P. Maurer

ENS Rennes

Recasages : *104, 107, 120.*

Référence : Pierre Colmez, Elements d'analyse et d'algèbre.

Classification des groupes abéliens finis

par la théorie des représentations

On rappelle d'abord quelques définition et résultats classiques de la théorie des représentations qui seront utiles pour la suite. On se reportera au livre de Colmez pour plus de détails.

On note $\mathrm{Irr}(G)$ l'ensemble des représentations irréductibles d'un groupe fini G.

Lemme 1. *Soit G un groupe abélien et (V,ρ) une représentation irréductible de G. Alors* $\dim(V)=1$.

Démonstration. Soit $g\in G$ et λ une valeur propre de $\rho(g)$. Alors l'espace propre $E_\lambda\subset V$ est stable par G : en effet, pour $x\in E_\lambda$ et $h\in G$, on a $g\cdot(h\cdot x)=(g\cdot h)\cdot x=h\cdot(g\cdot x)=h\cdot\lambda x=\lambda h\cdot x$. Comme V est irréductible et que E_λ n'est pas nul, on en déduit que $V=E_\lambda$.[1]

Cette construction étant valable pour tout $g\in G$, on a donc :

$$\forall g\in G\quad \exists\lambda_g\in G\quad \forall x\in V\quad g\cdot x=\lambda_g x.$$

Aussi, pour $x_0\in V$ non nul, l'espace $\mathrm{Vect}(x_0)$ est stable par G. Comme V est simple, on en déduit que $V=\mathrm{Vect}(x_0)$. □

Définition 2.

On appelle caractère d'une représentation (V,ρ) de G l'application $\chi_V: G\to\mathbb{C}$ définie par $\chi_V(g):=\mathrm{Tr}(\rho(g))$.

Si V est de dimension 1, $\mathrm{GL}(V)$ est isomorphe à $\mathbb{C}^*$, donc la représentation V s'identifie à un morphisme de groupes $\chi: G\to\mathbb{C}^*$. On appelle caractère linéaire de G un tel morphisme, et on note $\hat{G}$ l'ensemble des caractères linéaires de G.

Proposition 3. *Si V est une représentation de dimension 1 de G et χ le caractère linéaire associé, on a $\chi_V=\chi$: le caractère du caractère linéaire est le caractère linéaire lui-même.*

Muni du produit $(\chi_1\chi_2)(g):=\chi_1(g)\,\chi_2(g)$, l'ensemble $\hat{G}$ des caractères linéaires de G est un groupe commutatif. On l'appelle le groupe dual de G.

Remarque 4. Dans le cas où G est abélien, on déduit du lemme 1 que $\mathrm{Irr}(G)$ coïncide avec $\hat{G}$.

Théorème 5. *(Frobenius)*

Les caractères irréductibles forment une base des fonctions centrales, i.e des fonctions $\phi: G\to\mathbb{C}$ qui sont constantes sur les classes de conjugaison de G.

1. C'est le principe de la démonstration du lemme de Schur, qu'on aurait pu utiliser directement.

Corollaire 6. *Le nombre de représentations irréductibles de G est égal au nombre $|\mathrm{Conj}(G)|$ de classes de conjugaison dans G. En particulier, il est fini.*

Corollaire 7. *Si G est abélien, toute fonction $\phi: G \to \mathbb{C}$ est centrale, et l'ensemble des caractères linéaires $\hat{G}$ forme une base orthonormale des fonctions de G sur $\mathbb{C}$.*

Définition 8. *Soit G un groupe qui agit sur lui même à gauche. On définit la représentation régulière V_G de G comme l'espace vectoriel V_G de dimension $|G|$, de base $(e_h)_{h\in G}$, muni de l'action linéaire de G donnée par $g \cdot e_h = e_{g\cdot h}$.*

Remarque 9. Dans la base $(e_h)_{h\in G}$, la matrice de $g \in G$ est une matrice de permutation, dont le terme diagonal vaut 1 si et seulement si $gh = h$, et zéro sinon.

En particulier, on en déduit que $\chi_{V_G}(1) = |G|$ et $\chi_{V_G}(g) = 0$ si $g \neq 1$.

Proposition 10. *(formule de Burnside)*

Si W est une représentation irréductible de G, alors W apparaît dans la représentation régulière avec la multiplicité $\dim W$, et on a

$$\sum_{W \in \mathrm{Irr}(G)} (\dim W)^2 = |G|.$$

On rappelle également un lemme sur les groupes abéliens finis.

Proposition 11. *Soit G un groupe abélien fini.*

1. *Si $x \in G$ est d'ordre a et si $y \in G$ est d'ordre b, et si $a \wedge b = 1$, alors xy est d'ordre ab.*
2. *Si $a, b \in \mathbb{N}^*$ et si G contient des éléments d'ordre a et b, alors il contient un élément d'ordre $\mathrm{ppcm}(a, b)$.*
3. *Soit N le maximum des ordres des éléments de G. Alors on a $x^N = 1$ pour tout $x \in G$. On dit que N est l'exposant du groupe G.*

Le développement à proprement parler commence ici.

Lemme 12. *Soit G un groupe abélien fini. Alors G est isomorphe à $\hat{\hat{G}}$.*

Démonstration.

On définit l'application $\iota: G \to \hat{\hat{G}}$ par $i: \begin{cases} G & \to & \hat{\hat{G}} \\ g & \mapsto & \iota(x): \begin{cases} \hat{G} & \to & \mathbb{C}^* \\ \chi & \mapsto & \chi(g) \end{cases} \end{cases}$. On va montrer que ι est un isomorphisme de groupes.

- Vérifions que ι définit un morphisme de groupes. Pour $g, h \in G$, et $\chi \in \hat{G}$, puisque χ est un morphisme de groupes, on a

$$\begin{aligned} \iota(gh)(\chi) &= \chi(gh) \\ &= \chi(g)\,\chi(h) \\ &= \iota(g)\,(\chi) \cdot \iota(h)(\chi). \end{aligned}$$

  Ceci étant vrai pour tout $\chi \in \hat{G}$, on en déduit que $\iota(gh) = \iota(g)\,\iota(h)$.

- Vérifions que ι est injective. On se donne $g, h \in G$ tels que $\iota(g) = \iota(h)$.

  On définit les fonctions $\phi_g : G \to \mathbb{C}$ et $\phi_h : G \to \mathbb{C}$ par $\phi_g(x) = \delta_{x,g}$ et $\phi_h(x) = \delta_{x,h}$.

  Pour montrer que $g = h$, il suffit de vérifier que $\phi_g = \phi_h$. D'après le corollaire 7, on peut décomposer ϕ_g et ϕ_h sur la base orthonormale des caractères linéaires de G. On en déduit que

$$\phi_g = \sum_{\chi \in \hat{G}} \langle \phi_g, \chi \rangle \, \chi \quad \text{et} \quad \phi_h = \sum_{\chi \in \hat{G}} \langle \phi_h, \chi \rangle \, \chi,$$

  où

$$\langle \phi_g, \chi \rangle = \frac{1}{|G|} \sum_{x \in G} \overline{\phi_g(x)} \, \chi(x) = \frac{1}{|G|} \chi(g) \text{ et } \langle \phi_h, \chi \rangle = \frac{1}{|G|} \sum_{x \in G} \overline{\phi_h(x)} \, \chi(x) = \frac{1}{|G|} \chi(h).$$

  Puisque $\iota(g) = \iota(h)$, pour tout $\chi \in \hat{G}$ on a $\chi(g) = \chi(h)$, ce qui conclut que $\phi_g = \phi_h$.

- Finalement, la formule de Burnside (proposition 10) appliquée à G donne

$$\sum_{\chi \in \hat{G}} 1 = |G| \quad \text{donc} \quad |\hat{G}| = |G|,$$

  et on en déduit de même que $|\hat{G}| = \left|\hat{\hat{G}}\right|$, donc on a $|G| = \left|\hat{\hat{G}}\right|$. L'application ι est donc injective entre deux ensembles finis de même cardinal, ce qui prouve qu'elle est bijective. □

Lemme 13. *Soit G un groupe abélien fini. Alors G et $\hat{G}$ ont le même exposant.*

Démonstration. Soit H un groupe abélien fini. On note $N(H)$ sont exposant. Pour $\chi \in \hat{H}$, on a

$$\forall x \in H \quad \chi^{N(H)}(x) = \chi(x)^{N(H)} = \chi(x^{N(H)}) = \chi(1) = 1.$$

Ainsi, $N(\hat{H})$ divise $N(H)$, et en particulier, on a $N(\hat{H}) \leq N(H)$. En appliquant ce résultat à $H = G$ et à $H = \hat{G}$, on en déduit que $N(\hat{G}) \leq N(G)$ et $N\left(\hat{\hat{G}}\right) \leq N(\hat{G})$. Finalement, l'isomorphisme $G \simeq \hat{\hat{G}}$ donné par le lemme 12 permet de conclure que $N(G) = N(\hat{G})$. □

Théorème 14. *(Théorème de structure des groupes abéliens finis, existence)*

Soit G un groupe abélien fini. Alors il existe $r \in \mathbb{N}$ et des entiers $N_1, \ldots, N_r$, où N_1 est l'exposant de G et qui vérifient $N_{i+1} | N_i$ pour tout $i \leq r-1$, et qui sont tels que

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

Démonstration.

On raisonne par récurrence forte sur $n = |G|$. Pour $n = 1$, $G = \{e\} \simeq \prod_{i=1}^{1} \mathbb{Z}/\mathbb{Z}$, donc le résultat est vérifié (ou bien, G est aussi le produit vide).

On se donne un entier $n \in \mathbb{N}$ et on suppose le résultat vrai pour tout groupe H d'ordre k avec $k < n$. Soit G un groupe d'ordre n.

- Notons $N = N_1$ l'exposant de G. Pour tout $\chi \in \hat{G}$ et $g \in G$, on a

$$\chi^N(g) = \chi(g^N) = 1.$$

On en déduit que $\chi(g) \in \mathbb{U}_N$. Comme $\hat{G}$ est aussi d'exposant N (d'après le lemme 13), il existe un élément $\chi_1 \in \hat{G}$ d'ordre N, et le sous-groupe $\chi_1(G) \subset \mathbb{U}_N$ admet lui-même un élément d'ordre N. En effet, l'ordre des éléments de $\chi_1(G)$ divise N d'après ce qui précède, et s'il existe $K < N$ tel que $\forall g \in G\ \chi_1(g)^K = 1$, alors $\chi_1^K = 1$ avec $K < N$, ce qui contredit que l'ordre de χ_1 est N.

Ainsi, $\chi_1(G)$ est un sous-groupe de $\mathbb{U}_N$ qui contient un élément d'ordre N donc on a $\chi_1(G) = \mathbb{U}_N$. En particulier, il existe $x_1 \in G$ tel que $\chi_1(x_1) = e^{\frac{2i\pi}{N}}$.

- Notons p l'ordre de x_1. Par définition de N, on sait que p divise N. Par ailleurs, on a

$$\chi_1(x_1^p) = e^{\frac{2i\pi p}{N}} = 1.$$

On en déduit que $\dfrac{2i\pi p}{N} \in \mathbb{Z}$, donc N divise p. Ainsi, x_1 est d'ordre N dans G.

- On pose $H_1 = \langle x_1 \rangle$. Alors χ_1 induit un morphisme surjectif $\alpha : H_1 \to \mathbb{U}_N$. Comme $|H_1| = |\mathbb{U}_N| = N$, on en déduit que α est un isomorphisme. On va démontrer que

$$G \simeq H_1 \times \operatorname{Ker} \chi_1.$$[2]

Pour $x \in G$, on pose $a = \alpha^{-1}(\chi_1(x))$ et $b = (\alpha^{-1}(\chi_1(x)))^{-1} x$. On a alors $x = ab$, et $a \in H_1$. Par ailleurs,

$$\begin{aligned}
\chi_1(b) &= \chi_1((\alpha^{-1}(\chi_1(x)))^{-1})\, \chi_1(x) \\
&= \alpha((\alpha^{-1}(\chi_1(x)))^{-1})\, \chi_1(x) \\
&= (\alpha(\alpha^{-1}(\chi_1(x))))^{-1}\, \chi_1(x) \\
&= \chi_1(x)^{-1}\, \chi_1(x) \\
&= 1.
\end{aligned}$$

On en déduit que $b \in \operatorname{Ker} \chi_1$. Ainsi, on a $G = H_1 \operatorname{Ker} \chi_1$. Par ailleurs, comme $\alpha = \chi_{1|H_1}$, χ_1 est injectif sur H_1 et donc $H_1 \cap \operatorname{Ker} \chi_1 = \{e_G\}$. On en déduit le résultat.

- Puisque $\operatorname{Ker} \chi_1$ est un sous-groupe strict de G, on a $|\operatorname{Ker} \chi_1| < N$. En appliquant l'hypothèse de récurrence, on en déduit qu'il existe $r \in \mathbb{N}$ et des entiers $N_2, \dots, N_r$ tels que :

$$N_r | N_{r-1} | \dots | N_2 \quad \text{et} \quad \operatorname{Ker} \chi_1 \simeq \prod_{i=2}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

On a donc $G \simeq \displaystyle\prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$, et de plus, comme tout élément de g est d'ordre divisant N_1, on en déduit en particulier que $N_2 | N_1$ (par exemple en considérant $x_0 = (1, x, 1, \dots, 1)$ dans $G = (\mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \times \dots \times \mathbb{Z}/N_r\mathbb{Z})$, on a $x_0^{N_2} = 1$ donc $N_2 | N_1$).

Ceci conclut la récurrence.

□

2. On rappelle que si G, G_1 et G_2 sont des groupes, on a $G \simeq G_1 \times G_2$ si et seulement si il existe H_1, H_2 des sous-groupes de G tels que $G = H_1 H_2$ et $H_1 \cap H_2 = \{e_G\}$. Ici, comme H_1 et $\operatorname{Ker} \chi_1$ sont des sous-groupes de G, il suffit de montrer que $G = H_1 \operatorname{Ker} \chi_1$ et que $H_1 \cap \operatorname{Ker} \chi_1 = \{e_G\}$. Attention à ne pas confondre les groupes $H_1 H_2$ et $G_1 \times G_2$.