Lemme de prolongement des caractères irréductibles et théorème de structure des groupes abéliens finis

Ref : Peyré
Recasages : 102, 107

Lemme. *Soient G un groupe abélien fini et H un sous-groupe de G. Pour tout caractère $\chi \in \widehat{H}$, il existe un caractère $\tilde{\chi} \in \widehat{G}$ tel que $\tilde{\chi}|_H = \chi$.*

Démonstration : on procède par récurrence sur $[G:H]$. Si H est un sous-groupe de G tel que $[G:H] = 1$, alors $H = G$ et le résultat est acquis. Soit K un sous-groupe de G tel que $[G:K] \geqslant 2$. Supposons que le résultat est vérifié par tous les sous-groupes H tels que $[G:H] < [G:K]$, et montrons qu'il l'est encore par le sous-groupe K. Soit $x \in G$ tel que $x \notin K$. Notons $H = \langle x, K \rangle$. Alors $[G:H] < [G:K]$: grâce à l'hypothèse de récurrence, il suffit alors de prolonger les caractères de K à H.

À cet effet, donnons-nous $\chi \in \widehat{H}$. Notons encore r le plus petit entier $i \geqslant 1$ tel que $x^i \in K$; cet entier existe car G est fini. Comme $x^r \in K$, $\chi(x^r)$ est bien défini. Soit $\zeta \in \mathbb{U}$ une racine r-ème du nombre complexe $\chi(x^r) \in \mathbb{U}$.

Tout élément $z \in H$ s'écrit $z = sx^k$ avec $s \in K$ et $0 \leqslant k < r$. Une telle écriture est de plus unique : en effet, si $sx^k = tx^\ell$, avec $s, t \in K$ et $0 \leqslant k \leqslant \ell < r$, alors $x^{\ell-k} = ts^{-1} \in K$, donc $\ell - k = 0$ par choix de r ; ainsi, $k = \ell$, puis $s = t$.

Cela permet de définir sans ambiguïté l'application

$$\begin{array}{rccc} \tilde{\chi}\colon & H & \longrightarrow & \mathbb{U} \\ & sx^k & \longmapsto & \chi(s)\zeta^k \end{array} .$$

Montrons que cette application est un morphisme de groupes. Comme elle coïncide avec χ sur K, ce sera le prolongement cherché. ~~Soient sx^k et tx^ℓ deux éléments de H écrits comme ci-dessus. Par commutativité de G, on a $\tilde{\chi}(sx^k tx^\ell) = \tilde{\chi}(stx^{k+\ell})$. Deux cas se présentent alors : si $k + \ell < r$, on a directement $\tilde{\chi}(stx^{k+\ell}) = \chi(st)\zeta^{k+\ell} = \chi(s)\zeta^k\chi(t)\zeta^\ell = \tilde{\chi}(sx^k)\tilde{\chi}(tx^\ell)$. Si $k + \ell \geqslant r$, on a tout de même $k + \ell < 2r$ puisque k et ℓ sont strictement plus petits que r. Donc $k + \ell - r < r$, et $\tilde{\chi}(stx^{k+\ell}) = \tilde{\chi}(sx^r tx^{k+\ell-r}) = \chi(stx^r)\zeta^{k+\ell-r}$ puisque $x^r \in K$. Comme $\zeta^r = \chi(x^r)$, il vient $\tilde{\chi}(stx^{k+\ell}) = \chi(st)\zeta^{k+\ell}$, et on peut conclure comme précédemment.~~

Il s'ensuit que $\tilde{\chi}$ est bien un morphisme de groupes, ce qui achève la preuve du lemme. ■

Théorème. *Soient G un groupe abélien fini non trivial. Il existe un entier $r \geqslant 1$ et des entiers $n_1, \ldots, n_r \geqslant 2$ tels que $n_r | n_{r-1} | \ldots | n_1$ et $G \cong \mathbb{U}_{n_1} \times \ldots \times \mathbb{U}_{n_r}$.*

Démonstration : on procède à nouveau par récurrence, cette fois-ci sur $|G|$. Si $|G| = 2$, alors $G \cong \mathbb{U}_2$ et le résultat est acquis. Soit G un groupe tel que $|G| \geqslant 3$. Supposons que le résultat est vrai pour tous le groupes dont le cardinal est strictement plus petit que $|G|$, et montrons qu'il l'est encore par G.

À cet effet, notons n_1 l'exposant de G. Comme G est abélien, il possède un élément x d'ordre n_1. Le groupe $\langle x \rangle$ étant cyclique d'ordre n_1, il existe un isomorphisme $\chi\colon \langle x \rangle \to \mathbb{U}_{n_1}$. Alors $\chi \in \widehat{\langle x \rangle}$; d'après le lemme, il existe donc $\tilde{\chi} \in \widehat{G}$ prolongeant χ.

Tout élément de G est d'ordre divisant n_1, donc $\tilde{\chi}$ est en fait à valeurs dans $\mathbb{U}_{n_1}$. Cela permet de définir sans ambiguïté l'application

$$\begin{array}{rccc} \alpha\colon & G & \longrightarrow & \langle x \rangle \times (G/\langle x \rangle) \\ & s & \longmapsto & (\chi^{-1} \circ \tilde{\chi}(s), \overline{s}) \end{array} ,$$

qui est un morphisme de groupe comme composée de morphismes de groupes. De plus, si $s \in \operatorname{Ker} \alpha$, on a alors $s \in \langle x \rangle$, donc $\chi^{-1} \circ \tilde{\chi}(s) = s$, ce qui entraîne $s = 1$. Ainsi, α est injectif. Comme G est $\langle x \rangle \times (G/\langle x \rangle)$ ont même cardinal, α est en fait un isomorphisme.

Or $|G/\langle x \rangle| < |G|$, donc par hypothèse de récurrence, il existe des entiers $n_2, \ldots, n_r$ vérifiant $n_r | n_{r-1} | \ldots | n_2$ et $G/\langle x \rangle \cong \mathbb{U}_{n_2} \times \ldots \times \mathbb{U}_{n_r}$. On a donc $G \cong \mathbb{U}_{n_1} \times \ldots \times \mathbb{U}_{n_r}$; il ne reste plus qu'à montrer que $n_2 | n_1$. L'élément $(0, \xi, 0, \ldots, 0) \in \mathbb{U}_{n_1} \times \ldots \times \mathbb{U}_{n_r}$ est d'ordre n_2, donc G possède un élément d'ordre n_2, ce qui entraîne que $n_2 | n_1$ puisque tous les élément de G sont d'ordre divisant n_1. ■

$x^{k+\ell} = x^{rq+s'}$ Donc :

$\tilde{\chi}(stx^{k+\ell}) = \tilde{\chi}(st(x^r)^q)\zeta^{s'} = \tilde{\chi}(s)\tilde{\chi}(t)\tilde{\chi}(x^r)^q\zeta^{s'}$
$= \tilde{\chi}(s)\tilde{\chi}(t)\zeta^{rq+s'}$
$= \tilde{\chi}(s)\tilde{\chi}(t)\zeta^{k+\ell}$
$= \tilde{\chi}(sx^k)\tilde{\chi}(tx^\ell)$

car $\zeta^r = \tilde{\chi}(x^r)$