Feuille 6 : Dirichlet et Chebotarev

Une *fonction arithmétique* est une fonction $f\colon \mathbb{N}_{>0} \to \mathbb{C}$. Elle est dite *multiplicative* si $f(1) = 1$ et

$$f(nm) = f(n)f(m)$$

si $\text{pgcd}(m, n) = 1$. De plus, on dit que f est *totalement multiplicative* si $f(nm) = f(n)f(m)$ pour tout n et m.

Si f et g sont des fonctions arithmétiques, on définit leur *produit de convolution* par la formule

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d)$$

Exercice 1. Soit F le groupe abélien des fonctions arithmétique par rapport à la somme.

1. Montrer que $(F, +, *)$ est un anneau commutatif. Expliciter son unité.
2. Montrer que $F^* = \{f \in F \text{ telles que } f(1) \neq 0\}$.
3. Soit $n = \prod_{i=1}^{r} p_i^{e_i}$ la décomposition en facteurs premiers de $n \in \mathbb{N}$. On défini la fonction $\mu\colon \mathbb{N} \to \mathbb{C}$ par $\mu(n) = (-1)^r$ si chaque $e_i = 1$ et $\mu(n) = 0$ sinon. Montrer que μ est l'inverse (par rapport à la convolution) de $\mathbf{1}$, la fonction constant égale à 1 : c'est la *fonction de Möbius*.
4. En déduire la *formule d'inversion de Möbius* : si f et g sont des fonctions arithmétiques, alors

   $$g(n) = \sum_{d|n} f(d) \text{ pour tout } n \geq 1$$

   si et seulement si f est la *transformée de Möbius* de g :

   $$f(n) = \sum \mu(d)g(n/d) \text{ pour tout } n \geq 1$$

5. Montrer que

   $$\left(\sum_{i=1}^{\infty} \frac{f(n)}{n^s}\right)\left(\sum_{i=1}^{\infty} \frac{g(n)}{n^s}\right) = \sum_{i=1}^{\infty} \frac{(f * g)(n)}{n^s}$$

Exercice 2. 1. Soit f une fonction multiplicative bornée. Montrer que la série de Dirichlet $\sum f(n)/n^s$ converge absolument pour $\Re(s) > 1$ et

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_{p} \sum_{m=0}^{\infty} f(p^m)p^{-sm}$$

2. Soit f une fonction totalement multiplicative bornée. On a

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_p \frac{1}{1 - f(p)p^{-s}}$$

Exercice 3. 1. Exprimer à l'aide de $\zeta(s)$ les séries de Dirichlet associées à $\mu(n)$ et $\mu(n)^2$.

2. Montrer que

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

Exercice 4. Montrer le théorème de la progression arithmétique de Dirichlet : pour tout entiers naturels non nuls a et b premiers entre eux, il existe une infinité de nombres premiers de la forme $a + nb$, où $n > 0$.

Exercice 5. 1. Soit $f \in \mathbb{Z}[x]$ tel que f est scindé modulo p pour presque tout p. Montrer que f est scindé sur $\mathbb{Q}$.

2. Montrer que si un groupe fini G agit transitivement sur un ensemble X non trivial, il existe $g \in G$ tel que $\forall x \in X, g \cdot x \neq x$.
3. Montrer qu'un polynôme $f \in \mathbb{Z}[x]$ irréductible qui a une racine modulo p pour presque tout p est de degré 1.
4. Trouver un polynôme à coefficients entiers qui n'a pas de racine dans $\mathbb{Z}$ mais en a modulo tout nombre premier.

Exercice 6. Soit K un corps de nombres. Montrer que les idéaux premiers sont équidistribués dans $\mathrm{Cl}(K)$.