Travail encadré de Mathématiques

Le Théorème de Progression Arithmétique de Dirichlet

Auteur :
Sacha Cardonna

Référent :
Sylvain Brochard

Introduction

Les nombres premiers forment l'une des notions les plus simples des mathématiques, mais également l'une des plus déroutantes. En effet, il s'agit d'un concept de base en arithmétique, et sert pourtant de fondation dans de nombreuses théories mathématiques avancées. Ils sont toujours autant étudiés depuis de nombreuses années, mais restent auréolés de mystères : il n'existe pas de formule algébrique permettant d'atteindre un nombre premier, donc il reste impossible d'en obtenir une définition ensembliste satisfaisante. Depuis EUCLIDE, nous avons le résultat suivant :

THÉORÈME. *Il existe une infinité de nombres premiers.*

Preuve. Supposons qu'il n'existe qu'un nombre fini de nombres premiers $\{p_1, p_2, \ldots, p_n\}$. Considérons alors le produit augmenté $p = 1 + \prod_{i=1}^{n} p_i$. On constate que pour tout $i \in [\![1, n]\!]$, le reste de la division euclidienne de p par p_i est égal à 1. Comme p n'est divisible par aucun nombre premier, p est premier, ce qui contredit que l'hypothèse que la liste $\{p_1, p_2, \ldots, p_n\}$ contient tous les nombres premiers. □

Les nombreux résultats qui ont suivi depuis nous apportent la preuve que cette classe de nombre n'a pas fini de surprendre les mathématiciens. Les applications des travaux sur les nombres premiers sont très nombreuses : on peut citer notamment la cryptographie, avec l'algorithme `RSA`, qui sert à la plupart des transactions sécurisées sur internet. L'objectif de ce travail est de démontrer le théorème de progression arithmétique de Dirichlet :

THÉORÈME. *Soient $a, m \in \mathbb{N}^*$, tels que $a \wedge m = 1$. Il existe une infinité de nombres premiers p vérifiant $p \equiv a[m]$. Autrement dit, la progression arithmétique suivante :*

$$\{a + mn\}_{n\in\mathbb{N}} = \{a, a + m, a + 2m, ...\}$$

admet une infinité de nombres premiers. En notant $\mathcal{P}$ l'ensemble des nombres premiers, on a donc :

$$\operatorname{card}\left(\mathcal{P} \cap \{a + mn\}_{n\in\mathbb{N}}\right) = \infty$$

En 1785, au cours de sa démonstration de la loi de réciprocité quadratique, le mathématicien Adrien-Marie Legendre introduit ce résultat sans le démontrer. Ce n'est que plus de cinquante ans plus tard, en 1837, que Gustav Lejeune-Dirichlet démontre ce théorème, devant l'Académie des Sciences de Berlin. Ce résultat, sortant du cadre de la théorie algébrique des nombres, est à l'origine de la récente théorie analytique des nombres, la branche des mathématiques consistant à utiliser des méthodes d'analyse mathématique pour résoudre des problèmes concernant les nombres entiers. Nous suivrons ainsi la preuve rédigée par ce dernier [1], mêlant l'arithmétique à la théorie des groupes et l'analyse complexe. Divisé en sept parties, l'objectif du travail est de balayer avec précision l'ensemble des mathématiques utiles à la résolution de notre problème. Nous commencerons par donner une preuve d'une version faible du théorème de Dirichlet, en utilisant la théorie des polynômes cyclotomiques.

Je tenais à remercier expressément monsieur Sylvain Brochard, maître de conférences à l'Université de Montpellier, pour son accompagnement tout au long de ce projet. La crise sanitaire, la surcharge de travail et sa vie familiale ne l'ont jamais empêché de suivre l'avancement de mon humble mémoire avec intérêt, de me donner des pistes de résolution pour certains problèmes, et de m'éclairer sur quelques notions qui me paraissaient obscures. Je lui exprime également toute ma gratitude et ma reconnaissance pour m'avoir soutenu dans l'avancement de mon cursus, et ce depuis le début de mes études en mathématiques. Monsieur Sylvain Brochard a grandement influencé mes objectifs et mes ambitions, m'a donné le goût de la recherche, et à ce titre j'espère poursuivre dans la voie qu'il a ouverte pour moi.

1. Il en existe aujourd'hui quelques autres, comme par exemple celle introduite par Harold N. Shapiro, qui est une démonstration purement algébrique.

Table des matières

Chapitre 1

Version faible du Théorème de Dirichlet

Dans cette section, on s'intéresse à une version faible du théorème de progression arithmétique :

Théorème 1.0.1 (Cas faible du théorème de Dirichlet) *Soit $n \in \mathbb{N}$, où $n \geq 1$. Il existe une infinité de nombres premiers p vérifiant $p \equiv 1[n]$.*

Leonhard Euler démontre ce théorème de manière purement algébrique, en s'aidant notamment dela théorie des polynômes cyclotomiques. On se charge ici de présenter cette preuve. Commençons tout d'abord par rappeler quelques définitions et résultats sur les outils mis en jeu au sein de la démonstration.

1.1 Définitions et résultats utiles

Définition 1.1.1 *Soit $\lambda \in \mathbb{N}$. λ est dit* premier *s'il admet exactement deux diviseurs entiers distincts positifs : λ et 1. De plus, deux nombres entiers sont dits* premiers entre eux *lorsqu'ils n'admettent aucun diviseur commun, sinon l'unité.*

On définit maintenant l'un des anneaux les plus célèbres de l'arithmétique.

Définition 1.1.2 *Soit $n \in \mathbb{N}$. On définit la relation d'équivalence $\sim$ sur $\mathbb{Z}$ par $x \sim y$ si et seulement si $n \mid x - y$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence. Alors $(\mathbb{Z}/n\mathbb{Z}, +, *)$ est un anneau.* [1]

Nous allons travailler avec le groupe cyclique des racines n-ièmes de l'unité, donc rappelons également ce qu'est un groupe cyclique :

Définition 1.1.3 *Un groupe G est dit* cyclique *s'il est à la fois* fini *et* monogène. [2]

1. Si $n \in \mathcal{P}$, $(\mathbb{Z}/n\mathbb{Z}, +, *)$ est un corps et on le note $\mathbb{F}_n^*$.
2. C'est-à-dire qu'il existe un élément $a \in G$ tel que tout élément du groupe est une puissance de a : on appelle alors a générateur du groupe G, et on note $G = \langle a \rangle$.

Définissons également l'indicatrice d'Euler, utile en théorie des groupes et essentielle pour la suite :

Définition 1.1.4 *L'indicatrice d'Euler est la fonction ϕ définie par :*

$$\begin{aligned}\phi\ : \mathbb{N}^* &\longrightarrow \mathbb{N}^* \\ n &\longmapsto \phi(n) = \text{card}\,\{\lambda \in [\![1, n]\!] \mid \text{pgcd}(n, \lambda) = \lambda \wedge n = 1\}\end{aligned}$$

Autrement dit, elle indique le nombre d'entiers premiers avec n entre 1 et n.

On rappelle aussi le théorème de Lagrange sur les groupes.

Théorème 1.1.5 (Lagrange) *Soit G un groupe fini, et H un sous-groupe de G. Alors le cardinal de H divise le cardinal de G.*

On se charge maintenant de définir le groupe des racines n-ièmes de l'unité, ainsi que les générateurs de ce groupe.

Définition 1.1.6 *Soit $n \in \mathbb{N}^*$. On appelle* groupe des racines n-ièmes de l'unité *l'ensemble $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ muni de la multiplication.*

Lemme 1.1.7 *$(\mathbb{U}_n, *)$ est un groupe cyclique.*

Preuve. On considère l'application suivante :

$$\begin{aligned}f\ : (\mathbb{Z}/n\mathbb{Z}, +) &\longrightarrow (\mathbb{U}_n, *) \\ \bar{k} &\longmapsto f(\bar{k}) = \exp\left(i\frac{2k\pi}{n}\right)\end{aligned}$$

L'application f est bien définie car $\exp\left(i\frac{2k\pi}{n}\right)$ ne dépend que de la classe de k modulo n. On peut vérifier rapidement que f est un morphisme de groupe. Soient maintenant $\bar{k}, \bar{k}' \in \mathbb{Z}/n\mathbb{Z}$. On a :

$$f(\bar{k}) = f(\bar{k}') \iff \exp\left(i\frac{2k\pi}{n}\right) = \exp\left(i\frac{2k'\pi}{n}\right) \iff \frac{2k\pi}{n} \equiv \frac{2k'\pi}{n}[2\pi] \iff k \equiv k'[n] \iff \bar{k} = \bar{k}'$$

Donc f est injective. Comme $\text{card}\,(\mathbb{Z}/n\mathbb{Z}) = \text{card}(\mathbb{U}_n)$, on en déduit que f est un isomorphisme. Ainsi comme $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, il en est de même pour $(\mathbb{U}_n, *)$. □

Lemme 1.1.8 *Les générateurs de $(\mathbb{U}_n, *)$ sont les $\xi_k = \exp(i\frac{2k\pi}{n})$, avec $k \in [\![0, n-1]\!]$, où k et n sont premiers entre eux.*

Preuve. On écrit $\mathbb{U}_n = \{1, \exp\left(i\frac{2\pi}{n}\right), \exp\left(i\frac{4\pi}{n}\right), \ldots, \exp\left(i\frac{2(n-1)\pi}{n}\right)\} = \{1, \lambda, \lambda^2, \ldots \lambda^{n-1}\}$ avec $\lambda = \exp\left(i\frac{2\pi}{n}\right)$, donc λ est un générateur de $\mathbb{U}_n$. Soit $k \in [\![1; n-1]\!]$. Alors ξ_k est un générateur de $\mathbb{U}_n$:

$$\begin{aligned}\exists k' \in [\![1; n-1]\!], (\xi_k)^{k'} = \lambda &\iff \exp\left(i\frac{2kk'\pi}{n}\right) = \exp\left(i\frac{2\pi}{n}\right) \\ &\iff kk' \equiv 1\ [n]\end{aligned}$$

On utilise alors l'identité de Bézout :

$$\exists k' \in [\![1, n-1]\!], kk' \equiv 1\ [n] \iff \exists k' \in [\![1, n-1]\!], \exists u \in \mathbb{Z}, kk' + un = 1 \iff k \wedge n = 1$$

ce qui achève la preuve. □

Définition 1.1.9 *Soit $n \in \mathbb{N}^*$. On nomme* racine primitive n-ième de l'unité *dans $\mathbb{C}$ tout générateur de $(\mathbb{U}_n, *)$: c'est-à-dire tout élément ξ tel que $\xi^k = 1$ pour $k \in [\![0, n-1]\!]$. On note désormais $\mathfrak{P}_n(\mathbb{C})$ l'ensemble des racines primitives n-ièmes de l'unité.*

1.2 Théorie des polynômes cyclotomiques

On s'intéresse maintenant aux polynômes cyclotomiques et on présente quelques résultats sur ceux-ci.

Définition 1.2.1 *Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. Le polynôme P est dit* primitif *si* $\operatorname{pgcd}(a_0, a_1, \ldots, a_n) = 1$.

Proposition 1.2.2 *Soient $P, Q \in \mathbb{Z}[X]$ tous deux primitifs. Alors le polynôme produit $R = PQ$ est primitif.*

Preuve. Soient $P, Q \in \mathbb{Z}[X]$ tels que $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$. Supposons que P et Q sont primitifs, et en raisonnant par l'absurde, montrons que $R(X) = PQ(X) = \sum_{k=0}^{n+m} c_k X^k$ est primitif. Si ce n'est pas le cas, il existe $p \in \mathcal{P}$ tel que p divise c_k pour tout $k \in [\![0, n+m]\!]$. Pour $A \in \mathbb{Z}[X]$, on note $\overline{A}$ le projeté [3] de P dans $(\mathbb{Z}/n\mathbb{Z})[X]$. Comme p divise tous les c_k, on a $\overline{R} = 0$, donc $\overline{PQ} = \overline{P} \times \overline{Q} = 0$. Mais $(\mathbb{Z}/n\mathbb{Z})[X]$ est intègre car $\mathbb{F}_p^*$ est un corps, donc on a $\overline{A} = 0$ ou $\overline{B} = 0$. Donc cela voudrait dire que p divise tous les a_k ou tous les b_k, ce qui est impossible car $\operatorname{pgcd}(a_0, a_1, \ldots, a_n) = \operatorname{pgcd}(b_0, b_1, \ldots, b_n) = 1$. Donc R est bien un polynôme primitif. □

Définition 1.2.3 *Soit $n \in \mathbb{N}^*$. On appelle* n-ième polynôme cyclotomique *le polynôme suivant :*

$$\Phi_n(X) = \prod_{\xi \in \mathfrak{P}_n(\mathbb{C})} (X - \xi)$$

3. Si $A = \sum_{k\in\mathbb{N}} s_k X^k$, son projeté est $\overline{A} = \sum_{k\in\mathbb{N}} \overline{s_k} X^k$, où $\overline{s_k}$ est la classe de s_k modulo p.

Proposition 1.2.4 *Les polynômes cyclotomiques sont unitaires, et* $\deg(\Phi_n(X)) = \phi(n)$.

Preuve. Soit $n \in \mathbb{N}^*$. L'écriture de $\Phi_n(X)$ en produit indique que son coefficient de plus haut degré (en l'occurrence le coefficient associé au monôme de degré $\text{card}(\mathfrak{P}_n(\mathbb{C}))$ est égal à 1. Donc il est unitaire.
Soit $\xi \in \mathfrak{P}_n(\mathbb{C})$. Les propriétés sur les groupes cycliques nous affirment que les éléments de $\mathfrak{P}_n(\mathbb{C})$ sont les ξ^k, où $k \in [\![1; n-1]\!]$ et $k \wedge n = 1$, donc $\text{card}(\mathfrak{P}_n(\mathbb{C})) = \phi(n)$. Donc par produit, $\deg(\Phi_n(X)) = \text{card}(\mathfrak{P}_n(\mathbb{C})) = \phi(n)$. □

On rappelle qu'une partition d'un ensemble X est un ensemble de parties non-vides de X deux-à-deux disjointes, dont l'union est égale à X. On cherche maintenant à décrire un produit de polynômes cyclotomiques sous la forme d'un polynôme plus facile à manipuler.

Lemme 1.2.5 *Soit* $n \in \mathbb{N}^*$. *Les* $\mathfrak{P}_d(\mathbb{C})$, *où* d *décrit l'ensemble des diviseurs de* n *dans* $\mathbb{N}^*$, *forment une partition de* $\mathbb{U}_n$.

Preuve. Soit $n \in \mathbb{N}^*$, soit $d \in \mathbb{N}^*$. Si $d \mid n$, alors $\mathfrak{P}_d(\mathbb{C}) \subset \mathbb{U}_d \subset \mathbb{U}_n$. D'après un corollaire du théorème de Lagrange, on sait que chaque racine n-ième de l'unité a pour ordre un diviseur de n, donc chacun des éléments de $\mathbb{U}_n$ appartient à un unique $\mathfrak{P}_d(\mathbb{C})$, où d est un diviseur de n. En effet, un élément de $\mathbb{U}_n$ est une racine primitive d-ième si et seulement si c'est un élément d'ordre d. □

De ce lemme on déduit alors :

Proposition 1.2.6 *Soit* $n \in \mathbb{N}^*$. *On peut écrire l'égalité suivante :*

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Une propriété fondamentale d'un polynôme cyclotomique est d'être à coefficients entiers. Pour démontrer cela, on démontre d'abord un lemme portant sur l'algèbre des polynômes.

Lemme 1.2.7 *Soient* $P, Q, R \in \mathbb{Q}[X]$ *des polynômes non nuls. Supposons que* $P \in \mathbb{Z}[X]$, *également que* $P = QR$, *où* P *et* Q *sont unitaires. Alors* $Q, R \in \mathbb{Z}[X]$.

Preuve. Il est évident que R est également unitaire, car P et Q le sont. On suppose que Q est de degré n, on peut alors l'écrire :

$$Q(X) = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n-1} a_i X^i + X^n$$

où les $a_i \in \mathbb{Q}$. On écrit les rationnels $a_i = \frac{p_i}{q_i}$, où $p_i \in \mathbb{Z}$ et $q_i \in \mathbb{N}^*$, tels que $p_i \wedge q_i = 1$. On choisit $q \in \mathbb{N}^*$ tel que q soit un multiple des q_i avec $i \in [\![0; n-1]\!]$. Alors $\exists z_i \in \mathbb{Z}$ tel que $\frac{p_i}{q_i} = \frac{z_i}{q}$. On écrit donc :

$$Q(X) = \sum_{i=0}^{n-1} a_i X^i + X^n = \frac{1}{q} \sum_{i=0}^{n-1} z_i X^i + X^n$$

On note maintenant :

$$Q_0(X) = \sum_{i=0}^{n-1} z_i X^i + qX^n$$

Et on suppose que $\text{pgcd}(q, z_0, z_1, \ldots, z_{n-1}) = 1$. Alors Q est primitif, et on a $Q_0 \in \mathbb{Z}[X]$, $Q(X) = \frac{1}{q} Q_0(X)$. De même, il existe $r \in \mathbb{N}^*$ tel qu'on a $R_0 \in \mathbb{Z}[X]$ primitif où $R(X) = \frac{1}{r} R_0(X)$. On a $P = QR$ donc $qrP = Q_0 R_0$, et comme par la proposition 1.2.2, qrP est primitif. Comme P est unitaire, le coefficient associé au degré le plus élevé du polynôme qrP est qr, or $qr = 1$ car qr est un entier qui divise tous les coefficients de qrP (qrP étant à coefficients entiers). Donc $q = r = 1$ et ainsi, $Q = Q_0 \in \mathbb{Z}[X]$ et $R = R_0 \in \mathbb{Z}[X]$. □

On peut maintenant démontrer que les coefficients d'un polynôme cyclotomique sont entiers.

Proposition 1.2.8 *Pour tout $n \in \mathbb{N}^*$, on a $\Phi_n(X) \in \mathbb{Z}[X]$.*

Preuve. On effectue une récurrence sur l'entier non nul n.
Pour $n = 1$, c'est évident car $\Phi_1(X) = X - 1$. Supposons maintenant la propriété vraie jusqu'au rang $n-1$. On pose, pour $n \geq 2$:

$$P(X) = \prod_{\substack{d|n \\ d<n}} \Phi_d(X)$$

Par hypothèse de récurrence, $P \in \mathbb{Z}[X]$, de plus P est clairement unitaire. Maintenant on écrit :

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X) \prod_{\substack{d|n \\ d<n}} \Phi_d(X) = \Phi_n(X) P(X)$$

Cette égalité indique que $\Phi_n(X) \in \mathbb{Q}[X]$ en faisant la division euclidienne de $X^n - 1$ par $P(X)$ dans $\mathbb{Q}[X]$. On se retrouve ainsi dans la même configuration que le lemme précédent, donc $\Phi_n(X) \in \mathbb{Z}[X]$, donc la propriété est vraie au rang n, ce qui achève la preuve. □

1.3 Démonstration d'une version faible

On arrive à l'ultime partie de ce chapitre introductif. Dans celle-ci, on démontre le théorème de progression arithmétique dans sa version faible. Avant de présenter la preuve, on a besoin de démontrer le lemme suivant :

Lemme 1.3.1 *Soit $n \in \mathbb{N}^*$. Soient $a \in \mathbb{N}$, $p \in \mathcal{P}$ tels que pour tout d diviseur strict de n, $p \mid \Phi_n(a)$ et $p \nmid \Phi_d(a)$. Alors $p \equiv 1\ [n]$.*

Preuve. On sait que $p \mid \Phi_n(a)$, donc $p \mid (a^n - 1)$, donc $a^n = 1$ dans $\mathbb{F}_p$. Si on note λ l'ordre de a dans $\mathbb{F}_p^*$, alors $\lambda \mid n$. On écrit donc :

$$a^\lambda - 1 = \prod_{d|\lambda} \Phi_d(a)$$

or $a^\lambda - 1 \equiv 0\ [p]$ et $\prod_{d|\lambda} \Phi_d(a)$ est non nul sauf si $\lambda = n$. Par théorème de Lagrange dans $\mathbb{F}_p^*$, on obtient que $n \mid (p-1)$ donc que $p \equiv 1\ [n]$. □

Il est maintenant temps de démontrer le :

Théorème 1.3.2 (Cas faible du théorème de Dirichlet) *Soit $n \in \mathbb{N}$, où $n \geq 1$. Il existe une infinité de nombres premiers p vérifiant $p \equiv 1\ [n]$.*

Preuve. On considère $p_1, p_2, \ldots, p_r \in \mathcal{P}$ tels que $p_1 \neq p_2 \neq \ldots \neq p_r$. On pose $N = n \prod_{i=1}^{r} p_i$. Supposons qu'il existe q tel que $q \equiv 1[N]$. Alors q est premier et $q \notin \{p_1, p_2, \ldots, p_r\}$. On effectue une récurrence sur r et on obtient des nombres premiers de plus en plus grands vérifiant la relation de congruence.
Donc $\text{card}\,(\mathcal{P} \cap \{a \in \mathbb{N}\ ;\ a \equiv 1[n]\}) = \infty$.
Posons maintenant $R = \frac{X^N - 1}{\Phi_N(X)}$. Par théorie des polynômes cyclotomiques, on constate que R et Φ_N n'admettent aucune racine commune : ces polynômes sont donc premiers entre eux. On peut donc écrire une relation de Bezout entre eux dans $\mathbb{Q}[X]$:

$$\exists U, V \in \mathbb{Q}[X], UR + V\Phi_N = 1$$

On sait que pour tout polynôme U non constant de $\mathbb{C}[X]$, $\lim\limits_{|x| \to \infty} |U(x)| = \infty$.
Donc comme Φ_N est non constant, $\exists a_0 \in \mathbb{N}, \forall a \geq a_0, |\Phi_N(a)| \geq 2$. Donc $\Phi_N(a)$ admet toujours un facteur premier q. On choisit alors un a de sorte que $aU, aV \in \mathbb{Z}[X]$. On a donc :

$$aU(a)R(a) + aV(a)\Phi_N(a) = a$$

On sait que $\Phi_N(a) \equiv 0[q]$ donc c'est aussi vrai pour $X^N - 1$, donc on en déduit que $a^N - 1 \equiv 0[q]$ et ainsi $a^N \equiv 1[q]$. Ainsi, $a \wedge q = 1$, il en découle $aU(a)R(a) \equiv a[q]$, donc $R(a) \wedge q = 1$. En particulier, pour tout diviseur d strict de N, on a $\Phi_d(a) \wedge q = 1$. Par le lemme précédent, on en déduit $q \equiv 1[N]$, ce qu'on souhaitait démontrer. □

Chapitre 2

Caractères des Groupes Abéliens finis

Dans ce chapitre, on s'intéresse aux homomorphismes d'un groupe commutatif fini dans $\mathbb{C}^*$, appelés caractères. Nous étudierons d'abord les propriétés des caractères, donnerons à leur ensemble une structure de groupe, discuterons de dualité, avant d'utiliser les relations d'orthogonalité, utiles pour la preuve du théorème de Dirichlet. Nous concluerons ce chapitre par une présentation de caractères spécifiques, appelés caractères de Dirichlet.
Dans cette partie, on désignera par G un groupe abélien fini. Sa loi sera notée $*$.

2.1 Propriétés des caractères et dualité

Commençons par donner une définition d'un caractère.

Définition 2.1.1 *On appelle* caractère *de G tout homomorphisme multiplicatif $\chi : G \to \mathbb{C}^*$.*
On appelle caractère trivial *le caractère χ_0 tel que pour tout $g \in G, \chi_0(g) = 1$.*

Dans cette section, nous utiliserons rapidement la notion de suite exacte, que l'on définit maintenant :

Définition 2.1.2 *Soient $G_0, G_1, \ldots$ des groupes et $f_0, f_1, \ldots$ des morphismes de groupes tels que $f_n : G_n \to G_{n+1}$. La suite :*

$$G_0 \xrightarrow{f_0} G_1 \xrightarrow{f_1} \ldots \xrightarrow{f_{n-1}} G_n \xrightarrow{f_n} G_{n+1} \xrightarrow{f_{n+1}} \ldots$$

est appelée suite exacte *si, pour tout $n \in \mathbb{N}$, on a $\mathrm{Im}(f_n) = \mathrm{Ker}(f_{n+1})$.*

Remarque 2.1.3 Soit $g \in G$. Le groupe $\langle \chi(g) \rangle$ est le sous-groupe engendré par $\chi(g)$. Son ordre divise $\mathrm{ord}(G)$, $\langle \chi(g) \rangle$ étant un quotient de G.

On rappelle maintenant l'indice du sous-groupe H dans G, essentiel pour la suite.

Définition 2.1.4 *Soit H un sous-groupe de G. On définit la relation suivante :*

$$\forall (s,t) \in G^2, s \sim_H t \Leftrightarrow st^{-1} \in H$$

Alors le cardinal de $G/\sim_H$ est appelé indice de H dans G, *on le note $[G : H]$.*

Définissons maintenant le dual d'un groupe.

Proposition 2.1.5 *Soient χ_1, χ_2 deux caractères d'un groupe abélien fini G. On définit le produit $\chi_1\chi_2$ en posant $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$, $g \in G$. L'ensemble des caractères de G muni de ce produit forme un groupe abélien $\widehat{G}$ appelé* dual *de G, dont l'élément neutre est le caractère trivial χ_0.*

Preuve. Prenons $g, g' \in G$, et $\chi_1, \chi_2 \in \widehat{G}$. On a :

$$\chi_1\chi_2(gg') = \chi_1(gg')\chi_2(gg') = \chi_1(g)\chi_1(g')\chi_2(g)\chi_2(g') = \chi_1\chi_2(g)\chi_1\chi_2(g')$$

Donc $\chi_1\chi_2$ est bien un caractère. L'inverse χ_1^{-1} de χ_1 est défini par $\chi_1^{-1}(g) = \frac{1}{\chi_1(g)}$ pour $g \in G$. La commutativité étant évidente, $\widehat{G}$ est donc bien un groupe, en particulier abélien. □

On présente maintenant un résultat permettant de lier les caractères d'un sous-groupe H au groupe G.

Proposition 2.1.6 *Soit H un sous-groupe de G. Tout caractère de H peut être prolongé en un caractère de G.*

Preuve. On pose $[G : H] = m$. On procède par récurrence sur m. Si $m = 1$, alors on a évidemment $H = G$. Maintenant, pour $m > 1$, on choisit $g \in G$ tel que $g \notin H$. Soit $n \in \mathbb{N}$ le plus petit entier supérieur à 1 tel que $g^n \in H$. Soit χ un caractère de H, et soit $t = \chi(g^n)$. Le groupe multiplicatif $\mathbb{C}^*$ est un groupe divisible [1], on peut donc choisir $u \in \mathbb{C}^*$ tel que $u^n = t$. On prend alors H' le sous-groupe engendré par H et par g : tout $h' \in H'$ s'écrit sous la forme $h' = hg^a$ où l'on peut prendre $a \in [\![0; n-1]\!]$ et $h \in H$.
Posons maintenant $\chi'(h') = \chi(h)u^a$.
On vérifie maintenant que $\chi' : H' \to \mathbb{C}^*$ est un caractère de H' prolongeant χ et que $\chi'(h')$ ne dépend pas de la décomposition de $h' = hg^a$ choisie. Supposons qu'il existe deux décompositions différentes $h_1g^{a_1} = h_2g^{a_2}$ de h', où $a_1 < a_2$. On a alors $g^{a_1-a_2} = h_2h_1^{-1} \in H$, or $a_1 - a_2 < n$, donc on a forcément que $a_1 = a_2$ et donc $h_1 = h_2$. Maintenant, on peut définir l'application suivante :

$$\begin{aligned} \chi' : H' &\longrightarrow \mathbb{C}^* \\ hg^a &\longmapsto \chi(h)u^a \end{aligned}$$

Nous allons montrer que χ' est un morphisme de groupes. Soient $h_1g^{a_1}, h_2g^{a_2} \in H'$. On sait que G est abélien, donc H' aussi, ainsi $\chi'(h_1g^{a_1}h_2g^{a_2}) = \chi'(h_1h_2g^{a_1+a_2})$. On a alors disjonction de cas. Soit on a $a_1 + a_2 < n$, alors :

$$\begin{aligned} \chi'(h_1h_2g^{a_1+a_2}) &= \chi(h_1h_2)u^{a_1+a_2} = \chi(h_1)\chi(h_2)u^{a_1+a_2} \\ &= \chi(h_1)u^{a_1}\chi(h_2)u^{a_2} = \chi'(h_1g^{a_1})\chi'(h_2g^{a_2}) \end{aligned}$$

1. C'est-à-dire qu'il admet pour chacun de ses éléments des racines n-ièmes pour tout n.

Soit alors $a_1 + a_2 \geq n$, mais quoi qu'il arrive $a_1 + a_2 < 2n$ car $a_1, a_2 < n$. Donc $a_1 + a_2 - n < n$, et ainsi :

$$\chi'(h_1h_2g^{a_1+a_2}) = \chi'(h_1h_2g^{a_1+a_2+n-n}) = \chi'(h_1h_2g^n g^{a_1+a_2-n}) = \chi(h_1h_2g^n)u^{a_1+a_2-n}$$

Or $u^n = \chi(g^n)$ donc $\chi'(h_1h_2g^{a_1+a_2}) = \chi(h_1h_2)u^{a_1+a_2}$. On obtient que χ' est bien un morphisme de groupes, donc comme elle coïncide avec χ sur H', il s'agit du prolongement recherché, ce qui achève la preuve. □

Deux remarques utiles maintenant pour montrer que $\widehat{G}$ est de même ordre que G.

Remarque 2.1.7 L'opération de restriction $\rho : \widehat{G} \to \widehat{H}$ définit un homomorphisme. De plus, d'après la proposition précédente, ρ est surjectif. Également, $\mathrm{Ker}(\rho)$ est formé des caractères de G qui sont triviaux sur H. Donc en munissant $\mathrm{Ker}(\rho)$ d'une structure de groupe, on a $\mathrm{Ker}(\rho) \simeq \widehat{G/H}$. Ce dernier isomorphisme résulte de la propriété universelle des groupes quotients : l'application $\omega : f \mapsto f \circ \pi$ (où $\pi : G \to G/H$ est la projection canonique) est un morphisme de groupe [2] de $\widehat{G/H}$ vers $\widehat{G}$. D'où la suite exacte suivante :

$$1 \longrightarrow \widehat{G/H} \longrightarrow \widehat{G} \longrightarrow \widehat{H} \longrightarrow 1$$

Remarque 2.1.8 Supposons que G soit cyclique, d'ordre n et de générateur a. On prend χ un caractère de G, alors $\omega = \chi(a)$ vérifie $\omega^n = 1$, donc est une racine n-ième de l'unité. Inversement, à partir de n'importe quel $\omega \in \mathbb{U}_n$, on peut définir un caractère χ de G au moyen de $g^k \mapsto \omega^k$, $k \in \mathbb{N}$. Ainsi l'application $\chi \mapsto \chi(g)$ est un isomorphisme de $\widehat{G}$ sur le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité, et donc on obtient que $\widehat{G}$ est cyclique d'ordre n. Prouvons le : soit $\chi \in \widehat{G}$ et $\chi(a) = b$. Alors on a $b^n = \chi(a)^n = \chi(a^n) = \chi(1) = 1$. Donc $b \in \mathbb{U}_n$, d'où $\mathrm{Im}(\chi) \subset \mathbb{U}_n$. On considère alors le morphisme φ suivant :

$$\begin{aligned} \varphi : \widehat{G} &\longrightarrow \mathbb{U}_n \\ \chi &\longmapsto \chi(a) \end{aligned}$$

On veut montrer que φ est un isomorphisme. Déjà, φ est injectif car si $\chi(a) = 1$ alors χ est identiquement égal à 1, puisque a est un générateur de G.
Soit $\eta \in \mathbb{U}_n$. Pour montrer que φ est surjectif, on introduit les deux morphismes suivants :

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow G \\ 1 &\longmapsto a \end{aligned} \qquad\qquad \begin{aligned} g : \mathbb{Z} &\longrightarrow \mathbb{U}_n \\ 1 &\longmapsto \eta \end{aligned}$$

Alors f est surjectif : pour tout $k \in \mathbb{Z}$, $f(k) = a^k$, et tout élément de G s'écrit a^r avec $r \in \mathbb{Z}$, et donc possède un antécédent par f. Egalement, $n\mathbb{Z} = \mathrm{Ker}(f) \subset \mathrm{Ker}(g)$. Ainsi, il existe un certain $\chi : G \to \mathbb{U}_n$ tel que $\chi \circ f = g$. Il vient que $\eta = g(1) = \chi \circ f(1) = \chi(a)$. Donc pour tout $\eta \in \mathbb{U}_n$, il existe $\chi \in \widehat{G}$ tel que $\varphi(\chi) = \eta$. On en déduit que φ est surjective. Ainsi $\widehat{G} \simeq \mathbb{U}_n$, donc $\widehat{G}$ est bien cyclique d'ordre n.

Proposition 2.1.9 *Le groupe dual $\widehat{G}$ est de même ordre que G.*

2. En effet, on voit rapidement que ω est injectif, et $\mathrm{Im}(\omega) = \mathrm{Ker}(\rho)$ grâce à la propriété universelle du quotient (car un morphisme nul sur H se factorise par G/H).

Preuve. Supposons que $\text{ord}(G) = n$. On procède par récurrence sur n. Le cas $n = 1$ est trivial. Pour $n > 1$, on prend H un sous-groupe cyclique non-trivial de G. On sait que $\text{ord}(\widehat{G}) = \text{ord}(\widehat{H}) \times \text{ord}(\widehat{G/H})$ par la remarque 2.1.7 ci-dessus. Or H et son dual sont de mêmes ordres (H étant un groupe cyclique). Également, G/H et son dual sont de mêmes ordres car $\text{ord}(G/H) < n$. Donc $\text{ord}(\widehat{G}) = \text{ord}(H) \times \text{ord}(G/H) = \text{ord}(G)$, ce qu'on voulait démontrer. □

Proposition 2.1.10 *Le groupe dual $\widehat{G}$ est isomorphe à G.*

Preuve. La proposition est déjà connue pour un groupe cyclique par la remarque 2.1.8 ci-dessus. On sait que tout groupe abélien fini est produit direct de m-groupes cycliques. On se charge donc de montrer que le produit direct des duaux est isomorphe au dual du produit, en considérant l'application suivante :

$$\begin{aligned} \psi : \widehat{G} &\longrightarrow \widehat{H_1} \times \cdots \times \widehat{H_m} \\ \chi &\longmapsto (\chi_{|H_1}, \ldots, \chi_{|H_m}) \end{aligned}$$

On constate que ψ est injective car $\text{Ker}(\psi) = \{\chi \in \widehat{G} \mid (\chi_{|H_1}, \ldots, \chi_{|H_m}) = (\chi_0, \ldots, \chi_0)\} = \{\chi_0\}$: en effet, si ψ n'est pas trivial, alors ψ n'est pas trivial sur au moins l'un des facteurs. L'égalité des ordres $\text{ord}(\widehat{G}) = \text{ord}(\widehat{H_1} \times \cdots \times \widehat{H_m})$ implique la surjectivité comme ψ est injective, donc ψ est un isomorphisme. □

On termine cette partie par une proposition qui lie G à son bidual.

Proposition 2.1.11 *Le groupe bidual $\hat{\widehat{G}}$ est canoniquement isomorphe à G.*

Preuve. Si $g \in G$, l'application $\delta_g : \chi \mapsto \chi(g)$ est un caractère de $\widehat{G}$. On obtient donc le morphisme δ suivant :

$$\begin{aligned} \delta : G &\longrightarrow \hat{\widehat{G}} \\ g &\longmapsto \delta_g(g) \end{aligned}$$

Montrons que δ est un isomorphisme. On sait qu'un groupe et son dual sont de même ordre, donc $\text{ord}(G) = \text{ord}(\widehat{G}) = \text{ord}(\hat{\widehat{G}})$. On doit donc juste démontrer que δ est injectif, c'est-à-dire que pour $g \in G$, $g \neq 1$, il existe un caractère χ de G tel que $\chi(g) \neq 1$. Soit H le sous-groupe de G engendré par g. En reprenant les notations de la remarque 2.1.8, on sait que pour tout $\eta \in \mathbb{U}_n$, il existe χ caractère de H tel que $\chi(g) = \eta$, donc si $\eta \neq 1$, $\chi(g) \neq 1$. De plus, on sait qu'on peut prolonger χ en un caractère de G. Donc δ est injectif, donc $\hat{\widehat{G}} \simeq G$, ce qu'il fallait prouver. □

2.2 Relations d'orthogonalité entre caractères

Dans cette section, on démontre les relations d'orthogonalité, qui seront utiles plus tard dans la preuve du théorème de progression arithmétique.

Théorème 2.2.1 *Soit G un groupe abélien fini. On a :*

$$\sum_{g\in G}\chi(g)=\begin{cases}\mathrm{ord}(G) & \text{si } \chi=\chi_0\\ 0 & \text{sinon.}\end{cases}$$

Preuve. Le fait que $\sum_{g\in G}\chi(g)=\mathrm{ord}(G)$ si $\chi=\chi_0$ est évident. Maintenant, si $\chi\neq\chi_0$, on prend $h\in G$ tel que $\chi(h)\neq\chi_0(h)=1$. Alors :

$$\chi(h)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(gh)=\sum_{g\in G}\chi(g)$$

Donc on en déduit la factorisation :

$$(\chi(h)-1)\sum_{g\in G}\chi(g)=0$$

Comme on sait que $\chi(h)\neq 1$, on a forcément que $\sum_{g\in G}\chi(g)=0$, ce qu'on voulait démontrer. □

On cite également un corollaire qui donne une seconde relation d'orthogonalité, déduite de la précédente.

Corollaire 2.2.2 *Soit G un groupe abélien fini, $\widehat{G}$ son dual. On a :*

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}\mathrm{ord}(G) & \text{si } g=e\\ 0 & \text{sinon.}\end{cases}$$

Preuve. Il suffit d'appliquer le théorème 2.2.1 sur $\widehat{G}$, et utiliser la proposition 2.1.11, qui montre que $\hat{\widehat{G}}\simeq G$. □

On note que ces deux relations sont des cas particuliers des relations d'orthogonalité de la théorie des caractères des groupes finis. En effet, ici nous travaillons sur des groupes exclusivement abéliens...

2.3 Caractères de Dirichlet

Ici, on définit les caractères de Dirichlet, fonctions particulières sur un ensemble de classes de congruences sur les entiers et à valeurs complexes. On commence par rappeler la définition d'une fonction multiplicative.

Définition 2.3.1 *Une* fonction multiplicative *est une fonction arithmétique $f : \mathbb{N} \to \mathbb{C}$ vérifiant $f(1) = 1$ et, pour tout $a, b \in \mathbb{N}$ tels que $a \wedge b = 1$, vérifiant $f(ab) = f(a)f(b)$.*
La fonction f est multiplicative au sens strict *si pour tout $a, b \in \mathbb{N}$, $f(ab) = f(a)f(b)$.*

Définition 2.3.2 *Soit $m \in \mathbb{N}^*$. On définit $(\mathbb{Z}/m\mathbb{Z})^*$ le* groupe multiplicatif des entiers inversibles modulo *m. C'est un groupe abélien fini, et son ordre est $\phi(m)$, où ϕ est l'indicatrice d'Euler.*
Un élément $\bar{a}$ appartient à $(\mathbb{Z}/m\mathbb{Z})^*$ si et seulement si $a \wedge m = 1$.

Définissons maintenant les caractères de Dirichlet modulo m.

Définition 2.3.3 *Un* caractère de Dirichlet *modulo m est un morphisme de groupes de $(\mathbb{Z}/m\mathbb{Z})^*$ dans le groupe multiplicatif $\mathbb{C}^*$ des complexes non-nuls. On peut l'étendre en une fonction définie sur $\mathbb{Z}$ en posant :*

$$\chi(a) = \begin{cases} \chi(\bar{a}) & \text{si } a \wedge m = 1 \\ 0 & \text{sinon.} \end{cases}$$

En l'étendant de cette manière, on a une fonction multiplicative. En effet, en prenant a, b tels que $a \wedge m = 1$ et $b \wedge m = 1$, on a bien $ab \wedge m = 1$, et la multiplicativité provient de la définition d'un caractère. Si a ou b n'est pas premier avec m, on sait que ab n'est pas premier avec m, et on a $\chi(a)\chi(b) = \chi(ab) = 0$. On note également que cette fonction est m-périodique.

Chapitre 3

Loi de Réciprocité Quadratique

On discute ici de la loi de réciprocité quadratique, qui permet de décrire explicitement les caractères modulaires, au rôle crucial dans les transformations des séries de Dirichlet. Dans ce chapitre, on utilise la notation suivante : on désigne, pour $p \in \mathcal{P}$, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ par $\mathbb{F}_p^*$.

3.1 Théorème des restes chinois

Dans cette section, on démontre le théorème des restes chinois énoncé avec la théorie des groupes.

Théorème 3.1.1 (Restes chinois) *Soient $n, m \in \mathbb{N}^*$, tels que $n \wedge m = 1$. Alors il existe un isomorphisme de groupe entre $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$.*

Preuve. Soit $\ell \in \mathbb{Z}$, soit $r \in \mathbb{N}^*$. On note $\bar{\ell}^r$ la classe de ℓ modulo r. On définit l'application suivante :

$$\begin{aligned} \Psi \ : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \ell &\longmapsto (\bar{\ell}^n, \bar{\ell}^m) \end{aligned}$$

L'application Ψ est un morphisme de groupes. On ajoute que si $\bar{\ell}^{nm} = \bar{s}^{nm}$ alors $\ell - s$ est un multiple de mn, donc un multiple commun de m et n. Ainsi on en déduit que $\Psi(\ell) = \Psi(s)$. Définissons donc une application définie sur le quotient $\mathbb{Z}/nm\mathbb{Z}$:

$$\begin{aligned} \bar{\Psi} \ : \mathbb{Z}/nm\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \bar{\ell}^{nm} &\longmapsto \bar{\Psi}(\bar{\ell}^{nm}) = \Psi(\ell) \end{aligned}$$

Comme Ψ est un morphisme de groupes, $\bar{\Psi}$ l'est également. Calculons $\mathrm{Ker}(\bar{\Psi})$:

$$\mathrm{Ker}(\bar{\Psi}) = \{\bar{\ell}^{nm} \in \mathbb{Z}/nm\mathbb{Z} \mid \bar{\ell}^n = \bar{0}^n \text{ et } \bar{\ell}^m = \bar{0}^m\}$$

Mais si l'entier ℓ est divisible par m et n premiers entre eux, alors $mn \mid l$. Donc $\bar{\ell}^{nm} = \bar{0}^{nm}$ et $\bar{\Psi}$ est injective. De plus, comme $\mathrm{card}(\mathbb{Z}/nm\mathbb{Z}) = \mathrm{card}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) < \infty$, on obtient que $\bar{\Psi}$ est bijective, ce qu'il fallait

démontrer. □

Remarque 3.1.2 Par récurrence, on peut étendre ce résultat au cas de r entiers $n_1, n_2, \ldots, n_r$ premiers entre eux deux-à-deux. On obtiendrait alors, en posant $\eta = \prod_{k=1}^{r} n_k$:

$$\begin{aligned} \Psi : \mathbb{Z}/\eta\mathbb{Z} &\longrightarrow \prod_{k=1}^{r} (\mathbb{Z}/n_k\mathbb{Z}) \\ \bar{\ell}^{\eta} &\longmapsto \Psi(\bar{\ell}^{\eta}) = \left(\bar{\ell}^{n_1}, \ldots, \bar{\ell}^{n_r}\right) \end{aligned}$$

qui est bien un isomorphisme de groupes.

3.2 Symbole de Legendre et critère d'Euler

Ici nous définissons le symbole de Legendre, puis après quelques préliminaires, nous présenterons une démonstration du critère d'Euler.

Définition 3.2.1 *On dit que $n \in \mathbb{N}$ est un* résidu quadratique *modulo $p \in \mathcal{P}$ si et seulement s'il existe $m \in \mathbb{Z}$ tel que $m^2 \equiv n[p]$. Dans le cas contraire, on dit que n est* non-résidu quadratique *modulo p.*

Définition 3.2.2 *Pour tout $n \in \mathbb{Z}$, et tout $p \in \mathcal{P}$ un nombre premier impair, on définit le* symbole de Legendre *:*

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \mid n \\ 1 & \text{si } p \nmid n \text{ et si } n \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } n \text{ est un non-résidu quadratique modulo } p. \end{cases}$$

Lemme 3.2.3 *Soit $p \in \mathcal{P}$ impair. L'ensemble des carrés non-nuls de $\mathbb{F}_p^*$ est un sous-groupe de $\mathbb{F}_p^*$ d'ordre $\frac{p-1}{2}$.*

Preuve. Considérons le morphisme de groupes f suivant :

$$\begin{aligned} f : \mathbb{F}_p^* &\longrightarrow \mathbb{F}_p^* \\ \bar{x} &\longmapsto \overline{x^2} \end{aligned}$$

Ainsi $\mathrm{Im}(f)$ est l'ensemble des carrés non nuls de $\mathbb{F}_p^*$ (c'en est un sous-groupe). Cherchons le cardinal de cet ensemble. Comme p est impair, on a que $\bar{1} \neq \overline{-1}$, donc $\mathrm{Ker}(f) = \{-1, 1\}$ et ce noyau est de cardinal 2. Or $\mathrm{ord}(\mathbb{F}_p^*) = \mathrm{card}\,(\mathrm{Ker}(f)) \times \mathrm{card}\,(\mathrm{Im}(f))$, soit $\mathrm{card}\,(\mathrm{Im}(f)) = \frac{p-1}{2}$. □

On rappelle aussi le petit théorème de Fermat.

Théorème 3.2.4 (Petit théorème de Fermat) *Soit $a \in \mathbb{N}$, soit $p \in \mathcal{P}$ tels que $a \wedge p = 1$. Alors $a^{p-1} \equiv 1[p]$.*

Preuve. Soit $a \in \mathbb{N}$ et soit $p \in \mathcal{P}$. Si $a \wedge p = 1$, $\overline{a}$ est dans le groupe multiplicatif $\mathbb{F}_p^*$, d'ordre $p-1$. Or d'après le théorème de Lagrange, $\text{ord}(a) \mid (p-1)$, donc :

$$\overline{a}^{p-1} = \overline{a^{p-1}} = \overline{1} \iff a^{p-1} \equiv 1[p]$$

Ce qu'on voulait montrer. □

Maintenant, on donne la preuve du critère d'Euler.

Proposition 3.2.5 (Critère d'Euler) *Pour tout $n \in \mathbb{Z}$, on a la congruence suivante :*

$$n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right)[p]$$

Preuve. Soit $n \in \mathbb{Z}$. Si $p \mid n$, la congruence est évidemment vraie. Supposons que $p \nmid n$.
Si n est un résidu quadratique, alors d'après le petit théorème de Fermat on a :

$$n^{\frac{p-1}{2}} \equiv (m^2)^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1[p]$$

Si n est non-résidu quadratique, alors $n^{(p-1)/2} \equiv -1[p]$. En effet, $n^{(p-1)/2} \not\equiv 1[p]$, puisque $\left(X^{(p-1)/2} - 1\right) \in \mathbb{F}_p[X]$ admet au plus $\frac{p-1}{2}$ racines. On en déduit du cas précédent que ses racines sont exactement les $\frac{p-1}{2}$ carrés de $\mathbb{F}_p^*$. De plus, on sait que $n^{(p-1)/2} \equiv \pm 1[p]$ car $\left(n^{(p-1)/2} - 1\right)\left(n^{(p-1)/2} + 1\right) = n^{p-1} - 1$ est divisible par p grâce au petit théorème de Fermat. □

3.3 Preuve de la loi de réciprocité quadratique

On se charge maintenant de donner la preuve de la loi de réciprocité quadratique. On commence avant tout par rappeler le théorème de Wilson, pour utiliser un lemme qui servira à la démonstration finale.

Théorème 3.3.1 (Wilson) *Soit $p \in \mathbb{N}$ tel que $p > 1$. Si le nombre p est premier alors on a la congruence $(p-1)! \equiv -1[p]$.*

Preuve. Supposons que $p \in \mathcal{P}$. Prenons deux polynômes $P, Q \in \mathbb{F}_p[X]$:

$$P(X) = X^{p-1} - \overline{1} \quad \text{et} \quad Q(X) = \prod_{k=1}^{p-1} \left(X - \overline{k}\right)$$

On constate que tout élément de $\mathbb{F}_p^*$ est racine de Q et de P. Donc le polynôme $P-Q$ admet tout élément de $\mathbb{F}_p^*$ comme racine, donc admet $p-1$ racines, or $\deg(P-Q) \leq p-2$. Donc $P-Q=0$, ainsi $P=Q$. Ainsi P et Q admettent le même coefficient constant qui est $\prod_{k=1}^{p-1}\left(-\overline{k}\right)! = -\overline{(p-1)!} = -\overline{1}$, et donc $(p-1)! \equiv -1[p]$, ce qu'on voulait. □

Lemme 3.3.2 *Soit $n \in \mathbb{N}$. Pour tout $p \in \mathcal{P}$ impair de la forme $p = 2n+1$, on a la congruence $(n!)^2 \equiv (-1)^{n+1}[p]$.*

Preuve. Il suffit de considérer :

$$(p-1)! \equiv \prod_{k=1}^{n} k(p-k) \equiv (-1)^n (n!)^2 [p]$$

Or par théorème de Wilson, p est premier donc $(p-1)! \equiv -1[p]$. Donc :

$$(p-1)! \equiv (-1)^n (n!)^2 \equiv -1[p] \iff (n!)^2 \equiv (-1)^{n+1}[p]$$

Ce qu'on souhaitait démontrer. □

Théorème 3.3.3 (Réciprocité quadratique) *Soient $p, q \in \mathcal{P}$ deux nombres premiers impairs distincts. En posant $n = \frac{p-1}{2}$ et $m = \frac{q-1}{2}$, on a alors :*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{mn}$$

Preuve. On définit G le quotient du groupe $\mathbb{F}_p^* \times \mathbb{F}_q^*$ par le sous-groupe $\{(\overline{1},\overline{1}), (\overline{-1},\overline{-1})\}$. On essaie de calculer de deux manières différentes le produit τ de tous les éléments de G.
Dans la suite de la preuve, on désigne par $[x,y]$ l'image dans G du couple $(\bar{x},\bar{y}) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$ par la projection canonique $\mathbb{F}_p^* \times \mathbb{F}_q^* \to G$.
Un élément de G s'écrit de manière unique comme $[a,b]$ où $a, b \in \mathbb{Z}$ vérifiant $0 < a \leq n$ et $0 < b < q$. On obtient donc une expression de τ :

$$\tau = \prod_{g \in G} g = \prod_{a=1}^{n}\prod_{b=1}^{q-1}[a,b] = \prod_{a=1}^{n}\left[a^{q-1}, (q-1)!\right] = \left[(n!)^{2m}, ((q-1)!)^n\right]$$

Le lemme précédent nous permet alors d'obtenir, en remarquant que n est pair :

$$\tau = \left[\left((n!)^2\right)^m, (-1)^n\right] = \left[(-1)^{m(n+1)}, 1\right] = \left[(-1)^{mn+n+m}, 1\right]$$

De plus, en utilisant le théorème des restes chinois, on peut affirmer que $\mathbb{F}_p^* \times \mathbb{F}_q^* \simeq (\mathbb{Z}/pq\mathbb{Z})^*$.
On définit $S \subset \{1, \ldots, (pq-1)/2\}$ l'ensemble formé par les entiers premiers avec p et q. Ainsi, un élément $x \in G$ s'écrit de manière unique comme $x = [a, a]$ où $a \in S$. On remarque qu'un entier $r \in \{1, \ldots, \frac{pq-1}{2}\}$ ne peut être divisible par p et par q.
Posons maintenant :

$$\mathcal{A} = \prod_{a \in S} a \quad \text{et} \quad \mathcal{B} = \prod_{a=1}^{n} qa$$

Or en considérant que $\frac{pq-1}{2} = nq + m = mp + n$, on déduit alors l'égalité :

$$\mathcal{A}\mathcal{B} = \prod_{a \in S} a \prod_{a=1}^{n} qa = \prod_{\substack{a=1 \\ a \wedge p = 1}}^{mp+n} a$$

En appliquant le critère d'Euler, on en déduit :

$$\begin{cases} \mathcal{B} \equiv q^n n! \equiv \left(\frac{q}{p}\right) n! \ [p] \\ \mathcal{A}\mathcal{B} \equiv n! \left((p-1)!\right)^m \equiv n!(-1)^m \ [p] \end{cases}$$

Et donc on a :

$$\mathcal{A} \equiv (-1)^m \left(\frac{q}{p}\right) [p] \quad \text{et} \quad \mathcal{A} \equiv (-1)^n \left(\frac{p}{q}\right) [q]$$

Le théorème est alors démontré en utilisant les identités $\tau = [\mathcal{A}, \mathcal{A}] = [(-1)^{mn+n+m}, 1]$. □

3.4 Résultat sur les caractères modulaires

Il existe un lien entre les caractères d'ordre 2 et les caractères de Legendre, dont on fait état dans cette partie. On rappelle tout d'abord la définition d'entier sans facteurs carrés.

Définition 3.4.1 *On dit qu'un entier $n \in \mathbb{Z}$ est* sans facteurs carrés *si celui-ci n'est divisible par aucun carré parfait*[1] *sauf 1.*

Maintenant une définition sur les homomorphismes ε et ω :

1. Un carré parfait est le carré d'un entier.

Définition 3.4.2 *Soit $n \in \mathbb{N}$ un entier impair. Soient $\varepsilon(n)$ et $\omega(n)$ les éléments de $\mathbb{Z}/2\mathbb{Z}$ suivants :*

$$\epsilon(n) \equiv \frac{n-1}{2} \ [2] = \begin{cases} 0 & si\ n \equiv 1[4] \\ 1 & si\ n \equiv -1[4] \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \ [2] = \begin{cases} 0 & si\ n \equiv \pm 1[8] \\ 1 & si\ n \equiv 5[8] \end{cases}$$

Donc ε est un donc un homomorphisme du groupe $(\mathbb{Z}/4\mathbb{Z})^*$ dans $\mathbb{Z}/2\mathbb{Z}$, et ω un homomorphisme de $(\mathbb{Z}/8\mathbb{Z})^*$ dans $\mathbb{Z}/2\mathbb{Z}$.

Proposition 3.4.3 *Soit a un entier non-nul sans facteurs carrés, et soit $m = 4|a|$. Il existe alors un unique caractère χ_a modulo m tel que $\chi_a(p) = \left(\frac{a}{p}\right)$ pour tout $p \in \mathcal{P}$ tel que $p \nmid m$. On a alors $\chi_a^2 = 1$ et $\chi_a \neq 1$ si $a \neq 1$.*

Preuve. Pour l'unicité de χ_a, c'est évident car tout entier premier à m est produit de nombres premiers ne divisant pas m ; de même pour le fait que $\chi_a^2 = 1$. Montrons maintenant l'existence de χ_a. On suppose que a est de la forme $a = \prod_{i=1}^k \ell_i$ où les ℓ_i sont des nombres premiers distincts et différents de 2. Pour $x \in \mathbb{Z}$, on définit χ_a comme le caractère :

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \prod_{i=1}^k \left(\frac{x}{\ell_i}\right)$$

Si $p \in \mathcal{P}$ est distinct de 2 et des ℓ_i alors [2], selon la loi de réciprocité quadratique, on a :

$$\chi_a(p) = (-1)^{\varepsilon(p)\sum_{i=1}^k \varepsilon(\ell_i)} \prod_{i=1}^k \left(\frac{p}{\ell_i}\right) = \prod_{i=1}^k (-1)^{\varepsilon(p)\varepsilon(\ell_i)}$$
$$= \prod_{i=1}^k \left(\frac{\ell_i}{p}\right) = \left(\frac{\prod_{i=1}^k \ell_i}{p}\right) = \left(\frac{a}{p}\right)$$

Et ce χ_a répond à la question. Si a est de la forme $-b$, $2b$ ou $-2b$, avec $b = \prod_{i=1}^k \ell_i$ sans facteurs carrés et impair, on prend pour χ_a le produit de χ_b avec le caractère $\chi_a(x) = (-1)^{\varepsilon(x)}$, $(-1)^{\omega(x)}$, ou $(-1)^{\varepsilon(x)+\omega(x)}$. Par construction, on a bien $\chi_a \neq 1$ si $a \neq 1$. □

2. Ainsi p est donc un nombre premier tel que $p \wedge m = 1$.

Chapitre 4

Séries de Dirichlet

Après avoir donné quelques propriétés sur les fonctions holomorphes, on discute dans cette section des séries de Dirichlet. Ces objets interviennent essentiellement en théorie analytique des nombres. Toute la preuve du théorème de progression arithmétique repose sur l'étude de séries de Dirichlet particulières, les séries $\mathcal{L}$, que nous étudierons dans le chapitre six.

4.1 Résultats utiles d'analyse complexe

Dans cette section, on rappelle les principaux éléments d'analyse complexe qu'on utilisera au cours de ce travail. Commençons par rappeler une définition des fonctions holomorphes.

Définition 4.1.1 *Soit U un ouvert de $\mathbb{C}$. On considère l'application $f : U \to \mathbb{C}$.*
On dit que f est dérivable au sens complexe*, ou* holomorphe *en un point z_0 de U si la limite suivante, appelée* dérivée *de f en z_0, existe :*

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

On dit que f est holomorphe sur l'ouvert *U si elle est holomorphe en tout point z_0 de U. Également, on appelle* fonction entière *une fonction holomorphe dans tout le plan complexe.*

Rappelons maintenant la formule intégrale de Cauchy, utile pour la suite de ce document.

Proposition 4.1.2 *Soit U un ouvert simplement connexe du plan complexe $\mathbb{C}$. On considère $f : U \to \mathbb{C}$ une fonction holomorphe sur U. Soit $\gamma : [a, b] \to \mathbb{C}$ un lacet*[1] *inclus dans U, et soit $z \in U \setminus \gamma([a, b])$. On a alors la formule suivante :*

$$f(z) \cdot \mathrm{Ind}_\gamma(z) = \frac{1}{2\pi i} \oint_\gamma \frac{f(\xi)}{\xi - z} \, \mathrm{d}\xi$$

où $\mathrm{Ind}_\gamma(z) = \frac{1}{2i\pi} \oint_\gamma \frac{\mathrm{d}\xi}{\xi - z}$ *désigne* l'indice *du point z par rapport au lacet γ.*

Cette formule se simplifie dans le cas où γ est un cercle C orienté positivement, contenant z et inclus dans U. En effet, l'indice de z par rapport à C vaut alors 1, d'où la formule [2] :

$$f(z) = \frac{1}{2\pi i} \oint_C \frac{f(\xi)}{\xi - z} \, \mathrm{d}\xi$$

Définissons maintenant le pôle d'une fonction holomorphe.

Définition 4.1.3 *Soient $U \subset \mathbb{C}$ un ouvert, $a \in U$, et $f : U \setminus \{a\} \to \mathbb{C}$ une fonction holomorphe. On dit que* est un pôle de *f s'il existe une fonction g holomorphe sur U telle que a $g(a) \neq 0$, et $n \in \mathbb{N}^*$ tels que pour tout $z \in U \setminus \{a\}$:*

$$(z - a)^n f(z) = g(z)$$

L'entier n est alors appelé ordre du pôle.

On définit les fonctions analytiques ainsi que le principe de prolongement analytique :

Définition 4.1.4 *On dit que $f : U \to \mathbb{C}$ est* analytique *lorsque, pour tout $z_0 \in U$, il existe un disque $D(z_0, r) \subset U$ et une série entière $\sum a_n z^n$ de rayon de convergence $R > r$ telle que, pour tout $z \in D(z_0, r)$:*

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

Définition 4.1.5 *Soient $V \subset U \subset \mathbb{C}$ deux ouverts, et $f : V \to \mathbb{C}$ une fonction analytique. On dit que f admet un* prolongement analytique à *U s'il existe une fonction analytique $g : U \to \mathbb{C}$ telle que $g|_V = f$.*

Le théorème d'unicité du prolongement analytique sera ainsi utile pour la suite :

Théorème 4.1.6 (Unicité du prolongement analytique) *Soient $V \subset U \subset \mathbb{C}$ deux ouverts, et $f : V \to \mathbb{C}$ une fonction analytique. Si f admet un prolongement analytique à U, alors ce prolongement est unique.*

On enchaîne maintenant sur quelques lemmes utiles pour discuter des séries de Dirichlet.

Lemme 4.1.7 *Soit U un ouvert de $\mathbb{C}$, et f_n une suite de fonctions holomorphes sur U, convergente uniformément sur tout compact vers une fonction f. Alors la fonction f est holomorphe sur U et toutes les dérivées de f_n convergent vers les dérivées de f.*

2. Cette formule montre que la valeur en un point d'une fonction holomorphe est entièrement déterminée par les valeurs de cette fonction sur n'importe quel cercle entourant ce point.

Preuve. Soit D un disque fermé contenu dans U, et soit C son bord, orienté positivement. La formule de Cauchy nous donne :

$$f_n(z_0) = \frac{1}{2\pi i} \oint_C \frac{f_n(z)}{z - z_0} \, \mathrm{d}z$$

où $z_0 \in D$. Par passage à la limite, on a :

$$f(z_0) = \frac{1}{2\pi i} \oint_C \frac{f(z)}{z - z_0} \, \mathrm{d}z$$

ce qui montre bien que f est holomorphe dans $\mathring{D}$. Pour montrer que les dérivées de f_n convergent vers les dérivées de f, on raisonne de manière identique en appliquant la formule suivante :

$$f'(z_0) = -\frac{1}{2\pi i} \oint_C \frac{f(z)}{(z - z_0)^2} \, \mathrm{d}z$$

ce qui achève la preuve. □

Lemme 4.1.8 (Abel) *Soient deux suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$. Pour tout $m, m', p \in \mathbb{N}$, on pose $A_{m,p}$ et $S_{m,m'}$ tels que :*

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

Alors on peut écrire ce qu'on appelle une transformation d'Abel :

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

Preuve. On a $a_m = A_{m,m}$ et pour tout $n > m$, on sait que $a_n = \sum_{n=m}^{n} a_n - \sum_{n=m}^{n-1} a_n = A_{m,n} - A_{m,n-1}$. On obtient alors :

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

Ce qu'on souhaitait démontrer. □

Lemme 4.1.9 *Soient $\alpha, \beta \in \mathbb{R}$ tels que $0 < \alpha < \beta$, et soit $z = x + iy$ un nombre complexe où $\Re(z) = x > 0$. On a alors :*

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq \left|\frac{z}{x}\right| (e^{-\alpha x} - e^{-\beta x})$$

Preuve. On écrit simplement :

$$e^{-\alpha z} - e^{-\beta z} = z \int_{\alpha}^{\beta} e^{-tz} \, \mathrm{d}t$$

On passe alors en valeurs absolues :

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq |z| \int_{\alpha}^{\beta} e^{-tx} \, \mathrm{d}t = \frac{|z|}{x}(e^{-\alpha x} - e^{-\beta x})$$

Ce qu'on souhaitait montrer. □

4.2 Définition et premières propriétés

On définit dans cette section les séries de Dirichlet et on démontre une proposition importante sur celles-ci. Nous terminerons par quelques corollaires utiles pour la suite.

Définition 4.2.1 *Soit $(\lambda_n)_{n\in\mathbb{N}}$ une suite de nombres réels telle que $\lim_{n\to\infty} \lambda_n = +\infty$. On suppose que tous les termes de la suite sont positifs*[3]*. Soit $(a_n)_{n\in\mathbb{N}}$ une suite quelconque de nombres complexes. On appelle* série de Dirichlet *d'exposants $(\lambda_n)_{n\in\mathbb{N}}$ une série de la forme :*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$$

où $z \in \mathbb{C}$.

Proposition 4.2.2 *Si la série de Dirichlet $f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$ converge pour $z = z_0$, alors elle converge uniformément dans tout domaine de la forme $\Re(z - z_0) \geq 0$, avec $|\arg(z - z_0)| \leq \alpha$, où $\alpha < \pi/2$.*

Preuve. Supposons qu'on ait une série de Dirichlet $f(z)$ convergente pour $z = z_0 = 0$. On a donc $\sum_{n=1}^{\infty} a_n$ qui converge. On prend un domaine $\Re(z) \geq 0$ et $|\arg(z)| \leq \alpha < \pi/2$. Soit $\varepsilon > 0$. On sait que $\sum_{n=1}^{\infty} a_n$

3. Quitte à supprimer les termes négatifs, en nombre fini.

converge donc il existe N tel que $\forall m, m' > N$, $\left|A_{m,m'}\right| \geq \varepsilon$, où $A_{m,m'} = \sum_{n=m}^{m'} a_n$. On applique alors la transformation d'Abel vue précédemment, avec $b_n = e^{-\lambda_n z}$:

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

Posons $z = x + iy$, et appliquons le lemme 4.1.9 pour obtenir, pour $m, m' > N$:

$$\left|S_{m,m'}\right| \leq \left(1 + \frac{|z|}{x} \sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x})\right)$$

On remarque que :

$$|\arg(z)| \leq \alpha \iff \cos(\arg(z)) \geq \cos(\alpha) \iff \frac{|z|}{\Re(z)} \leq \frac{1}{\cos(\alpha)}$$

On pose alors $k := (\cos(\alpha))^{-1}$, et on en déduit :

$$\left|S_{m,m'}\right| \leq \varepsilon \left(1 + k(e^{-\lambda_m x} - e^{-\lambda_{m'} x})\right)$$

D'où :

$$\left|S_{m,m'}\right| \leq \varepsilon\,(1 + k)$$

Ceci démontre la convergence uniforme dans $\Re(z) \geq 0$. □

On peut déduire de cette proposition une série de corollaire qu'on cite maintenant.

Corollaire 4.2.3 *Si f converge pour $z = z_0$, f converge pour tout z tel que $\Re(z) > \Re(z_0)$, la fonction ainsi définie étant holomorphe.*

Corollaire 4.2.4 *L'ensemble de convergence de la série f contient un demi-plan ouvert maximal, qu'on nomme demi-plan de convergence. Notons que si le demi-plan de convergence est donné par $\Re(z) > \rho$, on appelle ρ l'abscisse de convergence de la série considérée.*

Par abus de langage, $\mathbb{C}$ et $\emptyset$ sont considérés comme des demi-plans ouverts. Le corollaire suivant provient de la convergence uniforme, et du fait que $e^{-\lambda_n z} \to e^{-\lambda_n z_0}$.

Corollaire 4.2.5 *$f(z) \to f(z_0)$ lorsque z tend vers z_0 en restant dans le domaine $\Re(z - z_0)$, et $|\arg(z - z_0)| \leq \alpha$, avec $\alpha < \pi/2$.*

Corollaire 4.2.6 *La fonction f ne peut être identiquement nulle que que si tous ses coefficients sont nuls.*

Preuve. On montre d'abord que a_0 est nul en multipliant f par $e^{\lambda_0 z}$ puis en faisant tendre $z \to +\infty$ (en prenant $z \in \mathbb{R}$). La convergence uniforme montre que $f(z)e^{\lambda_0 z} \to a_0$, qui est de fait nul. On réitère l'opération sur a_1, a_2, etc. □

4.3 Séries de Dirichlet à coefficients positifs

La proposition suivante signifie que le domaine de convergence de f est limité par par une singularité de f située sur l'axe des réels.

Proposition 4.3.1 *Soit $f(z) = \sum a_n e^{-\lambda_n z}$ une série de Dirichlet où tous les coefficients a_n sont réels positifs. Soit ρ l'abscisse de convergence de la série f. Supposons que f converge sur le domaine $\Re(z) > \rho$ et que la fonction f puisse être prolongée analytiquement en une fonction holomorphe au voisinage de $z = \rho$. Il existe alors $\varepsilon > 0$ tel que pour $\Re(z) > \rho - \varepsilon$, f converge.*

Preuve. On raisonne de manière analogue à précedemment : on étudie le voisinage $z = \rho$ en supposant $\rho = 0$. La fonction f étant holomorphe à la fois sur $\Re(z) > 0$ et au voisinage de 0, elle est donc holomorphe sur le disque $D_\varepsilon = \{z \in \mathbb{C} \mid |z - 1| \leq 1 + \varepsilon\}$, où $\varepsilon > 0$. Ainsi sa série de Taylor converge dans D_ε, et par le lemme 4.1.7, on en déduit la dérivée p-ième de f, pour $\Re(z) > 0$:

$$f^{(p)}(z) = \sum_{n=0}^{\infty} a_n (-\lambda_n)^p e^{-\lambda_n z}$$

d'où :

$$f^{(p)}(1) = (-1)^p \sum_{n=0}^{\infty} a_n \lambda_n^p e^{-\lambda_n}$$

On écrit maintenant la série de Taylor, sur D_ε :

$$f(z) = \sum_{p=0}^{\infty} \frac{(z-1)^p}{p!} (-1)^p \sum_{n=0}^{\infty} a_n \lambda_n^p e^{-\lambda_n} = \sum_{p=0}^{\infty} \frac{(z-1)^p}{p!} f^{(p)}(1)$$

En prenant $z = -\varepsilon$:

$$f(z = -\varepsilon) = \sum_{p=0}^{\infty} \frac{(\varepsilon+1)^p}{p!} (-1)^p f^{(p)}(1)$$

Cette série est bien convergente. Or $(-1)^p f^{(p)}(1) = \sum_{n\geq 0} a_n \lambda_n^p e^{-\lambda_n}$ est par hypothèse convergente à termes positifs. Ainsi la série double à termes positifs suivante :

$$f(z=-\varepsilon) = \sum_{n=0}^{\infty}\sum_{p=0}^{\infty} \frac{(\varepsilon+1)^p}{p!} a_n \lambda_n^p e^{-\lambda_n}$$

est une série convergente. En rappelant la série $e^{\lambda_n(1+\varepsilon)} = \sum_{n=0}^{\infty} \frac{(\varepsilon+1)^p}{p!}\lambda_n^p$, on regroupe alors les termes pour obtenir :

$$\begin{aligned} f(z=-\varepsilon) &= \sum_{n=0}^{\infty} a_n e^{-\lambda_n} \sum_{p=0}^{\infty} \frac{(\varepsilon+1)^p}{p!}\lambda_n^p \\ &= \sum_{n=0}^{\infty} a_n e^{-\lambda_n} e^{\lambda_n(1+\varepsilon)} = \sum_{n=0}^{\infty} a_n e^{\lambda_n \varepsilon} \end{aligned}$$

ce qui démontre que la série de Dirichlet f converge, avec $\rho = 0$, pour $\Re(z) > -\varepsilon$. □

4.4 Séries de Dirichlet proprement dites

On définit maintenant un cas particulier de séries de Dirichlet, appelées séries proprement dites.

Définition 4.4.1 *Soit $(\lambda_n)_{n\in\mathbb{N}}$ une suite de nombres réels telle que $\lambda_n = \ln(n)$. Soit $(a_n)_{n\in\mathbb{N}}$ une suite quelconque de nombres complexes. On appelle* série de Dirichlet proprement dite *une série de la forme :*

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

où $s \in \mathbb{C}$.

Proposition 4.4.2 *Si les termes a_n sont bornés, il y a convergence absolue pour $\Re(s) > 1$.*

Preuve. Il s'agit d'une conséquence immédiate de la convergence des séries de Riemann $\sum_{n=1}^{\infty} n^{-\alpha}$ avec $\alpha > 1$. □

Proposition 4.4.3 *Si les sommes partielles $A_{m,p} = \sum_{n=m}^{p} a_n$ sont bornées, il y a convergence (pas nécessairement absolue) de f pour $\Re(s) > 0$.*

Preuve. Soit $k \in \mathbb{R}$. Supposons qu'on ait $|A_{m,p}| = |\sum_{n=m}^{p} a_n| \leq k$. On applique de nouveau le lemme

d'Abel vu précédemment, et on trouve :

$$\left|S_{m,m'}\right| = \left|\sum_{n=m}^{m'} a_n b_n\right| \leq k\left(\sum_{n=m}^{m'-1}\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| + \left|\frac{1}{(m')^s}\right|\right)$$

Grâce à la proposition 4.2.2, on peut supposer $s \in \mathbb{R}$, ce qui permet de réécrire cette inégalité sous la forme simplifiée : $\left|S_{m,m'}\right| \leq \frac{k}{m^s}$. On en déduit la convergence, évidente en faisant tendre $m' \to \infty$. □

Chapitre 5

Fonction ζ de Riemann

Dans ce bref chapitre, nous allons nous intéresser sommairement à la fonction ζ de Riemann, intéressante introduction à l'étude des fonctions $\mathcal{L}$. On commencera par discuter des produits eulériens, avant de déterminer les principales propriétés de la fonction ζ dont on a besoin.

5.1 Produits eulériens

Dans cette section, on considère f comme étant une fonction multiplicative et bornée.

Proposition 5.1.1 *La série de Dirichlet $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge absolument pour $\Re(s) > 1$. Sa somme dans ce domaine est alors le produit eulérien convergent suivant, pour $p \in \mathcal{P}$:*

$$\prod_{p\in\mathcal{P}} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} = \prod_{p\in\mathcal{P}} \left(1 + \frac{f(p)}{p^s} + \cdots + \frac{f(p^m)}{p^{ms}} + \dots\right)$$

Preuve. La convergence de $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ est dûe au fait qu'on a supposé f bornée : la proposition 4.4.2 permet de conclure. Soit maintenant $\Gamma \subset \mathcal{P}$ un ensemble fini de nombres premiers. On considère $\mathbb{N}(\Gamma)$ l'ensemble des entiers supérieurs à 1 dont tous les facteurs premiers sont dans Γ. On obtient directement l'égalité suivante :

$$\sum_{n\in\mathbb{N}(\Gamma)} \frac{f(n)}{n^s} = \prod_{p\in\Gamma} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}}$$

Lorsque le cardinal de Γ croît, on a $\sum_{n\in\mathbb{N}(\Gamma)} \frac{f(n)}{n^s} \longrightarrow \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$. On en déduit aisément que le produit eulérien converge, et que sa limite est égale à $\sum \frac{f(n)}{n^s}$. □

Proposition 5.1.2 *Si f est multiplicative au sens strict, on a :*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{f(p)}{p^s}}$$

Preuve. Comme f est supposée multiplicative au sens strict, on a $f(p^m) = f(p)^m$ pour chaque puissance de nombre premier. On a alors :

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathcal{P}} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} = \prod_{p \in \mathcal{P}} \sum_{k=0}^{\infty} \frac{f(p)^k}{p^{ks}} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{f(p)}{p^s}}$$

Ce qu'on voulait. □

5.2 Fonction ζ et quelques propriétés

Définition 5.2.1 *Soit $s \in \mathbb{C}$. On définit la série de Dirichlet suivante, sur le demi-plan $\Re(s) > 1$:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

On peut également écrire ζ sous forme de produit, grâce à la proposition 5.1.2 *:*

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

Cette fonction est communément appelée fonction Zêta de Riemann.

Remarque 5.2.2 La fonction ζ est bien définie car, pour tout $z \in \mathbb{C}$ tels que $\Re(z) > 1$:

$$\sum_{n=1}^{\infty} \left| \frac{1}{n^z} \right| = \sum_{n=1}^{\infty} \frac{1}{\Re(z)} < \infty$$

Proposition 5.2.3 *La fonction ζ est holomorphe et non-nulle sur le demi-plan $\Re(s) > 1$.*

Preuve. On doit vérifier que ζ est la somme d'une série holomorphe sur $\Re(s) > 1$ qui converge normalement sur tout compact de $\{s \in \mathbb{C} \mid \Re(s) > 1\}$. Soit $n \in \mathbb{N}$ tel que $n \geq 1$, la fonction $f : s \in \{s \in \mathbb{C} \mid \Re(s) > 1\} \mapsto n^{-s}$ est holomorphe pour $\Re(s) > 1$. Soit K un compact de $\{s \in \mathbb{C} \mid \Re(s) > 1\}$, il existe $\delta > 0$ tel que $K \subset \{s \in \mathbb{C} \mid \Re(s) \geq 1 + \delta\}$. Alors :

$$\sum_{n=1}^{\infty} \sup_{s \in K} \left| \frac{1}{n^2} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}} < \infty$$

et la non-nullité est évidente, ce qui achève la preuve. □

Proposition 5.2.4 *On peut écrire l'égalité :*

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

où ρ est une fonction holomorphe sur $\Re(s) > 0$.

Preuve. On peut tout d'abord remarquer que :

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

On écrit maintenant :

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s}\ \mathrm{d}t \right) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s})\ \mathrm{d}t$$

On pose alors maintenant :

$$\rho_n(s) = \int_n^{n+1} (n^{-s} - t^{-s})\ \mathrm{d}t$$

et

$$\rho(s) = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s})\ \mathrm{d}t = \sum_{n=1}^{\infty} \rho_n(s)$$

On doit maintenant montrer que ρ est bien définie et holomorphe sur $\Re(s) > 0$. On va donc montrer que $\sum \rho_n$ est normalement convergente sur tout compact inclus dans le demi-plan $\Re(s) > 0$. On a donc :

$$|\rho_n(s)| = \left| \int_n^{n+1} (n^{-s} - t^{-s})\ \mathrm{d}t \right| \leq \sup_{n \leq t \leq n-1} \left| n^{-s} - t^{-s} \right|$$

Par théorème des accroissements finis, on obtient $|\rho_n(s)| \leq \frac{|s|}{n^{\Re(s)+1}}$. Alors, pour tout $\varepsilon > 0$, on a donc bien une série qui converge normalement pour $\Re(s) \geq \varepsilon$. □

On termine en donnant maintenant deux corollaires, utiles pour la suite de notre mémoire.

Corollaire 5.2.5 *La fonction ζ a un pôle simple pour $s = 1$.*

Preuve. On le déduit de la proposition 5.2.4 ; en écrivant $\zeta(s) = \frac{1}{s-1} + \rho(s)$, le résultat est immédiat. □

Corollaire 5.2.6 *Lorsque $s \to 1$, on a :*

$$\sum_{p\in\mathcal{P}} p^{-s} \sim \ln\left(\frac{1}{s-1}\right)$$

alors que $\sum_{p\geq 2}\sum_{k\geq 2} p^{-ks}$ reste bornée.

Preuve. On utilise le développement en série entière $\ln(1+z) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}z^n}{n}$. On a donc :

$$\ln(\zeta(s)) = \sum_{k=1}^{\infty}\sum_{p\in\mathcal{P}} \frac{p^{-ks}}{k} = \sum_{p\in\mathcal{P}} \frac{1}{p^s} + \sum_{k=2}^{\infty}\sum_{p\in\mathcal{P}} \frac{p^{-ks}}{k}$$

On pose donc $\psi(s) = \sum_{k=2}^{\infty}\sum_{p\in\mathcal{P}} \frac{p^{-ks}}{k}$. Cette série est majorée :

$$\psi(s) = \sum_{k=2}^{\infty}\sum_{p\in\mathcal{P}} \frac{p^{-ks}}{k} \leq \sum_{k=1}^{\infty}\sum_{p\in\mathcal{P}} \frac{1}{p^{ks}} = \sum_{p\in\mathcal{P}} \frac{1}{p^s(p^s-1)} \leq \sum_{p\in\mathcal{P}} \frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$$

Ainsi par théorème d'encadrement, ψ reste bornée, et on remarque que $\ln(\zeta(s)) \sim \ln(\frac{1}{s-1})$ d'après le corollaire précédent, ce qui nous permet de conclure. □

Chapitre 6

$\mathcal{L}-$FONCTIONS DE DIRICHLET

Dans cette section, il est question de discuter des séries $\mathcal{L}$ de Dirichlet, pouvant être prolongées analytiquement sur le plan complexe en des $\mathcal{L}$-fonctions. Ces objets permettent des généralisations sur la fonction ζ de Riemann, et sont au centre de la démonstration du théorème de progression arithmétique.
Dans cette partie, on prend $s \in \mathbb{C}$, $m \in \mathbb{N}^*$ et χ un caratère de Dirichlet modulo m.

6.1 Définition et premières propriétés

Commençons par donner la définition des séries $\mathcal{L}$ de Dirichlet.

Définition 6.1.1 *La* $\mathcal{L}-$fonction de Dirichlet *associée à* χ *est la série suivante :*

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

En supposant qu'on a choisi d'étendre χ *sur* $\mathbb{Z}$ *tout entier, on remarque qu'on peut écrire :*

$$\mathcal{L}(s,\chi) = \sum_{n\wedge m=1} \frac{\chi(n)}{n^s} + \sum_{n\wedge m\neq 1} \frac{\chi(n)}{n^s} = \sum_{n\wedge m=1} \frac{\chi(n)}{n^s}$$

Car si $n \wedge m \neq 1$*, on sait que* $\chi(n) = 0$*.*

Proposition 6.1.2 *Supposons qu'on ait* $\chi = \chi_0$*, alors :*

$$\mathcal{L}(s,\chi_0) = \prod_{p|m}(1-p^{-s}) \sum_{n=1}^{\infty} \frac{\chi_0(s)}{n^s} = \prod_{p|m}(1-p^{-s})\zeta(s)$$

De plus, $\mathcal{L}(s,\chi_0)$ *est prolongeable analytiquement pour* $\Re(s) > 0$ *et admet* $s = 1$ *comme pôle simple.*

Preuve. On écrit simplement :

$$\mathcal{L}(s,\chi_0) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\nmid m} \frac{1}{1-p^{-s}} = \prod_{p|m}(1-p^{-s}) \prod_{p\in\mathcal{P}} \frac{1}{1-p^{-s}} = \prod_{p|m}(1-p^{-s})\zeta(s)$$

On obtient ce que l'on souhaitait. Quant au prolongement analytique de $\mathcal{L}(s,\chi_0)$, il découle des propriétés de la fonction ζ et des propositions énoncées dans le chapitre 4. □

Proposition 6.1.3 *Supposons qu'on ait $\chi \neq \chi_0$, alors la série $\mathcal{L}(s,\chi)$ converge sur le demi-plan $\Re(s) > 0$. On aura alors :*

$$\mathcal{L}(s,\chi) = \prod_{p\in\mathcal{P}} \frac{1}{1-\frac{\chi(p)}{p^s}} \quad \textit{pour} \quad \Re(s) > 1$$

Preuve. Sur le demi-plan $\Re(s) > 1$, on a déjà prouvé la convergence de $\mathcal{L}(s,\chi)$, en particulier la convergence absolue, χ étant multiplicative. On doit donc juste étudier la convergence sur $\Re(s) > 0$. D'après la proposition 4.4.3, il suffit donc de vérifier que les sommes $A_{u,v} = \sum_{n=u}^{v} \chi(n)$ sont bornées. Or les relations d'orthogonalités entre caractères (théorème 2.2.1 et son corollaire) nous permettent d'écrire $\sum_{n=u}^{u+m-1} \chi(n) = 0$, car on a supposé que $\chi \neq \chi_0$. On a donc juste à majorer les sommes $A_{u,v}$ qui comportent moins de m termes, pour $v - u < m$. Ainsi dans ce cas, la somme $A_{u,v}$ contient au plus $\phi(m)$ termes non-nuls (avec ϕ l'indicatrice d'Euler) par définition de χ, et chacun de ces termes est majoré par 1 en valeur absolue. Ainsi on a $|A_{u,v}| \leq \phi(m)$, ce qui démontre la convergence.
Montrons maintenant la décomposition en produit de $\mathcal{L}(s,\chi)$, en utilisant la proposition 5.1.1 ; cela revient à montrer que χ est bornée et multiplicative au sens strict. On sait que pour tout $n \in \mathbb{N}^*$, $|\chi(n)| \leq 1$, donc χ est bornée. D'autre part, pour $a, b \in \mathbb{N}^*$ tels que $a \wedge m = 1$ et $b \wedge m = 1$, on peut écrire :

$$\chi(ab) = \chi(\overline{a}\overline{b}) = \chi(\bar{a}\bar{b}) = \chi(\bar{a})\chi(\bar{b}) = \chi(a)\chi(b)$$

Par contre, si $a \wedge m \neq 1$, alors $ab \wedge m \neq 1$ et on a donc :

$$\chi(ab) = 0 = \chi(a)\chi(b)$$

Cela prouve que χ est complètement multiplicative, ce qu'on souhaitait démontrer. □

6.2 Etude de la non-nullité de $\mathcal{L}(1,\chi)$

La preuve du théorème de progression arithmétique repose en grande partie sur la propriété de non-nullité de $\mathcal{L}(1,\chi)$. On se charge ainsi d'étudier cette proposition. Dans cette partie, on prend $m \in \mathbb{N}^*$ et $p \in \mathcal{P}$. Si $\bar{p} \in (\mathbb{Z}/m\mathbb{Z})^*$, c'est-à-dire si $p \nmid m$, on pose $g(p) = \frac{\phi(m)}{n}$, où $n = \mathrm{ord}(\langle\bar{p}\rangle)$ dans $(\mathbb{Z}/m\mathbb{Z})^*$. On allège également les notations en prenant $\mathcal{G}_m = (\mathbb{Z}/m\mathbb{Z})^*$.

Lemme 6.2.1 *Si $p \nmid m$, on a l'identité suivante :*

$$\prod_{\chi \in \widehat{\mathcal{G}_m}} (1 - \chi(p)\Lambda) = (1 - \Lambda^n)^{g(p)}$$

Preuve. On prend $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité. On a montré dans le premier chapitre que $\text{card}(\mathbb{U}_n) = n$. On prouve dans un premier temps que :

$$\prod_{\omega \in \mathbb{U}_n} (1 - \omega\Lambda) = 1 - \Lambda^n$$

Pour tout $\omega \in \mathbb{U}_n$, on a $\left(\frac{1}{\omega}\right)^n = \frac{1}{\omega^n} = 1$, donc $\frac{1}{\omega}$ est une racine du polynôme $1 - \Lambda^n$. On a donc :

$$\begin{aligned} 1 - \Lambda^n &= -\prod_{\omega \in \mathbb{U}_n} (\Lambda - \frac{1}{\omega}) = -\prod_{\omega \in \mathbb{U}_n} \left(\frac{\omega\Lambda - 1}{\omega}\right) \\ &= \frac{-\prod_{\omega \in \mathbb{U}_n}(\omega\Lambda - 1)}{\prod_{\omega \in \mathbb{U}_n} \omega} = -(-1)^n \frac{\prod_{\omega \in \mathbb{U}_n}(1 - \omega\Lambda)}{\prod_{\omega \in \mathbb{U}_n} \omega} \\ &= \frac{(-1)^{n+1}}{\prod_{\omega \in \mathbb{U}_n} \omega} \prod_{\omega \in \mathbb{U}_n} (1 - \omega\Lambda) \end{aligned}$$

Le produit des $\omega \in \mathbb{U}_n$ dépend de la parité de n. De plus, on sait que pour tout $\omega \in \mathbb{U}_n$, il existe $k \in [\![0, n-1]\!]$ tel que $z = e^{2ik\pi/n}$. Ainsi, on a :

$$\prod_{\omega \in \mathbb{U}_n} \omega = \prod_{k=0}^{n-1} e^{2ik\pi/n} = \exp\left(\frac{2i\pi}{n} \sum_{k=0}^{n-1} k\right) = \exp\left(\frac{2i\pi n(n-1)}{2n}\right) = \exp((n-1)i\pi)$$

On en déduit que si n est pair, $\prod_{\omega \in \mathbb{U}_n} \omega = -1$, et sinon $\prod_{\omega \in \mathbb{U}_n} \omega = 1$, d'où le fait qu'on obtient :

$$\frac{(-1)^{n+1}}{\prod_{\omega \in \mathbb{U}_n} \omega} \prod_{\omega \in \mathbb{U}_n} (1 - \omega\Lambda) = \prod_{\omega \in \mathbb{U}_n} (1 - \omega\Lambda) = 1 - \Lambda^n$$

Maintenant, on montre que pour tout $\omega \in \mathbb{U}_n$, il existe $g(p)$ caractères $\chi \in \widehat{\mathcal{G}_m}$ tels que $\chi(p) = \omega$. On prend le morphisme suivant :

$$\begin{aligned} \psi : \widehat{\mathcal{G}_m} &\longrightarrow \mathbb{U}_n \\ \chi &\longmapsto \chi(p) \end{aligned}$$

On a $\text{Ker}(\psi) = \{\chi \in \widehat{\mathcal{G}_m} \mid \chi(p) = 1\}$. On sait de plus que $\text{card}\,(\text{Ker}(\psi)) \times \text{card}\,(\text{Im}(\psi)) = \text{card}\left(\widehat{\mathcal{G}_m}\right) = \phi(m)$, or ψ est surjective par construction, donc $\text{card}\,(\text{Im}(\psi)) = \text{card}\,(\mathbb{U}_n) = n$, d'où $\text{card}\,(\text{Ker}(\psi)) = \frac{\phi(m)}{n} = g(p)$. Donc pour tout $\omega \in \mathbb{U}_n$, il existe $g(p)$ caractères $\chi \in \widehat{\mathcal{G}_m}$ tels que $\chi(p) = \omega$.

De ce que l'on vient de montrer, on en déduit finalement, en notant $\Omega = \{\chi \in \widehat{\mathcal{G}_m} \mid \chi(p) = \omega\}$:

$$\begin{aligned}(1-\Lambda^n)^{g(p)} &= \left(\prod_{\omega\in\mathbb{U}_n}(1-\omega\Lambda)\right)^{g(p)} = \prod_{\omega\in\mathbb{U}_n}(1-\omega\Lambda)^{g(p)} \\ &= \prod_{\omega\in\mathbb{U}_n}\prod_{\chi\in\Omega}(1-\Lambda\chi(p)) = \prod_{\chi\in\widehat{\mathcal{G}_m}}(1-\Lambda\chi(p))\end{aligned}$$

Ce que l'on souhaitait démontrer. □

Définition 6.2.2 *On définit la fonction ζ_m par :*

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

C'est une série de Dirichlet à coefficients positifs et convergente pour $\Re(s) > 1$.

Proposition 6.2.3 *On peut écrire l'égalité :*

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

Preuve. D'après le lemme 6.2.1 et en utilisant le produit eulérien, on a, pour $\Re(s) > 1$:

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

Donc on peut écrire, en utilisant cette égalité :

$$\zeta_m(s) = \prod_{\chi\in\widehat{\mathcal{G}_m}}\mathcal{L}(s,\chi) = \prod_{\chi\in\widehat{\mathcal{G}_m}}\prod_{p\in\mathcal{P}}\frac{1}{1-\frac{\chi(p)}{p^s}}$$

On peut alors utiliser le produit eulérien de $\mathcal{L}$ ainsi que le lemme précédent, en prenant $\Lambda = p^{-s}$:

$$\zeta_m(s) = \prod_{\chi\in\widehat{\mathcal{G}_m}}\prod_{p\nmid m}\frac{1}{1-\frac{\chi(p)}{p^s}} = \prod_{p\nmid m}\prod_{\chi\in\widehat{\mathcal{G}_m}}\frac{1}{1-\frac{\chi(p)}{p^s}} = \prod_{p\nmid m}\frac{1}{(1-p^{-ns})^{g(p)}}$$

La convergence pour $\Re(s) > 1$ est claire, par définition [1]. □

Proposition 6.2.4 *La fonction $\mathcal{L}(1,\chi)$ est non-nulle pour tout $\chi \neq \chi_0$.*

1. En effet, le développement nous permet de constater que c'est une série de Dirichlet à coefficients entiers positifs, convergente d'après le chapitre 4.

Preuve. On raisonne par l'absurde en supposant qu'il existe un caractère χ tel que $\mathcal{L}(1,\chi) = 0$. Alors on obtient que $\zeta_m(1) = 0$ et ζ_m est holomorphe en $s = 1$ et converge, pour tout s tel que $\Re(s) > 0$ (car ζ_m est une série de Dirichlet à coefficients positifs). On peut minorer ainsi chaque terme du produit $\prod \frac{1}{(1-p^{-ns})^{g(p)}}$ de la manière suivante :

$$\frac{1}{(1-p^{-ns})^{g(p)}} = \left(\sum_{k=0}^{\infty} p^{-kns}\right)^{g(p)} \geq \sum_{k=0}^{\infty} p^{-k\phi(m)s} \geq p^{-\phi(m)s}$$

ainsi ζ_m a tous ses coefficients supérieurs à ceux de la série $\sum n^{-\phi(m)s}$, qui est divergente pour $s = \frac{1}{\phi(m)}$. On obtient une contradiction. □

Chapitre 7

Théorème de progression arithmétique

Nous arrivons à la dernière partie de ce travail, où l'on démontre le théorème de progression arithmétique de Dirichlet. Pour ce faire, nous allons le reformuler à l'aide de la notion de densité.

7.1 Densité analytique de $\Gamma \subset \mathcal{P}$

Définissons ainsi cette notion :

Définition 7.1.1 *On dit qu'une partie $\Gamma \subset \mathcal{P}$ a une densité analytique $\delta \in [0,1]$ si :*

$$\lim_{s \to 1} \frac{\sum_{p \in \Gamma} p^{-s}}{\ln\left(\frac{1}{s-1}\right)} = \delta$$

On constate que si $\text{card}(\Gamma) < \infty$, alors $\delta = 0$. De plus, d'après le chapitre sur la fonction ζ, la densité de l'ensemble des nombres premiers $\mathcal{P}$ est égale à 1. Cette notion permet ainsi de reformuler le théorème de progression arithmétique :

Théorème 7.1.2 (Progression arithmétique de Dirichlet) *Soit $m \geq 1$, et soit $a \in \mathbb{N}^*$ tel que $a \wedge m = 1$. Soit $\mathcal{P}_a$ l'ensemble des $p \in \mathcal{P}$ tels que $p \equiv a[m]$. Alors la densité de $\mathcal{P}_a$ est $\frac{1}{\phi(m)}$.*

C'est cet énoncé, équivalent à celui présenté en introduction, que nous allons prouver à la fin de ce chapitre.

7.2 Résultats préliminaires

Dans cette partie, on prend χ un caractère de Dirichlet modulo m et on définit :

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

Cette série est convergente pour $s > 1$. L'objectif est d'étudier le comportement de la fonction $\sum_{p\in\mathcal{P}_a} p^{-s}$ et de montrer que sa limite n'est pas finie [1] lorsque $s \to 1$.

Lemme 7.2.1 *Si $\chi = \chi_0$, on a la limite suivante :*

$$\lim_{s\to 1} \frac{f_{\chi_0}(s)}{\ln(s-1)^{-1}} = 1$$

Preuve. D'après une proposition précédente, on a :

$$\lim_{s\to 1} \frac{\sum_{p\in\mathcal{P}_a} p^{-s}}{\ln(s-1)^{-1}} = 1$$

Or la série $\sum_{p\in\mathcal{P}_a} p^{-s}$ et $f_{\chi_0}(s) = \sum_{p\nmid m} \chi_0(p)p^{-s} = \sum_{p\nmid m} p^{-s}$ ne diffèrent que d'un nombre fini de termes [2], ce qui indique que ces deux fonctions ont le même comportement à la limite, d'où le résultat :

$$\lim_{s\to 1} \frac{\sum_{p\nmid m} p^{-s}}{\ln(s-1)^{-1}} = 1$$

Ce qu'on souhaitait démontrer. □

Un autre lemme essentiel qui nous informe que f_χ reste bornée quand $s \to 1$:

Lemme 7.2.2 *Si $\chi \neq \chi_0$, alors f_χ est bornée quand $s \to 1$.*

Preuve. Par la proposition 6.1.3, on sait que $\mathcal{L}(s,\chi) = \prod_{p\in\mathcal{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, pour $\Re(s) > 1$. Également, on constate que les facteurs du produit sont sous la forme $(1-\alpha)^{-1}$, où $|\alpha| < 1$ On définit la détermination principale du logarithme comme ceci :

$$\ln\left(\frac{1}{1-\alpha}\right) = \sum_{k=1}^{\infty} \frac{\alpha^n}{n}$$

Ce qui nous donne l'égalité suivante, toujours pour $\Re(s) > 1$:

$$\ln\left(\mathcal{L}(s,\chi)\right) = \sum_{p\in\mathcal{P}} \ln\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right) = \sum_{p\in\mathcal{P}}\sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{ns}}$$

Or on peut décomposer la double somme :

$$\ln\left(\mathcal{L}(s,\chi)\right) = \sum_{p\in\mathcal{P}} \frac{\chi(p)}{p^s} + \sum_{p\in\mathcal{P}}\sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}$$

1. En effet, s'il y avait un nombre fini de termes dans la somme, alors on aurait une limite finie lorsque $s \to 1$, alors que chaque terme p^{-s} tend vers p^{-1}.
2. Ces termes sont les diviseurs premiers de m.

D'autre part, $f_\chi(s) = \sum_{p\nmid m} \frac{\chi(p)}{p^s} = \sum_{p\in\mathcal{P}} \frac{\chi(p)}{p^s}$ car si $p \mid m$, $\chi(p) = 0$. On a donc :

$$\ln\left(\mathcal{L}(s,\chi)\right) = f_\chi(s) + \sum_{p\in\mathcal{P}}\sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}$$

Or ici $\chi \neq \chi_0$, donc d'après la proposition 6.2.4, $\mathcal{L}(1,\chi) \neq 1$, ce qui assure que $\ln\left(\mathcal{L}(s,\chi)\right)$ est bornée quand $s \to 1$. Quant à la double somme $\sum_{p\in\mathcal{P}}\sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}$, elle est également bornée car :

$$\left|\sum_{p\in\mathcal{P}}\sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}\right| \leq \sum_{p\in\mathcal{P}}\sum_{n=2}^{\infty} \frac{1}{np^{ns}}$$

Et d'après le corollaire 5.2.6, $\sum_{p\in\mathcal{P}}\sum_{n=2}^{\infty} \frac{1}{np^{ns}}$ est bornée lorsque $s \to 1$. Donc $f_\chi(s)$ est une différence de fonctions bornées, donc elle est aussi bornée, ce qui achève la preuve. □

7.3 Démonstration du théorème

Nous sommes arrivé à la dernière étape avant la démonstration du théorème de progression arithmétique. Nous définissons ainsi la fonction $g_a(s) = \sum_{p\in\mathcal{P}_a} p^{-s}$, et on donne un résultat sur celle-ci avant la preuve finale.

Lemme 7.3.1 *On a le résultat suivant :*

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

Preuve. Par définition de f_χ, on a :

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

Or d'après la propriété des caractères, $\chi^{-1}(a)\chi(p) = \chi(a^{-1}p)$. Les relations d'orthogonalités sur $\mathcal{G}_m$ de la section 2.2 donnent alors :

$$\sum_{\chi\in\mathcal{G}_m} \chi(a^{-1}p) = \begin{cases} \mathrm{ord}(\mathcal{G}_m) = \phi(m) & \text{si } a^{-1}p \equiv 1[m] \Leftrightarrow p \in \mathcal{P}_a \\ 0 & \text{sinon.} \end{cases}$$

Donc on a :

$$\sum_{p\nmid m}\sum_{\chi\in\widehat{\mathcal{G}_m}} \frac{\chi^{-1}(a)\chi(p)}{p^s} = \sum_{p\in\mathcal{P}_a} \frac{\phi(m)}{p^s} = \phi(m)g_a(s)$$

ce qu'on souhaitait démontrer. □

Ce résultat, et tous ceux qui l'ont précédé permettent de démontrer le :

Théorème 7.3.2 (Progression arithmétique de Dirichlet) *Soit $m \geq 1$, et soit $a \in \mathbb{N}^*$ tel que $a \wedge m = 1$. Soit $\mathcal{P}_a$ l'ensemble des $p \in \mathcal{P}$ tels que $p \equiv a[m]$. Alors la densité de $\mathcal{P}_a$ est $\frac{1}{\phi(m)}$.*

Preuve. On calcule la densité de l'ensemble $\mathcal{P}_a$. D'après le lemme 7.3.1, on a :

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

Or si on décompose la somme, on obtient :

$$\frac{1}{\phi(m)} \sum_{\chi\in\widehat{\mathcal{G}_m}} \frac{\chi^{-1}(a) f_\chi(s)}{\ln(s-1)^{-1}} = \frac{1}{\phi(m)} \frac{f_{\chi_0}(s)}{\ln(s-1)^{-1}} + \frac{1}{\phi(m)} \sum_{\chi\neq\chi_0} \frac{\chi^{-1}(a) f_\chi(s)}{\ln(s-1)^{-1}}$$

Or, quand $s \to 1$, d'après le lemme 7.2.1, si $\chi = \chi_0$, $f_{\chi_0}(s) \sim \ln(s-1)^{-1}$, et d'après le lemme 7.2.2, si $\chi \neq \chi_0$, f_χ est bornée, donc $\sum_{\chi\neq\chi_0} \frac{\chi^{-1}(a) f_\chi(s)}{\ln(s-1)^{-1}} \to 0$. On obtient ainsi que :

$$\lim_{s\to 1} \frac{g_a(s)}{\ln(s-1)^{-1}} = \frac{1}{\phi(m)}$$

La densité analytique de $\mathcal{P}_a$ est donc $\delta = \frac{1}{\phi(m)}$, ce qui indique que l'ensemble des $p \in \mathcal{P}$ tels que $p \equiv a[m]$ est infini, mais également que ces nombres premiers sont également répartis selon les différentes classes modulo m premières à m. □

Bibliographie

[1] François de Marçay. *Analyse complexe.* Polycopié de cours, 2019.

[2] Gérald Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres.* Société mathématique de France, 1995.

[3] Hervé Gianella, Serge Francinou & Serge Nicolas. *Oraux X-ENS, Algèbre 1.* Cassini, 2016.

[4] Jean-Pierre Serre. *Cours d'arithmétique.* Presses universitaires de France, 1995.

[5] Pierre-Louis Montagard. *Algèbre linéaire et théorie des groupes.* Polycopié de cours, 2019.

[6] Sylvain Brochard. *Théorie des groupes.* Polycopié de cours, 2015.

[7] Xavier Gourdon. *Algèbre.* Ellipses, 2008.