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

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

Indications 1.
1. L'unité est la fonction $U\colon \mathbb{N} \to \mathbb{C}$ telle que $U(1) = 1$ et $U(n) = 0$ si $n > 1$.
2. Si $f \in F^*$, on construit à la main son inverse g et écrivant $(f * g)(1) = 1$ (pour trouver $g(1)$), $(f * g)(2) = 0$, $(f * g)(3) = 0$ etc. À chaque étape on divise seulement par $f(1)$.

3. Il suffit de montrer que $(\mathbf{1} * \mu)(n) = U(n)$ pour tout n. Si $n = 1$ l'égalité est claire. Si $n > 1$, soit P l'ensemble de premiers qui divisent n et soit k le cardinal de P. Les seuls d qui divisent n tels que $\mu(d) \neq 0$ sont les produits d'éléments distincts de P, et si $t \leq k$ on a $\binom{k}{t}$ facteurs avec t premiers, pour lesquels μ vaut $(-1)^t$. On trouve

$$\sum_{d|n} \mu(d) = \sum_{t=1}^{k} \binom{k}{t} (-1)^t = (1-1)^k = 0$$

4. $f(n) = \sum \mu(d) g(n/d)$ signifie $f = \mu * g$, mais μ est l'inverse de $\mathbf{1}$, donc ça équivaut à $\mathbf{1} * f = g$ et $(\mathbf{1} * f)(n) = \sum_{d|n} f(d)$.
5. Clair.

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

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

Indications 2. 1. La convergence est immédiate. Soit S un ensemble de premier et soit $\mathbb{N}(S)$ l'ensemble des $n \in \mathbb{N}$ tels que tous les facteurs premiers de n soit dans S. On a

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

Il suffit de prendre S de plus en plus grand.

2. Clair.

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

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

Indications 3. 1. On utilise l'exercice précèdent : μ et μ^2 sont multiplicatives et en calculant la série (qui a seulement deux termes) on a

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

et

$$\sum_{n=1}^{\infty} \mu(n)^2/n^s = \prod_p (1+p^{-s}) = \frac{\zeta(s)}{\zeta(2s)}$$

2. On a

$$\sum_{d|n} \varphi(d) = n$$

et donc par inversion de Möbius,

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

On trouve

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

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 $n > 0$.

Indications 4. Soit $K = \mathbb{Q}(\zeta_b)$ et $f \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $f(\zeta_b) = \zeta_b^a$. Vu que $\mathrm{Gal}(K/\mathbb{Q})$ est abelien, le singleton $\{f\}$ est une classe de conjugaison. L'exercice suit de Chebotarev.

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.

Indications 5.

1. On note K le corps de décomposition de f. Soit p un premier tel que f modulo p est scindé à racines simples (ce qui est vrai pour presque tout p). Si $\alpha \in \mathbb{C}$ est une racine de f, le polynôme minimal f_α de α divise f et il est donc scindé à racines simple modulo p. Le lemme de Hensel implique que f_α est scindé dans $\mathbb{Q}_p$ et donc p est totalement décomposé dans $\mathbb{Q}(\alpha)$. On en déduit que p est totalement décomposé dans K (car K est le compositum des $\mathbb{Q}(\alpha)$). En particulier, Frob_p est trivial pour presque tout p. Par le théorème de Chebotarev le groupe de Galois de f est réduit à la classe de conjugaison de l'élément neutre.
2. Si ce n'était pas le cas, on aurait

$$\bigcup_x \mathrm{Stab}_x = G$$

Or, les stabilisateurs sont des sous-groupes conjugués et un groupe ne peut pas être recouvert pas des conjugués de sous-groupes strict. En effet, si H est le sous-groupe et on fait agir G sur l'ensemble des parties de G par conjugaison, on a évidemment que $H \subseteq \mathrm{Stab}_H$, et donc l'orbite de H est de cardinal au plus $[G : H]$. Si $G = \bigcup_g g^{-1}Hg$ on peut écrire G comme union de $[G : H]$ sous-ensembles de cardinal égale au cardinal de H, qui doivent donc être disjoints, ce qui est absurde parce que $1 \in g^{-1}Hg$ pour tout $g \in G$.

3. On note encore K le corps de décomposition de f. Soit p un premier tel que p est non ramifié dans $\mathcal{O}_K$ et $f \bmod p$ a une racine $\bar{\alpha} \in \mathbb{F}_p$ (ce qui est vrai pour presque tout p). Soit $\alpha \in K$ un relèvement de $\bar{\alpha}$. Soit $\mathcal{P}$ au-dessus de p On a $\mathrm{Frob}_p(\alpha \bmod \mathcal{P}) = \mathrm{Frob}(\bar{\alpha}) = \bar{\alpha}$ donc $\mathrm{Frob}_p(\alpha)$ est une racine de f congrue à α modulo $\mathcal{P}$. Étant p non ramifié dans $\mathcal{O}_K$ (et donc dans $\mathcal{O}_{\mathbb{Q}[x]/f}$), on a que f est à racines simples dans $\overline{\mathbb{F}}_p$: en particulier, la réduction modulo $\mathcal{P}$ est une bijections entre les racines de f dans K et celles de $f \bmod p$ dans $\overline{\mathbb{F}}_p$ et on en déduit que $\mathrm{Frob}_p(\alpha) = \alpha$. On a montré que presque tous les Frobenius ont un point fixe en faisant agir le groupe de Galois sur l'ensemble des racines de f. Cela implique que chaque classe de conjugaison du groupe de Galois a un point fixe d'après Chebotarev. Puisque l'action sur les racines est transitive (f est irréductible), il y a qu'une racine.
4. On cherche un polynôme non irréductible sans racines. Un produit de deux quadratique ne fonction pas : par réciprocité quadratique et Dirichlet il existe toujours un premier congru à des non-carrés modulo deux nombres distincts. Avec trois en revanche, tout polynôme $(x^- a)(x^2 - b)(x^2 - ab)$ où a, b et ab ne sont pas des carrés dans $\mathbb{Q}$, tandis que modulo p le produit des deux non-carrés est un carré. On peut faire mieux avec par exemple le polynôme $(x^2 + x + 1)(x^3 - 2)$. Pour tout premier p, soit $p \equiv 1 \bmod 3$ et le polynôme cyclotomique a une racine, soit $p \equiv 2 \bmod 3$ et 2 est un cube modulo p.

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

Indications 6. C'est le groupe de Galois du corps de classes de Hilbert.