Théorème de structure des groupes abéliens finis

Bruno Winckler

Prérequis :
– théorie des groupes, groupes-quotients.

Table des matières

1 Caractère d'un groupe fini

Soit G un groupe abélien fini, de cardinal n. Je vais introduire la notion de caractère. Ils sont surtout utiles pour trouver des équivalents de la fonction exponentielle dès qu'on veut faire de l'analyse de Fourier ailleurs que sur $\mathbb{R}$. Mais notre dessein est tout autre ici : dans le cas des groupes finis, les caractères sont simples à étudier, et vont ici me fournir une nouvelle preuve du théorème de structure des groupes abéliens finis.

Définition 1 (Caractère) *On appelle caractère de G un morphisme de G dans $(\mathbb{C}^*, \cdot)$.*

En fait, comme le groupe est fini, on a $\chi(g)^n = \chi(g^n) = \chi(1) = 1$ pour tout $g \in G$, donc χ est à valeurs dans le sous-groupe des racines complexes de l'unité, ici noté $\mathbb{U}$. On note $\hat{G}$ l'ensemble des caractères de G.

Remarque. Pour tout groupe G, on a un caractère trivial : $\chi_0 : g \mapsto 1$.

Remarque. Étant donnés deux caractères de G, notés χ et χ', on en déduit un nouveau caractère, noté $\chi \cdot \chi'$ (ou $\chi\chi'$), défini par la formule $\chi \cdot \chi'(g) = \chi(g)\chi'(g)$. Si χ est un caractère, alors $\frac{1}{\chi(g)} = \overline{\chi(g)}$ pour tout g car χ est de module 1, et $\bar{\chi}$ est clairement un caractère, donc χ a un inverse dans $\hat{G}$ pour la loi $\cdot$. Alors, $(\hat{G}, \cdot)$ est un groupe, d'élément neutre χ_0.

Exemple. Supposons que $G = \mathbb{Z}/n\mathbb{Z}$. Comme 1 engendre G, il suffit de déterminer l'image de 1 par un caractère pour le connaître entièrement. Tout choix d'une racine n-ième de l'unité pour $\chi(1)$ détermine clairement un caractère, défini par $\chi(\bar{k}) = \exp(2ik\pi/n)$, donc $\hat{G} \simeq \mu_n$, où μ_n est le sous-groupe de $\mathbb{U}$ des racines n-ièmes de l'unité, or $\mu_n \simeq \mathbb{Z}/n\mathbb{Z} = G$. Donc $\hat{G} \simeq G$.

Exemple. Si G et H sont deux groupes abéliens, alors $\widehat{G \times H} \simeq \hat{G} \times \hat{H}$, *Via* l'application $\chi \mapsto (\chi(\cdot, 1), \chi(1, \cdot))$, de réciproque $(\chi, \eta) \mapsto ((g, h) \mapsto (\chi(g), \eta(h)))$. Alors, si G est un produit de groupes cycliques, par l'exemple précédent on a $\hat{G} \simeq G$. C'est, en fait, toujours le cas.

Remarque. Considérons un exemple non abélien. Si $G = \mathfrak{S}_5$, et si χ est un morphisme de G dans $\mathbb{C}^*$ alors, comme le noyau de χ est distingué, on a $\ker(\chi) \in \{1, \mathfrak{A}_5, \mathfrak{S}_5\}$. Le premier cas est impossible, car le groupe dérivé de G, c'est-à-dire $\mathfrak{A}_5$, est dans $\ker(\chi)$ (ou encore : si tel était le cas, χ serait injectif, donc G s'identifierait à un sous-groupe de $\mathbb{C}^*$ qui est abélien, mais G n'est pas abélien). Si $\ker(\chi) = \mathfrak{S}_5$, alors χ est le morphisme trivial. Enfin, dans le cas $\ker(\chi) = \mathfrak{A}_5$, alors χ se factorise *via* $G/\ker(\chi) \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mu_2 \subseteq \mathbb{U}$. Avoir χ non trivial impose $\chi(\tau \mod \mathfrak{A}_5) = -1$ pour $\tau \notin \mathfrak{A}_5$. Bref, G a deux caractères, et $\hat{G} \simeq \mathbb{Z}/2\mathbb{Z}$ (et d'ailleurs, $\widehat{\mathfrak{A}_4} = \{1\}$) : on est bien loin des exemples précédents ! En outre, on ne peut plus avoir d'isomorphisme $\hat{\hat{G}} \simeq G$ canonique, donné par $\chi \mapsto (g \mapsto \chi(g))$, qui est pourtant à la base de l'analyse de Fourier sur les groupes. Ceci peut justifier que le cas non abélien soit exclu. Le lecteur en exercice traitera le cas $G = \mathfrak{A}_4$, où on peut avoir $\ker(\chi) = (\mathbb{Z}/2\mathbb{Z})^2$ (le sous-groupe des double-transpositions) et alors $\mathfrak{A}_4/(\mathbb{Z}/2\mathbb{Z})^2 \simeq \mu_3$.

On pourrait dire beaucoup de choses intéressantes sur les caractères, mais ce qui m'intéresse pour la suite est le théorème de prolongement des caractères :

Proposition 2 (Prolongement des caractères) *Si $H \subseteq G$ est un sous-groupe de G, alors tout caractère de H se prolonge en un caractère de G. En d'autres mots, l'application $\hat{G} \to \hat{H}$, qui à χ associe sa restriction à H est surjective.*

Remarque. On peut même prouver que tout caractère de H se prolonge en exactement $\mathrm{card}(G/H)$ caractères de G. Comme $\hat{G} \to \hat{H}$ est un morphisme de groupes surjectif d'après la proposition, et de noyau $H^\perp = \{\chi \in \hat{G}; \chi(H) = 1\}$, toutes les fibres ont même cardinal, et ce cardinal égale $\mathrm{card}(H^\perp) = \mathrm{card}(G/H)$ grâce à $\hat{G}/H^\perp \simeq \hat{H}$ et $\mathrm{card}(\hat{G}) = \mathrm{card}(G)$, même si on ne l'a pas encore prouvé. En fait, on a aussi $\widehat{G/H} \simeq H^\perp$, *via* $\chi \mapsto \chi \circ (G \to G/H, g \mapsto gH)$.

Preuve de la proposition. On raisonne par récurrence sur l'indice r de H dans G. Si $r = \mathrm{card}(G/H) = 1$, il n'y a rien à dire car $G = H$. Supposons alors $r > 1$. Comme $H \neq G$, il existe un élément $g \in G \setminus H$. Notons K le sous-groupe engendré par H et g, et définissons un prolongement d'un caractère χ de H à ce sous-groupe K : comme G/H est de cardinal r, on a $g^r = 1 \mod H$, et $g^r \in H$.

Soit k le plus petit entier tel que $g^k \in H$ (c'est l'ordre de g dans G/H). Alors, $\chi(g^k)$ est bien défini, égal à ω, disons. Posons $\chi'(hg^l) = \chi(h)\omega^{l/k}$, où $\omega^{1/k}$ désigne abusivement une racine k-ième de ω (il y a k choix possibles). On vérifie que χ' est bien un caractère de H : si $h, h' \in H$ et $g^l, g^m \in \langle g \rangle$, alors

$$\chi'(hg^l \cdot h'g^m) = \chi'(hh' \cdot g^{l+m}) = \chi(hh')\omega^{(l+m)/k} = \chi(h)\omega^{l/k}\chi(h')\omega^{m/k} = \chi'(hg^l)\chi'(h'g^m),$$

et on peut vérifier que χ' ne dépend pas de la représentation sous la forme hg^l d'un élément de H', et c'est là l'intérêt de prendre k minimal. Donc on a bien prolongé χ en un caractère χ' de H'. Comme l'indice de H' dans G est strictement inférieur à celui de H dans G (on a $H \subsetneq H'$), l'hypothèse de récurrence permet de prolonger χ' en un caractère χ'' de G. Ce caractère χ'' est bien un prolongement de H. □

Remarque. Ceci prouve que $\mathrm{card}(\hat{G}) = \mathrm{card}(G)$. En effet, le morphisme de restriction de la proposition précédente est surjectif, de noyau $H^\perp \simeq \widehat{G/H}$, donc induit un isomorphisme $\hat{G}/(\widehat{G/H}) \simeq \hat{H}$. On a donc $\mathrm{card}(\hat{G}) = \mathrm{card}(\widehat{G/H})\mathrm{card}(\hat{H})$, ce qui nous permet de conclure par récurrence : si $n = 1$, il n'y a rien à dire, et si $n > 1$, soit H un sous-groupe cyclique de G. Comme $\hat{H} \simeq H$, on a $\mathrm{card}(\hat{H}) = \mathrm{card}(H)$, et par récurrence sur n on a $\mathrm{card}(\widehat{G/H}) = \mathrm{card}(G/H)$, donc $\mathrm{card}(\hat{G}) = \mathrm{card}(G/H)\mathrm{card}(H) = \mathrm{card}(G)$.

2 Théorème de structure des groupes abéliens finis

Le théorème de structure est le suivant ; il dit, en gros, que tout groupe abélien fini s'écrit comme produit de groupes cycliques $\mathbb{Z}/n\mathbb{Z}$. Avec une condition sur les cardinaux, on obtient d'ailleurs l'unicité, que je ne démontre pas ici.

Théorème 3 (Théorème de Kronecker) *Soit G un groupe abélien fini. Il existe une unique suite d'entiers positifs $d_n \geq d_{n-1} \geq \cdots \geq d_1 > 1$ tels que, d'une part, $d_i | d_{i+1}$ pour tout $1 \leq i < n$, et d'autre part :*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

On remarque que d_n doit être le plus grand ordre des éléments du groupe G. L'idée de la preuve est de considérer un élément d'ordre maximal x, en espérant pouvoir écrire $G \simeq \langle x \rangle \times G/\langle x \rangle$ pour ensuite conclure par récurrence. Cet isomorphisme n'a rien d'évident, il est en général faux de dire que $G \simeq H \times G/H$ pour H un sous-groupe de G : il suffit de prendre $G = \mathfrak{S}_3$ et $H = \mathfrak{A}_3$ pour s'en convaincre : comme $\mathfrak{S}_3/\mathfrak{A}_3 \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{A}_3$ est cyclique, engendré par un 3-cycle, le produit direct de ces deux groupes est abélien, ce qui n'est pas le cas de $\mathfrak{S}_3$. On peut aussi prendre un exemple abélien avec $G = \mathbb{Z}/4\mathbb{Z}$ et $H = 2\mathbb{Z}/4\mathbb{Z}$.

Preuve du théorème. Supposons G de cardinal au moins 2. Soit d_n l'ordre maximal d'un élément de G, et x un élément d'ordre d_n ; on a $\langle x \rangle \simeq \mathbb{Z}/d_n\mathbb{Z} \simeq \mu_{d_n}$. Soit χ l'isomorphisme entre $\langle x \rangle$ et

$\mu_{d_n} \subseteq \mathbb{U}$ (qui définit donc bien un caractère de $\langle x \rangle$), et $\eta : \mu_{d_n} \to \langle x \rangle$ sa bijection réciproque. Il existe un prolongement $\chi' : G \to \mathbb{U}$ de χ à tout G, par le théorème de prolongement des caractères. Comme l'ordre de x est supposé maximal, l'ordre de tout élément de G divise l'ordre de x (exercice), et on a $\chi(g^{d_n}) = \chi(g)^{d_n} = 1$ pour tout $g \in G$, donc χ' est en fait à valeurs dans μ_{d_n}. Alors, on a un isomorphisme entre G et $\langle x \rangle \times G/\langle x \rangle$ fourni par $g \mapsto (\eta \circ \chi'(g), g \mod \langle x \rangle)$. En effet, un élément du noyau de ce morphisme est, en particulier, un élément de $\langle x \rangle$, or $\eta \circ \chi'$ égale l'identité sur $\langle x \rangle$. Comme $\eta \circ \chi'(g) = g = 1$, le noyau est trivial, et le morphisme est injectif. Comme $\mathrm{card}(G) = \mathrm{card}(\langle x \rangle)\mathrm{card}(G/\langle x \rangle)$, le morphisme est en fait bijectif.

Alors, $G/\langle x \rangle$ est de cardinal strictement plus petit que G. Par récurrence, on obtient $G/\langle x \rangle$ comme un produit de groupes cycliques $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{n-1}\mathbb{Z}$ avec $d_1|d_2|\cdots|d_{n-1}$, puis G est isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{n-1}\mathbb{Z} \times \mathbb{Z}/d_n\mathbb{Z}$. Il est alors facile d'exhiber un élément d'ordre d_{n-1} dans G (en prenant un n-uplet avec 0 partout, sauf à la place $n-1$ où on met un 1), et comme l'ordre maximal d'un élément du groupe est divisible par l'ordre de tout élément du groupe, on en déduit que d_{n-1} divise d_n. □

Remarque. On a, en fait, utilisé le lemme suivant, valable pour un groupe fini :

Lemme 4 *Soit H un sous-groupe distingué de G, et $r : G \to H$ un morphisme tel que $r_{|H} = id_H$. Alors G est isomorphe à $H \times G/H$ via $g \mapsto (r(g), g \mod H)$.*

Preuve. En effet, le noyau de ce morphisme est $\ker(r) \cap \ker(g \mapsto g \mod H) = \ker(r) \cap H$. Mais si $g \in H$ vérifie $r(g) = 1$, alors $r(g) = g = 1$, donc $\ker(r) \cap H = \{1\}$. Le morphisme est donc injectif, et on conclut grâce aux cardinaux. □

Remarque. Grâce à ce théorème de structure, on trouve que $\hat{G} \simeq G$ pour tout groupe abélien fini.