FEUILLE DE TD 2

Exercice 1 (Le symbole de Legendre comme signature d'une permutation)**.** Soient p un nombre premier impair et a un entier qui n'est pas un multiple de p. Démontrer que le symbole de Legendre $\left(\frac{a}{p}\right)$ est égal à la signature de la permutation "multiplication par a" de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 2 (Calcul du signe de la somme de Gauss)**.** Soit p un nombre premier impair. Considérons la *somme de Gauss quadratique*, définie comme le nombre complexe

$$\mathrm{G}_p = \sum_{x \in \mathbb{F}_p} \exp\left(2\pi i \frac{x^2}{p}\right)$$

Le but de cet exercice est de démontrer la formule

$$\mathrm{G}_p = \begin{cases} \sqrt{p} & \text{si } p \equiv 1 \bmod 4, \\ i\sqrt{p} & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

Soient $\xi = \exp(2\pi i/p)$ et soit

$$\mathrm{S} = (\xi^{ij})_{0 \leq i,j \leq p-1}$$

la matrice de Vandermonde associée à $1, \xi, \ldots, \xi^{p-1}$.

(1) Calculer S^2 et en déduire $\det(\mathrm{S})^2 = (-1)^{p(p-1)/2} p^p$.

(2) En utilisant le fait que S est une matrice de Vandermonde, montrer $\det(\mathrm{S}) = i^{p(p-1)/2} p^{p/2}$.

(3) Montrer que les valeurs propres de S appartiennent à l'ensemble $\{\sqrt{p}, -\sqrt{p}, i\sqrt{p}, -i\sqrt{p}\}$.

(4) Notant u, v, r, s leurs multiplicités, démontrer les égalités

$$u + v = \frac{p+1}{2}, \quad r + s = \frac{p-1}{2}, \quad 2v - r - s \equiv \frac{p(p-1)}{2} \bmod 4.$$

(5) Montrer que la trace de S est égal à

$$\mathrm{Tr}(\mathrm{S}) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \xi^k.$$

(6) Conclure.

Exercice 3 (Une autre démonstration de la loi de réciprocité quadratique)**.** Le « calcul du signe » de l'exercice 2 est encore valable pour la somme de Gauss quadratique

$$\mathrm{G}_{pq} = \sum_{k=1}^{p\ell} \exp\left(2\pi i \frac{k^2}{p\ell}\right)$$

associée au produit $p\ell$ de deux nombres premiers impairs distincts. Plus généralement :

$$\mathrm{G}_n = \begin{cases} \sqrt{n} & \text{si } n \equiv 1 \bmod 4, \\ 0 & \text{si } n \equiv 0 \bmod 4, \\ i\sqrt{n} & \text{si } n \equiv 3 \bmod 4, \\ (1+i)\sqrt{n} & \text{si } n \equiv 0 \bmod 4. \end{cases}$$

En acceptant ce résultat, nous proposons une démonstration de la loi de réciprocité quadratique.

(1) Démontrer l'égalité

$$\mathrm{G}_{pq} = \sum_{x=1}^{p}\sum_{y=1}^{\ell} \exp\left(2\pi i \frac{(\ell x + py)^2}{p\ell}\right).$$

(2) Calculer $\sum_{x=1}^{p} \exp\left(2\pi i \frac{\ell x^2}{p}\right)$ selon que x soit un carré modulo p ou pas.

(3) En déduire l'égalité

$$\mathrm{G}_{p\ell} = \mathrm{G}_p \mathrm{G}_\ell \left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right).$$

(4) Démontrer la loi de réciprocité quadratique en écrivant

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = \frac{\mathrm{G}_{p\ell}}{\sqrt{p\ell}}\,\frac{\sqrt{p}}{\mathrm{G}_p}\,\frac{\sqrt{\ell}}{\mathrm{G}_\ell}.$$

Exercice 4 (Exemples de caractères de Dirichlet)**.** Soit $\mathrm{N} \geq 1$ un entier. Rappelons qu'un *caractère de Dirichlet modulo* N est un morphisme de groupes $\chi\colon (\mathbb{Z}/\mathrm{N}\mathbb{Z})^\times \to \mathbf{C}^\times$

(1) Faire la liste de tous les caractères de Dirichlet modulo 4 et 8.

(2) Faire la liste des caractères de Dirichlet modulo 7 qui sont d'ordre 3.

Exercice 5 (Orthogonalité des caractères)**.** Soit G un groupe abélien fini. Soit V l'espace vectoriel complexe des fonctions $\varphi\colon \mathrm{G} \to \mathbf{C}$, muni du produit hermitien

$$\langle \varphi, \psi \rangle = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} \overline{\varphi(g)}\psi(g)$$

Démontrer que les caractères de G forment une base orthonormée de V.

Exercice 6. Soit G un groupe abélien fini.

(1) Soit h un élément de G dont l'ordre m est un multiple de l'ordre de tout élément de G et soit H le sous-groupe cyclique de G engendré par h. Démontrer qu'il existe un caractère χ de G qui envoie h sur une racine primitive $m$ème de l'unité.

(2) Démontrer que l'image d'un tel χ est le sous-groupe de $\mathbf{C}$ formé des racines primitives

(3) Soit K le noyau de χ. Démontrer que $\mathrm{H} \cap \mathrm{K}$ est réduit à l'élément neutre, puis que G est isomorphe au produit $\mathrm{H} \times \mathrm{K}$.

Exercice 7 (Un groupe abélien fini et son dual sont isomorphes)**.**

(1) Soient G et H des groupes abéliens finis. Construire un isomorphisme entre le groupe de caractères du produit $\mathrm{G} \times \mathrm{H}$ et le produit $\widehat{\mathrm{G}} \times \widehat{\mathrm{H}}$ des groupes de caractères.

(2) Démontrer que tout groupe abélien fini est un produit de groupes cycliques.

(3) Soit G un groupe abélien fini. Démontrer que G et $\widehat{\mathrm{G}}$ sont isomorphes.