GÉNÉRATEURS DE $\mathcal{S}_n$

Référence : Combes, Algèbre et géométrie.

Leçons possibles :
101 : Groupe opérant sur un ensemble. Exemples et applications.
104 : Groupes finis. Exemples et applications.
105 : Groupe des permutations d'un ensemble fini. Applications.
108 : Exemples de parties génératrices d'un groupe. Applications.

Théorème 1. *Toute permutation $s \in \mathcal{S}_n$ est un produit de transpositions.*

Proposition 2. *Toute permutation $s \in \mathcal{S}_n$ s'écrit de manière unique (modulo l'ordre des termes) comme un produit de cycles disjoints*

$$s = c_1 c_2 \dots c_p.$$

L'ordre de s est le ppcm des ordres de c_1, c_2, …, c_p.

Proposition 3. *Soient G un groupe et $g \in G$. L'application $f : k \mapsto a^k$ est un homomorphisme de $\mathbb{Z}$ sur le sous-groupe $\langle a \rangle$ engendré par a.*

Si f est injectif, alors $\langle a \rangle$ est isomorphe à $\mathbb{Z}$.

Si f n'est pas injectif, alors $\langle a \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$ est le plus petit entier non nul tel que $a^n = e$. Dans ce cas, les entiers k tels que $a^k = e$ sont les multiples de n et $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$.

Proposition 4. *Les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$.*

Démonstration. Notons que $0 \in n\mathbb{Z}$. Soient g, g' dans $n\mathbb{Z}$, *i.e.* $g = nk$ et $g' = nk'$ avec k et k dans $\mathbb{Z}$. Ainsi $g - g' = n(k - k')$ appartient à $n\mathbb{Z}$. Il en résulte que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Réciproquement soit G un sous-groupe de $\mathbb{Z}$. Si G est réduit à $\{0\}$, alors $G = 0\mathbb{Z}$. Supposons désormais que $G \neq \{0\}$; alors il existe $g \neq 0$ dans G. Remarquons que $-g \in G$ donc $G \cap \mathbb{N}^* \neq \emptyset$. Soit n le plus petit élément de $G \cap \mathbb{N}^*$. Pour tout $k \in \mathbb{N}$ on a

$$nk = \underbrace{n + n + \dots + n}_{k \text{ fois}} \in G$$

et $n(-k) = -(nk) \in G$. Ainsi $n\mathbb{Z} \subset G$. Soit $g \in G$ positif. La division de g par n conduit à $g = nq + r$ avec $0 \leq r < n$ et $q \in \mathbb{N}$. Il en résulte que

$$r = g - \underbrace{n + n + \ldots + n}_{q \text{ fois}}$$

appartient à G. Supposons r non nul : alors n n'est pas le plus petit élément de $G \cap \mathbb{N}$: contradiction. Par suite $r = 0$ et $g = nq \in n\mathbb{Z}$. Si $g \in G$ est négatif, alors $-g \in G$ est positif et appartient donc à $n\mathbb{Z}$. Il s'en suit que $G \subset n\mathbb{Z}$ et donc $G = n\mathbb{Z}$. □

Démonstration de la Proposition 3. L'application $f_0 \colon \mathbb{N} \to \langle a \rangle$, $k \mapsto a^k$ vérifie

$$\forall\, k \in \mathbb{N} \qquad \forall\, k' \in \mathbb{N} \qquad f_0(k + k') = a^{k+k'} = a^k a^{k'} = f_0(k) f_0(k').$$

La propriété universelle du symétrisé $\mathbb{Z}$ de $\mathbb{N}$ permet de prolonger f_0 en un homomorphisme f de $\mathbb{Z}$ dans $\langle a \rangle$. Pour $k = -|k| < 0$, on a $f(-|k|) = f(|k|)^{-1} = (a^{|k|})^{-1} = a^k$. Par suite $\mathrm{im} f = \{a^k \,|\, k \in \mathbb{Z}\} = \langle a \rangle$.

D'après la Proposition 4 il existe $n \in \mathbb{N}$ tel que $\ker f = n\mathbb{Z}$. Si $n = 0$, alors f est injective ; c'est un isomorphisme f de $\mathbb{Z}$ dans $\langle a \rangle$. Si n est non nul, le théorème d'isomorphisme assure l'existence d'un isomorphisme $\overline{f}$ entre $\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z}$ et $\langle a \rangle$. Par définition le noyau de f est l'ensemble des $k \in \mathbb{Z}$ tels que $a^k = e$, c'est-à-dire l'ensemble $n\mathbb{Z}$ des multiples de n. Puisque 0, 1, …, $n-1$ sont des représentants des n classes modulo $n\mathbb{Z}$ leurs images $e = a^0$, a, a^2, …, a^{n-1} par $\overline{f}$ sont les éléments de $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f) = \langle a \rangle$. □

Proposition 5. *Soit E un ensemble. Soit G un groupe. Considérons une action à gauche de G sur E.*

(i) La relation

$$x \mathcal{R} y \iff (\exists\, g \in G \quad g \cdot x = y)$$

est une relation d'équivalence sur E.

(ii) Soit $x \in E$; alors

$$G_x = \big\{ g \in G \,|\, g \cdot x = x \big\}$$

est un sous-groupe de G.

(iii) Soit $x \in E$, soit $g_0 \in G$ et soit $y = g_0 \cdot x$. Alors

$$G_y = g_0 G_x g_0^{-1} \qquad\qquad \big\{ g \in G \,|\, g \cdot x = y \big\} = g_0 G_x$$

Démonstration de la Proposition 5. (i) Pour tout $x \in E$ on a $x \mathcal{R} x$ car $e \cdot x = x$; la relation $\mathcal{R}$ est donc réflexive. Si $x \mathcal{R} y$ alors il existe $g \in G$ tel que $g \cdot x = y$ d'où $x = g^{-1} \cdot y$, *i.e.* $y \mathcal{R} x$. Ainsi $\mathcal{R}$ est symétrique. Enfin elle est transitive car

$$(g \cdot x = y \text{ et } g' \cdot y = z) \Rightarrow g' g \cdot x = z$$

(ii)

(iii) Pour tout g dans G on a d'une part

$$\begin{aligned} g \in G_y &\iff g \cdot (g_0 \cdot x) = g_0 \cdot x \\ &\iff (g_0^{-1} g g_0) \cdot x = x \\ &\iff g_0^{-1} g g_0 \in G_x \\ &\iff g \in g_0 G_x g_0^{-1} \end{aligned}$$

d'autre part

$$\begin{aligned} g \in G_y &\iff g \cdot x = y \\ &\iff g \cdot x = g_0 \cdot x \\ &\iff g_0^{-1} g \cdot x = x \\ &\iff g_0^{-1} g \in G_x \\ &\iff g \in g_0 G_x \end{aligned}$$

□

Démonstration de la Proposition 2. La Proposition 4 assure que $k \mapsto s^k$ est un homomorphisme du groupe additif $\mathbb{Z}$ dans $\mathcal{S}_n$. C'est une action de $\mathbb{Z}$ sur l'ensemble $E = \{1, 2, \ldots, n\}$. Soient $\mathcal{O}_1$, $\mathcal{O}_2$, …, $\mathcal{O}_p$ les orbites qui ne sont pas réduites à un point, *i.e.* les orbites des éléments du support de s. Soit i_1 dans $\mathcal{O}_1$. Son stabilisateur est un sous-groupe de $\mathbb{Z}$ donc de la forme $k\mathbb{Z}$ (Proposition 4). Les éléments de $\mathcal{O}_1$ sont

$$i_1,\ i_2 = s(i_1),\ i_3 = s(i_2) = s^2(i_1),\ \ldots,\ i_k = s(i_{k-1}) = s^{k-1}(i_1).$$

D'après la Proposition 5 iii) ces éléments sont bijectivement associés aux classes de $\mathbb{Z}$ modulo le stabilisateur $k\mathbb{Z}$ et sont donc distincts. On a $s^k(i_1) = i_1$. L'action de s sur l'orbite $\mathcal{O}_1$ est la même que celle du cycle $c_1 = (i_1\ i_2\ \ldots\ i_k)$. De même il existe des cycles $c_2, c_3, \ldots, c_p$ ayant pour supports les orbites $\mathcal{O}_2$, $\mathcal{O}_3$, …, $\mathcal{O}_p$ ayant la même action que s sur ces orbites. Les cycles c_1, c_2, …, c_p commutent car ils sont disjoints et $(c_1 c_2 \ldots c_p)(i) = s(i)$ pour tout point i du support $\bigcup_{m=1}^{p} \mathcal{O}_m$ de s. Les autres éléments de E sont fixes par s et $c_1 c_2 \ldots c_p$ donc $s = c_1 c_2 \ldots c_p$.

Montrons l'unicité (modulo l'ordre des cycles) de l'expression $s = c_1 c_2 \ldots c_p$ par récurrence sur p. Si $p = 0$, *i.e.* si $s = \mathrm{id}$, l'unicité est évidente. Soit $p \geq 1$. Supposons que les permutations pouvant s'exprimer comme produit de moins de p cycles disjoints ont une écriture unique (modulo l'ordre des cycles). Considérons une permutation s qui est le produit de p cycles disjoints :

$$s = c_1 c_2 \ldots c_p$$

Soit $s = c'_1 c'_2 \ldots c'_q$ une autre décomposition de s en cycles disjoints. Soit i un élément du support $\mathcal{O}_1$ de c_1. Il appartient au support d'un des cycles c'_j et à un seul. Quitte à réindicer les c'_j on peut supposer que i appartient au support de c'_1. Pour tout r dans $\mathbb{Z}$ on a

$$s^r(i) = c_1^r(i) = {c'_1}^r(i).$$

Ainsi $c_1 = c'_1$. Par conséquent $c_1 c_2 \ldots c_p = c'_1 c'_2 \ldots c'_q$ entraîne $c_2 c_3 \ldots c_p = c'_2 c'_3 \ldots c'_q$. D'après l'hypothèse de récurrence on obtient $p = q$ et $\{c_2, c_3, \ldots, c_p\} = \{c'_2, c'_3, \ldots, c'_p\}$.

Comme les cycles commutent on a pour tout entier n

$$s^n = c_1^n c_2^n \dots c_p^n$$

Les supports des c_i étant disjoints, $s^n = \mathrm{id}$ si et seulement si $(c_1^n, c_2^n, \dots, c_p^n) = (\mathrm{id}, \mathrm{id}, \dots, \mathrm{id})$, *i.e.* si et seulement si n est multiple commun des ordres $k_1, k_2, \dots, k_p$ de $c_1, c_2, \dots, c_p$. Le plus petit entier strictement positif n tel que $s^n = \mathrm{id}$ est donc $\mathrm{ppcm}(k_1, k_2, \dots, k_p)$. □

Démonstration du Théorème 1. D'après la Proposition 2 il suffit de montrer que tout cycle $(i_1\ i_2\ \dots\ i_p)$ est un produit de transpositions. Montrons par récurrence sur la longueur p du cycle que

$$(i_1\ i_2\ \dots\ i_p) = (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p).$$

La formule est vraie pour $p = 2$.

Supposons que $p > 2$ et que la formule soit vraie pour $p-1$, *i.e.*

$$(i_1\ i_2\ \dots\ i_{p-1}) = (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_{p-1});$$

alors

$$(i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p) = (i_1\ i_2\ \dots\ i_{p-1})(i_{p-1}\ i_p) = (i_1\ i_2\ \dots\ i_p).$$

□