

Théorème de Structure des groupes abéliens finis

(rédigé par *Émilie Tezenas*)

Leçons : 104 ; 108 ; 110

Références : COLMEZ, *Éléments d'analyse et d'algèbre (et de théorie des nombres)*

Théorème 1 (Théorème de structure des groupes abéliens finis). Soit G un groupe abélien fini. Alors il existe un entier r et des entiers n_1, n_2, \dots, n_r tels que $n_r | \dots | n_2 | n_1$ et

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$$

L'idée est d'exhiber un sous-groupe de G d'ordre n_1 et un morphisme faisant intervenir ce sous-groupe. La notion d'exposant d'un groupe abélien fini va permettre de préciser cette idée.

Définition 1. On appelle exposant de G le maximum des ordres des éléments de G . On le note dorénavant m .

Lemme 1. Pour tout $g \in G$, $o(g) | m$. En particulier, l'exposant d'un groupe abélien fini est le ppcm des ordres de ses éléments.

Démonstration du lemme. Soit $x \in G$ tel que $o(x) = m$. Soit $y \in G$ différent de x . On note l son ordre. Le but est de montrer que $\text{ppcm}(l, m) = m$. Ainsi, on aura montré que $l | m$.

Notons $\text{ppcm}(l, m) = p_1^{\alpha_1} \dots p_q^{\alpha_q}$ la décomposition en facteurs premiers du ppcm.

Alors par construction de cette décomposition en utilisant les valuations de chaque nombre premier, pour tout $i \in \{1, q\}$, deux cas peuvent se produire :

- soit $p_i^{\alpha_i} | m$, et alors $x^{m/p_i^{\alpha_i}}$ est d'ordre $p_i^{\alpha_i}$ (à vérifier, mais pas difficile)
- soit $p_i^{\alpha_i} | l$, et alors $y^{l/p_i^{\alpha_i}}$ est d'ordre $p_i^{\alpha_i}$ (à vérifier, mais pas difficile)

Dans tous les cas, on trouve un élément $z_i \in G$ d'ordre $p_i^{\alpha_i}$.

On note $z = z_1 \dots z_q$. Alors z est d'ordre $\text{ppcm}(l, m)$ (Par récurrence, le cas à deux éléments repose sur la commutativité des éléments, et le fait que leurs ordres sont premiers entre eux).

Or, par définition de m , $o(z) \leq m$. Mais par définition du ppcm, $\text{ppcm}(l, m) \geq m$. Donc $\text{ppcm}(l, m) = m$ et $l | m$. \square

Démonstration du théorème de structure. Soit G un groupe abélien fini. On note toujours m son exposant.

Soit $x \in G$ d'ordre m (existe, m est le maximum des ordres). On note $H = \langle x \rangle$. Alors $H \simeq \mathbb{Z}/m\mathbb{Z}$.

On pose

$$\begin{aligned} \chi : H &\longrightarrow \mathbb{C}^* \\ z = x^k &\longmapsto e^{\frac{2i\pi}{m}k} \end{aligned}$$

χ est un caractère de H . C'est même un isomorphisme entre H et \mathbb{U}_m .

D'après le théorème de prolongement des caractères que l'on prouvera après, χ peut être prolongé en un caractère sur G , que l'on note χ' .

On a vu que tout ordre d'un élément de G divise l'exposant de G . Donc pour tout $g \in G$, $\chi'(g)^m = \chi'(g^m) = \chi'(e) = 1$. Donc χ' est à valeurs dans \mathbb{U}_m . χ' est même surjectif, puisque c'est un prolongement de χ qui était lui-même surjectif.

On obtient donc un morphisme de groupe surjectif entre G et \mathbb{U}_m .

On note $N = \text{Ker}(\chi')$. Le but est maintenant de montrer que

$$G \simeq H \times N$$

Posons

$$\begin{aligned} f : H \times N &\longrightarrow G \\ (h, n) &\longmapsto hn \end{aligned}$$

Alors :

- f est injective : si $hn = h'n'$, alors $h^{-1}h' = n^{-1}n' \in H \cap N$. Or, χ est injectif sur H , donc $H \cap N = H \cap \text{Ker}(\chi) = \{e\}$. D'où $h^{-1}h' = e$ i.e. $h = h'$ et donc $n = n'$.
- f est surjective : $|G| = |\text{Im}(\chi)| |\text{Ker}(\chi)| = |H| |N|$. Donc en combinant l'injectivité et l'égalité des cardinaux, on a la surjectivité.
- Enfin, f est un morphisme : $f((h, n)(h', n')) = f((hh', nn')) = hh'nn' = hnh'n'$ car G est abélien.

Donc on a bien un isomorphisme

$$G \simeq H \times N \simeq \mathbb{Z}/m\mathbb{Z} \times N$$

On itère ensuite le raisonnement sur N pour obtenir les autres invariants. Les relations de divisibilité proviennent du fait que m est l'exposant de G , et que donc tout ordre d'un élément de G divise m . \square

Théorème 2 (de prolongement des caractères). Soit G un groupe abélien fini et H un sous-groupe de G . Alors tout caractère linéaire de H peut être prolongé en un caractère linéaire de G .

Démonstration du lemme. On raisonne par récurrence sur l'indice de H .

Initialisation : $[G : H] = 1$ Cela signifie que $G = H$. Donc un caractère de H est déjà un caractère de G .

Hérédité : $[G : H] > 1$ Soit alors $x \in G \setminus H$. On note $K = \langle H, x \rangle$. Soit χ un caractère linéaire de H .

On a $[G : K] < [G : H]$ donc l'hypothèse de récurrence s'applique à K . Il reste donc à prolonger χ à K .

On note $n = \min\{k \in \mathbb{N} \text{ tel que } x^k \in H\}$. Ce \min existe bien puisque l'ensemble $\{k \in \mathbb{N} \text{ tel que } x^k \in H\}$ est inclus dans \mathbb{N} et est non vide : G est un groupe fini, donc x admet un ordre, et $x^{o(x)} = e \in H$.

Alors pour tout $z \in K$, il existe un unique couple $(y, l) \in H \times \llbracket 0, n-1 \rrbracket$ tel que $z = y.x^l$.

En effet, l'existence est immédiate vu la définition de K , celle de n , et le caractère abélien de G .

Supposons qu'il existe $(y, l), (\tilde{y}, \tilde{l})$ tels que $yx^l = \tilde{y}.x^{\tilde{l}}$. On peut supposer que $l < \tilde{l}$. Alors $\tilde{y}^{-1}.y = x^{\tilde{l}-l} \in H$. Or, $\tilde{l} - l < n$. Par minimalité de n , on a donc $\tilde{l} = l$, et ainsi $y = \tilde{y}$. L'unicité est donc bien démontrée.

Revenons au prolongement de χ . On procède par analyse synthèse.

◆ Analyse : Supposons χ prolongé en un caractère de K , que l'on note $\tilde{\chi}$. Alors on a

- d'une part $\tilde{\chi}(x^n) = \chi(x^n)$, car $x^n \in H$
- d'autre part, $\tilde{\chi}(x^n) = \tilde{\chi}(x)^n$ car $\tilde{\chi}$ est un morphisme.

Finalement, $\tilde{\chi}(x)$ est une racine $n^{\text{ème}}$ de $\chi(x^n)$.

◆ Synthèse : Soit ζ une racine $n^{\text{ème}}$ de $\chi(x^n)$. Posons

$$\begin{aligned} \tilde{\chi} : K &\longrightarrow \mathbb{C}^* \\ z = y.x^l &\longmapsto \chi(y)\zeta^l \end{aligned}$$

- $\tilde{\chi}$ est bien à valeurs dans \mathbb{C}^* , car χ l'est.
- $\tilde{\chi}$ prolonge χ , vu l'unicité d'écriture des éléments de K démontrée plus tôt.
- Il reste à vérifier que $\tilde{\chi}$ est bien un morphisme.

Soit $z = y.x^l$ et $z' = y'.x^{l'}$. Alors

$$\tilde{\chi}(z.z') = \tilde{\chi}(y.y'.x^{l+l'})$$

Deux cas peuvent se produire :

- Si $l+l' < n$: Alors $\tilde{\chi}(z.z') = \chi(y.y')\zeta^{l+l'} = \chi(y)\chi(y')\zeta^l\zeta^{l'} = \tilde{\chi}(z)\tilde{\chi}(z')$.
- Si $l+l' \geq n$: On ne peut pas appliquer directement la définition de $\tilde{\chi}$. On écrit alors $l+l' = n+k$, avec $k < n$ et ainsi :

$$\begin{aligned} \tilde{\chi}(z.z') &= \tilde{\chi}(y.y'.x^{n+k}) \\ &= \tilde{\chi}(y.y'.x^n.x^k) \\ &= \chi(y.y'.x^n).\zeta^k \\ &= \chi(y)\chi(y')\chi(x^n)\zeta^{l+l'-n} \quad \text{Car } x^n \in H \\ &= \chi(y)\chi(y')\chi(x^n)\zeta^{-n}\zeta^l\zeta^{l'} \end{aligned}$$

Or, on a choisit ζ comme une racine $n^{\text{ème}}$ de $\chi(x^n)$. Donc finalement on a bien :

$$\tilde{\chi}(z.z') = \chi(y)\chi(y')\zeta^l\zeta^{l'} = \tilde{\chi}(z)\tilde{\chi}(z')$$

Donc $\tilde{\chi}$ est un morphisme, donc un caractère de K , qui prolonge χ . Le théorème s'en déduit par la récurrence annoncée : on prolonge $\tilde{\chi}$ à G .

□

Remarques :

L'isomorphisme de la fin existe dans un cadre plus général : il faut que H et N soient distingués dans G , et que leur intersection soit réduite au neutre.