Leçon 110 : Structure et dualité des groupes abéliens finis. Applications.

Développements :

Structure des groupes abéliens finis (avec démo de $|G| = |\widehat{G}|$ par le prolongement des caractères), Transformée de Fourier rapide.

Bibliographie :

Peyré, Rombaldi.

Rapport du jury 2017 :

Pour l'édition 2018 du concours, l'intitulé de cette leçon évolue en Structure et dualité des groupes abéliens finis. Applications. Les commentaires qui suivent prennent en compte cette évolution. Le théorème de structure des groupes abéliens finis a une place de choix dans cette leçon, et la dualité des groupes abéliens finis doit être détaillée. Comme application, la cyclicité du groupe multiplicatif d'un corps fini est tout à fait adaptée. D'ailleurs, des exemples de caractères, additifs, ou multiplicatifs dans le cadre des corps finis, sont les bienvenus. Il est possible de s'intéresser aux sommes de Gauss. Pour aller plus loin, la leçon peut naturellement déboucher sur l'introduction de la transformée de Fourier discrète qui pourra être vue comme son analogue analytique, avec ses formules d'inversion, sa formule de Plancherel , mais dans une version affranchie des problèmes de convergence, qui font le sel des leçons d'Analyse sur ce sujet. Ainsi, la leçon peut mener à introduire la transformée de Fourier rapide sur un groupe abélien dont l'ordre est une puissance de 2 ainsi que des applications à la multiplication d'entiers, de polynômes et éventuellement au décodage de codes via la transformée de Hadamard.

Rapport du jury 2016 :

Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications.

Le théorème de structure des groupes abéliens finis a une place de choix dans cette leçon. On pourra en profiter pour montrer l'utilisation de la dualité dans ce contexte. Comme application, la cyclicité du groupe multiplicatif d'un corps fini est tout à fait adaptée. D'ailleurs, des exemples de caractères, additifs, ou multiplicatifs dans le cadre des corps finis, sont les bienvenus. S'ils le désirent, les candidats peuvent s'intéresser aux sommes de Gauss. L'algèbre du groupe est un objet intéressant, surtout sur le corps des complexes, où elle peut être munie d'une forme hermitienne. On peut l'introduire comme une algèbre de fonctions, munie d'un produit de convolution, mais il est aussi agréable de la voir comme une algèbre qui « prolonge » la mutiplication du groupe. La transformée de Fourier discrète pourra être vue comme son analogue analytique, avec ses formules d'inversion, sa formule de Plancherel, mais dans une version affranchie des problèmes de convergence, incontournables en analyse de Fourier. On pourra y introduire la transformée de Fourier rapide sur un groupe abélien d'ordre une puissance de 2 ainsi que des applications à la multiplication d'entiers, de polynômes et éventuellement au décodage de codes via la transformée de Hadamard.

1 Groupe dual d'un groupe abélien fini

1.1 Caractères d'un groupe fini

Définition 1 (Peyré p2). *Caractère. Dual de G.*

Exemple 2 (Peyré p11). *La signature sur S_n.*

Proposition 3 (Peyré p2). *$\widehat{G}$ est un groupe pour la multiplication des applications.*

Proposition 4 (Peyré p2). *Les caractères sont à valeurs dans le groupe des racines de l'unité .*

Application 5 (Peyré p3). *$\widehat{G}$ est un groupe fini abélien.*

Proposition 6 (Peyré p3). *Tout élément de $\widehat{G}$ est constant sur les classes de conugaison.*

1.2 Dual d'un groupe cyclique

Proposition 7. *Si G est cyclique, alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et à U_n.*

Proposition 8 (Peyré p4). *Eléments du dual d'un groupe cyclique.*

Proposition 9 (Peyré p4). *Le dual d'un groupe cyclique est isomorphe à ce groupe.*

Remarque 10. *L'isomorphisme n'est pas canonique.*

Contre exemple 11 (Peyré p12). *Faux pour un groupe non abélien. $\widehat{S_n} \simeq \mathbb{Z}/2\mathbb{Z}$.*

Application 12 (Peyré p5). $\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$.

Exemple 13 (Peyré p226). *Tables de caractères de $\mathbb{Z}/3\mathbb{Z}$, de $(\mathbb{Z}/5\mathbb{Z})^*$.*

1.3 Quelques isomorphismes structurels (cas d'un groupe abélien quelconque)

Proposition 14 (Peyré p6). *[Romb] Prolongement des caractères.*

Proposition 15 (Peyré p7). $|G| = |\widehat{G}|$.

Contre exemple 16. $\mathbb{Z}/2\mathbb{Z}$ *non isomorphe à* $\widehat{S_n}$.

Proposition 17 (Colmez p250). $G \simeq \widehat{\widehat{G}}$. *Expliciter l'isomorphisme.*

Proposition 18 (Colmez p251). *[Peyré p9]* G *et* $\widehat{G}$ *ont même exposant.*

Application 19 (Colmez p252). *Théorème de structure des groupes abéliens finis.*

Définition 20 (Combes p67). *Suite des invariants.*

Corollaire 21 (Combes p67). *Réciproque de Lagrange et décomposition en puissance de nombres premiers.*

Contre exemple 22 (Romb). A_4 *ne contient pas de sous-groupes d'ordre* 6.

Exemple 23 (Combes p68). $\mathbb{Z}/60\mathbb{Z} * \mathbb{Z}/72\mathbb{Z}$.

Exemple 24. *Le groupe des bitranspositions de* S_4 *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 25 (Peyré p8). $\widehat{G_1} \times \widehat{G_2} \to \widehat{G_1 \times G_2}; (\chi_1, \chi_2) \mapsto ((g_1, g_2) \mapsto \chi - 1(g_1)\chi_1(g_2))$ *est un isomorphisme.*

Corollaire 26 (Peyré p8). $G \simeq \widehat{G}$.

Exemple 27. *Table de* $(\mathbb{Z}/15\mathbb{Z})^*$.

1.4 Caractères d'un corps fini

Proposition 28 (Perrin). *Si* K *est un corps, alors* K^* *est cyclique. (c'est ce que veux le jury ?)*

Exemple 29 (Ortiz). *Exemples de générateurs.*

Définition 30 (Peyré p29). *Caractères additifs et multiplicatifs sur un corps fini.*

Proposition 31 (Peyré p30). *Description de* $\widehat{F_q^*}$.

Corollaire 32 (Peyré p30). $\widehat{F_q^*} \simeq F_q^*$.

Remarque 33. *Description non canonique.*

Proposition 34 (Peyré p30). $F_q \simeq F_p^r$.

Définition 35 (Peyré p30). *Application trace.*

Proposition 36 (Peyré p30). *La trace est une forme* k *linéaire non nulle.*

Définition 37 (Peyré p31). *Caractère canonique.*

Proposition 38 (Peyré p31). *Description des caractères additifs.*

1.5 Orthogonalité

Définition 39 (Peyré p44). *Orthogonal d'un groupe.*

Exemple 40 (Peyré p44). $G^\perp = \{1\}$.

Proposition 41 (Peyré p9). $\sum \chi(g) = 0$ *ou* 1.

Proposition 42 (Peyré p10). *Orthogonalité des caractères.*

Proposition 43 (Peyré p44). $H^\perp \simeq \widehat{G/H}$. *C'est un sous-groupe de cardinal* $|G|/|H|$.

2 Transformée de Fourier sur un groupe abélien fini

2.1 Espace vectoriel des fonctions d'un groupe abélien

Définition 44 (Peyré p3). *Espace* $\mathbb{C}[G]$ *des fonctions sur un groupe.*

Proposition 45 (Peyré p3). *Structure d'espace hermitien.*

Proposition 46 (Peyré p3). *Base de l'espace des fonctions* $\mathbb{C}[G]$.

Corollaire 47. $\dim(\mathbb{C}[G]) = |G|$.

Proposition 48 (Peyré p10). *Les éléments du dual d'un groupe abélien fini forment une base orthonormale de l'espace vectoriel des fonctions de ce groupe.*

2.2 L'algèbre $\mathbb{C}[G]$

Remarque 49 (Peyré p16). *La multiplication confère à* $\mathbb{C}[G]$ *une structure d'algèbre mais elle ne prend pas en compte la structure de* G.

Définition 50 (Peyré p16). *Produit de convolution.*

Remarque 51. *Le produit de convolution correspond à la somme de deux variables aléatoires indépendantes.*

Proposition 52 (Peyré p17). $\mathbb{C}[G]$ *a une structure d'algèbre.*

Proposition 53 (Peyré p17,p18). *Tout morphisme de groupes de* G *dans* $\mathbb{C}^*$ *se prolonge de manière unique en un morphisme d'algèbres de* $\mathbb{C}[G]$ *dans* $\mathbb{C}$. *(Avec la transformée de Fourier ?)*

2.3 Transformée de Fourier sur un groupe abélien

Définition 54 (Peyré p14). *Coefficient de Fourier.*

Exemple 55. $\widehat{\chi_1}(\chi_2) = 0$ *ou* $|G|$.

Définition 56 (Peyré p14). *Transformée de Fourier.*

Proposition 57 (Peyré p15). *Formule d'inversion.*

Proposition 58 (Peyré p15). *c et F sont des isomorphismes d'ev de* $\mathbb{C}[G]$ *sur* $\mathbb{C}[\widehat{G}]$.

Proposition 59 (Peyré p15). *Formule de Plancherel.*

Application 60 (Peyré p23). *Répartition de probabilité.*

Proposition 61 (Peyré p18). *F est un isomorphisme d'algèbres. + Convolution.*

Application 62 (Peyré). *Calcul du déterminant circulant.*

Proposition 63 (Peyré p44). *Formule de Poisson.*

Remarque 64 (Peyré p96). *Lien avec le continu. Définition de* $\widehat{f}$ *pour* $f \in L^1$. *Les seuls morphismes continus de* $(\mathbb{R}, +)$ *dans* $(U, *)$ *sont les* $t \mapsto e^{it\xi}$.

3 Transformée de Fourier discrète

3.1 Transformée de Fourier discrète

Remarque 65. *Utilisée dans la quasi-totalité des algorithmes numériques digitaux.*

Remarque 66. *On se place désormais sur le groupe cyclique* $G = \mathbb{Z}/N\mathbb{Z}$. *On note* $w_N = e^{2i\pi/N}$, *et on rappelle que les caractères de G sont les* χ_k : $n \mapsto e^{2ikn\pi/N} = w_N^{kn}$,$0 \leq k \leq n-1$. *On notera* $\widehat{f}(k) = \widehat{f}(\chi_k)$.

Définition 67 (Peyré p64). *On appelle transformée de Fourier de* $f = (f(n))_{0\leq n\leq N}$ *le vecteur* $(\widehat{f}(n))_{0\leq n\leq N}$. *On définit ainsi la transformée de Fourier comme une application* $\mathbb{C}^N \to \mathbb{C}^N$.

Proposition 68 (Peyré p64). *On a alors* $\widehat{f}(k) = \sum f(n) w_N^{-nk}$.

Proposition 69 (Peyré p65). *Transformée de Fourier inverse, isomorphisme, formule de Plancherel.*

3.2 Transformée de Fourier rapide

Proposition 70 (Peyré p66). *On suppose que* $N = 2p$, $p \in \mathbb{N}^*$. *On a* $\widehat{f}(k) = \sum_{n=0}^{N/2-1} f(2n) w_N^{-2nk} + \sum_{n=0}^{N/2-1} f(2n+1) w_N^{-(2n+1)k}$. *Ainsi, si on définit* $f_p = (f(0), f(2), .., f(N-2))$ *et* $f_i = (f(1), f(3), .., f(N-1))$, *on a : Pour* $k \in \{0, .., N/2-1\}$, $\widehat{f}(k) = \widehat{f}_p(k) + w_N^k \widehat{f}_i(k)$. *Pour* $k \in \{N/2, ..., N-1\}$, $\widehat{f}(k) = \widehat{f}_p(k-N/2) - w_N^{k-N/2} \widehat{f}_i(k-N/2)$. *On a ainsi un algorithme de calcul récursif qui permet le calcul de la transformée de Fourier en* $O(Nlog(N))$ *opérations.*

Remarque 71. *Cet algorithme permet aussi le calcul de la transformée inverse, en remplaçant* w_N^{-1} *par* w_N *et en divisant le résultat final par N.*

3.3 Application : multiplication de polynômes

Proposition 72. *Le calcul de la transformée de Fourier de* $(f(0), .., f(N-1))$ *revient aussi à évaluer le polynôme* $P = f(0) + f(1)X + \Delta\Delta\Delta + f(N-1)X^{N-1}$ *en* $1, w_N^{-1}, .., w_N^{-(N-1)}$. *La transformée de Fourier inverse revient alors à interpoler le polynôme prenant les valeurs* $\widehat{f}(0), .., \widehat{f}(N-1)$ *en* $1, w_N^{-1}, .., w_N^{-(N-1)}$. *Ainsi, si* P, Q *sont deux polynômes de degré N, on peut calculer les coefficients de leur produit PQ via l'algorithme suivant :*

1. *Les évaluer en* $1, w_{2N}^{-1}, .., w_{2N}^{-(2N-1)}$.
2. *Effectuer le produit terme à terme* $PQ(1) = P(1)Q(1), .., PQ(w_{2N}^{-(2N-1)} = P(w_{2N}^{-(2N-1)})Q(w_{2N}^{-(2N-1)})$.
3. *Interpoler le polynôme PQ par transformée de Fourier inverse.*