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

On considère G un groupe abélien fini, de cardinal n.

1 Caractères d'un groupe abélien fini

Définition 1. On appelle caractère de G un morphisme de G dans $\mathbf{C}^*$. L'ensemble des caractères de G est noté $\hat{G}$.

Proposition 2. *Sur $\hat{G}$, on définit la loi de composition interne $\cdot$ par $(\chi \cdot \varphi)(g) = \chi(g)\varphi(g)$. L'ensemble $\hat{G}$ muni de cette loi est un groupe, appelé groupe dual de G.*

Proposition 3. *Les caractères de G sont à valeurs dans le groupe des racines n–ième de l'unité $\mathbf{U}_n$.*

Corollaire 4. *Soient $\chi \in \hat{G}$ et $g \in G$.*

1. $|\chi(g)| = 1$.
2. $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$.

Exemple 5. Si G est cyclique engendré par x, posons ζ une racine n–ième primitive de l'unité. Alors $\hat{G}$ est cyclique, engendré par χ_1 où $\chi_1(x^k) = \zeta^k$. Ainsi, G et $\hat{G}$ sont isomorphes.

Lemme 6 (prolongement de caractères)**.** *Soit H un sous-groupe de G. Tout caractère de H se prolonge en un caractère de G.*

Théorème 7 (structure des groupes abéliens finis)**.** *Il existe des entiers $1 < d_k | \cdots | d_1$ tels que G soit isomorphe au produit $\mathbf{Z}/d_k\mathbf{Z} \times \cdots \times \mathbf{Z}/d_1\mathbf{Z}$. De plus, les entiers $d_k, \ldots, d_1$ sont uniques, on les appelles les invariants de G.*

Corollaire 8. *Les groupes G et $\hat{G}$ sont isomorphes. En particulier, ils ont même cardinal.*

Remarque 9. Ce serait faux si G n'était pas abélien : pour $n \geqslant 3$, les seuls morphismes de $\mathfrak{S}_n$ dans $\mathbf{C}^*$ sont le morphisme trivial et la signature mais $\mathfrak{S}_n$ n'est pas de cardinal 2.

Exemple 10. À isomorphisme près, il n'y a que 6 groupes abéliens d'ordre $600 = 2^3 \times 5^2 \times 3$. Ses invariants possibles sont : (600), (5;120), (2;300), (10;60), (2;2;150) et (2;10;30).

Application 11. Soit K un corps fini, alors K^* est un groupe cyclique.

2 Bidual et orthogonalité des caractères

Définition 12. On appelle groupe bidual de G le groupe dual de $\hat{G}$.

Proposition 13. *Le groupe G est isomorphe à son bidual via l'isomorphisme suivant :*

$$\begin{array}{ccc} G & \longrightarrow & \hat{\hat{G}} \\ g & \longmapsto & (\chi \mapsto \chi(g)) \end{array}$$

Définition 14. On note $\mathbf{C}[G]$ l'ensemble des fonctions de G dans $\mathbf{C}$. On définit sur $\mathbf{C}[G]$ un produit scalaire hermitien :

$$\langle f \mid g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$$

Si $g \in G$, on note $\delta_g \in \mathbf{C}[G]$ la fonction qui vaut 1 sur g et 0 ailleurs.

Lemme 15. *Soit $\chi \in \hat{G}$, alors $\sum_{g \in G} \chi(g)$ vaut $|G|$ si $\chi = \mathbf{1}$ et 0 sinon.*

Théorème 16. *Les éléments de $\hat{G}$ forment une base orthonormée de $\mathbf{C}[G]$.*

Corollaire 17. *Soient $g, h \in G$, alors $\sum_{\chi \in \hat{G}} \chi(g)\overline{\chi(h)}$ vaut $|G|$ si $g = h$ et 0 sinon.*

3 Transformation de Fourier

Définition 18. Soit $f \in \mathbf{C}[G]$ et soit $\chi \in \hat{G}$. On définit le coefficient de Fourier de f par $c_f(\chi) = \langle f \mid \chi \rangle$. On définit alors l'application *transformation de Fourier* $\mathscr{F}$ par :

$$\begin{array}{rccc} \mathscr{F} : & \mathbf{C}[G] & \longrightarrow & \mathbf{C}[\hat{G}] \\ & f & \longmapsto & \hat{f} \end{array}$$

où $\hat{f}$ est définie par $\hat{f}(\chi) = |G| c_f(\overline{\chi}) = \sum_{x \in G} f(x)\chi(x)$.

Théorème 19. *La transformée de Fourier vérifie :*

1. *$\mathscr{F}$ est un isomorphisme d'espaces vectoriels.*
2. *La réciproque est donnée par $f = \sum_{\chi \in \hat{G}} c_f(\chi)\chi = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi^{-1}$.*
3. *$\mathscr{F}$ est (presque) une isométrie : $\langle f \mid g \rangle_G = \frac{1}{|G|} \langle \hat{f} \mid \hat{g} \rangle_{\hat{G}}$.*

Définition 20. Soient $f, g \in \mathbf{C}[G]$, on définit le produit de convolution $f * g$ par :

$$f * g(x) = \sum_{hk=x} f(h)g(k) = \sum_{h \in G} f(h)g(xh^{-1})$$

Proposition 21. *Le produit de convolution est unitaire, commutatif, associatif et bilinéaire. On munit ainsi $\mathbf{C}[G]$ d'une structure d'algèbre.*

Théorème 22. *Soient $f, g \in \mathbf{C}[G]$, alors $\widehat{f * g} = \hat{f} \cdot \hat{g}$ et $c_{f*g} = |G|\, c_f \cdot c_g$.*

Définition 23. Soit H un sous-groupe de G, on appelle orthogonal de H le sous-groupe de $\hat{G}$ défini par $H^\perp = \{\chi \in \hat{G} \mid \forall h \in H,\ \chi(h) = 1\}$.

Lemme 24. *On a un isomorphisme $H^\perp \cong \widehat{G/H}$.*

Théorème 25 (formule de Poisson)**.** *Soit H un sous-groupe de G. Si $f \in \mathbf{C}[G]$, alors :*

$$\forall x \in G,\ \frac{1}{|H|} \sum_{h \in H} f(xh) = \frac{1}{|G|} \sum_{\chi \in H^\perp} \hat{f}(\overline{\chi})\chi(x)$$

Application 26 (transformée de Fourier rapide)**.** Soit $G = G_a = \mathbf{Z}/n\mathbf{Z}$ où $n = 2^a$. Soit $f \in \mathbf{C}[G]$ et soient ω une racine n–ième de l'unité et χ_ω le caractère associé. Notons $\mathscr{F}_a$ la transformation de Fourier sur G_a. On définit f_{pair} et f_{impair} dans $\mathbf{C}[G_{a-1}]$ par $f_{\text{pair}}(p) = f(2p)$ et $f_{\text{impair}}(p) = f(2p+1)$. Alors :

$$\mathscr{F}_a[f](\chi_\omega) = \mathscr{F}_{a-1}[f_{\text{pair}}](\chi_{\omega^2}) + \omega\, \mathscr{F}_{a-1}[f_{\text{impair}}](\chi_{\omega^2})$$

On en déduit une méthode de calcul par récurrence de $\mathscr{F}_a[f]$, de complexité $O(n \log_2 n)$.

4 Dualité sur les corps finis

Soit p un nombre premier et soit $q = p^r$. On considère dans cette section le corps fini $\mathbf{F}_q$. Celui-ci est muni de deux structures de groupe : une structure de groupe additif $(\mathbf{F}_q, +)$ et une structure de groupe multiplicatif $(\mathbf{F}_q^*, \times)$.

Définition 27.

1. Les éléments de $\widehat{\mathbf{F}_q}$ sont appelés les caractères additifs. Ce sont les morphismes $\psi : \mathbf{F}_q \to \mathbf{C}^*$.
2. Les éléments de $\widehat{\mathbf{F}_q^*}$ sont appelés les caractères multiplicatifs. Ce sont les morphismes $\chi : \mathbf{F}_q^* \to \mathbf{C}^*$.

Proposition 28. *Puisque $\mathbf{F}_q^*$ est cyclique, soit ζ un générateur de $\mathbf{F}_q^*$, de sorte que $\mathbf{F}_q^* = \{1, \zeta, \ldots, \zeta^{q-2}\}$. Les $q-1$ caractères multiplicatifs sont donnés par les χ_j :*

$$\forall j \in \{0, \ldots, q-2\},\ \chi_j(\zeta^k) = \mathrm{e}^{\frac{2i\pi}{q-1} jk}$$

Définition 29. Soit $\alpha \in \mathbf{F}_q$, on appelle trace de α sur $\mathbf{F}_p$ le nombre $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{r-1}}$.

Proposition 30. *La trace est une forme $\mathbf{F}_p$–linéaire non nulle à valeurs dans $\mathbf{F}_p$.*

Définition 31. On définit le caractère additif canonique ψ_1 par $\psi_1(x) = e^{\frac{2i\pi}{p}\mathrm{Tr}(x)}$.

Théorème 32. *Soit $a \in \mathbf{F}_q$, l'application ψ_a définie par $\psi_a(x) = \psi_1(ax)$ est un caractère additif. Réciproquement, tout caractère additif est de cette forme. L'application $a \mapsto \psi_a$ est un isomorphisme entre $\mathbf{F}_q$ et $\widehat{\mathbf{F}_q}$.*

Définition 33. Soient $\chi \in \widehat{\mathbf{F}_q^*}$ et $\psi \in \widehat{\mathbf{F}_q}$. On définit la somme de Gauss $G(\chi,\psi)$ par :

$$G(\chi,\psi) = \sum_{x\in\mathbf{F}_q^*} \chi(x)\psi(x)$$

Proposition 34. *Soit $\chi \in \widehat{\mathbf{F}_q^*}$, alors $\chi = \frac{1}{q}\sum_{\psi\in\widehat{F_q}} G(\chi,\overline{\psi})\psi$.*

Proposition 35. *Soient $\chi \in \widehat{\mathbf{F}_q^*}$ et $\psi \in \widehat{\mathbf{F}_q}$.*

1. *Si $a,b \in \mathbf{F}_q$, alors $G(\chi,\psi_{ab}) = \overline{\chi(a)}\,G(\chi,\psi_b)$.*
2. *$G(\chi,\overline{\psi}) = \chi(-1)\,G(\chi,\psi)$.*
3. *$G(\overline{\chi},\psi) = \chi(-1)\,\overline{G(\chi,\psi)}$.*

Proposition 36. *Soient $\chi \in \widehat{\mathbf{F}_q^*}$ et $\psi \in \widehat{\mathbf{F}_q}$.*

$$G(\chi,\psi) = \begin{cases} q-1 & \text{si } \chi = \chi_0 \text{ et } \psi = \psi_0 \\ -1 & \text{si } \chi = \chi_0 \text{ et } \psi \neq \psi_0 \\ 0 & \text{si } \chi \neq \chi_0 \text{ et } \psi = \psi_0 \end{cases}$$

Dans les autres cas, $|G(\chi,\psi)|^2 = q$. De plus, si $\chi \neq \chi_0$ et $\psi \neq \psi_0$, alors $G(\chi,\psi)G(\overline{\chi},\psi) = q\,\chi(-1)$.

Proposition 37. *Soit $\chi \in \widehat{\mathbf{F}_q^*}$ et soit m son ordre, c'est-à-dire le plus petit entier $k \in \mathbf{N}^*$ tel que $\chi^k = \chi_0$. Alors $\chi(-1) = -1$ ssi m est pair et $\frac{q-1}{m}$ est impair.*

Remarque 38. Les sommes de Gauss et leurs propriétés sont des ingrédients essentiels d'une preuve de la loi de réciprocité quadratique.

Développements

1. Prolongement de caractères et structure des groupes abéliens finis. **[7]**
2. Formule de Poisson discrète. **[25]**

Références

— CALDERO et GERMONI, *Nouvelles histoires hédonistes de groupes de géométries, tome II*.
— COMBES, *Algèbre et géométrie*.
— PEYRÉ, *L'algèbre discrète de la transformée de Fourier*.