Université Joseph Fourier
Mathématiques

Représentations de groupes finis et TFD

Extraits de devoirs à la maison 2010-16
en préparation à l'agrégation.

I Les représentations irréductibles du groupe diédral.

Soit n entier ≥ 3. On note D_n le sous–groupe de $\mathrm{O}(\mathbb{R}^2)$ fait des isométries qui conservent le polygone régulier à n côtés centré en 0 et passant par $(1,0)$. On rappelle que $|D_n| = 2n$ et que D_n est engendré par r et s, où r est la rotation d'angle $2\pi/n$ et s la symétrie orthogonale d'axe Ox.

1. Soient Γ un groupe et a, b deux éléments de Γ. Montrer qu'il existe un morphisme de D_n dans Γ qui envoie s sur a et r sur b si et seulement si a et b vérifient les relations:

$$b^n = 1\,, \quad a^2 = (ab)^2 = 1\,. \qquad (*)$$

2. Déduire de 1. tous les morphismes de D_n dans $\mathbb{C}^\times$ (distinguer selon la parité de n).

3. Soit k entier. Montrer avec 1. qu'on définit un morphisme f_k de D_n dans lui-même en posant: $f_k(r^l) = r^{lk}$, $f_k(sr^l) = sr^{lk}$.

On note ρ la représentation naturelle de D_n dans $\mathbb{C}^2$, issue de l'inclusion naturelle de $\mathrm{O}(\mathbb{R}^2)$ dans $\mathrm{GL}(\mathbb{C}^2)$. On définit la représentation $\rho_k = \rho \circ f_k$ de D_n dans $\mathbb{C}^2$ (k entier).

4. On suppose désormais que l'entier k est compris entre 1 et $(n-1)/2$. Montrer ρ_k est irréductible (prouver que $\rho_k(r)$ et $\rho_k(s)$ n'ont pas de droite propre commune).

5. Donner le caractère χ_k de ρ_k et en déduire que les représentations ρ_k sont deux à deux non isomorphes.

6. En distinguant suivant la parité de n, calculer la somme des carrés des représentations irréductibles de D_n (de degré 1 ou 2) ainsi mises en évidence. Conclure qu'on en a obtenu la liste complète, à isomorphisme près.

7. Écrire les classes de conjugaison de D_n (suivant la parité de n; dessin des symétries du polygone régulier?) Comparer le nombre des classes d'isomorphisme de représentations irréductibles avec le nombre de classes de conjugaison de D_n.

8. Si k' est un entier compris entre $(n+1)/2$ et $n-1$, à quelle représentation $(\mathbb{C}^2, \rho_{k'})$ est–elle isomorphe?

II Les représentations irréductibles de $\mathfrak{A}_5$.

On rappelle que le groupe alterné $\mathfrak{A}_5$ est simple, isomorphe au groupe des isométries positives de l'icosaèdre régulier. Pour $\sigma \in \mathfrak{A}_5$, on notera $cl(\sigma)$ sa classe de conjugaison dans $\mathfrak{A}_5$ et $<\sigma>$ son sous-groupe engendré.

0. *Rappel sur les représentations par permutation* Supposons donnée une action du groupe fini G sur l'ensemble fini X. On lui associe la représentation linéaire par permutation de G sur le $\mathbb{C}$–espace vectoriel de base $B_X = (e_x)_{x\in X}$ indexée par X définie par: $g \cdot e_x = e_{g\cdot x}$ $(g \in G,\, x \in X)$.
On vérifie alors facilement que:

(i) pour chaque orbite ω de l'action, le sous-espace engendré par les $e_x, x \in \omega$ est une sous–représentation de G.

(ii) la valeur du caractère de cette représentation en $g \in G$ est le nombre d'éléments de X fixés par g.

(iii) la représentation considérée est somme directe des sous-représentations $\mathbb{C}s$ et W, où s désigne la somme des e_x, $x \in X$ et W désigne l'hyperplan d'équation: $\sum_{x\in X} \lambda_x = 0$ dans la base B_X.

(iv) dans le cas de l'action naturelle de $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$, W est dit *représentation standard* de $\mathfrak{S}_n$; on montre qu'elle est irréductible (voir aussi *Serre*, exo 2 p29).

1. Donner le nombre d'éléments de chaque ordre dans $\mathfrak{A}_5$ et la répartition des éléments d'ordre 2 et 3 en classes de conjugaison.

2. Dans cette question on désigne par σ un 5-cycle de $\mathfrak{A}_5$.

a) Montrer que σ et σ^{-1} sont conjugués dans $\mathfrak{A}_5$.

b) Donner le nombre de 5-Sylow de $\mathfrak{A}_5$ et en déduire que $cl(\sigma)$ contient au moins 12 éléments.

c) Conclure enfin que $\mathrm{card}(cl(\sigma)) = 12$. Que vaut $cl(\sigma) \cap <\sigma>$? Combien y a–t–il de classes de conjugaison dans $\mathfrak{A}_5$?

d) Donner un élément η de $\mathfrak{S}_5$ tel que $\eta\sigma\eta^{-1} = \sigma^2$ et justifier que la conjugaison par η induit un automorphisme $\theta\colon \tau \mapsto \eta\tau\eta^{-1}$ de $\mathfrak{A}_5$ qui échange les deux classes de conjugaison de 5–cycles.

e) Déduire de b) le cardinal du normalisateur N de $<\sigma>$ dans $\mathfrak{A}_5$. Donner le nombre d'éléments de chaque ordre dans N.

3. Etudier la restriction à $\mathfrak{A}_5$ de la représentation standard de $\mathfrak{S}_5$ (voir 0.(iii), (iv)): donner les valeurs de son caractère χ_W sur les classes de conjugaison de $\mathfrak{A}_5$ et montrer son irréductibilité.

4. a) Déduire du rappel ci–dessus concernant le groupe des isométries de l'icosaèdre régulier une représentation complexe (V, ρ) de dimension 3 du groupe $\mathfrak{A}_5$.

b) Donner la valeur du caractère χ_V de V sur chaque classe de conjugaison de $\mathfrak{A}_5$ (on pensera à la forme canonique des éléments de $SO_3(\mathbb{R})$). Montrer que cette représentation est irréductible.

c) On pose $\rho' = \rho \circ \theta$. Montrer que (V, ρ') est une représentation de $\mathfrak{A}_5$ qui est aussi irréductible et donner les valeurs de son caractère χ'_V sur chaque classe de conjugaison. Les représentations ρ et ρ' sont–elles équivalentes?

5. (*cette question n'est pas indispensable pour traiter 6.*) On considère l'action de $\mathfrak{A}_5$ par conjugaison sur l'ensemble de ses 5-Sylow. La représentation par permutation qui s'en déduit est alors somme directe de la représentation triviale et d'une représentation notée S, de caractère χ_S (voir 0.(iii)).

a) Déduire de 0.(ii) et 2.e) la valeur de χ_S sur les 3–cycles et sur les 5–cycles.

b) Soit τ d'ordre 2 dans $\mathfrak{A}_5$. Montrer que τ est dans le normalisateur d'exactement deux 5-Sylow de $\mathfrak{A}_5$. En déduire $\chi_S(\tau)$ et montrer que la représentation S est irréductible.

6. Déterminer les degrés des représentations irréductibles de $\mathfrak{A}_5$ (considérées à équivalence près) et écrire la table des caractères de $\mathfrak{A}_5$.

III Le groupe dicyclique d'ordre 12 et sa table.

1. Expliciter le groupe $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$, et montrer qu'il existe un unique morphisme non trivial de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$, noté φ.

Dans la suite on note G le groupe produit semi–direct $\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$ (les lois des facteurs sont donc notées additivement). Ce groupe non abélien à 12 éléments est dit *groupe dicyclique*.

2. Déterminer le sous–groupe dérivé $D(G)$ (sans calculs). Expliciter les éléments du groupe $\widehat{G_{ab}}$.

3. Donner la liste des degrés des caractères irréductibles de G.

Dans les questions 5 *et* 6*, on s'efforcera de raisonner de manière à minimiser les calculs.*

4. Justifier que $(\overline{0}, \overline{2})$ est dans le centre de G. Montrer que c'est l'unique élément de G d'ordre 2 (utiliser le morphisme p_2 de projection sur le 2^d facteur), puis trouver les éléments d'ordre 6 et l'ordre de chaque élément.

5. Trouver les classes de conjugaison de G et donner les cardinaux des centralisateurs. Compléter alors les colonnes des éléments d'ordre 4.

6. Si χ un caractère irréductible de G, on rappelle que le produit de χ par tout caractère ψ de degré 1 est un caractère irréductible de G. En déduire une relation entre les caractères de degré > 1 de G (utiliser un caractère de degré 1 qui ne vaut pas 1 en $(\overline{0}, \overline{2})$).

7. Compléter la table des caractères de G.

8. Soit V la représentation par permutation correspondant à l'action de G par conjugaison sur ses 2–Sylow. Donner la décomposition de V en irréductibles, à isomorphisme près.

9. Montrer que si G est un groupe de cardinal 12 alors $\operatorname{card} \widehat{G} > 1$. En déduire que G n'est pas simple. Donner toutes les listes possibles pour les degrés des caractères irréductibles.

10. Citer les groupes à 12 éléments que vous connaissez et étudier s'ils sont isomorphes entre eux. Ont–ils même table de caractères? (*)Votre liste est–elle complète, à isomorphisme près?

IV Groupe non abélien d'ordre pq.

On se donne deux nombres premiers p et q tels que p divise $q-1$; on note $r = (q-1)/p$ (en particulier on explicitera complètement le cas $p = 3$, $q = 7$). On pourra utiliser les théorèmes de Sylow.

1. a) Justifier que $C_p = \{y^r \,|\, y \in \mathbb{F}_q^\times\}$ est l'unique sous–groupe d'ordre p de $\mathbb{F}_q^\times$.

b) On note $\Gamma = \{\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \,|\, x \in C_p,\, y \in \mathbb{F}_q\}$. Montrer que Γ est un sous–groupe non abélien d'ordre pq de $\mathrm{GL}_2(\mathbb{F}_q)$.

2. Dans la suite, on considère G un groupe non abélien d'ordre pq (il résulte de 1. qu'un tel groupe existe).

a) Montrer que G possède un unique sous–groupe N d'ordre q, qui est distingué. Déterminer le sous–groupe dérivé $D(G)$ et l'abélianisé $G_{ab} = G/D(G)$.

b) Combien G possède–t–il de sous–groupes d'ordre p?

c) Montrer que le centre de G est trivial et que tout élément de G d'ordre p possède exactement q conjugués.

d) Soit $b \in G$ d'ordre p. Montrer que l'ensemble des classes de conjugaison de G qui ne sont pas dans N admet $b, \ldots, b^{p-1}$ pour système de représentants (on pourra considérer les images dans l'abélianisé). Donner le cardinal de ces classes.

e) Quel est le nombre de conjugués d'un élément d'ordre q? Conclure que G admet $p + r$ classes de conjugaison.

f) Pour les cas $|G| = 21$ puis $p = 2$, décrire les classes incluses dans N, en fonction d'un élément a d'ordre q (on peut traiter toute la suite indépendamment de cette question).

3. On se donne donc un système $1, a_1 = a, \ldots, a_r, b, \ldots, b^{p-1}$ de représentants des classes de conjugaison de G (où les a_i sont dans N).

a) À quel groupe s'identifie le groupe dual $\mathrm{Hom}(G, \mathbb{C}^\times)$ de G? Expliciter tous les caractères de degré 1 de G sur le système ci–dessus.

b) Montrer que tout caractère irréductible de degré > 1 de G s'annule en chaque b^k, $1 \leq k \leq p-1$ (utiliser les relations sur les colonnes de la table de caractères).

c) Montrer que G possède exactement r caractères irréductibles de degré > 1. Pour la suite on pourra utiliser le résultat que leur degré divise $|G|$.

d) En utilisant la formule de Burnside sur les degrés des caractères irréductibles, déterminer les degrés de tous les caractères irréductibles de G.

4. On suppose $|G|$ impair.

a) Soit $x \neq 1$ dans G. Montrer que si x était conjugué à son inverse, sa classe de conjugaison serait de cardinal pair. Conclure que x n'est pas conjugué à son inverse.
Dans la suite on pose donc $a_2 = a^{-1}$ (cf. 3).

b) Si χ est un caractère de G, que vaut $\chi(a^{-1})$?

c) Montrer qu'il existe un caractère irréductible χ de G tel que $\chi(a) \notin \mathbb{R}$. Que dire alors de $\bar{\chi}$?

d) Dans le cas $|G| = 21$, dresser la table des caractères de G (utiliser a)).

5. Pour $p = 2$, on tombe sur les groupes diédraux D_q, q premier ≥ 3. Dresser la table de D_5.

V Groupe de Heisenberg.

Soit $N \in \mathbb{N}^*$; on note A le groupe abélien additif $\mathbb{F}_2^N$. Pour $x = (x_i)_{1 \leq i \leq N}$ et $y = (y_i)_{1 \leq i \leq N}$ dans A, on pose $< x, y >= \sum_{i=1}^N x_i y_i \in \mathbb{F}_2$. On rappelle que $\mathbb{C}[A]$ est l'espace hermitien des fonctions de A dans $\mathbb{C}$, dont une base est constituée des fonctions caractéristiques $(\delta_x)_{x \in A}$; on note $\widehat{A}$ le groupe dual de A.

a) Si $(x, y) \in A \times A$, on pose $\chi_y(x) = (-1)^{<x,y>}$. Vérifier que l'application $y \mapsto \chi_y$ définit un isomorphisme de groupes de A sur $\widehat{A}$.

b) On *convient* de noter $\mathcal{F}$ l'endomorphisme de $\mathbb{C}[A]$ défini par $\mathcal{F}(f)(x) = 2^{-N/2} \sum_{y \in A} \chi_x(y) f(y)$, où $f \in \mathbb{C}[A]$ et $x \in A$. Vérifier que $\mathcal{F}$ est une isométrie involutive. Montrer que $\mathrm{tr}(\mathcal{F}) = 0$ et, si $N \geq 2$, $\det(\mathcal{F}) = 1$.

Sur $(\mathbb{F}_2)^{2N+1}$, on considère la loi interne

$$(\alpha, a', a'') \cdot (\beta, b', b'') = (\alpha + \beta + < a', b'' >,\, a' + b',\, a'' + b'')\,,$$

où $\alpha, \beta \in \mathbb{F}_2$, et a', a'', b', b'' appartiennent à A.

c) Montrer que cette loi munit $(\mathbb{F}_2)^{2N+1}$ d'une structure de groupe qu'on notera $\mathcal{H}$. Vérifier que le centre Z de $\mathcal{H}$ a deux éléments, et que $\mathcal{H}/Z \simeq (\mathbb{F}_2)^{2N}$.

d) Décrire les classes de conjugaison de $\mathcal{H}$. Montrer qu'il y en a $2^{2N} + 1$.

Pour $h = (\alpha, a', a'') \in \mathcal{H}$, on définit l'endomorphisme $\rho(h)$ de $\mathbb{C}[A]$ par:

$$\big(\rho(h)(f)\big)(x) = (-1)^{\alpha + <x,a''>} f(x + a')\,,$$

où $f \in \mathbb{C}[A]$ et $x \in A$.

e) Montrer que l'on définit ainsi une représentation $(\mathbb{C}[A], \rho)$ de $\mathcal{H}$; montrer que cette représentation est irréductible.

f) Donner toutes les représentations irréductibles de $\mathcal{H}$ sur $\mathbb{C}$, à isomorphisme près.

VI Théorème de Burnside-Brauer.

Soit G un groupe fini d'ordre ≥ 2. On considère χ le caractère d'une représentation *fidèle* V de G, et ψ un caractère irréductible de G.

a) Soit $n \geq 2$ un entier et soient $(\lambda_i)_{1 \leq i \leq n}$ n complexes de module 1, dont la somme est n. Montrer que chaque λ_i vaut 1.

b) Pour quels $g \in G$ a–t–on $\chi(g) = \dim V$?

c) Pour $n \in \mathbb{N}$, on note $a_n = (\psi, \chi^n)$. Montrer que la série formelle $F(T) = \sum_{n \geq 0} a_n T^n$ est une fraction rationnelle complexe dont on étudiera le nombre et la multiplicité des pôles. En déduire qu'il existe une infinité de a_n non nuls.

d) Plus précisément, déduire de l'écriture de F comme fraction un entier $q \geq 1$ tel que la suite $(a_n)_n$ est récurrente linéaire d'ordre q à partir du rang 1. Par suite l'un au moins des a_n, pour $1 \leq n \leq q$, est non nul.

e) Interpréter ce résultat en terme de représentations. L'hypothèse de fidélité de V est–elle nécessaire?

f) Traiter l'exemple où V est la représentation standard du groupe $\mathfrak{S}_4$: décomposer χ^2,.. jusqu'à l'apparition de chaque caractère irréductible de $\mathfrak{S}_4$.

VII Transformée de Fourier (1)

Soit G un groupe abélien fini. On utilise les notations usuelles: groupe dual $\widehat{G}$, algèbre de groupe $\mathbb{C}[G]$, transformée de Fourier $\mathcal{F}$: $\mathbb{C}[G] \to \mathbb{C}[\widehat{G}]$, voir *Peyré*. Si $f \in \mathbb{C}[G]$, on note $|\mathrm{supp}(f)|$ le nombre d'éléments $g \in G$ tels que $f(g) \neq 0$.

a) Soient f_1 et f_2 dans $\mathbb{C}[G]$. Comparer les produits hermitiens $< f_1, f_2 >$ et $< \mathcal{F}(f_1), \mathcal{F}(f_2) >$.

b) Pour $f \in \mathbb{C}[G]$, expliciter $\mathcal{F} \circ \mathcal{F}(f) \in \mathbb{C}[\widehat{\widehat{G}}]$ en fonction de f, de l'isomorphisme canonique $\Phi : G \to \widehat{\widehat{G}}$, et du passage à l'inverse $i : G \to G$.

VIII TFD et le principe d'incertitude.

On note d'abord $G = \mathbb{Z}/n\mathbb{Z}$ ($n \geq 2$) et on considère f non nulle dans l'algèbre de groupe $\mathbb{C}[G]$. On note $\mathrm{supp}(f) = \{a_1, \ldots, a_s\}$ son support, c.a.d. l'ensemble des $x \in G$ tels que $f(x) \neq 0$.
On regarde la transformée de Fourier (TFD) $\widehat{f} \in \mathbb{C}[\widehat{G}]$ de f comme une fonction sur $\mathbb{Z}/n\mathbb{Z}$, soit $\widehat{f}\colon \bar{l} \mapsto \sum_{k=0}^{n-1} f(\bar{k})\zeta^{kl}$, où $\zeta = e^{-2\pi i/n}$. On définit de même $\mathrm{supp}(\widehat{f})$. On souhaite établir le principe d'incertitude :

$$|\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})| \geq |G| \quad (*)$$

1. Montrer que $\widehat{f}$ n'est pas identiquement nulle sur l'ensemble $\{\bar{0}, \ldots, \overline{s-1}\}$.

2. Dans cette question on veut montrer que plus généralement, pour tout $\bar{r}$ dans $\mathbb{Z}/n\mathbb{Z}$, $\widehat{f}$ n'a pas s zéros consécutifs $\{\bar{r}, \ldots, \overline{s-1+r}\}$.

a) Fixant $\bar{r} \neq \bar{0}$, on note $f_1 \in \mathbb{C}[G]$ la fonction telle que pour tout $\bar{l} \in \mathbb{Z}/n\mathbb{Z}$, $\widehat{f_1}(\bar{l}) = \widehat{f}(\bar{l} + \bar{r})$. Déterminer f_1 et montrer qu'elle a même support que f.

b) Conclure.

3. Déduire de 2. que $(*)$ est vérifiée pour f (*on pourra commencer par le cas où s divise n; ou pourra ensuite noter d le plus petit entier plus grand que n/s*).

4. On prend maintenant pour G un groupe abélien fini quelconque de cardinal n. Notant $\widehat{G}$ son groupe dual, et $f \in \mathbb{C}[G]$, la transformée de Fourier $\widehat{f}$ de f appartient à $\mathbb{C}[\widehat{G}]$. On généralise immédiatement la notion de support à ce contexte (*on peut montrer que $(*)$ est encore vérifiée*).
Soit H un sous–groupe de G et $f \in \mathbb{C}[G]$ la fonction indicatrice de H. Calculer les valeurs de $\widehat{f}$. En déduire $|\mathrm{supp}\,(f)| \times |\mathrm{supp}\,(\widehat{f})|$.

IX Transformée de Fourier discrète et deux applications.

La partie 0. sert aux deux parties A et B, qui sont indépendantes entre elles.
"Rappels": Soit $n \geq 2$ un entier. On pose $\zeta = \exp(2i\pi/n)$. On notera $\bar{l}$ la classe d'un entier l modulo n. La transformée de Fourier discrète associée au groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ peut être définie comme l'endomorphisme $\mathcal{F}$ de l'espace $F_{[n]} =: F$ des fonctions de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$ tel que pour tous $f \in F$ et $\bar{l} \in \mathbb{Z}/n\mathbb{Z}$, $\mathcal{F}f(\bar{l}) = \widehat{f}(\bar{l}) = \sum_{\bar{m} \in \mathbb{Z}/n\mathbb{Z}} f(\bar{m})\zeta^{-lm}$. On rappelle que $\mathcal{F}(f * g) = \mathcal{F}(f) \cdot \mathcal{F}(g)$, pour tous f, g dans F,où $f * g$ est le produit de convolution $\bar{l} \mapsto \sum_{\bar{m} \in \mathbb{Z}/n\mathbb{Z}} f(\bar{m})g(\bar{l} - \bar{m})$ et $\cdot$ désigne le produit usuel des fonctions à valeurs complexes.

0. Soit $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, on note D_a l'endomorphisme de F tel que $D_a(f)(\bar{l}) = f(a\bar{l})$ ($l \in \mathbb{Z}$). Vérifier les propriétés suivantes, pour toute $f \in F_{[n]}$ et tout $l \in \mathbb{Z}$:
(i) $\mathcal{F}\mathcal{F}f(-\bar{l}) = \widehat{\widehat{f}}(-\bar{l}) = nf(\bar{l})$ *(formule d'inversion)*
(ii) $\mathcal{F} \circ D_a = D_{a^{-1}} \circ \mathcal{F} \in \mathrm{End}(F)$. Expliciter le résultat pour $a = -\bar{1}$.

(on pourra se ramener à établir (i) pour les fonctions indicatrices $\delta_{\bar{j}}$, $\bar{j} \in \mathbb{Z}/n\mathbb{Z}$).

A) Loi de réciprocité quadratique.

1. On suppose désormais que $n = p$ est premier impair. On se donne $f \in F_{[p]} = F$ telle que $f(\bar{0}) = 0$ et que f soit multiplicative: $f(xy) = f(x)f(y)$, pour tous $x, y \in \mathbb{Z}/p\mathbb{Z}$. Pour k entier ≥ 2, établir que la puissance de convolution f^{*k} est donnée par

$$f^{*k}(\bar{l}) = \sum_{\substack{m_1+\cdots+m_k=\bar{l} \\ m_i \in (\mathbb{Z}/p\mathbb{Z})^\times}} f(m_1 \cdots m_k) \quad (l \in \mathbb{Z})\,.$$

On rappelle que pour tout entier l premier à p, le symbole de Legendre $\left(\frac{l}{p}\right)$ vaut 1 si $\bar{l}$ est un carré mod p et -1 sinon. Le critère d'Euler affirme que $\left(\frac{l}{p}\right) \equiv l^{(p-1)/2} \bmod p$ (preuve?). Ainsi le symbole de Legendre définit un caractère multiplicatif de $(\mathbb{Z}/p\mathbb{Z})^\times$. On notera encore $\left(\frac{\bar{l}}{p}\right)$ pour $\left(\frac{l}{p}\right)$. On définit l'élément h_p de F par $\bar{0} \mapsto 0$, et $\bar{l} \mapsto \left(\frac{l}{p}\right)$ si $\bar{l} \neq \bar{0}$.

2. a) Montrer que $\widehat{h}_p(-x) = h_p(x)\,\widehat{h}_p(-\bar{1})$ $(x \in \mathbb{Z}/p\mathbb{Z})$. En déduire que $\widehat{h}_p$ et h_p sont proportionnelles.

b) On considère la "somme de Gauss"

$$g = \widehat{h}_p(-\bar{1}) = \sum_{l=1}^{p-1} \left(\frac{l}{p}\right) \zeta^l\,.$$

En calculant la transformée de Fourier de l'expression du a), montrer que $g^2 = (-1)^{(p-1)/2} p$.

c) Soit q un autre nombre premier impair $(q \neq p)$. D'après b), on a $g^{q-1} \in \mathbb{Z}$. Montrer que l'on a

$$g^{q-1} \equiv (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \bmod q\,.$$

3. a) Pour $k \geq 2$ entier, on définit l'élément $a\colon x \mapsto \left[\widehat{h}_p(-x)\right]^k$ de F. Montrer avec 1. que pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $\widehat{a}(x) = p \sum_{\substack{m_1+\cdots+m_k=x \\ m_i \in (\mathbb{Z}/p\mathbb{Z})^\times}} \left(\frac{m_1 \cdots m_k}{p}\right)$.

b) On suppose désormais k impair. Déduire de 2a) que $\widehat{a}(x) = g^{k+1}\, h_p(-x)$ $(x \in \mathbb{Z}/p\mathbb{Z})$.

c) Déduire de a),b) et 2b) que $g^{k-1}(-1)^{(p-1)/2}\, p \left(\frac{-q}{p}\right) = p \sum_{\substack{m_1+\cdots+m_k=\bar{q} \\ m_i \in (\mathbb{Z}/p\mathbb{Z})^\times}} \left(\frac{m_1 \cdots m_k}{p}\right)$.

d) En prenant $k = q$ montrer que

$$g^{q-1} = \left(\frac{q}{p}\right) \sum_{\substack{m_1+\cdots+m_q=\bar{q} \\ m_i\in(\mathbb{Z}/p\mathbb{Z})^\times}} \left(\frac{m_1\cdots m_q}{p}\right).$$

e) Montrer que $\sum_{\substack{m_1+\cdots+m_q=\bar{q} \\ m_i\in(\mathbb{Z}/p\mathbb{Z})^\times}} \left(\frac{m_1\cdots m_q}{p}\right)$ est congru à 1 modulo q.

Indication: On montrera que si les m_i ne sont pas tous égaux, le nombre des q–uplets $(m'_j)_j$ obtenus par permutation circulaire de $(m_1, \ldots, m_q)$ est égal à q.

f) En déduire la *loi de réciprocité quadratique :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

B) Filtrage des polygones.

On identifie le plan $\mathbb{R}^2$ à $\mathbb{C}$. Soit Π un polygone du plan à n côtés, de sommets $z_1, \ldots, z_n$ ($n \geq 3$). On lui associe l'élément z de $F_{[n]} =: F$ tel que $z(\bar{l}) = z_l$, $1 \leq l \leq n$. On définit Π' le polygone dérivé de Π par ses sommets $Dz(\bar{1}), \ldots, Dz(\bar{n})$, où on pose $Dz(\bar{l}) = \frac{1}{2}(z(\bar{l}-\bar{1}) + z(\bar{l}))$. En itérant on définit le $r^{\text{ième}}$ polygone dérivé $\Pi^{(r)}$ de Π ($r \geq 2$) comme $(\Pi^{(r-1)})'$. On note d l'élément $\frac{1}{2}(\delta_{\bar{0}} + \delta_{\bar{1}})$ de F. On souhaite montrer que la suite des polygones $\Pi^{(r)}$ converge vers le centre de gravité de Π, le point d'affixe $\frac{1}{n}\sum_l z_l$.

a) Vérifier que $Dz = d * z$. Exprimer l'élément $D^r z$ de F associé au polygone $\Pi^{(r)}$ en fonction de d, r, z.

b) Soient $f \in F$ et $(f_r)_r$ une suite d'éléments de F. Montrer que $(f_r)_r$ converge vers f dans F si et seulement si la suite $(\widehat{f_r})_r$ converge vers $\widehat{f}$ dans F.

c) Déterminer la transformée de Fourier de d puis de sa puissance de convolution d^{*r}, $r \geq 1$, et montrer que la suite $(\mathcal{F}(d^{*r}))_r$ converge vers $\delta_{\bar{0}}$.

d) En déduire la limite de la suite $(\mathcal{F}(D^r z))_r$ et conclure avec b) que $(D^r z)_r$ tend vers la constante $\frac{1}{n}\sum_l z_l$.

X Sommes de Gauss via la TFD, et loi de réciprocité.

Soit $p \geq 3$ un nombre premier. On note $\zeta = e^{2\pi i/p}$. Partant du corps $\mathbb{F}_p$ on considère son groupe additif $(\mathbb{F}_p, +)$, muni de sa transformée de Fourier $\mathcal{F}_{add}\colon \mathbb{C}[\mathbb{F}_p] \to \mathbb{C}[\widehat{\mathbb{F}_p}]$, et son groupe multiplicatif $\mathbb{F}_p^\times$ (cyclique). On étend tout élément χ de $\widehat{\mathbb{F}_p^\times}$ en un élément $\tilde{\chi}$ de $\mathbb{C}[\mathbb{F}_p]$, en posant $\tilde{\chi}(\bar{0}) = 0$. Pour tout φ dans $\widehat{\mathbb{F}_p}$, on note $G(\chi, \varphi)$ la somme $\sum_{x\in\mathbb{F}_p^\times} \chi(x)\varphi(x) = \mathcal{F}_{add}(\tilde{\chi})(\varphi)$.

On rappelle que les éléments de $\widehat{\mathbb{F}_p}$ sont exactement les $\varphi_k := \varphi_1^k$, où $0 \leq k \leq p-1$ et φ_1 est le morphisme $\bar{l} \mapsto e^{2\pi i l/p} = \zeta^l$. On note encore $\varphi_{\bar{k}} = \varphi_k$ ($\bar{k} \in \mathbb{F}_p$).

1. Pour x, y dans $\mathbb{F}_p$, $y \neq \bar{0}$, montrer que $G(\chi, \varphi_{xy}) = \overline{\chi(y)} G(\chi, \varphi_x)$.

On note que φ_{xy} est le morphisme $u \mapsto \varphi_x(yu)$ et on fait le changement de variable $v = yu$ dans la somme de Gauss.

2. Montrer que $G(\chi, \overline{\varphi}) = \chi(-\bar{1}) G(\chi, \varphi)$ et $G(\overline{\chi}, \varphi) = \chi(-\bar{1}) \overline{G(\chi, \varphi)}$.

La première formule se déduit de 1. en prenant $x = -\bar{1}$ (noter que $\chi(-\bar{1}) = \pm 1$ est réel). La seconde s'en déduit alors en conjuguant.

3. Évaluer $G(\chi, \varphi)$ si φ est le caractère trivial.

On a $G(1,1) = p-1$. Si χ n'est pas trivial, on a $G(\chi, 1) = \sum_{x \in \mathbb{F}_p^\times} \chi(x) = (p-1) < \chi, 1 >= 0$. NB: ce produit hermitien est dans $\mathbb{C}[\mathbb{F}_p^\times]$.

4. On suppose χ et φ non triviaux. La *formule de Plancherel* affirme que

$$< \mathcal{F}_{add}(\tilde{\chi}), \mathcal{F}_{add}(\tilde{\chi}) >= p < \tilde{\chi}, \tilde{\chi} > \ .$$

En déduire que $|G(\chi, \varphi)| = \sqrt{p}$, puis que $G(\chi, \varphi) G(\overline{\chi}, \varphi) = p\chi(-\bar{1})$.

La formule de Plancherel ci-dessus donne: $< G(\chi, \cdot), G(\chi, \cdot) >= p < \tilde{\chi}, \tilde{\chi} >= \sum_{x \in \mathbb{F}_p^\times} |\chi(x)|^2 = p-1$. Fixant $x \in \mathbb{F}_p^\times$, xy décrit $\mathbb{F}_p$ quand y parcourt $\mathbb{F}_p$, ainsi le carré hermitien de gauche vaut $\frac{1}{p} \sum_{y \in \mathbb{F}_p} \overline{G(\chi, \varphi_{xy})} G(\chi, \varphi_{xy})$, c'est-à-dire par 1. et 3. $\frac{1}{p} \sum_{y \in \mathbb{F}_p^\times} |\chi(y)|^2 |G(\chi, \varphi_x)|^2 = \frac{p-1}{p} |G(\chi, \varphi_x)|^2$. On obtient donc $|G(\chi, \varphi)| = \sqrt{p}$. La 2e formule en résulte facilement avec 2.

On prend $\chi = \eta_p$ le symbole de Legendre sur $\mathbb{F}_p^\times$: $\eta_p(x)$ vaut 1 ou -1 selon que x est ou non un carré de $\mathbb{F}_p^\times$. On rappelle le *critère d'Euler:* pour tout $x \in \mathbb{F}_p^\times$, $\overline{\eta_p(x)} = x^{\frac{p-1}{2}}$ dans $\mathbb{F}_p$.

5. Déduire de 4. que $G(\eta_p, \varphi_1)^2 = (\sum_{x \in \mathbb{F}_p^\times} \eta_p(x) \zeta^x)^2 = (-1)^{\frac{p-1}{2}} p$.

En effet η_p est à valeurs réelles (± 1) et par le critère d'Euler $\eta_p(-\bar{1})$ vaut $(-1)^{\frac{p-1}{2}}$.

Dans la suite on note $\tilde{p}$ cet entier, et $G = G(\eta_p, \varphi_1)$. On a donc montré $G^2 = \widetilde{p}$. On se donne maintenant un nombre premier impair q distinct de p. On considère le sous–anneau $A = \mathbb{Z}[\zeta]$ de $\mathbb{C}$, et on note (q) l'idéal de A engendré par l'entier q.

6. Montrer que $(q) \neq A$ (on pourra utiliser une certaine –base de $[\zeta] \supset A$). En déduire la caractéristique de l'anneau $A/(q)$.

7. En déduire que dans le quotient $A/(q)$, G^q a même image que $\eta_p(q) G$.

8. Montrer alors que les entiers $\widetilde{p}^{q-1/2}$ et $\eta_p(q)$ ont même classe dans $\mathbb{Z}/q\mathbb{Z}$.

9. Conclure que $\eta_p(q) \eta_q(p) = (-1)^{\frac{(p-1)(q-1)}{4}}$ (*loi de réciprocité quadratique*).

XI Le cas des groupes simples.

Soit G un groupe fini simple non abélien. On considère une représentation non triviale (V, ρ) de degré n de G.

1.a) Montrer que la représentation V est fidèle.

b) On note $H = \mathrm{Im}\rho$. Montrer que H a un centre trivial et que $H \subset \mathrm{SL}(V)$.

2. On suppose ici que $n = 2$.

a) Montrer que V est une représentation irréductible.

b) Montrer que $\mathrm{SL}(V)$ possède un *unique* élément d'ordre 2, qui est central.

On rappelle que le degré des représentations irréductibles divise l'ordre du groupe.

c) En déduire une contradiction.

3. Que pouvez-vous dire de l'entier n? des entiers m tels que $\mathrm{GL}_m(\mathbb{C})$ possède un sous–groupe isomorphe à G?

- ♢ -