108 - Exemples de parties génératrices d'un groupe. Applications.

Version ambitieuse

1 Généralités

Définition 1.1. *Soit G un groupe et $P \subset G$ une partie. Le sous-groupe de G engendré par P est le plus petit sous-groupe (au sens de l'inclusion) de G contenant P. On le note $\langle P \rangle$.*

Remarque 1.2. Ce sous-groupe est bien défini, et il est unique. On dispose en effet de deux caractérisations de $\langle P \rangle$:

1. une description interne : $\langle P \rangle = \{g_1^{\varepsilon_1} \dots g_r^{\varepsilon_r} : g_i \in P, \varepsilon_i = \pm 1, \forall i\}$.
2. une description externe :
$$\langle P \rangle = \bigcap_{\substack{H < G \\ P \subset H}} H\,.$$

Exemples :
- Le sous-groupe de G engendré par l'ensemble vide est réduit à l'élément neutre.
- Si $G = \mathbb{Z}$, on a $\langle \{1\} \rangle = \langle \{-1\} \rangle = \mathbb{Z}$, $\langle \{2\} \rangle = 2\mathbb{Z}$ (entiers pairs), et $\langle \{2;3\} \rangle = \mathbb{Z}$.

Définition 1.3. *Soit G un groupe. Le sous-groupe dérivé de G, noté $D(G)$, est le sous-groupe de G engendré par les commutateurs de G, i.e. les éléments de la forme $[g,h] := g \cdot h \cdot g^{-1} \cdot h^{-1}$.*

Proposition 1.4. *Le sous-groupe $D(G)$ est distingué, et $G^{\mathrm{ab}} := G/D(G)$ est le plus grand quotient abélien de G : pour tout groupe abélien A et tout morphisme $\varphi : G \to A$, il existe un unique morphisme $\overline{\varphi} : G^{\mathrm{ab}} \to A$ tel que $\varphi = \overline{\varphi} \circ \pi$, où $\pi : G \to G^{\mathrm{ab}}$ est la surjection canonique.*

Définition 1.5. *On dit qu'une partie $P \subset G$ est génératrice si $\langle P \rangle = G$.*

Exemples :
- L'ensemble des commutateurs est une partie génératrice de $D(G)$.
- $\{1\}$ et $\{2;3\}$ sont des parties génératrices de $\mathbb{Z}$.
- Soit G un groupe fini, et p le plus petit facteur premier de $|G|$. Alors toute partie de cardinal $> \frac{|G|}{p}$ est génératrice.

Définition 1.6. *Un groupe G est dit de type fini s'il admet une partie génératrice finie.*

Exemples :
- Un groupe fini est de type fini.
- Tout quotient d'un groupe de type fini est de type fini.
- Soit $H \triangleleft G$ un sous-groupe distingué. Si H et G/H sont de type fini, alors G est de type fini.
- Un sous-groupe d'un groupe de type fini n'est pas toujours de type fini. Par exemple, le sous-groupe de $\mathfrak{S}(\mathbb{Z})$ engendré par la transposition $(0\,1)$ et la translation $n \mapsto n+1$ est de type fini, alors que son sous-groupe des permutations de support fini ne l'est pas.
- Q et $\mathbb{R}$ ne sont pas de type fini.

2 Groupes abéliens

2.1 Groupes monogènes

Définition 2.1. *Un groupe G est dit monogène s'il est engendré par un seul élément. Un groupe cyclique est un groupe monogène fini.*

Exemples :
- $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ sont monogènes.
- Un groupe d'ordre premier est cyclique.
- $\mathbb{Z}^2$ n'est pas monogène.

Lemme 2.2. *Soit G un groupe et H un sous-groupe du centre $Z(G)$ de G.*
Si G/H est monogène, alors G est abélien.

Corollaire 2.3. *Soit p un nombre premier. Tout groupe d'ordre p^2 est abélien.*

Proposition 2.4. *Soit G un groupe monogène, muni d'un générateur g_0.*

1. *Si g_0 est d'ordre fini (égal à n), alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*
2. *Si g_0 n'est pas d'ordre fini, alors G est isomorphe à $\mathbb{Z}$.*

Proposition 2.5. *Le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ admet exactement $\varphi(n)$ générateurs. Ces générateurs sont les éléments $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ (avec $k \in \mathbb{Z}$) tels que k est premier avec n.*

Théorème 2.6. ⋆ *Soit K un corps et $G < (K^\times, \cdot)$ un sous-groupe fini. Alors G est cyclique.*

Application : problème du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$, protocoles Diffie-Hellman (partage de secret) et ElGamal (cryptographie).

2.2 Groupes abéliens de type fini

Théorème 2.7. ⋆ *Soit G un groupe abélien de type fini.*
Il existe un unique $r \in \mathbb{N}$ et une unique suite d'entiers positifs $(d_1, \dots, d_s) \in \mathbb{N}^s$ tels que pour tout i, $d_i | d_{i+1}$ et $G \xrightarrow{\sim} \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$.

Corollaire 2.8. *Soit G un groupe abélien de type fini. Soient r et s les entiers donnés par le théorème 2.7. Alors le nombre minimal de générateurs de G est égal à $r+s$.*

Étudions maintenant le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Théorème 2.9. ⋆⋆ *Soit p un nombre premier et $n \geq 1$.*

1. *Si p est impair, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique d'ordre $p^{n-1} \cdot (p-1)$.*
2. *Si $p = 2$, le groupe $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est cyclique d'ordre 2^{n-1} si $n \leq 2$, il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ si $n \geq 3$.*

Corollaire 2.10. *Pour tout $n \geq 1$, le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 1, 2, 4, p^m$ ou $2p^m$, avec p premier impair.*

2.3 D'autres groupes abéliens

Théorème 2.11. *Soit $G < (\mathbb{R}, +)$ un sous-groupe.*
Alors G est dense ou monogène (i.e. de la forme $\mathbb{Z} \cdot \alpha$, pour un $\alpha \in \mathbb{R}$).

Exemple : Soit $x, y \in \mathbb{R}$, $y \neq 0$. Alors le sous-groupe $\langle x, y \rangle = \mathbb{Z} \cdot x + \mathbb{Z} \cdot y$ est dense dans $\mathbb{R}$ si et seulement si $\frac{x}{y} \notin \mathbb{Q}$.

Corollaire 2.12. $\star$ *On note $\mathbb{U} < (\mathbb{C}^\times, \cdot)$ le groupe des nombres complexes de module 1. Soit $G < (\mathbb{U}, \cdot)$.*
Alors G est dense ou il existe $n \in \mathbb{N}$ tel que G est le groupe cyclique $\mathbb{U}_n$ des racines n-ièmes de l'unité. Par exemple, si $\alpha \in \mathbb{R}$, le sous-groupe engendré par $e^{2i\pi\alpha}$ est fini si $\alpha \in \mathbb{Q}$, équiréparti (donc dense) sinon.

3 Exemples de groupes non abéliens

3.1 Groupe symétrique

Théorème 3.1. $\star$ *Le groupe $\mathfrak{S}_n$ est engendré par les cycles ; par les transpositions ; par les transpositions $(1\ i)$, $2 \leq i \leq n$; par les transpositions $(i\ i+1)$, $1 \leq i \leq n-1$; par la transposition $(1\ 2)$ et le cycle $(1\ 2 \dots n)$.*

Le second point permet notamment de définir le morphisme signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$.

Corollaire 3.2. *Soit K un corps, E, F des K-espaces vectoriels et $f : E^n \to F$ une application n-linéaire. Si f est alternée, alors f est antisymétrique.*

Une application géométrique :

Théorème 3.3. $\star$ *On se place dans un espace affine euclidien de dimension 3.*

1. *Le groupe des isométries d'un tétraèdre régulier est isomorphe à $\mathfrak{S}_4$.*
2. *Le groupe des isométries directes d'un cube ou d'un octaèdre est isomorphe à $\mathfrak{S}_4$.*

Une application en théorie des groupes :

Théorème 3.4. $\star\star$ *Pour tout $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.*

Proposition 3.5. *Soit $P \subset \mathfrak{S}_n$ une partie formée de transpositions. Si $\langle P \rangle = \mathfrak{S}_n$, alors $|P| \geq n-1$.*

On rappelle que $\mathfrak{A}_n := \ker(\varepsilon : \mathfrak{S}_n \to \{\pm 1\})$.

Théorème 3.6. *Pour tout $n \geq 1$,*

1. *le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.*
2. *si $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

Corollaire 3.7. *Pour tout $n \geq 1$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$, et si $n \geq 5$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$.*

Corollaire 3.8. $\star$ *Pour tout $n \geq 3$, $n \neq 4$, le groupe $\mathfrak{A}_n$ est simple.*

3.2 Groupe linéaire

Soit K un corps. L'algorithme du pivot de Gauss assure les résultats suivants :

Théorème 3.9. $\star$

1. *Le groupe $\mathrm{SL}_n(K)$ est engendré par les matrices de transvections $I_n + \lambda \cdot E_{i,j}$, $\lambda \in K$ et $1 \leq i < j \leq n$, où $E_{i,j}$ est la matrice dont tous les coefficients sont nuls, sauf le coefficient d'indice (i,j) qui vaut 1.*
2. *Le groupe $\mathrm{GL}_n(K)$ est engendré par les matrices de transvections et les matrices de dilatations $D_i(\lambda) := I_n + (\lambda - 1) \cdot E_{i,i} = \mathrm{diag}(1, \dots, 1, \lambda, 1, \dots, 1)$, $\lambda \in K^\times$ et $1 \leq i \leq n$.*

Théorème 3.10. $\star\star$ *Soit A un anneau euclidien. Alors $\mathrm{SL}_n(A)$ est engendré par les matrices de transvections, et $\mathrm{GL}_n(A)$ est engendré par les matrices de transvections et de dilatations.*

Exemple : $\star\star\star$ Si $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ (anneau principal non euclidien), alors le résultat précédent est faux : il existe une matrice dans $\mathrm{SL}_2(A)$ qui n'est pas produit de matrices de transvections.

Corollaire 3.11. *Les groupes $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{R})^+$, $\mathrm{SL}_n(\mathbb{C})$ et $\mathrm{GL}_n(\mathbb{C})$ sont connexes par arcs.*

Corollaire 3.12 (Frobenius-Zolotarev)**.** $\star$ *Soit $K = \mathbb{F}_q$ un corps fini à q éléments. Si $a \in \mathbb{F}_q^\times$, on note $\left(\frac{a}{q}\right) = 1$ si a est un carré dans K et -1 sinon. On rappelle l'injection naturelle $\iota : \mathrm{GL}_n(\mathbb{F}_q) \to \mathfrak{S}((\mathbb{F}_q)^n)$. Alors pour tout $A \in \mathrm{GL}_n(\mathbb{F}_q)$, $\varepsilon(\iota(A)) = \left(\frac{\det(A)}{q}\right)$.*

Proposition 3.13. *Si $n \geq 3$ (resp. $n \geq 2$), les matrices de transvections sont conjuguées dans $\mathrm{SL}_n(K)$ (resp. $\mathrm{GL}_n(K)$).*

Corollaire 3.14.
1. *Si $n > 2$ ou $|K| \neq 2$, alors $D(\mathrm{GL}_n(K)) = \mathrm{SL}_n(K)$.*
2. *Si $n > 2$ ou $|K| \neq 2, 3$, alors $D(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K)$.*

Théorème 3.15. $\star\star$ *Si $n > 2$ ou $|K| \neq 2, 3$, alors $\mathrm{PSL}_n(K)$ est simple.*

Exemple : $\mathrm{PSL}_3(\mathbb{F}_4)$ et $\mathrm{PSL}_4(\mathbb{F}_2)$ sont simples, de même cardinal 20160, mais non isomorphes.

3.3 Groupe orthogonal

Théorème 3.16. $\star\star\star$ *Soit (E, q) un espace vectoriel de dimension n sur un corps K (de caractéristique différente de 2) muni d'une forme quadratique non dégénérée.*

1. *Si $n \geq 2$, le groupe $\mathbf{O}(q)$ est engendré par les réflexions. Plus précisément, tout élément de $\mathbf{O}(q)$ est produit d'au plus n réflexions. Dans le cas euclidien, tout $u \in \mathbf{O}_n(\mathbb{R})$ est produit de $\mathrm{rg}(u - \mathrm{id})$ réflexions, et ce nombre est minimal.*
2. *Si $n \geq 3$, le groupe $\mathbf{SO}(q)$ est engendré par les renversements. Plus précisément, tout élément de $\mathbf{SO}(q)$ est produit d'au plus n renversements.*

Corollaire 3.17. *Pour tout $n \geq 2$, le groupe $\mathbf{SO}_n(\mathbb{R})$ est connexe par arcs.*

Corollaire 3.18. *Pour tout $n \geq 2$, $D(\mathbf{O}_n(\mathbb{R})) = \mathbf{SO}_n(\mathbb{R})$ et si $n \geq 3$, $D(\mathbf{SO}_n(\mathbb{R})) = \mathbf{SO}_n(\mathbb{R})$.*

Proposition 3.19. *Pour tout $n \geq 3$, les renversements sont conjugués dans $\mathbf{SO}_n(\mathbb{R})$.*

Théorème 3.20. $\star\star$ *Pour tout $n \geq 3$, $n \neq 4$, le groupe $\mathbf{PSO}_n(\mathbb{R})$ est simple.*

Théorème 3.21. ⋆⋆ *Tout automorphisme de* $\mathbf{SO}_3(\mathbb{R})$ *est intérieur.*

Les renversements permettent de paramétrer les rotations de $\mathbb{R}^3$ de façon similaire au paramétrage usuel $\mathbb{U} \xrightarrow{\sim} \mathbf{SO}_2(\mathbb{R})$, et d'étudier les rotations de $\mathbb{R}^4$:

Théorème 3.22. ⋆⋆⋆ *On note G le groupe des quaternions de norme 1. Alors on a un isomorphisme canonique $G/\{\pm 1\} \xrightarrow{\sim} \mathbf{SO}_3(\mathbb{R})$.*

Théorème 3.23. ⋆⋆⋆ *On a un isomorphisme canonique $\mathbf{PSO}_4(\mathbb{R}) \xrightarrow{\sim} \mathbf{SO}_3(\mathbb{R}) \times \mathbf{SO}_3(\mathbb{R})$. En particulier, ce groupe n'est pas simple.*

3.4 Générateurs des p-groupes

Définition 3.24. *Soit G un groupe de type fini. On définit le sous-groupe de Frattini $\phi(G)$ de G comme l'intersection des sous-groupes maximaux de G.*

Proposition 3.25. *Le sous-groupe $\phi(G)$ est caractéristique dans G (donc distingué).*

Proposition 3.26. *Le sous-groupe $\phi(G)$ est exactement l'ensemble des éléments $g \in G$ tels que pour toute partie $P \subset G$, $\langle P \cup \{g\}\rangle = G \implies \langle P\rangle = G$.*

Théorème 3.27. ⋆⋆ *Soit G un p-groupe. Alors $G/\phi(G)$ est le plus grand quotient abélien de G d'exposant p, et $\dim_{\mathbb{F}_p}(G/\phi(G))$ est le cardinal minimal d'une partie génératrice de G.*

4 Étude plus précise des générateurs

4.1 Présentation par générateurs et relations

4.1.1 Groupes libres

Définition 4.1. *Soit X un ensemble. On note X^{-1} un ensemble en bijection avec X, et on note $x \mapsto x^{-1}$ une bijection entre X et X^{-1}. L'ensemble $M(X)$ des mots (finis) sur l'alphabet $X \cup X^{-1}$ est muni de la loi de concaténation des mots. $L(X)$ est le quotient de $M(X)$ par la relation d'équivalence engendrée par : $m \sim m'$ s'il existe $x \in X \cup X^{-1}$, et $a, b \in M(X)$, tels que $m = a \cdot b$ et $m' = a \cdot x \cdot x^{-1} \cdot b$.*

Proposition 4.2. *L'ensemble $L(X)$, muni de la loi de concaténation des mots, est un groupe, appelé groupe libre sur X. Il vérifie la propriété universelle suivante : pour tout groupe G et toute application $\varphi : X \to G$, il existe un unique morphisme de groupes $\widetilde{\varphi} : L(X) \to G$ tel que $\varphi = \widetilde{\varphi} \circ \iota$, où $\iota : X \to L(X)$ est l'injection naturelle. En outre, $L(X)$ est engendré par $\iota(X)$.*

Exemples :
- Le groupe libre sur un générateur est isomorphe à $\mathbb{Z}$.
- Le groupe libre sur deux générateurs est le groupe des mots sur l'alphabet $\{a, b, a^{-1}, b^{-1}\}$, écrits sous leur forme minimale (après simplification de aa^{-1}, $a^{-1}a$, bb^{-1} et $b^{-1}b$).

Exemple : ⋆⋆ Soient $A = \begin{pmatrix} \frac{1}{3} & -2\frac{\sqrt{2}}{3} & 0 \\ 2\frac{\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & -2\frac{\sqrt{2}}{3} \\ 0 & 2\frac{\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}$. Alors le sous-groupe G de $\mathbf{SO}_3(\mathbb{R})$ engendré par A et B est un groupe libre à deux générateurs

Une application de cet exemple :

Théorème 4.3 (Banach-Tarski)**.** ⋆⋆⋆ *Soient $A, B \subset \mathbb{R}^3$ deux parties non vides. Alors il existe des partitions $A = A_1 \cup \cdots \cup A_n$ et $B = B_1 \cup \cdots \cup B_n$, et $g_1, \ldots, g_3$ des isométries directes de $\mathbb{R}^3$, telles que $B_i = g(A_i)$ pour tout i.*

4.1.2 Présentations par générateurs et relations

Définition 4.4. *Soit X un ensemble et $\mathcal{R} \subset L(X)$. Le groupe présenté par générateurs X et relations $\mathcal{R}$ est $\langle X|\mathcal{R}\rangle := L(X)/\langle\mathcal{R}\rangle'$, où $\langle\mathcal{R}\rangle'$ est le sous-groupe distingué engendré par $\mathcal{R}$.*

Proposition 4.5. *Soit G un groupe, $\varphi : X \to G$ une application. Si pour tout $r \in \mathcal{R}$, l'évaluation $\varphi(r)$ du mot r dans G est égale à l'élément neutre, alors il existe un unique morphisme de groupes $\overline{\varphi} : \langle X|\mathcal{R}\rangle \to G$ tel que $\varphi = \overline{\varphi} \circ \iota$. Si $\overline{\varphi}$ est un isomorphisme (en particulier $\varphi(X)$ engendre G), on dit que $\langle X|\mathcal{R}\rangle$ est une présentation de G.*

4.1.3 Quelques exemples

Théorème 4.6. ⋆⋆ *Il y a exactement cinq groupes d'ordre 8, donnés par les présentations :*

$$A_1 = \langle a|a^8\rangle\,,\ A_2 = \langle a, b|a^4, b^2, aba^{-1}b^{-1}\rangle\,,\ A_3 = \langle a, b, c|a^2, b^2, c^2, (ab)^2, (ac)^2, (bc)^2\rangle\,,$$
$$\mathbb{D}_4 = \langle r, s|r^4, s^2, (rs)^2\rangle\,,\ \mathbb{H}_8 = \langle i, j|i^4, i^2j^2, ijij^{-1}\rangle\,.$$

Théorème 4.7. $\mathbf{D}_n = \langle r, s|r^n, s^2, (rs)^2\rangle$.

Le résultat suivant peut permettre de construire un automorphisme extérieur de $\mathfrak{S}_6$.

Théorème 4.8. ⋆⋆

$$\mathfrak{S}_n = \left\langle s_1, \ldots, s_{n-1} \;\middle|\; \begin{array}{l} \forall\, 1 \le i \le n-1\,,\ s_i^2 \\ \forall\, 1 \le i \le n-2\,,\ (s_is_{i+1})^3 \\ \forall\, 1 \le i < j-1 \le n-2\,,\ (s_is_j)^2 \end{array} \right\rangle.$$

En étudiant l'action de $\mathrm{PSL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré, on obtient :

Théorème 4.9. ⋆⋆ $\mathrm{PSL}_2(\mathbb{Z}) = \langle a, b|a^2, b^3\rangle$, *présentation donnée par les matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.*

4.2 Graphe de Cayley et croissance

4.2.1 Définitions

Définition 4.10. *Soit G un groupe muni d'une partie génératrice S, stable par inverse et contenant le neutre e. Le graphe de Cayley de G associé à S est le graphe dont les sommets sont les éléments de G, et deux sommets $g, h \in G$ sont reliés si et seulement si $g \cdot h^{-1} \in S$.*

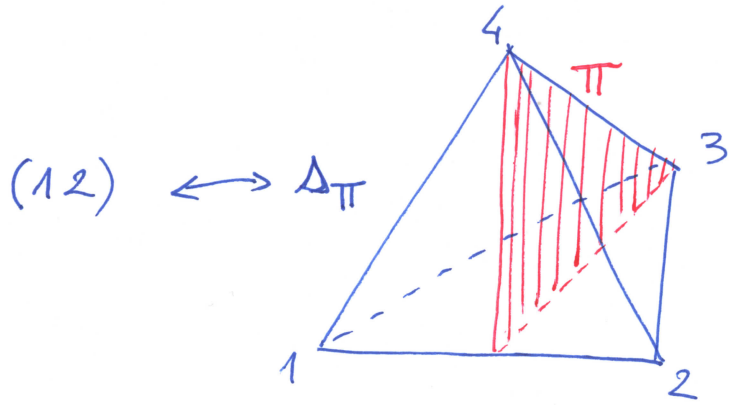
Ce graphe munit G d'une distance, et on note $b(n)$ le cardinal de la boule de centre e et de rayon n. On cherche à relier la géométrie du graphe aux propriétés algébriques du groupe G.

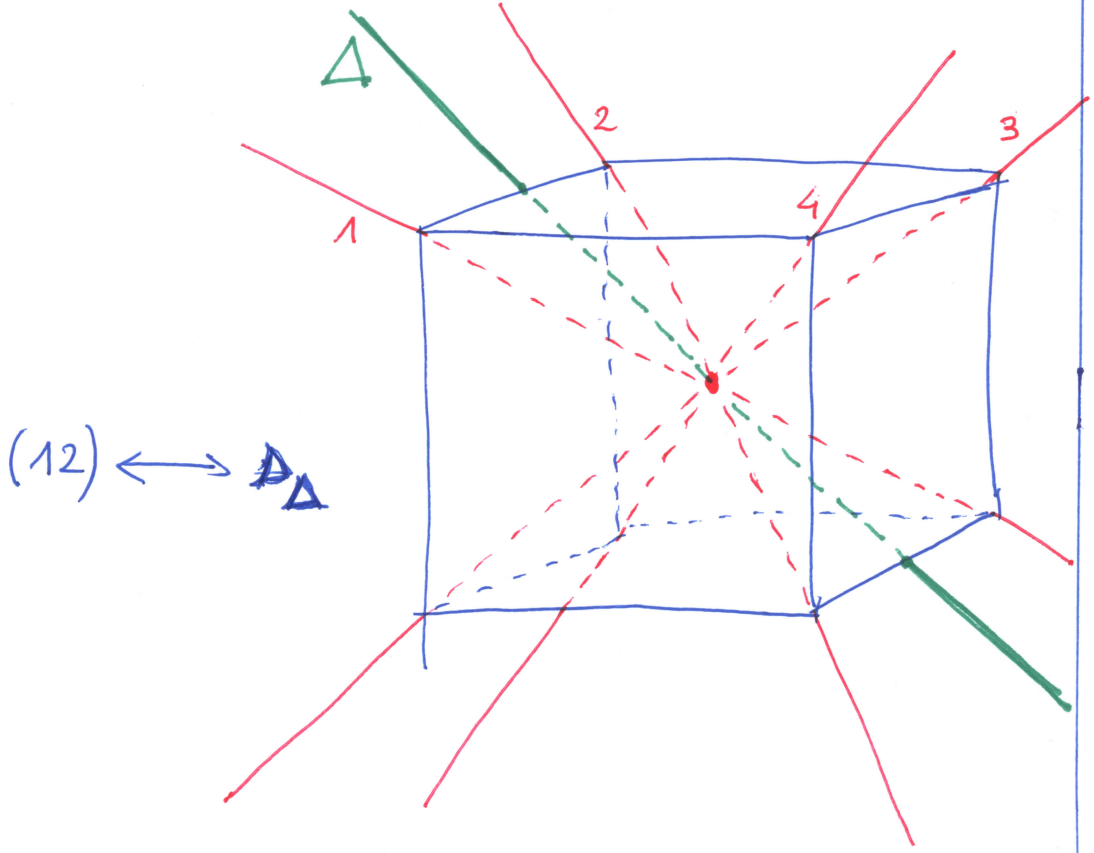
Exemples :
- Si $G = \mathbb{Z}^r$, la suite $b(n)$ est de l'ordre de n^r (croissance polynomiale).
- Si G est libre à r générateurs, la suite $b(n)$ est de l'ordre de r^n (croissance exponentielle).

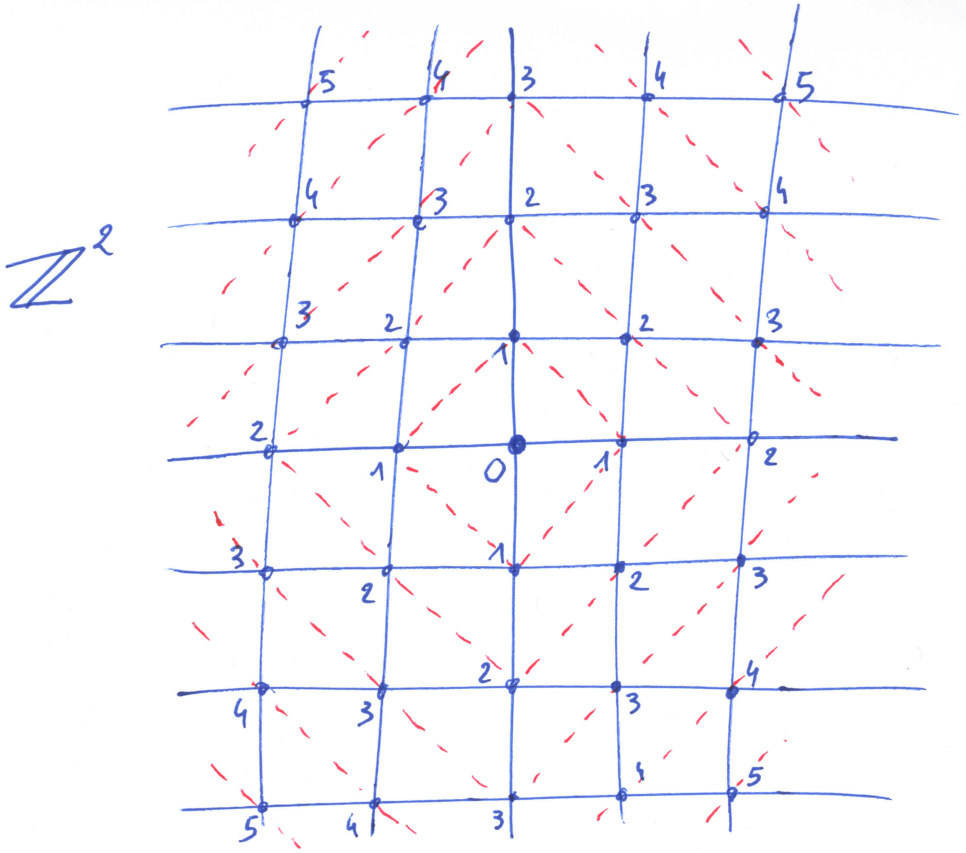
Proposition 4.11. *Il existe $C, D > 0$ telle que $b(n) \le C \cdot D^n$.*

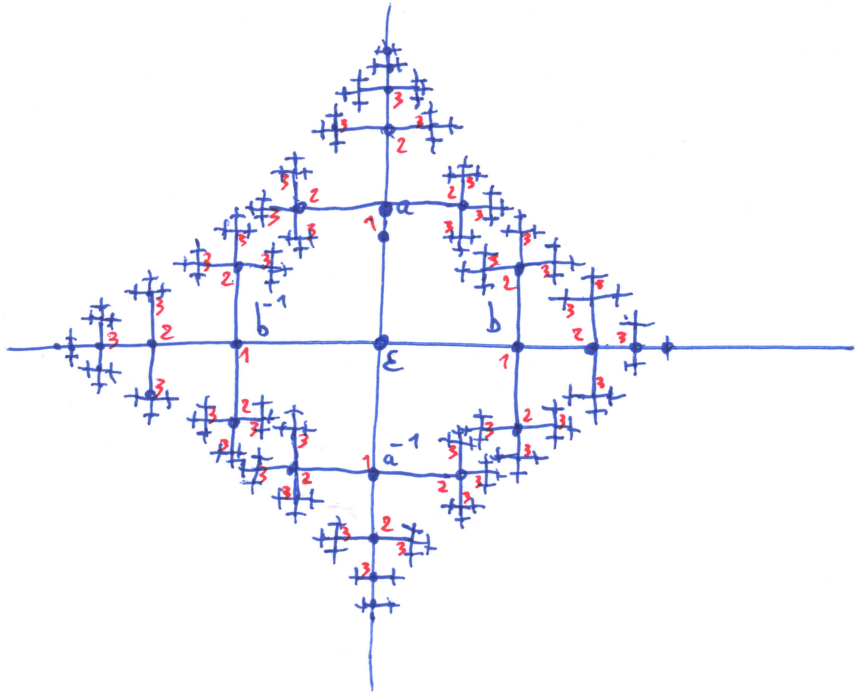
4.2.2 Quelques exemples

Théorème 4.12. ⋆⋆⋆
1. *Si $G = \mathrm{SL}_2(\mathbb{Z})$, alors $b(n)$ est à croissance exponentielle.*
2. *Si G est nilpotent, alors $b(n)$ est à croissance polynomiale.*
3. *Si $G = \mathbb{Z}^2 \rtimes \mathbb{Z}$ (résoluble), via la matrice $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $b(n)$ est à croissance exponentielle.*


(12) ⟷ Δ_π
4
π
3
1
2


(12) ⟷ $\mathcal{D}_\Delta$
Δ
1
2
3
4


$\mathbb{Z}^2$
0


L_2
a
a^{-1}
b
b^{-1}
ε