Travail d'études et de recherche

Graphes à grand tour de taille

Auteur: André Kappes
(andre.kappes@gmx.net)

Tutor: Odile Garotta

Grenoble

16 juin 2020

Université Joseph Fourier Grenoble 1
Master Mathématiques 2004-2005

1 Introduction

Le tour de taille d'un graphe est la longueur du plus petit circuit. Pour un graphe fini, connexe, k-régulier le tour de taille est toujours plus petit que le logarithme du nombre de sommets. Le but de cet article est de constuire explicitement une famille de graphes, dont le nombre de sommets tend vers l'infini et dont le tour de taille croît aussi vite que le logarithme du nombre de sommets – en d'autres termes, une famille de graphes qui a un grand tour de taille.

De tels graphes peuvent être utiles dans la modélisation d'un réseau de propagation d'information. En maximisant le tour de taille, on cherche à éviter les redondances. Le fait que le nombre de sommets d'une telle famille tend vers l'infini reflète l'exigence d'avoir des réseaux arbitrairement grands. La restriction aux graphes k-réguliers est aussi bien naturelle : certes, le meilleur réseau pour transmettre de l'information entre m sommets est donné par le graphe complet (i.e. il existe une arête de chaque sommet vers chaque autre sommet), le nombre d'arêtes est pourtant $\frac{1}{2}m(m-1)$, il croît avec le carré du nombre de sommets. Les graphes k-réguliers sont ainsi un bon compromis entre les contraintes économiques et le désir d'avoir un bon réseau de transmission : le nombre d'arêtes est $\frac{1}{2}k\,m$, il croît linéairement en m, le nombre de sommets.

La construction proposée n'utilise que des moyens élémentaires. On emploie le théorème des quatre carrés de Jacobi et les quaternions, ainsi que le groupe fini $\mathrm{PGL}_2(q)$ sur le corps fini $\mathbb{F}_q$, q premier. On rappellera les résultats utilisés au début de l'article. Pourtant, on suppose que le lecteur connaît quelques notions de l'algèbre, comme groupe et anneau et qu'il est en particulier familier aux groupes libres.

2 Préliminaires

2.1 Graphes et graphes de Cayley

2.1.1 Définitions

Définition. Un couple $X = (V, E)$, où V est un ensemble non vide (dit *les sommets*) et $E \subseteq V \times V$ est une relation sur V (dite *les arêtes*), est dit *graphe*. On note $|X| = |V|$ le nombre de sommets. Pour un tel graphe, on définit les propriétés suivantes :

— *fini* : le nombre de sommets est fini
— *symétrique* : E est une relation symétrique
— *sans boucles* : $\forall x \in V : (x, x) \notin E$
— *k-régulier ($k \in \mathbb{N}$)* : il y a exactement k arêtes partant de chaque sommet

Définition. Soit $X = (V, E)$ un graphe. On dit que $Y = (V', E')$ est un *sous-graphe* de X, si $\emptyset \neq V' \subset V$ et $E' \subset E \cap V' \times V'$.

Définition. Soit $X = (V, E)$ un graphe symétrique et sans boucles.

1. Soit $m \in \mathbb{N}$. $(x_0, \ldots, x_m) \in V^{m+1}$ s'appelle *chemin de longueur m de x_0 à x_m dans* X, si $(x_i, x_{i+1}) \in E$, quel que soit $0 \leq i \leq m-1$ (quand $m > 0$) et si la condition

$$x_{i-1} \neq x_{i+1} \text{ pour } 1 \leq i \leq m-1.$$

est remplie (dès que $m \geq 2$), i.e. on interdit un aller-retour sur la même arête. On dit que X est *connexe*, s'il existe un chemin de chaque sommet vers chaque autre sommet.

2. Soit $m > 2$. $C = (x_0, \ldots, x_m) \in V^{m+1}$ est un *circuit de longueur* m, si C est un chemin avec $x_m = x_0$
3. *Le tour de taille*[1] $g(X)$ d'un graphe X est la longueur du plus petit circuit dans X. S'il n'existe pas de circuit dans X, on pose $g(X) = +\infty$ et on dit que X est un arbre.

2.1.2 Une borne supérieure du tour de taille

Pour un graphe fini, connexe et k-régulier, nous allons maintenant trouver une borne supérieure du tour de taille.

Proposition 1. *Soit $X = (V, E)$ un graphe fini, connexe, symétrique, sans boucles et k-régulier avec $k \geq 2$. Alors*

$$g(X) \leq 2 \log_{k-1} |X| + 2 \log_{k-1} \left(\frac{k - 2 + 2/|X|}{k} \right) + 2$$

Preuve: Supposons d'abord par l'absurde $g(X) = +\infty$. Soit $x_0 \in V$. Par $k \geq 2$, on trouve $x_1 \in V$, tel que $(x_0, x_1) \in E$ et puis successivement des éléments $x_j \in V$ tel que $(x_{j-1}, x_j) \in E$ et $x_j \neq x_{j-2}$, $j \geq 2$. Comme il n'y a pas de circuit dans X, tous les x_j sont distinct et on a un nombre infini de sommets, une contradiction.

Notons maintenant $r = [\frac{1}{2}(g(X) - 1)]$, le plus grand entier plus petit que $\frac{1}{2}(g(X) - 1)$. Pour $x \in V$, on définit par récurrence la boule de rayon $s \in \mathbb{N}$ autour de x

$$B_0(x) = \{x\}, \qquad B_1(x) = B_0(x) \cup \{v \in V : (x, v) \in E\}$$

$$B_s(x) = B_{s-1}(x) \cup \{v \in V : \exists\, w \in B_{s-1}(x) \text{ tel que } (w, v) \in E\}, \quad s \geq 2$$

ainsi que des parties $E_s(x)$ de E

$$E_0(x) = \emptyset, \qquad E_1(x) = \{(v, w) \in E : v \in B_0(x),\, w \in B_1(x)\}$$

$$E_s(x) = E_{s-1}(x) \cup \{(v, w) \in E : v \in B_{s-1}(x),\, w \in B_s(x)\}, \quad s \geq 2$$

Alors, le couple $X_s(x) = (B_s(x), E_s(x))$ est un sous-graphe de X. On voit déjà qu'il n'y a pas d'arêtes entre deux éléments de $B_s(x) \setminus B_{s-1}(x)$ dans $X_s(x)$. De plus, pour $1 \leq s \leq r$, on a la propriété suivante[2]

$$\text{Pour tout } v \in B_s(x) \setminus B_{s-1}(x), \text{ il y a un unique } w \in B_{s-1}(x) \text{ tel que } (w, v) \in E_s. \quad (1)$$

On montre (1) par récurrence sur $1 \leq s \leq r$. Le cas $s = 1$ est évident. Soit $1 \leq s \leq r - 1$ et soit (1) vrai pour tout $1 \leq l \leq s$. Supposons par l'absurde que (1) n'est pas vraie pour $s + 1$. Comme l'existence d'un tel w est garantie par la définition de $B_{s+1}(x)$ et $E_{s+1}(x)$, seulement l'unicité ne peut être valable. Alors, il existe un $v \in B_{s+1}(x) \setminus B_s(x)$ et $u \neq w$ dans $B_s(x)$ tel que (u, v) et $(w, v) \in E_s$. Par hypothèse de récurrence, on trouve pour $u, w \in B_s(x)$

1. "girth" en anglais, "Taillenweite" en allemand
2. On peut en fait démontrer plus : $X_s(x)$ est un arbre

d'uniques chemins de longueurs $t_1, t_2 \leq s$ jusqu'à l'origine x. On les note $(u = u_0, \ldots, u_{t_1} = x)$ et $(w = w_0, \ldots, w_{t_2} = x)$, d'où on obtient un circuit

$$(x = u_{t_1}, \ldots, u_0 = u, v, w = w_0, \ldots, w_{t_2} = x)$$

de longueur $t_1+2+t_2 \leq 2s+2$. Mais $2s+2 \leq 2(r-1)+2 = 2[\frac{1}{2}(g(X)-1)] \leq g(X)-1 < g(X)$, d'où on a trouvé un circuit de longueur strictement plus petite que $g(X)$ dans X.

On voudrait maintenant compter le nombre de sommets de $X_r(x)$. On remarque que

$$B_r(x) = \bigcup_{s=0}^{r} C_s(x) \qquad \text{avec } C_s(x) = B_s(x) \setminus B_{s-1}(x), s > 0 \text{ et } C_0(x) = \{x\}$$

Par $B_{s-1}(x) \subset B_s(x)$, $1 \leq s \leq r$, les cercles $C_s(x)$ sont bien disjoints. Vu qu'il y a k arêtes partant d'un sommet, on a déjà $|C_1(x)| = k$. Quand $2 \leq s \leq r$, remarquons d'abord que toutes les k arêtes partant d'un sommet de $B_{s-1}(x)$ sont dans $X_r(x)$. La propriété (1) montre que, pour chaque sommet de $C_{s-1}(x)$, il y a exactement $k-1$ sommets qu'on peut atteindre dans $C_s(x)$. En effet, seulement un sommet est dans $B_{s-2}(x)$ et il n'y a pas d'arêtes entre les éléments de $C_{s-1}(x)$; sinon, on aurait un circuit de longueur plus petite que $2(s-2)+3 < g(X)$. De plus, on déduit de (1) que tous ces $k-1$ sommets sont issus d'un unique élément dans $C_{s-1}(x)$, d'où la formule $|C_s(x)| = (k-1)|C_{s-1}|$. On obtient donc

$$\begin{aligned} |X_r(x)| = |B_r(x)| &= \sum_{i=0}^{r} |C_s(x)| = 1 + k + k(k-1) + k(k-1)^2 + \ldots + k(k-1)^{r-1} \\ &= 1 + k \sum_{i=0}^{r-1} (k-1)^i = 1 + k\,\frac{(k-1)^r - 1}{k-2} \end{aligned}$$

En utilisant l'inégalité triviale $|B_r(x)| \leq |X|$ on obtient

$$\begin{aligned} |B_r(x)| &= \frac{k(k-1)^r - 2}{k-2} \leq |X| \\ \Rightarrow \quad (k-1)^r &\leq |X| \left(\frac{k-2+2/|X|}{k} \right) \end{aligned}$$

En prenant le logarithme de base $k-1$, on obtient

$$[\frac{1}{2}(g(X)-1)] = r \leq \log_{k-1} |X| + \log_{k-1} \left(\frac{k-2+2/|X|}{k} \right)$$

et finalement

$$g(X) \leq 2 \log_{k-1} |X| + 2 \log_{k-1} \left(\frac{k-2+2/|X|}{k} \right) + 2$$

□

Soit $(X_n)_{n\in\mathbb{N}}$ une famille de graphes k-réguliers ($k \geq 2$), connexes, symétriques et finis, telle que $|X_n| \to \infty$ ($n \to \infty$). On sait maintenant que le tour de taille satisfait

$$g(X_n) \leq (2 + o(1)) \log_{k-1} |X_n|$$

où $o(1)$ est une quantité qui tend vers 0 lorsque $n \to \infty$. Nous nous intéressons aux familles, qui satisfont

$$\text{Il existe } C > 0 \text{ telle que } g(X_n) \geq (C + o(1)) \log_{k-1} |X_n|$$

et nous disons qu'une telle famille a un grand tour de taille. Evidemment, on a déjà $C \leq 2$.

D'abord, il n'est pas vraiment clair que de tels graphes existent : une première preuve non constructive a été trouvée par Erdös et Sachs 1962 [3], avec la constante $C = 1$. Notre but est une construction explicite d'une telle famille de graphes avec même une constante meilleure $C = 4/3$.

Les graphes utilisés seront des graphes de Cayley du groupe fini $\mathrm{PGL}_2(q)$, construits à partir d'un ensemble provenant des solutions du théorème des quatre carrés de Jacobi.

2.1.3 Graphes de Cayley

Définition. Soient $(\Gamma, \cdot)$ un groupe et $S \subset \Gamma$ une partie finie, telle que $1 \notin S$ et $S^{-1} \subset S$. *Le graphe de Cayley*, noté $\mathcal{G}(\Gamma, S) = (V, E)$ est défini par $V = \Gamma$ et $(x, y) \in E$, si et seulement s'il existe $s \in S$ tel que $y = x \cdot s$.

Remarque 2.
- $\mathcal{G}(\Gamma, S)$ *n'a pas de boucles (car* $1 \notin S$*).*
- $\mathcal{G}(\Gamma, S)$ *est symétrique (car* $S^{-1} \subset S$*).*
- $\mathcal{G}(\Gamma, S)$ *est* k*-régulier avec* $k = |S|$*, car* $xs_1, \ldots, xs_k$ *sont* k *sommets distincts autour de* $x \in \Gamma$ *(où* $S = \{s_1, \ldots, s_k\}$*).*
- $\mathcal{G}(\Gamma, S)$ *est connexe, si et seulement si* Γ *est engendré par* S*, car il existe un chemin de chaque sommet vers le sommet* 1*, l'élément neutre de* Γ*.*
- Γ *agit par automorphisme sur* $\mathcal{G}(\Gamma, S)$*, plus précisément par multiplication à gauche :*

$$\mathcal{G}(x \cdot \Gamma, S) = \mathcal{G}(\Gamma, S), \qquad \text{pour tout } x \in \Gamma.$$

Remarque 3. *Soit* $\mathcal{G}(\Gamma, S)$ *un graphe de Cayley et* Γ' *un sous-groupe de* Γ*, tel que* $S \subset \Gamma'$*. Alors,* $\mathcal{G}(\Gamma', S)$ *est un sous-graphe de* $\mathcal{G}(\Gamma, S)$*.*

Preuve: Soient $\mathcal{G}(\Gamma, S) = (V, E)$ et $\mathcal{G}(\Gamma', S) = (V', E')$. Alors, $(x, y) \in E' \Rightarrow [(x, y) \in V' \times V'$ et $\exists\, s \in S$ tel que $y = xs] \Rightarrow (x, y) \in E \cap V' \times V'$, car $V' = \Gamma' \subset \Gamma = V$. $\square$

2.2 Somme de quatre carrés

Théorème 4. (Jacobi) *Soit* n *un entier positif impair. Alors, l'équation*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n \tag{2}$$

admet $8 \cdot \sum_{d|n} d$ *solutions dans* $\mathbb{Z}^4$*.*

Avant de démontrer le théorème, introduisons deux notations. On pose pour n, $k \in \mathbb{N}$, $k > 1$

$$r_k(n) = |\{(x_1, \ldots, x_k) \in \mathbb{Z}^k : \sum_{i=1}^{k} x_i^2 = n\}|$$

le nombre de possiblités d'écrire n comme une somme de k carrés et

$$N_k(n) = |\{(x_1, \ldots, x_k) \in \mathbb{N}^k : \sum_{i=1}^{k} x_i^2 = n \text{ avec } x_i \equiv 1 \,(\mathrm{mod}\ 2), 1 \leq i \leq k\}|$$

le nombre de représentations de n comme une somme de k carrés d'entiers impairs positifs.

Pour la preuve du Théorème 4, nous avons besoin de la proposition suivante sur les sommes de deux carrés.

Proposition 5. *Soit $n \in \mathbb{N}$. Notons $d_1(n)$ le nombre de diviseurs de n congruents 1 modulo 4 et $d_3(n)$ le nombre de diviseurs de n congruents 3 modulo 4. Alors,*

$$r_2(n) = 4(d_1(n) - d_3(n)).$$

Preuve: Cf. [1], p.45, Theorem 2.2.11. pour la preuve. □

Preuve: (du Théorème 4)
La preuve utilise les trois égalités

$$\begin{aligned} & r_4(4n) = r_4(2n) \quad \text{pour tout } n \in \mathbb{N} \\ & r_4(2n) = 3r_4(n) \quad \text{pour tout } n \in \mathbb{N} \text{ impair} \\ \text{et} \quad & r_4(4n) = 16N_4(4n) + r_4(n) \quad \text{pour tout } n \in \mathbb{N} \text{ impair} \end{aligned}$$

que nous allons montrer dans trois lemmes au-dessous. Avec ces égalités, on obtient pour $n \in \mathbb{N}$ impair

$$\begin{aligned} 3r_4(n) &= r_4(2n) = r_4(4n) \\ &= 16N_4(4n) + r_4(n) \end{aligned}$$

d'où

$$r_4(n) = 8N_4(4n).$$

Il reste donc à montrer l'égalité :

$$N_4(4n) = \sum_{d|n} d \qquad \text{pour } n \in \mathbb{N} \text{ impair.}$$

Comme une somme de quatre carrés est une somme de deux sommes de deux carrés, on a

$$N_4(4n) = \sum_{(s,t) \in \mathbb{N}^2 :\, s+t=4n} N_2(s)\, N_2(t)$$

Maintenant s et t sont forcément congruents 2 modulo 4, car on ne regarde que les solutions à coordonnées impaires. Donc, on a

$$N_4(4n) = \sum_{\substack{(s,t)\in\mathbb{N}^2:\, s+t=4n,\\ s\equiv t\equiv 2(\mathrm{mod}\ 4)}} N_2(s)N_2(t)$$

On cherche à exprimer $N_2(s)$ en termes de $r_2(s)$. Dans la formule $r_2(s) = 4(d_1(s) - d_3(s))$ donnée par Proposition 5, le facteur 4 disparaît quand on compte seulement les solutions positives. Comme $s \equiv 2(\mathrm{mod}\ 4)$ implique que s est carré de deux entiers impairs, on a

$$N_2(s) = d_1(s) - d_3(s)$$

De plus $s/2$ est impair, d'où on obtient

$$N_2(s) = \sum_{(a,b)\in\mathbb{N}^2:\, s=2ab} (-1)^{\frac{a-1}{2}}$$

où a et b sont impairs. En effet,

$$(-1)^{\frac{a-1}{2}} = \begin{cases} +1, & \text{si } a \equiv 1(\mathrm{mod}\ 4) \\ -1, & \text{si } a \equiv 3(\mathrm{mod}\ 4) \end{cases}$$

De la même façon, on obtient pour $N_2(t)$

$$N_2(t) = \sum_{(c,d)\in\mathbb{N}^2:\, t=2cd} (-1)^{\frac{c-1}{2}} = \sum_{(c,d)\in\mathbb{N}^2:\, t=2cd} (-1)^{\frac{1-c}{2}}$$

et puis

$$N_4(4n) = \sum_{\substack{(a,b,c,d)\in\mathbb{N}^4,\ \text{impairs}\\ 2ab+2cd=4n}} (-1)^{\frac{a-c}{2}}$$

On fait maintenant un changement de variables

$$a = x + y, \quad b = v - w, \quad c = x - y \quad d = v + w$$

avec l'inverse

$$x = \frac{a+c}{2}, \quad y = \frac{a-c}{2}, \quad v = \frac{b+d}{2}, \quad w = \frac{d-b}{2}$$

qui nous donne bien une bijection entre

$$\{(a,b,c,d) \in \mathbb{N}^4 :\ a,b,c,d \text{ impairs},\ ab + cd = 2n\}$$

et $\{(x,y,v,w) \in \mathbb{Z}^4 :\ n = xv - yw,\ |y| < x,\ |w| < v,\ x \not\equiv y(\mathrm{mod}\ 2),\ v \not\equiv w(\mathrm{mod}\ 2)\}$

Ainsi, on a

$$N_4(4n) = \sum_{\substack{(x,y,v,w)\in\mathbb{Z}^4:\, n=xv-yw,\, |y|<x,\, |w|<v,\\ x\not\equiv y(\mathrm{mod}\ 2),\, v\not\equiv w(\mathrm{mod}\ 2)}} (-1)^y$$

Notons d'abord, que x et v sont positifs. Selon les cas $y < 0$, $y = 0$ et $y > 0$, on divise cette somme dans trois parties :

$$N_4(4n) = N_- + N_0 + N_+$$

Nous montrons $N_- = N_+ = 0$. Ensuite, l'examination de N_0 va nous donner le résultat.

Première étape : $N_- = N_+$. En effet, l'application

$$(x, y, v, w) \mapsto (x, -y, v, -w)$$

est une bijection entre les indices de N_+ et de N_-.

Deuxième étape : $N_+ = 0$. L'ensemble des indices de N_+ est

$$Q = \{(x, y, v, w) \in \mathbb{N}^4 : n = xv - yw,\ 0 < y < x,\ |w| < v,\ x \not\equiv y (\mathrm{mod}\ 2),\ v \not\equiv w (\mathrm{mod}\ 2)\}.$$

On fait un changement de variables $\alpha : Q \to \mathbb{N}^4$, $(x, y, v, w) \mapsto (x', y', v', w')$, défini par

$$x' = 2u(x, y)v - w, \quad y' = v, \quad v' = y, \quad w' = 2u(x, y)y - x$$

où $u(x, y)$ dénote l'unique entier positif, tel que

$$2u(x, y) - 1 < \frac{x}{y} < 2u(x, y) + 1$$

(En effet, $\frac{x}{y} > 1$ et c'est un nombre rationnel qui n'est pas un entier impair, puisque x et y n'ont pas la même parité.)

Maintenant, α vérifie les trois propriétés

1. $\alpha(Q) \subset Q$. C'est un calcul pénible, mais facile.
2. $\alpha^2 = \mathrm{Id}$. Notons que $u(x', y') = u(x, y)$. En effet, on a $\frac{x'}{y'} = \frac{2u(x,y)v - w}{v} = 2u(x, y) - \frac{w}{v}$ et $2u(x, y) - 1 < 2u(x, y) - \frac{w}{v} < 2u(x, y) + 1$ à cause de $|w| < v$. Puis, on montre facilement que $\alpha^2 = \mathrm{Id}$.
3. $y' \not\equiv y \,(\mathrm{mod}\ 2)$, si $(x, y, v, w) \in Q$. Comme $n = xv - yw$ est impair, on a $xv \not\equiv yw \,(\mathrm{mod}\ 2)$. Supposons par l'absurde $v \equiv y \,(\mathrm{mod}\ 2)$. Alors $v,\ y \not\equiv 0 \,(\mathrm{mod}\ 2)$ par l'équation précédente. Mais $y \equiv v \equiv 1 \,(\mathrm{mod}\ 2)$ entraîne $x \equiv w \equiv 0 \,(\mathrm{mod}\ 2)$, car $x \not\equiv y$, $v \not\equiv w \,(\mathrm{mod}\ q)$, d'où n est pair, une contradiction.

On déduit de 1. et 2. que α est une bijection et on a donc

$$N_+ = \sum_{(x,y,v,w) \in Q} (-1)^y = \sum_{(x',y',v',w') \in Q} (-1)^{y'}$$

d'où $N_+ = 0$, car le terme associé à $(x', y', v', w') \in Q$ est le négatif du terme associé à $(x, y, v, w) \in Q$ (par 3.). Alors $N_- = N_+ = 0$ et il nous en reste

$$N_4(4n) = N_0 = \sum_{(x,v,w) \in P} 1$$

avec

$$P = \{(x, v, w) \in \mathbb{Z}^3 : n = xv,\ |w| < v,\ v \not\equiv w (\mathrm{mod}\ 2)\}$$

Nous devons donc compter le nombre d'éléments de P. Comme n est impair, v et x sont forcément impairs. Puis, pour $v \in \mathbb{N}$ impair fixé, il y a exactement v entiers pairs dans l'intervalle $[-v, v]$, d'où

$$N_4(4n) = N_0 = |P| = \sum_{(x,v) \in \mathbb{N}^2 :\, xv = n} v = \sum_{v | n} v,$$

ce qui complète la preuve. □

Passons maintenant aux preuves des égalités utilisées.

Lemme. *Pour $n \in \mathbb{N}$, on a* $r_4(4n) = r_4(2n)$.

Preuve: Soit $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ une solution de $x_1^2+x_2^2+x_3^2+x_4^2 = 4n$. En regardant cette équation modulo 4, on trouve que les x_i sont soit tous pairs, soit tous impairs (car les carrés modulo 4 sont 0 et 1). Le changement de variables $\mathbb{Z}^4 \to \mathbb{Z}^4$, $(x_1, x_2, x_3, x_4) \mapsto (y_1, y_2, y_3, y_4)$ défini par

$$y_1 = \frac{x_1 - x_2}{2}, \quad y_2 = \frac{x_1 + x_2}{2}, \quad y_3 = \frac{x_3 - x_4}{2}, \quad y_4 = \frac{x_3 + x_4}{2}$$

est bien défini et nous donne une bijection entre les solutions de $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4n$ et celles de $y_1^2+y_2^2+y_3^2+y_4^2 = 2n$. En effet, on définit l'inverse à partir des relations $x_1 = y_1+y_2$, $x_2 = y_2 - y_1$, $x_3 = y_3 + y_4$, $x_4 = y_4 - y_3$. □

Lemme. *Pour $n \in \mathbb{N}$ impair, on a* $r_4(2n) = 3r_4(n)$.

Preuve: Soit $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ une solution de $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2n$. On regarde cette équation modulo 4. Comme n est impair, il y a exactement deux coordonnées impaires dans (x_1, x_2, x_3, x_4), d'où chaque solution appartient à exactement un des trois classes

$$\begin{cases} x_1 \equiv x_2 \pmod 4 \\ x_3 \equiv x_4 \pmod 4 \end{cases}, \quad \begin{cases} x_1 \equiv x_3 \pmod 4 \\ x_2 \equiv x_4 \pmod 4 \end{cases}, \quad \begin{cases} x_1 \equiv x_4 \pmod 4 \\ x_2 \equiv x_3 \pmod 4 \end{cases}$$

Comme dans la preuve du lemme précédent, on trouve pour chaque cas un changement de variables $\mathbb{Z}^4 \to \mathbb{Z}^4$, $(x_1, x_2, x_3, x_4) \mapsto (y_1, y_2, y_3, y_4)$, qui est bijectif et envoie une solution de $x_1^2+x_2^2+x_3^2+x_4^2 = 2n$ sur une solution de $y_1^2+y_2^2+y_3^2+y_4^2 = n$, ce qui nous donne le résultat. □

Lemme. *Pour $n \in \mathbb{N}$ impair, on a* $r_4(4n) = 16N_4(4n) + r_4(n)$.

Preuve: Soit $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ une solution de $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4n$. Comme on a vu dans la preuve du premier lemme, soit tous les x_i sont pairs, soit ils sont tous impairs. Dans le premier cas, le changement de variables $\mathbb{Z}^4 \to \mathbb{Z}^4$, $(x_1, x_2, x_3, x_4) \mapsto (y_1, y_2, y_3, y_4)$, où $y_i = x_i/2$, $1 \le i \le 4$ est une bijection entre l'ensemble des solutions de $x_1^2+x_2^2+x_3^2+x_4^2 = 4n$ à coordonnées paires et les solutions de $y_1^2 + y_2^2 + y_3^2 + y_4^2 = n$. On en a donc $r_4(n)$.

Dans le deuxième cas, on a $16N_4(4n)$ solutions. Le facteur $2^4 = 16$ provient du choix du signe de chaque coordonnée (N_4 ne compte que des solutions positives, tandis que r_4 compte les solutions dans $\mathbb{Z}^4$). □

Notons encore qu'on obtient exactement $8\,(p + 1)$ solutions de (2), quand on applique le Théorème 4 à un nombre premier $n = p$. Maintenant, supposons $p \equiv 1 \pmod 4$. En réduisant l'équation (2) modulo 4, on trouve qu'exactement un des x_i est impair et que les autres sont

pairs (car 0 et 1 sont les seuls carrés modulo 4). Ainsi, on obtient

$$|\{(x_1, x_2, x_3, x_4) \in \mathbb{Z} : x_1^2 + x_2^2 + x_3^2 + x_4^2 = p \text{ et } x_1 \text{ impair}, \ x_1 > 0\}| = p + 1$$

Ces $p + 1$ solutions jouent un rôle important dans la construction de nos graphes. On les regardera dans le contexte des quaternions que l'on introduit dans la prochaine partie.

2.3 Quaternions

2.3.1 Quaternions sur un anneau A quelconque

Soit A un anneau commutatif avec unité. Sur le A-module $(A^4, +)$, on définit une opération "$\cdot$", en posant pour $\alpha = (a_1, a_2, a_3, a_4)$ et $\beta = (b_1, b_2, b_3, b_4) \in A^4$:

$$\alpha \cdot \beta = (c_1, c_2, c_3, c_4), \text{ où}$$

$$c_1 = a_1\,b_1 - a_2\,b_2 - a_3\,b_3 - a_4\,b_4 \qquad c_2 = a_1\,b_2 + a_2\,b_1 + a_3\,b_4 - a_4\,b_3$$
$$c_3 = a_1\,b_3 - a_2\,b_4 + a_3\,b_1 + a_4\,b_2 \qquad c_4 = a_1\,b_4 + a_2\,b_3 - a_3\,b_2 + a_4\,b_1$$

Définition. L'ensemble A^4 avec ces deux opérations "$+$" et "$\cdot$" est noté $\mathbb{H}(A)$, *les quaternions sur A.*

On introduit les abréviations

$$1 = (1, 0, 0, 0), \quad i = (0, 1, 0, 0), \quad j = (0, 0, 1, 0), \quad k = (0, 0, 0, 1)$$

à l'aide desquelles, on réécrit

$$\mathbb{H}(A) = \{\alpha = a_1\,1 + a_2\,i + a_3\,j + a_4\,k \quad \text{avec } a_1, a_2, a_3, a_4 \in A\}$$

En appliquant la définition de "$\cdot$", on voit que 1, i, j et k sont soumis aux relations suivantes :

$$i^2 = j^2 = k^2 = -1, \ ij = -ji = k, \ jk = -kj = i, \ ki = -ik = j$$

Proposition. *L'ensemble $\mathbb{H}(A)$ est un anneau non-commutatif avec unité 1. De plus, il existe un morphisme d'anneaux injectif $\psi : A \hookrightarrow \mathbb{H}(A)$, $a \mapsto a \cdot 1$, qui permet de considérer A comme un sous-anneau de $\mathbb{H}(A)$* [3].

Preuve: En calculant, on montre que "$\cdot$" est associative, que "$\cdot$" est distributive par rapport à "$+$" et que 1 est l'élément neutre de "$\cdot$". Les relations pour 1, i, j et k au-dessus montrent la non-commutativité.

L'application ψ est évidemment additive et multiplicative et injective. □

Définition. Soit $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in \mathbb{H}(A)$. On définit *le quaternion conjugué* $\overline{\alpha}$ comme l'élément $a_1 - a_2 i - a_3 j - a_4 k$ et *la norme de* α comme $N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

3. Dorénavant, on identifie souvent $a \in A$ avec le quaternion $\alpha = a \cdot 1$

Remarque 6.

1. *Le centre*[4] $\mathcal{Z}(\mathbb{H}(A)^\times)$ *de* $\mathbb{H}(A)^\times$ *est le groupe* $A^\times = A^\times \cdot 1 \subset \mathbb{H}(A)^\times$.
2. *L'application* $\overline{\cdot} : \mathbb{H}(A) \to \mathbb{H}(A)$ *vérifie* $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$, *quels que soient* α, $\beta \in \mathbb{H}(A)$
3. $N : \mathbb{H}(A) \longrightarrow A$ *est multiplicative.*

Preuve: Afin de faciliter l'écriture, notons $e_1 = 1$, $e_2 = i$, $e_3 = j$ et $e_4 = k$.
1. D'abord, on remarque que $s\alpha = \alpha s$ pour tout $s \in A^\times$ (et même pour $s \in A$), d'où $A^\times \subset \mathcal{Z}(\mathbb{H}(A)^\times)$. Soit alors $\alpha = \sum_{i=1}^4 a_i\, e_i$ dans le centre de $\mathbb{H}(A)^\times$. Alors,

$$\begin{aligned} \alpha\, e_j &= \sum_{i=1}^4 a_i\, e_i\, e_j = a_1\, e_j + \sum_{i=2}^4 a_i\, (-e_j\, e_i) \\ &= e_j\, \alpha = e_j\, a_1 + \sum_{i=2}^4 a_i\, e_j\, e_i \end{aligned}$$

pour tout $j \in \{2,3,4\}$, donc $2\sum_{i=2}^4 a_i\, e_j\, e_i = 0$ et puis $a_2 = a_3 = a_4 = 0$, ce qui montre $\mathcal{Z}(\mathbb{H}(A)^\times) \subset A^\times$.
2. On trouve pour α, $\beta \in \mathbb{H}(A)$

$$\begin{aligned} \overline{\alpha\,\beta} &= (a_1\, b_1 - a_2\, b_2 - a_3\, b_3 - a_4\, b_4) - (a_1\, b_2 + a_2\, b_1 + a_3\, b_4 - a_4\, b_3)i \\ &\quad - (a_1\, b_3 - a_2\, b_4 + a_3\, b_1 + a_4\, b_2)j - (a_1\, b_4 + a_2\, b_3 - a_3\, b_2 + a_4\, b_1)k \\ &= (b_1\, a_1 - b_2\, a_2 - b_3\, a_3 - b_4\, a_4) + (b_1\, (-a_2) + (-b_2)\, a_1 + b_3\, a_4 - b_4\, a_3)i \\ &\quad + (b_1\, (-a_3) - b_2\, a_4 + (-b_3)\, a_1 + b_4\, a_2)j + (b_1\, (-a_4) + b_2\, a_3 - b_3\, a_2 + (-b_4)\, a_1)k \\ &= \overline{\beta}\,\overline{\alpha} \end{aligned}$$

3. En utilisant 2., on trouve

$$N(\alpha\,\beta) = \alpha\,\beta\overline{\alpha\,\beta} = \alpha\,\beta\,\overline{\beta}\,\overline{\alpha} = \alpha\,\overline{\alpha}\,\beta\overline{\beta} = N(\alpha)\,N(\beta)$$

pour tout α, $\beta \in \mathbb{H}(A)$. □

Définition. Soit $\alpha \in \mathbb{H}(A)$. On dit que α est *irréductible*, si α n'est pas inversible et si $\alpha = \beta\,\gamma$ dans $\mathbb{H}(A)$ entraîne que β ou γ est dans $\mathbb{H}(A)^\times$.

2.3.2 Quaternions sur $\mathbb{Z}$

En particulier, en se plaçant dans le cadre $A = \mathbb{Z}$, on obtient les trois résultats suivants.

Proposition 7. *Soit* $\alpha \in \mathbb{H}(\mathbb{Z})$. *Alors* $N(\alpha) = 1 \Leftrightarrow \alpha \in \mathbb{H}(\mathbb{Z})^\times$. *En particulier, les éléments inversibles de* $\mathbb{H}(\mathbb{Z})$ *sont exactement* $\{\pm 1, \pm i, \pm j, \pm k\}$.

Preuve: Remarquons d'abord que $N(\alpha) = 1$ implique $\alpha \in \mathbb{H}(A)^\times$, quel que soit l'anneau A, car $1 = N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha$, d'où $\overline{\alpha}$ est l'inverse de α.

4. Le centre $\mathcal{Z}(G)$ d'un groupe G est le sous-groupe défini par $\mathcal{Z}(G) = \{g \in G : \forall\, h \in G,\, gh = hg\}$

Dans le cas $A = \mathbb{Z}$, $\alpha \in \mathbb{H}(\mathbb{Z})^\times$ implique $1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$ et puis $N(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$. Par $N(\alpha) \geq 0$ pour tout $\alpha \in \mathbb{H}(\mathbb{Z})$, on obtient le résultat.

Enfin, on remarque que $\{\pm 1, \pm i, \pm j, \pm k\}$ sont les seuls éléments de norme 1 dans $\mathbb{H}(\mathbb{Z})$. □

Proposition 8. *Chaque $\alpha \in \mathbb{H}(\mathbb{Z}) \setminus \{0\}$ peut s'écrire comme un produit de quaternions irréductibles.*

Preuve: On procède par récurrence sur $N(\alpha)$. $N(\alpha) \neq 0$ quel que soit $\alpha \in \mathbb{H}(\mathbb{Z}) \setminus \{0\}$. Si $N(\alpha) = 1$, alors α est inversible, donc un produit de zéro irréductibles. Supposons donc $N(\alpha) > 1$. Si α est irréductible, il n'y a rien à prouver ; sinon, on trouve β, γ dans $\mathbb{H}(\mathbb{Z})$, tels que $\alpha = \beta\,\gamma$ et que ni β, ni γ est inversible. Cela entraîne $N(\beta)$, $N(\gamma) > 1$. Or $N(\alpha) = N(\beta)\,N(\gamma)$ par la Remarque 6, d'où $N(\beta)$, $N(\gamma) < N(\alpha)$. Par l'hypothèse, β et γ sont produits d'irréductibles, d'où α l'est aussi. □

Proposition 9. *Si $\delta \in \mathbb{H}(\mathbb{Z})$ est irréductible, alors $N(\delta)$ est un nombre premier dans $\mathbb{Z}$.*

Preuve: Cf. [1], p.66, Corollary 2.6.10. pour la preuve. □

2.3.3 Quaternions sur $\mathbb{F}_q$

Regardons maintenant les quaternions sur le corps fini $\mathbb{F}_q$ à q éléments (où q est premier et impair). On a le lemme suivant :

Lemme. *L'équation $1 + x^2 + y^2 = 0$ admet une solution dans $\mathbb{F}_q$, q premier et impair.*

Preuve: Les ensembles $A = \{1 + x^2 : x \in \mathbb{F}_q\}$ et $B = \{-y^2 : y \in \mathbb{F}_q\}$ sont deux ensembles à $\frac{q+1}{2}$ éléments. Pour le voir, on considère l'homomorphisme $\varphi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times,\ x \mapsto x^2$. Le noyau contient certainement $\{-1, 1\}$ (et $-1 \neq 1$ car $q \neq 2$) et chaque élément a du noyau satisfait $a^2 - 1 = 0$, donc $(a-1)(a+1) = 0$, d'où $a = \pm 1$. On obtient donc

$$|\mathrm{Im}\,(\varphi)| = \frac{|\mathbb{F}_q^\times|}{|\ker(\varphi)|} = \frac{q-1}{2}$$

En comptant aussi 0, on obtient le résultat pour A et B. Comme $|\mathbb{F}_q| = q$, A et B se rencontrent forcément. □

Ce lemme montre aussi, que $\mathbb{H}(k)$ (où k est un corps) n'est pas forcément un corps (certes non-commutatif). Pour x, $y \in \mathbb{F}_q$ tel que $1 + x^2 + y^2 = 0$ et $\alpha = 1 + yi + xj \in \mathbb{H}(\mathbb{F}_q)$, on a $\alpha\overline{\alpha} = N(\alpha) = 0$ et α, $\overline{\alpha} \neq 0$, d'où α n'est pas inversible. Examinons maintenant la structure de $\mathbb{H}(\mathbb{F}_q)$: fixons x et y qui satisfont $1 + x^2 + y^2 = 0$ et considérons l'application

$$\Phi_q : \mathbb{H}(\mathbb{F}_q) \longrightarrow \mathrm{M}_2(\mathbb{F}_q), \quad \alpha = a_1 + a_2 i + a_3 j + a_4 k \longmapsto \begin{pmatrix} a_1 + a_2 x + a_4 y & -a_2 y + a_3 + a_4 x \\ -a_2 y - a_3 + a_4 x & a_1 - a_2 x - a_4 y \end{pmatrix}$$

Proposition 10. *Φ_q est un isomorphisme d'anneaux. Il vérifie* $\det(\Phi_q(\alpha)) = N(\alpha)$ *pour tout* $\alpha \in \mathbb{H}(\mathbb{F}_q)$ *; de plus,* $\Phi_q(\alpha\,\overline{\alpha}) = \Phi_q(\overline{\alpha}\,\alpha)$ *est une matrice scalaire.*

Preuve: Comme $\mathbb{H}(\mathbb{F}_q)$ est bien un $\mathbb{F}_q$-espace vectoriel de base $1, i, j, k$ et $\mathrm{M}_2(\mathbb{F}_q)$ l'est aussi (on prend $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ comme base), on peut réécrire Φ_q de la manière suivante en une application linéaire $\widetilde{\Phi}_q : \mathbb{F}_q^4 \to \mathbb{F}_q^4$, où

$$\widetilde{\Phi}_q(\alpha) = \widetilde{\Phi}_q(a_1, a_2, a_3, a_4) = \begin{pmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 0 & -x & 0 & -y \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

La matrice de $\widetilde{\Phi}_q$ est inversible (son déterminant vaut $2 \not\equiv 0 \pmod q$), donc $\widetilde{\Phi}_q$ est un isomorphisme d'espaces vectoriels et Φ_q lui-même aussi.

Il reste à démontrer la multiplicativité de Φ_q. Ecrivons $e_1 = 1$, $e_2 = i$, $e_3 = j$ et $e_4 = k$. Pour $\alpha = \sum_{i=1}^4 a_i\, e_i,\ \beta = \sum_{j=1}^4 b_j\, e_j \in \mathbb{H}(\mathbb{F}_q)$, on a

$$\Phi_q(\alpha\,\beta) = \Phi_q(\sum_{i,j=1}^4 a_i b_j e_i e_j) = \sum_{i,j=1}^4 a_i b_j \Phi_q(e_i\, e_j)$$

et

$$\Phi_q(\alpha)\,\Phi_q(\beta) = \sum_{i=1}^4 a_i \Phi_q(e_i) \sum_{j=1}^4 b_j \Phi_q(e_j) = \sum_{i,j=1}^4 a_i b_j \Phi_q(e_i)\Phi_q(e_j)$$

par la linéarité de Φ_q. Φ_q est donc multiplicative, si $\Phi_q(e_i\, e_j) = \Phi_q(e_i)\Phi_q(e_j)$ pour $1 \le i, j \le 4$. Notons que

$$\Phi_q(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \Phi_q(e_2) = \begin{pmatrix} x & -y \\ -y & -x \end{pmatrix},\ \Phi_q(e_3) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\quad \Phi_q(e_4) = \begin{pmatrix} y & x \\ x & -y \end{pmatrix}$$

En calculant tous les produits de ces éléments, on vérifie que la condition ci-dessus est bien remplie. Donc, Φ_q est multiplicative et l'anneaux $\operatorname{Im}\Phi_q = \mathrm{M}_2(\mathbb{F}_q)$ est isomorphe à $\mathbb{H}(\mathbb{F}_q)$. □

2.4 Groupes finis

Nous venons de constater dans la Proposition 10 que $\mathbb{H}(\mathbb{F}_q) \cong \mathrm{M}_2(\mathbb{F}_q)$, q premier, $\neq 2$. Donc $\mathrm{GL}_2(q)$, le groupe des matrices 2×2 inversible à coefficients dans $\mathbb{F}_q$ est isomorphe à $\mathbb{H}(\mathbb{F}_q)^\times$. Il est pourtant quelquefois plus commode de travailler dans $\mathrm{GL}_2(q)$, car par exemple le nombre d'éléments est facile à estimer. Ainsi utilise-t-on les groupes suivants dans la construction de nos graphes.

Le groupe $\mathrm{GL}_2(q)$
Le nombre d'éléments de $\mathrm{GL}_2(q)$ est $q\,(q-1)\,(q^2-1)$. En effet, on a (q^2-1) possibilités de choisir la première colonne d'une matrice inversible et on en a $q^2 - q$ pourque la deuxième colonne reste linéairement indépendante de la première.

Le groupe $\mathrm{SL}_2(q)$
Le sous-groupe $\mathrm{SL}_2(q)$ de $\mathrm{GL}_2(q)$ est formé des matrices de déterminant 1. On a donc $\mathrm{SL}_2(q) = \ker(\det : \mathrm{GL}_2(q) \to \mathbb{F}_q^\times)$, ce qui entraîne

$$|\mathrm{SL}_2(q)| = |\ker \det| = \frac{|\mathrm{GL}_2(q)|}{|\mathrm{Im}\ \det|} = q(q^2-1)$$

car det est surjective.

Le groupe $\mathrm{PGL}_2(q)$
Notons $\mathcal{Z}(\mathrm{GL}_2(q))$ le centre de $\mathrm{GL}_2(q)$. Comme $\mathrm{GL}_2(q) \cong \mathbb{H}(\mathbb{F}_q)^\times$ via l'isomorphisme Φ_q, la Remarque 6 nous montre que $\mathcal{Z}(\mathrm{GL}_2(q))$ est formé de matrices scalaires. On définit alors $\mathrm{PGL}_2(q)$ comme le quotient de $\mathrm{GL}_2(q)$ par son centre et il s'ensuit que $|\mathrm{PGL}_2(q)| = q\,(q^2-1)$.

Le groupe $\mathrm{PSL}_2(q)$
Soit $\kappa_q : \mathrm{GL}_2(q) \to \mathrm{PGL}_2(q)$ ce passage au quotient. On pose $\mathrm{PSL}_2(q) = \kappa_q(\mathrm{SL}_2(q))$. Pour calculer l'ordre de $\mathrm{PSL}_2(q)$, on regarde la restriction de κ_q sur $\mathrm{SL}_2(q)$. Le noyau de cette restriction est l'intersection du noyau de κ_q avec $\mathrm{SL}_2(q)$, donc égal à $\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)\}$. Comme $q \neq 2$, ceci sont deux éléments différents. On obtient donc

$$|\mathrm{PSL}_2(q)| = \frac{|\mathrm{SL}_2(q)|}{|\ker \kappa_q \cap \mathrm{SL}_2|} = \frac{1}{2}\,q\,(q^2-1)$$

Remarque 11. *Soit $A \in \mathrm{GL}_2(q)$. On a $\kappa_q(A) \in \mathrm{PSL}_2(q)$ si et seulement si $\det A$ est un carré dans $\mathbb{F}_q$.*

Preuve: $\kappa_q(A) \in \mathrm{PSL}_2(q) \Leftrightarrow A = b \cdot C$, où $C \in \mathrm{SL}_2(q)$ et $b \in \mathbb{F}_q \Leftrightarrow 1 = \det C = \det(b^{-1} \cdot A) = b^{-2} \cdot A \Leftrightarrow \det A = b^2$ un carré dans $\mathbb{F}_q$. □

Dans la preuve du Théorème 21, on va utiliser une propriété des sous-groupes propres de $\mathrm{PSL}_2(q)$, énoncée dans le théorème suivant. Ici, on note $[g,h] = g\,h\,g^{-1}h^{-1}$ le commutateur de deux éléments g et h de $\mathrm{PSL}_2(q)$.

Théorème 12. (Dickson) *Soit q un nombre premier, $q \geq 7$. Alors chaque sous-groupe propre H de $\mathrm{PSL}_2(q)$ d'ordre $|H| > 60$ est métabélien, i.e. $[[g_1,g_2],[g_3,g_4]] = 1$ pour tous g_1, g_2, g_3, $g_4 \in H$.*

Preuve: Cf. [1], Theorem 3.3.4. pour la preuve. □

3 Les Graphes $X_{p,q}$

Passons maintenant à la construction de notre famille de graphes $X_{p,q} = \mathcal{G}(\Gamma_{p,q}, S_{p,q})$. Dorénavant, supposons que p et q sont deux nombres premiers impairs distincts et que $p \equiv 1 \pmod 4$. Afin de définir notre ensemble $S_{p,q}$, retournons aux $(p+1)$ solutions de

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = p, \qquad x_1, x_2, x_3, x_4 \in \mathbb{Z}, \qquad x_1 \text{ impair et } x_1 > 0$$

Chacune de ces solutions nous fournit un quaternion entier. Notons S_p l'ensemble des quaternions obtenus dans $\mathbb{H}(\mathbb{Z})$. Puis, considérons la réduction modulo q,

$$\rho_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$$

que l'on compose avec l'isomorphisme $\Phi_q : \mathbb{H}(\mathbb{F}_q) \to \mathrm{M}_2(\mathbb{F}_q)$ de (2.3.3). Soit $\alpha \in S_p$, alors $\det(\Phi_q \circ \rho_q)(\alpha) = N(\alpha) = p \neq 0$ dans $\mathbb{F}_q$, car $p \neq q$, d'où $(\Phi_q \circ \rho_q)(\alpha)$ est une matrice inversible. De plus, on constate que $\overline{\alpha}$ est dans S_p pour tout $\alpha \in S_p$ et que $(\Phi_q \circ \rho_q)(\alpha\,\overline{\alpha})$ est une matrice scalaire. Cela suggère de passer au quotient par les matrices scalaires et de travailler dans $\mathrm{PGL}_2(q)$ – afin de remplir la condition $S^{-1} \subset S$. On pose

$$S_{p,q} = \kappa_q \circ \Phi_q \circ \rho_q(S_p)$$

Proposition 13.

1. ${S_{p,q}}^{-1} \subset S_{p,q}$.
2. *Si* $q > 2\sqrt{p}$, *alors* $(\kappa_q \circ \Phi_q \circ \rho_q)_{|S_p}$ *est injective et* $1 \notin S_{p,q}$.

Preuve: Ecrivons $\alpha = a_1 + a_2\,i + a_3\,j + a_4\,k$ et $\beta = b_1 + b_2\,i + b_3\,j + b_4\,k \in \mathbb{H}(\mathbb{Z})$.

1. L'inverse de $A = (\kappa_q \circ \Phi_q \circ \rho_q)(\alpha)$ est l'image de $\overline{\alpha} \in S_p$ sous $\kappa_q \circ \Phi_q \circ \rho_q$.

2. Montrons d'abord que $\rho_{q|S_p}$ est injectif : supposons que α et β sont deux éléments différents de S_p. Alors, il existe un $i \in \{1,2,3,4\}$ tel que $a_i \neq b_i$. Par $a_i^2,\ b_i^2 \leq p$, on sait que $a_i,\ b_i \in [-\sqrt{p}, \sqrt{p}\,]$. Or $q > 2\sqrt{p}$, d'où $a_i \not\equiv b_i \pmod q$ (en effet, si $a_i = b_i + tq,\ t \in \mathbb{N} \setminus \{0\}$, alors $|a_i - b_i| = |t|\,q > 2\sqrt{p}$, une contradiction). Alors, $\rho(\alpha) \neq \rho(\beta)$.

Soient ensuite $A = \Phi_q(\rho_q(\alpha))$, $B = \Phi_q(\rho_q(\beta))$. Alors, $\kappa_q(A) = \kappa_q(B)$ implique $A = c \cdot B$ avec $c \in \mathbb{F}_q^\times$. En appliquant le déterminant, on obtient $\det A = c^2 \cdot \det B$ avec $\det A = \det B = p \neq 0$ dans $\mathbb{F}_q$, d'où $c^2 = 1$ et puis $c = \pm 1$. Mais $c = -1$ entraîne $A = -B$, d'où $\alpha \equiv -\beta \pmod q$ ce qui est équivalent à $a_i + b_i = tq$ pour $1 \leq i \leq 4$, où $t \in \mathbb{Z}$. De nouveau, on a $a_i,\ b_i \in [-\sqrt{p}, \sqrt{p}\,]$ pour $1 \leq i \leq 4$, ce qui implique $a_i + b_i \in [-2\sqrt{p}, 2\sqrt{p}\,]$ et puis $t = 0$, car $q > 2\sqrt{p}$. On obtient enfin $\alpha = -\beta$ dans $\mathbb{H}(\mathbb{Z})$, donc $a_1 = -b_1$, ce qui contredit le fait que $a_1,\ b_1 > 0$. Alors, $c = 1$ et $\alpha = \beta$.

Pour le dernier point, supposons par l'absurde qu'il existe un $\alpha \in S_p$, tel que $(\kappa_q \circ \Phi_q \circ \rho_q)(\alpha) = 1 \in \mathrm{PGL}_2(q)$. Donc $\Phi_q(\rho_q(\alpha)) = c \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right),\ c \in \mathbb{F}_q^\times$. Alors, $c \cdot 1 = \rho_q(\alpha)$, d'où $\alpha - \hat{c} \equiv 0 \pmod q$ avec $\hat{c} \in c = \hat{c} + q\mathbb{Z}$. Donc, $a_2,\ a_3,\ a_4 \in q\mathbb{Z}$. Encore une fois, on utilise le fait que $|a_i| \leq \sqrt{p},\ 1 \leq i \leq 4$ et on déduit de $q > 2\sqrt{p}$ que $a_2 = a_3 = a_4 = 0$ dans $\mathbb{Z}$. Mais cela revient à dire que $a_1^2 = p$ dans $\mathbb{Z}$, une contradiction. □

On remarque que $S_{p,q} \subset \mathrm{PSL}_2(q)$ si et seulement si p est un carré dans $\mathbb{F}_q$ en utilisant Remarque 11, car $\det(\Phi_q \circ \rho_q)(\alpha) = p$ pour tout $\alpha \in S_p$.

Définition. Soit $q > 2\sqrt{p}$. On distingue les deux cas :

1. Si p est un carré dans $\mathbb{F}_q$, alors $S_{p,q} \subset \mathrm{PSL}_2(q)$ et on définit

$$X_{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q}).$$

Ceci est un graphe $(p+1)$-régulier à $\frac{1}{2}\,q\,(q^2-1)$ sommets.

2. Si p n'est pas un carré dans $\mathbb{F}_q$, alors $S_{p,q} \subset \mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$ et on définit

$$X_{p,q} = \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q}).$$

Ceci est un graphe $(p+1)$-régulier à $q\,(q^2-1)$ sommets.

Il reste encore à démontrer que ce graphe est bien connexe : cela revient à dire que $S_{p,q}$ est une partie génératrice du groupe correspondant. Ensuite, on voudrait estimer le tour de taille de $X_{p,q}$. Dans la partie suivante, on abordera ces deux problèmes en construisant des graphes $Y_{p,q}$ que l'on comparera aux graphes $X_{p,q}$.

4 Les Graphes $Y_{p,q}$

Notre point de départ est l'ensemble

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : N(\alpha) = p^k\,,\, k \in \mathbb{N} \text{ et } \alpha \equiv 1 \,(\mathrm{mod}\ 2)\}.$$

On vérifie facilement, que Λ' est un monoïde multiplicatif dans $\mathbb{H}(\mathbb{Z})$ et que $S_p \subset \Lambda'$. L'objectif est maintenant de construire à partir de Λ' un groupe libre Λ qui est engendré par S_p.

Définition. *Un mot ω sur l'alphabet S_p* est un élément $\omega = \alpha_1 \cdots \alpha_m$ de Λ', où $\alpha_i \in S_p$ pour $1 \le i \le m$, avec $m > 0$ (ou $\omega = 1$ et $m = 0$). Dans ce cas, *la longueur d'un mot* est m. On dit qu'un mot est *réduit* lorsqu'il ne contient aucun sous-mot de la forme $\alpha\,\overline{\alpha}$ ou $\overline{\alpha}\,\alpha$.

Théorème 14. *Soit $\alpha \in \Lambda'$ et $N(\alpha) = p^r, r \in \mathbb{N}$. Alors α s'écrit de façon unique*

$$\alpha = \varepsilon\, p^k\, \omega_m,$$

où $\varepsilon \in \{\pm 1\}$, ω_m est un mot réduit de longueur m sur S_p et $k \in \mathbb{N}$ vérifie $r = 2k + m$.

Preuve: On montre d'abord l'existence d'une telle écriture : Par la Proposition 8, on sait qu'il existe des éléments irréductibles $\delta_1, \ldots \delta_s \in \mathbb{H}(\mathbb{Z})$, tels que

$$\alpha = \delta_1 \cdots \delta_s$$

Comme $N(\delta_i)$ divise $p^r = N(\alpha)$ et comme $N(\delta_i)$ est un nombre premier (cf. Proposition 9), on a $N(\delta_i) = p$ pour tout i, d'où $s = r$.
Pour i fixé, il existe maintenant $\varepsilon_i \in \mathbb{H}(\mathbb{Z})^\times$ et $\gamma_i \in S_p$, tels que $\delta_i = \varepsilon_i\,\gamma_i$. En effet, si $\delta_i = d_1 + d_2\,i + d_3\,j + d_4\,k$, on déduit de $N(\delta_i) = p \equiv 1 \,(\mathrm{mod}\ 4)$, qu'il existe un unique $j \in \{1,2,3,4\}$ tel que d_j est impair. Soit e_j le symbole de $\{1,i,j,k\}$ correspondant à la j-ième coordonnée. On pose alors $\widetilde{\varepsilon_i} = \mathrm{sign}(d_j)\,e_j \in \mathbb{H}(\mathbb{Z})^\times$, d'où $\gamma_i = \widetilde{\varepsilon_i}\,\delta_i \in S_p$ et $\delta_i = \varepsilon_i\,\gamma_i$, si l'on pose $\varepsilon_i = \widetilde{\varepsilon_i}^{-1}$.
Donc, α s'écrit de la manière

$$\alpha = \varepsilon_1\,\gamma_1 \cdots \varepsilon_r\,\gamma_r$$

En appliquant le raisonnement au-dessus à un élément de la forme $\gamma\,\varepsilon$ avec $\gamma \in S_p\,, \varepsilon \in \mathbb{H}(\mathbb{Z})^\times$, on trouve $\gamma' \in S_p$ et $\varepsilon' \in \mathbb{H}(\mathbb{Z})^\times$, tels que $\gamma\,\varepsilon = \varepsilon'\,\gamma'$. Donc on peut mettre tous les inversibles à gauche et écrire

$$\alpha = \varepsilon\,\gamma_1' \cdots \gamma_r'$$

avec un inversible ε et des éléments $\gamma_i' \in S_p$, $1 \leq i \leq r$. Afin d'obtenir un mot réduit, on sort tous les facteurs de la forme $\gamma' \overline{\gamma}'$ ou $\overline{\gamma}' \gamma'$ qui donnent un facteur p et on obtient alors

$$\alpha = \varepsilon \, p^k \, \omega_m$$

avec ω_m un mot réduit de longueur $m \in \mathbb{N}$ et $k \in \mathbb{N}$ tel que $r = 2k + m$. Regardons cette équation modulo 2 : Comme $p \equiv 1 \,(\mathrm{mod}\ 2)$ et α, $\omega_m \equiv 1 \,(\mathrm{mod}\ 2)$, on a

$$1 \equiv \alpha \equiv \varepsilon \,(\mathrm{mod}\ 2)$$

d'où $\varepsilon \in \{\pm 1\}$, ce qui montre l'existence.

Pour montrer l'unicité, nous allons compter le nombre de mots réduits sur S_p et le comparer au nombre de solutions donné par le Théorème de Jacobi 4. Ce théorème nous dit que l'équation $N(\alpha) = p^r$, possède

$$8 \sum_{d|p^r} d = 8 \left(\frac{p^{r+1} - 1}{p - 1} \right) \quad \text{solutions pour } \alpha \in \mathbb{H}(\mathbb{Z})$$

Tenant compte du fait que l'on a fixé la coordonnée impaire si $\alpha \in \Lambda'$, il y a exactement

$$2 \left(\frac{p^{r+1} - 1}{p - 1} \right) \text{ possibilités pour } \alpha \in \Lambda'$$

D'autre part, le nombre de mots réduits de longueur m est

$$\begin{cases} 1 & \text{si } m = 0 \\ (p+1)\, p^{\,m-1} & \text{si } m > 0 \end{cases}$$

Ceci découle du fait que pour un mot de longueur $m > 0$, on a $(p + 1)$ possibilités pour la première lettre et p possibilités pour chaque lettre suivante, car on doit éviter tout sous-mot de la forme $\gamma \overline{\gamma}$ et $\overline{\gamma} \gamma$. Ensuite, on compte le nombre d'expressions de la forme $\varepsilon \, p^k \, \omega_m$, où $\varepsilon \in \{\pm 1\}$, ω_m est un mot réduit de longueur m et $2k + m = r$. Selon la parité de r, m est ou bien toujours pair, ou bien toujours impair. Donc, on obtient

$$\begin{cases} 2 \left(1 + \displaystyle\sum_{\substack{0<m\leq r \\ m \text{ pair}}} (p+1)\, p^{\,m-1} \right) = 2 \left(1 + \displaystyle\sum_{\substack{0<m\leq r \\ m \text{ pair}}} p^{\,m} + p^{\,m-1} \right) & \text{si } r \text{ est pair} \\ 2 \left(\displaystyle\sum_{\substack{0<m\leq r \\ m \text{ impair}}} (p+1)\, p^{\,m-1} \right) = 2 \left(\displaystyle\sum_{\substack{0<m\leq r \\ m \text{ impair}}} p^{\,m} + p^{\,m-1} \right) & \text{si } r \text{ est impair} \end{cases}$$

ce qui se simplifie dans chaque cas en $2\,(p^{r+1} - 1)/(p - 1)$, donc le nombre d'éléments coïncide. Or, on sait par l'existence, que chaque α de norme $p^r, r \in \mathbb{N}$ et dont la première coordonnée est impaire, s'écrit de cette façon, d'où une telle écriture doit être unique. $\square$

Notons ensuite, que $\alpha \in S_p$ entraîne $\overline{\alpha} \in S_p$ et que $\alpha \neq \overline{\alpha}$. On peut donc écrire S_p de la façon

$$S_p = \{\alpha_1, \ldots, \alpha_{\frac{p+1}{2}}, \overline{\alpha}_1, \ldots, \overline{\alpha}_{\frac{p+1}{2}}\}$$

Pour faire apparaître un groupe libre, on considère la relation d'équivalence $\sim$ sur Λ' définie par

$$\alpha \sim \beta \text{ si et seulement s'il existe } \varepsilon \in \{\pm 1\},\ k,\ l \in \mathbb{N} \text{ tels que } p^k\alpha = \varepsilon\, p^l\beta$$

On note $\Lambda = \Lambda'/\sim$ et $\tau : \Lambda' \to \Lambda,\ x \mapsto [x]$ l'application quotient. La remarque suivante nous montre que l'on peut considérer S_p comme une partie de Λ, que nous allons noter $[S_p]$.

Remarque 15. *$\tau_{|S_p}$ est injective.*

Preuve: Soient $\alpha,\ \beta \in S_p$ tels que $[\alpha] = [\beta]$. Il existe $\varepsilon \in \{\pm 1\}$, k,$l \in \mathbb{N}$ tels que $p^k\alpha = \varepsilon\, p^l\beta$. Supposons $l \geq k$, alors $\alpha = \varepsilon p^{l-k}\beta$. Mais α est réduit, d'où $\alpha = \beta$ par le Théorème 14. On traite le cas $l < k$ analoguement. □

Corollaire 16. *Λ est un groupe libre sur les $\frac{p+1}{2}$ générateurs $\{[\alpha_1], \ldots, [\alpha_{\frac{p+1}{2}}]\}$.*

Preuve: Il est facile à démontrer que $\sim$ est compatible avec la multiplication dans Λ'. Donc, Λ est un monoïde. Puis, soit $[\alpha] \in \Lambda$, alors $[\overline{\alpha}]$ est l'inverse, car $[\alpha]\,[\overline{\alpha}] = [\overline{\alpha}]\,[\alpha] = [N(\alpha)] = [1]$. Donc Λ est un groupe.

Notons d'abord que $\Sigma = \{[\alpha_1], \ldots, [\alpha_{\frac{p+1}{2}}]\}$ est bien un ensemble à $\frac{p+1}{2}$ éléments par Remarque 15. Afin de montrer que Λ est libre de base Σ, on considère le Théorème 14 qui se lit dans ce contexte de la manière suivante : Σ engendre Λ et chaque classe d'équivalence $[\omega] \in \Lambda$ a un unique représentant $\widehat{\omega}$ qui est un mot réduit sur Σ. Il reste donc à vérifier la propriété de groupe libre ci-dessous. □

Proposition 17. *Soit G un groupe et X une partie génératrice de G. Supposons que pour chaque élément $\omega \in G$, il existe un unique entier m et d'uniques $x_{i_1}, \ldots, x_{i_m} \in X$ et $\varepsilon_k \in \{\pm 1\}, 1 \leq k \leq m$, tels que*

$$\begin{cases} \omega = 1 & \text{si } m = 0 \\ \omega = x_{i_1}^{\varepsilon_1} \cdots x_{i_m}^{\varepsilon_m} & \text{si } m > 0, \quad \text{où } \ x_{i_k}^{\varepsilon_k} \neq x_{i_{k+1}}^{-\varepsilon_{k+1}} \text{ pour tout } 1 \leq k \leq m-1. \end{cases}$$

Alors G est libre de base X.
En d'autres termes, chaque mot sur X a un unique représentant réduit. Ici, la notion d'un mot réduit est plus générale (un mot ω sur X s'appelle réduit, s'il ne contient aucun sous-mot de la forme $x\,x^{-1}$ ou $x^{-1}x$ avec $x \in X$).

Preuve: Soit $L(X)$ le groupe libre de base X. Par la propriété universelle de $L(X)$, il existe un unique morphisme de groupes $\varphi : L(X) \to G$, tel que le diagramme commute. On va montrer que φ est un isomorphisme.

Notons d'abord qu'on a $\varphi(\iota(x)) = x$ pour tout $x \in X$. Comme φ est un morphisme, l'antécédent d'un élément $x_{i_1}^{\varepsilon_1} \cdots x_{i_m}^{\varepsilon_m} \in G$, où $x_{i_k} \in X$, $\varepsilon_k \in \{\pm 1\}$, $1 \leq k \leq m$ est l'élément $\iota(x_{i_1})^{\varepsilon_1} \cdots \iota(x_{i_m})^{\varepsilon_m}$ dans $L(X)$. Or, X est une partie génératrice de G, d'où φ est surjective.

Supposons ensuite qu'il existe $\omega \in L(X)$, $\omega \neq 1_{L(X)}$, tel que $\varphi(\omega) = 1_G$. L'image de ι dans $L(X)$ est par définition une partie génératrice de $L(X)$, donc il existe $x_{i_k} \in X$, $\varepsilon_k \in \{\pm 1\}$, $1 \leq k \leq m$, tels que $\omega = \iota(x_{i_1})^{\varepsilon_1} \cdots \iota(x_{i_m})^{\varepsilon_m}$. Quitte à remplacer tous les $\iota(x)\,\iota(x)^{-1}$ et

$\iota(x)^{-1}\iota(x)$ dans l'écriture de ω par $1_{L(X)}$, on peut se ramener à

$$\omega = \iota(x_{i_1})^{\varepsilon_1} \cdots \iota(x_{i_m})^{\varepsilon_m}$$

avec $m > 0$ (car $\omega \neq 1_{L(X)}$) et $\iota(x_{i_k}^{\varepsilon_k}) \neq \iota(x_{i_{k+1}})^{-\varepsilon_{k+1}}$ pour $1 \leq k \leq m-1$. Donc

$$1_G = \varphi(\omega) = x_{i_1}^{\varepsilon_1} \cdots x_{i_m}^{\varepsilon_m}$$

et $x_{i_k}^{\varepsilon_k} \neq x_{i_{k+1}}^{-\varepsilon_{k+1}}$, $1 \leq k \leq m-1$ avec $m > 0$. Mais ceci contredit l'unicité de l'écriture dans G, d'où $\ker(\varphi) = \{1_{L(X)}\}$ et φ est injective. Ceci complète la preuve. □

A nouveau, considérons $\rho_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$ la réduction modulo q. Par la propriété universelle de Λ comme groupe libre, on trouve maintenant un unique morphisme π_q', qui fait commuter le diagramme En le composant avec Φ_q et κ_q, nous obtenons un morphisme de groupes

$$\pi_q = (\kappa_q \circ \Phi_q \circ \pi_q') : \Lambda \longrightarrow \mathrm{PGL}_2(q)$$

On observe que $(\pi_q \circ \tau)(S_p) = S_{p,q}$, d'où on peut définir (par Proposition 13) :

Définition. Soit $q > 2\sqrt{p}$. Le graphe $Y_{p,q}$ est défini par

$$Y_{p,q} = \mathcal{G}(\mathrm{Im}\,\pi_q, S_{p,q}).$$

Ceci est un graphe $(p+1)$-régulier, connexe.

Notons que l'on a bien $\mathrm{Im}\,\pi_q \subset \mathrm{PSL}_2(q)$, si p est un carré modulo q. Par la Remarque 3, on sait déjà que $Y_{p,q}$ est un sous-graphe connexe de $X_{p,q}$. Malheureusement, on ne connaît pas a priori le nombre de sommets de $Y_{p,q}$. En revanche, le tour de taille de $Y_{p,q}$ est facile à estimer, car $Y_{p,q}$ est donné comme quotient d'un arbre – l'arbre du groupe libre Λ : la proposition suivante nous en donne une première indication.

Proposition 18. *Soit $L(X)$ le groupe libre de base $\{x_1, \ldots, x_n\}$ et notons $S = \{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\}$. Soit N un sous-groupe normale de $L(X)$ et notons $\pi : L(X) \to L(X)/N$ l'application quotient. Supposons que $\pi_{|S}$ est injective. Alors,*

$$g(\mathcal{G}(L(X), S)) = \min\{m : m \text{ longueur du mot } \omega \in N,\ \omega \neq 1 \text{ sur l'alphabet } S\},$$

i.e. le tour de taille de $\mathcal{G}(L(X), S)$ est le minimum des longueurs des mots différents de 1 dans N.

Preuve: Ecrivons $g = g(\mathcal{G}(L(X), S))$. Pour démontrer l'égalité, construisons d'abord un circuit à partir d'un élément $\omega \in N \setminus \{1\}$. On a $\omega = y_1 \cdots y_m$ avec $y_i \in S$, $1 \leq i \leq m$ et on peut supposer que l'écriture de ω est réduite. Cela implique d'abord $m > 2$:

m n'est pas 1 ; sinon, $\pi(y_1) = 1 = \pi(y_1^{-1})$, mais $y_1 \neq y_1^{-1}$, une contradiction avec $\pi_{|S}$ injective.

m n'est pas 2 ; sinon, $1 = \pi(y_1\, y_2)$, d'où $\pi(y_1) = \pi(y_2^{-1})$, donc $y_1 = y_2^{-1}$ et $\omega = y_1 y_2 = y_2^{-1} y_2$ n'a pas été réduit.

Ensuite, $\prod_{i=1}^{k}\pi(y_i)\neq\prod_{i=1}^{k+2}\pi(y_i)$, $(1\leq k\leq m-2)$, car $\pi(y_{k+1})\neq\pi(y_{k+2})^{-1}$, parce que ω est réduit et $\pi_{|S}$ est injective. Alors

$$C=(1,\pi(y_1),\pi(y_1)\pi(y_2),\ldots,\underbrace{\prod_{i=1}^{m}\pi(y_i)}_{=\pi(\omega)=1_{L(X)/N}})$$

est un circuit de longueur m, ce qui montre que g est inférieur ou égal le minimum sur les m.

Examinons la réciproque. Comme $\mathcal{G}(L(X),S)$ est un graphe de Cayley, on peut supposer que tout circuit dans $\mathcal{G}(L(X),S)$ commence à 1, quitte à translater par un élément de $L(X)$. Soit alors $C=(1,s_1,s_1s_2,\ldots,\prod_{i=1}^{g}s_i)$ un circuit de longueur g, où $s_i\in L(X)/N$, $1\leq i\leq g$. Il existe d'uniques $y_i\in S$ tel que $\pi(y_i)=s_i$, $1\leq i\leq g$. Or, $1=\prod_{i=1}^{g}s_i=\pi(\prod_{i=1}^{g}y_i)$, donc $y=\prod_{i=1}^{g}y_i\in\ker\pi=N$. Si on suppose par l'absurde $y=1$, on trouve un indice $j\in\{1,\ldots,g-2\}$ tel que $\prod_{i=1}^{j}y_i=\prod_{i=1}^{j+2}y_i$ (sinon, y serait un mot réduit sur S de longueur $g>2$, donc $\neq 1$). Mais $\prod_{i=1}^{j}s_i=\pi(\prod_{i=1}^{j}y_i)=\pi(\prod_{i=1}^{j+2}y_i)=\prod_{i=1}^{j+2}s_i$, ce qui viole la condition du circuit.

On a donc trouver un élément y dans $N\setminus\{1\}$ qui s'écrit comme un mot de longueur g sur S. □

Examinons maintenant le noyau de l'application π_q. On a

$$\ker\pi_q=\{[\alpha]\in\Lambda:\alpha=a_1+a_2\,i+a_3\,j+a_4\,k,\ q\text{ divise }a_2,a_3,a_4\}$$

Pour le vérifier, soit $[\alpha]\in\Lambda$, tel que $\pi_q(\alpha)=1$, i.e. $(\kappa_q\circ\Phi_q\circ\rho_q)(\beta)=1$ pour chaque $\beta\in[\alpha]$. Donc $(\Phi_q\circ\rho_q)(\beta)=c\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $c\in\mathbb{F}_q$ et puis $\rho_q(\beta)=c\cdot 1$, ce qui est équivalent à $\beta\equiv\hat{c}\,(\mathrm{mod}\ q)$ avec $\hat{c}\in c=\hat{c}+q\,\mathbb{Z}$. Alors, si $\beta=b_1+b_2\,i+b_3\,j+b_4\,k\in\mathbb{H}(\mathbb{Z})$, on a b_2, b_3, $b_4\equiv 0\,(\mathrm{mod}\ q)$.

Réciproquement, soit $\beta\in[\alpha]$ et $\alpha\equiv a\cdot 1\,(\mathrm{mod}\ q)$, $a\in\mathbb{Z}$. Alors $p^l\beta=\varepsilon\,p^k\alpha$, où k, $l\in\mathbb{N}$ et $\varepsilon\in\{\pm1\}$. Comme p est inversible modulo q, il existe $s\in\mathbb{Z}$ tel que $s\,p\equiv 1\,(\mathrm{mod}\ q)$ et $\beta\equiv\varepsilon\,s^lp^k\alpha\equiv\varepsilon\,s^lp^ka\cdot 1\,(\mathrm{mod}\ q)$ d'où

$$\kappa_q(\Phi_q(\rho_q(\beta)))=\kappa_q(\Phi_q(b\cdot 1))=\kappa(b\begin{pmatrix}1&0\\0&1\end{pmatrix})=1_{\mathrm{PGL}_2(q)}$$

avec $b=\varepsilon\,s^lp^ka\ +q\,\mathbb{Z}$. Ceci est valable quel que soit $\beta\in[\alpha]$, d'où $[\alpha]\in\ker\pi_q$.

Proposition 19. *$g(Y_{p,q})\geq 2\log_p q$. De plus, si p n'est pas un carré dans $\mathbb{F}_q$, alors $g(Y_{p,q})\geq 4\log_p q$.*

Démontrons d'abord un lemme auxiliaire.

Lemme. *Soit $q\in\mathbb{Z}$ un premier impair qui ne divise pas a, $b\in\mathbb{Z}$. Alors*

$$a^2\equiv b^2\,(\mathrm{mod}\ q^2)\implies\left[a\equiv b\,(\mathrm{mod}\ q^2)\quad\text{ou}\quad a\equiv -b\,(\mathrm{mod}\ q^2)\right]$$

Preuve: Comme q est premier, $(a-b)\equiv 0\,(\mathrm{mod}\ q)$ ou $(a+b)\equiv 0\,(\mathrm{mod}\ q)$. Si q divise $(a-b)$ et $(a+b)$, il divise $2a$, donc a (car $q\neq 2$). Supposons donc que q ne divise pas $(a-b)$. Or, le pgcd de $(a-b)$ et q^2 est 1, il existe donc $s\in\mathbb{Z}$ tel que $s(a-b)\in 1+q^2\mathbb{Z}$. Alors

$$(a^2-b^2)\equiv 0\,(\mathrm{mod}\ q^2)\ \Rightarrow\ s(a-b)(a+b)\equiv s\cdot 0\,(\mathrm{mod}\ q^2)\ \Rightarrow\ 1\cdot(a+b)\equiv 0\,(\mathrm{mod}\ q^2)$$

d'où $a \equiv b \,(\mathrm{mod}\ q^2)$. Egalement, on trouve $a \equiv -b \,(\mathrm{mod}\ q^2)$, si l'on suppose que q ne divise pas $(a+b)$. □

Preuve: (de la Proposition)

Notons g pour $g(Y_{p,q})$. Comme Λ est libre et $\mathrm{Im}\,\pi_q \cong \Lambda/\ker \pi_q$, nous allons appliquer Proposition 18 pour $N = \ker \pi_q$. Puis, $\pi_{q|[S_p]} = (\pi_q \circ \tau)_{|S_p} = (\kappa_q \circ \Phi_q \circ \rho_q)_{|S_p}$ est bien injective. Alors

$$g = \min\{m : m \text{ longueur du mot } [\alpha] \in \ker \pi_q,\ [\alpha] \neq [1],\ \text{ sur l'alphabet } [S_p]\}$$

par Proposition 18. Prenons maintenant un $[\alpha] \in \ker \pi_q \setminus \{[1]\}$, où le minimum est atteint, et soit $\alpha = a_1 + a_2\, i + a_3\, j + a_4\, k \in \Lambda'$ son représentant réduit. On obtient alors

$$N(\alpha) = a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{\,g} \tag{3}$$

Comme $[\alpha] \neq [1]$, il existe un $i \in \{2,3,4\}$ tel que a_i est non nul $(*)$. D'autre part, q divise a_2, a_3 et a_4, donc $p^{\,g} \geq a_i^2 = t^2 q^2 \geq q^2$, avec $t \in \mathbb{Z} \setminus \{0\}$. Cela implique

$$g \geq 2\, \log_p q$$

Si p n'est pas un carré modulo q, alors g doit être pair : sinon, on aurait $g = 2k+1$, $k \in \mathbb{N}$; comme $p \not\equiv 0 \,(\mathrm{mod}\ q)$, on trouve $s \in \mathbb{Z}$ tel que $s \cdot p \equiv 1 \,(\mathrm{mod}\ q)$, d'où $p^{\,g} = p^{2k+1} \equiv a_1^2 \,(\mathrm{mod}\ q)$ est équivalent à $p \equiv s^{2k} a_1^2 \equiv (s^k a_1)^2 \,(\mathrm{mod}\ q)$ et p serait un carré modulo q. Donc $g = 2k$, $k \in \mathbb{N}$.

L'équation (3) nous donne en fait

$$p^{2k} \equiv a_1^2 \,(\mathrm{mod}\ q^2)$$

Par le lemme auxiliaire, on trouve

$$p^{\,k} \equiv a_1 \,(\mathrm{mod}\ q^2) \qquad \text{ou} \qquad p^{\,k} \equiv -a_1 \,(\mathrm{mod}\ q^2)$$

et même

$$p^{\,k} \equiv a_1 \,(\mathrm{mod}\ 2q^2) \qquad \text{ou} \qquad p^{\,k} \equiv -a_1 \,(\mathrm{mod}\ 2q^2) \tag{4}$$

parce que p et a_1 sont impairs et $q \neq 2$. De plus, on a $a_1^2 \leq p^{\,g}$, donc $|a_1| \leq p^{\,k}$.

Supposons maintenant par l'absurde $g = 2k < 4\, \log_p q$, ce qui est équivalent à $p^{\,k} < q^2$. Alors

$$|p^{\,k} \mp a_1| \leq p^{\,k} + |a_1| \leq 2\, p^{\,k} < 2q^2$$

Ajouté à l'équation (4), cela nous donne $p^{\,k} = \pm a_1$ et puis $p^{\,g} = a_1^2$. Il s'ensuit que $a_2 = a_3 = a_4 = 0$, une contradiction avec $(*)$. □

Corollaire 20. *$|Y_{p,q}| \geq \frac{q}{p}$. De plus, si p n'est pas un carré modulo q, $|Y_{p,q}| \geq \frac{q^2}{p}$.*

Preuve: Ecrivons $g = g(Y_{p,q})$ et $N = |Y_{p,q}|$. Rappelons l'inégalité de la Proposition 1, qui nous donne

$$g \leq 2 \log_p N + 2 \log_p \left(\frac{p - 1 + 2/N}{p+1} \right) + 2$$

De la Proposition 19, on tire $2\log_p q \leq g$. En réunissant les deux inégalités et en appliquant le logarithme, on obtient

$$q \leq N \cdot \underbrace{\left(\frac{p-1+2/N}{p+1}\right)}_{\leq 1} \cdot p$$

d'où le résultat. Si p n'est pas un carré modulo q, alors $4\log_p q \leq g$ par Proposition 19 et on conclut de la même façon. □

Théorème 21. *Si $q > p^8$, alors $X_{p,q}$ est connexe et donc $Y_{p,q} = X_{p,q}$.*

Preuve:
Il faut montrer que

$$\operatorname{Im}\pi_q = \begin{cases} \mathrm{PSL}_2(q) & \text{si } p \text{ est un carré modulo } q \\ \mathrm{PGL}_2(q) & \text{si } p \text{ n'est pas un carré modulo } q \end{cases}$$

Posons $H = \operatorname{Im}\pi_q \cap \mathrm{PSL}_2(q)$. Alors, il suffit de montrer $H = \mathrm{PSL}_2(q)$. Cela est évident dans le premier cas. Dans le deuxième cas, nous savons déjà que $S_{p,q} \subset \mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$. Or $\mathrm{PSL}_2(q)$ est un sous-groupe d'indice 2 de $\mathrm{PGL}_2(q)$, d'où $\mathrm{PGL}_2(q) = \mathrm{PSL}_2(q) \cup g \cdot \mathrm{PSL}_2(q)$, pour $g \in \mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$ quelconque. Donc, $S_{p,q}$ engendre déjà $\mathrm{PGL}_2(q)$, si $H = PSL_2(q)$.

Afin d'appliquer le théorème 12, il nous faut $|H| > 60$ et il faut démontrer que H n'est pas métabélien. On sait ensuite que H n'est pas un sous-groupe propre, d'où $H = \mathrm{PSL}_2(q)$.

Vérifions d'abord $|H| > 60$: en employant le Corollaire 20 et en utilisant le fait que $p \geq 5$ (par $p \equiv 1 \pmod 4$) et l'hypothèse $q > p^8$, on obtient

$$|Y_{p,q}| = |\operatorname{Im}\pi_q| \geq \frac{q}{p} > 120$$

Si $\operatorname{Im}\pi_q \not\subset \mathrm{PSL}_2(q)$, H reste un sous-groupe d'indice 2 dans $\operatorname{Im}\pi_q$, d'où on obtient $|H| > 60$ dans tous les cas.

Pour démontrer que H n'est pas métabélien, on va trouver quatre éléments g_1, g_2, g_3, $g_4 \in H$ tels que

$$[[g_1, g_2], [g_3, g_4]] \neq 1.$$

Si d'abord p est un carré modulo q, alors on choisit quatre éléments de $S_{p,q} \subset H$ de la manière suivante : soit $g_1 \in S_{p,q}$ quelconque, prenons $g_2 \in S_{p,q}$ tel que $g_2 \notin \{g_1^{\pm 1}\}$. Puis, on pose $g_3 = g_1$ et on choisit $g_4 \in S_{p,q}$ tel que $g_4 \notin \{g_1^{\pm 1}, g_2^{\pm 1}\}$. Notons que cela est possible, grâce à $|S_{p,q}| = p + 1 \geq 6$. En calculant $[[g_1, g_2], [g_3, g_4]]$, on trouve un mot réduit de longueur 16 sur $S_{p,q}$. Or, par Proposition 19, $g(Y_{p,q})$ satisfait

$$g(Y_{p,q}) \geq 2\,\log_p q > 16 \qquad (\text{car } q > p^8)$$

et par conséquent, tout mot réduit de longueur 16 sur $S_{p,q}$, ne peut être égal 1, parce qu'il nous fournirait un circuit de longueur inférieure ou égale 16 dans $Y_{p,q}$.

Si p n'est pas un carré modulo q, on choisit d'abord trois éléments h_1, h_2, $h_3 \in S_{p,q}$ comme suit : soit $h_1 \in S_{p,q}$ quelconque, h_2, tel que $h_2 \notin \{h_1^{\pm}\}$ et h_3, tel que $h_3 \notin \{h_1^{\pm}, h_2^{\pm}\}$. Puis, on définit $g_1 = h_1 h_3$, $g_2 = h_2 h_3$, $g_3 = h_1 h_2$ et $g_4 = h_3 h_2$. Comme H est un sous-groupe d'indice 2, les g_i sont dans H (ils sont produits de deux éléments de $\operatorname{Im}\pi_q \setminus H$). Ensuite,

$[g_1, g_2] = h_1 h_3 h_2 h_1^{-1} h_3^{-1} h_2^{-1}$ et $[g_3, g_4] = h_1 h_2 h_3 h_1^{-1} h_2^{-1} h_3^{-1}$ et $[[g_1, g_2], [g_3, g_4]]$ est un mot réduit de longueur 24 sur $S_{p,q}$. En utilisant la Proposition 19, on obtient

$$g(Y_{p,q}) \geq 4 \log_p q > 24 \qquad (\text{car } q > p^8)$$

et on conclut par le même argument qu'au premier cas. □

Corollaire 22. *Soit $q > p^8$. Alors le graphe $X_{p,q}$ est $(p+1)$-régulier et connexe. De plus, on peut estimer le tour de taille $g(X_{p,q})$é*

1. *Si p est un carré modulo q, alors*

$$g(X_{p,q}) \geq \frac{2}{3} \log_p |X_{p,q}|$$

2. *Si p n'est pas un carré modulo q, alors*

$$g(X_{p,q}) \geq \frac{4}{3} \log_p |X_{p,q}|$$

Preuve: Il ne reste que les estimations à montrer. On sait déjà

$$|X_{p,q}| = \left\{ \begin{array}{ll} \frac{1}{2} q^2 (q-1) & \text{si } p \text{ est un carré modulo } q \\ q^2 (q-1) & \text{si } p \text{ n'est pas un carré modulo } q \end{array} \right\} \leq q^3$$

En employant Proposition 19, on obtient le résultat. □

5 Conclusion

Remarquons d'abord que la constante 4/3, trouvée dans le cas où p n'est pas un carré modulo q, est déjà optimale. En effet, un travail de Biggs et Boshier montre que

$$g(X_{p,q}) \leq 4 \log_p q + \log_p 4 + 2$$

d'où on obtient le résultat puisque $|X_{p,q}|$ croît cubique en q.

Par ailleurs, on peut affaiblir les hypothèses utilisées. La restriction $p \equiv 1 \pmod 4$ n'est pas vraiment nécessaire. On peut également construire les graphes $X_{p,q}$ et montrer leur connexité dans le cas $p \equiv 3 \pmod 4$. Même la borne inférieure de $g(X_{p,q})$, trouvée dans Corollaire 22 est seulement modifiée par un terme d'ordre $o(1)$. Plus précisément,

$$g(X_{p,q}) \geq 4 \log_p q - \log_p 4$$

dans le cas, où p n'est pas un carré modulo q (cf. Proposition 19). Cependant, on ne trouve pas de groupe libre dans le cas $p \equiv 3 \pmod 4$, car S_p a une structure différente. Le fait que l'on s'est limité au cas $p \equiv 1 \pmod 4$ n'a donc pour but que de dégager plus de structures sousjacentes.

Notons enfin, que les graphes $X_{p,q}$ ont encore plus de bonnes propriétés. Ils sont en fait des graphes de Ramanujan (cf. [1], p.114, Theorem 4.2.2., Remark 4.2.3.). Pourtant, il n'y a – à ma connaissance – pas de moyens de le démontrer avec des méthodes élémentaires.

Références

[1] **G. Davidoff, P. Sarnak, A. Valette,** *"Elementary number theory, group theory and Ramanujan graphs"*, Cambridge University Press, London Math. Soc. Student Texts 55 (2003)

[2] **A. Valette,** *"Graphes à grand tour de taille"*, Images des mathématiques (2004)

[3] **P. Erdös, H. Sachs,** *Reguläre Graphen gegebener Taillenweite mit minimaler Knollenzahl*, Wiss. Z. Univ. Halle-Wittenberg Math. Nat. R., (1963), p.251-258