Groupes cycliques

Marc Lorenzi

22 décembre 2025

D'une certaine façon, les *groupes cycliques* sont les groupes finis les plus simples que l'on puisse considérer.

Définition 1. Le groupe fini $(G, \times)$ est *cyclique* lorsqu'il existe $g \in G$ tel que $G = \{g^k : k \in \mathbb{Z}\}$. Un tel g est un *générateur* de G.

Si g est un générateur du groupe G, nous noterons $G =< g >$.

Pour tout $n \in \mathbb{N}^*$, deux exemples bien connus de groupes cycliques sont le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ des entiers modulo n et le groupe $(\mathcal{U}_n, \times)$ des racines n^{es} de l'unité dans $\mathbb{C}$. On a $\mathbb{Z}/n\mathbb{Z} =< 1 >$ et $\mathcal{U}_n =< e^{2i\pi/n} >$.

Proposition 1. *Soit G un groupe cyclique de cardinal $n \in \mathbb{N}^*$ et de neutre e. Soit g un générateur de G.*

- *Pour tout $k \in \mathbb{Z}$, $g^k = e$ si et seulement si $k \in n\mathbb{Z}$.*
- *Pour tous $i, j \in \mathbb{Z}$, $g^i = g^j$ si et seulement si $j - i \in n\mathbb{Z}$.*
- $G = \{e, g, g^2, \ldots, g^{n-1}\}$.

Démonstration. La deuxième propriété est clairement conséquence de la première. En effet, $g^i = g^j$ si et seulement si $g^{j-i} = e$.

Notons $E = \{k \in \mathbb{Z} : g^k = e\}$.

Comme G est fini, il existe $i, j \in \mathbb{Z}$ distincts tels que $g^i = g^j$. De là, $g^{j-i} = e$ donc $j - i \in E$. L'ensemble E n'est donc pas vide. Soient $i, j \in E$. On a $g^{i+j} = g^i g^j = e^2 = e$, donc $i + j \in E$. Enfin, pour tout $i \in E$, $g^{-i} = (g^i)^{-1} = e^{-1} = e$, donc $-i \in E$. Ainsi, E est un sous-groupe de $\mathbb{Z}$. Il existe donc $m \in \mathbb{N}$ tel que $E = m\mathbb{Z}$.

Soient $0 \leq < i < j < m$. On a $0 < j - i < n$, donc $j - i \notin m\mathbb{Z}$. De là, $g^{j-i} \neq e$, donc $g^i \neq g^j$. Les éléments $e, g, g^2, \ldots, g^{m-1}$ sont donc distincts deux à deux. Soit maintenant $k \in \mathbb{Z}$. Effectuons la division euclidienne de k par m : $k = qm + r$ où $q \in \mathbb{Z}$ et $0 \leq r < m$. On a alors

$$g^k = (g^m)^q g^r = e^q g^r = g^r$$

Ainsi, $G = \{e, g, g^2, \ldots, g^{m-1}\}$ est de cardinal m. On en déduit $m = n$. □

Proposition 2. *Pour tout $n \in \mathbb{N}^*$, il existe, à isomorphisme près, un unique groupe cyclique de cardinal n.*

Démonstration. Soit $n \in \mathbb{N}^*$. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique de cardinal n, d'où l'existence. Soit $(G, \times)$ un groupe cyclique de cardinal n et de neutre e. Soit g un générateur de G. Pour tous $i, j \in \mathbb{Z}$, si $i \equiv j \bmod n$, alors $g^i = g^j$. On peut donc passer au quotient et considérer l'application $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ définie pour tout $k \in \mathbb{Z}$ par $f(k + n\mathbb{Z}) = g^k$.

Pour tous $k, k' \in \mathbb{Z}$,

$$f((k + n\mathbb{Z}) + (k' + n\mathbb{Z})) = f((k + k') + n\mathbb{Z}) = g^{k+k'} = g^k g^{k'} = f(k + n\mathbb{Z})f(k' + n\mathbb{Z})$$

Ainsi, f est un morphisme de groupes. Pour tout $x \in G$, il existe $k \in \mathbb{Z}$ tel que $x = g^k = f(k + n\mathbb{Z})$, donc f est surjective. Enfin, soit $k \in \mathbb{Z}$. Supposons que $k + n\mathbb{Z} \in \ker f$. On a alors $g^k = e$, donc $k \in n\mathbb{Z}$, d'où $k + n\mathbb{Z} = n\mathbb{Z}$. Ainsi, $\ker f = \{n\mathbb{Z}\}$ donc f est injective. Les deux groupes $\mathbb{Z}/n\mathbb{Z}$ et G sont donc isomorphes. □

Proposition 3. *Soit G un groupe cyclique. Tous les sous-groupes de G sont cycliques.*

Dans les propositions qui suivent, G est un groupe cyclique de cardinal n et e est le neutre de G. On note g un générateur de G.

Démonstration. Soit H un sous-groupe de G. Si $H = \{e\}$, alors $H =< e >$. Supposons donc $H \neq \{e\}$. Soit k le plus petit entier naturel non nul tel que $g^k \in H$. Soit $x = g^\ell \in H$ où $\ell \in \mathbb{Z}$. Effectuons la division euclidienne de ℓ par k : $\ell = qk + r$ où $q \in \mathbb{Z}$ et $0 \leq r < k$. On a $g^r = g^\ell (g^k)^{-q} \in H$. Par minimalité de k, $r = 0$ et donc $\ell = qk$. Ainsi, $H \subseteq < g^k >$. Inversement, $g^k \in H$ donc, par stabilité de H par élévation aux puissances, $< g^k > \subseteq H$. Ainsi, $H =< g^k >$ est cyclique. □

Proposition 4. *Pour tout $k \in \mathbb{Z}$, $< g^k > =< g^{n \wedge k} >$.*

Démonstration. Soit $k \in \mathbb{Z}$. Soit $H =< g^k >$. Soit $\delta = n \wedge k$. Il existe $u, v \in \mathbb{Z}$ tels que $uk + vn = \delta$. De là,

$$g^\delta = (g^k)^u (g^n)^v = (g^k)^u \in H'$$

et donc $< g^\delta > \subseteq H$. Inversement, k est multiple de δ, donc $g^k \in < g^\delta >$, d'où $H \subseteq < g^\delta >$. Ainsi, $H =< g^\delta >$. □

Proposition 5. *Soit d un diviseur de n. Le groupe G possède un unique sous-groupe de cardinal d. Ce sous-groupe est $< g^{n/d} >$.*

Démonstration. Soit $h = g^{n/d}$. Soit $H =< h >$. Pour tout entier naturel $k < d$, $kn/d < n$, donc $h^k \neq e$. De plus, $h^d = g^n = e$. Donc, H est de cardinal d.

Soit H' un sous-groupe de G de cardinal d. On a $H' =< g^k >$ où $0 \leq k < n$. Soit $\delta = n \wedge k$. Par la proposition 4, $H =< g^\delta >$. Comme δ divise n, la première partie de la preuve montre que H' est

de cardinal n/δ. Or, H' est de cardinal d, donc $n/\delta = d$, d'où $\delta = n/d$. Puis $H' =< g^{n/d} >= H$. □

Proposition 6. *Pour tout $k \in \mathbb{Z}$, le cardinal de $< g^k >$ est $n/(n \wedge k)$.*

Démonstration. Soit $k \in \mathbb{Z}$. Soit $\delta = n \wedge k$. Par la proposition 4, $< g^k >=< g^\delta >$. Par la proposition 5, le cardinal de ce groupe est n/δ. □

Proposition 7. *Soit H un sous-groupe de G. Le cardinal de H divise le cardinal de G.*

Nous avons là un cas particulier d'un résultat beaucoup plus général, le *théorème de Lagrange*, qui affirme que dans *tout* groupe fini, le cardinal d'un sous-groupe divise le cardinal du groupe.

Démonstration. Par la proposition 3, H est cyclique. Par la proposition 4, $H =< g^\delta >$ où δ divise n. Par la proposition 5, le cardinal de H est n/δ, un diviseur de n. □

La *fonction indicatrice d'Euler* est la fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ définie par

$$\varphi(n) = |\{k \in [\![1, n]\!] : k \wedge n = 1\}|$$

Proposition 8. *G possède $\varphi(n)$ générateurs.*

Démonstration. Soit $k \in [\![1, n]\!]$. Par la proposition 6, g^k engendre G si et seulement si $n/(n \wedge k) = n$, c'est à dire $n \wedge k = 1$. □

Ce qui précède nous permet de montrer une formule remarquable concernant la fonction indicatrice d'Euler.

Proposition 9.

$$n = \sum_{d|n} \varphi(d)$$

Démonstration. Pour tout diviseur d de n, notons G_d l'ensemble des éléments de G qui engendrent un sous-groupe de G de cardinal d. On a l'union disjointe

$$G = \bigcup_{d|n} G_d$$

Pour tout diviseur d de n, G possède un unique sous-groupe H de cardinal d et H est cyclique. Les éléments de G_d sont les générateurs de H. Par la proposition 8, H possède $\varphi(d)$ générateurs, et donc $|G_d| = \varphi(d)$. Ainsi,

$$n = |G| = \sum_{d|n} |G_d| = \sum_{d|n} \varphi(d)$$

□