Groupes monogènes

Un groupe G est dit *monogène* s'il est engendré par un de ses éléments. Si g est un de ces générateurs, on a donc $\mathrm{G} = \left\{ g^n \,\middle|\, n \in \mathbb{Z} \right\}$.

$\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ sont des groupes monogènes, 1 et $\bar{1}$ constituant des générateurs évidents (notons que, dans un cas comme dans l'autre, la loi de groupe étant donnée additivement, la puissance n-ième d'un élément g est notée ng plutôt que g^n). Par ailleurs, si n et k appartiennent à $\mathbb{Z}$, la puissance n-ième de k est effectivement égale au produit usuel $n \times k$, ce que suggère la notation nk. Parallèlement, la « puissance » $n\bar{k}$, pour $n \in \mathbb{Z}$ et $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$, coïncide avec le produit usuel : $n\bar{k} = \overline{nk} = \bar{n}\bar{k}$.

Le but est ici de démontrer que, réciproquement, tous les groupes monogènes sont isomorphes à $\mathbb{Z}$ ou à l'un des $\mathbb{Z}/n\mathbb{Z}$, de déterminer leurs sous-groupes, leurs générateurs, leurs automorphismes et leurs morphismes à valeurs dans un groupe général G.

Avant de commencer, convenons de deux notations :

- Si a est un élément d'un groupe G, on note $\varphi_a : \begin{array}{ccc} \mathbb{Z} & \to & \mathrm{G} \\ k & \mapsto & a^k \end{array}$. C'est tautologiquement un morphisme de groupes.
- Si a est un élément d'un groupe G vérifiant $a^n = 1_\mathrm{G}$, on note $\psi_a^{(n)} : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathrm{G} \\ \bar{k} & \mapsto & a^k \end{array}$. Cette application est bien définie car, si $\bar{k} = \overline{k'}$, on peut trouver un entier q tel que $k' = qn + k$, et $a^{k'} = a^{nq+k} = (a^n)^q a^k = a^k$. Il est alors immédiat qu'elle est un morphisme.

Avec cette définition, a est un générateur de G si et seulement si $\varphi_a : \mathbb{Z} \to \mathrm{G}$ est surjectif.

Une dernière définition (importante) : l'*ordre* d'un élément $g \in \mathrm{G}$ est le plus petit entier $n > 0$ tel que $g^n = 1_\mathrm{G}$ (si un tel entier n'existe pas, on dit que l'élément est d'ordre infini).

Classification des groupes monogènes

Proposition. Soit G un groupe monogène. Alors G est isomorphe à $\mathbb{Z}$ ou il existe $n \geqslant 1$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Notons que ces cas s'excluent mutuellement, puisque ces groupes n'ont même pas le même cardinal : $|\mathbb{Z}/n\mathbb{Z}| = n$ et $|\mathbb{Z}| = \infty$.

Preuve. Soit donc $x \in \mathrm{G}$ un élément générateur [1] : $\mathrm{G} = \left\{ x^k \,\middle|\, k \in \mathbb{Z} \right\}$. La disjonction se fait selon l'ordre de x.

- Si x est d'ordre infini, considérons le morphisme $\varphi_x : \mathbb{Z} \to \mathrm{G}$. Ce morphisme est surjectif puisque x engendre G et injectif : si $\varphi_x(n) = \varphi_x(n')$, $x^n = x^{n'}$, donc $x^{n-n'} = 1$. Quitte à remplacer $n - n'$ par son opposé, on peut utiliser le fait qu'x est d'ordre

1. Notons qu'*a priori*, rien ne nous indique que G est abélien, et qu'il est donc exclu d'utiliser la notation additive.

infini : cela implique $n - n' = 0$. Notons qu'en fait, on a redémontré le fait qu'un morphisme est injectif si et seulement si son noyau est réduit au sous-groupe trivial.
– Si x est d'ordre n, on peut considérer $\psi = \psi_x^{(n)} : \mathbb{Z}/n\mathbb{Z} \to \mathrm{G}$. C'est encore un morphisme surjectif. Montrons qu'il est injectif : soit $\bar{k} \in \ker\psi$. Puisque $\bar{k}$ est un élément de $\mathbb{Z}/n\mathbb{Z}$, on peut supposer que $0 \leqslant k < n$. On a donc $x^k = 1$. Mais n est, par construction, minimal parmi les entiers strictement positifs possédant cette propriété. On a donc $k = 0$, et $\ker\psi = \{\bar{0}\}$

Dans tous les cas, on a donc exhibé un isomorphisme $\varphi : \mathbb{Z} \to \mathrm{G}$ ou $\psi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{G}$. □

Un corollaire de cette preuve est important : le cardinal d'un groupe monogène est égal à l'ordre de ses générateurs. C'est un résultat utilisé en permanence dans l'étude des sous-groupes monogènes d'un groupe général.

Sous-groupes

On a pour commencer des sous-groupes monogènes $k\mathbb{Z} = \left\{ku \,\middle|\, u \in \mathbb{Z}\right\}$ de $\mathbb{Z}$. Puisque $k\mathbb{Z} = (-k)\mathbb{Z}$, on peut même se restreindre aux cas où $k \geqslant 0$. On les a en fait tous de cette façon :

Proposition. Soit H un sous-groupe de $\mathbb{Z}$. Alors il existe $k \geqslant 0$ tel que $\mathrm{H} = k\mathbb{Z}$.

Preuve. Si $\mathrm{H} = \{0\}$, on peut écrire $\mathrm{H} = 0\mathbb{Z}$. Sinon, il existe dans H un élément non nul et, quitte à en prendre l'opposé, il existe même un entier strictement positif. Soit donc $k = \min(\mathrm{H} \cap \mathbb{N}^*)$. On va montrer que $\mathrm{H} = k\mathbb{Z}$.

Déjà, H contient k. Il contient donc également $\langle k\rangle = k\mathbb{Z}$. Reste à montrer l'inclusion réciproque. Soit $h \in \mathrm{H}$: on en écrit la division euclidienne par k : $h = qk + r$, avec $0 \leqslant r < k$. On a alors $r = h - qk$, et donc $r \in \mathrm{H}$. Par minimalité de k, on a $r = 0$ et $h = qk \in k\mathbb{Z}$. On a ainsi montré que $\mathrm{H} = k\mathbb{Z}$. □

On a donc montré que tout sous-groupe de $\mathbb{Z}$ est un sous-groupe monogène. La même chose est valable pour $\mathbb{Z}/n\mathbb{Z}$.

Proposition. Soit $n \geqslant 1$. Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par un élément $\bar{k}$, avec k divisant n.

Preuve. On pourrait refaire une preuve similaire à celle de la proposition précédente. Il est cependant plus économique d'utiliser ce que l'on sait déjà sur $\mathbb{Z}$. Soit donc $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme [2] de groupes qui envoie k sur $\bar{k}$. C'est un morphisme évidemment surjectif. Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. $\varphi^{-1}[\mathrm{H}]$ est alors un sous-groupe de $\mathbb{Z}$, qui contient $\ker\pi = n\mathbb{Z}$. On peut donc l'écrire $k\mathbb{Z}$, avec k positif. Puisqu'il contient $n\mathbb{Z}$, k divise n. En outre, puisque π est surjectif, on a $\mathrm{H} = \pi\left[\pi^{-1}[\mathrm{H}]\right] = \pi[k\mathbb{Z}]$. Cela démontre la proposition, puisque l'on a toujours, étant donné un morphisme $\chi : \mathrm{G}_1 \to \mathrm{G}_2$ et un élément $g \in \mathrm{G}_1$: $\chi[\langle g\rangle] = \chi\left[\left\{g^n \,\middle|\, n \in \mathbb{Z}\right\}\right] = \left\{\chi(g^n) \,\middle|\, n \in \mathbb{Z}\right\} = \left\{\chi(g)^n \,\middle|\, n \in \mathbb{Z}\right\} = \langle\chi(g)\rangle$. On a donc $\mathrm{H} = \langle\bar{k}\rangle$. □

2. C'est un morphisme important, d'ailleurs égal à $\varphi_{\bar{1}}$. On le nommera bientôt *surjection canonique*.

Notons que ces sous-groupes $\mathrm{H} = \langle \bar{k} \rangle$ sont tous différents. En effet, la première proposition (ou plutôt sa preuve) nous a montré que le cardinal du groupe engendré par un élément était égal à l'ordre de cet élément. Or, il est facile de voir que, si k divise n, l'ordre de $\bar{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ est n/k. On a obtenu au passage un autre résultat sur le groupe cyclique qui est une espèce de réciproque au théorème de Lagrange.

Proposition. Soit G un groupe cyclique d'ordre n et d un diviseur de n. Alors G possède un unique sous-groupe d'ordre d.

Générateurs

Proposition. Les générateurs de $\mathbb{Z}$ sont 1 et -1. Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ $(0 \leqslant k < n)$ tels que k et n sont premiers entre eux.

Preuve. Puisque 1 est générateur de $\mathbb{Z}$, k est générateur de $\mathbb{Z}$ si et seulement si $1 \in \langle k \rangle$, c'est-à-dire si et seulement s'il existe $u \in \mathbb{Z}$ tel que $1 = ku$, ce qui n'arrive que pour $k = \pm 1$. De la même façon, on a la suite d'équivalences :

$$\begin{aligned} \langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \bar{1} \in \langle \bar{k} \rangle \\ &\Leftrightarrow \exists u \in \mathbb{Z} : \bar{1} = u\bar{k} \\ &\Leftrightarrow \exists u, v \in \mathbb{Z} : 1 = uk + vn \\ &\Leftrightarrow k \wedge n = 1, \end{aligned}$$

la dernière équivalence provenant du théorème de Bézout. □

Morphismes

Commençons par une remarque aussi facile qu'utile : si G et H sont deux groupes, G étant monogène engendré par x et $\alpha, \beta : \mathrm{G} \to \mathrm{H}$ sont deux morphismes prenant la même valeur sur x, alors ils coïncident sur tous les éléments de la forme x^k, c'est-à-dire sur tout le groupe G et $\alpha = \beta$. Autrement dit, un morphisme est déterminé par sa valeur sur un générateur. [3]

Proposition. Soit G un groupe. On a

$$\begin{aligned} \mathrm{Hom}(\mathbb{Z}, \mathrm{G}) &= \left\{ \varphi_a \,\middle|\, a \in \mathrm{G} \right\} \\ \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) &= \left\{ \psi_a^{(n)} \,\middle|\, a \in \mathrm{G}, a^n = 1 \right\}. \end{aligned}$$

Preuve. Les $\varphi_a : \mathbb{Z} \to \mathrm{G}$ sont bien des morphismes et, si $\chi : \mathbb{Z} \to \mathrm{G}$ est un morphisme, χ et $\varphi_{\chi(1)}$ sont des morphismes coïncidant sur 1 donc, d'après la remarque, $\chi = \varphi_{\chi(1)}$.

De même, si $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{G}$ est un morphisme, soit $a = \chi(\bar{1})$. On a $a^n = \chi(\bar{1})^n = \chi(n\bar{1}) = \chi(\bar{0}) = 1$ donc $\psi_a^{(n)}$ est bien définie. C'est alors un morphisme coïncidant avec χ sur $\bar{1}$, et $\chi = \psi_a^{(n)}$. □

3. Notons que le même résultat serait vrai, *mutatis mutandis*, dans un cadre plus général : deux morphismes coïncidant sur une partie coïncident sur le sous-groupe engendré par cette partie.

En particulier, $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$, car 0 est le seul $a \in \mathbb{Z}$ tel que $na = 0$. La détermination de $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ est plus subtile : il faut déterminer tous les éléments $\bar{k}$ de $\mathbb{Z}/m\mathbb{Z}$ tels que $n\bar{k} = 0$, c'est-à-dire tous les éléments de $\mathbb{Z}/m\mathbb{Z}$ dont l'ordre divise n.

On va donc déterminer plus précisément cet ensemble $\left\{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \,\middle|\, n\bar{k} = \bar{0}\right\}$ qui est souvent noté $\mathbb{Z}/m\mathbb{Z}[n]$. On peut d'abord remarquer que, parce que le groupe est abélien, cet ensemble est un sous-groupe de $\mathbb{Z}/m\mathbb{Z}$. En fait, en posant $d = m \wedge n$, on va démontrer que cet ensemble n'est rien d'autre que le sous-groupe de cardinal d de $\mathbb{Z}/m\mathbb{Z}$, c'est-à-dire le sous-groupe H engendré par $\overline{n/d}$.

Tout d'abord, H est inclus dans $\mathbb{Z}/m\mathbb{Z}[n]$: tout élément de H a un ordre divisant d, donc *a fortiori* divisant n. Mais $\mathbb{Z}/m\mathbb{Z}[n]$ ne peut pas être plus grand que H : puisque c'est un sous-groupe de $\mathbb{Z}/m\mathbb{Z}$, il est cyclique, donc son cardinal est égal à l'ordre de ses générateurs. Or cet ordre est par définition un diviseur de n et de m, donc un diviseur de d. Ainsi, $\mathbb{Z}/m\mathbb{Z}[n]$ a au plus d éléments, et il est donc égal à H.

Pour la proposition suivante, on convient de noter [4] $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ tels que k et n sont premiers entre eux (autrement dit, tels que $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$).

Proposition. $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, x \mapsto -x\}$. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \left\{\psi_a^{(n)} \,\middle|\, a \in (\mathbb{Z}/n\mathbb{Z})^\times\right\}$.

Preuve. On a déjà $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) = \left\{\varphi_a \,\middle|\, a \in \mathbb{Z}\right\}$ et $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \left\{\psi_a^{(n)} \,\middle|\, a \in \mathbb{Z}/n\mathbb{Z}\right\}$. Il reste à déterminer lesquels de ces morphismes sont des isomorphismes.

On a vu qu'en général, l'image par un morphisme de $\langle g \rangle$ n'est rien d'autre que le sous-groupe engendré par l'image de g. Pour que φ_a (resp. $\psi_a^{(n)}$) soit surjectif, il faut et il suffit donc que a soit un générateur, c'est-à-dire que $\varphi_a \in \{\mathrm{id}, x \mapsto -x\}$ (resp. $a \in (\mathbb{Z}/n\mathbb{Z})^\times$).

Réciproquement, dans ce cas, on a affaire à un isomorphisme : cela est immédiat dans le cas de $\mathbb{Z}$, et cela provient pour $\mathbb{Z}/n\mathbb{Z}$ du fait qu'une application surjective entre deux ensembles finis de même cardinal est automatiquement injective. □

4. Cette notation étrange provient du fait qu'en général, si A est un anneau, on note $\mathrm{A}^\times$ les éléments de A qui admettent un inverse pour la multiplication. Muni de la multiplication, c'est alors un groupe que l'on appelle le *groupe des unités de l'anneau*. Ici, cela correspond bien aux éléments premiers avec n, d'après le théorème de Bézout.