Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 23/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Quatrième partie : Théorie Analytique des Nombres

Fascicule 8 : Chapitre 4, sections 4.1 à 4.3 (15 pages)

4 Théorie analytique des nombres

4.1 La fonction zêta de Riemann et le théorème des nombres premiers

Pour $x > 0$ on désigne par $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x :

$$\pi(x) = \sum_{p \le x} 1. \tag{4.1}$$

Ainsi $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10\,000) = 1229$.

Le théorème des nombres premiers, conjecturé par Gauss en 1792, a été démontré par Hadamard et de la Vallée Poussin en 1896. Il s'énonce :

Théorème 4.2 (Théorème des nombres premiers). *Pour $x \to \infty$ on a*

$$\pi(x) \sim \frac{x}{\log x}\cdot$$

Une approximation de $\pi(x)$ meilleure que $x/\log x$ est donnée par la fonction *logarithme intégral*

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}\cdot$$

La démonstration de Hadamard et de la Vallée Poussin repose sur l'analyse complexe et la fonction zêta de Riemann. La série $\sum_{n\ge1} n^{-s}$ converge normalement, donc uniformément pour s dans un compact du demi plan $\Re s > 1$. Par conséquent elle définit une fonction analytique dans ce demi-plan qui est la fonction zêta (introduite par Riemann en 1859 dans son unique article de théorie des nombres) :

$$\zeta(s) = \sum_{n\ge1} \frac{1}{n^s}\cdot$$

Les valeurs de cette fonction pour s réel positif avaient déjà été étudiées par Euler en 1736. Il montrait notamment que pour s entier positif pair le quotient $\zeta(s)/\pi^s$ est un nombre rationnel. Par exemple $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$. Euler ne s'est pas contenté d'étudier les valeurs de cette

fonction pour s positif, il a aussi considéré le cas des entiers négatifs (où la série diverge), par exemple $\zeta(0) = -1/2$, $\zeta(-1) = -1/12$. Il a établi que ζ s'annule en les entiers négatifs pairs et prend une valeur rationnelle non nulle en les entiers négatifs impairs.

Le *théorème fondamental de l'arithmétique* selon lequel l'anneau $\mathbf{Z}$ est factoriel est intégré dans l'énoncé suivant qui éclaire l'importance du rôle joué par la fonction zêta dans l'étude de la répartition des nombres premiers.

Théorème 4.3 (Produit d'Euler). *Le produit infini $\prod_p (1-p^{-s})$ étendu aux nombres premiers p, est uniformément sur tout compact du demi plan $\Re s > 1$. Il définit une fonction analytique dans ce demi plan qui vérifie*

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

Le fait que la série harmonique $\sum_{n\geq 1} 1/n$ diverge permet d'en déduire que la série $\sum_p 1/p$ est aussi divergente.

Démonstration. En faisant le produit pour les nombres premiers $\leq X$ des séries géométriques

$$\frac{1}{1-p^{-s}} = \sum_{m\geq 0} \frac{1}{p^{ms}}$$

on trouve

$$\prod_{p\leq X} \frac{1}{1-p^{-s}} = \prod_{p\leq X} \sum_{m\geq 0} \frac{1}{p^{ms}} = \sum_{n\in\mathcal{N}(X)} \frac{1}{n^s},$$

où $\mathcal{N}(X)$ est l'ensemble des entiers positifs dont tous les facteurs premiers sont $\leq X$. Alors pour $\Re s = \sigma > 1$ on a

$$\left|\zeta(s) - \prod_{p\leq X} \frac{1}{1-p^{-s}}\right| = \left|\sum_{n\notin\mathcal{N}(X)} \frac{1}{n^s}\right| \leq \sum_{n>X} \left|\frac{1}{n^s}\right| = \sum_{n>X} \frac{1}{n^\sigma}\cdot$$

La définition de la convergence d'un produit infini dont tous les facteurs sont différents de 0 impose que le produit ne soit pas nul. Afin de vérifier $\zeta(s) \neq 0$ pour $\Re s > 1$, on utilise le développement en série de Taylor de la détermination principale du logarithme complexe : pour $|u| < 1$,

$$\log(1-u) = -\sum_{m\geq 1} \frac{u^m}{m}\cdot$$

On remplace u par p^{-s} :

$$\log(1-p^{-s}) = -\sum_{m\geq 1} \frac{p^{-ms}}{m}$$

et on trouve, pour $\Re s > 1$,

$$\zeta(s) = \exp\left(\sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}\right). \tag{4.4}$$

Donc $\zeta(s) \neq 0$ pour $\Re s > 1$. □

On écrit (4.4) sous la forme

$$\log \zeta(s) = \sum_p \sum_{m \geq 1} \frac{1}{m p^{ms}}.$$

En dérivant, on obtient le développement en série de la dérivée logarithmique de ζ dans ce demi plan.

Corollaire 4.5. *La série*

$$\sum_p \sum_{m \geq 1} \frac{1}{m p^{ms}}$$

définit une fonction analytique dans le demi plan $\Re s > 1$ qui est une détermination analytique du logarithme de $\zeta(s)$ dans ce demi plan. De plus la dérivée logarithmique de $\zeta(s)$ vérifie pour $\Re s > 1$:

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_{m \geq 1} \frac{\log p}{p^{ms}}.$$

Le développement en série de ζ'/ζ peut aussi s'écrire

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n \geq 1} \frac{\Lambda(n)}{n^s}$$

où Λ désigne la *fonction de Mangoldt*

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m \text{ avec } p \text{ premier} \\ 0 & \text{si } n \text{ n'est pas une puissance d'un nombre premier.} \end{cases}$$

Théorème 4.6 (Prolongement analytique de la fonction zêta de Riemann). *La fonction $\zeta(s) - 1/(s-1)$ se prolonge en une fonction analytique dans le demi plan $\Re s > 0$.*

Démonstration. On écrit, pour $n \geq 1$,

$$\frac{1}{n^s} = s \int_n^\infty t^{-s-1} dt.$$

Alors

$$\zeta(s) = s \sum_{n \geq 1} \int_n^\infty t^{-s-1} dt = s \int_1^\infty [t] t^{-s-1} dt$$

car $\sum_{n=1}^t 1 = [t]$. Donc

$$\zeta(s) = s \int_1^\infty t^{-s} dt + s \int_1^\infty ([t] - t) t^{-s-1} dt.$$

Le premier terme vaut

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

et la seconde intégrale est convergente dans $\Re s > 0$ où elle définit une fonction holomorphe.

□

Exercice. Vérifier

$$\lim_{s\to 1}\left(\zeta(s)-\frac{1}{s-1}\right)=\gamma$$

où γ est la *constante d'Euler* :

$$\gamma=\lim_{N\to\infty}\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{N}-\log N.$$

Ainsi la fonction zêta de Riemann se prolonge en une fonction méromorphe dans le demi plan $\Re s>0$ avec un pôle simple en $s=1$, de résidu 1. Une des étapes essentielles dans la démonstration du théorème des nombres premiers 4.2 consiste à montrer qu'il existe une constante $A>0$ telle que la fonction ζ, ainsi prolongée, ne s'annule pas dans le rectangle

$$1-\frac{A}{\log|\Im s|}<\Re s<1.$$

En 1903 E. Landau a montré que le théorème 4.2 des nombres premiers peut se déduire d'un énoncé plus faible, qui avait été obtenu dès 1892 par Hadamard :

Théorème 4.7. *La fonction ζ ne s'annule pas sur la droite $\Re s=1$, $s\neq 1$.*

Il en résulte que la fonction

$$\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1},$$

définie pour $\Re s>1$, s'étend en une fonction holomorphe dans un voisinage de la droite $\Re s=1$.

Riemann a démontré en 1859 que la fonction zêta s'étendait en une fonction méromorphe dans tout le plan complexe, avec un unique pôle simple en $s=1$, et que de plus cette fonction ainsi étendue vérifiait une équation fonctionnelle. Pour l'écrire on introduit la fonction Gamma d'Euler

Proposition 4.8. *L'intégrale*

$$\Gamma(s)=\int_0^\infty e^{-t}t^{s-1}dt$$

définit une fonction holomorphe pour $\Re s>0$ qui vérifie l'équation fonctionnelle

$$\Gamma(s+1)=s\Gamma(s).$$

Elle se prolonge en une fonction méromorphe dans $\mathbf{C}$ ayant un pôle simple en tous les entiers ≤ 0.

Démonstration. Il est facile de vérifier que l'intégrale converge et définit une fonction analytique dans le demi plan $\Re s>0$. En intégrant par parties on trouve

$$\Gamma(s)=\left[\frac{1}{s}e^{-s}+t^s\right]_0^\infty-\frac{1}{s}\int_0^\infty e^{-t}t^s dt=\frac{1}{s}\Gamma(s+1).$$

Cette équation fonctionnelle permet de prolonger la fonction par la formule

$$\Gamma(s)=\frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n)}.$$

Le membre de droite est bien défini pour $\Re s > -n-1$, celui de gauche seulement pour $\Re s > 0$. Pour $\Re s > 0$, les deux membres coïncident. En prenant $s \in \mathbf{C}$ quelconque et en choisissant $n > -\Re s - 1$, on définit $\Gamma(s)$ en prenant comme définition le membre de droite : il ne dépend pas de n et on obtient ainsi une fonction analytique dans $\mathbf{C} \setminus \{0,\ -1,\ -2\ldots\}$ ayant un pôle simple en $s = -n$ pour n entier ≥ 0 ; le résidu est $(-1)^n/n!$ (avec $0! = 1$, comme il se doit). □

Remarque. Comme $\Gamma(1) = 1$ on en déduit $\Gamma(n+1) = n!$.

On définit une fonction entière dans $\mathbf{C}$ par

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Le seul pôle de ζ est $s = 1$. De plus ζ s'annule aux entiers pairs strictement négatifs et ne s'annule pas aux entiers négatifs impairs. Les pôles de $\Gamma(s/2)$ sont tous les entiers pairs ≤ 0 et Γ ne s'annule pas en $s = 1$. C'est pourquoi la fonction ξ est entière (analytique dans $\mathbf{C}$). Sa valeur en $s = 0$ et en $s = 1$ est 1, ce qui revient à dire que l'on a $\Gamma(1/2) = \sqrt{\pi}$. En effet, en effectuant le changement de variables $t = x^2$ on trouve

$$\Gamma(1/2) = \int_0^\infty e^{-t}t^{-1/2}dt = 2\int_0^\infty e^{-x^2}dx.$$

Donc

$$\frac{1}{4}\Gamma(1/2)^2 = \int_0^\infty\int_0^\infty e^{-x^2-y^2}dxdy = \int_0^\infty\int_0^{\pi/2} e^{-r^2}rdrd\theta = \left[-\frac{1}{2}e^{-r^2}\right]_0^\infty \frac{\pi}{2} = \frac{\pi}{4}.$$

B. Riemann a aussi démontré :

Théorème 4.9 (Equation fonctionnelle de la fonction zêta de Riemann). *La fonction ξ vérifie*

$$\xi(s) = \xi(1-s).$$

L'axe de symétrie est $\Re s = 1/2$, l'équation fonctionnelle permet de bien connaître la fonction ζ dans le demi plan $\Re s < 0$ grâce au produit infini qui converge dans $\Re s > 1$. Par exemple les seuls zéros de ζ dans ce demi plan $\Re s < 0$ sont les entiers négatifs pairs.

Le domaine $0 < \Re s < 1$ est la *bande critique* et la droite $\Re s = 1/2$ est la *droite critique*. C'est Riemann qui a montré l'importance des zéros non triviaux (c'est-à-dire dans la bande critique) de la fonction zêta pour l'étude des nombres premiers. Après Euler il a montré le lien entre la fonction zêta et la fonction π – cf. (4.1) en établissant la relation

$$\frac{1}{s}\log\zeta(s) = \int_0^s \frac{\pi(x)}{x^{s-1}}\frac{dx}{x}$$

pour $\Re s > 1$. Le *produit de Hadamard*, qui permet d'exprimer une fonction entière comme produit infini étendu à l'ensemble des zéros, s'écrit [1]

$$\zeta(s) = \frac{2^{s-1}\pi^s}{e^{((\gamma/2)+1)s}(s-1)\Gamma(1+(s/2))}\prod_\varrho\left(1-\frac{s}{\varrho}\right)e^{s/\varrho}$$

[1] Le produit infini sur ϱ est la limite, pour T tendant vers l'infini, du produit étendu à l'ensemble fini des ϱ de partie imaginaire $\leq T$.

où ϱ décrit les zéros de ζ dans la bande critique, et il a estimé le nombre de zéros dans un rectangle $[0,1]\times[0,iT]$ de cette bande : pour $t\to\infty$ il vaut

$$\frac{T}{2\pi}\log\frac{T}{2\pi}-\frac{T}{2\pi}+O(\log T).$$

On démontre le théorème 4.9 qui donne l'équation fonctionnelle de la fonction zêta de Riemann en utilisant la *Formule de Poisson* qui relie la série des valeurs aux entiers rationnels d'une fonction intégrable f sur $\mathbf{R}$ à la série des valeurs de sa transformée de Fourier

$$\widehat{f}(y)=\int_{-\infty}^{+\infty}f(x)e^{2i\pi xy}dx.$$

Si la fonction $x\mapsto\sum_{n\in\mathbf{Z}}f(x+n)$ est continue et à variations bornées sur $[0,1]$, alors

$$\sum_{n\in\mathbf{Z}}f(n)=\sum_{m\in\mathbf{Z}}\widehat{f}(m).$$

Cette formule de Poisson permet de montrer que la *série thêta*

$$\theta(u)=\sum_{n\in\mathbf{Z}}e^{-\pi un^2}$$

satisfait l'équation fonctionnelle, pour $u\in\mathbf{R}_+^\times$:

$$\theta(1/u)=\sqrt{u}\theta(u).$$

On montre ensuite que la fonction ξ du théorème 4.9 satisfait, pour $\Re s>1$,

$$\xi(s)=s(s-1)\int_0^\infty\frac{(\theta(u)-1)u^{s/2}}{2u}du.$$

Pour terminer cette section voici l'énoncé d'un des principaux problèmes ouverts en théorie des nombres.

Conjecture 4.10 (Hypothèse de Riemann). *Les zéros complexes de ζ dans la bande critique sont tous sur la droite critique : si $s\in\mathbf{C}$ vérifie $0<\Re s<1$ et $\zeta(s)=0$, alors $\Re s=1/2$.*

On trouvera d'autres informations sur la fonction zêta de Riemann dans le texte de P. Cartier [Ca].

4.2 Le théorème de la progression arithmétique de Dirichlet

A.M. Legendre a conjecturé en 1785 et Lejeune Dirichlet a démontré en 1837 le théorème de la progression arithmétique :

Théorème 4.11 (Dirichlet). *Soient a et b deux entiers positifs premiers entre eux. Alors il existe une infinité de nombres premiers p congrus à a modulo b.*

La démonstration du théorème 4.2 des nombres premiers s'étend aux progressions arithmétiques et permet de préciser cet énoncé. Pour a et b entiers positifs et pour $x>0$, on désigne par $\pi(x;a,b)$ le nombre de nombres premiers p dans l'intervalle $2\leq p\leq x$ qui sont congrus à a modulo b :

Théorème 4.12. *Soient a et b deux entiers positifs premiers entre eux. Pour $x\to\infty$ on a*

$$\pi(x;a,b)\sim\frac{x}{\varphi(b)\log x}.$$

4.2.1 Caractères

Soit A un groupe abélien d'exposant fini et soit m un multiple de l'exposant ; autrement dit tout élément x de A vérifie $mx = 0$. Les homomorphismes de A dans un groupe cyclique d'ordre m forment un groupe, qui ne dépend (à isomorphisme près) ni du groupe cyclique d'ordre m choisi (deux groupes cycliques d'ordre m sont isomorphes), ni du choix de m multiple de l'exposant de A. En effet, si m_0 est l'exposant de A et si C_m est un groupe cyclique d'ordre m multiple de m_0, alors pour tout homomorphisme de A dans C_m l'image de A appartient à l'unique sous-groupe de C_m d'ordre m_0. On définit le *dual de* A par

$$\widehat{A} = \mathrm{Hom}(A, C_m).$$

Par exemple si k est un corps qui contient les racines m-ièmes de l'unité, alors $\widehat{A}$ est isomorphe au *groupe des caractères de* A, qui sont les homomorphismes de A dans le groupe multiplicatif $k^\times$. On prendra le plus souvent pour k le corps des nombres complexes (les caractères de G sont les homomorphismes de G dans le groupe multiplicatif $\mathbf{U}$ des nombres complexes de module 1, comme l'exposant de A est fini son image est dans le groupe de torsion de $\mathbf{U}$, qui est le groupe des racines de l'unité), mais on peut aussi prendre un corps fini $\mathbf{F}_q$, la condition pour que $\mathbf{F}_q$ contienne les racines m-ièmes de l'unité s'écrivant $m|q-1$, c'est-à-dire $q \equiv 1 \pmod{m}$.

Aussi $\widehat{A}$ est isomorphe au groupe des homomorphismes de A dans le groupe $\mathbf{Q}/\mathbf{Z}$. Noter que $\mathbf{Q}/\mathbf{Z}$ est le groupe de torsion de $\mathbf{R}/\mathbf{Z}$, il est isomorphe au groupe de torsion de $\mathbf{U}$, c'est-à-dire le groupe des racines de l'unité dans $\mathbf{C}$.

Si le groupe C_m est noté additivement, l'élément neutre de $\widehat{A}$ est l'application constante $x \mapsto 0$, tandis que s'il est noté multiplicativement, c'est $x \mapsto 1$.

4.2.2 Dual d'un groupe abélien fini

Le dual est défini pour un groupe abélien d'exposant fini. Il est donc bien défini pour un groupe abélien fini.

Proposition 4.13. *Un groupe cyclique est isomorphe à son dual.*

Démonstration. Soit A un groupe cyclique et soit m son ordre. Alors l'exposant de A est m. Le dual de A est donc isomorphe au groupe des endomorphismes de A. Un tel endomorphisme est déterminé par l'image d'un générateur. Soit x un générateur de A et soit ψ l'application identité de A dans A.

Quand on note A additivement, pour $0 \leq k < m$ l'application $k\psi : A \to A$ qui envoie x sur kx est un endomorphisme de A. En notation multiplicative on considère l'application $\psi^k : A \to A$ qui envoie x sur x^k.

On obtient ainsi tous les endomorphismes de A. De plus ψ est d'ordre m dans $\widehat{A}$. Donc ψ est un générateur du groupe $\widehat{A}$ et par conséquent $\widehat{A}$ est cyclique d'ordre m.

□

Noter que cet isomorphisme entre A et $\widehat{A}$ quand A est cyclique dépend du choix d'un générateur : il n'y a pas plus d'isomorphisme canonique entre A et $\widehat{A}$ que de générateur privilégié d'un groupe cyclique. Il existe exactement $\varphi(m)$ isomorphismes entre un groupe cyclique A d'ordre m et son dual $\widehat{A}$.

Soient A et B deux groupes abéliens finis et soit $f : A \to B$ un homomorphisme de groupes. On lui associe un homomorphisme $f\widehat{\ } : \widehat{B} \to \widehat{A}$ défini de la manière suivante : soit m un multiple commun de l'exposant de A et de celui de B. Si $\psi : B \to C_m$ est un homomorphisme de B dans un groupe cyclique C_m d'ordre m, on pose $f\widehat{\ }(\psi) = \psi \circ f$, qui est un homomorphisme de A dans C_m :

$$f\widehat{\ }(\psi) : A \xrightarrow{f} B \xrightarrow{\psi} C_m.$$

Si $f : A_1 \to A_2$ et $g : A_2 \to A_3$ sont deux homomorphismes de groupes, alors $(g \circ f)\widehat{\ } = f\widehat{\ } \circ g\widehat{\ }$: c'est l'homomorphisme $\widehat{A_3} \to \widehat{A_1}$ qui envoie $\psi : A_3 \to C_m$ sur $\psi \circ g \circ f : A_1 \to C_m$.

Théorème 4.14. *Si B et C sont deux groupes abéliens finis et si $A = B \times C$ est leur produit direct, alors $\widehat{A}$ est isomorphe au produit direct $\widehat{B} \times \widehat{C}$.*

Démonstration. Notons A additivement. Soient $f : A \to B$, $g : A \to C$ les projections de $A = B \times C$ sur chacun des deux facteurs et $i : B \to A$, $j : C \to A$ les injections canoniques. Alors

$$\begin{array}{rccc} f\widehat{\ } + g\widehat{\ } : & \widehat{B} \times \widehat{C} & \to & \widehat{A} \\ & (\psi_1, \psi_2) & \mapsto & \psi_1 \circ f + \psi_2 \circ g \end{array}$$

et

$$\begin{array}{rccc} (i\widehat{\ }, j\widehat{\ }) : & \widehat{A} & \to & \widehat{B} \times \widehat{C} \\ & \psi & \mapsto & (\psi \circ i, \psi \circ j) \end{array}$$

sont deux isomorphismes inverses.

□

En combinant la proposition 4.13 et le théorème 4.14 on déduit du théorème de structure des groupes abéliens finis :

Corollaire 4.15. *Un groupe abélien fini est isomorphe à son dual.*

Lemme 4.16. *Soient G un groupe abélien fini d'ordre n, x un élément de G d'ordre r et ζ une racine primitive r-ième de l'unité. Il existe n/r caractères de G tels que $\xi(x) = \zeta$. De plus on a, dans $\mathbf{C}[T]$,*

$$\prod_{\chi \in \widehat{G}} (1 - \chi(x)T) = (1 - T^r)^{n/r}.$$

Pour $r = 1$ le lemme se réduit à dire que $\widehat{G}$ a n éléments qui envoient tous 1 sur 1.

Si G est cyclique d'ordre n et que l'on prend $r = n$, le lemme dit que si x est un générateur de G, alors pour tout caractère χ de G l'image $\chi(x)$ est une racine r-ième de 1, pour toute racine r-ième de 1 il existe un unique χ qui envoie x sur cette racine, et enfin χ est entièrement connu quand on connaît $\chi(x)$.

Démonstration. Comme $x^r = 1$ pour tout $\chi \in \widehat{G}$ on a $\chi(x)^r = 1$ et donc $\chi(x)$ est une racine r-ième de l'unité. L'application $\chi \mapsto \chi(x)$ de $\widehat{G}$ dans le groupe cyclique des racines de l'unité d'ordre divisant r est un homomorphisme dont le noyau est constitué par les caractères triviaux sur le sous-groupe cyclique H de G engendré par x. Le noyau est isomorphe au dual de G/H, il a donc n/r éléments et par conséquent l'image a r éléments.

□

4.2.3 Bidual

Nous avons vu qu'il n'y avait pas d'isomorphisme canonique entre un groupe abélien fini et son dual. En revanche nous allons voir qu'il y a un isomorphisme canonique entre un groupe abélien et son bidual.

Proposition 4.17. *Soit A un groupe abélien fini. Soit m un multiple de l'exposant de A et soit C_m un groupe cyclique d'ordre m. À un élément x de A on associe l'élément $\widetilde{x}$ de $\widehat{\widehat{A}}$ qui envoie $\chi \in \widehat{A}$ sur $\chi(x) \in C_m$. Alors l'application*

$$\begin{array}{ccc} A & \to & \widehat{\widehat{A}} \\ x & \mapsto & \widetilde{x} \end{array}$$

est un isomorphisme de groupes.

La démonstration de la proposition 4.17 repose sur le lemme de séparation suivant, dans lequel nous notons e l'élément neutre de A (donc $e = 0$ en notation additive et $e = 1$ en notation multiplicative).

Lemme 4.18. *Soit A un groupe abélien fini et soit $x \in A \setminus \{e\}$. Alors il existe $\chi \in \widehat{A}$ tel que $\chi(x) \neq 1$.*

Démonstration. Ce lemme est clair quand A est cyclique, le cas général s'en déduit par le théorème de structure des groupes abéliens finis.

□

Démonstration de la proposition 4.17. L'application $x \mapsto \widetilde{x}$ est un homomorphisme de groupes de A dans son bidual, le lemme 4.18 montre qu'elle est injective, et comme A et son bidual ont le même nombre d'éléments (on sait déjà grâce au théorème de structure des groupes abéliens finis que ces deux groupes sont isomorphes) elle est aussi surjective.

□

4.2.4 Orthogonalité des caractères

On désigne par A un groupe abélien fini, par e son élément neutre, par m son exposant, par k un corps contenant les racines m-ièmes de l'unité et par $\widehat{A}$ le groupe des homomorphismes de A dans le groupe multiplicatif de k. Les éléments de $\widehat{A}$ sont les caractères de A. Ce groupe $\widehat{A}$ est une des formes du dual de A, mais ici nous allons utiliser non seulement la structure multiplicative de k mais aussi sa structure additive. Le caractère unité χ_1 de A (encore appelé *caractère principal de A*) est l'application constante

$$\begin{array}{rccc} \chi_1 : & A & \to & k^\times \\ & x & \mapsto & 1. \end{array}$$

Lemme 4.19. *Soit A un groupe abélien fini.*
(i) Soit $\chi \in \widehat{A}$. Alors

$$\sum_{x \in A} \chi(x) = \begin{cases} 0 & si\ \chi \neq \chi_1, \\ |A| & si\ \chi = \chi_1. \end{cases}$$

(ii) Soit $x \in A$. Alors

$$\sum_{\chi \in \widehat{A}} \chi(x) = \begin{cases} 0 & \text{si } x \neq e, \\ |A| & \text{si } x = e. \end{cases}$$

Démonstration. Commençons par démontrer *(i)*. Soit $y \in A$. Notons A additivement *(la rédaction de la démonstration en notation multiplicative est laissée en exercice)*. L'application $y \mapsto x + y$ est une bijection de A sur A, donc

$$\sum_{x \in A} \chi(x + y) = \sum_{x \in A} \chi(x).$$

Par ailleurs $\chi(x + y) = \chi(x)\chi(y)$, donc

$$\sum_{x \in A} \chi(x + y) = \chi(y) \sum_{x \in A} \chi(x).$$

Par conséquent

$$\big(1 - \chi(y)\big) \sum_{x \in A} \chi(x) = 0$$

pour tout $y \in A$. Si $\chi \neq \chi_1$ alors il existe $y \in A$ tel que $\chi(y) \neq 1$, d'où on déduit

$$\sum_{x \in A} \chi(x) = 0.$$

Dans le cas $\chi = \chi_1$ tous les $\chi(x)$, $x \in A$ valent 1 et il y en a $|A|$. Cela complète la démonstration de *(i)*.

Pour la démonstration de *(ii)* on peut soit répéter la démonstration de *(i)* en utilisant le lemme 4.18, soit utiliser le théorème 4.17 : notons $\tilde{x}$ l'élément de $\widehat{\widehat{A}}$ associé à $x \in A$ par l'isomorphisme canonique entre A et son bidual ; on écrit

$$\sum_{\chi \in \widehat{A}} \chi(x) = \sum_{\chi \in \widehat{A}} \tilde{x}(\chi)$$

et on utilise *(i)* avec A remplacé par $\widehat{A}$. □

Exercice. Pour a et x dans A vérifier

$$\frac{1}{|A|} \sum_{\chi \in \widehat{A}} \overline{\chi}(a)\chi(x) = \begin{cases} 1 & \text{si } x = a, \\ 0 & \text{si } x \neq a. \end{cases}$$

Remarque. Le $\mathbf{C}$-espace vectoriel $\mathbf{C}^A$, qui est de dimension $|A|$, est muni d'une structure Hilbertienne grâce au produit scalaire

$$\langle x, y \rangle = \frac{1}{|A|} \sum_{a \in A} x(a)\overline{y(a)}.$$

Un caractère χ de A considéré comme application de A dans $\mathbf{C}^\times$ est un élément de $\mathbf{C}^A$. Comme ses valeurs sont dans le cercle unité $\mathbf{U} = \{z \in \mathbf{C}\ ;\ |z| = 1\}$, le caractère $\overline{\chi}$ obtenu en composant χ avec l'automorphisme de conjugaison complexe de $\mathbf{C}$ est l'inverse χ^{-1} de χ dans le groupe $\widehat{A}$.

Le produit scalaire de deux caractères χ' et χ'' est alors

$$\begin{aligned}\langle \chi', \chi'' \rangle = & \quad \frac{1}{|A|} \sum_{a \in A} \chi'(a)\overline{\chi''(a)} \\ = & \quad \frac{1}{|A|} \sum_{a \in A} \chi'(a)\chi''^{-1}(a) \\ = & \quad \frac{1}{|A|} \sum_{a \in A} \chi' \circ \chi''^{-1}(a) \\ = & \quad \begin{cases} 1 & \text{si } \chi' = \chi'', \\ 0 & \text{si } \chi' \neq \chi''. \end{cases}\end{aligned}$$

La dernière égalité résulte du lemme 4.19. Ainsi ce lemme exprime que les caractères de A forment une base orthonormée de $\mathbf{C}^A$.

On peut comparer ce résultat au suivant : soit $\mathbf{T} = \mathbf{R}/\mathbf{Z}$ le tore de dimension 1 (isomorphe à $\mathbf{U}$ par l'application $z \mapsto e^{2i\pi z}$). Un caractère de $\mathbf{T}$ est un homomorphisme *continu* de $\mathbf{T}$ dans $\mathbf{C}^\times$; les caractères de $\mathbf{T}$ forment un sous-groupe $\widehat{\mathbf{T}}$ de $\mathbf{C}^{\mathbf{T}}$. Pour chaque $n \in \mathbf{Z}$ l'application

$$\begin{array}{rccc} e_n : & \mathbf{T} & \to & \mathbf{C}^\times \\ & t & \mapsto & e^{2i\pi nt} \end{array}$$

est un caractère de $\mathbf{T}$, et on obtient ainsi tous les éléments de $\widehat{\mathbf{T}}$. De plus la famille $(e_n)_{n \in \mathbf{Z}}$ forme une base orthonormale de l'espace de Hilbert $L^2(\mathbf{T})$ des fonctions définies sur $\mathbf{T}$ et de carré intégrable (pour la mesure de Lebesque sur $[0, 1[$) pour le produit scalaire

$$\langle f, g \rangle = \int_0^1 f(t)\overline{g(t)}dt.$$

4.2.5 Caractères de Dirichlet

Soit q un entier ≥ 2. Le groupe multiplicatif $(\mathbf{Z}/q\mathbf{Z})^\times$ des éléments inversibles de l'anneau $\mathbf{Z}/q\mathbf{Z}$ est d'ordre $\varphi(q)$. Un élément du dual de $(\mathbf{Z}/q\mathbf{Z})^\times$ définit une application de l'ensemble des entiers premiers avec q à valeurs dans $\mathbf{C}^\times$ qui vérifie

$$\chi(ab) = \chi(a)\chi(b) \quad \text{pour tout } (a, b) \in \mathbf{Z}^2 \text{ avec } (ab, q) = 1$$

et

$$\chi(a + q) = \chi(a) \qquad \text{pour tout } a \in \mathbf{Z} \text{ avec } (a, q) = 1.$$

On prolonge χ en une application notée encore χ de $\mathbf{Z}$ dans $\mathbf{C}$ par $\chi(a) = 0$ si $(a, q) \neq 1$ et $\chi(0) = 0$.

On appelle *caractère de Dirichlet* (ou encore *caractère modulaire*) les applications $\mathbf{Z} \to \mathbf{C}$ ainsi obtenues. On notera D_q l'ensemble de celles qui proviennent de $(\mathbf{Z}/q\mathbf{Z})^\times$: ce sont les *caractères modulo* q. L'ensemble D_q a donc $\varphi(q)$ éléments. Pour $\chi \in D_q$ on a

$$\chi^{-1}(0) = \{a \in \mathbf{Z}\ ;\ (a, q) \neq 1\}.$$

Le *caractère principal modulo q* est l'application $\chi_1 = \mathbf{Z} \to \mathbf{C}^\times$ définie par

$$\chi_1(n) = \begin{cases} 0 & \text{si } (n,q) \neq 1, \\ 1 & \text{si } (n,q) = 1. \end{cases}$$

Pour $q = 1$ le quotient $\mathbf{Z}/1\mathbf{Z}$ n'est pas un anneau, mais on convient que $(\mathbf{Z}/1\mathbf{Z})^\times = \{1\}$. Avec cette convention $D_1 = \{\chi_1\}$ où

$$\chi_1(n) = \begin{cases} 0 & \text{si } n = 0, \\ 1 & \text{si } n \neq 0. \end{cases}$$

Exemple. Il y a deux caractères modulo 4, le caractère principal χ_1 modulo 4 et le caractère χ_2 défini par

$$\chi_2(n) = \begin{cases} 0 & \text{si } n \text{ est pair}, \\ 1 & \text{si } n \equiv 1 \pmod 4, \\ -1 & \text{si } n \equiv -1 \pmod 4. \end{cases}$$

Il y a quatre caractères modulo 8, le caractère principal χ_1, le caractère χ_2, le caractère χ_3 défini par

$$\chi_3(n) = \begin{cases} 0 & \text{si } n \text{ est pair}, \\ 1 & \text{si } n \equiv \pm 1 \pmod 8, \\ -1 & \text{si } n \equiv \pm 5 \pmod 8 \end{cases}$$

et le caractère $\chi_2\chi_3$.

Si p est un nombre premier impair le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$, donc le groupe dual aussi. Soit a une racine primitive modulo p (la classe de a modulo p est un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$). Pour chacune des $p-1$ racines $p-1$-ièmes de l'unité ζ, on définit un caractère ψ_ζ modulo p par

$$\psi_\zeta(n) = \begin{cases} 0 & \text{si } p|n, \\ \zeta^u & \text{si } n \equiv a^u \pmod p. \end{cases}$$

Par exemple le choix $\zeta = -1$ (licite car p est impair) correspond à l'unique caractère de Dirichlet modulo p qui soit d'ordre 2 ; il est associé au symbole de Legendre :

$$\psi_{-1}(n) = \begin{cases} 0 & \text{si } p|n, \\ \left(\dfrac{n}{p}\right) & \text{si } (n,p) = 1. \end{cases}$$

4.2.6 Série L attachée à un caractère

Soit f une application de l'ensemble des nombres premiers dans $\mathbf{C}$. On a (formellement, ou si on préfère en supposant f à support fini, c'est-à-dire $f(p) = 0$ pour p suffisamment grand)

$$\begin{aligned} \sum_{p \equiv a \pmod m} f(p) &= \frac{1}{\varphi(m)} \sum_\chi \sum_p \overline{\chi}(a)\chi(p)f(p) \\ &= \frac{1}{\varphi(m)} \sum_{p \nmid m} f(p) + \frac{1}{\varphi(m)} \sum_{\chi \neq 1} \overline{\chi}(a) \sum_p \chi(p) f(p). \end{aligned}$$

Définition. Soit χ un caractère de Dirichlet modulo m. On définit la série L de Dirichlet attachée à χ par

$$L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s}.$$

Par exemple si χ_1 est le caractère principal modulo m on a

$$\chi_1(n) = \begin{cases} 1 & \text{si } \operatorname{pgcd}(m, n) = 1, \\ 0 & \text{si } \operatorname{pgcd}(m, n) > 1 \end{cases}$$

et donc

$$L(\chi_1, s) = \sum_{\substack{n \geq 1 \\ \operatorname{pgcd}(m,n)=1}} n^{-s} = \zeta(s) \prod_{p \mid m} (1 - p^{-s}).$$

Proposition 4.20. *L'abscisse de convergence de la série $L(\chi, s)$ est*

$$\sigma = \begin{cases} 0 & \textit{si } \chi \neq \chi_1, \\ 1 & \textit{pour } \chi = \chi_1. \end{cases}$$

Démonstration. Pour un caractère χ modulo m qui n'est pas le caractère principal on a

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

pour tout entier r, donc

$$\left| \sum_{n \leq x} \chi(n) \right| \leq m.$$

□

Théorème 4.21 (Produit d'Euler généralisé). *Soient m un entier positif et χ un caractère de Dirichlet modulo m. Le produit infini*

$$\prod_p (1 - \chi(p) p^{-s}) \tag{4.22}$$

étendu aux nombres premiers p, est uniformément convergent sur tout compact du demi plan $\Re s > 1$. Il définit une fonction analytique $L(\chi, s)$ dans ce demi plan qui vérifie

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

Démonstration. On reprend la démonstration du théorème 4.3 qui est le cas particulier du caractère principal modulo 1. En faisant le produit pour les nombres premiers $\leq X$ des séries géométriques

$$\frac{1}{1 - \chi(p) p^{-s}} = \sum_{m \geq 0} \frac{\chi(p)^m}{p^{ms}}$$

on trouve

$$\prod_{p\le X}\frac{\chi(p)}{1-p^{-s}} = \prod_{p\le X}\sum_{m\ge 0}\frac{\chi(p)^m}{p^{ms}} = \sum_{n\in\mathcal{N}(X)}\frac{\chi(n)}{n^s},$$

où $\mathcal{N}(X)$ est encore l'ensemble des entiers positifs dont tous les facteurs premiers sont $\le X$. Alors pour $\Re s = \sigma > 1$ on a

$$\left| L(\chi,s) - \prod_{p\le X}\frac{\chi(p)}{1-p^{-s}}\right| < \sum_{n>X}\frac{1}{n^\sigma}.$$

□

Corollaire 4.23. *Dans le demi plan $\Re s > 1$ la fonction $L(\chi,s)$ ne s'annule pas et une détermination analytique de son logarithme est*

$$\sum_p\sum_{m\ge 1}\frac{\chi(p)^m}{mp^{ms}}.$$

De plus la dérivée logarithmique de $L(\chi,s)$ vérifie pour $\Re s > 1$:

$$\frac{L'(\chi,s)}{L(\chi,s)} = -\sum_p\sum_{m\ge 1}\frac{\chi(p)^m\log p}{p^{ms}} = -\sum_{n\ge 1}\frac{\chi(p)^m\Lambda(n)}{n^s}.$$

Le résultat clé de la démonstration par Dirichlet de son théorème de la progression arithmétique est le pendant du théorème de Hadamard 4.7 :

Théorème 4.24. *Pour tout caractère de Dirichlet χ différent du caractère principal χ_1,*

$$L(\chi,1)\neq 0.$$

Cet énoncé est équivalent au fait que le produit Eulérien (4.22) converge en $s=1$.

4.3 Autres fonctions zêta

Nous avons vu que l'écriture de la fonction zêta de Riemann à la fois comme série de Dirichlet et comme produit d'Euler (Théorème 4.3) était une formulation du théorème fondamental de l'arithmétique. L'existence et l'unicité de la décomposition des idéaux d'un corps de nombres en produit d'idéaux premiers donne lieu à la fonction zêta de Dedekind (voir par exemple [Co] Définition 4.9.11 ; pour le cas particulier de $\mathbf{Z}[i]$, voir aussi [Ca] § 2.6).

Théorème 4.25. *Soit K un corps de nombres. La fonction zêta de Dedekind, définie pour $\Re s > 1$ par la série*

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s},$$

où la somme est étendue à l'ensemble des idéaux entiers non nuls de $\mathbf{Z}_K$, est égale au produit infini

$$\prod_{\mathfrak{p}}\left(1-N(\mathfrak{p})^{-s}\right)^{-1},$$

où le produit est étendu aux idéaux premiers non nuls de $\mathbf{Z}_K$.

Bien entendu pour $K = \mathbf{Q}$ on retrouve la fonction zêta de Riemann. Dans le cas général cette fonction admet encore un prolongement analytique (en une fonction méromorphe dans $\mathbf{C}$ avec un unique pôle simple en $s = 1$) et une équation fonctionnelle, qui fait intervenir plusieurs quantités, liées au corps de nombres K, que nous avons déjà rencontrées : le degré $n = [K : \mathbf{Q}]$, le nombre de plongements réels r_1 et le nombre de plongements complexes non réels $2r_2$ (avec $r_1 + 2r_2 = n$), le discriminant Δ, le nombre de classes d'idéaux h, le nombre de racines de l'unité w. Elle fait aussi intervenir le *régulateur* R du corps K, qui est le volume du réseau dans un hyperplan de $\mathbf{R}^{r_1+r_2}$ qui est l'image par le plongement logarithmique du groupe des unités.

On introduit la fonction

$$\Lambda(s) = |\Delta|^{s/2} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{r_1} \left(\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)\right)^{r_2} \zeta_K(s).$$

Alors l'équation fonctionnelle de la fonction zêta de Dedekind du corps K est $\Lambda(s) = \Lambda(1 - s)$.

De plus la fonction ζ_K a un zéro en $s = 0$ de multiplicité $r = r_1 + r_2 - 1$ (le rang du groupe des unités de K) et

$$\lim_{s\to 0} s^{-r}\zeta_K(s) = -hR/w.$$

Par l'équation fonctionnelle, cela signifie que le résidu en $s = 1$ est

$$\lim_{s\to 1}(s-1)\zeta_K(s) = 2^{r_1}(2\pi)^{r_2}\frac{hR}{w\sqrt{\Delta}}.$$

L'*hypothèse de Riemann généralisée* dit encore que les zéros de ζ_K dans la bande critique sont sur la droite critique.

Les fonctions L associées à un caractère de Dirichlet ont aussi des généralisations : on définit des fonctions L (Artin) attachées à une extension Galoisienne K/k de corps de nombres et à un caractère du groupe de Galois. Dans le cas d'une extension cyclotomique de $\mathbf{Q}$ on retombe sur les fonctions L précédentes.

On introduit aussi des fonctions ζ et L attachées à d'autres objets géométriques, notamment
• les courbes elliptiques (Hasse Weil), ce qui donne lieu à la Conjecture de Birch et Swinnerton-Dyer (voir par exemple [Co] Conjecture 7.3.9),
• les formes modulaires,
• les représentations automorphes (programme de Langlands, théorie du corps de classes non abélien).

Ce ne sont que les premiers exemples : les fonctions zêta et L jouent un rôle important dans de multiples domaines, aussi bien en géométrie diophantienne (fonction zêta de Hasse–Weil attachée à une variété) que dans l'étude des systèmes dynamiques.

Références

[Ca] Pierre Cartier, An introduction to Zeta functions, *From number theory to physics*,Springer-Verlag, Berlin, (1992), Chap. I p. 1–63.

[Co] Henri Cohen, A course in computatioonal algebraic number theory, Graduate Textes in Math. **138** (1993).