Université Paris 7 – Denis Diderot
U.F.R. de Mathématiques
D.E.U.G. Mathématiques : MT 282

8 novembre 1994

B. Keller

La classification des sommes de groupes $\mathbf{Z}/n\mathbf{Z}$

Exemple. Considérons les groupes abéliens

$$\begin{aligned} A &= \mathbf{Z}/48 \oplus \mathbf{Z}/900 \oplus \mathbf{Z}/30 \\ B &= \mathbf{Z}/1200 \oplus \mathbf{Z}/60 \oplus \mathbf{Z}/18. \end{aligned}$$

Ici, le symbôle $\mathbf{Z}/n$ signifie $\mathbf{Z}/n\mathbf{Z}$, et nous écrivons $\oplus$ au lieu de $\times$ pour faire apparaître que nous ne regardons que la structure de groupe abélien (et non pas celle d'anneau).

Question : est-ce que A est isomorphe à B ?

Pour répondre, nous allons remplacer A et B par des groupes isomorphes obtenus en appliquant le lemme chinois autant de fois que possible. Ainsi, le lemme chinois nous donne des isomorphismes

$$\begin{aligned} \mathbf{Z}/48 &\cong \mathbf{Z}/3 \oplus \mathbf{Z}/16 \\ \mathbf{Z}/900 &\cong \mathbf{Z}/9 \oplus \mathbf{Z}/4 \oplus \mathbf{Z}/25 \\ \mathbf{Z}/30 &\cong \mathbf{Z}/2 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/5. \end{aligned}$$

En substituant dans l'expression pour A nous trouvons

$$A \cong (\mathbf{Z}/3 \oplus \mathbf{Z}/16) \oplus (\mathbf{Z}/9 \oplus \mathbf{Z}/4 \oplus \mathbf{Z}/25) \oplus (\mathbf{Z}/2 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/5).$$

Puisque l'opération $\oplus$ est 'commutative à isomorphisme près', nous pouvons réarranger les termes pour obtenir

$$A \cong (\mathbf{Z}/16 \oplus \mathbf{Z}/4 \oplus \mathbf{Z}/2) \oplus (\mathbf{Z}/9 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/3) \oplus (\mathbf{Z}/25 \oplus \mathbf{Z}/5).$$

De même, les décompositions $1200 = 16 \times 25 \times 3$, $60 = 3 \times 4 \times 5$, $18 = 2 \times 9$, montrent que nous avons

$$\begin{aligned} B &\cong (\mathbf{Z}/16 \oplus \mathbf{Z}/25 \oplus \mathbf{Z}/3) \oplus (\mathbf{Z}/4 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/5) \oplus (\mathbf{Z}/2 \oplus \mathbf{Z}/9) \\ &\cong (\mathbf{Z}/16 \oplus \mathbf{Z}/4 \oplus \mathbf{Z}/2) \oplus (\mathbf{Z}/9 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/3) \oplus (\mathbf{Z}/25 \oplus \mathbf{Z}/5). \end{aligned}$$

Nous voyons ainsi que A est bien isomorphe à B.

Analysons ce raisonnement : nous sommes partis d'un groupe abélien

$$A = A(\alpha) := \mathbf{Z}/n_1 \oplus \mathbf{Z}/n_2 \oplus \ldots \oplus \mathbf{Z}/n_k$$

donné par une suite $\alpha = (n_1, n_2, \ldots, n_k)$ d'entiers ≥ 2. Nous avons décomposé chacun des nombres n_i en un produit de puissances de nombres premiers. Nous

arrangeons ces puissances pour obtenir la *suite $\pi(\alpha)$ de puissances de nombres premiers associée à α*

$$\pi(\alpha) = (p_1^{e_{11}}, p_1^{e_{12}}, \ldots, p_i^{e_{ij}}, \ldots, p_r^{e_{rs}})$$

où $p_1 < p_2 < \ldots < p_r$ et $e_{i1} \geq e_{i2} \geq \ldots$ pour tout i. Le lemme chinois nous a fourni un isomorphisme

$$A(\alpha) \cong A(\pi(\alpha))$$

De même, nous avons calculé la suite des puissances $\pi(\beta)$ associée à la suite β qui déterminait le groupe $B = A(\beta)$. Nous avons pu conclure que $A \cong B$ parce que nous avions l'égalité $\pi(\alpha) = \pi(\beta)$ et donc $A = A(\alpha) \cong A(\pi(\alpha)) = A(\pi(\beta)) \cong A(\beta) = B$.

Cet argument est parfaitement général et montre la condition suffisante ('si') du théorème suivant

Théorème. *Soient $\alpha = (n_1, n_2, \ldots, n_k)$ et $\beta = (m_1, m_2, \ldots, m_l)$ deux suites d'entiers supérieurs à 1 et*

$$\begin{aligned} A &= \mathbf{Z}/n_1 \oplus \mathbf{Z}/n_2 \oplus \ldots \oplus \mathbf{Z}/n_k \ , \\ B &= \mathbf{Z}/m_1 \oplus \mathbf{Z}/m_2 \oplus \ldots \oplus \mathbf{Z}/m_l. \end{aligned}$$

Alors A est isomorphe à B si et seulement si les suites de puissances premières associées à α et β sont égales.

Remarque. En utilisant le lemme chinois nous avons déjà démontré la condition suffisante du théorème. En vue de cette démonstration, la condition nécessaire ('seulement si') peut être interprétée comme l'affirmation que *toute isomorphie entre sommes de groupes $\mathbf{Z}/n\mathbf{Z}$ est conséquence du lemme chinois* (appliqué plusieurs fois, bien entendu).

Il reste à démontrer que si $\pi(\alpha) \neq \pi(\beta)$, alors $A \ncong B$.

Exemples. 1) Le groupe $A = \mathbf{Z}/2 \oplus \mathbf{Z}/2$ a le même ordre que le groupe $B = \mathbf{Z}/4$. Néanmoins, les deux ne sont pas isomorphes. En effet, si $a = (\overline{x}, \overline{y})$ est un élément quelconque de A, alors

$$2a = a + a = (\overline{2x}, \overline{2y}) = (\overline{0}, \overline{0}) = 0.$$

S'il existait un isomorphisme $\phi : A \to B$, les éléments de B jouiraient de la même propriété. En effet, tout élement b de B s'écrirait $b = \phi(a)$ pour un $a \in A$, et on aurait

$$2b = b + b = \phi(a) + \phi(a) = \phi(a + a) = \phi(0) = 0.$$

Or, l'élément $\overline{1}$ de $B = \mathbf{Z}/4$ ne vérifie pas cette condition car $\overline{2} \neq \overline{0}$ dans $\mathbf{Z}/4$.

2) Les groupes $A = \mathbf{Z}/3 \oplus \mathbf{Z}/2 \oplus \mathbf{Z}/2$ et $B = \mathbf{Z}/3 \oplus \mathbf{Z}/4$ ont le même ordre. En vue du premier exemple, il est plausible qu'il ne soient pas isomorphes. Pour montrer cette affirmation, supposons qu'il existe un isomorphisme $\phi : \mathbf{Z}/3 \oplus \mathbf{Z}/2 \oplus \mathbf{Z}/2 \to \mathbf{Z}/3 \oplus \mathbf{Z}/4$. Regardons les sous-groupes A_4 et B_4 formés des éléments x de A (resp. B) tels que $4x = 0$. Il est (presque) clair (voir ci-dessous) que l'application

$$A_4 \to B_4 \ , a \mapsto \phi(a)$$

est un isomorphisme. Or nous avons

$$\begin{aligned} A_4 &= \{(\overline{0}, \overline{u}, \overline{v}) \mid \overline{u}, \overline{v} \in \mathbf{Z}/2\} \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \\ B_4 &= \{(\overline{0}, \overline{w}) \mid \overline{w} \in \mathbf{Z}/4\} \cong \mathbf{Z}/4. \end{aligned}$$

Ainsi, ϕ nous fournirait un isomorphisme entre $\mathbf{Z}/2 \oplus \mathbf{Z}/2$ et $\mathbf{Z}/4$ en contradiction avec le premier exemple.

Nous allons systématiser la technique utilisée dans ces exemples.

Sous-groupes de m-torsion

Si A est un groupe abélien et m un entier ≥ 2, le *sous-groupe de m-torsion de A* est

$$A_m := \{a \in A \mid ma = 0\} \quad (ma = \underbrace{a + \ldots + a}_{m})$$

et son *sous-groupe de m^∞-torsion* est

$$A_{m^\infty} := \{a \in A \mid \text{il existe } k \in \mathbf{N} \text{ tel que } m^k a = 0\}.$$

Exemples. 1) Nous avons

$$\begin{aligned} (\mathbf{Z}/6)_2 &= \{\overline{0}, \overline{3}\} \cong \mathbf{Z}/2 \\ (\mathbf{Z}/6)_3 &= \{\overline{0}, \overline{2}, \overline{4}\} \cong \mathbf{Z}/3. \end{aligned}$$

2) Si p est un nombre premier et $n \geq 1$, alors

$$(\mathbf{Z}/p^n)_{p^\infty} = \mathbf{Z}/p^n$$

car $p^n \overline{x} = \overline{0}$ pour tout $\overline{x} \in \mathbf{Z}/p^n$. Si q est un nombre premier différent de p, alors

$$(\mathbf{Z}/q^n)_{p^\infty} = \{\overline{0}\}.$$

En effet, q^n et p^k sont premiers entre eux de façon que l'équation

$$p^k \overline{x} = \overline{0} \text{ (resp. } p^k x = q^n y \text{ pour un y} \in \mathbf{Z})$$

n'admet que $\overline{x} = \overline{0}$ pour solution (lemme de Gauss).

3) Si p est premier et $k \leq n$, alors

$$(Z/p^n)_{p^k} = \{\overline{0}, \overline{p^{n-k}}, 2\overline{p^{n-k}}, \ldots, (p^k - 1)\overline{p^{n-k}}\}$$

qui est isomorphe à $\mathbf{Z}/p^k$ par l'isomorphisme qui envoie $\overline{1}$ sur $\overline{p^{n-k}}$. Si $k \geq n$, alors $(\mathbf{Z}/p^n)_{p^k} = \mathbf{Z}/p^n$. Donc

$$(\mathbf{Z}/p^n)_{p^k} \cong \begin{cases} \mathbf{Z}/p^k & \text{si } k \leq n \\ \mathbf{Z}/p^n & \text{si } k \geq n. \end{cases}$$

Lemme. *Soient A et B des groupes abéliens.*

a) On a $(A \oplus B)_m = A_m \oplus B_m$ *et* $(A \oplus B)_{m^\infty} = A_{m^\infty} \oplus B_{m^\infty}$.

b) Si $f : A \to B$ *est un homomorphisme, alors* $f(A_m) \subset B_m$. *Si* f *est un isomorphisme, l'application induite* $A_m \to B_m$, $a \mapsto f(a)$ *est un isomorphisme. Donc*

$$A \cong B \Longrightarrow (A_m \cong B_m \text{ et } A_{m^\infty} \cong B_{m^\infty}).$$

Exemples. 4) Soient p et q deux nombres premiers différents et $A = \mathbf{Z}/p^3 \oplus \mathbf{Z}/p^2 \oplus \mathbf{Z}/q^5 \oplus \mathbf{Z}/q^4$. Alors l'exemple 2) et l'énoncé a) du lemme montrent qu'on a

$$\begin{aligned} A_{p^\infty} &\cong \mathbf{Z}/p^3 \oplus \mathbf{Z}/p^2 \\ A_{q^\infty} &\cong \mathbf{Z}/q^5 \oplus \mathbf{Z}/q^4. \end{aligned}$$

5) Généralisons l'exemple 4). Soit π une suite de puissances de nombres premiers, p un nombre premier et π_p la suite des puissances de p qui apparaissent dans π. Alors l'exemple 2) et l'énoncé b) du lemme montrent qu'on a

$$A(\pi)_{p^\infty} \cong A(\pi_p).$$

Démonstration du lemme : a) Par définition de la structure de groupe sur $A \oplus B$, nous avons $m(a,b) = (ma, mb)$ et $0_{A\oplus B} = (0,0)$. Donc $m(a,b)$ s'annule si et seulement si $ma = 0$ et $mb = 0$ ce qu'il fallait démontrer. De même pour le cas m^∞.

b) Si $a \in A_m$, nous avons $mf(a) = f(ma) = f(0) = 0$, d'où l'inclusion. Supposons que f est un isomorphisme et soit $g : B \to A$ l'isomorphisme inverse. Alors nous avons $g(B_m) \subset A_m$ et on voit que l'application $B_m \to A_m$, $b \mapsto g(b)$ est l'inverse de l'application $A_m \to B_m$, $a \mapsto f(a)$. Les deux sont donc des isomorphismes inverses l'un de l'autre. De même pour le cas m^∞.

Suite de la démonstration du théorème

Supposons que α et β sont comme dans le théorème et que $A(\alpha) \cong A(\beta)$. Il faut montrer que $\pi(\alpha) = \pi(\beta)$. Nous savons que $A(\alpha) \cong A(\pi(\alpha))$ et $A(\beta) \cong A(\pi(\beta))$. Donc l'hypothèse implique que $A(\pi(\alpha)) \cong A(\pi(\beta))$. Soit p un nombre premier et notons $\pi_p(\alpha)$ la suite des puissances de p qui apparaissent dans $\pi(\alpha)$. Par l'exemple 5) nous avons

$$A(\pi(\alpha))_{p^\infty} \cong A(\pi_p(\alpha)) \text{ et } A(\pi(\beta))_{p^\infty} \cong A(\pi_p(\beta)).$$

Donc $A(\pi_p(\alpha)) \cong A(\pi_p(\beta))$. Il reste à démontrer que si π et π' sont deux suites de puissances de p, alors $A(\pi) \cong A(\pi')$ implique $\pi = \pi'$.

Pour cela, nous allons calculer l'ordre du sous-groupe de p^k-torsion

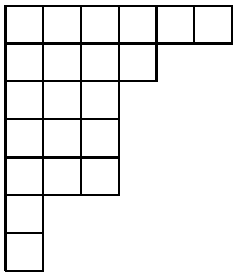
$$A(\pi)_{p^k} \cong A(\pi')_{p^k} \text{ (d'après l'énoncé b) du lemme)}$$

pour tout $k \in \mathbf{N}$ et montrer que ces nombres déterminent la suite π. Nous nous contentons de traiter un exemple représentatif :

Exemple. Supposons que

$$\pi = (p^6, p^4, p^3, p^3, p^3, p, p)$$

et notons $e_1 = 6$, $e_2 = 4$, ...,$e_7 = 1$ les exposants qui interviennent dans π. Nous représentons π par son *diagramme de Young*



La i-ième ligne de ce diagramme est formé de e_i cases. Notons que $A(\pi)$ est d'ordre p^e, où $e = e_1 + \ldots + e_8$ est le *nombre total de cases du diagramme de Young*. D'après l'énoncé a) du lemme et l'exemple 3), nous avons

$$A(\pi)_{p^k} \cong \mathbf{Z}/p^{f_{1k}} \oplus \mathbf{Z}/p^{f_{2k}} \oplus \ldots \oplus \mathbf{Z}/p^{f_{8,k}}$$

où $f_{ik} = \min(e_i, k)$. Par exemple

$$A(\pi)_{p^4} = \mathbf{Z}/p^4 \oplus \mathbf{Z}/p^4 \oplus \mathbf{Z}/p^3 \oplus \mathbf{Z}/p^3 \oplus \mathbf{Z}/p^3 \oplus \mathbf{Z}/p \oplus \mathbf{Z}/p.$$

En particulier, l'ordre de $A(\pi)_{p^k}$ est de p^{f_k} où f_k est la somme sur i des f_{ik}. Or, f_{ik} est le nombre de cases de la i-ième ligne qui se trouvent à gauche de la position k, et f_k est donc le nombre total de cases qui se trouvent dans les colonnes d'indice 1 à k. Par conséquent, $f_k - f_{k-1}$ est la longueur de la k-ième colonne. Comme le diagramme peut être reconstruit à partir de ses colonnes, il est déterminé par les ordres des groupes $A(\pi)_{p^k}$ ce qu'il fallait démontrer.