

Développement : Structure des groupes abéliens finis

Leçons : 102, 103, 104, 110, 120.

Soit G un groupe abélien fini.

Lemme. *Soit H un sous-groupe de G . Tout caractère de H se prolonge en un caractère de G .*

Démonstration. Soit $\chi \in \widehat{H}$. Par récurrence sur $[G : H]$.

Si $[G : H] = 1$, alors $H = G$ et le résultat est vrai.

Si $[G : H] > 1$, alors il existe $x \in G, x \notin H$. Soit $K = \langle H, x \rangle$. Prolongeons χ à K .

Étape 1 : Expression des éléments de K .

Soit $p = \min\{q \in \mathbb{N}^*, x^q \in H\}$ (existe et vaut au plus $\text{ord}(x)$). Alors tout élément $z \in K$ s'écrit de façon unique $z = yx^k, y \in H, k \in \llbracket 0, p-1 \rrbracket$. En effet, si $yx^k = y'x^{k'}$ avec $k \leq k'$, alors $x^{k'-k} = yy'^{-1} \in H$ et $k' - k \leq p - 1$, donc $k = k'$ et $y = y'$.

Étape 2 : Analyse.

Soit $\tilde{\chi} \in \widehat{K}$ qui prolonge χ . Soit $\zeta = \tilde{\chi}(x)$. Alors $\zeta^p = \tilde{\chi}(x^p) = \chi(x^p)$ donc ζ est une racine p -ème de $\chi(x^p)$. De plus, si $yx^k \in K, \tilde{\chi}(yx^k) = \chi(y)\zeta^k$.

Étape 3 : Synthèse.

Soit ζ une racine p -ème de $\chi(x^p)$. On définit $\tilde{\chi}$ par $\tilde{\chi}(yx^k) = \chi(y)\zeta^k$. Par unicité de l'écriture des éléments de K , cette application est bien définie et prolonge χ . Montrons que c'est un morphisme. Soient $h = yx^k, h' = y'x^{k'} \in K$.

— Si $k + k' \leq p - 1$, alors $\tilde{\chi}(hh') = \tilde{\chi}(yy'x^{k+k'}) = \chi(yy')\zeta^{k+k'} = \chi(y)\zeta^k\chi(y')\zeta^{k'} = \tilde{\chi}(h)\tilde{\chi}(h')$.

— Si $p \leq k + k' \leq 2p - 1$, alors

$$\tilde{\chi}(hh') = \tilde{\chi}(yy'x^p x^{k'+k-p}) = \chi(yy'x^p)\zeta^{k+k'-p} = \chi(y)\chi(y')\chi(x^p)\zeta^{k+k'-p} = \chi(y)\zeta^k\chi(y')\zeta^{k'} = \tilde{\chi}(h)\tilde{\chi}(h').$$

Ainsi $\tilde{\chi}$ prolonge χ à K , et $[G : K] < [G : H]$ donc par hypothèse de récurrence, on peut prolonger $\tilde{\chi}$ à G entier. \square

Lemme. *Si H sous-groupe distingué de G et $\varphi : G \rightarrow H$ morphisme de groupes tel que $\varphi|_H = \text{Id}_H$, alors $\psi : G \rightarrow H \times G/H, x \mapsto (\varphi(x), xH)$ est un isomorphisme de groupes.*

Démonstration. Soit $x \in \ker(\psi)$. Alors $\varphi(x) = e_G$ et $xH = H$ donc $x \in \ker(\varphi) \cap H$.

Mais comme $x \in H, x = \varphi(x) = e_G$, donc ψ injective. On conclut par cardinalité. \square

Théorème. *Il existe une (unique) suite d'entiers d_1, \dots, d_n telle que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$ et $\forall i, d_i | d_{i+1}$.*

Démonstration. Supposons $|G| \geq 2$.

Soient $d_n = \max\{\text{ord}(x), x \in G\}$, et $x \in G$ tel que $d_n = \text{ord}(x)$. On a $\langle x \rangle \simeq \mathbb{Z}/d_n\mathbb{Z} \simeq \mathbb{U}_{d_n}$, soit $\chi : \langle x \rangle \rightarrow \mathbb{U}_{d_n} \subset \mathbb{C}^*$ qui réalise l'isomorphisme, soit $\mu : \mathbb{U}_{d_n} \rightarrow \langle x \rangle$ la réciproque. Par le lemme de prolongement, il existe $\tilde{\chi} : G \rightarrow \mathbb{C}^*$ qui prolonge χ . Comme $\text{ord}(x)$ est maximal, pour tout $g \in G, \text{ord}(g)$ divise $\text{ord}(x) = d_n$ (sinon, xg est d'ordre $\text{ord}(x) \frac{\text{ord}(g)}{\text{ord}(x) \wedge \text{ord}(g)}$ strictement supérieur à x). Ainsi, pour tout $g \in G, \tilde{\chi}(g)^{d_n} = \tilde{\chi}(g^{d_n}) = 1$, donc $\tilde{\chi}$ est à

valeurs dans \mathbb{U}_{d_n} . Alors $\mu \circ \tilde{\chi}$ induit l'identité sur $\langle x \rangle$ donc d'après le lemme, $\psi \begin{cases} G & \rightarrow \langle x \rangle \times G/\langle x \rangle \\ g & \mapsto (\mu \circ \tilde{\chi}(g), g\langle x \rangle) \end{cases}$ est un isomorphisme. Par récurrence, $G/\langle x \rangle$ est isomorphe à une suite $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_{n-1}\mathbb{Z}$ avec $d_1 | \dots | d_{n-1}$. Alors G isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$, et en considérant un élément d'ordre d_{n-1} (par exemple $(0, \dots, 0, 1, 0)$), d_{n-1} divise l'ordre de x soit d_n . \square

Références

G. Peyré, L'ALGÈBRE DISCRÈTE DE LA TRANSFORMÉE DE FOURIER, Ellipses, p. 10.

Notes personnelles

Un joli développement qui en plus passe bien dans la leçon 110. Attention, référence seulement pour le premier lemme, le reste est à apprendre par cœur. La preuve de l'unicité peut se trouver dans Combes ou dans Algèbre L3 chez Pearson.