Méthodes analytiques en théorie des nombres : Le théorème de la progression arithmétique de Dirichlet

Vincent GAROT et Victor ISSA

Le but de cet exposé sera de démontrer le théorème suivant dû Dirichlet :

Théorème 0.0.1. *Soit $m \geq 1$ et a des entiers, soit $P_a(m)$ l'ensemble des nombres premiers $p = a \ mod \ m$ alors :*

- *Si $a \wedge m \neq 1$ alors $P_a(m)$ est vide.*
- *Si $a \wedge m = 1$ alors $P_a(m)$ est infini.*

La preuve du théorème fait intervenir des méthodes analytiques classiques de la théorie des nombres et consistera à montrer que la fonction :

$$g_a(s) = \sum_{p \in P_a(m)} \frac{1}{p^s}$$

admet un pôle en $s = 1$.

1 Caractères d'un groupe abélien fini

Définition 1.0.1. *Soit G un groupe abélien fini on note $\widehat{G} = Hom(G, \mathbb{C}^\times)$ le dual de G, les éléments de $\widehat{G}$ sont les caractères de G. Le produit point par point munit $\widehat{G}$ d'une structure de groupe abélien.*

Proposition 1.0.2. *Soit H un sous-groupe de G, alors le morphisme de restriction $\widehat{G} \longrightarrow \widehat{H}$ est surjectif, c'est à dire que tout caractère de H se prolonge à G.*

Proof. On raisonne par récurrence sur l'indice de H, si H est d'indice 1 alors $G = H$ et il n'y a rien à prouver. Supposons que le résultat soit vrai pour les groupes d'indice $< n$, soit H un groupe d'indice n. Le groupe quotient G/H est d'ordre n donc par le théorème de Lagrange pour tout $x \in G$, $\overline{x}^n = \overline{1}$, c'est à dire $x^n \in H$. Soit $\chi \in \widehat{H}$, on considère le groupe $K =< H, x >$, K est d'indice $< n$, donc par hypothèse de récurrence tout caractère de K se prolonge en un caractère de G, il suffit de montrer que χ se prolonge en un caractère de H. On a $x^n \in H$, soit m le plus petit entier vérifiant $x^m \in H$, posons $t = \chi(x^m)$ et soit $w \in \mathbb{C}^\times$ une racine m-ième de t, on a $\chi(x^m) = w^m$. Si $k \in K$ il existe $h \in H$ et $a \in \mathbb{Z}$ tel que $k = hx^a$, on pose alors $\chi'(k) = \chi(h)w^a$. De plus si $hx^a = h'x^b$ alors $x^{a-b} = h'h^{-1} \in H$ ainsi $m|a-b$ donc si on écrit $a - b = dm$ alors :

$$\chi(x^{a-b}) = \chi(x^m)^d = (w^m)^d = w^{a-b}$$

et comme $\chi(x^{a-b}) = \chi(h')\chi(h)^{-1}$ on en déduit que $\chi(h)w^a = \chi(h')w^b$, ce qui prouve que χ' est bien défini. On a montré que χ se prolongait à K et donc à G par hypothèse de récurrence, cqfd. □

Dans la suite on admet que $\#G = \#\widehat{G}$

Proposition 1.0.3. *G et $\widehat{\widehat{G}}$ sont canoniquement isomorphe.*

Proof. Soit $ev : G \longrightarrow \widehat{\widehat{G}}$ l'application définie par $ev_x(\chi) = \chi(x)$, alors ev un morphisme de groupe, il suffit de vérifier qu'il est injectif. Soit $x \neq 1$ un élément de G d'ordre n, on considère H le groupe engendré par x, soit $\xi \neq 1$ une racine n-ième de l'unité, alors $\chi(x^m) = \xi^m$ défini un caractère de H qui par 1.0.2 s'étend en un caractère χ de G vérifiant $\chi(x) = \xi \neq 1$, ainsi $ev_x(\chi) \neq 1$ ce qui prouve que ev_x est injectif, cqfd . □

Proposition 1.0.4 (Relation d'orthogonalité)**.** *On a,*

- $\sum_{g\in G}\chi(g)=\begin{cases}0 \text{ si } \chi\neq 1\\ \#G \text{ si } \chi=1\end{cases}$
- $\sum_{\chi}\chi(g)=\begin{cases}0 \text{ si } g\neq 1\\ \#G \text{ si } g=1\end{cases}$

Proof.
- Si $\chi=1$ le résultat est clair, supposons que $\chi\neq 1$ et soit $y\in G$ tel que $\chi(y)\neq 1$. L'application $g\mapsto yg$ est une bijection de G dans lui même de réciproque $g\mapsto y^{-1}g$, ainsi par le changement de variable $h=yg$ on a :

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

et comme $\chi(y)\neq 1$ ceci impose $\sum_{g\in G}\chi(g)=0$.

- On applique le point précédent au groupe $\widehat{G}$ on obtient que si $g\in G$ alors :

$$\sum_{\chi\in\widehat{G}}ev_g(\chi)=\begin{cases}0 \text{ si } g\neq 1\\ \#\widehat{G} \text{ si } g=1\end{cases}$$

et comme $\#G=\#\widehat{G}$ on a démontré le résultat voulu.

□

2 Séries L

Définition 2.0.1. *Soit $f:\mathbb{N}\to\mathbb{C}$,*

- *On dit que f est multiplicative lorsque pour tous entiers n et m* premiers entre eux *on a :*

$$f(mn)=f(n)f(m)$$

- *On dit que f est complètement multiplicative lorsque pour tous entiers n et m on a :*

$$f(mn)=f(n)f(m)$$

Définition 2.0.2. *Soit f une fonction multiplicative, la série L associée à f est la fonction holomorphe $L(f,\cdot)$ définie par :*

$$L(f,s)=\sum_{n\geq 1}\frac{f(n)}{n^s}$$

On dit que $L(f,\cdot)$ converge absolument en s_0 lorsque la série $\sum_{n\geq 1}\left|\frac{f(n)}{n^{s_0}}\right|$ converge

Proposition 2.0.3. *Soit f une fonction multiplicative bornée, sa série L converge absolument sur le demi-plan $Re\ s>1$ et on a :*

$$L(f,s)=\prod_{p}\sum_{\alpha\geq 0}\frac{f(p^\alpha)}{p^{\alpha s}}$$

Proof. Soit M un majorant de f, on a $\left|\frac{f(n)}{n^s}\right|\leq\frac{M}{n^{Re\ s}}$, donc $L(f,.)$ converge absolument sur le demi-plan $Re\ s>1$. Si $n=p_1^{\alpha_1}\times\cdots\times p_k^{\alpha_k}$ où les p_j sont des nombres premiers 2 à 2 distincts, alors comme f est multiplicative :

$$f(n)=f(p_1^{\alpha_1})\times\cdots\times f(p_k^{\alpha_k})$$

Notons $E(k)$ l'ensemble des entiers dont les facteurs premiers sont parmis les k premiers nombres premiers $p_1,\ldots,p_k$ alors pour tout complexe s du demi-plan $Re\ s>1$, on a :

$$\sum_{n\in E(k)}\frac{f(n)}{n^s}=\sum_{\alpha_1\geq 0}\cdots\sum_{\alpha_k\geq 0}\prod_{i=1}^{k}\frac{f(p_i^{\alpha_i})}{p_i^{\alpha_i s}}=\prod_{i=1}^{k}\sum_{\alpha\geq 0}\frac{f(p_i^{\alpha})}{p_i^{\alpha s}}$$

Lorsque que $k\longrightarrow+\infty$ le membre de droite converge vers $\prod_p\sum_{\alpha\geq 0}\frac{f(p^\alpha)}{p^{\alpha s}}$ de plus comme $\mathbb{N}^*$ est la réunion croissante des $E(k)$ le terme de gauche converge vers $L(f,s)$, cqfd.

□

3 Série L associée à un caractère

Soit G_m le groupe des unités de l'anneau $\mathbb{Z}/m\mathbb{Z}$, on appelle caractère modulo m les carctères de G_m c'est à dire les morphisme

$$G_m\longrightarrow\mathbb{C}^\times$$

Un caractère χ modulo m se relève en un fonction complètement multiplicative, il suffit de poser :

$$\overline{\chi}(n)=\begin{cases}\chi(n \bmod m) \text{ lorsque } m\wedge n=1\\ 0 \text{ sinon}\end{cases}$$

On confondera χ et $\overline{\chi}$ dans la suite.

Proposition 3.0.1. *Si $\chi\neq 1$ est un caractère modulo m, alors sa série L converge absolument dans le demi-plan Re $s>1$ et converge dans le demi-plan Re $s>0$, de plus on a :*

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

Proof. G_m est fini d'ordre $n=\phi(m)$ ainsi si χ est un caractère modulo m on a pour $x\in G_m$, $\chi(x)^n=\chi(x^n)=1$ donc χ est à valeurs dans le groupe des racines n- ième de l'unité en particulier $\chi(x)$ est de module 1. On en déduit que $\overline{\chi}$ est bornée et complètement multiplicative la proprosition 2.0.3 assure alors que $L(\chi,s)$ converge sur le demi-plan *Re* $s>1$ et que :

$$L(\chi,s)=\prod_p\sum_{\alpha\geq 0}\frac{\chi(p^\alpha)}{p^{\alpha s}}$$

enfin comme χ est complètement multiplcative, on a $\chi(p^\alpha)=\chi(p)^\alpha$ d'où,

$$\sum_{\alpha\geq 0}\frac{\chi(p^\alpha)}{p^{\alpha s}}=\sum_{\alpha\geq 0}\left(\frac{\chi(p)}{p^s}\right)^\alpha=\frac{1}{1-\frac{\chi(p)}{p^s}}$$

Il reste à montrer que $L(\chi,\cdot)$ converge dans le demi-plan *Re* $s>0$, car alors l'expression obtenue dans le demi-plan *Re* $s>1$ sera valide dans le demi-plan *Re* $s>0$ par prolongement analytique. Posons, $X_n=\sum_{k=1}^n\chi(k)$ Par sommation d'Abel on a pour tout entier $N\geq 1$:

$$\sum_{n=1}^{N}\frac{\chi(n)}{n^s}=\sum_{n=1}^{N-1}X_n\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)+\frac{X_N}{N^s}$$

or on a $\frac{1}{n^s}-\frac{1}{(n+1)^s}=\frac{(1+\frac{1}{n})^s-1}{(n+1)^s}\sim\frac{s}{n^{s+1}}$ donc dès que *Re* $s>0$ la série $\sum_{n\geq 1}\frac{1}{n^s}-\frac{1}{(n+1)^s}$ converge absolument, ainsi par le critère d'Abel il suffit donc de montrer que X_n est borné pour en déduire que $L(\chi,s)$ converge. Or comme $\chi\neq 1$, par la relation d'othogonalité on a :

$$\sum_{k=n+1}^{n+m}\chi(k)=\sum_{g\in G_m}\chi(g)=0$$

ainsi $X_{n+m}=X_n$ donc X_n est périodique de période m ce qui conclut.

□

Proposition 3.0.2. *Soit $F(s) = \prod_{p|m} \frac{1}{1-\frac{1}{p^s}}$, on a :*

$$L(1,s) = F(s)\zeta(s)$$

En particulier $L(1,\cdot)$ se prolonge analytiquement au demi-plan Re $s > 0$ et admet un pôle simple en $s = 1$

Proof. Soit $\chi_0 = 1$, χ_0 est complètement multiplicative et bornée par le même calcul que pour la démonstration de la proposition prédédente on a :

$$L(1,s) = \prod_p \frac{1}{1-\frac{\chi_0(p)}{p^s}}$$

De plus on a $\chi_0(p) = 0$ si $p|m$ et $\chi_0(p) = 1$ si $p \wedge m = 1$, ainsi :

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

puis comme on peut écire pour $Re\ s > 1$

$$\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}}$$

On a $L(1,s) = F(s)\zeta(s)$ de plus la fonction F est holomorphe sur $Re\ s > 0$ et ne s'y annule pas, comme la fonction ζ se prolonge sur $Re\ s > 0$ en une fonction méromorphe avec un unique pôle en $s = 1$, on en déduit que $L(1,s)$ se prolonge sur $Re\ s > 0$ avec un unique pôle en $s = 1$.

□

En particulier on a montré que si $\chi \neq 1$ alors $L(\chi, 1)$ existe, le point essentiel de la preuve du théorème de Dirichlet est de montrer que $L(\chi, 1) \neq 0$. Dans la suite on fixe un entier $m \geq 1$ et on s'intéresse à l'ensemble des séries $L(\chi, .)$ pour χ parcourant $\widehat{G_m}$ l'ensemble des caractères modulo m, en particulier on pose :

$$\zeta_m(s) = \prod_\chi L(\chi, s)$$

Lemme 3.0.3. *Si p est premier à m, on note $f(p)$ l'ordre de p dans G_m et $g(p)$ l'indice du groupe engendré par p dans G_m, alors on a :*

$$\prod_\chi (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)}$$

Proof. Soit n un entier et $\mathcal{U}_n$ le groupe des racines n-ième de l'unité, on a :

$$1 - T^n = \prod_{\xi\in\mathcal{U}_n} (1 - \xi T)$$

Si $\chi \in \widehat{G}_m$ alors $\chi(\overline{p})^{f(p)} = \chi(\overline{p}^{f(p)}) = 1$ donc $\chi(\overline{p})$ est une racine $f(p)$-ième de l'unité. Soit ξ une racine $f(p)$-ième de l'unité, dénombrons l'ensemble des caractères χ vérifiant $\chi(\overline{p}) = \xi$. Soit H le groupe engendré par p dans G_m, puisque H est cyclique, $\chi(\overline{p}^n) = \xi^n$ est l'unique caractère de H vérifiant $\chi(\overline{p}) = \xi$, un tel caractère se prolonge de $[G_m : H] = g(p)$ façons à G_m. Ainsi il existe $g(p)$ caractère de G_m vérifiant $\chi(\overline{p}) = \xi$, ainsi :

$$\prod_\chi (1 - \chi(p)T) = \prod_{\xi\in\mathcal{U}_{f(p)}} (1 - \chi T)^{g(p)} = (1 - T^{f(p)})^{g(p)}$$

□

Lemme 3.0.4. *Sur le demi-plan $Re\ s > 1$, on a :*

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

Proof. Soit s dans le demi-plan $Re\ s > 1$, par les propositions 3.01 et 3.0.2 pour tout $\chi \in \widehat{G}_m$:
$L(\chi, s) = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}$
Ainsi,

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

or par le lemme 3.0.3 en $T = \frac{1}{p^s}$ on a pour $p \wedge m = 1$ $\prod_\chi (1 - \frac{\chi(p)}{p^s}) = (1 - \frac{1}{p^{f(p)s}})^{g(p)}$, de plus si $p|m$ alors pour tout caractère $\chi(p) = 0$ donc $\prod_\chi (1 - \frac{\chi(p)}{p^s}) = 1$, finalement :

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

□

Théorème 3.0.5. *ζ_m a un pôle simple en $s = 1$ si et seulement si pour tout $\chi \neq 1$, $L(\chi, 1) \neq 0$*

Proof. Si $\chi \neq 1$ alors $L(\chi, \cdot)$ est holomorphe sur le demi-plan $Re\ s > 0$ d'aprés 3.0.1, et si $\chi = 1$ alors $L(\chi, \cdot)$ a un pôle simple en $s = 1$ d'aprés 3.0.2. Si il existe un $\chi \neq 1$ tel que $L(\chi, 1) = 0$ alors $L(\chi, \cdot)L(1, \cdot)$ n'a pas de pôle en 1 et donc ζ_m n'as pas de pôle en 1. Réciproquement si pour tout $\chi \neq 1$, $L(\chi, 1) \neq 0$ alors comme $L(1, \cdot)$ admet un pôle en $s = 1$, ζ_m en admet un également.

□

4 Le théorème de Dirichlet

Proposition 4.0.1. *Lorsque $s \to 1$, on a :*

$$\sum_p \frac{1}{p^s} \sim \log \frac{1}{s-1}$$

Proof. On a $\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}}$ donc,

$$\log \zeta(s) = \sum_p \log \frac{1}{1 - \frac{1}{p^s}} = \sum_p \sum_{k\geq 1} \frac{1}{kp^{ks}}$$

On pose $\psi(s) = \sum_p \sum_{k\geq 2} \frac{1}{kp^{ks}}$, si $r = Re\ s > 1$ alors :

$$|\psi(s)| \leq \sum_p \sum_{k\geq 2} \frac{1}{p^{kr}} \leq \sum_{k\geq 2} (\zeta(kr) - 1) \leq \sum_{k\geq 2} (\zeta(k) - 1)$$

et $\sum_{k\geq 2}(\zeta(k) - 1) = \sum_{n\geq 2} \sum_{k\geq 2} \frac{1}{n^k} = \sum_{n\geq 2} \frac{1}{n(n-1)} = 1$, d'où $\psi(s) = O(1)$, ainsi :

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + O(1)$$

comme $\log \zeta(s) \sim \log \frac{1}{s-1}$ on en déduit le résultat.

□

Définition 4.0.2. *Soit $A \subset \mathbb{P}$, on dit que A a pour densité $\delta \in \mathbb{R}$ lorsque :*

$$\frac{1}{log \frac{1}{s-1}} \sum_{p\in A} \frac{1}{p^s} \longrightarrow \delta$$

Théorème 4.0.3. *On note $P_a(m)$ l'ensemble des premiers p tel que $p = a\ mod\ m$,*

- *si $a \wedge m \neq 1$ alors $P_a(m) = \emptyset$*
- *si $a \wedge m = 1$ alors $P_a(m)$ est infini et a pour densité $\frac{1}{\phi(m)}$*

On rappelle que $g_a(s) = \sum_{p \in P_a(m)} \frac{1}{p^s}$, pour tout $\chi \in \widehat{G_m}$, posons:

$$f_\chi(s) = \sum_{p \wedge m = 1} \frac{\chi(p)}{p^s}$$

alors f_χ converge dans le demi-plan $Re\ s > 1$ et on a le lemme suivant :

Lemme 4.0.4. *On a* $g_a(s) = \frac{1}{\phi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s)$

Proof. On a,

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_{p \wedge m = 1} \frac{1}{p^s} \sum_\chi \chi(a^{-1}p)$$

or par la relation d'orthogonalité on a :

$$\sum_\chi \chi(a^{-1}p) = \begin{cases} \phi(m) \text{ si } a^{-1}p = 1 \bmod m \\ 0 \text{ sinon} \end{cases}$$

Or la condition $a^{-1}p = 1 \bmod m$ signifie exactement que $p \in P_a(m)$ ainsi on a :

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_{p \in P_a(m)} \frac{1}{p^s} \phi(m)$$

ce qui conclut la preuve

□

Lemme 4.0.5. *Lorsque* $s \longrightarrow 1$ *on a,*

- *Si* $\chi = 1$ *alors* $f_\chi(s) \sim \log \frac{1}{s-1}$
- *Si* $\chi \neq 1$ *alors* $f_\chi(s) = O(1)$

Proof.

- Si $\chi = 1$ on a $f_\chi(s) = \sum_p \frac{1}{p^s} + O(1)$ donc par la proposition 4.0.1 on a bien $f_\chi(s) \sim \log \frac{1}{s-1}$
- Si $\chi \neq 1$ on a :

$$\log L(\chi, s) = \sum_p \log \frac{1}{1 - \frac{\chi(p)}{p^s}} = \sum_p \sum_{n \geq 1} \frac{\chi(p)^n}{n p^{ns}} = f_\chi(s) + \sum_{p|m} \frac{\chi(p)}{p^s} + \sum_p \sum_{n \geq 2} \frac{\chi(p)^n}{p^{ns}}$$

comme $\chi \neq 1$ d'aprés 3.0.1 $\log L(\chi, s)$ est bornée au voisinnage de 1, $\sum_{p|m} \frac{\chi(p)}{p^s}$ est borné donc holomorphe au voisinnage de 1, enfin :

$$\left| \sum_p \sum_{n \geq 2} \frac{\chi(p)^n}{p^{ns}} \right| \leq \sum_p \sum_{n \geq 2} \frac{1}{p^{n Re\ s}} \leq 1$$

et donc nécessairement f_χ est bornée au voisinnage de $s = 1$.

□

Preuve du théorème. □

En combinant le lemme 4.0.4 au lemme 4.0.3 on obtient que :

$$g_a(s) = \frac{1}{\phi(m)} \log \frac{1}{s-1} + O(1)$$

ce qui prouve le résultat annoncé