108. Exemples de parties génératrices d'un groupe : indications de solutions

1. a) Oui, r est unique, comme vu dans la leçon. Une façon de le retrouver rapidement est de constater que dans $\mathbf{Z}^n$, on a n éléments indépendants du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}^n$ (par exemple les éléments de la base canonique), tandis que si $m < n$, toute famille de n éléments de $\mathbf{Z}^m$ est liée dans $\mathbf{Q}^m$, donc aussi liée dans $\mathbf{Z}^m$ en chassant les dénominateurs.

b) Comme le groupe abélien A admet une partie génératrice finie (disons de cardinal m), il est isomorphe au quotient de $\mathbf{Z}^m$ par un certain sous-groupe I. Or tout sous-groupe de $\mathbf{Z}^m/I$ est de la forme H/I, où H est un sous-groupe de $\mathbf{Z}^m$ qui contient I. Le théorème vu dans la leçon dit que H est alors isomorphe à un certain $\mathbf{Z}^r$ (avec $r \leq m$), donc H/I est engendré par r éléments puisque c'est le cas de H.

c) L'hypothèse implique qu'il existe une matrice A, inversible dans $M_n(\mathbf{Z})$, et dont le premier vecteur colonne est a (on prend pour A la matrice qui envoie la base canonique de $\mathbf{Z}^n$ sur une base dont le premier vecteur est a). Si $(c_1, ..., c_n)$ est la première ligne de A^{-1}, alors on obtient $\sum_{i=1}^n c_i a_i = 1$, ce qui donne le résultat.

d) Par Bezout, il existe $(c_1, ..., c_n)$ dans $\mathbf{Z}^n$ avec $\sum_{i=1}^n c_i a_i = 1$. On définit alors f en envoyant le i-ième vecteur de la base canonique sur c_i, ce qui donne bien $f(a) = 1$. D'après le thórème vu dans la leçon, le noyau N de f admet une base, notons-la $(b_1, ..., b_r)$ et montrons que $(a, b_1, ..., b_r)$ est une base de $\mathbf{Z}^n$. Soit $x \in \mathbf{Z}^n$, posons $f(x) = u \in \mathbf{Z}$, alors $f(x - ua) = 0$, donc $(x - ua) \in N$ se décompose sur la base $(b_1, ..., b_r)$. Si d'autre part $0 = ua + \sum_{i=1}^r \alpha_i b_i$ avec u et les α_i dans $\mathbf{Z}$, on obtient $uf(a) = u = 0$ vu que $\sum_{i=1}^r \alpha_i b_i \in N = \ker f$, puis $\sum_{i=1}^r \alpha_i b_i = 0$ donc tous les α_i sont nuls, étant donné que $(b_1, ..., b_r)$ est une base de N.

2. Soit S une partie génératrice de G. Notons T l'ensemble des éléments de G qui sont dans S ou dont l'inverse est dans S. Pour tout $r \in \mathbf{N}$, notons G_r l'ensemble des éléments g de G de la forme

$$g = x_1 x_2 ... x_r,$$

avec $x_i \in T$ pour tout i (avec la convention habituelle que le produit vide est le neutre de G). Alors, le fait que S engendre G dit que G est la réunion des G_r pour $r \in \mathbf{N}$. Chaque G_r est fini (car T est fini, et le cardinal de G_r est au plus celui de T^r), donc G est (au plus) dénombrable comme union dénombrable d'ensembles finis.

La réciproque est fausse, même pour les groupes abéliens. Par exemple, comme on l'a déjà vu, $(\mathbf{Q}, +)$ n'est pas engendré par une partie finie. De même pour $\mathbf{Z}^{(\mathbf{N})}$ (qui admet une famile libre infinie).

3. a) Le produit se simplifie et donne

$$t_0 a_1 ... a_n t_n^{-1} = t_0 h t_n^{-1}.$$

Par convention $t_0 = 1$; comme par définition t_n est dans T et vérifie $t_n = \tilde{h}$ avec $h \in H$, on obtient que t_n et 1 ont la même classe dans $H \setminus G$, et donc $t_n = 1$ puisqu'on a pris $1 \in T$. Finalement le produit vaut bien h.

b) On sait que t_k est dans T et il vérifie $(t_{k-1} a_k) t_k^{-1} \in H$: en effet il existe, par définition de t_{k-1}, un élément $h \in H$ tel que

$$t_{k-1} = h a_1 ... a_{k-1},$$

d'où $t_{k-1} a_k \in H(a_1 ... a_k)$, qui est bien dans la même classe à droite selon H que t_k par définition de t_k. Ainsi $t_k = \widetilde{t_{k-1} a_k}$.

On remplace alors dans la formule du a) chaque t_i^{-1} par $(\widetilde{t_{i-1} a_i})^{-1}$, ce qui donne que h est produit d'éléments de la forme $ta(\widetilde{ta})^{-1}$ avec $t \in T$ et $a \in S \cup S^{-1}$.

c) Comme $t' = \widetilde{ta}$ et $a = s^{-1}$, l'égalité voulue est équivalente à :

$$t = \widetilde{t's}.$$

Or t est bien dans T et il est dans la même classe à droite selon H que $t's$ car (par définition) $t' \in H(ta)$ d'où $t's \in H(tas) = Ht$. Ceci signifie exactement que $t' = \widetilde{t's}$ comme on voulait.

d) D'après b), tout élément de H est produit d'éléments de la forme $u = ta(\widetilde{ta})^{-1}$ avec $t \in T$ et $a \in S \cup S^{-1}$. Mais si $a \in S^{-1}$, le c) montre que u est l'inverse d'un élément de la forme $t's(\widetilde{t's})^{-1}$ avec $t' \in T$ et $s \in S$. Finalement les éléments de la forme $ta(\widetilde{ta})^{-1}$ avec $t \in T$ et $a \in S$ suffisent donc pour engendrer G.

e) Comme G est engendré par une partie finie, on peut prendre S fini. Si on suppose de plus H d'indice fini dans G, alors T est fini et le d) montre que H est engendré par une partie finie (dont le cardinal est au plus celui de $T \times S$).

4. Traitons par exemple le cas de $\mathrm{SL_n}(\mathbf{R})$ (le cas de $SL_n(\mathbf{C})$ est identique). Soit $M \in \mathrm{SL_n}(\mathbf{R})$, il suffit de relier M à l'identité par un chemin continu à valeurs dans $M \in \mathrm{SL_n}(\mathbf{R})$. Pour $t \in [0,1]$, posons

$$A_t := \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},$$

de sorte que $T := \mathrm{Diag}(I_{n-2}, A_1)$ est la matrice standard de transvection. L'engendrement de $\mathrm{SL_n}(\mathbf{R})$ par les transvections permet alors d'écrire

$$M = M_1 ... M_r,$$

où chaque M_i s'écrit elle-même $M_i = P_i T P_i^{-1}$ avec $P_i \in \mathrm{GL_n}(\mathbf{R})$. Posons $M_i(t) = P_i T_t P_i^{-1}$, avec $T_t := \mathrm{Diag}(I_{n-2}, A_t)$, et définissons

$$M(t) = \prod_{i=1}^{r} M_i(t).$$

On a alors $M(t) \in \mathrm{SL_n}(\mathbf{R})$ avec $M(0) = I_n$ et $M(1) = \prod_{i=1}^{r} M_i = M$ comme on voulait.

On obtient ensuite que $\mathrm{GL_n}(\mathbf{C})$ est connexe comme l'image du connexe $\mathrm{SL_n}(\mathbf{C}) \times \mathbf{C}^*$ par l'application $(M, \lambda) \to \lambda M$ (observer que $\mathbf{C}^*$ est connexe et que $u \mapsto^n$ est surjective de $\mathbf{C}^*$ dans $\mathbf{C}^*$, avec $\det(\lambda M) = \lambda^n \det M$). Le même argument donne que le groupe $\mathrm{GL_n}^+(\mathbf{R})$ des matrices réelles de déterminant > 0 est connexe. Comme il est homéomorphe au groupe $\mathrm{GL_n}^-(\mathbf{R})$ des matrices réelles de déterminant < 0 (en considérant $M \mapsto NM$, où N est une matrice fixée de déterminant -1), on en déduit finalement que $\mathrm{GL_n}^-(\mathbf{R})$ est connexe. Ainsi $\mathrm{GL_n}^-(\mathbf{R})$ et $\mathrm{GL_n}^+(\mathbf{R})$ sont les deux composantes connexes de $\mathrm{GL_n}(\mathbf{R})$.

Enfin, $SO_n(\mathbf{R})$ est connexe : le cas $n = 1$ est trivial; dans le cas $n = 2$, on peut utiliser la réduction d'une rotation du plan et dans le cas $n \geq 3$ l'engendrement par les renversements, la preuve est alors similaire à celle de la connexité de $\mathrm{SL}_n(\mathbf{R})$. On peut aussi utiliser directement la réduction d'une matrice de $O_n(\mathbf{R})$.