Deux façons de décomposer un groupe abélien fini

18 octobre 2023

Soit G un groupe abélien fini, noté additivement. Nous allons définir deux types de «décomposition» de G :

- ⋄ Une *décomposition du premier type* est un isomorphisme

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$$

  où les d_i sont des entiers supérieurs ou égaux à 2 tels que $d_1|d_2|\ldots|d_r$. Nous dirons que $(d_1, \ldots, d_r)$ est la *famille d'entiers associée* à une telle décomposition.
- ⋄ Une *décomposition du second type* est un isomorphisme

$$G \simeq \prod_{j \in J} \mathbb{Z}/p_j^{n_j}\mathbb{Z}$$

  où J est un ensemble fini d'indices, où les p_j sont des nombres premiers et où les n_j des entiers strictement positifs (on ne demande pas que les p_j soient deux à deux distincts). Nous dirons que $(p_j^{n_j})_{j \in J}$ est la *famille d'entiers associée* à une telle décomposition.

(A) Donnons-nous une décomposition du premier type D de G, de famille d'entiers associée $(d_1, \ldots, d_r)$. Pour tout i écrivons $d_i = \prod_k p_{ik}^{n_{ik}}$ où les p_{ik} sont des nombres premiers deux à deux distincts et les d_{ik} des entiers > 0. Le lemme chinois fournit pour tout i un isomorphisme entre $\mathbb{Z}/d_i\mathbb{Z}$ et $\prod_k \mathbb{Z}/p_{ik}^{n_{ik}}\mathbb{Z}$. En combinant la décomposition du premier type intialement donnée avec ces isomorphismes on obtient un isomorphisme $G \simeq \prod_{ik} \mathbb{Z}/p_{ik}^{n_{ik}}\mathbb{Z}$, qui est une décomposition du second type D' de G. Notons que la famille d'entiers associée à D' ne dépend à permutation près que de la famille d'entiers $(d_1, \ldots, d_r)$ associée à D (et pas de l'isomorphisme précis qui définit D, qui n'a joué aucun rôle).

(B) Réciproquement, supposons donnée une décomposition du second type Δ de G, de famille d'entiers associés $(p_j^{n_j})_{j \in J}$, et expliquons comment en déduire une décomposition du premier type Δ' de G. On procède récursivement sur le cardinal de J.

- ⋄ Si J est vide alors G est trivial, et on prend pour Δ' la décomposition triviale (dont la famille d'entiers associée est la famille vide).
- ⋄ Supposons que J est non vide. Soit $\mathscr{P}$ l'ensemble des nombres premiers apparaissant dans la famille des p_j, et pour chaque $p \in \mathscr{P}$, soit e_p le plus grand des exposants n_j où j est tel que $p_j = p$. Posons $d = \prod_{p \in \mathscr{P}} p^{n_p}$. Pour chaque p dans $\mathscr{P}$ il y a au moins un indice j tel que $p_j = p$ et $n_j = e_p$, et si j' est un autre indice tel que $p_{j'} = p$ alors $n_{j'} \leqslant e_p$.

La décomposition initiale $G \simeq \prod_j \mathbb{Z}/p_j^{n_j}\mathbb{Z}$ peut ainsi se récrire

$$G \simeq \prod_{j\in J'} \mathbb{Z}/p_j^{n_j} \times \prod_{p\in\mathscr{P}} \mathbb{Z}/p^{e_p}\mathbb{Z} \simeq \prod_{j\in J'} \mathbb{Z}/p_j^{n_j} \times \mathbb{Z}/d\mathbb{Z}$$

où J' est un sous-ensemble strict de J et où $d = \prod_{p\in\mathscr{P}} p^{e_p}$ (on utilise le lemme chinois pour le second isomorphisme.) Pour tout $j \in J'$, il résulte de notre construction que $p_j \in \mathscr{P}$ et que l'exposant n_j est majoré par e_{p_j}. Par raisonnement récursif on peut appliquer l'algorithme au groupe $\prod_{j\in J'} \mathbb{Z}/p_j^{n_j}$, et l'on obtient ainsi un isomorphisme

$$\prod_{j\in J'} \mathbb{Z}/p_j^{n_j} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z}$$

où les d_i sont supérieurs ou égaux à 2 et où $d_1|d_2|\ldots|d_s$. Si $s \neq 0$ l'entier d_s est obtenu par une construction analogue à celle de l'entier d ci-dessus, et donc est de la forme $\prod_{p\in\mathscr{P}} p^{f_p}$ où f_p est un entier compris entre 0 et e_p, et il divise en particulier d. Si l'on pose $r = s+1$ et $d_r = d$ on obtient alors un isomorphisme $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$ qui est par ce qui précède une décomposition Δ' du premier type de G. Notons que la famille d'entiers $(d_1, \ldots, d_r)$ associée à Δ' ne dépend que de la famille d'entiers $(p_j^{n_j})$ associée à Δ (et pas de l'isomorphisme précis qui définit Δ, qui n'a joué aucun rôle).

Nous vous laissons vous convaincre que ces deux constructions sont réciproques l'une de l'autre dans le sens suivant.

Si l'on part d'une décomposition du premier type D de G, qu'on applique l'algorithme décrit en (A) à D pour obtenir une décomposition du second type D' puis qu'on applique l'algorithme décrit en (B) à D' pour obtenir une nouvelle décomposition du premier type D'' de G, alors D et D'' ont même famille d'entiers associée.

Et si l'on part d'une décomposition du second type Δ de G, qu'on applique l'algorithme décrit en (B) à Δ pour obtenir une décomposition du premier type Δ' puis qu'on applique l'algorithme décrit en (A) à Δ' pour obtenir une nouvelle décomposition du second type (Δ'') de G, alors Δ et Δ'' ont même famille d'entiers associée à permutation près (notez qu'on ne peut pas espérer mieux puisque dans une décomposition du second type on peut toujours permuter les $p_j^{n_j}$, alors que dans une décomposition du premier type la condition de divisibilité empêche de permuter les d_i).

Exemple de mise en œuvre de l'algorithme (A). Soit G le groupe

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}.$$

Comme $6 = 2 \cdot 4$, que $12 = 2^2 \cdot 3$, que $24 = 2^3 \cdot 3$ et que $72 = 2^3 \cdot 3^2$, le lemme chinois appliqué à chacun des facteurs fournit un isomorphisme

$$G \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$$

qui est une décomposition du second type de G, dont on préfèrera la version permutée qui regroupe les termes nombre premier par nombre premier

$$G \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}.$$

Exemple de mise en œuvre de l'algorithme (B). Soit G le groupe

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}.$$

On commence par prendre pour chaque nombre premier apparaissant dans la décomposition ci-dessus un facteur où il apparaît avec exposant maximal et on «fusionne» les termes ainsi choisis grâce au lemme chinois, puis on recommence. (À chaque étape, nous avons coloré les termes sélectionnés).

$$\begin{aligned}
G &\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \\
&\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \\
&\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3600\mathbb{Z} \\
&\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3600\mathbb{Z} \\
&\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3600\mathbb{Z} \\
&\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/300\mathbb{Z} \times \mathbb{Z}/3600\mathbb{Z} \\
&\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/300\mathbb{Z} \times \mathbb{Z}/3600\mathbb{Z} \\
&\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/300\mathbb{Z} \times \mathbb{Z}/3600\mathbb{Z},
\end{aligned}$$

ce qui fournit une décomposition du premier type de G.

Existence et unicité des décompositions Soit G un groupe abélien fini. Le théorème 3.9.4 du poly assure que G possède une décomposition du premier type, et que deux décompositions du premier type de G ont même famille d'entiers associée.

Nous allons maintenant démontrer que G possède une décomposition du second type, et que deux décompositions du second type de G ont même famille d'entiers associées à permutation près.

Existence. On a rappelé que G possède une décomposition du premier type. En lui appliquant l'algorithme (A) vu plus haut, on obtient une décomposition du second type de G.

Unicité. Soient Δ_1 et Δ_2 deux décompositions du second type de G. L'algorithme (B) vu plus haut leur associe deux décompositions du premier type Δ_1' et Δ_2' de G, qui par le résultat de cours qu'on vient de rappeler, ont même famille d'entiers associée. En appliquant l'algorithme (A) à Δ_1' et Δ_2' on obtient deux décompositions du second type Δ_1'' et Δ_2'' de G qui ont même famille d'entiers associée à permutation près (parce que la famille d'entiers associés à Δ_i'' ne dépend à permutation près que de celle associée à Δ_i') ; mais on sait par ailleurs que la famille d'entiers associe à Δ_i'' coïncide à permutation près avec celle associée à Δ_i, les algorithmes (A) et (B) étant réciproques l'un de l'autre ; ceci achève la démonstration.