Exemples de parties génératrices de groupes

Définition du groupe dérivé : Si G est un groupe, on note $D(G)$ le sous-groupe de G engendré par les commutateurs $[x,y] := xyx^{-1}y^{-1}$, $x, y \in G$. C'est le plus petit sous-groupe N distingué dans G tel que G/N soit abélien.

Exemples à connaître : $D(S_n) = A_n$, $D(A_n) = A_n$ si $n \geq 5$ car A_n est simple dans ce cas et $D(A_4) = K$ le sous-groupe $\{1, (12)(34), (13)(24), (14)(23)\}$.

Exercice 1 Soit D_4 le groupe diédral d'ordre 8. Alors $\mathrm{Aut}D_4 \simeq D_4$.

Indication : $D_4 = \langle r, s\rangle$ avec $r^4 = 1$, $s^2 = 1$, $srs = r^{-1}$. On vérifie facilement que $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}D_4$, $(a, \epsilon) \mapsto \varphi_{a,\epsilon} : D_4 \to D_4$, $r \mapsto r^{(-1)^\epsilon}$, $s \mapsto r^a s$ est un isomorphisme de groupes.

Définition du groupe libre : Soit A un ensemble. On note A^{-1} un ensemble disjoint de A et en bijection avec A. On note $A \to A^{-1}$, $a \mapsto a^{-1}$ une bijection et on posera $(a^{-1})^{-1} := a$ si $a \in A$. On note $M(A)$ l'ensemble des mots en $A \cup A^{-1}$ *i.e.* l'ensemble des suites finies $x_1...x_n$ où $x_i \in A \cup A^{-1}$ et $n \geq 0$ (on notera 1 le mot vide (quand $n = 0$)). Le nombre n est la longueur du mot. On dit qu'un mot $x_1...x_n$ est réduit si pour tout i, $x_i \neq x_{i+1}^{-1}$. Si m_1 et m_2 sont des mots de longueur n_1 et n_2, le mot $m_1.m_2$ est de longueur $n_1 + n_2$. On dit que deux mots m et m' sont adjacents s'il existe des mots u et v, un élément $x \in A \cup A^{-1}$ tels que $\{m, m'\} = \{uxx^{-1}v, uv\}$. On dit que deux mots m, m' sont équivalents s'il existe des mots $t_0, ..., t_k$ tels que t_i et t_{i+1} sont adjacents pour tout i et $m = t_0, m' = t_n$. C'est une relation d'équivalence notée $\sim$. On note $L(A) := M(A)/\sim$. On munit cet ensemble de la loi suivante : $[m] * [m'] := [m.m']$. C'est bien défini et $(L(A), *)$ est un groupe : le groupe libre engendré par A. L'application $A \to L(A)$, $x \mapsto [x]$ est injective. Propriété universelle : Si $f : A \to G$ est une application vers un groupe G alors, il existe un unique morphisme $\overline{f} : L(A) \to G$ qui prolonge f.

Présentation de groupes : Soit A un ensemble et R une partie de $L(A)$. On note $\langle A|R\rangle := L(A)/N$ où N est le plus petit sous-groupe distingué de $L(A)$ contenant R.

Propriété universelle :

si $f : A \to G$ est une application vers un groupe. Alors si $R \subseteq \ker f$, il existe un unique morphisme de groupes $\overline{f} : \langle A|R\rangle \to G$ tel que $\overline{f}(x \bmod N) = f(x)$ pour tout $x \in A$.

Si $R = \{r_1, ..., r_n\}$, on note parfois : $\langle A, R\rangle = \langle A|r_1 = ... = r_n = 1\rangle$. *cf.* [1] pour plus de détails.

Exemples de présentations :

$D_n = \langle r, s \ : \ r^n, s^2\rangle$, $S_n = \langle s_1, ...s_{n-1} \ : \ s_i^2, (s_i s_{i+1})^3, (s_i s_j)^2 \text{ si } j \geq i+2\rangle$.

Ce n'est pas absolument nécessaire mais cela vaut le coup de mentionner les présentations de groupe et la notion de groupe libre mais seulement si on est à l'aise avec.

Développements possibles :

i) Simplicité de $\mathrm{SO}_3(\mathbb{R})$ (utilise que toute rotation est produit de renversements (=rotation d'angle π). *cf.* [3]

ii) Simplicité de $\mathrm{PSL}_n(\mathbb{K})$ si $n \geq 3$ ou $n = 2$ et $|\mathbb{K}| \geq 4$ (*cf.* [2]) Attention $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ et $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq A_4$ ne sont pas simples.

iii) La structure des groupes abéliens de type fini : *cf.* [3].

Théorème 0.1 *Si G est un groupe abélien de type fini, alors il existe $r \geq 0$ et des entiers $1 < d_1|...|d_k$ tels que :*

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_k\mathbb{Z} \ .$$

De plus r et les d_i sont uniquement déterminés par G.

Ce n'est pas trop long si on s'y prend bien et si on admet le résultat des réductions des matrices à coefficients entiers : si $A \in \mathscr{M}_{p,q}(\mathbb{Z})$ alors $A =$ PDQ où $P \in \mathrm{GL}_p(\mathbb{Z})$, $Q \in \mathrm{GL}_q(\mathbb{Z})$, $D =$

$$\left(\begin{array}{cccccc|c} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & d_1 & & & \\ & & & & \ddots & & \\ & & & & & d_k & \\ \hline & & & & & & 0 \end{array}\right)$$

où $1 < d_1|...|d_k$ sont des entiers. Point clé de la démonstration : si $M \leq \mathbb{Z}^n$ sous-groupe, alors M est un $\mathbb{Z}-$module libre engendré par moins de n éléments.

En effet, on raisonne par récurrence sur n. Si $n = 1$ c'est facile. Si $n > 1$, alors on peut trouver, par hypothèse de récurrence, une base de $M \cap \mathbb{Z}^{n-1} \oplus 0 : f_1, ..., f_s$ avec $s \leq n-1$. De plus, l'ensemble $\{\lambda \in \mathbb{Z} : {}^{\exists} x \in \mathbb{Z}^{n-1}, (x, \lambda) \in M\}$ est un sous-groupe de $\mathbb{Z}$ donc engendré par un entier $d \in \mathbb{Z}$. Si $d = 0$, $M \subseteq \mathbb{Z}^{n-1} \oplus 0$ et on a terminé. Sinon soit $f \in M$ dont le dernier coefficient est d. Il est clair que $\mathbb{Z}f_1 \oplus ... \oplus \mathbb{Z}f_s \oplus \mathbb{Z}f = M$.

On en déduit que si M est un $\mathbb{Z}-$module de type fini, il existe un morphisme surjectif $\mathbb{Z}^n \to M$. Notons K le noyau. Comme $K \leq \mathbb{Z}^n$,

K est un $\mathbb{Z}-$module libre de rang $r \leq n$. On peut donc trouver un morphisme $f : \mathbb{Z}^r \to \mathbb{Z}^n$ tel que $\mathbb{Z}^n/f(\mathbb{Z}^r) \simeq M$. Soit A la matrice de f dans les bases canoniques de $\mathbb{Z}^r$ et $\mathbb{Z}^n$. On réduit la matrice $A = PDQ$ où $D =$ et on trouve $M \simeq \mathbb{Z}^n/f(\mathbb{Z}^r) \simeq M/D(\mathbb{Z}^r) \simeq \mathbb{Z}^n/\mathbb{Z} \oplus ... \oplus \mathbb{Z} \oplus d_1\mathbb{Z} \oplus ... \oplus d_k\mathbb{Z} \simeq \mathbb{Z}^s \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_k\mathbb{Z}$ et $d_1|...|d_k$ qui conviennent s avec bien entendu : $s = n - \operatorname{rg}(A)$.

Démonstration de l'unicité : si $G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_k\mathbb{Z} \simeq \mathbb{Z}^{r'} \oplus \mathbb{Z}/d'_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d'_{k'}\mathbb{Z}$ avec des entiers r, r', $d_1|...|d_k$ et $d'_1|...|d'_{k'}$. Posons G_t le sous-groupe des éléments de torsion de G : $G_t = \{x \in G : {}^{\exists}d > 0,\ dx = 0\}$. On a alors $G/G_t \simeq \mathbb{Z}^r \simeq \mathbb{Z}^{r'}$. Donc $r = r'$ (c'est par exemple la dimension du $\mathbb{Z}/p\mathbb{Z}-$espace vectoriel $(G/G_t)/p(G/G_t)$ pour n'importe quel p premier).

On a aussi $G_t \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_k\mathbb{Z} \simeq \mathbb{Z}/d'_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d'_{k'}\mathbb{Z}$. Donc $(d_k) = (d'_{k'}) = \operatorname{Ann}(G_t) = \{k \in \mathbb{Z} : kG_t = 0\}$. Donc $d_k = d'_{k'}$. Comme $d_1|...|d_k$, $d_{k-1}G_t \simeq d_{k-1}\mathbb{Z}/d_k\mathbb{Z} \simeq d_{k-1}\mathbb{Z}/d'_1\mathbb{Z} \oplus ... \oplus d_{k-1}\mathbb{Z}/d'_{k'}\mathbb{Z}$. Si on compare les cardinaux, on voit que :

$$d_{k-1}\mathbb{Z}/d'_1\mathbb{Z} \oplus ... \oplus d_{k-1}\mathbb{Z}/d'_{k'-1}\mathbb{Z} = 0$$

en particulier, $d'_{k'-1}|d_{k-1}$. De même $d_{k-1}|d'_{k'-1}$ et $d_{k-1} = d'_{k'-1}$. On peut continuer et on voit par récurrence que $k = k'$ et $d_i = d'_i$ pour tout i.

iv) Une *réflexion orthogonale* r est un élément de $O_n(\mathbb{R})$ tel que $\dim\ker r - I_n = n - 1$; un *retournement (ou renversement)* est une rotation $r \in \mathrm{SO}_n(\mathbb{R})$ telle que $\dim\ker r - I_n = n - 2$ et $\dim\ker r + I_n = 2$.

Théorème 0.2 *Les réflexions orthogonales engendrent $O_n(\mathbb{R})$ et les retournements engendrent $\mathrm{SO}_n(\mathbb{R})$. De plus tout $f \in O_n(\mathbb{R})$ peut se décomposer en produit de $n - \dim\ker(f - I_n)$ réflexions mais non moins. Toute rotation $r \in \mathrm{SO}_n(\mathbb{R})$ peut s'écrire comme produit de $n-\dim\ker(r-I_n)$ (qui est pair) retournements mais non moins.*

Remarque importante : Avec ce théorème on peut ajouter l'application suivante.

Soit $\sigma \in S_n$, on décompose $\sigma = c_1...c_r$ en produit de cycles à supports disjoints alors σ (on compte tous les cycles, y compris ceux de longueur 1, *par exemple pour une transposition,* $r = n - 1$). Alors σ peut se décomposer en un produit de $n - r$ transpositions mais non moins.

Par exemple : $(12...n) = (12)(23)...(n - 1n)$ *est un produit de* $n - 1$ *transpositions mais non moins ...*

En effet, une permutation $\sigma \in S_n$ peut s'identifier à sa matrice $M_\sigma = (\delta_{i,\sigma(j)})_{1\leq i,j\leq n} \in O_n(\mathbb{R})$. Notons e_i, $1 \leq i \leq n$, les vecteurs de la base

canonique de $\mathbb{R}^n$. Si $c = (j_1, ..., j_l)$ est un cycle de longueur l, notons $v_c := e_{j_1} + ... + e_{j_l} \in \mathbb{R}^n$. Il est facile de voir que le vecteur v_c est invariant par c et que si $\sigma = c_1...c_r$ est la décomposition de σ en cycles à supports disjoints, alors $e_{c_1}, ..., e_{c_r}$ forment une base de $\ker M_\sigma - I_n$. On en déduit que $n - \dim \ker(M_\sigma - I_n) = n - r$. De plus on en déduit aussi qu'une transposition correspond à une réflexion orthogonale ...

Références

[1] D. Guin et Th. Hausberger. *Algebre I.* Collection enseignement SUP MATH. EDP sciences, 2008.

[2] S. Lang. *Algebre.* Dunod, 2014.

[3] E. B. Vinberg. *A course in algebra*, volume 56 of *Graduate text in mathematics.* American mathematical society, 2003.