma_i \in \mathbf{Q}$. Supposons par exemple que γ_1 n'est pas entier et écrivons-le $\gamma_1 = m + \theta$ avec m entier et $0 < \theta < 1$. On pose $\beta_1 = \alpha - m\alpha_1, \beta_2 = \alpha_2, \dots, \beta_n = \alpha_n$. C'est encore une base de $\mathbf{K}$ dans $\mathfrak{O}$, et $\Delta((\beta_i)) = \theta^2\Delta((\alpha_i))$. Cela contredit la minimalité du discriminant. Ainsi, γ_1 et de manière analogue les autres γ_i sont entiers. D'où $\mathfrak{O}$ de rang n sur $\mathbf{Z}$. □

Proposition 4.4. Soit n le rang de $\mathfrak{O}$ en tant que $\mathbf{Z}$-module libre. Si $\mathfrak{a}$ est un idéal non nul de $\mathfrak{O}$, alors $\mathfrak{O}/\mathfrak{a}$ est fini. De plus, si a est un entier non nul, $\mathfrak{O}/(a)$ possède a^n éléments.

6. *i.e.* toute suite d'idéaux croissante est stationnaire, où encore tout $\mathfrak{O}$-sous-module de $\mathfrak{O}$ est de type fini sur $\mathfrak{O}$.

Preuve. D'après la proposition précédente, on écrit $\mathfrak{O} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$; on commence par (ii)

i. Posons $S = \{\sum \gamma_i\alpha_i | 0 \leq \gamma_i < a\}$ un ensemble de représentants de $\mathfrak{O}/(a)$. Cela donne $|\mathfrak{O}/(a)| = a^n$.

ii. Soit maintenant $\mathfrak{a}$ est un idéal non nul de $\mathfrak{O}$, on fixe $\alpha \in \mathfrak{a}$ non nul. Il existe des entiers $a_1, \ldots, a_m$ tels que $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$. Prendre m minimal nous permet d'avoir a_m non nul. De plus $a_m = -(\alpha^m + a_1\alpha^{m-1} + \cdots + a_{m-1}\alpha) \in \mathfrak{a} \cap \mathbf{Z}$. Cela implique que $\mathfrak{O}/(a_m)$ se surjecte dans $\mathfrak{O}/\mathfrak{a}$, d'où la finitude de $\mathfrak{O}/\mathfrak{a}$ par (i).

□

On déduit de ces premières propriétés le point de départ de notre analyse : $\mathfrak{O}$, c'est à dire l'anneau des entiers de $\mathbf{K}$, est un anneau *noethérien*. Toute suite $(\mathfrak{a}_i)$ d'idéaux croissante stationne nécessairement car la suite $\mathfrak{O}/\mathfrak{a}_i$ est une suite décroissante d'anneaux finis.

Remarque.
1. Ces anneaux d'entiers représentent une classe importante d'anneaux noethériens, ce n'est pas une notion superflue comme nous le verrons juste après.
2. Par exemple, $\mathbf{Z}[i\sqrt{5}]$ (l'anneau des entiers de $\mathbf{Q}(i\sqrt{5})$) n'est pas factoriel car : $6 = (1 - i\sqrt{5})(1 + i\sqrt{5}) = 2 \cdot 3$, mais est noethérien.
3. D'autres anneaux noethériens sont donnés par adjonction d'indéterminées. Plus précisement, le *théorème de la base de Hilbert* énonce que si A est noethérien, alors pour tout n entier, $A[X_1, \ldots, X_n]$ l'est aussi.

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathfrak{O}$. On sait par la proposition 4.4 que $\mathfrak{O}/\mathfrak{p}$ est un anneau fini, intègre. C'est un corps. Donc $\mathfrak{p}$ est maximal, et $\mathfrak{O}$ est un anneau de Dedekind.

Proposition 4.5. Soit $\mathfrak{O}$ est un anneau de Dedekind. Par conséquent, tout idéal [7] de $\mathfrak{O}$ peut s'écrire comme un produit d'idéaux premiers, de manière unique à l'ordre des facteurs près.

Preuve. On procède en deux étapes.

1. *Existence* : Soit $\mathfrak{a}$ un idéal propre de $\mathfrak{O}$. Comme $\mathfrak{O}/\mathfrak{a}$ est fini, $\mathfrak{a}$ est contenu dans un idéal maximal $\mathfrak{p}_1$ [8]. On admet que « contenir c'est diviser », cela se montre à partir de la caractère fini du nombre de classes de $\mathbf{K}$ (cf. note 9). Il existe donc un certain idéal $\mathfrak{b}_1$ tel que $\mathfrak{a} = \mathfrak{p}_1\mathfrak{b}_1$. Si $\mathfrak{b}_1 \neq \mathfrak{O}$, le même raisonnement itéré fournit une chaîne croissante d'idéaux $\mathfrak{a} \subset \mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \cdots$. La noethérianité de $\mathfrak{O}$ montre que $\mathfrak{b}_t$ stationne à $\mathfrak{O}$. Ainsi,
$$\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_t.$$
2. *Unicité* : Soient s, t tels que $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_t = \mathfrak{q}_1 \ldots \mathfrak{q}_s$, avec $t > 0$ minimal. Si $\mathfrak{p}_1$ n'est égal à aucun des $\mathfrak{q}_i$, on trouve $\alpha_i \in \mathfrak{q}_i \backslash \mathfrak{p}_1$ pour tout i. Alors $\prod \alpha_i \in \mathfrak{a} \backslash \mathfrak{p}_1$, c'est une contradiction. On peut donc simplifier (par exemple en multipliant par

7. Nous ne parlerons pas d'idéaux fractionnaires, ou très peu. Ces derniers sont les $\mathfrak{O}$-sous-modules $\mathfrak{b}$ de $\mathbf{K}$ de type fini, ou de manière équivalente les $c\mathfrak{b}$ avec $c \in \mathbf{K}$ et $\mathfrak{b}$ un idéal de $\mathfrak{O}$.

8. En effet, on peut prendre pour $\mathfrak{p}_1$ tout idéal propre $\mathfrak{b}$ de $\mathfrak{O}$ contenant $\mathfrak{a}$ qui minimise $|\mathfrak{O}/\mathfrak{b}|$, on se passe ainsi du lemme de Krull qui nécessite l'axiome du choix.

l'inverse de $\mathfrak{p}_1$ dans le groupe des idéaux fractionnaires [9] de $\mathfrak{O}$) par $\mathfrak{p}_1$ et contredire la minimalité de t.

Avant d'étudier comment se comporte la décomposition d'idéaux par extension de corps, on conclut par le très important théorème des restes chinois.

Théorème 4.6 (des restes chinois)**.** *Soit $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i}$ un idéal non nul de $\mathfrak{O}$. Alors le morphisme naturel $\varphi : \mathfrak{O} \mapsto \prod \mathfrak{O}/\mathfrak{p}_i^{n_i}$ est surjectif, de noyau $\mathfrak{a}$; on a l'isomorphisme*

$$\mathfrak{O}/\mathfrak{a} \simeq \prod \mathfrak{O}/\mathfrak{p}_i^{n_i}.$$

Preuve. Le noyau de l'application est exactement l'ensemble des éléments qui appartiennent à chacun des $\mathfrak{p}_i^{n_i}$, *i.e.* à $\mathfrak{a}$. Montrons que ce morphisme est surjectif. L'idéal $\mathfrak{b} = \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_t^{n_t}$ n'est pas divisible par $\mathfrak{p}_1$. Soit α dans $\mathfrak{b}$ et pas dans $\mathfrak{p}_1$. L'image de α dans le corps $\mathfrak{O}/\mathfrak{p}_1$ est non nulle, d'inverse β. Dans $\mathfrak{O}$, cela ce reformule par l'existence de $\delta \in \mathfrak{p}$ tel que $\alpha\beta = 1 - \delta$. Ainsi, $1 - \delta^{n_1}$ est un multiple de β, contenu dans $\mathfrak{p}_1^{n_1}$ son image par φ est donc $(1, 0, \ldots, 0)$. Cela conclut la surjectivité de φ par symétrie. □

Nous utiliserons surtout la formulation suivante.

Corollaire 4.7. Étant donnés $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ des idéaux premiers entre eux deux à deux, et $\alpha_i \in \mathfrak{O}$, on dispose de $\alpha \in \mathfrak{O}$ tel que

$$\alpha \equiv \alpha_i \pmod{\mathfrak{a}_i} \quad \text{pour tout} \quad i \in [\![1, n]\!].$$

4.2.2. *Décomposition des idéaux dans une extension.*

Soit $p \in \mathbf{Z}$ un nombre premier. On peut écrire, avec des notations évidentes, sa décomposition en idéaux premiers :

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}. \tag{10}$$

De plus, $\mathfrak{O}/\mathfrak{p}_i$ est un corps fini sur $\mathbf{Z}/p\mathbf{Z}$ de degré noté f_i. Essayons de relier ces grandeurs dans le cas général.

Définition 4. Soit $\mathfrak{a}$ un idéal entier de $\mathfrak{O}$. Sa *norme* est définie par $\mathrm{N}(\mathfrak{a}) = [\mathfrak{O} : \mathfrak{a}] = |\mathfrak{O}/\mathfrak{a}|$.

Cette définition est cohérente avec la norme introduite sur les éléments de $\mathbf{K}$: $N((\alpha)) = [\mathfrak{O} : (\alpha)] = N_{\mathbf{K}/\mathbf{Q}}(\alpha)$. De plus, si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux entiers de $\mathfrak{O}$, alors $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$, ce qu'on admet ici.

Soit $\mathfrak{p}$ un idéal premier de $\mathfrak{O}$, et $n > 0$. Alors $\mathfrak{p}^n \neq \mathfrak{p}^{n-1}$ car $\mathfrak{p}$ est premier. Prenons $\alpha \in \mathfrak{p}^{n-1} \backslash \mathfrak{p}^n$, Alors on a un morphisme induit $\mathfrak{O} \to \mathfrak{p}^{n-1}/\mathfrak{p}^n : x \mapsto \alpha x$. Le noyau de cette flèche est $\mathfrak{p}$. Montrons qu'elle est surjective : si $\beta \in \mathfrak{p}^{n-1}$, alors $(\beta)/\mathfrak{p}^{n-1}$ [10] et $\mathfrak{p}^n$ sont premiers entre eux. Par le théorème des restes chinois, on dispose de $x \in \mathfrak{O}$ tels que

$$x \equiv \beta \pmod{\mathfrak{p}^n} \qquad \text{et} \qquad x \equiv 0 \pmod{(\beta)/\mathfrak{p}^{n-1}}$$

L'image de x par $\mathfrak{O}/\mathfrak{p} \to \mathfrak{p}^{n-1}/\mathfrak{p}^n$ est alors β. Donc $\mathfrak{O}/\mathfrak{p} \simeq \mathfrak{p}^{n-1}/\mathfrak{p}^n$, et en particulier $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$.

9. Ce groupe à une grande importance en théorie algébrique des nombres. Par exemple, le résidu de l'unique pôle de $\zeta_{\mathbf{K}}$ en $s = 1$ est proportionnel à son nombre de classes (c.f. Prop. 5.2). En fait, l'inverse de $\mathfrak{p}$ est $\mathfrak{p}' = \{\beta \in \mathbf{K},\ \beta\mathfrak{p} \subset \mathfrak{O}\}$. Le preuve complète est par exemple dans [K.I98].

10. Cette notation tient pour la division de (β) par $\mathfrak{p}^{n-1}$: soit la décomposition de $(\beta) = \mathfrak{p}^{n-1} \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$. Alors $(\beta)/\mathfrak{p}^{n-1} := \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$.

Lemme 4.8. Avec les notations ci-dessus, on a l'égalité :

$$\boxed{n = \sum_{i=1}^{g} e_i f_i} \tag{11}$$

Preuve. En prenant les normes dans (10), on obtient $N((p)) = \prod_{i=1}^{g} [\mathfrak{O} : \mathfrak{p}_i]^{e_i}$ soit $p^n = \prod_{i \leq g} p^{f_i e_i}$, d'où l'égalité. □

4.2.3. *Lien à la décomposition polynomiale sur* $(\mathbf{Z}/p\mathbf{Z})[X]$.

Précisons la décomposition d'un nombre premier p dans une extension de $\mathbf{Q}$, disons $\mathbf{Q}(\alpha)$, permise par le théorème de l'élément primitif. Dans un premier temps nous allons supposer que l'anneau des entiers de $\mathbf{Q}(\alpha)$ est $\mathbf{Z}[\alpha]$ (C'est le cas pour les $\sqrt{d}$, d sans facteur carré congru à 1 modulo 4 ; des corps cyclotomiques, cf. l'exemple 4.14). En fait, la décomposition de (p) peut être comprise sur la réduction modulo p du polynôme minimal de α sur $\mathbf{Q}$, noté Π_α.

Proposition 4.9. Avec les notations ci-dessus, on définit pour Q diviseur de $\overline{\Pi}_\alpha$ l'idéal $I(Q) = p\mathbf{Z}[\alpha] + \tilde{Q}(\alpha)\mathbf{Z}[\alpha]$ où $\tilde{Q}$ est n'importe quel relevé à $\mathbf{Z}[X]$ de Q [11].

Alors $Q \mapsto I(Q)$ est une bijection entre les diviseurs unitaires du polynôme minimale de α sur $(\mathbf{Z}/p\mathbf{Z})[X]$ et les idéaux contenant p de $\mathbf{Z}[\alpha]$. De plus,

$$(\mathbf{Z}/p\mathbf{Z})[X]/(Q(X)) \cong \mathbf{Z}[\alpha]/(I(Q)). \tag{12}$$

Preuve. La preuve consiste en deux flèches inverses donnant (12). Partons de $\mathbf{Z}[\alpha] \xrightarrow{\sim} \mathbf{Z}[X]/(\Pi_\alpha)$, ce qui amène

$$\begin{array}{ccccc} \mathbf{Z}[\alpha] & \xrightarrow{\sim} & \mathbf{Z}[X]/(\Pi_\alpha) & \longrightarrow & (\mathbf{Z}/p\mathbf{Z})[X]/(\overline{\Pi}_\alpha) \\ P(\alpha) & \longmapsto & P(X) \pmod{\Pi_\alpha} & \longmapsto & \overline{P}(X) \pmod{\overline{\Pi}_\alpha} \end{array}$$

En composant une nouvelle fois par $(\mathbf{Z}/p\mathbf{Z})[X]/(\overline{\Pi}_\alpha) \longrightarrow (\mathbf{Z}/p\mathbf{Z})[X]/(Q)$, le diagramme se factorise par propriété universelle par $\mathbf{Z}[\alpha]/(I(Q))$. D'où un morphisme canonique $\mathbf{Z}[\alpha]/(I(Q)) \to (\mathbf{Z}/p\mathbf{Z})[X]/(Q)$. Un morphisme réciproque n'est pas plus dur à trouver. Il suffit alors de vérifier que les deux flèches obtenues sont réciproques l'une de l'autre. □

Soit, dans $\mathbf{Z}/p\mathbf{Z}[X]$:

$$\overline{\Pi}_\alpha = P_1^{e_1} \cdots P_g^{e_g}.$$

La proposition précédente donne que P_1 est premier si et seulement si $I(P_1)$ est premier. Ainsi, trouver la décomposition de (p) revient à calculer les $I(P_i)$ pour $i \leq g$.

Remarque. Lorsque $\mathfrak{O}$ n'est plus égal à $\mathbf{Z}[\alpha]$, ce dernier est seulement un sous-groupe d'indice finie. Dès lors, $\mathbf{Z}[\alpha]\left[\frac{1}{N}\right] = \mathfrak{O}\left[\frac{1}{N}\right]$ et la proposition 4.9 s'applique à $\mathfrak{O}\left[\frac{1}{N}\right]$.

11. Si R et S sont deux relevés de Q à $\mathbf{Z}[X]$, alors $R(\alpha) - S(\alpha)$ est par définition dans $p\mathbf{Z}[\alpha]$, donc $I(Q)$ est bien défini.

4.3. **Extension galoisienne de corps de nombres sur Q.**

On prend $\mathbf{K}$ une extension galoisienne finie sur $\mathbf{Q}$. L'ensemble des automorphismes de $\mathbf{K}$ qui laissent $\mathbf{Q}$ invariant, muni de la loi de composition des applications, forme un groupe appelé le *groupe de Galois* de l'extension, noté $G = \mathrm{Gal}(\mathbf{K}/\mathbf{Q})$. On s'intéresse à la décomposition des idéaux premiers (p) de $\mathbf{Q}$ dans $\mathbf{K}$.

Lemme 4.10. Soit p un nombre premier. Soit $\mathfrak{P}$ et $\mathfrak{Q}$ deux idéaux de $\mathbf{K}$ au dessus de p [12]. Alors ces deux idéaux sont conjugués par l'action de G.

Preuve. En effet, le théorème 4.6 donne $x \in \mathbf{K}$ tel que $x \equiv 0 \pmod{\mathfrak{P}}$ et $x \equiv 1 \pmod{\sigma\mathfrak{Q}}$ pour tout $\sigma \in G$. On en déduit que x est dans $\mathfrak{P}$, et $N_{\mathbf{K}/\mathbf{Q}}(x) \in (p)$. Or (p) est premier donc un certain $\sigma(x)$ appartient à (p), donc à $\mathfrak{Q}$, ce qui contredit le deuxième point. □

Cette transitivité de G sur les idéaux au dessus de (p) imposée sur $\mathbf{K}$ implique que les degrés résiduels et les indices de ramification sont égaux entre eux :

Proposition 4.11. Dans une extension galoisienne finie, on décompose $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ en premiers de $\mathbf{K}$. Alors

1. $\forall i \in [\![1, g]\!]$, $e_i := e_p$ et $f_i := f_p$ avec les f_i les degrés résiduels.
2. $e_p f_p g = n$.

Preuve. Pour i donné, il existe $\sigma \in G$ tel que $\sigma\mathfrak{P}_1 = \mathfrak{P}_i$. Dès lors, $\mathfrak{O}_\mathbf{K}/\mathfrak{P}_1 \simeq \mathfrak{O}_\mathbf{K}/\sigma\mathfrak{P}_1 = \mathfrak{O}_\mathbf{K}/\mathfrak{P}_i$. Donc $f_1 = f_i$.

Soit τ la permutation des indices $\{1, \ldots, g\}$ qu'induit σ. Puisque $\sigma(p) = (p)$, on a

$$\mathfrak{P}_{\tau(1)}^{e_1} \cdots \mathfrak{P}_{\tau(g)}^{e_g} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

D'où, par unicité de la décomposition, l'égalité des e_i. 2. découle de l'égalité (11). □

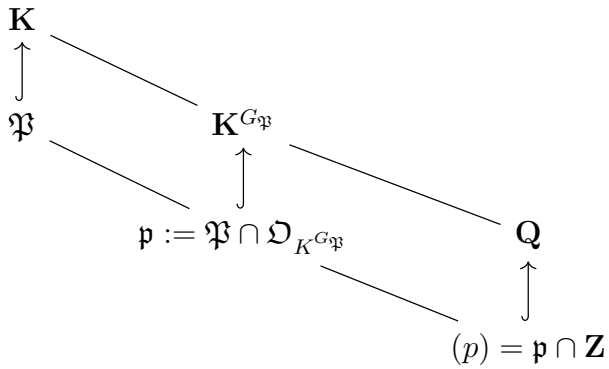
4.3.1. *Groupes de décomposition.*

Une dernière étape définitionnelle est nécessaire avant de pouvoir lier ces constructions entre elles. Il s'agit de comprendre le sous groupe de Galois qui fixe un premier $\mathfrak{P}$ de $\mathbf{K}$, dit *groupe de décompostion*, défini par $G_\mathfrak{P} = \{\sigma \in \mathrm{Gal}(\mathbf{K}\backslash\mathbf{Q}),\ \sigma\mathfrak{P} = \mathfrak{P}\}$.

Ainsi, si on note (p) le premier en dessous de $\mathfrak{P}$ dans $\mathbf{Q}$, $\mathfrak{O}_\mathbf{K}/\mathfrak{P}$ s'interprète comme une extension du corps $\mathbf{Z}/p\mathbf{Z}$. Étant donné $\sigma \in G_\mathfrak{P}$, notons $\tilde{\sigma}$ sa réduction modulo $\mathfrak{P}$, qui fixe $\mathbf{Q}$ donc $\mathbf{Z}/p\mathbf{Z}$, et est alors dans $\mathrm{Gal}\left((\mathfrak{O}_\mathbf{K}/\mathfrak{P})/(\mathbf{Z}/p\mathbf{Z})\right)$. Le but de cette section est de démontrer que le morphisme $G_\mathfrak{P} \to \mathrm{Gal}\left((\mathfrak{O}_\mathbf{K}/\mathfrak{P})/(\mathbf{Z}/p\mathbf{Z})\right)$ est en fait surjectif en toute généralité, et injectif si (p) ne se ramifie pas dans $\mathbf{K}$. C'est l'objet du corollaire 4.12. On notera $\mathbf{F}_\mathfrak{P}$ et $\mathbf{F}_p$ ces deux corps.

Considérons $\mathbf{K}^{G_\mathfrak{P}}$ le sous-corps de $\mathbf{K}$ fixé par $G_\mathfrak{P}$. On a donc la tour suivante :

12. On montre aussi que les idéaux de $\mathbf{K}$ dans la décomposition de $p\mathfrak{O}_\mathbf{K}$ sont exactement ceux au dessus de $p\mathfrak{O}_\mathbf{K} = \prod_{k\geq 1} \mathfrak{P}_k^{e_k}$.
   - si $\mathfrak{P}$ est un idéal premier au dessus de p, alors $\prod_{k\geq 1} \mathfrak{P}_k^{e_k} \subset \mathfrak{P}$ dans $\mathfrak{O}_\mathbf{K}$. Or $\mathfrak{P}$ est premier donc il contient l'un des $\mathfrak{P}_k$, et lui est égal par maximalité.
   - Réciproquement, tout les $\mathfrak{P}_k$ vérifient : $p = p\mathfrak{O}_\mathbf{K} \cap \mathbf{Z} = \left(\prod_{k\geq 1} \mathfrak{P}_k^{e_k}\right) \cap \mathbf{Z} \subset \mathfrak{P}_k \cap \mathbf{Z}$. On en déduit $p = \mathfrak{P}_k \cap \mathbf{Z}$.



Le corps $\mathbf{F}_p$ s'injecte canoniquement dans $\mathfrak{O}_{\mathbf{F}_\mathfrak{P}}/\mathfrak{p}$. Le point est que $\mathbf{F}_p$ est isomorphe à $\mathfrak{O}_{K^{G_\mathfrak{P}}}/\mathfrak{p}$.

En effet,

— Pour x entier sur $\mathbf{Q}$, la réduction de x, vu dans $\mathfrak{O}_{\mathbf{K}^{G_\mathfrak{P}}}$ modulo $\mathfrak{p}$ est nulle si et seulement si $x \in \mathfrak{p}$ c'est à dire $x \in \mathfrak{p} \cap \mathbf{Z} = (p)$.

— Soit maintenant $x \in \mathfrak{O}_{\mathbf{K}^{G_\mathfrak{P}}}$, on cherche y dans $\mathbf{Z}$ tel que $x \equiv y \pmod{\mathfrak{P}}$. Pour cela, on remarque que pour tout $\sigma \notin G_\mathfrak{P}$, $\sigma^{-1}\mathfrak{P}$ est premier à $\mathfrak{P}$. Donc $\mathfrak{p}_\sigma = \sigma^{-1}\mathfrak{P} \cap \mathfrak{O}_{\mathbf{K}^{G_\mathfrak{P}}}$ est premier à $\mathfrak{p}$ et les restes chinois donnent $y \in \mathfrak{O}_{\mathbf{K}^{G_\mathfrak{P}}}$ tel que

$$y \equiv x \pmod{\mathfrak{p}} \tag{13}$$

$$y \equiv 1 \pmod{\mathfrak{p}_\sigma}, \quad \sigma \neq 1 \quad (\text{soit } \sigma(y) \equiv 1 \pmod{\mathfrak{p}}) \tag{14}$$

Alors $N_\mathbf{Q}^{\mathbf{K}^{G_\mathfrak{P}}}(y)$ est un élément de $\mathbf{Z}$, et modulo $\mathfrak{P}$,

$$N_\mathbf{Q}^{\mathbf{K}^{G_\mathfrak{P}}}(y) = \prod_{\sigma \in G_\mathfrak{P}} \sigma(y) \overset{(14)}{\equiv} \prod_{\sigma \in G} \sigma(y) \equiv N_\mathbf{Q}^\mathbf{K}(x) = x \pmod{\mathfrak{P}}.$$

On en déduit l'isomorphisme suivant, et le corollaire qui suit.

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} \mathfrak{O}_{\mathbf{K}^{G_\mathfrak{P}}}/\mathfrak{p} \tag{15}$$

Corollaire 4.12. Soit $\mathbf{K}/\mathbf{Q}$ une extension galoisienne finie, p un nombre premier et $\mathfrak{P}$ un idéal premier de $\mathbf{K}$ au dessus de (p), de degré de ramification e_p. On note encore $G_\mathfrak{P}$ le groupe de décomposition de $\mathfrak{P}$. Alors :

1. la flèche (15) est toujours surjective,
2. son noyau $I_\mathfrak{P}$, dit *groupe d'inertie* de $\mathfrak{P}$, est de cardinal e_p.

Ainsi (15) est un isomorphisme de groupe si et seulement si p ne se ramifie pas dans $\mathbf{K}$.

Preuve.

1. Notons $\mathbf{F}_\mathfrak{p}$ le corps $\mathfrak{O}_{\mathbf{K}^{G_\mathfrak{P}}}/\mathfrak{p}$. D'après l'équation 15, on a $\mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_p) = \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})$. D'après le théorème 4.1 de l'élément primitif, on dispose de $\alpha \in \mathbf{F}_\mathfrak{P}$ tel que $\mathbf{F}_\mathfrak{P} = \mathbf{F}_\mathfrak{p}(\alpha)$. Soit Π le polynôme minimal de α sur $\mathbf{F}_\mathfrak{p}$. Alors tout $\sigma \in \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})$ stabilise les racines de Π. Or $\mathrm{Gal}(\mathbf{K}/\mathbf{K}^{G_\mathfrak{P}})$ agit transitivement sur ces dernières. On en déduit l'existence de $\tau \in \mathrm{Gal}(\mathbf{K}/\mathbf{K}^{G_\mathfrak{P}})$ tel que $\tau(\alpha) = \sigma(\alpha)$ et donc $\tilde{\tau}$ réduit modulo $\mathfrak{P}$ est égal à σ.

   En résumé, $G_\mathfrak{P} \longrightarrow \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})$ est surjectif.

2. Il s'agit de calculer, par surjectivité, $|I_{\mathfrak{P}}| = |G_{\mathfrak{P}}|/|\mathrm{Gal}(\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_p)|$. Par définition f_p est le degré de $\mathbf{K}_{\mathfrak{P}}$ sur $\mathbf{K}_p$. De plus l'action de G sur les idéaux de $\mathbf{K}$ divisant p est *transitive* et $G_{\mathfrak{P}}$ est le stabilisateur de $\mathfrak{P}$. donc $|G_{\mathfrak{P}}| = \frac{|G|}{g} = e_p f_p$. On en déduit que $|I_{\mathfrak{P}}|$ est égal à e_p. □

4.3.2. *Finitude du phénomène de ramification.*

Un point crucial est le théorème qui suit, que l'on admet. Cela nous permettra de ne s'occuper dans le théorème de Chebotarev uniquement des premiers non ramifiés. Il y a ramification si $\mathfrak{p}$ contient l'*idéal discriminant* de $\mathfrak{O}_{\mathbf{L}}$ sur $\mathfrak{O}_{\mathbf{K}}$, l'idéal de $\mathfrak{O}_{\mathbf{K}}$ engendré par les discriminants de bases de $\mathbf{L}$ sur $\mathbf{K}$ contenu dans $\mathfrak{O}_{\mathbf{L}}$. La preuve est dans le chapitre 5 de Samuel ([Sam60]), et nécessite de la localisation.

Remarque. Dans le cas où $\mathbf{K} = \mathbf{Q}$ est le corps des rationnels, on sait que $\mathfrak{O}_{\mathbf{L}}$ est un anneau de Dedekind et un $\mathbf{Z}$-module libre. Alors le discriminant absolu $\mathfrak{D}_{\mathbf{L}/\mathbf{Q}}$ coïncide avec l'idéal discriminant de $\mathfrak{O}_{\mathbf{L}}$ sur $\mathbf{Z}$.

Théorème 4.13. *Soit* $\mathbf{K}$ *un corps de nombre et* $\mathbf{L}$ *une extension finie de* $\mathbf{K}$*. Soit* $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{O}_{\mathbf{K}})$*, alors on a l'équivalence*

i. $\mathfrak{p}$ *se ramifie dans* $\mathfrak{O}_{\mathbf{L}}$*,*

ii. $\mathfrak{p}$ *contient l'idéal discriminant de* $\mathbf{L}$ *sur* $\mathbf{K}$*.*

En conséquence, les idéaux qui se ramifient sur $\mathbf{L}$ *sont en nombre fini.*

Exemple 4.14. — *Corps quadratiques.* Soit d un entier positif sans facteurs carrés, on forme le corps quadratique $\mathbf{Q}(\sqrt{d})$. On sait que l'anneau des entiers est donné par

$$\begin{cases} \mathbf{Z}[\sqrt{d}] & \text{si} \quad d \equiv 2,3 \pmod 4 \\ \mathbf{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{si} \quad d \equiv 1 \pmod 4. \end{cases}$$

le discrimant de la base $(1, \sqrt{d})$ (resp. $(1, \frac{1+\sqrt{d}}{2})$) vaut alors $D = 4d$ (resp. $D = d$).

Dans les deux cas, les nombres premiers qui se ramifient dans $\mathbf{Q}(\sqrt{d})$ sont les diviseurs premiers de d (et 2 si $d \equiv 3 \pmod 4$).

— *Corps cyclotomiques.* Soit $n > 0$ premier et $\mathbf{Q}_n$ le n-ième corps cyclotomique. Le calcul de l'anneau des entiers $\mathfrak{O}_n$ de $\mathbf{Q}_n$ est très dur [13]. Soit N tel que $\mathfrak{O}_n\left[\frac{1}{N}\right] = \mathbf{Z}[z]\left[\frac{1}{N}\right]$. Un nombre premier $p \in \mathbf{P}$ ne divisant pas N se ramifie donc dans $\mathbf{Q}_n$ si et seulement si $p|\Delta(1, z, \ldots, z^{n-2})$. En utilisant la proposition 4.2, on se ramène à calculer

$$\Delta(1, z, \ldots, z^{n-2}) = N_{\mathbf{Q}_n/\mathbf{Q}}(\Phi_n'(z)).$$

Or $(X-1)\Phi_n(X) = X^n - 1$ donc $\Phi_n'(z) = \frac{nz^{n-1}}{z-1}$. Or la norme de n, z et $z-1$ sont égales à n^{n-1}, 1 et n. Le discriminant de $(1, z, z^2, \ldots, z^{n-2})$ est donc égal à $\pm n^{n-2}$.

Les nombres premiers qui se ramifient sont donc des diviseurs de n ou de N.

13. Une base est donnée par $(1, z, z^2, \ldots, z^{n-2})$ où z est une racine primitive n-ième de l'unité, c'est donc $\mathbf{Z}[z]$.

4.4. **Élément de Frobenius.**

Dans cette sous-section, on se place dans sur un corps de nombres $\mathbf{K}$ et p un nombre premier *non-ramifié* dans $\mathbf{K}$. On a vu que l'on a un isomorphisme de $G_\mathfrak{p}$ dans $\mathrm{Gal}((\mathfrak{O}_\mathbf{K}/\mathfrak{p})/(\mathbf{Z}/p\mathbf{Z}))$. On remarque que $\mathbf{F}_\mathfrak{p}/\mathbf{F}_p = (\mathfrak{O}_\mathbf{K}/\mathfrak{p})/(\mathbf{Z}/p\mathbf{Z})$ est une extension de corps fini. Son groupe de Galois est en fait cyclique :

Lemme 4.15. Le groupe de Galois G de $\mathbf{F}_\mathfrak{p}/\mathbf{F}_p$ est cyclique. Un générateur distingué de G est donné par l'automorphisme de corps $\mathrm{Fr}_\mathfrak{p} : x \mapsto x^p$. On l'appelle *élément de Frobenius*.

Preuve. Soit p^f le degré de $\mathbf{F}_\mathfrak{p}$ sur $\mathbf{F}_p$. Alors $\varphi_\mathfrak{p}$ est d'ordre p^α pour un certain $\alpha \leq f$. Or comme $x^{p^\alpha} = x$ pour tout $x \in \mathbf{F}_\mathfrak{p}$ et le polynôme $X^{p^\alpha} - X$ est scindé sur $\mathbf{F}_\mathfrak{p}$ et admet au moins p^f racines. D'où $\alpha \geq f$. □

On relève $\mathrm{Fr}_\mathfrak{p}$ en un élément $\left(\frac{\mathbf{K}/\mathbf{Q}}{\mathfrak{p}}\right) \in G$ encore appelé Frobenius de l'extension $\mathbf{K}/\mathbf{Q}$. Il est déterminé par la relation

$$\forall \alpha \in \mathfrak{O}_\mathbf{K},\ \left(\frac{\mathbf{K}/\mathbf{Q}}{\mathfrak{p}}\right)\alpha \equiv \alpha^{p^f} \pmod{\mathfrak{p}}.$$

On remarque que si $\mathfrak{q} = \sigma\mathfrak{p}$ est un autre premier au dessus de p, alors $\left(\frac{\mathbf{K}/\mathbf{Q}}{\mathfrak{q}}\right) = \sigma\left(\frac{\mathbf{K}/\mathbf{Q}}{\mathfrak{p}}\right)\sigma^{-1}$. Ainsi, la classe de conjugaison de l'élément de Frobenius dans G ne dépend que de p, notons la $\left[\frac{\mathbf{K}/\mathbf{Q}}{p}\right]$. Nous pouvons maintenant formuler le théorème de Chebotarev sur $\mathbf{Q}$.

Théorème 4.16. *Soit $\mathbf{K}/\mathbf{Q}$ une extension galoisienne de corps de nombres, de groupe de Galois G. Etant donné $\sigma \in C$ sa classe de conjugaison dans G, on note $P_\mathbf{K}(\sigma)$ l'ensemble des nombres premiers p non ramifiés dans $\mathbf{K}$*[14] *tel que $\left[\frac{\mathbf{K}/\mathbf{Q}}{p}\right] = C$. Alors $P_\mathbf{K}(\sigma)$ à un densité analytique égale à $\frac{|C|}{|G|}$.*

14. Par le théorème 4.13, ils sont en nombre fini.

5. Démonstration du théorème de Chebotarev dans des cas particuliers

Soit $\mathbf{K}$ un corps de nombres galoisien. On décrit dans la suite deux résolutions du théorème de Chebotarev : le cas abélien et général. Le premier ne nécessite pas d'analyse supplémentaire, étant un corollaire du cas cyclotomique. Le second nécessite une généralisation naturelle des fonctions zêtas et L associées à des extensions de corps de nombres, selon [Neu86].

5.1. Dans le cas abélien.

Une extension *abélienne* de corps impose la commutativité du groupe de Galois associé. Le résultat qui suit (et que l'on admet) décrit exactement ces dernières.

Théorème 5.1 (Kronecker-Weber)**.** *Toute extension abélienne de corps de nombres est incluse dans une extension cyclotomique.*

Remarque. — Ce théorème est l'aboutissement d'une toute autre théorie, celle du *corps de classes* que nous n'aborderons malheureusement dans ce mémoire.

— Par exemple, $\mathbf{Q}(\sqrt{p})$ extension quadratique p-ième a un groupe de Galois $\mathbf{Z}/2\mathbf{Z}$ ce qui implique que $\sqrt{p} \in \mathbf{Q}(\zeta_n)$ pour un certain $n > 0$.

Par exemple, si $p \equiv 1 \pmod 4$, la somme quadratique de Gauss est très simple et jolie :

$$\sum_{k=0}^{p-1} \exp\left(\frac{2\pi i k^2}{p}\right) = \sqrt{p}.$$

Preuve (du théorème de Chebotarev abélien). Soit $\mathbf{K}/\mathbf{Q}$ comme ci-dessus, et G son groupe de Galois. D'après le théorème 5.1, on dispose de $n > 0$ tel que $\mathbf{K} \hookrightarrow \mathbf{Q}_n$. G est donc un quotient $(\mathbf{Z}/n\mathbf{Z})^\times/H$. Traitons le cas où $\mathbf{K} = \mathbf{Q}_n$ est cyclotomique, il s'agit de le reformuler le théorème de Dirichlet.

Soit k un élément de G et p premier, ne divisant pas n. Notons $\mathfrak{O}_n$ l'anneau des entiers de $\mathbf{Q}_n$. Dire que $k \overset{(*)}{=} \left(\frac{\mathbf{Q}_n/\mathbf{Q}}{p}\right)$, c'est écrire

$$\zeta_n^k \equiv \zeta_n^p \pmod{p\mathfrak{O}_n}.$$

Si $\delta = k - p$ est non nul modulo n, cela amène $\zeta_n^\delta \equiv 1 \pmod{p\mathfrak{O}_n}$ et le polynôme $X^n - 1$ aurait une racine multiple dans $\mathfrak{O}_n/p\mathfrak{O}_n$. Or p est premier à n ce qui est contradictoire par dérivation. $(*)$ équivaut donc à $k \equiv p \pmod n$. Or par le théorème de Dirichlet (démontré en première section, théorème 1.1), la densité analytique de tels p vaut $\frac{1}{\varphi(n)}$.

Pour un $\mathbf{K}$ abélien général, soit k dans G, défini modulo H et p dans $P_{\mathbf{K}}(\bar{k})$. Alors $\bar{k}$ provient d'un Frobenius si et seulement si $\bar{p} = \bar{k}$ dans G. Il correspond donc à chaque élément de la classe de k un nombre premier p. Donc $\mathrm{d}(P_{\mathbf{Q}_n/\mathbf{Q}}(k)) = \frac{1}{|H|}\mathrm{d}(P_{\mathbf{K}/\mathbf{Q}}(\bar{k}))$. On conclut par :

$$\boxed{\mathrm{d}(P_{\mathbf{K}/\mathbf{Q}}(\bar{k})) = \frac{|H|}{\varphi(n)} = \frac{1}{|G|}.}$$

□

5.2. **Dans le cas général.**

On démontre enfin le théorème de Chebotarev à l'aide de la conjecture d'Artin. On définit la fonction zêta de Riemann dans notre extension $\mathbf{K}/\mathbf{Q}$.

5.2.1. *Fonctions zêta de Dedekind et L d'Artin.*

Définition 5. La *fonction zêta de Dedekind* sur $\mathbf{K}$ est définie par

$$\zeta_{\mathbf{K}}(s) = \sum_{\mathfrak{a}} \frac{1}{N_{\mathbf{Q}}^{\mathbf{K}}(\mathfrak{a})^s} \quad \text{pour} \quad s \in \Omega_1,$$

la somme portant sur les idéaux de $\mathfrak{O}_{\mathbf{K}}$.

De manière analogue à $\zeta = \zeta_{\mathbf{Q}}$, nous avons les propriétés suivantes, toutes démontrées dans [Neu86] :

Proposition 5.2. Soit n le degré de l'extension de $\mathbf{K}$ sur $\mathbf{Q}$.

1. La série définissant la fonction zêta de Riemann a une abscisse de convergence égale à 1 et converge uniformément sur tout Ω_σ pour $\sigma > 1$.
2. Celle-ci admet un prolongement analytique sur $\Omega_{1-\frac{1}{n}}$ sauf un pôle simple en $s = 1$. Son résidu en ce pôle fournit des informations importantes sur le corps $\mathbf{K}$, via la jolie formule dûe à Dedekind :
$$\lim_{1^+}(s-1)\zeta_{\mathbf{K}}(s) = \frac{2^{r_1}(2\pi)^{r_2} \cdot R}{m\sqrt{|D|}} \cdot h,$$
où r_1 (resp. r_2) sont le nombre de places finies (reps. infinies) de $\mathbf{K}$ (avec donc $r_1 + 2r_2 = n$) ; R et D le régulateur et déterminant de $\mathbf{K}$; m son nombre d'unité et h son nombre de classes [15].
3. Pour $\mathrm{Re}(s) > 1$, on a
$$\zeta_{\mathbf{K}}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N_{\mathbf{Q}}^{\mathbf{K}}(\mathfrak{p})^{-s}},$$
le produit portant sur les idéaux premiers de $\mathfrak{O}_{\mathbf{K}}$.

Soit (ρ, V) une représentation de G. On note χ le caractère associé à ρ. Pour $\mathfrak{p}$ premier (disons au dessus d'un nombre premier p) de $\mathbf{K}$ et $G_{\mathfrak{p}}$ son groupe de décomposition, on sait que $G_{\mathfrak{p}}/I_{\mathfrak{p}}$ est cyclique engendré par le Frobenius $\mathrm{Fr}_{\mathfrak{p}}$. On peut alors le voir comme un endomorphisme de $V^{I_{\mathfrak{p}}}$ le module fixé par le groupe d'inertie de $\mathfrak{p}$. Alors la quantité $\det(1 - \mathrm{Fr}_{\mathfrak{p}} p^{-s} \ ; \ V^{I_{\mathfrak{p}}})$ est indépendante de $\mathfrak{p}$.

En effet, étant donnés deux $\mathfrak{p}$ et $\mathfrak{q}$ au dessus de p, alors ces derniers, leur groupe de décomposition et leur groupe d'inertie sont conjugués.

De plus, puisque deux représentations de même trace χ sont conjuguées [16] entre elles, $\det(1 - \mathrm{Fr}_{\mathfrak{p}} p^{-s} \ ; \ V^{I_{\mathfrak{p}}})$ ne dépend de χ. Cela motive la définition suivante.

15. C'est à dire le cardinal du groupe *fini* des idéaux fractionnaires de $\mathfrak{O}_{\mathbf{K}}$ quotienté par les idéaux principaux. La formule du résidu est une conséquence de la théorie de Minkowski, qui peut être trouvée dans [Sam60], [K.I98], [Neu86], ...

16. Il serait long de développer la théorie des représentations, nous renvoyons chapitre 9 du cours d'algèbre 1 de Gaëtan Chenevier.

Définition 6. La *fonction L d'Artin* associée à la représentation (ρ, V) est définie par

$$\forall s \in \Omega_1, \quad L(s, \chi, \mathbf{K}/\mathbf{Q}) = \prod_p \frac{1}{\det(1 - \mathrm{Fr}_\mathfrak{p} p^{-s}; V^{I_\mathfrak{p}})}. \tag{16}$$

Proposition 5.3. Pour tout $\sigma > 1$, $L(s, \chi, \mathbf{K}/\mathbf{Q})$ est absolument convergente et holomorphe sur Ω_σ.

Preuve. Soit $s > \sigma$ et (λ_i) les $d = \dim V^{I_\mathfrak{p}}$ valeurs propres de $\mathrm{Fr}_\mathfrak{p}$. Puisque $\mathrm{Fr}_\mathfrak{p}$ est d'ordre fini, les (λ_i) sont des racines de l'unité. Ainsi,

$$\det(1 - \mathrm{Fr}_\mathfrak{p} p^{-s} \ ; \ V^{I_\mathfrak{p}}) = \prod_{i=1}^{d} (1 - \lambda_i p^{-s}),$$

donc $L(s, \chi, \mathbf{K}/\mathbf{Q})$ converge absolument, et la série est holomorphe en s. □

Les propriétés qui suivent sont prouvées dans [Neu86] dans le cas d'une extension de corps de nombres générale.

Proposition 5.4. (1) Soit $\chi = \mathbf{1}$ le caractère principal de G alors $L(s, \mathbf{1}, \mathbf{K}/\mathbf{Q})$ est égale à la fonction zêta $\zeta_\mathbf{K}(s)$ de $\mathbf{K}$.

(2) Soient χ_1, χ_2 deux caractères de G, alors

$$L(s, \chi_1 + \chi_2, \mathbf{K}/\mathbf{Q}) = L(s, \chi_1, \mathbf{K}/\mathbf{Q}) L(s, \chi_2, \mathbf{K}/\mathbf{Q}).$$

Les deuxième et troisième points de cette proposition nous permettent la décomposition suivante. Soit χ le caractère principal, associé à la représentation régulière de G, et $\chi = \sum_\alpha r_\alpha \chi_\alpha$ sa décomposition en caractère irréductible.

En particulier, le caractère principal apparaît dans cette décomposition avec multiplicité $r_\alpha = 1$. On en déduit

$$\zeta_\mathbf{K}(s) = \zeta(s) \cdot \prod_{\chi_\alpha \neq \mathbf{1}} L(s, \chi_\alpha, \mathbf{K}/\mathbf{Q})^{r_\alpha}.$$

En section 3, nous avons déduit sur les fonctions L de Hecke (cas particulier associé au représentation de dimension 1) une équation fonctionnelle, point de départ pour prolonger à $\mathbf{C}$ holomorphiquement nos outils. Cependant, cela est bien plus délicat avec des fonctions L d'Artin générales, ce que conjecture Artin :

5.2.2. *Démonstration conjecturale dans le cas général.*

Dans la suite, nous *supposerons* cette conjecture vraie pour montrer notre dernier résultat. On abrégera $L(s, \chi_\alpha, \mathbf{K}/\mathbf{Q}) = L(s, \chi)$ s'il n'y a pas ambiguïté.

Proposition 5.5. Soit $\chi \neq \mathbf{1}$ un caractère et L sa fonction d'Artin. Alors $L(1, \chi) \neq 0$.

Preuve. On a l'égalité

$$\zeta_\mathbf{K}(s) = \zeta(s) \cdot \prod_\alpha L(s, \chi_\alpha)^{r_\alpha}.$$

Sachant que $\zeta_\mathbf{K}$ et ζ admettent toutes deux un pôle simple en 1, aucun des $L(s, \chi_\alpha)$ holomorphes sur $\mathbf{C}$ (d'après la conjecture d'Artin !) ne peut s'annuler en 1. □

Remarque. C'est ici que joue l'hypothèse analytique très puissante. Sans celle-ci, nous aurions dû expliciter la *correspondance d'Artin* qui lie les fonctions L d'Artin, qui nous renseignent sur le comportement arithmétique des Frobenius (c'est elles qui nous servent ici) et les fonctions L de Dirichlet, dont la connaissance au voisinage de 1 est meilleure.

Preuve (du théorème de Chebotarev). On reprend les notations de l'énoncé du théorème 4.16 de Chebotarev. Soit $M = P_{\mathbf{K}}(\sigma)$ avec $\sigma \in G$ fixé, on s'intéresse à la quantité $\sum_{p\in M} \frac{1}{N(p)^s}$ lorsque s réel tend vers 1. On peut la réécrire :

$$\sum_{p\in M} \frac{1}{N(p)^s} = \sum_{p} \frac{\mathbf{1}_\sigma(\mathrm{Fr}_p)}{N(p)^s}.$$

L'indicatrice est ici une fonction centrale de G et se décompose donc comme combinaison linéaire des caractères irréductibles de G : $\mathbf{1}_\sigma = \sum_\chi \lambda_\chi \chi$ avec $\lambda_1 = \langle \mathbf{1}, \mathbf{1}_\sigma \rangle = \frac{1}{|G|}\sum_g \mathbf{1}_{\mathrm{Fr}_p}(g) = \frac{|C|}{|G|}$. Alors :

$$\sum_{p\in M} \frac{1}{N(p)^s} = \sum_\chi \lambda_\chi f_\chi(s) \quad \text{avec} \quad f_\chi(s) = \sum_{p\in M} \frac{\chi(\mathrm{Fr}_p)}{N(p)^s}.$$

Calculons $\ln L(s,\chi) = -\sum_p \ln(\det(1-\mathrm{Fr}_p N(p)^{-s})) = \sum_p \sum_{k\geq 1} \frac{1}{k}\frac{\chi(\mathrm{Fr}_p)^k}{N(p)^s} = \sum_p \frac{\chi(\mathrm{Fr}_p)}{N(p)^s} + R(s)$ avec $R(s) = \sum_p \sum_{k\geq 2} \frac{1}{k}\frac{\chi(\mathrm{Fr}_p)^k}{N(p)^s}$. Si $\chi \neq \mathbf{1}$, $R(s)$ et $\ln(L(s,\chi)$ restent bornés quand s tend vers 1, donc il en est de même de f_χ. Ainsi :

$$\mathrm{d}(P_{\mathbf{K}}(\sigma)) = \lim_{s\to 1} \frac{\sum_\chi \lambda_\chi f_\chi(s)}{\sum_p \frac{1}{N(p)^s}} = \lambda_1 = \frac{|C|}{|G|},$$

ce qui démontre le théorème de Chebotarev.

Annexe A. Prolongement de L_m à Ω_0.

Soit $s \in \Omega_0$. Une transformation d'Abel sur $L_m(s)$ donne

$$L_m(s) = \sum_{n\geq 1} \frac{1}{n^{s+m/2}} \sum_{|z|^2=n} z^m = \sum_{n\geq 1} \left(\frac{1}{n^{s+m/2}} - \frac{1}{(n+1)^{s+m/2}} \right) S_m(n)$$

où $S_n(m) = \sum_{z\in\mathcal{D}_n} z^m$ et $\mathcal{D}_n$ est l'ensemble des $\frac{a+ib}{\sqrt{n}}$ dans $\mathbf{D} = D(0,1)$.

1. D'une part, pour $m = 0$, l'encadrement $\pi(n-1) \leq S_0(n) \leq \pi(n+1)$ donne $S_0(n) = |\mathcal{D}_n| \sim \pi n$. Pour $m \geq 1$, montrons que $S_m(n) = \mathcal{O}(n^{m/2})$ ce qui conclura.
2. Si m est impair ou congru à 2 modulo 4, $S_m(n)$ est nul par symétrie selon multiplication par -1 ou i respectivement.
3. Supposons $m > 4$ multiple de 4. Pour $z_0 \in \mathcal{D}_n$, on note Δ le plus petit carré supérieur droit à z_0 à côtés dans $\mathcal{D}_n$. On a pour $z \in \Delta$:

$$|z^m - z_0^m - mz_0^{m-1}(z-z_0) - \binom{m}{2} z_0^{m-2}(z-z_0)^2 - \binom{m}{3} z_0^{m-3}(z-z_0)^3 - \binom{m}{4} z_0^{m-4}(z-z_0)^4| \leq C_m \left(\frac{1}{\sqrt{n}}\right)^5 = C_n$$

où C_m est une constante absolue ne dépendant que de m. En intégrant l'inégalité sur Δ (partie réelle puis imaginaire) et en sommant sur $\mathcal{D}_n$ (on utilise le point 2) :

$$\left| 0 - \frac{1}{n} S_m(n) - 0 - \binom{m}{4} \sum_{z_0\in\mathcal{D}_n} z_0^{m-4} \int_\Delta (z-z_0)^4 \mathrm{d}z \right| \leq C_m \frac{1}{n^2\sqrt{n}}.$$

Les suites $S_m(n)$ et $\sqrt{n}S_{m-4}(n)$ sont donc de différence bornée. Le même procédé pour $m = 4$ donne : $S_4(n) = \mathcal{O}(\sqrt{n})$. Par récurrence, $S_m(n)$ est un $\mathcal{O}(n^{m/2})$. Sachant que

$$\frac{1}{n^{s+m/2}} - \frac{1}{(n+1)^{s+m/2}} \sim \frac{s+m/2}{n^{s+m/2+1}}$$

en n, cela montre en remontant la transformation d'Abel que L_m est aussi défini sur Ω_0. □

Annexe B. Courbes elliptiques, observations, tores

D'autre part, l'équirépartition est très liée aux théorèmes et conjectures suivantes.

Conjecture B.1 (Satō-Tate)**.** Soit $0 \leq \theta_p \leq \pi$ solution de l'équation $p+1-N_p = 2\sqrt{p}\cos\theta_p$ et E une *courbe elliptique* n'admettant pas de *multiplication complexe*. Alors, pour deux réels quelconques $0 \leq \alpha < \beta \leq \pi$ tels que

$$\lim_{N\to\infty} \frac{\mathrm{Card}\{p \leq N : \alpha \leq \theta_p \leq \beta\}}{\mathrm{Card}\{p \leq N\}} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta \,\mathrm{d}\theta.$$

Cette section est assez indépendante des autres, elle nous a permis d'aborder les *courbes elliptiques* et une meilleure compréhension des conjectures et résultats y étant liés. On détaillera cependant ci-dessous quelques motivations algébriques intrinsèques, en rapport avec l'équirépartition [Col11].

Définition 7. Une *courbe elliptique* réelle est, sous forme réduite, un ensemble de points du plan vérifiant la relation $y^2 = x^3+ax+b$ avec a, b deux constantes réelles. On considère aussi son équivalent projectif $y^2z = x^3 + axz^2 + bz^3$ ce qui nous permet de parler de la solution à l'infini de la courbe.

Soit (E) une courbe elliptique réelle. Son nombre de composante connexe dans le plan est donné par son *déterminant* $\Delta = -16(4a^3+27b^2)$. On définit l'ensemble de ses points rationnels, $E(\mathbf{Q})$ et $\overline{E}(\mathbf{Q})$. C'est en fait un groupe (abélien), muni de la loi suivante : étant donnés P, Q deux points de $E(\mathbf{Q})$, Soit R le point (peut-être infini) le point d'intersection de la droite passant par P et Q avec la courbe (E). Alors $P+Q := -R$. D'après un théorème de Mordell-Weil, c'est un groupe abélien de type fini. L'étude du *rang* de ce groupe est au centre du problème du millénaire suivant :

Théorème B.2 (Conjecture de Swinnerton-Dyer)**.** *Soit (E) une courbe elliptique à coefficients entiers. Soit le nombre N_p de solutions de (E) sur $\mathbf{F}_p$, par la remarque qui suit, on notera $N_p = p+1-a_p$ pour $p \in \mathbf{P}$. On associe une fonction L (de* Hasse-Weil*) par*

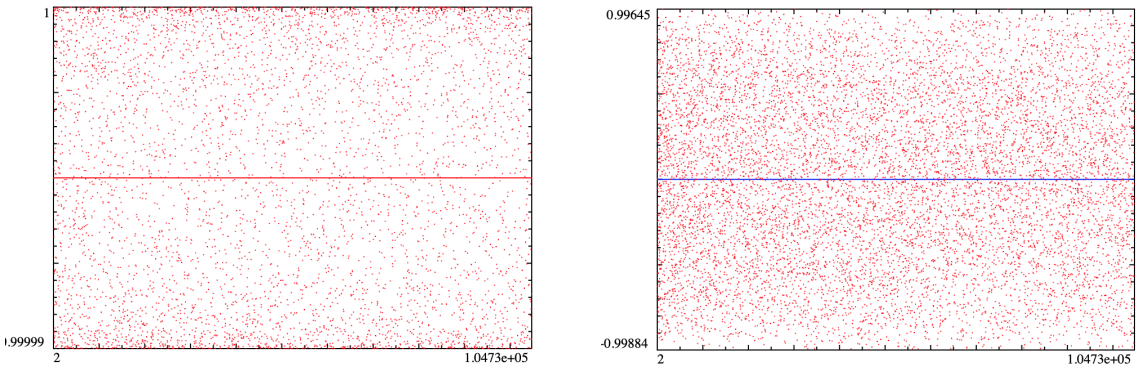
$$L(E/\mathbf{Q}, s) = \prod_{p\in\mathbf{P}} \left(1 - a_p p^{-s} + \varepsilon(p)p^{1-2s}\right)^{-1}.$$

où $\varepsilon(p)$ vaut 1 ou -1 selon que la réduction de (E) modulo p présente ou non une singularité*.*

Alors le rang de (E) sur $\mathbf{Q}$ est donné par l'ordre du 0 de $L(E/\mathbf{Q}, s)$ en $s = 1$.

Remarque. C'est le nombre a_p qui mesure le comportement de (E) sur $\mathbf{F}_p$, la « variation » du nombre de solution autour des $p+1 = \mathrm{Card}\,\mathbf{F}_p \cup \{\infty\}$: $|a_p| < 2\sqrt{p}$ pour tout $p \in \mathbf{P}$ (théorème dû à Hasse).

Remarquons l'analogie (qui n'est pas de surface) suivant laquelle à toute courbe elliptique à coefficients entiers, on associe une fonction L qui, localement, contrôle le comportement de p. Comme notre répartition des angles θ_p, une étude analytique en un point privilégié est incontournable. Le lien entre ses deux formulations est donnée par la conjecture de Satō-Tate énoncée en début d'appendice.



(A) Courbe elliptique ($y^2 = x^3 + 1$) à mult. complexe

(B) Courbe elliptique ($y^2 = x^3 + 7$) sans mult. complexe

FIGURE 1 – Graphe de la répartition des $p \mapsto \frac{a_p}{2\sqrt{p}}$ pour $p < 10^5$ avec et sans multiplication complexe (via PARI GP).

Une courbe elliptique sur $\mathbf{Q}$ présente une *multiplication complexe* si en plus de la loi de groupe présentée ci-dessus, la courbe possède d'autre symétrie. Plus formellement, si le groupe des automorphismes de la courbe elliptique n'est pas trivial, comme illustré ci-dessus.

Références

[Col11] Pierre Colmez. *Éléments d'analyse et d'algèbre (et de théorie des nombres)*. Éditions Polytechnique, 2011.

[K.I98] M. Rosen K.Ireland. *A Classical Introduction to Modern Number Theory*. Springer, 1998.

[Neu86] Jürgen Neurkirch. *Class Field Theory*. Springer-Verlag, 1986.

[Sam60] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, 1960.

[Ser94a] Jean-Pierre Serre. *Abelian l-adic représentations*. W.A. Benjamin, inc, 1994.

[Ser94b] Jean-Pierre Serre. *Cours d'arithmétique*. PUF, 1994.