FORMULE DE POISSON DISCRÈTE

[Pey04, §II.3, p44]

ÉNONCÉ

Soit G un groupe abélien fini et H un sous-groupe de G.

LEMME. *$H^{\#} \simeq \widehat{G/H}$ est de cardinal $\frac{|G|}{|H|}$.*

PROPOSITION. [FORMULE DE POISSON DISCRÈTE]
Pour toute fonction $f : G \longrightarrow \mathbb{C}$, et pour tout $g \in G$, on a :

$$\sum_{h \in H} f(gh) = \frac{|H|}{|G|} \sum_{\chi \in H^{\#}} \widehat{f}(\overline{\chi})\, \chi(g)\,.$$

En particulier ($g = 1$), on a $\displaystyle\sum_{h \in H} f(h) = \frac{|H|}{|G|} \sum_{\chi \in H^{\#}} \widehat{f}(\overline{\chi})$.

DÉVELOPPEMENT

Commençons par le lemme. Regardons l'application :

$$\varphi : \begin{array}{ccc} \widehat{G/H} & \longrightarrow & H^{\#} \\ \chi & \longmapsto & \widetilde{\chi} : g \longmapsto \chi(gH) \end{array}.$$

Pour tout $\chi \in \widehat{G/H}$, il est clair que $\widetilde{\chi}$ est bien un caractère. Comme de plus $\widetilde{\chi}(h) = \chi(H) = 1$ pour tout $h \in H$, ceci justifie que l'application φ est bien définie.
De plus, il est immédiat de vérifier que φ est un morphisme de groupes.

Vérifions que φ est bijective.

- Pour l'injectivité, il est clair que $\widetilde{\chi_1} = \widetilde{\chi_2}$ implique $\chi_1 = \chi_2$ par surjectivité de l'application $G \longrightarrow G/H, g \longmapsto gH$, et puisque $\chi_1(gH) = \widetilde{\chi_1}(g) = \widetilde{\chi_2}(g) = \chi_2(gH)$ pour tout $g \in G$.
- Pour la surjectivité, fixons $\gamma \in H^{\#}$ et définissons $\chi \in \widehat{G/H}$ par $\chi(gH) = \gamma(g)$ pour tout $g \in G$. Cette application est bien définie puisque si $gH = g'H$, alors $g(g')^{-1} \in H$ et donc $\gamma\big(g(g')^{-1}\big) = 1$, ou encore $\gamma(g) = \gamma(g')$. C'est bien un caractère puisque par passage au quotient χ hérite de la structure de morphisme.

Ainsi $H^{\#} \simeq \widehat{G/H}$, d'où l'on déduit immédiatement

$$\left|H^{\#}\right| = \frac{|G|}{|H|}\,.$$

Passons maintenant à la formule de POISSON.
On note S un système de représentants de G/H dans G [1].
Soit donc $f : G \longrightarrow \mathbb{C}$. Regardons l'application :

$$\widetilde{f} : \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \sum_{h \in H} f(gh) \end{array}.$$

Remarquons que $\widetilde{f}$ est invariante par H, puisque si $g \in G$ et $h \in H$:

$$\widetilde{f}(gh) = \sum_{h' \in H} f(ghh') = \sum_{h'' \in H} f(gh'') = \widetilde{f}(g)\,.$$

L'application $\widetilde{f}$ passe donc au quotient et définit une application [2] $\widetilde{f} : G/H \longrightarrow \mathbb{C}$.
On peut donc décomposer $\widetilde{f}$ en série de FOURIER [3] :

$$\forall g \in G, \quad \widetilde{f}(\overline{g}) = \sum_{\chi \in \widehat{G/H}} \langle \widetilde{f} \mid \chi \rangle\, \chi(\overline{g})\,.$$

Fixons $\chi \in \widehat{G/H}$. Comme $S \times H \longrightarrow G, (g,h) \longmapsto gh$ est bijective, il vient :

$$\begin{aligned} \langle \widetilde{f} \mid \chi \rangle &= \frac{1}{|G/H|} \sum_{g \in S} \widetilde{f}(\overline{g})\, \overline{\chi(\overline{g})} = \frac{|H|}{|G|} \sum_{g \in S} \sum_{h \in H} f(gh)\, \overline{\chi(\overline{g})} \\ &= \frac{|H|}{|G|} \sum_{g' \in G} f(g')\, \overline{\chi(\overline{g'})} \qquad \text{puisque } \chi(\overline{gh}) = \chi(\overline{g}) \\ \langle \widetilde{f} \mid \chi \rangle &= \frac{|H|}{|G|} \sum_{g' \in G} f(g')\, \overline{\widetilde{\chi}(g')} = \frac{|H|}{|G|} \widehat{f}(\overline{\widetilde{\chi}})\,. \end{aligned}$$

D'où finalement, pour tout $g \in G$, en utilisant le lemme :

$$\sum_{h \in H} f(gh) = \sum_{\chi \in \widehat{G/H}} \frac{|H|}{|G|} \widehat{f}(\overline{\widetilde{\chi}})\, \chi(\overline{g}) = \frac{|H|}{|G|} \sum_{\widetilde{\chi} \in H^{\#}} \widehat{f}(\overline{\widetilde{\chi}})\, \widetilde{\chi}(g)\,.$$

COMMENTAIRES

Il faut connaître la formule de POISSON vue en analyse, qui s'écrit presque de la même manière !

La formule de POISSON discrète peut notamment être utilisée en théorie des codes correcteurs.

1. $S \longrightarrow G/H, g \longmapsto gH$ est bijective
2. toujours appelée $\widetilde{f}$
3. c'est en fait la formule d'inversion, qui découle du fait que $\hat{G}$ est une base orthonormée de $\mathcal{F}(G,\mathbb{C})$