Rapport de stage (Licence 3)

Fonction de croissance des groupes de type fini

Université de Nantes

Simon Masson

21 Avril – 16 Mai 2014

Table des matières

I Préliminaires et définitions

1 Le groupe spécial linéaire $\mathrm{SL}_2(\mathbb{Z})$

Définition 1 (groupe spécial linéaire)**.** Le groupe spécial linéaire est un sous-groupe de $\mathrm{GL}_2(\mathbb{Z})$. Il contient les matrices de dimension 2 à coefficients dans $\mathbb{Z}$ de déterminant 1.

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

Posons $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On a la proposition suivante :

Proposition. *Le groupe $SL_2(\mathbb{Z})$ est engendré par S et T.*

On étudiera par la suite la croissance du groupe $\mathrm{PSL}_2(\mathbb{Z})$, quotient de $\mathrm{SL}_2(\mathbb{Z})$ par $\{\pm I\}$.

2 Notions de préordre $\preceq$ et relation d'équivalence $\sim$ associée

Soient f, g des suites réelles positives, croissantes à partir d'un certain rang.

Définition 2 (préodre)**.** On dit que $f(N) \preceq g(N)$ s'il existe $A, N_A \in \mathbb{N}^*$ tels que

$$\forall N \geqslant N_A \qquad f(N) \leqslant g(AN)$$

Définition 3 (relation d'équivalence associée à $\preceq$)**.** On dit que $f(N) \sim g(N)$ s'il existe $A, N_A \in \mathbb{N}^*$ tels que

$$\forall N \geqslant N_A \qquad f(N) \leqslant g(AN) \text{ et } g(N) \leqslant f(AN)$$

Proposition.

$$f(N) \preceq g(N) \text{ et } g(N) \preceq f(N) \iff f(N) \sim g(N)$$

Démonstration. Il s'agit de prouver le sens direct. On prend $M := \max(N_A, N_B)$, et alors pour tout $N \geqslant M$, on a $f(N) \leqslant g(AN)$ et $g(N) \leqslant f(BN)$. Donc $f \sim g$. □

3 Longueur, boule et cardinal

Définition 4 (groupe de type fini)**.** On dit qu'un groupe G est de type fini s'il est engendré par une partie finie S.

Définition 5 (longueur)**.** Si $x \in G$, on appelle longueur de x relativement à S l'entier :

$$\ell_S(x) = \min \left\{ p \geqslant 1, \exists (s_1, \ldots, s_p) \in S^p, x = \prod_{k=1}^{p} s_k \right\}$$

Par convention, $\ell_S(0) = 1$.

Définition 6 (boule de rayon N)**.** Pour $n \in \mathbb{N}$, on appelle boule de rayon N l'ensemble

$$G_N = \{x \in G, \ell_S(x) \leqslant N\}$$

Définition 7 (fonction de croissance)**.** On définit la fonction de croissance du couple (G, S) par

$$\begin{array}{rccc} \gamma_S : & \mathbb{N} & \longrightarrow & \mathbb{N}^* \\ & N & \longmapsto & \mathrm{Card} G_N \end{array}$$

On illustrera par la suite toutes ces notions sur différents exemples.

4 Notions de théorie des groupes

On rappelle quelques notions de théorie des groupes :

Définition 8 (sous-groupe dérivé)**.** Le sous-groupe dérivé $[G, G]$ de G est le sous-groupe engendré par les commutateurs $[x, x] = xx'x^{-1}x'^{-1}$ pour $x, x' \in G$.

On notera par la suite $G^{(0)} = G$ et pour $n \in \mathbb{N}$, $G^{(n+1)} = [G^{(n)}, G]$.

Définition 9 (centre d'un groupe)**.** Le centre d'un groupe G est l'ensemble

$$Z(G) = \{c \in G, \forall g \in G, gc = cg\}$$

Définition 10 (groupe nilpotent)**.** On dit qu'un groupe G est nilpotent s'il existe $N \in \mathbb{N}$ tel que $G^{(N)} = \{1\}$.

II Exemples

Dans ce chapitre, nous allons étudier trois exemples afin d'assimiler les nouvelles notions (longueur, croissance, etc.).

1 Le groupe additif $(\mathbb{Z}^p, +)$

On s'intéresse d'abord à $\mathbb{Z}^2$, puis on généralisera avec $\mathbb{Z}^p$.

Pour $x = (p, q) \in \mathbb{Z}^2$, on utilise pour la longueur $\ell_S(x) = |p| + |q|$.
En effet, pour $x \in \mathbb{Z}^2$ de décomposition dans la base canonique $x = pe_1 + qe_2$, on a $\ell_S(x) \leqslant |p| + |q|$. De plus, on peut écrire $x = ae_1 + a'(-e_1) + be_2 + b'(-e_2)$. Donc $p = a - a'$ et $q = b - b'$, et $|p| + |q| \leqslant a + a' + b + b'$. Or, $a + a' + b + b'$ est exactement le nombre d'éléments de S utlisés dans la décomposition de x. D'où $\ell_S(x) \geqslant |p| + |q|$ et donc $\ell_S(x) = |p| + |q|$.
Cette définition correspond donc à la longueur vue précédemment.

Proposition. *$\mathbb{Z}^2$ est à croissance polynomiale de degré 2.*

Démonstration. (n° 1)
Examinons l'ensemble G_N (les éléments de longueur $\leqslant N$) : il est représenté sur la figure suivante.

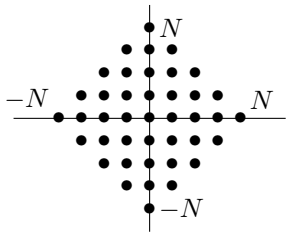

FIGURE II.1 – Boule de rayon N dans $\mathbb{Z}^2$

Comme le montre la figure qui suit, on a pour $N \geqslant 1$, Card G_N = Card G_{N-1}+$4N$.

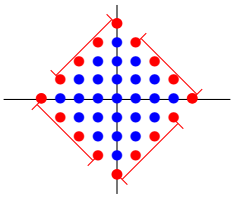

FIGURE II.2 – G_5 en fonction de G_4

On en déduit :

$$\gamma_S(N) = \text{Card}G_N = \text{Card}G_{N-1} + 4N = \cdots = \text{Card}G_0 + 4\sum_{i=1}^{N} i = 1 + 4\frac{N(N+1)}{2} = 2N^2 + 2N + 1$$

□

On a prouvé que $\mathbb{Z}^2$ est à croissance de degré 2. Pour généraliser au cas de $\mathbb{Z}^p$ pour $p \in \mathbb{N}$, on va effectuer une preuve géométrique que $\mathbb{Z}^2 \sim N^2$, mais cette démonstration sera applicable au cas général $\mathbb{Z}^p$.

Démonstration. (n° 2)

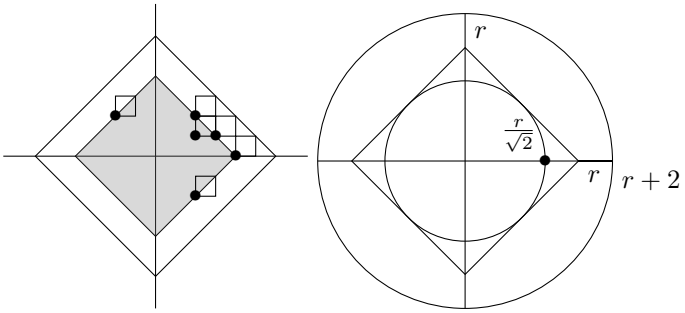

FIGURE II.3 – Encadrements de $\gamma_S(N)$ par des boules

On note Λ_k^p la boule de rayon k issue de la norme $\|\cdot\|_p$.
Sur la figure de gauche, Λ_N^1 est coloré en gris, et si on trace tous les carrés de coté 1 de sommet inférieur gauche dans G_N, on a :

$$\text{Aire}(\cup\text{carrés}) = \gamma_S(N)$$

car tous les carrés sont d'aire égale à 1. On a donc l'encadrement suivant :

$$\Lambda_N^1 \leqslant \gamma_S(N) \leqslant \Lambda_{N+2}^1$$

Sur la figure de droite, on utilise la norme $\|\cdot\|_2$: on a $\Lambda^2_{r/\sqrt{2}} \leqslant \Lambda^1_r \leqslant \Lambda^1_{r+2} \leqslant \Lambda^2_{r+2}$.
Comme l'aire d'un disque de rayon N est πN^2, on a alors :

$$\pi(N/\sqrt{2})^2 \leqslant \Lambda^1_N \leqslant \Lambda^1_{N+2} \leqslant \pi(N+2)^2$$

On en déduit donc :

$$\pi N^2/2 \leqslant \gamma_S(N) \leqslant \pi N^2 + 4\pi N + 4\pi$$

et d'où :

$$\gamma_S(N) \sim N^2$$

□

Généralisation

En dimension 3, le volume d'une boule de rayon R est $\frac{4}{3}\pi R^3 \sim R^3$.

Proposition. *En dimension p, le volume d'une boule de rayon R est polynomial de degré p.*

Conséquence : Avec les groupes $\mathbb{Z}^p$, on effectue toutes les croissances polynomiales.

2 Le groupe de Heisenberg

Pour $m,n,p \in \mathbb{Z}$, $h(m,n,p) = \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}$.

$$a = h(1,0,0) \qquad b = h(0,1,0) \qquad c = h(0,0,1)$$

Définition 11 (groupe de Heisenberg)**.** Le groupe de Heisenberg G est le sous-groupe de $\mathrm{GL}_3(\mathbb{Z})$

$$\{h(m,n,p) \mid m,n,p \in \mathbb{Z}\}$$

Proposition. *G est engendré par $\{a^{\pm 1}, b^{\pm 1}\}$.*

Démonstration. Pour $m,n \in \mathbb{Z}$,
$a^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$, $b^m = \begin{pmatrix} 1 & m & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $c = bab^{-1}a^{-1}$, $a^n b^m c^p = \begin{pmatrix} 1 & m & p \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$. □

Proposition. *Son centre $Z(G)$ est engendré par $\{c\}$.*

Démonstration. Il est facile de montrer que

$$\forall k \in \mathbb{Z} \qquad b^k a = ab^k c^k \qquad\qquad ba^k = a^k bc^k \tag{II.1}$$

Pour $x \in Z(G)$ de la forme $x = a^m b^n c^p$, il faut donc $xa = ax$ et $xb = bx$.
Comme $c \in Z(G)$ et grâce aux formules (II.1),
$xa = (a^m b^n c^p)a = (a^m b^n a)c^p = a^m(ab^n c^n)c^p = a^{m+1}b^n c^{n+p}$ $\qquad ax = a^{m+1}b^n c^p$

$bx = b(a^m b^n c^p) = (ba^m)(b^n c^p) = (a^m bc^m)(b^n c^p) = a^m b^{n+1} c^{p+m}$ $\qquad xb = a^m b^{n+1} c^p$
On en déduit donc (en évaluant « terme à terme ») que

$$m = n = 0$$

Donc $x = c^p$ et $Z(G)$ est engendré par c. □

Proposition. *Si $\ell_S(h(m,n,p)) \leqslant N$, alors*

$$|m| \leqslant N \qquad |n| \leqslant N \qquad |p| \leqslant N^2$$

Démonstration. On effectue une récurrence sur N :
La propriété est vraie au rang 0. Supposons la vraie au rang N, et prenons $x = a^m b^n c^p$ dans G de longueur $N+1$ (c'est le seul cas qui mérite d'être étudié). On pose $x = s_1 \cdots s_{N+1} = a^m b^n c^p$ avec $s_k \in S$. Quelles sont les valeurs possibles de s_1 ?

- Cas 1 : $s_1 = a$
  On note $y = s_2 \cdots s_{N+1} = a^{m-1} b^n c^p$. $\ell_S(y) \leqslant N$ donc par hypothèse de récurrence, $|m-1| \leqslant N$, $|n| \leqslant N$ et $|p| \leqslant N^2$. On a donc $|m| \leqslant N+1$, $|n| \leqslant N \leqslant N+1$ et $|p| \leqslant N^2 \leqslant (N+1)^2$.
- Cas 2 : $s_1 = a^{-1}$
  On traite ce cas de la même manière que précédemment.
- Cas 3 : $s_1 = b^{-1}$
  On note $y = s_2 \cdots s_{N+1} = (ba^m) b^n c^p = a^m b^{n+1} c^{p+m}$. Comme dans le cas 1, $\ell_S(y) \leqslant N$ donc $|m| \leqslant N+1$, $|n| \leqslant N+1$ et $|p| \leqslant N^2 + |m| \leqslant (N+1)^2$.
- Cas 4 : $s_1 = b$
  On traite ce cas de la même manière que précédemment.

□

Proposition. *Le groupe de Heisenberg est à croissance polynomiale de degré 4.*

Démonstration.

1. D'après la proposition précédente, $\mathrm{Card} G_n = \mathrm{Card}\{(m,n,p) \mid \ell_S(h(m,n,p)) \leqslant N\}$.
   On en déduit que
   $$\gamma_S(N) \leqslant \underbrace{(2N+1)^2}_{\text{choix pour } m,n} \underbrace{(2N^2+1)}_{\text{choix pour } p}$$
   Donc $\gamma_S(N) \leqslant (4N^2+4N+1)(2N^2+1) = 8N^4 + 8N^3 + 6N^2 + 4N + 1$
   $$\gamma_S(N) \preceq 8N^4 + 8N^3 + 6N^2 + 4N + 1$$

2. Comme $b^q a^q b^{-q} a^{-q} = c^{q^2}$, on a $\ell_S(c^{q^2}) \leqslant 4q$ et en particulier, $\ell_S(c) \leqslant 4$.
   Notons $p = E(\sqrt{q})$ et $r = q - p^2$. On a donc :
   $$p \leqslant \sqrt{q} < p+1 \Longrightarrow p > \sqrt{q} - 1 \Longrightarrow p^2 \geqslant q - 2\sqrt{q} + 1$$
   et
   $$r = q - p^2 \leqslant q - (q - 2\sqrt{q} + 1) = 2\sqrt{q} - 1 \Longrightarrow p + r \leqslant \sqrt{q} + 2\sqrt{q} - 1 = 3\sqrt{q} - 1$$
   D'où
   $$c^q = c^{p^2+r} = c^{p^2} \cdot (bab^{-1}a^{-1})^r \Longrightarrow \ell_S(c^q) \leqslant 4p + 4r \leqslant 12\sqrt{q} - 4$$

Il suit que $\ell_S(a^m b^n c^p) \leqslant \ell_S(a^m)+\ell_S(b^n)+\ell_S(c^p) \leqslant |m|+|n|+12\sqrt{p}-4 \leqslant N+N+12N-4 = 14N-4$

Donc on a trouvé au moins $(2N+1)^2(2N^2+1)$ éléments différents dans G_{14N-4} et donc $\gamma_S(14N-4) \geqslant 8N^4+8N^3+6N^2+4N+1$, c'est-à-dire $\gamma_S(14N-4) \succeq 8N^4+8N^3+6N^2+4N+1$.

On peut donc conclure :

$$\gamma_S(N) \sim N^4$$

□

Résultat de Gromov

Un résultat que M. Gromov a établi est le suivant :

Proposition. *Un groupe de type fini est à croissance polynomiale si, et seulement s'il contient un sous-groupe nilpotent d'indice fini.*

Comme G est à croissance de degré 4, il est donc nilpotent.
En effet, prenons $x, x' \in G$.

$$[x,x'] = a^m b^n c^p a^{m'} b^{n'} c^{p'} a^{-m} b^{-n} c^{mn-p} a^{-m'} b^{-n'} c^{m'n'-p'} = c^{mn+m'n'}$$

Donc $G^{(1)} = \{c^n, n \in \mathbb{Z}\} = Z(G)$, et d'où $G^{(2)} = [Z(G), G] = \{1\}$.
G est bien (2-)nilpotent.

3 Le groupe $\mathrm{PSL}_2(\mathbb{Z})$

$G = \mathrm{PSL}_2(\mathbb{Z})$ est le quotient de $\mathrm{SL}_2(\mathbb{Z})$ par $\{I, -I\}$.

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$\mathrm{SL}_2(\mathbb{Z})$ est engendré par A et C. On pose $B = AC = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. On note $a, b, \mathbf{1}$ les classes respectives de A, B et I dans G.
a est d'ordre 2 et b est d'ordre 3 car $A^2 = B^3 = -I$.
On pose $M_\beta = (B^{\beta_1}A)\cdots(M^{\beta_r}A)$ avec $\beta_i \in \{1,2\}$ pour tout i.
Pour $(\alpha_1, \alpha_2) \in \{0,1\}^2$, on considère $U = \{u_\gamma\}$ tels que :

$$\begin{cases} u_\gamma &= a^{\alpha_1}\left(\prod_{k=1}^{r-1} b^{\beta_k} a\right) b^{\beta_r} a^{\alpha_2} & \text{si } r \geqslant 2 \\ u_\gamma &= a^{\alpha_1} b^{\beta_r} a^{\alpha_2} & \text{si } r = 1 \end{cases}$$

Proposition. $\big\{\{1,a\}, U\big\}$ *est une partition de* G.

Démonstration. a et b engendrent $\mathrm{PSL}_2(\mathbb{Z})$, et $a^2 = b^3 = \mathbf{1}$ donc $S = \{a, b, b^2\}$ est une partie génératrice de $\mathrm{PSL}_2(\mathbb{Z})$ qui ne possède pas $\mathbf{1}$. Les éléments de G sont tous de la forme u_γ, sauf a et $\mathbf{1}$. Donc $G = \{\mathbf{1}, a\} \cup U$.
Notons m_β la classe de M_β dans G. Comme $a^2 = \mathbf{1}$, on a $m_\beta = (b^{\beta_1}a)\cdots(b^{\beta_r}a) = a^{\alpha_1} u_\gamma a^{\alpha_2+1}$.
Comme m_β n'est pas une puissance de a, u_γ n'est égal ni à $\mathbf{1}$, ni à a. On a donc trouvé une partition de G. □

Proposition.

$$\forall u \in U \qquad \exists! r \in \mathbb{N}^* \qquad \exists! \gamma \in \underbrace{\{0,1\}^2}_{\alpha_i} \times \underbrace{\{1,2\}^r}_{\beta_i} \qquad u = u_\gamma$$

Démonstration. Soient $r, s \in \mathbb{N}^*$ et $\gamma = ((\alpha_1, \alpha_2); (\beta_1, \cdots, \beta_r)), \gamma' = ((\alpha'_1, \alpha'_2); (\beta'_1, \cdots, \beta'_r))$ tels que $u_\gamma = u_{\gamma'}$
Comme $a = a^{-1}$ et $b^3 = \mathbf{1}$, on a :

$$\begin{aligned} u_\gamma = u_{\gamma'} &\iff a^{\alpha_1} \left(\prod_{k=1}^{r-1} b^{\beta_k} a \right) b^{\beta_r} a^{\alpha_2} = a^{\alpha'_1} \left(\prod_{l=1}^{s-1} b^{\beta'_l} a \right) b^{\beta'_s} a^{\alpha'_2} \\ &\iff \underbrace{a^{\alpha_1} \left(\prod_{k=1}^{r-1} b^{\beta_k} a \right) b^{\beta_r} a^{\alpha_2+\alpha'_2} b^{3-\beta'_s} \left(\prod_{l=1}^{s-1} a b^{3-\beta'_l} \right)}_{d} a^{\alpha'_1} = \mathbf{1} \end{aligned}$$

$d = a^{\alpha_1+\alpha'_1}$ donc d vaut 1 ou a. Il n'est donc pas de la forme m_β, ce qui impose $\alpha_2 + \alpha'_2 \equiv 0 \mod 2$ et $\beta_r - \beta'_s \equiv 0 \mod 3$. Comme α_2 et α'_2 valent 0 ou 1, on a nécessairement $\alpha_2 = \alpha'_2$. De même, $\beta_r = \beta'_s$.
En recommençant un nombre fini de fois, on prouve que $\gamma = \gamma'$. □

Proposition. *Le groupe modulaire $PSL_2(\mathbb{Z})$ est un groupe de type fini, engendré par $S = \{a, b, b^2\}$, et dont la croissance est exponentielle.*

Démonstration. D'après la proposition précédente, $\ell_S(u_\gamma) \leqslant \alpha_1 + \alpha_2 + 3(r-1) + 2 \leqslant 3r + 1$
Dans G, comptons les éléments de longueur $\leqslant 3r + 1$: ils sont au moins 2^{r+2} (2 choix pour les β_i et 2 choix pour les α_i).
Donc $\gamma_S(3r + 1) \geqslant 2^{r+2} \geqslant 2^r$.
On a donc $\mathrm{e}^r \sim 2^r \preceq \gamma_S(r)$, et comme la croissance est au plus exponentielle, on obtient :

$$\gamma_S(r) \sim \mathrm{e}^r$$

□

III Théorème de Gromov

Maintenant que nous sommes habitués aux groupes et à l'étude de leur croissance, nous allons étudier le théorème de Gromov et sa preuve.

1 Enoncé du théorème

G est un groupe engendré par un ensemble fini, et γ est sa fonction de croissance.

Théorème (Gromov)**.** *Supposons G infini, $m > 0$, et $\gamma(m) - \gamma(m-1) \leqslant m$. Alors G possède un sous-groupe isomorphe à $\mathbb{Z}$ d'indice $\leqslant m^4$.*

2 Définitions

On utilise les mêmes définitions que dans les parties précédentes. On y ajoute un « vocabulaire » adapté : celui des mots.

Définition 12 (mot)**.** Un mot est un élément du groupe.

Définition 13 (alphabet)**.** La partie génératrice S engendre S^* appelé alphabet. C'est l'ensemble de tous les mots de S.

On désigne par 1 le mot vide.

Définition 14 (mot p-périodique)**.** $v = v_1 \dots v_m \in S^*$ est p-périodique si $v_i = v_{i+p}$ pour $1 \leqslant i < i + p \leqslant m$.

3 Propriétés des mots périodiques

Lemme 1. *Supposons que $p \in \{1, \dots, m\}$, et $v = v_1 v_2 \dots v_{p+m} \in S^*$ vérifiant $v_1 \dots v_m = v_{p+1} \dots v_{p+m}$. Alors v est p-périodique.*

Démonstration. Prenons $1 \leqslant i < i + p \leqslant m + p$, c'est-à-dire $1 \leqslant i \leqslant m$. Par hypothèse, la i^{e}lettre de $v_1 \dots v_m$ est la i^{e}lettre de $v_{p+1} \dots v_{p+m}$. C'est exactement la définition de p-périodicité. □

On note $(a, b) := \text{pgcd}(a, b)$.

Lemme 2. *Supposons que $0 < q \leqslant p$ et que $v \in S^*$ est un mot p-périodique qui possède un sous-mot q-périodique de longueur $\geqslant p+q-1$.*
Alors v est d-périodique, où $d = (p,q)$.

Démonstration. Soit $v_i \dots v_j$ un sous-mot q-périodique de longueur $\geqslant p+q-1$, donc $j \geqslant (i-1)+p+q-1$. On effectue la division euclidienne de p par q : $p = tq + r$ avec $0 \leqslant r < q$.

Cas 1 $r = 0$.

On a donc q divise p. Pour $i > 1$, on a donc $v_{i-1} = v_{i-1+p} = v_{(i-1)+p-(t-1)q} = v_{i-1+q}$. Donc $v_{i-1} \dots v_j$ est lui-aussi q-périodique. De la même façon, pour $j < |v|$, on a $v_i \dots v_{j+1}$ est aussi q-périodique. En répétant le raisonnement (un nombre fini de fois), v est q-périodique.

Cas 2 $r > 0$.

On effectue une récurrence sur p.

AFFIRMATION : *$v_i \dots v_{i+q+r-2}$ est r-périodique.*

En effet, $i \leqslant k < k+r \leqslant i+q+r-2 \iff i \leqslant k \leqslant i+q-2$, d'où $k+p \leqslant (i+q-2)+p \leqslant j$. Donc $v_k = v_{k+p} = v_{k+p-tq} = v_{k+r}$. D'où l'affirmation.
$v_i \dots v_{i+q+r-2}$ est donc r-périodique, et sa longueur est $q+r-1$. Par l'hypothèse de récurrence appliquée à $q < p$, on a $v_i \dots v_j$ est (q,r)-périodique. Mais $(q,r) = (p,q) = d$, donc $v_i \dots v_j$ est d-périodique. Comme d divise p, on se reporte donc au **cas 1**.

□

Théorème (de périodicité)**.** *Supposons $v \in S^*$ de longueur $\geqslant m > 0$, et c le nombre de différents sous-mots de v de longueur m. On suppose de plus que $c \leqslant m$ et que $|v| \geqslant c+m$.*
Alors, il existe $0 < p \leqslant c$ et $\alpha, \beta, \gamma \in S^*$ tels que

$$v = \alpha\beta\gamma$$

avec $|\alpha| \leqslant c-p$, $|\gamma| \leqslant c-p$, et β est p-périodique.

Démonstration. On écrit $v = v_1 \dots v_M$ $(v_i \in S)$.

AFFIRMATION 0 :
$\exists p \in \{1, \dots, c\}$ et un sous-mot p-périodique de v de longueur $\geqslant m+p$.

Posons $w_i = v_i \dots v_{i+m-1}$. Donc $w_1, \dots, w_{M-m+1}$ sont les sous-mots successifs de v de longueur m. Comme $M-m+1 \geqslant c+1$, deux termes de $w_1, \dots, w_{c+1}$ doivent être égaux. Notons $w_\lambda = w_\mu$. On pose $p = \mu - \lambda$. On a $0 < p \leqslant c$, et $v_\lambda \dots v_{\lambda+m-1} = v_{\lambda+p} \dots v_{\lambda+p+m-1}$. Donc $v_\lambda \dots v_{\lambda+p+m-1}$ est p-périodique.
Prenons un sous-mot $w = v_i \dots v_j$ de v de longueur maximale, avec la propriété d'être p-périodique pour un $p \leqslant c$. On suppose que p est la plus petite période. Par l'affirmation 0, $|w| = j-i+1 \geqslant m+p \iff j \geqslant i+m+p-1$.
On va maintenant prouver que

$$i \leqslant (c+1) - p \tag{III.1}$$

Par l'absurde, on aurait $i+p > c+1$, et parmi les $c+1$ sous-mots successifs $w_{(i+p)-(c+1)}, \dots, w_{i+p-1}$, deux devraient être identiques, disons $w_k = w_l$. On pose $q = l-k$. Comme précédemment, puisque $w_k = w_l$ et d'après le premier lemme, $w' := v_k \dots v_{k+q+m-1}$ est q-périodique. On peut supposer que q est minimal (w' n'est r-périodique pour aucun $r < q$, sinon on peut prendre un autre w'). Pour aboutir à une contradiction (raisonnement par l'absurde), on prouve les trois affirmations suivantes :

Affirmation 1 :
$k < i$

Par l'absurde, supposons $k \geqslant i$.
Comme $l \in [\![(i+p)-(c+1), (i+p)-1]\!]$, $l \leqslant i+p-1$ et donc $q = l-k \leqslant i+p-1-k = \underbrace{(i-k-1)}_{\leqslant 0 \text{ par hypothèse}} + p < p$

De plus $w' = v_k \dots v_{k+q+m-1}$ est q-périodique de longueur $\geqslant p+q-1$. Par le second lemme, w est q-périodique, ce qui contredit la minimalité de p (période minimale).

Affirmation 2 :
En joignant w et w', on peut trouver un sous-mot de longueur $\geqslant p+q-1$.

On l'exhibe facilement : c'est $v_i \dots v_{k+q+m-1}$. Sa longueur est :

$$k+q+m-1-(i-1) = \underbrace{k}_{\substack{\leqslant \\ (i+p)-(c+1)}} +q+m-i \geqslant (i+p)-(c+1)+q+m-1 = p+q+\underbrace{(m-c)}_{\geqslant 0} -1 \geqslant p+q-1$$

Affirmation 3 :
$p = q$

Si $q < p$, alors par l'affirmation 2 et le lemme 2, w est q-périodique, ce qui contredit la minimalité de p. De même, $p < q$ contredit la minimalité de q.
De ces trois affirmations, on conclut que le sous-mot $v_k \dots v_j$ obtenu en joignant w et w' est p-périodique, et de longueur $\geqslant |w|$. Ceci contredit la maximalité de w (en terme de longueur), et (III.1) est prouvé.
En d'autres termes, $v_1 \dots v_{i-1}$ est de longueur $\leqslant c-p$. Par un argument symétrique, $v_{j+1} \dots v_M$ est aussi de longueur $\leqslant c-p$. On termine la preuve en écrivant $\alpha = v_1 \dots v_{i-1}$, $\beta = v_i \dots v_j$, et $\gamma = v_{j+1} \dots v_M$. □

Prenons W un fermé de S^*. Notons γ_W la fonction de croissance associée à W :

$$\gamma_W(n) = \#\{w \in W, |w| \leqslant n\}$$

Remarquons que $\gamma_W(m) - \gamma_W(m-1)$ est le nombres d'éléments de longueur m.

Corollaire. *On suppose $W \subset S^*$ fermé tel que $\gamma_W(m) - \gamma_W(n-1) \leqslant m$ pour $m \in \mathbb{N}^*$. Alors, il existe des constantes positives C et D telles que $\gamma_W(n) \leqslant Cn + D$ pour tout n. De plus, si W est infini, il existe $w \neq 1 \in W$ tel que $w^n \in W$ pour tout n.*

Démonstration. On pose $c := \gamma_W(m) - \gamma_W(m-1)$, et on fixe $n \geqslant m + c$. On prend $v \in W$ de longueur n. D'après le théorème de périodicité, on peut écrire $v = \alpha\beta\gamma$, et v est complètement déterminé par :

- La période p de β ($1 \leqslant p \leqslant c$) ;
- Le sous-mot α (de longueur $m \geqslant (c-p)+p$) ;
- Le sous-mot γ (de longueur m également).

Il y a donc au plus $c \cdot c \cdot c = c^3$ possibilités pour v, et on a donc établi que :

$$\gamma_W(n) - \gamma_W(n-1) \leqslant c^3 \qquad \forall n \geqslant m + c$$

Il suit que $\gamma_W(n) \leqslant c^3 \cdot n + D$ (pour un certain D).
Si W est infini, il possède des « longs » mots. Par le théorème de périodicité, et par le principe des tiroirs, $\exists w \neq 1$ dont toutes les puissances sont encore dans W. □

Corollaire. *Supposons que W est fermé, et que $\gamma_W(n)$ n'est majorée par aucune fonction linéaire (en n). Alors, pour tout n,*

$$\gamma_W(n) \geqslant \frac{1}{2}(n+1)(n+2)$$

Démonstration. Par le corollaire précédent, notre hypothèse implique que :

$$\gamma_W(n) - \gamma_W(n-1) \geqslant n + 1 \qquad \forall n > 0$$

On a alors :

$$\begin{aligned}\gamma_W(n) &= \gamma_W(0) + (\gamma_W(1) - \gamma_W(0)) + \cdots + (\gamma_W(n) - \gamma_W(n-1)) \\ &\geqslant 1 + 2 + \cdots + (n+1) \\ &= \frac{1}{2}(n+1) \cdot (n+2)\end{aligned}$$

□

4 Application aux groupes

Définition 15. On étend l'ordre $<$ sur S à un ordre sur S^* (que l'on note aussi $<$) tel que

$$v < w \iff \begin{cases} |v| < |w| \\ \text{ou } |v| = |w| \text{ et } v \text{ précède } w \text{ dans l'alphabet.} \end{cases}$$

Lemme 3. *Soient $G' \subset G$ des groupes engendrés (respectivement) par S' et S finis, avec $S' \subset S$. Soient γ' et γ leurs fonctions de croissance respective. On suppose que*

$$\lim_{n\to\infty} \gamma(n)^{1/n} = 1$$

et qu'il existe $C \in \mathbb{R}$ tel que

$$\frac{\gamma(n)}{\gamma'(n)} \leqslant C \qquad \textit{pour } n \textit{ assez grand}$$

Alors, G' est d'indice $\leqslant C$ dans G.

Démonstration. Soit $\varepsilon > 0$.

Affirmation :
$\forall k \in \mathbb{N}$, *il y a une infinité de* $n \in \mathbb{N}$ *tels que* $\frac{\gamma'(k+n)}{\gamma'(n)} \leqslant 1 + \varepsilon$.

Par l'absurde, on aurait : $\exists k, N$ tels que $\frac{\gamma'(k+n)}{\gamma'(k)} > 1+\varepsilon$ pour tout $n \geqslant N$. Mais alors pour $r \geqslant N$, on aurait :

$$\frac{\gamma'(r)}{\gamma'(N)} = \underbrace{\frac{\gamma'(r)}{\gamma'(r-k)}}_{>1+\varepsilon} \cdot \underbrace{\frac{\gamma'(r-k)}{\gamma'(r-2k)}}_{>1+\varepsilon} \cdot \ldots \cdot \underbrace{\frac{\gamma'(r-(l-1)k)}{\gamma'(r-lk)}}_{>1+\varepsilon} \cdot \underbrace{\frac{\gamma'(r-lk)}{\gamma'(N)}}_{>1+\varepsilon} \geqslant (1+\varepsilon)^{l+1}$$

Donc $\frac{\gamma'(r)}{\gamma'(N)} \geqslant (1+\varepsilon)^{l+1} \geqslant (1+\varepsilon)^l$.
Comme $S' \subset S$, $\gamma(r) \geqslant \gamma'(r)$, et donc $\gamma(r) \geqslant \gamma'(N)(1+\varepsilon)^l$. Donc γ n'est pas sous-exponentielle, ce qui est absurde.
Soient k donné, et $g_1, \ldots g_t \in G$ de longueur (dans S) $\leqslant k$. Montrons que t est borné par C indépendamment de k : prenons m assez grand tel que $\gamma(k+m) \leqslant C \cdot \gamma'(k+m)$ et posons $p = \gamma'(m)$. Soient $h_1, \ldots, h_p$ des éléments distincts de longueur $\leqslant m$ dans G'. Alors les $g_i h_j$ sont tous distincts, de longueur (dans X) $\leqslant k+m$. D'où $tp \leqslant \gamma(k+m)$, et donc (pour m assez grand),

$$t \leqslant \frac{\gamma(k+m)}{\gamma'(m)} \leqslant C \cdot \frac{\gamma'(k+m)}{\gamma'(m)}$$

Donc pour tout $\varepsilon > 0$, il y a une infinité de m tels que $t \leqslant C \cdot (1+\varepsilon)$, et donc $t \leqslant C$. □

On peut désormais prouver ce théorème (version simplifiée du théorème de Gromov) :

Théorème (Gromov, simplifié)**.** *Si G est infini, et que $c := G(m) - G(m-1) \leqslant m$, alors, G a un sous-groupe $G' \cong \mathbb{Z}$ d'indice $\leqslant \frac{c^4}{2}$.*

Démonstration. On considère G engendré par $A = S \cup S^{-1}$. Par le premier corollaire du théorème de périodicité, $\gamma(n) \leqslant c^3 n + D$ (où D est une constante). D'autre part, La seconde partie de ce même corollaire indique que G a un sous-groupe (qu'on note G') $\cong \mathbb{Z}$. Notons $G' = \langle a \rangle$ avec $|a| \leqslant c$ (G' est le sous-groupe engendré par a). On introduit alors la fonction γ' relative aux longueurs dans $S' := \{a\}$: $\gamma'(n) = 2n+1$. Bien-sûr, on ne sait pas si $S' \subset S$, mais en posant $S'' = S \cup S'$, il est facile de voir que γ'' (définie de la même manière que γ') satisfait :

$$\gamma'(n) \leqslant \gamma(cn) \leqslant c^4 n + D$$

On a alors $\frac{\gamma''(n)}{\gamma'(n)} \leqslant \frac{c^4}{2} + \varepsilon$ pour n assez grand, et $\varepsilon > 0$. En appliquant le dernier lemme, on conclut que G' est d'indice $\leqslant \frac{c^4}{2}$ dans G. □