Décomposition cyclique d'un groupe abélien fini

Combes, *Algèbre et géométrie*, page 65

Théorème : Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers q_1 supérieur ou égal à deux, q_2 multiple de q_1,...,q_k multiple de q_{k-1}, uniques, tels que G soit isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/q_k\mathbb{Z})$.

Lemme : *Soient G un groupe abélien fini et $a \in G$ d'ordre $o(a)$ maximum. Alors, pour tout $y \in G/ < a >$, il existe $x \in G$ tel que $\overline{x} = y$ et tel que $o(x) = o(y)$.*

Démonstration du lemme : Notons additivement la loi de composition de G. Soient φ l'homomorphisme canonique de G sur $G/ < a >$ et soit s l'ordre de $y \in G/ < a >$. Considérons $x \in G$ tel que $\varphi(x) = y$. ON a $\varphi(sx) = sy = 0$ et donc $sx \in \mathrm{Ker}(\varphi) =< a >$. Il existe donc $k \in \mathbb{N}$ tel que $0 \leq k < o(a)$ et $sx = ka$. Par division euclidienne,

$$k = sq + r \quad \text{avec} 0 \leq r < s$$

d'où $sx = ka = sqa + ra$. Posons $x' = x - qa$. On a

$$\varphi(x') = \varphi(x) = y \quad \text{d'où} s = o(y)|o(x')$$

Supposons $r \neq 0$. On a $sx' = sx - sqa = ra$. On obtient donc que $o(sx') = \frac{o(x')}{o(x') \wedge s}$, soit $o(sx') = \frac{o(x')}{s}$. On en déduit que

$$o(x') = so(sx') = so(ra) = s\frac{o(a)}{o(a) \wedge r}$$

Du fait que $o(a)$ est maximum, on a $o(x') \leq o(a)$. La relation précédente donne alors $s \leq o(a) \wedge r \leq r$. Cela contredit la condition du reste de la division euclidienne donc $r = 0$ et $sx' = ra = 0$. Cela prouve que $o(x')|s$ et donc que $o(x') = o(y)$.

Démonstration de l'Existence dans le Théorème.

Montrons l'existence de cette suite, par récurrence sur l'ordre n de G. Pour $n = p$ premier, la propriété est vérifiée : G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Supposons établie l'existence pour les groupes d'ordre strictement inférieur à n, et considérons G d'ordre n. Soit $a \in G$ d'ordre m maximum. On a $m > 1$ car $G \neq \{e\}$, donc $G/ < a >$ est d'ordre strictement inférieur à $|G| = n$. D'après l'hypothèse de récurrence, il existe dans $G/ < a >$ des sous-groupes cycliques $G'_1 =< a'_1 >$, ..., $G'_{k-1} =< a'_{k-1} >$ d'ordres q_1, ..., q_{k-1} tels que $1 < q_1| \ldots |q_{k-1}$ et tels que $G/ < a >= G'_1 \times \ldots \times G'_{k-1}$. D'après le lemme, il existe dans G des représentants $a_1, \ldots a_{k-1}$ de a'_1,...,a'_{k-1} ayant les mêmes ordres. Vérifions que G est produit direct des sous-groupes cycliques $G_1 =< a_1 >$,...,$G_{k-1} =< a_{k-1} >$,$G_k =< a >$.

Soit φ l'homomorphisme canonique de G sur $G/ < a >$. Pour tout $x \in G$, il existe n_1, ..., n_{k-1}, avec $0 \leq n_1 < o(a_i)$ pour $i = 1, \ldots, k-1$, uniques, tels que

$$\varphi(x) = n_1a'_1 + \ldots + n_{k-1}a'_{k-1} = \varphi(n_1a_1 + \ldots + n_{k-1}a_{k-1})$$

Il existe donc un élément n_ka de $\mathrm{Ker}(\varphi) =< a >$ avec $0 \leq n_k < m = o(a)$ et tel que $x = (n_1a_1 + \ldots + n_{k-1}a_{k-1}) + n_ka$. Ainsi $G = G_1 + \ldots + G_k$.

Vérifions que cette expression de x est unique, et alors G sera le produit direct des sous-groupes $G_1, \ldots, G_k$. Soit $x = m_1a_1 + \ldots + m_ka$ une autre expression de x du type précédent. Alors $\varphi(x) = n_1a'_1 + \ldots + n_{k-1}a'_{k-1} = m_1a'_1 + \ldots + m_{k-1}a'_{k-1}$. Comme $G/ < a >$ est produit direct de $G'_1, \ldots, G'_{k-1}$, on a $n_1 = m_1, \ldots, n_{k-1} = m_{k-1}$. On en déduit ensuite $n_ka = m_ka$ d'où $n_k = m_k$ puisqu'on a $0 \leq n_k < o(a)$ et $0 \leq m_k < o(a)$.

L'ordre de $x_0 = (a_1, \ldots, a_{k-1}, a) \in G_1 \times \ldots \times G_k$ est le ppcm de $o(a_1)$, ..., $o(a)$. On a donc $o(x_0) \geq o(a)$. Comme $o(a)$ est le maximum des ordres des éléments de G, on en déduit que $o(a) = o(x_0) = ppcm\,(o(a_1), \ldots, o(a_{k-1}), o(a))$ et donc que $o(a_1)| \ldots |o(a_{k-1})|o(a)$.

Démonstration de l'Unicité dans le Théorème.

Montrons l'unicité de la suite $q_1, \ldots, q_k$ par récurrence sur l'ordre n de G.

Si $n = p$ est premier, la suite (q_i) est unique, réduite à p. Supposons établie l'unicité pour les groupes d'ordre strictement inférieur à n. Considérons un groupe G d'ordre $n > 1$. Considérons deux décompositions

$$G = G_1 \times \ldots \times G_k = G'_1 \times \ldots \times G'_m$$

avec $G_i \simeq \mathbb{Z}/q_i\mathbb{Z}$, $G'_j \simeq \mathbb{Z}/q'_j\mathbb{Z}$, $1 < q_1| \ldots |q_k$, $1 < q'_1| \ldots |q'_m$.

Soit p un facteur premier de q_1, et donc de $q_2, \ldots, q_k$. Comme G est abélien, $f : x \mapsto px$ est un endomorphisme de G.Il laisse stable chacun des sous-groupes G_i, car ces sous-groupes sont cycliques.

$f(G_1) \subset G_1$ est l'unique sous-groupe de G_1 d'ordre $\frac{q_1}{p}$. De même, $f(G_2) \subset G_2$,...,$f(G_k) \subset G_k$ sont d'ordres $\frac{q_1}{p}, \ldots, \frac{q_k}{p}$. On a

$$(f(G_1) + \ldots + f(G_i)) \cap f(G_{i+1}) \ \subset \ (G_1 + \ldots + G_i) \cap G_{i+1} = \{0\}$$

pour $i = 1, \ldots, k-1$, donc $f(G)$ est produit direct de $f(G_1), \ldots, f(G_k)$, et on a $|f(G)| = \frac{q_1 \ldots q_k}{p^k} = \frac{|G|}{p^k}$.

De même, on a $f(G'_j) \subset G'_j$ pour $j = 1 \ldots m$, et $f(G) = f(G'_1) \times \ldots \times f(G'_m)$. Puisque $q'_1 | \ldots | q'_m$, il existe r tel que p ne divise pas $q'_1, \ldots, q'_r$ et p divise $q'_{r+1}, \ldots, q'_m$. On a alors $f(G'_1) = G'_1$ car $f : x \mapsto px$ est alors un automorphisme de G'_1. De même, $f(G'_2) = G'_2$, ..., $f(G'_r) = G'_r$. Par contre, les ordres de $f(G'_{r+1}), \ldots, f(G'_m)$ sont $\frac{q'_{r+1}}{p}, \ldots, \frac{q'_m}{p}$, donc $|f(G)| = q'_1 \ldots q'_r \frac{q'_{r+1} \cdots q'_m}{p^{m-r}} = \frac{|G|}{p^{m-r}}$.

En comparant les deux valeurs de $f(G)$ obtenues, on voit que $k = m - r \leq m$. En échangeant les rôles, on obtient de même $m \leq k$, et donc $m = k$. On en déduit que $r = 0$, et que p divise $q'_1, \ldots, q'_k$. D'après l'hypothèse de récurrence, la décomposition cyclique de $f(G)$ est unique. Les deux suites $\frac{q_1}{p}, \ldots, \frac{q_k}{p}$ et $\frac{q'_1}{p}, \ldots, \frac{q'_k}{p}$ sont donc égales, et les suites $q_1, \ldots, q_k$ et $q'_1, \ldots, q'_k$ sont égales.