Le théorème de densité de Chebotarev

Bait Rayane

Année 2021-2022

Université de Paris
Sous la direction de Herblot Mathilde et Galateau Aurélien

Table des matières

0 Introduction

Lors de l'étude de certains ensembles de nombres premiers l'une des premières questions posées est : En existe-t-il une infinité ? Une manière d'y répondre est d'en calculer la "proportion parmi tout les nombres premiers" en un sens à préciser. Intuitivement si cette proportion n'est pas nulle, notre ensemble est infini.

Deux résultats utilisant cette méthode sont présentés ici, le premier est le théorème de la progression arithmétique de Dirichlet affirmant que dans toute progression arithmétique de la forme $a+bn$ avec $pgcd(a,b) = 1$, une infinité de nombres premiers apparaît. Le second se présente comme suit : Soit $\mathbb{K}/\mathbb{Q}$ une extension finie galoisienne de groupe de Galois G. À tout nombre premier p qui ne se ramifie pas dans K correspond un morphisme $\sigma_p \in G$ défini à classe de conjugaison près. On pose la question suivante. Soit $\sigma \in G$, existe-t-il une infinité de nombres premiers p tels que $\sigma \in C(\sigma_p)$, où $C(\sigma_p)$ est la classe de conjugaison de σ_p dans G ? C'est à cette question que le théorème de Chebotarev répond.

Ce second théorème est rencontré relativement tard en théorie algébrique des nombres, beaucoup de résultats intermédiaires sont nécessaires à la compréhension des outils utilisés dans sa preuve. On en fera donc ici qu'un rappel partiel et on se référera au traitement de [2] des résultats classiques de théorie algébrique des nombres (chapitre 1,2,3,4), le chapitre 2 consistera donc en des rappels de ces chapitres. On admet en plus les résultats et définitions classiques de théorie de Galois.

1 Le théorème de la progression arithmétique de Dirichlet

Dans cette partie on admet des résultats bien connus sur les fonctions holomorphes ou les suites et séries de fonctions d'une variable complexe ainsi que sur la théorie des caractères. On suivra ici [1], chapitre 6.

Le but de cette partie est de montrer le résultat suivant :

Théorème 1.0.1. *Soit a et m deux entiers premiers entre eux. Alors il existe une infinité de nombre premier p tel que*

$$p \equiv a \mod m$$

Qui peut être précisé comme suit avec la notion de densité :

Définition 1.0.2. Soit P l'ensemble des nombres premiers de $\mathbb{N}$ et A un sous-ensemble de P. On dira que A a pour densité $d(A)$ lorsque la limite

$$\lim_{s\to 1,\ s>1} (\sum_{p\in A} \frac{1}{p^s})/(\ln \frac{1}{s-1})$$

existe et que cette limite vaut $d(A)$.

Avec cette définition on voit alors que tout $A \subset P$ ayant une densité non nulle est infini, en effet si A était fini la quantité $\sum_{p\in A} \frac{1}{p^s}$ serait finie et aurait alors pour densité 0.

Théorème 1.0.3. *Soit a et m deux entiers premiers entre eux et P_a l'ensemble des nombres premiers p tels que $p \equiv a \mod m$, alors P_a a une densité et sa densité vaut $\frac{1}{\phi(m)}$, où $\phi(m)$ désigne la fonction indicatrice d'Euler.*

La première sous partie constituera une base pour l'étude des fonctions L et justifiera l'utilisation de cette définition pour la densité. La deuxième sous-partie permettra, à l'aide des propriétés des fonctions L, de donner un équivalent de $\sum_{p\in P_a} \frac{1}{p^s}$ pour $s \to 1$ et ainsi prouver le théorème 1.0.3.Commencons par introduire quelques lemmes qui nous serons utiles par la suite.

Lemme 1.0.4. *(Lemme d'Abel) Soient (a_n) et (b_n) deux suites. Posons :*

$$A_{m,p} = \sum_{n=m}^{p} a_n \text{ et } S_{m,m'} = \sum_{n=m}^{m'} a_n b_n$$

On a alors :

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'}$$

Preuve : La preuve consiste à remplacer a_n par $A_{m,n} - A_{m,n-1}$ puis à réorganiser les termes.

Lemme 1.0.5. *Soient $0 < \alpha < \beta$ et $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 0$. On a alors :*

$$|e^{-\alpha z} - e^{-\beta z}| \leq |\frac{z}{\mathrm{Re}(z)}|(e^{-\alpha \mathrm{Re}(z)} - e^{-\beta \mathrm{Re}(z)})$$

Preuve : On a

$$e^{-\alpha z} - e^{-\beta z} = z.\int_{\alpha}^{\beta} e^{-tz} dt$$

d'où en passant aux valeurs absolues

$$|e^{-\alpha z} - e^{-\beta z}| \ \leq \ |z| \int_{\alpha}^{\beta} e^{-tRe(z)} = |\frac{z}{Re(z)}|(e^{-\alpha Re(z)} - e^{-\beta Re(z)})$$

qui est le résultat voulu. □

1.1 Séries de Dirichlet et fonction zêta

Définition 1.1.1. Soit (λ_n) une suite strictement croissante de nombres réels qui tend vers $+\infty$. On appelle série de Dirichlet d'exposants (λ_n) toute série de la forme :

$$\sum a_n e^{-\lambda_n s} \ , a_n \in \mathbb{C}, \ s \in \mathbb{C}$$

Soit $f(s)$ une série de Dirichlet où l'on aura supposé les λ_n positifs. Les résultats que l'on montrera sur $f(s)$ seront toujours valables sur une série de Dirichlet quelconque car on peut se ramener à notre cas en supprimant un nombre fini de termes, on appellera à nouveau par $f(s)$ sa somme là ou elle converge. Pour $\rho \in \mathbb{R}$ on appelle $D(\rho)$ le demi plan ouvert $\{z \in \mathbb{C} \mid Re(z) > \rho\}$ de $\mathbb{C}$.

Proposition 1.1.2. *Si f converge en s_0, elle converge uniformément sur $D(Re(s_0))$.*

Preuve : Quitte à remplacer s par $s - s_0$ on peut supposer que $s_0 = 0$. L'hypothèse veut alors dire que $\sum a_n$ est convergente. Il suffit de prouver que $f(s)$ converge uniformément dès que $Re(s) > 0$ et $|Arg(s)| \leq \alpha$ où $\alpha < \frac{\pi}{2}$. On peut reformuler la deuxième hypothèse en

$$\frac{|z|}{Re(z)} = \frac{1}{\cos(Arg(s))} \leq k$$

où $k \geq 1$. Soit $\epsilon > 0$. Comme $\sum a_n$ converge, il existe N tel que $|A_{m,m'}| \leq \epsilon$ dès que $m, m' \geq N$, les notations étant celles du lemme d'Abel. On applique celui-ci avec $b_n = e^{-\lambda_n s}$, on obtient :

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n s} - e^{-\lambda_{n+1} s}) + A_{m,m'} e^{-\lambda_{m'} s}$$

en prenant $m, m' \geq N$ et en passant aux valeurs absolues on a

$$|S_{m,m'}| \leq \epsilon(\sum_{n=m}^{m'-1} |e^{-\lambda_n s} - e^{-\lambda_{n+1} s}| + 1)$$

enfin on applique le lemme 1.0.5 à chaque terme de la somme ce qui nous donne

$$|S_{m,m'}| \leq \epsilon(\frac{|s|}{Re(s)} \sum_{n=m}^{m'-1} |e^{-\lambda_n Re(s)} - e^{-\lambda_{n+1} Re(s)}| + 1)$$

puis

$$|S_{m,m'}| \leq \epsilon(k(e^{-\lambda_n m} - e^{-\lambda_n m'}) + 1)$$

Et enfin

$$|S_{m,m'}| \leq \epsilon(k+1)$$

qui ne dépend plus de s dans le domaine considéré d'où la convergence uniforme sur ce domaine puis sur $D(s_0)$. □

Dans la suite on laissera le cas général pour se concentrer sur le cas particulier des séries de Dirichlet proprement dites qui correspond au cas où $\lambda_n = \log(n)$, $f(s)$ aura donc la forme $\sum \frac{a_n}{n^s}$.

Proposition 1.1.3. *Si (a_n) est bornée, f converge absolument et est holomorphe sur $D(1)$.*

Pour montrer cette proposition, on a besoin du lemme suivant :

Lemme 1.1.4. *Soit U un ouvert de $\mathbb{C}$, et soit (f_n) une suite de fonctions holomorphes sur U qui converge uniformément sur tout compact vers une fonction f. La fonction f est alors holomorphe dans U.*

Preuve du lemme : Soit D un disque fermé contenu dans U, et soit C son bord orienté dans le sens direct. D'après la formule de Cauchy, on a

$$f_n(s_0) = \int_C \frac{f_n(s)}{s - s_0} ds$$

pour tout $s_0 \in \mathring{D}$. Comme D est compact, par l'hypothèse de convergence uniforme on obtient en passant à la limite

$$f(s_0) = \int_C \frac{f(s)}{s - s_0} ds$$

d'où l'holomorphie de f sur $\mathring{D}$ puis sur U. □

Preuve de la propostion : Montrons que $\sum_{n\geq 1} \frac{a_n}{n^s}$ converge absolument. Si les a_n sont majorés par $M \in \mathbb{R}$ on a

$$\sum_{n\geq 1} | \frac{a_n}{n^s} | \leq M. \sum_{n\geq 1} \frac{1}{n^\alpha}$$

où le terme de droite est une série de Riemann de paramètre $\alpha = Re(s)$, d'où la convergence absolue pour $s \in D(1)$. □

Proposition 1.1.5. *Si les $A_{m,p} = \sum_{n=m}^{p} a_n$ sont bornées, f converge et est holomorphe sur $D(0)$.*

Preuve : Supposons que pour tout $m, p \in \mathbb{N}$ on ait $|A_{m,p}| \leq K$. En appliquant le lemme d'Abel, on obtient

$$|S_{m,m'}| \leq K(\sum_{m}^{m'-1} |\frac{1}{n^s} - \frac{1}{(n+1)^s}| + |\frac{1}{m'^s}|)$$

il suffit de montrer la convergence pour s réel, alors le résultat sera une conséquence de la proposition 1.1.2. Supposons donc s réel, on peut enlever les valeurs absolues et simplifier l'expression ce qui donne

$$|S_{m,m'}| \leq K((\frac{1}{m^s} - \frac{1}{(m')^s}) + \frac{1}{m'^s})$$

puis

$$|S_{m,m'}| \leq \frac{K}{m^s}$$

d'où la convergence en passant à la limite $m' \longrightarrow +\infty$. □

Définition 1.1.6. Une fonction $g : \mathbb{N}^* \longrightarrow \mathbb{C}$ est dite multiplicative si

$$g(1) = 1$$

et

$$g(nm) = g(n)g(m)$$

dès que les entiers n et m sont premiers entre eux.

Soit g une fonction multiplicative et bornée. On suppose à partir de maintenant que $a_n = g(n)$, $f(s)$ est donc de la forme $\sum \frac{g(n)}{n^s}$, elle converge absolument et est holomorphe sur $D(1)$ par les résultats précédents.

Lemme 1.1.7. *Dans $D(1)$, $f(s)$ est égale au produit infini*

$$\prod_{p \in P} (\sum_{m \geq 0} g(p^m) p^{-ms})$$

Preuve : Soit S un sous-ensemble fini de P et soit $N(S)$ l'ensemble des entiers non nuls dont tous les facteurs premiers sont dans S. Chaque élément $n \in N(S)$ s'écrit alors $n = \prod_{p \in S} p^{\alpha_p}$ et on a

$$\frac{g(n)}{n^s} = \prod_{p \in S} g(p^{\alpha_p}) p^{-\alpha_p s}$$

d'où en développant

$$\prod_{p \in S} (\sum_{m \geq 0} g(p^m) p^{-ms})$$

on voit que $\frac{g(n)}{n^s}$ apparaît une et une seule fois pour chaque $n \in N(S)$ et la somme en résultant est

$$\sum_{n \in N(S)} \frac{g(n)}{n^s}$$

ce résultat étant vrai pour tout $S \subset P$, lorsque S tend vers P le produit tend alors vers $f(s)$ qui est le résultat voulu. □

Lemme 1.1.8. *Si maintenant g vérifie $g(nm) = g(n)g(m)$ pour chaque paire d'entiers (n, m), on a :*

$$f(s) = \prod_{p \in P} \frac{1}{1 - g(p)p^{-s}}$$

Il s'agit du produit eulérien de f.

Preuve : Pour tout $m \geq 0$ et tout $p \in P$ on a :

$$g(p^m)p^{-ms} = (g(p)p^{-s})^m$$

la série $\sum_{m \geq 0} g(p^m)p^{-ms}$ est alors une série géométrique dont la somme vaut $\frac{1}{1 - g(p)p^{-s}}$, d'où le résultat. □

On introduit maintenant la fonction zêta de Riemann.

Définition 1.1.9. On appelle fonction zêta de Riemann notée ζ la somme de la série $\sum_{n \geq 1} \frac{1}{n^s}$.

On a vu qu'elle est bien définie et holomorphe sur $D(1)$, en effet on est dans le cas où $g \equiv 1$ qui est multiplicative au sens strict et bornée.

Proposition 1.1.10. *(Produit Eulérien) Sur $D(1)$ on a :*

$$\zeta(s) = \prod_{p \in P} \frac{1}{1 - p^{-s}}$$

Preuve : On applique directement le lemme 1.1.8.. □

Proposition 1.1.11. *On a :*

$$\zeta(s) = \frac{1}{s - 1} + \Phi(s)$$

où Φ est holomorphe sur $D(0)$.

Preuve : On remarque que

$$\frac{1}{s - 1} = \int_1^{+\infty} t^{-s} dt = \sum_{n=1}^{+\infty} \int_n^{n+1} t^{-s} dt$$

On peut donc écrire

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{+\infty} \Big(\frac{1}{n^s} - \int_n^{n+1} t^{-s} dt \Big)$$

$$= \frac{1}{s-1} + \sum_{n=1}^{+\infty} \int_n^{n+1} (n^{-s} - t^{-s}) dt$$

On pose alors

$$\Phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s}) dt \quad \text{et} \quad \Phi(s) = \sum_{n=1}^{+\infty} \Phi_n(s)$$

On voudrait maintenant appliquer le lemme 1.1.4, chaque Φ_n est holomorphe sur $D(0)$ car $s \longmapsto n^{-s} - t^{-s}$ est holomorphe pour tout $t \in [n, n+1]$. Montrons donc que $\sum_{n\geq 1} \Phi_n(s)$ converge normalement sur tout compact de $D(0)$. Soit K un compact de $D(0)$, on a :

$$|\Phi_n(s)| \leq \sup_{s\in K} \Big(\sup_{t\in[n,n+1]} |n^{-s} - t^{-s}| \Big)$$

mais $(n^{-s} - t^{-s})$ a pour dérivée $\dfrac{s}{t^{s+1}}$ de valeur absolue strictement monotone pour t et atteignant son maximum en $t = n$, d'où

$$|\Phi_n(s)| \leq \sup_{s\in K} \Big(\frac{|s|}{n^{Re(s)+1}} \Big)$$

puis la convergence normale découle du fait que $\Phi(s)$ est alors majorée par une série de Riemann de paramètre $Re(s) + 1 > 1$ d'où le résultat. □

Corollaire 1.1.12. *On a :*

$$\zeta(s) \sim_1 \frac{1}{s-1}$$

Preuve : Par la proposition précédente Φ reste bornée dans un voisinage de 1, d'où le résultat. □

À partir de maintenant on appellera par log la branche principale du logarithme qui peut être définie par $\log\Big(\dfrac{1}{1-\alpha}\Big) = \sum_{n=1}^{+\infty} \dfrac{\alpha^n}{n}$ pour $|\alpha| < 1$. Alors log est bien définie sur $D(0)$, $\log(1) = 0$ et on peut vérifier que

$$\log\Big(\frac{1}{(1-\alpha)(1-\beta)}\Big) = \log\Big(\frac{1}{1-\alpha}\Big) + \log\Big(\frac{1}{1-\beta}\Big)$$

pour $|\alpha|, |\beta| < 1$.

Corollaire 1.1.13. *Lorsque $s \to 1$ on a :*

$$\sum_{p\in P} p^{-s} \sim \log\Big(\frac{1}{s-1}\Big)$$

tandis que

$$\sum_{p\in P, n\geq 1} \frac{(p^{-s})^n}{n}$$

reste bornée.

Preuve : Soit $s \in D(1)$, on va faire tendre s vers 1 dans $D(1)$ donc on peut le supposer dans un petit voisinage de 1. La quantité $\log \dfrac{1}{s-1}$ est alors bien définie et on a par le produit Eulérien de ζ (proposition 1.1.10):

$$\begin{aligned}
\log \zeta(s) &= \log\Big(\prod_{p\in P} \frac{1}{1-p^{-s}}\Big) \\
&= \sum_{p\in P} \log\Big(\frac{1}{1-p^{-s}}\Big) \\
&= \sum_{p\in P, n\geq 1} \frac{(p^{-s})^n}{n} \\
&= \sum_{p\in P} p^{-s} \; + \sum_{p\in P, n\geq 2} \frac{(p^{-s})^n}{n}
\end{aligned}$$

comme $\log \zeta(s) \sim_1 \log(\frac{1}{s-1})$ il suffit de montrer que $\sum_{p\in P, n\geq 2} \frac{(p^{-s})^n}{n}$ reste bornée dans un voisinage de 1 alors on aura $\sum_{p\in P} p^{-s} \sim_1 \log(\frac{1}{s-1})$ qui est le résultat voulu. Mais on a les majorations suivantes

$$\begin{aligned}
\sum_{p\in P, n\geq 2} \Big|\frac{(p^{-s})^n}{n}\Big| &\leq \sum_{p\in P, n\geq 2} \big|(p^{-s})^n\big| \\
&\leq \sum_{p\in P} \big|p^{-2s}\big| \\
&\leq \sum_{p\in P} \big|p^{-s}(p-1)^{-s}\big| \\
&\leq \sum_{p\in P} p^{-1}(p-1)^{-1} \\
&\leq \sum_{n=2}^{+\infty} n^{-1}(n-1)^{-1} = 1
\end{aligned}$$

en effet la série $\sum_{n\geq 2} n^{-1}((n-1)^{-1}) = \sum_{n\geq 1}(n+1)^{-1}n^{-1}$ est convergente et le calcul s'effectue en remarquant que

$$(n+1)^{-1}n^{-1} = n^{-1} - (n+1)^{-1}$$

d'où le résultat. □

Cet équivalent permet alors de donner du sens à la définition de densité introduite en début de

partie. Il existe en fait une notion de densité dite naturelle que l'on définit de la manière suivante : Si A est un ensemble de nombre premier, on définit la densité naturelle de A comme la limite de $\dfrac{|A \cap [1,n]|}{P \cap [1,n]}$ lorsque $n \to \infty$. Même si celle-ci semble être la "bonne" notion de densité, elle n'existe pas toujours et est bien plus difficile à calculer que celle de Dirichlet. De plus on peut montrer que si celle-ci existe elle coïncide avec la densité de Dirichlet.

1.2 Fonctions L de Dirichlet

Soit $m \geq 1$ un entier. On note $G(m)$ le groupe des inversibles de $\mathbb{Z}/m\mathbb{Z}$ et $\widehat{G(m)}$ son dual, qui correspond à l'ensemble des caractères de degré 1 sur $G(m)$. $G(m)$ est un groupe abélien fini d'ordre $\phi(m)$ (où ϕ désigne l'indicatrice d'Euler). On note $\overline{n}$ la classe de $n \in \mathbb{Z}$ dans $G(m)$.

Définition 1.2.1. On appelle caractère modulo m un caractère χ de $G(m)$ que l'on étend à $\mathbb{Z}$ en posant

$$\chi(n) = \chi(\overline{n}) \quad \text{si } n \text{ est premier à } m,\ \chi(n) = 0 \quad \text{sinon.}$$

On peut maintenant introduire les fonctions L de Dirichlet. Soit χ un caractère modulo m.

Définition 1.2.2. On appelle fonction L de Dirichlet correspondant à χ et m la série de Dirichlet définie par

$$L(s,\chi) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}$$

Remarquons que $L(s,\chi)$ est une série de Dirichlet proprement dîte telle que $a_n = \chi(n)$ où χ est multiplicative au sens strict et bornée. Lorsque $\chi = 1$, on a

$$L(s,1) = \prod_{p|m}(1-p^{-s})\zeta(s)$$

qui est le produit d'une fonction holomorphe et non nulle sur $D(0)$ avec ζ qui est, on l'a vu, méromorphe sur $D(0)$ avec un seul pôle simple en 1 d'où $L(s,1)$ est méromorphe sur $D(0)$ avec un unique pôle simple en 1.

De plus lorsque $\chi \neq 1$ les sommes $A_{u,v}$ (avec les notations du lemme d'Abel) sont bornées par $\phi(m)$. Montrons le dernier point. On peut supposer $(v-u) < m$, en effet par la proposition 1.2.2, on a

$$\sum_{n=u}^{u+m-1} \chi(n) = 0$$

Si maintenant $x \in \mathbb{Z}$ est premier à m alors

$$\chi(x^{\phi(m)}) = \chi(x)^{\phi(m)} = \chi(\overline{x}^{\phi(m)}) = \chi(1) = 1$$

d'où $\chi(x)$ est une racine $\phi(m)$-ème de l'unité. En particulier $|\chi(x)| \leq 1$ pour tout $x \in \mathbb{Z}$ d'où

$$\left|\sum_{n=u}^{v} \chi(n)\right| \leq \sum_{n=u}^{v} |\chi(n)| \leq \phi(m)$$

qui est le résultat voulu. Par les propositions 1.1.3., 1.1.5. et le lemme 1.1.8. $L(s,\chi)$ converge absolument et est holomorphe sur $D(1)$, converge et est holomorphe sur $D(0)$ et dans $D(1)$ on a :

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

Dans la suite, si p est premier et ne divise pas m on notera $o(p)$ l'ordre de $\overline{p}$ dans $G(m)$ et $q(p) = \phi(m)/o(p)$ qui est l'ordre du groupe quotient $G(m)/ < \overline{p} >$.

Lemme 1.2.3. *Si p ne divise pas m, on a l'identité*

$$\prod_{\chi\in\widehat{G(m)}} (1-\chi(p)T) = (1-T^{o(p)})^{q(p)}$$

Preuve : Soit U_k l'ensemble des racines k-èmes de l'unité, on a :

$$\prod_{w\in U_{o(p)}} (1-wT) = 1-T^{o(p)}$$

de plus on sait par la théorie des caractères que l'opération de restriction de $\chi \in \widehat{G(m)}$ dans $\widehat{< \overline{p} >}$ est un homomorphisme surjectif de noyau les caractères triviaux sur $< \overline{p} >$, d'où la suite exacte courte

$$\{1\} \to \widehat{\frac{G(m)}{< \overline{p} >}} \to \widehat{G(m)} \to \widehat{< \overline{p} >} \to 1$$

Et il existe un unique caractère χ_1 de $< \overline{p} >$ tel que $\chi_1(p) = w$ pour chaque $w \in U_{o(p)}$ que l'on peut étendre en $\overline{\chi_1}$ un caractère de $G(m)$. Enfin l'application $\chi \longrightarrow \chi.\overline{\chi_1}^{-1}$ est une bijection de $\widehat{G(m)}$ dans lui même et envoie le noyau de la restriction sur l'ensemble des caractères χ de $G(m)$ tels que $\chi(\overline{p}) = w$. D'où il existe exactement $q(p)$ caractères tels que $\chi(\overline{p}) = w$. En mettant en commun les deux résultats on obtient directement le résultat voulu. □

On définit maintenant la fonction $\zeta_m(s)$ comme le produit

$$\zeta_m(s) := \prod_{\chi\in\widehat{G(m)}} L(s,\chi)$$

On a la proposition suivante :

Proposition 1.2.4. *On a :*

$$\zeta_m(s) = \prod_{p\nmid m} \frac{1}{(1-\frac{1}{p^{o(p)s}})^{q(p)}}$$

C'est une série de Dirichlet à coefficients entiers positifs, convergeant dans $D(1)$.

Preuve : On va appliquer le lemme 1.2.3. avec $T = p^{-s}$, rappelons que $\chi(p) = 0$ lorsque $p \mid m$, on a :

$$\begin{aligned}\prod_{\chi\in\widehat{G(m)}} L(s,\chi) &= \prod_{\chi\in\widehat{G(m)}} \Big(\prod_{p\in P} \frac{1}{1-\chi(p)p^{-s}}\Big) \\ &= \prod_{p\in P}\Big(\prod_{\chi\in\widehat{G(m)}} \frac{1}{1-\chi(p)p^{-s}}\Big) \\ &= \prod_{p\nmid m} \frac{1}{(1-p^{-o(s)s})^{q(p)}}\end{aligned}$$

Qui est le résultat voulu. Le produit converge dans $D(1)$ comme produit de séries de Dirichlet convergentes dans $D(1)$.

□

En développant le produit on voit que ζ_m est une série de Dirichlet à coefficients positifs puis qu'elle est holomorphe sur $D(1)$. Cette remarque est importante car pour prouver le prochain théorème on va avoir besoin du lemme suivant sur les séries de Dirichlet à coefficients positifs.

Lemme 1.2.5. *Soit f une série de Dirichlet à coefficients positifs. Supposons que f converge sur $D(\rho)$ et qu'elle est prolongeable analytiquement en un voisinage de ρ. Alors il existe $\epsilon > 0$ tel que f converge sur $D(\rho - \epsilon)$.*

Preuve : Pour une preuve du lemme, on pourra se référer à [1] p.112. □

La première étape de la preuve du théorème qui nous interesse consiste en le théorème suivant :

Théorème 1.2.6.

- *ζ_m a un pôle simple pour $s = 1$.*
- *$L(1,\chi) \neq 0$ pour tout $\chi \neq 1$*

Preuve : Remarquons que le second point implique le premier. En effet on a vu en début de partie que $L(s,1)$ a un pôle en $s = 1$, alors si $L(1,\chi) \neq 0$ pour $\chi \neq 1$, ζ_m à un pôle en $s = 1$. Montrons donc le second point. On procède par l'absurde, supposons que pour un $\chi \neq 1$ on ait $L(1,\chi) = 0$. La fonction ζ_m serait alors holomorphe en $s = 1$, comme les $L(s,\chi)$ sont holomorphes sur $\mathcal{D}(0)\backslash\{1\}$, ζ_m serait holomorphe sur $D(0)$. Par le lemme 1.2.5. on peut donc reculer son domaine de convergence à $D(0)$. On considère maintenant $p \in P$, on a

$$\sum_{n=0}^{+\infty} p^{-n\phi(m)s} = \sum_{n=0}^{+\infty} p^{-no(p)q(p)s} \leq \Big(\sum_{n=0}^{+\infty} p^{-no(p)s}\Big)^{q(p)} = \frac{1}{(1-p^{-o(p)s})^{q(p)}}$$

ζ_m étant le produit du deuxième terme pour tout $p \nmid m$, par le même procédé de majoration la série ζ_m aurait tout ses coefficients supérieurs à ceux de la série :

$$\sum_{(n,m)=1} n^{-\phi(m)s}$$

qui diverge pour $s = 1/\phi(m)$ d'où le résultat voulu. □

1.3 Le théorème de Dirichlet

Comme vu en début de chapitre, le but de cette partie sera de déterminer un équivalent de $g_a(s) := \sum_{p\in P_a} p^{-s}$ pour $s \to 1$ et ainsi déterminer la densité de P_a. Soit χ un caractère modulo m. On pose

$$f_\chi(s) = \sum_{p\nmid m} \chi(p)p^{-s}$$

Lemme 1.3.1. *f_χ converge sur $D(1)$ et on a:*

- *Si $\chi = 1$, $f_\chi \sim_1 log(1/(s-1))$.*
- *Si $\chi \neq 1$, f_χ reste bornée lorsque $s \to 1$.*

Preuve : Le premier point est une conséquence directe de la première partie du corollaire 1.1.13 car $f_\chi(s)$ ne diffère de $\sum_{p\in P} p^{-s}$ que par un nombre fini de termes. Le second point est une conséquence de la seconde partie du même corollaire. En effet, on a

$$\log L(s,\chi) = f_\chi(s) + F_\chi(s))$$

avec $F_\chi(s) = \sum_{p,n\geq 2} \chi(p)^n (np)^{-ns}$ mais

$$|F_\chi(s)| \leq \sum_{p\in P, n\geq 2} (np)^{-ns}$$

de plus par le théorème 1.2.5.*b*) $L(1,\chi) \neq 0$ donc $\log L(s,\chi)$ et $F_\chi(s)$ restent bornées quand $s \to 1$, il en est donc de même pour $f_\chi(s)$. □

Lemme 1.3.2. *On a :*

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi\in\widehat{G(m)}} \chi(a)^{-1} f_\chi(s)$$

Preuve : On a

$$\sum_{\chi\in\widehat{G(m)}} \chi(a)^{-1} f_\chi(s) = \sum_{p\nmid m} \Big(\sum_{\chi\in\widehat{G(m)}} \chi(a^{-1}p)\Big) p^{-s}$$

mais les relations d'orthogonalité des caractères de $G(m)$ donnent

$$\sum_{\chi\in\widehat{G(m)}} \chi(a^{-1}p) = \phi(m) \quad \text{si} \quad a^{-1}p \equiv 1 \mod m$$

$$= 0 \qquad \text{sinon.}$$

on a donc bien

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi\in\widehat{G(m)}} \chi(a)^{-1} f_\chi(s).$$

□

On peut maintenant prouver le théorème :

Théorème 1.3.3. *L'ensemble P_a a une densité et sa densité vaut $\frac{1}{\phi(m)}$.*

Corollaire 1.3.4. *L'ensemble P_a est infini.*

Preuve : Par le lemme 1.3.2.

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi \in \widehat{G(m)}} \chi(a)^{-1} f_\chi(s)$$

mais par le lemme 1.3.1.

$$\sum_{\chi \in \widehat{G(m)}} \chi(a)^{-1} f_\chi(s) \sim \log \frac{1}{s-1}$$

pour $s \to 1$ d'où

$$g_a(s) \sim \frac{1}{\phi(m)} \log \frac{1}{s-1}$$

ce qui veut bien dire que P_a a pour densité $\frac{1}{\phi(m)}$. □

1.4 Une application du théorème de Dirichlet

Il existe de nombreuses applications du théorème de la progression arithmétique de Dirichlet, ici nous traitons un résultat basique de la théorie de Galois inverse qui se trouve être une conséquence de ce théorème. La question est la suivante : Soit G un groupe. Existe-t-il une extension galoisienne L de $\mathbb{Q}$ de groupe de Galois G ? La plus grande conjecture à ce sujet est la suivante : Tout groupe fini est le groupe de Galois d'une extension galoisienne des nombres rationnels. On se restreint ici au cas bien plus modeste où G est abélien fini.

Soit donc G un groupe abélien fini, c'est un $\mathbb{Z}$-module de type fini. Grâce au théorème de structure sur les Z-modules de type fini, on peut supposer que G est de la forme

$$\bigoplus_i \mathbb{Z}_{q_i^{\beta_i}}$$

où les q_i sont des nombres premiers non nécessairement distincts. On veut montrer qu'il existe une extension galoisienne de groupe de Galois G. Il suffit de faire apparaître $\bigoplus_i \mathbb{Z}_{q_i^{\beta_i}}$ dans

$$(\mathbb{Z}_m)^* \cong \mathbb{Z}_n \times \prod_{i=1}^{k} Z_{p_i - 1}$$

où $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ est un entier décomposé en produit de facteurs premiers. Comme les $\mathbb{Z}_{p_i-1}$ sont cycliques il suffit de trouver des p_i tels que $q_i^{\beta_i}$ divise $p_i - 1$ (condition $(*)$)alors $\bigoplus_i \mathbb{Z}_{q_i^{\beta_i}}$ sera un sous groupe de $\prod_i \mathbb{Z}_{p_i-1}$ correspondant à un groupe de Galois. En effet, si on considère ζ une racine primitive m-ème de l'unité dans $\mathbb{C}$ alors on sait par le cours que $\mathbb{Q}(\zeta)/\mathbb{Q}$ a pour groupe de

Galois $G_1 \cong (\mathbb{Z}_m)^*$, le théorème de correspondance de Galois fournira alors un corps E tel que $\mathbb{Q} \subset E \subset \mathbb{Q}(\zeta)$ et $Gal(\mathbb{Q}(\zeta)/E) \cong G$ qui est le résultat voulu.

On réécrit la condition $(*)$ en

$$\forall i = 1, ..., N \quad \exists p_i > q_i^{\beta_i} \quad et \quad p_i \equiv 1 \mod q_i^{\beta_i}$$

qui est une conséquence immédiate du théorème de la progression arithmétique de Dirichlet appliqué à $q_i^{\beta_i}$ et 1 d'où le résultat.

2 Anneaux d'entiers de corps de nombres

On rappelle ici quelques définitions et résultats sans preuve qui nous serons utiles par la suite. Les anneaux sont supposés commutatifs et unitaires.

2.1 Anneaux d'entiers

Définition 2.1.1. Soit R un anneau et A un sous-anneau de R.

- On dit que $x \in R$ est entier sur A si il existe $P \in A[X]$ unitaire tel que $P(x) = 0$.
- L'ensemble des éléments $x \in R$ entiers sur A forment un sous anneau A' de R que l'on appelle fermeture intégrale de A dans R.
- On dit que A est intégralement clos s'il est intègre et que sa fermeture intégrale dans son corps des fractions est A lui-même.

Proposition 2.1.2. *Soit R un anneau et A un sous anneau de R. Les propriétés suivantes sont équivalentes :*

- *$x \in R$ est entier sur A.*
- *Il existe B un sous A-module de type fini de R tel que $x \in B$.*

Proposition 2.1.3. *Soit R un anneau intègre et A un sous-anneau de R tel que R est entier sur A. Alors A est un corps si et seulement si R est un corps.*

Définition 2.1.4. Soit R un anneau et A un sous-anneau de R tel que R est un A-module libre de rang n.

- On appelle trace de $x \in R$ la trace de la multiplication par x en tant qu'endomorphisme du A-module R. On la note $Tr_{R/A}(x)$ ou $Tr(x)$ lorsque le contexte est clair.
- On appelle norme de $x \in R$ le déterminant de la multiplication par x en tant qu'endomorphisme du A-module R. On la note $N_{R/A}(x)$ ou $N(x)$ lorsque le contexte est clair.
- Pour toute famille $(x_1, ..., x_n) \in R^n$ on définit le discriminant de cette famille par

$$D(x_1, ..., x_n) = det((Tr(x_i x_j))_{1 \leq i,j \leq n})$$

Proposition 2.1.5. *Soient K/L une extension séparable de degré n, x un élément de L et P son polynôme minimal dans K. La trace et la norme de x sont entières sur A et en notant $x_1, ..., x_n$ les racines de P on a*

$$Tr(x) = x_1 + ... + x_n$$

et

$$N(x) = x_1...x_n$$

La proposition 2.1.6. que l'on montre à l'aide de 2.1.5. sera utile lors du prochain chapitre.

Proposition 2.1.6. *Dans les mêmes conditions que précédemment. En notant $\sigma_1, ..., \sigma_n$ les n K-plongements de L dans une de ses clôtures algébriques, on a pour toute K-base $(x_1, ..., x_n)$ de L*

$$D(x_1, ..., x_n) = det((\sigma_i(x_j))_{1 \leq i,j \leq n}) \neq 0.$$

Définition 2.1.7. Soit R un anneau et A un sous-anneau de R tel que R est un A-module libre de rang n. On appelle discriminant de R sur A et note $\mathfrak{D}_{R/A}$ l'idéal engendré par le discriminant d'une A-base de R.

Le discriminant de R sur A est bien défini car on montre par un bref calcul que si $(x_1, ..., x_n)$ et $(y_1, ...y_n)$ sont deux A-bases de R alors $D(x_1, ..., x_n) = p^2 D(y_1, ..., y_n)$ où p est le déterminant de la matrice de passage de $(x_1, ..., x_n)$ à $(y_1, ..., y_n)$ alors $p \in A^\times$ et ils définissent donc le même idéal.

Théorème 2.1.8. *Soient A un anneau intégralement clos de caractéristique 0, K son corps des fractions, L une extension finie de degré n de K et R la fermeture intégrale de A dans L. Alors R est un sous A-module d'un A-module libre de rang n et contient une base de L sur K.*

2.2 Modules noethérien et anneau de Dedekind

Définition 2.2.1. On dit qu'un module est noethérien si tout ses idéaux sont de types fini.

En particulier on dit qu'un anneau est noethérien si ses idéaux sont de type finis.

Proposition 2.2.2. *Si A est un anneau noethérien et E un A-module de type fini alors E est noethérien.*

Lemme 2.2.3. *Dans un anneau noethérien, tout idéal contient un produit d'idéaux premiers.*

Définition 2.2.4. On appelle anneau de Dedekind tout anneau noethérien, intégralement clos dont les ideaux premiers non nuls sont maximaux.

Théorème 2.2.5. *Soient A un anneau de Dedekind de caractéristique 0, K son corps des fractions, L une extension finie de K et R la fermeture intégrale de A dans L. Alors B est un anneau de Dedekind et un A-module de type fini.*

Définition 2.2.6. Soient A un anneau de Dedekind, K son corps des fractions. On appelle idéal fractionnaire de A tout A-module de type fini contenu dans K. On note $I(A)$ l'ensemble des idéaux fractionnaires de A. On dit de plus qu'un idéal fractionnaire est entier s'il est contenu dans A. On note de plus $P(A)$ l'ensemble des idéaux fractionnaires principaux de A.

On appelle $\mathfrak{A}(A)$ l'ensemble des idéaux premiers de A.

Théorème 2.2.7. *Soient A un anneau de Dedekind. L'ensemble $I(A)\backslash\{0\}$ est un groupe pour la multiplication usuelle des idéaux. De plus, tout idéal fractionnaire non nul I de A s'écrit de manière unique sous la forme*

$$I = \prod_{\mathfrak{p}\in\mathfrak{A}(A)} \mathfrak{p}^{n_{\mathfrak{p}}(I)}$$

où les $n_{\mathfrak{p}}(I)$ sont des entiers relatifs presque tous nuls.

Dans le cas des corps de nombre, l'anneau des entiers de ces corps sont par définition des fermetures intégrales de $\mathbb{Z}$ dans des extensions finies de $\mathbb{Q}$. Ce sont donc des anneaux de Dedekind par le théorème 3.2.2. donc le théorème 3.2.4. s'applique.

3 Discriminant et ramification

Dans la suite A est un anneau intègre de caractéristique 0, K son corps des fractions, L une extension de degré n de K et R la fermeture intégrale de A dans L.

3.1 Localisation dans un anneau de Dedekind

On rappelle ici quelques résultats sur la localisation dans les anneaux de Dedekind.

Proposition 3.1.1. *Soit S une partie multiplicative de A. Alors $S^{-1}R$ est la fermeture intégrale de $S^{-1}A$ dans L.*

Proposition 3.1.2. *On suppose que A est un anneau de Dedekind. Alors, $S^{-1}A$ est un anneau de Dedekind.*

Proposition 3.1.3. *Soit $\mathfrak{p}$ un idéal premier non nul de A et $S = A\backslash\mathfrak{p}$. Alors $S^{-1}A$ est principal et il existe p premier de $S^{-1}A$ tel que les idéaux de $S^{-1}A$ sont exactement les $(p^n)n \geq 1$.*

La prochaine proposition rend compte de l'utilité de la localisation dans les anneaux de Dedekind, en effet en combinant celle ci avec 3.1.3. on pourra toujours se ramener au cas principal ce qui sera particulièrement utile dans la prochaine partie.

Proposition 3.1.4. *Soit S une partie multiplicative de A et $\mathfrak{m}$ un idéal maximal de A tel que $\mathfrak{m} \cap S = \emptyset$. Alors*

$$S^{-1}A/\mathfrak{m}S^{-1}A \cong A/\mathfrak{m}$$

3.2 Décomposition des idéaux premiers dans une extension

Soit A un anneau de Dedekind de caractéristique 0, K son corps des fractions, L une extension de degré n de K et R la fermeture intégrale de A dans L. Par le théorème 2.2.5., R est un anneau

de Dedekind. Soit $\mathfrak{p}$ un idéal premier non nul de A. On peut décomposer l'idéal $R\mathfrak{p}$ en produits d'idéaux premiers entiers de R

$$\prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$$

avec $e_i \geq 1$ pour chaque i.

Proposition 3.2.1. *Si $\mathfrak{D}$ est un idéal premier de R tel que $R\mathfrak{p} \subset \mathfrak{D}$ alors $\mathfrak{D} = \mathfrak{P}_i$ pour un certain i.*

Preuve : Soit $\mathfrak{P}$ un idéal premier de R. La condition $R\mathfrak{p} \subset \mathfrak{D}$ implique $R\mathfrak{p}\mathfrak{D}^{-1} \subset A$ d'où $n_{\mathfrak{P}}(R\mathfrak{p}) \geq \mathfrak{n}_{\mathfrak{P}}(\mathfrak{D}) \geq 0$ pour tout $\mathfrak{P} \in \mathfrak{A}(R)$. Le résultat en découle directement. □

Notons que si $R\mathfrak{p} \subset \mathfrak{D}$ alors $R\mathfrak{p} \cap A \subset \mathfrak{D} \cap A$ or $R\mathfrak{p} \cap A = \mathfrak{p}$ est maximal donc $\mathfrak{p} = \mathfrak{D} \cap A$. D'où

$$A \to R \to R/\mathfrak{P}_i$$

a pour noyau $\mathfrak{p}$ donc $A/\mathfrak{p}$ s'identifie à un sous-anneau de $R/\mathfrak{P}_i$. Enfin par 3.2.2. ces deux anneaux sont des corps et R est un A-module de type fini donc $R/R\mathfrak{p}$ est un $A/\mathfrak{p}$-espace vectoriel de dimension finie. On définit maintenant deux nouvelles quantités.

Définition 3.2.2. On appelle degré résiduel de $\mathfrak{P}_i$ sur A la dimension du $A/\mathfrak{p}$-espace vectoriel $R/\mathfrak{P}_i$.

Définition 3.2.3. On appelle indice de ramification de $\mathfrak{P}_i$ sur A l'exposant e_i de la décomposition de $R\mathfrak{p}$ dans R.

Enfin, remarquons que $R\mathfrak{p} \cap A = \mathfrak{p}$. En effet l'inclusion $\supset$ est claire. D'un autre côté $R\mathfrak{p} \cap A$ est un idéal de A qui contient un idéal maximal, comme $1 \notin R\mathfrak{p}$, $\subset$ est vraie. D'où $R/R\mathfrak{p}$ est un $A/\mathfrak{p}$-espace vectoriel de dimension finie par le même argument que précédemment. Pour K un corps et L une extension finie de K on note $[L : K]$ la dimension de L en tant que K-espace vectoriel.

Théorème 3.2.4. *Avec les notations précédentes on a $\sum_{i=1}^{q} e_i f_i = [R/R\mathfrak{p} : A/\mathfrak{p}] = n$*

En fait, on verra dans la prochaine partie que si L/K est galoisienne, alors $e_1 = e_2 = ... = e_q$ et $f_1 = f_2 = ... = f_q$ d'où $n = efq$ en notant $e = e_1$ et $f = f_1$.
Preuve : Pour la première égalité, remarquons que tout quotient de la forme

$$\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i,$$

où $\mathfrak{B}$ est un produit d'idéaux de la forme $\mathfrak{P}_1^{e_1}...\mathfrak{P}_{i-1}^{e_{i-1}}\mathfrak{P}_i^{k}$ avec $0 \leq k \leq q$, est un R-module annulé par $\mathfrak{P}_i$ d'où $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ est un $R/\mathfrak{P}_i$-espace vectoriel et on a l'isomorphisme d'espaces vectoriels suivant

$$R/R\mathfrak{p} \cong R/\mathfrak{P}_1 \bigoplus \mathfrak{P}_1/\mathfrak{P}_1^2 \bigoplus ... \bigoplus \mathfrak{P}_1^{e_1}/\mathfrak{P}_1^{e_1}\mathfrak{P}_2 \bigoplus ... \bigoplus \mathfrak{P}_1^{e_1}...\mathfrak{P}_q^{e_q-1}/\mathfrak{P}_1^{e_1}...\mathfrak{P}_q^{e_q}$$

en plus $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ est un espace vectoriel de dimension 1 sur $R/\mathfrak{P}_i$ car ses sous espaces vectoriels sont des sous R-modules de $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ et donc des ensembles de la forme $\mathfrak{q}/\mathfrak{B}\mathfrak{P}_i$ avec $\mathfrak{q}$ un idéal de R tel que $\mathfrak{B}\mathfrak{P}_i \subset \mathfrak{q} \subset \mathfrak{B}$ mais la décomposition en idéaux premiers dans R implique que $\mathfrak{q} = \mathfrak{B}\mathfrak{P}_i$ ou $\mathfrak{q} = \mathfrak{B}$ d'où le résultat. Enfin $R/\mathfrak{P}_i$ est de dimension f_i sur $A/\mathfrak{p}$ et il y a e_i espaces vectoriels de la forme $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ d'où le résultat.

Pour la deuxième égalité on se place d'abord dans le cas ou A est principal. Par le théorème 3.1.6. R est alors un A-module libre de rang n et une A-base de R donne par réduction modulo $R\mathfrak{p}$ une $A/\mathfrak{p}$-base de $R/R\mathfrak{p}$. On se ramène à ce cas en localisant A et R en $S = A\backslash\mathfrak{p}$. On note $A' = S^{-1}A$ et $R' = S^{-1}R$ les anneaux de fractions correspondants. On sait que A' est un anneau principal possédant un unique idéal maximal $A'\mathfrak{p}$ et que R' est la fermeture intégrale de A' dans L. On a alors $[R'/R'\mathfrak{p} : A'/A'\mathfrak{p}] = n$ par le cas principal. De plus R' est un anneau de Dedekind, $R'\mathfrak{p}$ se décompose donc en idéaux premiers. Remarquons que par 4.2.1. $\mathfrak{P}_i \cap A\backslash\mathfrak{p} = \emptyset$ donc par 4.1.1. $R'\mathfrak{P}_i$ est un idéal premier non nul de R'. Enfin la décomposition de $R\mathfrak{p}$ dans R donne directement

$$R'\mathfrak{p} = \prod_{i=1}^{q} (R'\mathfrak{P}_i)^{e_i}.$$

On applique alors la première partie de la preuve à A' et B' ce qui donne

$$n = [R'/R'\mathfrak{p} : A'/A'\mathfrak{p}] = \sum_{i=1}^{q} e_i [R'/R'\mathfrak{P}_i : A'/A'\mathfrak{p}]$$

mais $A'/A'\mathfrak{p} \cong A/\mathfrak{p}$ et $R'/R'\mathfrak{P}_i \cong R/\mathfrak{P}_i$ d'où $[R'/R'\mathfrak{P}_i : A'/A'\mathfrak{p}] = f_i$ pour chaque i puis le résultat voulu. □

Proposition 3.2.5. *On a l'isomorphisme*

$$R/R\mathfrak{p} \cong \prod_{i=1}^{q} R/\mathfrak{P}_i^{e_i}$$

Il suffit d'appliquer le lemme chinois sachant que $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = R$ dès que $i \neq j$, en effet il est clair que le seul idéal maximal contenant $\mathfrak{P}_i^{e_i}$ est $\mathfrak{P}_i$. On rappelle l'énoncé du lemme.

Lemme 3.2.6. *Soit A un anneau, et $(\mathfrak{a}_i)_{i=1,\dots,q}$ une famille finie d'idéaux de A tels que $\mathfrak{a}_i + \mathfrak{a}_j = A$ dès que $i \neq j$. On a alors l'isomorphisme*

$$A/\mathfrak{a}_1 \dots \mathfrak{a}_q \cong \prod_{i=1}^{r} A/\mathfrak{a}_i$$

3.3 Discriminant et Ramification

On garde les notations de 3.2.

Définition 3.3.1. On dit que $\mathfrak{p}$, en tant qu'idéal de A, se ramifie dans R (ou dans L) si l'un des indices de ramification e_i est plus grand que 1.

Définition 3.3.2. On suppose que K et L sont des corps de nombres. On appelle idéal discriminant de R sur A (ou de L sur K), et on note $\mathfrak{O}_{R/A}$ (ou $\mathfrak{O}_{L/K}$) l'idéal de A engendré par les discriminants des bases de L sur K contenues dans R.

Remarquons que cette définition coïncide avec 3.1.5. lorsque R est un A-module libre, en effet une K-base de L contenue dans R est en particulier une famille libre de R sur A de rang $[L : K]$ donc le discriminant de cette base est associé dans A à n'importe quelle base de R sur A comme on l'a vu précédemment. De plus par 3.1.3. et 3.1.4. l'idéal discriminant est un idéal entier non nul de A.

On énonce maintenant le résultat principal de cette partie qui permet de déterminer quels sont les idéaux de A qui se ramifient dans R. On justifiera ensuite la définition d'idéal discriminant et on donnera une preuve de ce résultat.

Théorème 3.3.3. *Un idéal premier $\mathfrak{p}$ de A se ramifie dans R si et seulement si $\mathfrak{p} \mid \mathfrak{O}_{R/A}$*

Corollaire 3.3.4. *L'ensemble des idéaux premiers $\mathfrak{p}$ de A qui se ramifient dans R est fini.*

Le corollaire est une conséquence immédiate du fait que $\mathfrak{O}_{R/A} \neq (0)$ comme on l'a vu dans la dernière remarque.

Définition 3.3.5. On dit qu'un anneau est réduit s'il n'a d'autre élément nilpotent que 0.

On remarque dans un premier temps que l'isomorphisme $R/R\mathfrak{p} \cong \prod_{i=1}^{q} R/\mathfrak{P}_i^{e_i}$ définit de manière évidente une structure de $A/\mathfrak{p}$-algèbre de dimension finie sur $R/R\mathfrak{p}$. La condition $\mathfrak{p}$ se ramifie dans R se réécrit donc $R/R\mathfrak{p}$ est non réduite et on a le lemme suivant :

Lemme 3.3.6. *(Lemme 1) Soit F un corps fini ou de caractéristique 0 et $\mathfrak{F}$ une F-algèbre de dimension finie sur F. Pour que $\mathfrak{F}$ soit réduite, il faut et il suffit que $\mathfrak{D}_{\mathfrak{F}/F} \neq (0)$.*

Ici $\mathfrak{D}_{\mathfrak{F}/F}$ désigne le discriminant de $\mathfrak{F}$ sur F au sens de 3.1.5.. On aura besoin des lemmes suivants :

Lemme 3.3.7. *Soit B un anneau noethérien réduit. Alors l'idéal (0) est intersection finie d'idéaux premiers.*

Preuve : Par le lemme 3.2.3. (0) est un produit d'idéaux premiers $\mathfrak{p}_1^{e_1}...\mathfrak{p}_q^{e_q}$. Soit alors $x \in \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_q$, on a $x^{e_1+\cdots+e_q} = 0$ d'où $x = 0$ car B est réduit. □

Lemme 3.3.8. *Soient A un anneau, B_1,...,B_q des anneaux contenant A qui sont des A-modules libres de rang fini, et $B = \prod_{i=1}^{q} B_i$ leur anneau produit. Alors $\mathfrak{D}_{B/A} = \prod_{i=1}^{q} \mathfrak{D}_{B_i/A}$.*

Preuve : On se ramène au cas $q = 2$ par récurrence. Soient alors $(x_1, ..., x_m), (y_1, ..., y_n)$ des A-bases de $B_1 \times \{0\}$ et $\{0\} \times B_2$, $(x_1, ..., x_m, y_1, ..., y_n)$ est alors une base de $B_1 \times B_2$ et $Tr(x_i y_j) = Tr(0) = 0$. D'où $D(x_1, ..., x_m, y_1, ..., y_n)$ s'écrit

$$\begin{vmatrix} Tr(x_i x_{i'}) & 0 \\ 0 & Tr(y_j y_{j'}) \end{vmatrix}$$

ce qui donne le résultat voulu.

Preuve du lemme 1 : Supposons d'abord $\mathfrak{F}$ non réduite et soit $x \in \mathfrak{F}$ un élément nilpotent non nul. On pose $x_1 = x$ et on complète ce début de base en une base $(x_1, ..., x_n)$ de $\mathfrak{F}$ sur F. Alors x_1x_j est nilpotent, et ainsi la multiplication par x_1x_j est un endomorphisme nilpotent qui a donc pour seule valeur propre 0, d'où $Tr(x_1x_j) = 0$ pour chaque j. La matrice $(Tr(x_ix_j))$ a donc une ligne nulle, d'où $\mathfrak{D}_{\mathfrak{F}/F} = (D(x_1, ..., x_n)) = (0)$.

Réciproquement, supposons $\mathfrak{F}$ réduite. Alors $(0) = \bigcap_{i=1}^{q} \mathfrak{P}_i$ où les P_i sont des idéaux premiers de $\mathfrak{F}$. Comme $\mathfrak{F}/\mathfrak{P}_i$ est une algèbre intègre de dimension finie sur F, c'est un corps. Donc $\mathfrak{P}_i$ est un idéal maximal de $\mathfrak{F}$, de sorte que $\mathfrak{P}_i + \mathfrak{P}_j = \mathfrak{F}$ pour $i \neq j$. Ainsi $\mathfrak{F}$ est isomorphe au produit $\prod_{i=1}^{q} \mathfrak{F}/\mathfrak{P}_i$. On a donc $\mathfrak{D}_{L/K} = \prod_{i=1}^{q} \mathfrak{D}_{(\mathfrak{F}/\mathfrak{P}_i)/K)}$ par 3.3.8.. Or les $\mathfrak{D}_{(\mathfrak{F}/\mathfrak{P}_i)/K)}$ sont non nuls par 2.1.6., d'où $D_{\mathfrak{F}/F} \neq 0$. □

On peut donc réduire davantage la condition $\mathfrak{p}$ se ramifie dans R par $\mathfrak{D}_{(R/\mathfrak{p}R)/(A/\mathfrak{p})} = 0$ car $A/\mathfrak{p}$ est un corps fini. Or posons $S = A\backslash\mathfrak{p}$, $A' = S^{-1}A$, $R' = S^{-1}R$ et $\mathfrak{p}' = \mathfrak{p}A'$. Alors A' est un anneau principal, R' est un A'-module libre, et on a $A/\mathfrak{p} \cong A'/\mathfrak{p}'$ et $R/\mathfrak{p}R \cong R'/\mathfrak{p}'R'$. En notant alors $(e_1, ..., e_n)$ une base de R' sur A', la relation $\mathfrak{D}_{(R/\mathfrak{p}R)/(A/\mathfrak{p})} = 0$ équivaut à $D(e_1, ..., e_n) \in \mathfrak{p}'$. En effet il est clair que $D(\bar{e_1}, ..., \bar{e_n}) = \overline{D(e_1, ..., e_n)}$ où pour $x \in R'$, $\bar{x}$ désigne l'image de x dans le quotient $R'/\mathfrak{p}'R'$ et $\overline{D(e_1, ..., e_n)}$ désigne l'image dans le quotient $A'/\mathfrak{p}'A'$ de $D(e_1, ..., e_n)$. Ceci étant, si $D(e_1, ..., e_n) \in \mathfrak{p}'$ et si $(x_1, ..., x_n)$ est une base de L sur K contenue dans R, on a $x_i = \sum a'_{ij}e_j$ avec $a'_{ij} \in A'$, d'où $D(x_1, ..., x_n) = det(a_{ij})^2 D(e_1, ..., e_n) \in \mathfrak{p}'$. Comme $\mathfrak{p}' \cap A = \mathfrak{p}$, on en déduit $D(x_1, ..., x_n) \in \mathfrak{p}$ et $\mathfrak{D}_{R/A} \subset \mathfrak{p}$. Réciproquement, si $\mathfrak{D}_{R/A} \subset \mathfrak{p}$, on a $D(e_1, ..., e_n) \subset \mathfrak{p}'$ car on peut écrire $e_i = y_i/s$ avec $y_i \in R$ et $s \in S$ pour $1 \leq i \leq n$. Ainsi

$$D(e_1, ..., e_n) = s^{-2} D(x_1, ..., x_n) \in A'\mathfrak{D}_{R/A} \subset \mathfrak{p}A' = \mathfrak{p}'$$

Ce qui conclut la preuve du théorème. □

4 Le théorème de Chebotarev

Cette partie présente le théorème de Chebotarev et motive les prochaines parties. On appelle discriminant d'un polynôme le discriminant usuel obtenu à partir du résultant et on le note $\Delta(P)$. On a montré en 1.3 que toute progression arithmétique de la forme $a+bm$, $pgcd(a, b) = 1$, contient une infinité de nombre premiers, c'est le théorème de la progression arithmétique de Dirichlet. Le théorème de Chebotarev en est une généralisation. Il a été d'abord conjecturé par Frobenius en tant que généralisation de son propre théorème que l'on va énoncer ici sans preuve afin d'introduire la substitution de Frobenius d'un nombre premier p.

Soit $P \in \mathbb{Z}[X]$ de discriminant non nul. Le polynôme P définit une extension galoisienne K de $\mathbb{Q}$ et son groupe de Galois G peut être vu comme un sous-groupe de S_n où $n = deg(P)$. On sait de plus que tout élément de S_n se décompose en produit de cycles disjoint, par exemple la permutation $\sigma_1 = (6)(7)(45)(123) \in S_7$ est décomposée en produit de cycles disjoints. D'un autre côté pour p un nombre premier tel que $p \nmid \Delta(P)$, P mod p se décompose en produit de facteurs irréductibles dont les degrés forment une partition de n. On introduit alors deux notations :

Définition 4.0.1. On appelle type de σ, et on note $type(\sigma)$, la partition de n à laquelle elle correspond où on définit une partition de n comme un t-uple

$$(i_1, ..., i_k) \quad \text{vérifiant} \quad i_j \leq i_l$$

pour tout $j \leq l$ et

$$\sum_{j=1}^{k} i_j = n.$$

On a alors $type(\sigma_1) = (1, 1, 2, 3)$.

Définition 4.0.2. On appelle type de P par rapport à p, et on note $type(P, p)$, la partition formée par les degrés des facteurs irréductibles de P *mod* p.

Avec ces notations, le théorème de Frobenius s'énonce ainsi.

Théorème 4.0.3. *Soit $\sigma \in G$. La densité des nombre premiers p tels que $type(P, p) = type(\sigma)$ existe et vaut $\frac{|T(\sigma)|}{|G|}$ où $T(\sigma) = \{\epsilon \in G \mid type(\epsilon) = type(\sigma)\}$.*

Le théorème de Frobenius affirme que la "proportion" de nombres premiers p tels que le type de P par rapport p est donnée est proportionnelle au nombre d'éléments de G ayant cette même décomposition.

On aimerait maintenant savoir si cet énoncé implique celui de Dirichlet. Pour cela on peut tenter de trouver un polynôme P tel que les éléments du groupe de Galois qu'il définit ne dépendent un à un que d'une classe *mod* p. Prenons $P = X^{12} - 1$, on exclut $p = 2, 3$ car $2, 3 \mid \Delta(P)$. On considère maintenant l'extension correspondant à P de F_p que l'on note $F_p(\alpha)$. Le type de P par rapport à p est entièrement déterminé par l'action de $Frob_p$, le morphisme de Frobenius, sur les racines de P. En effet on sait par la théorie de Galois que le groupe de Galois d'un polynôme agit transitivement sur ses facteurs irréductibles et que $Gal(F_p(\alpha)/F_p)$ est engendré par $Frob_p$. En particulier, l'orbite de l'action de $Frob_p$ correspond à l'orbite de la multiplication par p dans $\mathbb{Z}/12\mathbb{Z}$. D'où $type(P, p)$ ne dépend que de p *mod* 12 et par un calcul rapide on a les types suivants

$$\begin{aligned}
p \equiv 1 \ mod\ 12 \ : &\quad 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 \\
p \equiv 5 \ mod\ 12 \ : &\quad 1, 1, 1, 1, 2, 2, 2, 2 \\
p \equiv 7 \ mod\ 12 \ : &\quad 1, 1, 1, 1, 1, 1, 2, 2, 2 \\
p \equiv 11 \ mod\ 12 \ : &\quad 1, 1, 2, 2, 2, 2, 2
\end{aligned}$$

Alors le théorème de Frobenius pour $X^{12} - 1$ implique le théorème de Dirichlet dans le cas $(a, 12)$ tel que $pgcd(a, 12) = 1$. Mais si l'on tente de généraliser ce résultat on tombe par exemple sur le cas $X^{10} - 1$ ou cette fois on obtient les types suivants

$$\begin{aligned}
p \equiv 1 \ mod\ 10 \ : &\quad 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 \\
p \equiv 3, 7 \ mod\ 10 \ : &\quad 1, 1, 4, 4 \\
p \equiv 1 \ mod\ 10 \ : &\quad 1, 1, 2, 2, 2, 2
\end{aligned}$$

Les cas $p \equiv 3$ *mod* 10 et $p \equiv 7$ *mod* 10 ne sont plus distingués donc le théorème de Frobenius pour $P = X^m - 1$ n'implique par le théorème de Dirichlet. On va maintenant formuler une généralisation du théorème de Frobenius qui revient au théorème de Dirichlet dans le cas $X^m - 1$.

4.1 Groupe de décomposition et groupe d'inertie

On utilise les mêmes notations que dans 3.1. Soit A un anneau de Dedekind de caractéristique 0, K son corps des fractions, L une extension galoisienne de degré n de K, G son groupe de Galois et R la fermeture intégrale de A dans L. Dans la suite, pour $\mathfrak{p}$ un idéal premier non nul de A et $\mathfrak{P}$ un idéal premier de R, on dira que $\mathfrak{P} \mid \mathfrak{p}$ si $\mathfrak{P}$ apparaît dans la décomposition de $R\mathfrak{p}$ dans R.

Proposition 4.1.1. *Le groupe de Galois G agit sur $I_e(R)$ l'ensemble des idéaux de R par*

$$\begin{aligned} G \times I_e(R) &\longrightarrow I_e(R) \\ (\sigma, I) &\longmapsto \sigma(I) = \{\sigma(x) : x \in I\} \end{aligned}$$

Preuve : Il suffit de remarquer que si $x \in R$ est entier sur A, $\sigma(x)$ aussi. Pour le voir on prend $P \in A[X]$ unitaire tel que $P(x) = 0$. Alors $\sigma(P(x)) = P(\sigma(x)) = 0$ d'où $\sigma(R) \subset R$. □

En fait on a $\sigma(R) = R$ pour tout $\sigma \in G$. Il suffit d'appliquer le même raisonnement avec σ^{-1}, ce qui donne $\sigma^{-1}(R) \subset R$ puis $R \subset \sigma(R)$. De plus, si $\mathfrak{p}$ est un idéal premier non nul de A et $\mathfrak{P} \mid \mathfrak{p}$ alors $\sigma(\mathfrak{P}) \mid \mathfrak{p}$. En effet on applique σ à la relation $\mathfrak{P} \cap A = \mathfrak{p}$ et le résultat est immédiat. On dira que $\mathfrak{P}$ et $\sigma(\mathfrak{P})$ sont conjugués. On veut maintenant maintenant montrer que l'ensemble des $\mathfrak{P}$ tel que $\mathfrak{P} \mid \mathfrak{p}$ n'est autre que l'ensemble des conjugués de $\mathfrak{P}$:

Proposition 4.1.2. *Soit $\mathfrak{p}$ un idéal premier non nul de A. Le groupe de Galois G agit transitivement sur l'ensemble $\{\mathfrak{P} \mid \mathfrak{p}\}$.*

On aura besoin du lemme suivant :

Lemme 4.1.3. *Soit $\mathfrak{P}_1, ..., \mathfrak{P}_r$ des idéaux premiers de R et $\mathfrak{b}$ un idéal de R tel que $\mathfrak{b} \not\subset \mathfrak{P}_i$ pour tout i. Alors il existe $b \in \mathfrak{b}$ tel que $b \notin \mathfrak{P}_i$ pour tout i.*

Preuve du Lemme : On peut supposer que les $\mathfrak{P}_i$ sont tels que $\mathfrak{P}_i \not\subset \mathfrak{P}_j$ pour tout $i \neq j$, on peut supposer de plus que les $\mathfrak{P}_i$ sont maximaux. Soit $x_{ij} \in \mathfrak{P}_j$ tel que $x_{ij} \notin \mathfrak{P}_i$. Comme $\mathfrak{b} \not\subset \mathfrak{P}_i$, il existe $a_i \in \mathfrak{b}$ tel que $a_i \notin \mathfrak{P}_i$ pour chaque i. On pose alors

$$b_i = a_i \prod_{j \neq i} x_{ij}$$

On a $b_i \in \mathfrak{b}$, $b_i \in \mathfrak{P}_j$ pour $j \neq i$ et $b_i \notin \mathfrak{P}_i$ car sinon a_i ou l'un des x_{ij}, $j \neq i$, serait dans $\mathfrak{P}_i$. On pose alors $b = b_1 + b_2 + ... + b_q$, on a en notant $\pi_{\mathfrak{P}_i}$ la projection canonique de R dans $R/\mathfrak{P}_i$:

$$\pi_{\mathfrak{P}_i}(b) = \pi_{\mathfrak{P}_i}(b_i) \neq 0$$

d'où le résultat. □

Preuve de la proposition : Soit $\mathfrak{P}$ tel que $\mathfrak{P} \mid \mathfrak{p}$. supposons qu'il existe $\mathfrak{P}'$ tel que $\mathfrak{P}' \mid \mathfrak{p}$ et $\mathfrak{P}'$ n'est pas conjugué de $\mathfrak{P}$. On applique le lemme à $\sigma(\mathfrak{P})$ et $\mathfrak{P}'$ qui sont maximaux et distincts pour tout $\sigma \in G$. On obtient un élément $x \in \mathfrak{P}'$ tel que $x \notin \sigma(\mathfrak{P}')$ pour tout $\sigma \in G$. On considère alors

$$N(x) = \prod_{\sigma \in G} \sigma(x)$$

clairement $N(x) \in \mathfrak{P}'$ et par 2.1.5., $N(x) \in A$ donc $N(x) \in \mathfrak{P}' \cap A = \mathfrak{p}$. D'autre part $x \notin \sigma^{-1}(\mathfrak{P})$, d'où $\sigma(x) \notin \mathfrak{P}$ pour tout $\sigma \in G$. Comme $\mathfrak{P}$ est premier, on en déduit que $N(x) \notin \mathfrak{P}$, ce qui contredit $N(x) \in \mathfrak{p}$. □

Corollaire 4.1.4. *Les idéaux premiers $\mathfrak{P}$ tels que $\mathfrak{P} \mid \mathfrak{p}$ ont même indice de ramification et même degré résiduel.*

Preuve : Soit $\mathfrak{P}_1$, $\mathfrak{P}_2$ tels que $\mathfrak{P}_1, \mathfrak{P}_2 \in \{\mathfrak{P} \mid \mathfrak{p}\}$ et soit $\sigma \in G$ tel que $\mathfrak{P}_2 = \sigma(\mathfrak{P}_1)$. La suite

$$1 \to \mathfrak{P}_1 \to R \xrightarrow{\sigma} R \to R/\mathfrak{P}_2 \to 1$$

est exacte d'où $\mathfrak{P}_1$ et $\mathfrak{P}_2$ ont même degré résiduel. En plus $R/R\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} R/\mathfrak{P}^{n_\mathfrak{p}(\mathfrak{P})}$ par 3.2.5. et si π désigne la projection de R sur $R/R\mathfrak{p}$, alors $\pi \circ \sigma$ permute les coordonnées des éléments du produit. Combiner ce dernier résultat avec l'identité $\sigma(\mathfrak{P}_1^{n_\mathfrak{p}(\mathfrak{P}_1)}) = \sigma(\mathfrak{P}_1)^{n_\mathfrak{p}(\mathfrak{P}_1)} = \mathfrak{P}_2^{n_\mathfrak{p}(\mathfrak{P}_1)}$ permet alors de conclure sur les indices de ramification. □

On notera e l'indice de ramification des $\mathfrak{P}$ tels que $\mathfrak{P} \mid \mathfrak{p}$ et f leurs degrés résiduels. Alors en notant $q = |\{\mathfrak{P} \mid \mathfrak{p}\}|$, on a $n = efq$.

Définition 4.1.5. Soit $\mathfrak{P}_1 \in \{\mathfrak{P} \mid \mathfrak{p}\}$. On appelle groupe de décomposition de $\mathfrak{P}_1$ et on note $D(\mathfrak{P}_1)$ le sous groupe de G formé des σ tels que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_1$.

Pour $\sigma \in D(\mathfrak{P})$ on peut définir un $A/\mathfrak{p}$-automorphisme de $R/\mathfrak{P}$ que l'on note $\overline{\sigma}$ par $\overline{\sigma}(\overline{x}) := \overline{\sigma(x)}$, par définition de $D(\mathfrak{P})$ on vérifie facilement que $\overline{\sigma}$ définit bien un $A/\mathfrak{p}$-automorphisme de $R/\mathfrak{P}$. On considère maintenant le morphisme de groupes

$$\sigma \longmapsto \overline{\sigma}$$

il a pour noyau l'ensemble des $\sigma \in D(\mathfrak{P})$ tels que $\sigma(x) - x \in \mathfrak{P}$ pour tout $x \in R$.

Définition 4.1.6. On appelle groupe d'inertie de $\mathfrak{P}$ et on note $I(\mathfrak{P})$ le groupe

$$I(\mathfrak{P}) = \{\sigma \in D(\mathfrak{P}) \mid \sigma(x) - x \in \mathfrak{P}\ \forall x \in \mathbb{R}\}$$

C'est aussi le noyau du morphisme de groupe défini précédemment et donc un sous-groupe distingué de $D(\mathfrak{P})$.
On admet maintenant le résultat suivant qui est traité en [2] (chap 6, p.106).

Proposition 4.1.7. *L'extension $R/\mathfrak{P}$ de $A/\mathfrak{p}$ est galoisienne de degré f, de groupe de Galois D/I.*

Corollaire 4.1.8. *Pour que $\mathfrak{p} \in \mathfrak{A}(A)$ ne se ramifie pas dans R, il faut et il suffit que le groupe d'inertie $I(\mathfrak{P})$ soit réduit à l'identité.*

En effet, par la proposition 4.1.7. le groupe d'inertie à pour cardinal exactement l'indice de ramification de $\mathfrak{p}$. On peut maintenant introduire la substitution de Frobenius d'un idéal premier $\mathfrak{p}$.

4.2 La substitution de Frobenius

On garde les notations du chapitre précédent. Soit $\mathfrak{p}$ un idéal premier de A qui ne se ramifie pas dans R et $\mathfrak{P}$ un idéal premier de R tel que $\mathfrak{P} \mid \mathfrak{p}$. Par 4.1.8. le groupe d'inertie de $\mathfrak{P}$ est trivial et donc le groupe de décomposition de $\mathfrak{P}$ est canoniquement isomorphe au groupe de Galois G' de $R/\mathfrak{P}/A/\mathfrak{p}$. En notant $\bar{\pi}$ cet isomorphisme on définit maintenant la substitution de Frobenius.

Définition 4.2.1. On appelle substitution de Frobenius de $\mathfrak{p}$ le générateur $\sigma_{\mathfrak{P}}$ de $D(\mathfrak{P})$ pour chaque $\mathfrak{P} \mid \mathfrak{p}$, tel que $\bar{\pi}(\sigma) = (\bar{x} \mapsto \bar{x}^{N(\mathfrak{p})})$ est le générateur privilégié de G'. On la note alors $(\mathfrak{P}, L/K)$.

Proposition 4.2.2. *Soit $\sigma(\mathfrak{P}_1) = \mathfrak{P}$ pour $\sigma \in G$. Alors $D(\mathfrak{P}) = \sigma D(\mathfrak{P}_1)\sigma^{-1}$.*

La substitution de Frobenius est alors définie à classe de conjugaison près et en particulier dans le cas où G est abélien, celle-ci ne dépend que de $\mathfrak{p}$. On la note alors $(\mathfrak{p}, L/K)$. On considère maintenant $K \subset E \subset L$ une extension galoisienne intermédiaire de L/K, on a

Proposition 4.2.3. *On note f le degré résiduel de $\mathfrak{P} \cap E$ sur K. Alors*

$$(\mathfrak{P}, L/E) = (\mathfrak{P}, L/K)^f$$

et

$$(\mathfrak{P} \cap E, E/K) = (\mathfrak{P}, L/K)|_E$$

Preuve : On pourra se réferer à [2] (chap. 6, p.108) pour une preuve. □

On étudie maintenant le cas où L/K est cyclotomique.

Proposition 4.2.4. *Lorsque $L = K(\zeta)/K$ est cyclotomique avec ζ une racine m-ème de l'unité, $(\mathfrak{p}, L/K)$ ne dépend que de la norme de $\mathfrak{p}$ modulo m.*

Preuve : Tout morphisme d'une extension cyclotomique est entièrement défini par son action sur ζ. Ici $(\mathfrak{p}, L/K)$ envoie ζ sur $\zeta^{N(\mathfrak{p})}$ et donc ne dépend que de l'orbite de $N(\mathfrak{p})$ modulo m d'où le résultat. □

Il est maintenant nécessaire de lier les notations $\Delta(P)$ et $\mathfrak{O}(L/K)$. Lorsque $\Delta(P) \neq 0$ et L est le corps de décomposition de P on a la proposition :

Proposition 4.2.5.

$$\mathfrak{O}(L/K) = (\Delta(P)).$$

On peut maintenant énoncer le théorème de Chebotarev.

Théorème 4.2.6. *(théorème de densité de Chebotarev) Soit $P \in F[X]$ unitaire de discriminant non nul, K un corps de décomposition de P et $\sigma \in G = Gal(K/F)$. La densité de l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $\Delta(P) \not\subset \mathfrak{p}$ et tels qu'il existe $\mathfrak{P} \mid \mathfrak{p}$ tel que $\sigma_{\mathfrak{P}} \in C(\sigma)$, où $C(\sigma)$ est la classe de conjugaison de σ, existe et vaut $\frac{|C(\sigma)|}{|G|}$.*

Remarquons Les idéaux premiers $\mathfrak{p}$ étant en nombre fini. Ceux-ci n'influent pas sur la densité voulue. La preuve du théorème nécessite de se placer dans le cas ou le corps de base n'est plus $\mathbb{Q}$ mais un corps de nombre F. La notion de densité utilisée en première partie n'est donc plus valable, on va donc considérer une nouvelle fonction zêta, la fonction zêta de Dedekind.

4.3 Fonctions L de Dirichlet généralisées

Soit A l'anneau des entiers d'un corps de nombre K. On suppose ici connus les résultats usuels sur les valeurs absolues de corps de nombres. On note M_K l'ensemble des valeurs absolues normalisées de K i.e. telles que leur restriction à $\mathbb{Q}$ est une valeur absolue réelle usuelle ou une valeur absolue p-adique.

Définition 4.3.1. On appelle *cycle* de K tout produit formel

$$\mathfrak{m} = \prod_{M_K} v^{m(v)}$$

où les $m(v)$ sont positifs et presque tous nuls.

Si $m(v) > 0$ pour v réelle on se restreint au cas où $m(v) = 1$. On utilisera la notation $\mathfrak{m} = \prod_{M_K \setminus \{v_\infty\}} \mathfrak{p}^{m(\mathfrak{p})} \times \mathfrak{p}_\infty$ où $\mathfrak{p}_\infty$ désigne la valeur absolue réelle. Lorsque $m(p_\infty) = 0$ on utilisera sans distinction la notation $\mathfrak{m}$ pour désigner l'idéal de K correspondant. L'étude de la fonction zêta de Dedekind est un cas particulier de l'étude des fonctions L de Dirichlet généralisées à un corps de nombres que l'on va parcourir ici. Soit $\mathfrak{m} = \prod_{i=1}^{q} \mathfrak{p}_i^{e_i}$ un idéal de A. On appelle $I_\mathfrak{m}(A)$ (resp. $P_\mathfrak{m}(A)$) le groupe des idéaux (resp. idéaux principaux) premiers à $\mathfrak{m}$. On rappelle que l'on a le théorème :

Théorème 4.3.2. *Le groupe quotient* $\dfrac{I(A)}{P(A)}$ *est fini.*

Corollaire 4.3.3. *On a*

$$I_\mathfrak{m}(A)/P_\mathfrak{m}(A) \cong I(A)/P(A)$$

et chaque classe de $I_\mathfrak{m}(A)/P_\mathfrak{m}(A)$ *admet un représentant entier.*

Preuve : Il suffit de montrer que chaque classe de $I(A)/P(A)$ à un représentant dans $I_\mathfrak{m}(A)$. Soit donc $\mathfrak{K}$ une classe de $I(A)/P(A)$ et $\mathfrak{a} \in \mathfrak{K}$, on peut le supposer entier. On commence, à l'aide du lemme chinois, par résoudre les congruences

$$\alpha \equiv p_i^{e_i} \ mod \ \mathfrak{p}^{e_i+1}$$

où les $p_i \in \mathfrak{p}_i$ est premier pour chaque i. Alors $\mathfrak{a}(\alpha^{-1}) \in I_\mathfrak{m}(A)$ ce qui conclut la preuve. □

On reprend maintenant la notation $\mathfrak{m}$ pour désigner $\mathfrak{m} \times v_\infty$. On note maintenant $P_\mathfrak{m} := P_\mathfrak{m}(A)$ lorsque aucune confusion n'est à craindre, de même pour $I_\mathfrak{m}(A)$. On considère maintenant le sous-groupe $P(\mathfrak{m})$ de $P_\mathfrak{m}$ dont les éléments sont ceux de $P_\mathfrak{m}$ tels que pour toute valeur absolue réelle v induite par $\sigma_v \in G$ telle que $m(v) > 0$ dans $\mathfrak{m}$. On a $\sigma_v(P(\mathfrak{m})) \subset \mathbb{R}^+$. On considère maintenant le quotient $I_\mathfrak{m}/P(\mathfrak{m})$.

Théorème 4.3.4. *Le groupe* $I_\mathfrak{m}/P(\mathfrak{m})$ *est fini.*

Preuve : La preuve peut être trouvée dans [3](chap. VI, p.127). □

Il s'avère que ce groupe généralise la notion de progression arithmétique *mod* m à un corps de nombre quelconque et justifie l'appellation fonction L de Dirichlet généralisées.

On considère χ un caractère du groupe abélien fini $I_\mathfrak{m}/P(\mathfrak{m})$

Définition 4.3.5. Soit I un idéal entier non nul de A. On appelle norme de I et on note $N(I)$ le nombre $card(A/I)$.

Proposition 4.3.6. *La norme d'idéal est multiplicative.*

Proposition 4.3.7. *Soit $x \in A$, alors $|N(x)| = N(Ax)$, où $N(x)$ désigne la norme de x au sens de 2.1.4.*

On étend χ en un caractère de $I_e(A)$ de la même manière qu'en partie 1.

Définition 4.3.8. On appelle fonction L de K associée à χ la série

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

où la somme parcourt les idéaux non nuls de A.

Définition 4.3.9. On appelle fonction zêta de Dedekind de K et on note ζ_K la série $L(1, s)$.

On cherche à déterminer $N(\mathfrak{p})$ pour $\mathfrak{p}$ un idéal premier de K. On sait que pour $\mathfrak{p}$ un idéal premier de A, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ pour un certain p premier. On a vu en 3.2 que A/Ap est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie égale à $[K : \mathbb{Q}]$. En particulier A/Ap à pour cardinal $p^{[K:\mathbb{Q}]}$. Enfin

$$N(Ap) = \prod_{i=1}^{q} N(\mathfrak{p}_i)^{e_i}$$

ou les $\mathfrak{p}_i$ sont par 3.2.1. exactement les idéaux premiers tels que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ d'où $N(\mathfrak{p}_i) = p_i^f$ avec $1 \leq f_i \leq [K : \mathbb{Q}]$, f_i est en fait par 3.2.4. le degré résiduel de $\mathfrak{p}_i$ sur $\mathbb{Z}$. On peut maintenant prouver la proposition suivante :

Proposition 4.3.10. *Pour tout caractère χ de $I_{\mathfrak{m}}/P(\mathfrak{m})$. La fonction L associée à χ converge absolument sur $D(1)$, y est holomorphe et on a*

$$L(\chi, s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{a})}{N(\mathfrak{p})}}$$

où le produit parcourt les idéaux premiers non nuls de A.

Preuve : On note log la branche principale du logarithme. On prend formellement le logarithme du produit

$$f(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{a})}{N(\mathfrak{p})}}$$

ce qui donne la série

$$\log(f(s)) = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{\chi(\mathfrak{p})}{kN(\mathfrak{p})^{-ks}}$$

et on a

$$\log(f(s)) = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{\chi(\mathfrak{p})}{kN(\mathfrak{p})^{-ks}} = \sum_{p} \sum_{\mathfrak{p} \in E_p} \sum_{k=1}^{\infty} \frac{\chi(\mathfrak{p})}{kN(\mathfrak{p})^{-ks}}$$

d'où

$$|\log(f(s))| \leq \sum_{k,p} \frac{1}{kp^{k[K:\mathbb{Q}]Re(s)}} \leq [K:\mathbb{Q}] \times \log(\zeta(s))$$

dans $D(1)$ ce qui donne la convergence absolue et uniforme dans $D(1)$ du produit

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})}} = \exp\Big(\sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{\chi(\mathfrak{p})}{kN(\mathfrak{p})^{-ks}} \Big).$$

Par l'unique décomposition en idéaux premiers des idéaux de A, on montre ensuite l'égalité exactement de la même manière que pour le produit eulérien des fonctions L de Dirichlet vue en 1.1.7.. □

On voudrait maintenant montrer que $L(1, s)$ admet un pôle simple en $s = 1$.
On sait que chaque classe admet un représentant entier sur A. On commence donc par décomposer $L(\chi, s)$ en une somme finie

$$L(\chi, s) = \sum_{\mathfrak{K}} L_{\mathfrak{K}}(\chi, s)$$

où la somme parcourt les classes $\mathfrak{K}$ de $I_{\mathfrak{m}}/P(\mathfrak{m})$ et $\zeta_{\mathfrak{K},K}(s) = \sum_{\mathfrak{a} \in \mathfrak{K} \cap I_e(A)} \frac{1}{N(\mathfrak{a})^s}$. On peut en fait se ramener à l'étude de la fonction zêta de Riemann.

Théorème 4.3.11. *Soit $\mathfrak{K}$ une classe de $I_{\mathfrak{m}}/P(\mathfrak{m})$. Si l'on note $j(\mathfrak{K}, t)$ le nombre d'idéaux $\mathfrak{a}$ de A tels que $N(\mathfrak{a}) \leq t$ alors on a*

$$j(\mathfrak{K}, t) = Ct + O(t^{1-(1/[K:\mathbb{Q}])}),\ t \to \infty,$$

où $C > 0$ est une constante qui ne dépend que de K.

Corollaire 4.3.12. *La fonction zêta de K a un pôle simple en $s = 1$.*

La preuve est admise et traitée dans [3](chap. VIII p.161).

Corollaire 4.3.13. *On a*

$$\sum_{\mathfrak{p} \in P_K} 1/N(\mathfrak{p})^s \sim_1 log(\frac{1}{s-1})$$

La preuve est la même que dans le cas $K = \mathbb{Q}$. □

Définition 4.3.14. On définit alors la densité analytique sur le corps K d'un ensemble P_1 d'idéaux premiers de K par la limite, si elle existe,

$$d(P_1) = \lim_{s\to 1, s>1} \big(\sum_{\mathfrak{p}\in P_1} \frac{1}{N(\mathfrak{p})^s}\big)/\log(\frac{1}{s-1})$$

On admet maintenant deux théorèmes sans preuves qui sont conséquences d'un théorème plus profond de la théorie du corps de classes que l'on énonce maintenant :

Théorème 4.3.15. *(Loi de réciprocité d'Artin) On suppose que L/K est abélienne. Il existe H un sous-groupe du quotient $I_\mathfrak{m}/P(\mathfrak{m})$ tel que $I_\mathfrak{m}/H \cong Gal(L/K)$ où l'isomorphisme est donné par $\mathfrak{p} \longmapsto (\mathfrak{p}, L/K)$ en étendant ce morphisme aux idéaux fractionnaires par multiplicativité.*

Théorème 4.3.16. *Pour tout caractère $\chi \neq 1$ de $I_\mathfrak{m}/P(\mathfrak{m})$, on a $L(\chi, 1) \neq 0$.*

On a alors le théorème de Dirichlet généralisé :

Corollaire 4.3.17. *On note $a_\mathfrak{m} = [I_\mathfrak{m} : P(\mathfrak{m})]$ l'ordre du groupe $I_\mathfrak{m}/P(\mathfrak{m})$ et $\mathfrak{K}_0$ une de ses classes. Alors $d(\mathfrak{K}_0 \cap \mathfrak{A}(A)) = 1/a_\mathfrak{m}$.*

Preuve : On procède exactement de la même manière que pour la preuve du théorème de Dirichlet en multipliant par $\chi(\mathfrak{K}_0^{-1})$ les relations à la place de $\chi(a^{-1})$, les relations d'orthogonalité permettent alors de conclure. □

En fait pour $P(\mathfrak{m}) \subset H \subset I_\mathfrak{m}$ un sous-groupe de $I_\mathfrak{m}$ le résultat reste vrai en remplaçant $a_\mathfrak{m}$ par $h_\mathfrak{m} = [I_\mathfrak{m} : H]$, en particulier pour H tel que $I_\mathfrak{m}/H \cong Gal(L/K)$ ce qui donne la preuve du théorème de Chebotarev dans le cas abélien. Cependant, la preuve originale de Chebotarev n'utilise pas de théorie du corps de classes, on expose alors une partie de sa stratégie dans la prochaine partie.

4.4 Preuve du théorème

Soit K un corps de nombres et L une extension galoisienne finie de K. La preuve originale de Chebotarev est en trois partie. D'abord une réduction au cas où L/K est abélienne, puis le cas particulier où L/K est cyclotomique et enfin une résolution dans le cas abélien. On expose ici la première et la troisième partie du raisonnement. On pose $n = [L : K]$ et $G = Gal(L/K)$.

Preuve : Soit $\sigma \in G$, on note E le sous corps de L fixé par $< \sigma >$ et f l'ordre de σ. On veut montrer que le théorème est vrai pour $(L/K, C(\sigma))$ si et seulement si il est vrai pour $(L/E, \{\sigma\})$. Soit $P_{L/K,\mathfrak{m}}(\sigma)$ l'ensemble des idéaux premiers $\mathfrak{p}$ de K vérifiant l'hypothèse et premier à $\mathfrak{m}$. Soit de plus $\bar{P}_{L/K,\mathfrak{m}}(\sigma)$ l'ensemble des idéaux premiers de L tels que $\mathfrak{P} \mid \mathfrak{p}$ et $(\mathfrak{P}, L/K) = \sigma$ pour $\mathfrak{p} \in P_{L/K,\mathfrak{m}}(\sigma)$. Soit maintenant $P'_{L/E,\mathfrak{m}}(\sigma)$ l'ensemble des idéaux premiers $\mathfrak{q}$ de $P_{L/E,\mathfrak{m}}(\sigma)$ ayant comme degré résiduel 1 sur $\mathfrak{q} \cap K$. Alors $\bar{P}_{L/K,\mathfrak{m}}(\sigma)$ et $P'_{L/E,\mathfrak{m}}(\sigma)$ sont en bijection. En effet par 4.2.3., $(\mathfrak{P} \cap E, E/K) = (\mathfrak{P}, L/K)|_E = \sigma|_E$, mais par définition de E, $\sigma|_E = id_E$. Donc $D(\mathfrak{q})$ est

réduit à l'identité, d'où le degré résiduel de $\mathfrak{q}$ sur L est 1. Si N désigne le cardinal de $\{\mathfrak{P} \mid \mathfrak{p}\}$, on a alors d'un côté

$$[L : K] = [L : E] \times [E : K] = f[E : K]$$

et de l'autre

$$[L : K] = efN = fN$$

d'où $N = [L : K]$ et l'assertion voulue. Mais $P'_{L/E,\mathfrak{m}}(\sigma)$ ne diffère de $P_{L/E,\mathfrak{m}}(\sigma)$ que par les idéaux premiers $\mathfrak{q} \mid \mathfrak{p}$ étant ramifiés ou ayant degré résiduel > 1 sur $\mathbb{Q}$, mais ceux-ci ont densité de Dirichlet 0. Si on considère maintenant

$$\rho \ : \ P'_{L/E,\mathfrak{m}}(\sigma) \longmapsto P'_{L/K,\mathfrak{m}}(\sigma) \ ; \ \mathfrak{q} \longmapsto \mathfrak{q} \cap K$$

Alors ρ est surjective et pour chaque $\mathfrak{p} \in P_{L/K,\mathfrak{m}}(\sigma)$, $\rho^{-1}(\mathfrak{p}) \cong \{\mathfrak{P} \in \bar{P}_{L/K,\mathfrak{m}}(\sigma) \ ; \ \mathfrak{P} \mid \mathfrak{p}\}$ par la bijection précédente. Mais si l'on note $Z(\sigma) = \{\tau \in G \ ; \ \tau\sigma = \sigma\tau\}$, alors $\{\mathfrak{P} \in \bar{P}_{L/K,\mathfrak{m}}(\sigma) \ ; \ \mathfrak{P} \mid \mathfrak{p}\}$ a même cardinal que $Z(\sigma)/ < \sigma >$. En effet les groupes de décomposition de $\mathfrak{P}_1, \mathfrak{P}_2 \in \{\mathfrak{P} \in \bar{P}_{L/K,\mathfrak{m}}(\sigma) \ ; \ \mathfrak{P} \mid \mathfrak{p}\}$ sont conjugués, disons $D(\mathfrak{P}_1) = \tau D(\mathfrak{P}_2)\tau^{-1}$, donc $(\mathfrak{P}_1, L/K) = (\mathfrak{P}_2, L/K)$ si et seulement si τ commute avec $(\mathfrak{P}_2, L/K)$. Enfin on obtient alors

$$d(P_{L/K,\mathfrak{m}}(\sigma)) = \frac{1}{[Z(\sigma) :< \sigma >]} d(P'_{L/E,\mathfrak{m}}(\sigma))$$

En supposant que le théorème de Chebotarev est vrai pour L/E et σ on obtient alors

$$d(P_{L/K,\mathfrak{m}}(\sigma)) = \frac{f}{|Z(\sigma)|} \frac{1}{f} = \frac{|C(\sigma)|}{|G|}$$

On peut donc se restreindre au cas ou L/K est abélienne. Remarquons qu'avec la loi de réciprocité d'Artin, on a prouvé le théorème de densité de Chebotarev.
La seconde partie de la méthode de Chebotarev consiste à résoudre le cas ou $L = K(\zeta)$, pour ζ une racine m-ème de l'unité tel que (m) est premier à $\mathfrak{O}_{L/K}$. La preuve suit une démarche similaire à celle de Dirichlet qui est en fait le cas particulier $L = \mathbb{Q}(\zeta)$ et $K = \mathbb{Q}$. Cependant elle nécessite les fonctions L d'Artin qui généralisent les fonctions L abéliennes. Leur traitement étant assez technique on admet cette partie qui ne contient pas les idées clés de Chebotarev.

Par la première partie on peut supposer L/K abélienne. Soit m un nombre premier de $\mathbb{N}$ tel que (m) est premier à $\mathfrak{O}_{L/K}$ et ζ une racine primitive m-ème de l'unité. Alors $H = Gal(K(\zeta)/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ et $Gal(L(\zeta)/K) \cong G \times H$. Il est clair que si $\mathfrak{p}$ un idéal premier de K a pour substitution (σ, τ) dans $G \times H$ alors il a pour substitution σ dans G. Alors en notant d_{inf} la quantité définie de la même manière que la densité en remplaçant la limite par une limite inférieure on a

$$d_{inf}(P_{L/K,\mathfrak{m}}(\sigma)) \geq \sum_{\tau \in H} d_{inf}(P_{L(\zeta)/K}((\sigma, \tau)))$$

Soit maintenant $\sigma \in G$ et $\tau \in H$. On suppose que n divise l'ordre de τ, alors $< (\sigma, \tau) >$ et $G \times \{1\}$ ont intersection triviale. En effet $(\sigma^k, \tau^k) = (\sigma', 1)$ implique $n \mid k$ d'où $\sigma^k = 1$. Alors le sous corps E de $K(\zeta)$ fixé par $< (\sigma, \tau) >$ vérifie $E(\zeta) = L(\zeta)$ de sorte que $E(\zeta)/L$ est cyclotomique. En

effet l'extension $L(\zeta)/E.K(\zeta)$ a pour groupe de Galois $Gal(L(\zeta)/E) \cap Gal(L(\zeta)/K(\zeta)) = \{id\}$. Par la deuxième partie, la densité $d(P_{L(\zeta)/E}((\sigma,\tau))$ existe et à la valeur annoncée. Par la première partie c'est donc aussi le cas pour $d(P_{L(\zeta)/K}((\sigma,\tau)))$ qui vaut alors $1/|G||H|$. En notant H_n les éléments de H d'ordre divisible par n et en sommant sur τ de la même manière que dans l'inégalité précédente on obtient

$$d_{inf}(P_{L/K,\mathfrak{m}}(\sigma)) \geq |H_n|/|G||H|$$

mais par le théorème de Dirichlet on peut toujours trouver m tel que (m) est premier à $\mathfrak{O}_{L/K}$ et $m \equiv 1 \; mod \; n^k$ pour tout k d'où en faisant varier m sur ceux-ci on obtient

$$d_{inf}(P_{L/K,\mathfrak{m}}(\sigma)) \geq 1/|G|$$

On définit maintenant d_{sup} comme la densité de Dirichlet où l'on remplace la limite par une limite supérieure. Le résultat étant vrai pour chaque σ et les $P_{L/K,\mathfrak{m}}(\sigma)$ étant disjoint on a $1 \geq \sum_{\sigma \in G} d_{inf}(P_{L/K,\mathfrak{m}}(\sigma)) \geq |G| \times 1/|G|$ d'où $d_{inf}(P_{L/K,\mathfrak{m}}(\sigma)) = 1/|G|$. Alors par définition de la densité et

$$\sum_{\mathfrak{p} \in P_{L/K,\mathfrak{m}}(\sigma)} \frac{1}{N(\mathfrak{p})^s} / \log(\frac{1}{s-1})$$

étant strictement décroissante sur $]1, +\infty[$, il suffit que la limite supérieure existe pour qu'elle coïncide avec la limite inférieure. Ce qui est clair, d'où $d(P_{L/K,\mathfrak{m}}(\sigma))$ existe et à la valeur annoncée. □

Références :

[1] Jean-Pierre Serre, Cours d'arithmétique, Presses Universitaires de France, 1994.
[2] Pierre Samuel, Théorie algébrique des nombres, Hermann, 1997.
[3] Serge Lang, Algebraic number theory, Springer-Verlag, New York, 1994.
[4] Jürgen Neukirch, Algebraic number theory, Springer-Verlag, Berlin, 1999.
[5] P. Stevenhagen et H.W. Lenstra, Jr., *Chebotarëv and his Density Theorem*,
https://www.math.leidenuniv.nl/ hwl/PUBLICATIONS/1996d/art.pdf