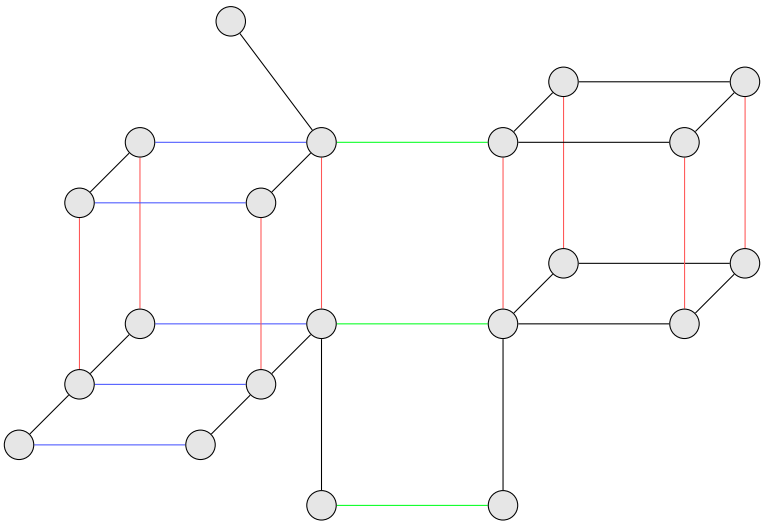
Lecture dirigée de recherche : La géométrie des groupes de cactus

Enzo PERRIER et Étienne AFFALOU

Supervisé par Bert WIEST

Janvier-Mars 2024



Des hyperplans dans un graphe médian.

Résumé

Les groupes de cactus, définis par générateurs et relations, apparaissent dans différents domaines des mathématiques. En vue de donner une solution efficace et explicite au problème de conjugaison et au problème du mot, on prouve que les graphes de Cayley des groupes de cactus sont médians. Cette propriété relève de la théorie géométrique des groupes dont on utilise les premières notions.

Ce document se base sur la lecture de l'article d'Anthony Genevois, *Cactus groups from the viewpoint of geometric group theory*. Toutes les références bibliographiques se trouvent à la fin du document.

Remerciements

Nous remercions Bert Wiest pour sa gentillesse, pour sa patience, pour nous avoir sortis des mauvaises pistes et pour nous avoir éclairé sur le vocabulaire de la théorie géométrique des groupes, bien différent de celui de la théorie des groupes élémentaire. Redécouvrir la théorie des groupes sous un nouvel angle était fascinant, merci encore à Bert Wiest d'avoir proposé ce sujet de lecture dirigée.

Table des matières

1 Groupes de cactus

1.1 Groupe défini par générateurs et relations

Lorsque $n \in \mathbb{N}^*$, les groupes symétriques $(\mathfrak{S}_n, \circ)$, les groupes diédraux $(D_n, \times)$ et les groupes cycliques $(\mathbb{Z}/n\mathbb{Z}, +)$ sont définis par des lois de compositions déjà existantes et bien définies (la composition des applications, le produit matriciel et l'addition de classes d'équivalence dans le groupe quotient). Nous allons voir qu'il est possible de présenter les groupes *par générateurs et relations*.

On trouve la construction des groupes définis par générateurs et relations qui suit dans [**1**].

DÉFINITION Soit $n \in \mathbb{N}^*$. Soit $\mathcal{A}$ un ensemble fini à n éléments. On note $a_1, \cdots, a_n$ les éléments de $\mathcal{A}$.
Soit $\mathcal{A}^{-1}$ un ensemble en bijection avec $\mathcal{A}$ et disjoint de $\mathcal{A}$. On écrit $\mathcal{A}^{-1} = \{a_1^{-1}, \cdots, a_n^{-1}\}$.
Un **mot** sur $\mathcal{A}$ est un k-uplet d'éléments de $\mathcal{A} \cup \mathcal{A}^{-1}$ où $k \in \mathbb{N}$. Le **mot vide** est par convention le seul mot à 0 élément, et on le note 1. On pose alors $\mathcal{M}(\mathcal{A})$ l'ensemble des mots sur $\mathcal{A}$.

Si un mot sur un ensemble fini est un k-uplet, on dit aussi qu'il est de **longueur** k.

NOTATION Si $\mathcal{A} = \{a_1, \cdots, a_n\}$ est un ensemble fini, alors un élément $m \in \mathcal{M}(\mathcal{A})$ s'écrit

$$m = (a_{i_1}^{\varepsilon_1}, \cdots, a_{i_k}^{\varepsilon_k})$$

où $k \in \mathbb{N}^*$ avec $i_1, \cdots, i_k \in \{1, \cdots, n\}$ et $\forall j \in \{1, \cdots, k\}, \varepsilon_j = \pm 1$. Dans la suite, un tel mot m sera noté

$$m = a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k}.$$

EXEMPLE : Sur l'ensemble $\mathcal{A} = \{a_1, a_2, a_3\}$, le mot $m = (a_2, a_3^{-1}, 1, a_1^{-1}, a_2)$ sera noté $m = a_2 a_3^{-1} 1 a_1^{-1} a_2$.

DÉFINITION Soit $n \in \mathbb{N}^*$. Soit $\mathcal{A}$ un ensemble fini à n éléments. On note $a_1, \cdots, a_n$ les éléments de $\mathcal{A}$.
On définit une loi $\cdot$ sur $\mathcal{M}(\mathcal{A})$ par $\forall m \in \mathcal{M}(\mathcal{A})$,

$$1 \cdot m = m \cdot 1 = m$$

et si $u = a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k}$ et $v = a_{j_1}^{\delta_1} \cdots a_{j_p}^{\delta_p}$ sont deux mots non vides sur $\mathcal{A}$,

$$u \cdot v = a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k} a_{j_1}^{\delta_1} \cdots a_{j_p}^{\delta_p}$$

où $k, p \in \mathbb{N}^*$ avec $i_1, \cdots, i_k, j_1, \cdots, j_p \in \{1, \cdots, n\}$, $\forall k' \in \{1, \cdots, k\}, \varepsilon_{k'} = \pm 1$ et $\forall p' \in \{1, \cdots, p\}, \delta_{p'} = \pm 1$.

EXEMPLE : Sur l'ensemble $\mathcal{A} = \{a_1, a_2, a_3\}$, on a $(a_2 a_2^{-1} a_3 a_1).(a_2 a_1^{-1} 1 a_3^{-1}) = a_2 a_2^{-1} a_3 a_1 a_2 a_1^{-1} a_3^{-1}$.

REMARQUE : La longueur de $u \cdot v$ est donc égale à la somme de la longueur de u et de la longueur de v.

PROPOSITION Soit $n \in \mathbb{N}^*$. Soit $\mathcal{A}$ un ensemble fini à n éléments. Alors, $(\mathcal{M}(\mathcal{A}), \cdot)$ est un monoïde.

PREUVE : Tout d'abord, par définition de $\cdot$, $(\mathcal{M}(\mathcal{A}), \cdot)$ est un magma. De plus, on vérifie que la loi $\cdot$ est associative et que 1 est neutre pour $\cdot$ dans $\mathcal{M}(\mathcal{A})$. Ainsi, $(\mathcal{M}(\mathcal{A}), \cdot)$ est un monoïde.

REMARQUE : Le seul élément de $\mathcal{M}(\mathcal{A})$ qui est inversible pour la loi $\cdot$ est 1.

DÉFINITION Soit $n \in \mathbb{N}^*$. Soit $\mathcal{A}$ un ensemble fini à n éléments. Soient $u, v \in \mathcal{M}(\mathcal{A})$.
On dit que u et v sont **adjacents** et on note $u\mathbf{A}v$ lorsque $\exists t_1, t_2 \in \mathcal{M}(\mathcal{A}), \exists a \in \mathcal{A} \cup \mathcal{A}^{-1}$ tels que

$$(u = t_1 \cdot t_2 \text{ et } v = t_1 \cdot a \cdot a^{-1} \cdot t_2) \quad \text{ou} \quad (u = t_1 \cdot a \cdot a^{-1} \cdot t_2 \text{ et } v = t_1 \cdot t_2)$$

avec la convention $(a^{-1})^{-1} = a$ pour $a \in \mathcal{A}$.

On va maintenant définir une relation d'équivalence sur l'ensemble des mots sur un ensemble fini.

Définition Soit $n \in \mathbb{N}^*$. Soit $\mathcal{A}$ un ensemble fini à n éléments. Soient $u, v \in \mathcal{M}(\mathcal{A})$.
On définit la relation binaire $\mathbf{R}$ par $u\mathbf{R}v$ si et seulement si $\exists k \in \mathbb{N}^*, \exists t_1, \cdots, t_k \in \mathcal{M}(\mathcal{A})$ tels que

$$u = t_1, \quad v = t_k \quad \text{et} \quad \forall i \in \{1, \cdots, k-1\}, t_i \mathbf{A} t_{i+1} \text{ (si } k > 1).$$

Proposition Soit $\mathcal{A}$ un ensemble fini. La relation $\mathbf{R}$ est une relation d'équivalence sur $\mathcal{M}(\mathcal{A})$.

Preuve : La relation $\mathbf{R}$ est réflexive car $\forall u \in \mathcal{M}(\mathcal{A})$, on a $u\mathbf{R}u$ (c'est le cas où $k = 1$ dans la définition de $\mathbf{R}$).
La relation $\mathbf{A}$ est symétrique par définition, donc $\mathbf{R}$ est symétrique aussi (vu la condition de la définition de $\mathbf{R}$).
Enfin, si $u, v, w \in \mathcal{M}(\mathcal{A})$ vérifient $u\mathbf{R}v$ et $v\mathbf{R}w$, alors $\exists k \in \mathbb{N}^*, \exists t_1, \cdots, t_k \in \mathcal{M}(\mathcal{A})$ tels que

$$u = t_1, \quad v = t_k \quad \text{et} \quad \forall i \in \{1, \cdots, k-1\}, t_i \mathbf{A} t_{i+1} \text{ (si } k > 1)$$

et on a également $\exists m \in \mathbb{N}^*, \exists t_k, \cdots, t_{k+m} \in \mathcal{M}(\mathcal{A})$ tels que

$$v = t_k, \quad w = t_{k+m} \quad \text{et} \quad \forall j \in \{0, \cdots, m-1\}, t_{k+j} \mathbf{A} t_{k+j+1} \text{ (si } m > 1).$$

Ainsi, en prenant $k + m \in \mathbb{N}^*$ et $t_1, \cdots, t_k, \cdots, t_{k+m} \in \mathcal{M}(\mathcal{A})$ on obtient que $u\mathbf{R}w$ et donc que $\mathbf{R}$ est transitive.
Finalement, la relation $\mathbf{R}$ est bien une relation d'équivalence.

L'introduction de la relation d'équivalence $\mathbf{R}$ permet de construire l'ensemble des classes d'équivalence que l'on notera $F(\mathcal{A}) = \mathcal{M}(\mathcal{A})/\mathbf{R}$. Nous allons voir que cette relation est compatible avec la loi $\cdot$ et que $F(\mathcal{A})$ est un groupe.

Proposition Soit $\mathcal{A}$ un ensemble fini. La relation $\mathbf{R}$ est compatible avec la loi $\cdot$ définie précédemment.
Ainsi, on peut définir la loi

$$\begin{array}{rccc} \bullet & : & F(\mathcal{A}) \times F(\mathcal{A}) & \longrightarrow & F(\mathcal{A}) \\ & & (\overline{u}, \overline{v}) & \longmapsto & \overline{u \cdot v} \end{array}$$

avec la notation $F(\mathcal{A}) = \mathcal{M}(\mathcal{A})/\mathbf{R}$. Muni de cette loi, $F(\mathcal{A})$ est un groupe.

Preuve : Soient $u, u', v, v' \in \mathcal{M}(\mathcal{A})$ tels que $u\mathbf{R}v$ et $u'\mathcal{R}v'$. Montrons que $(u \cdot u')\mathbf{R}(v \cdot v')$.
Par définition, $\exists k \in \mathbb{N}^*, \exists t_1, \cdots, t_k \in \mathcal{M}(\mathcal{A})$ tels que

$$u = t_1, \quad v = t_k \quad \text{et} \quad \forall i \in \{1, \cdots, k-1\}, t_i \mathbf{A} t_{i+1} \text{ (si } k > 1),$$

et $\exists k' \in \mathbb{N}^*, \exists t'_1, \cdots, t'_{k'} \in \mathcal{M}(\mathcal{A})$ tels que

$$u' = t'_1, \quad v' = t'_{k'} \quad \text{et} \quad \forall i \in \{1, \cdots, k'-1\}, t'_i \mathbf{A} t'_{i+1} \text{ (si } k' > 1).$$

Par définition de la loi $\cdot$, $u \cdot u' = t_1 t'_1$ et $v \cdot v' = t_k t'_{k'}$. Montrons que

$$(t_1 t'_1)\mathbf{R}(t_k t'_1).$$

Comme $t_1 \mathbf{A} t_2$, $\exists a_1 \in \mathcal{A} \cup \mathcal{A}^{-1}, \exists T_1, T_2 \in \mathcal{M}(\mathcal{A})$ tels que

$$(t_1 = T_1 \cdot T_2 \text{ et } t_2 = T_1 \cdot a_1 \cdot a_1^{-1} \cdot T_2) \quad \text{ou} \quad (t_1 = T_1 \cdot a_1 \cdot a_1^{-1} \cdot T_2 \text{ et } t_2 = T_1 \cdot T_2)$$

et donc

$$(t_1 t'_1 = T_1 \cdot (T_2 \cdot t'_1) \text{ et } t_2 t'_1 = T_1 \cdot a_1 \cdot a_1^{-1} \cdot (T_2 \cdot t'_1)) \quad \text{ou} \quad (t_1 t'_1 = T_1 \cdot a_1 \cdot a_1^{-1} \cdot (T_2 \cdot t'_1) \text{ et } t_2 t'_1 = T_1 \cdot (T_2 \cdot t'_1)).$$

Cela prouve que $(t_1 t'_1)\mathbf{A}(t_2 t'_1)$ et donc en particulier, $(t_1 t'_1)\mathbf{R}(t_2 t'_1)$. On montre de la même manière que $(t_2 t'_1)\mathbf{R}(t_3 t'_1)$ et par récurrence (dans laquelle on utilise la transitivité de $\mathbf{R}$) on montre que $(t_1 t'_1)\mathbf{R}(t_k t'_1)$ comme annoncé.
De la même manière, on montre que $(t_k t'_1)\mathbf{R}(t_k t'_{k'})$. Ainsi, on a montré que

$$(u \cdot u')\mathbf{R}(t_k t'_1) \text{ et que } (t_k t'_1)\mathbf{R}(v \cdot v')$$

étant donné que $u \cdot u' = t_1 t'_1$ et que $v \cdot v' = t_k t'_{k'}$. Par transitivité, on a bien $(u \cdot u')\mathbf{R}(v \cdot v')$.
La loi $\bullet$ est donc bien définie. Montrons que $(F(\mathcal{A}), \bullet)$ est un groupe.
L'élément neutre du magma $(F(\mathcal{A}), \bullet)$ est la classe de 1 pour la relation $\mathbf{R}$, notée $\overline{1}$. En effet,

$$\forall u \in \mathcal{M}(\mathcal{A}), \overline{u} \bullet \overline{1} = \overline{u \cdot 1} = \overline{u} \quad \text{et} \quad \overline{1} \bullet \overline{u} = \overline{1 \cdot u} = \overline{u}.$$

Par associativité de la loi $\cdot$, la loi $\bullet$ est également associative. Effectivement $\forall u, v, w \in \mathcal{M}(\mathcal{A})$,

$$\overline{u} \bullet (\overline{v} \bullet \overline{w}) = \overline{u} \bullet \overline{v \cdot w} = \overline{u \cdot (v \cdot w)} = \overline{(u \cdot v) \cdot w} = \overline{u \cdot v} \bullet \overline{w} = (\overline{u} \bullet \overline{v}) \bullet \overline{w}.$$

Enfin, montrons que tout élément de $F(\mathcal{A})$ est inversible pour $\bullet$ en utilisant la définition des éléments de $\mathcal{M}(\mathcal{A})$. Soit $m \in \mathcal{M}(\mathcal{A})$. Par définition, si $\mathcal{A}$ est de cardinal $n \in \mathbb{N}^*$ et si on note $a_1, \cdots, a_n$ les éléments de $\mathcal{A}$, $\exists k \in \mathbb{N}^*$, $\exists i_1, \cdots, i_k \in \{1, \cdots, n\}$ et $\forall j \in \{1, \cdots, k\}, \exists \varepsilon_j \in \{1, -1\}$ tels que

$$m = a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k} \text{ d'où } \overline{m} = \overline{a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k}}.$$

Soit $m' = a_{i_k}^{-\varepsilon_k} \cdots a_{i_1}^{-\varepsilon_1}$. D'une part, par définition de la relation $\mathbf{R}$,

$$\overline{m} \bullet \overline{m'} = \overline{a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k}} \bullet \overline{a_{i_k}^{-\varepsilon_k} \cdots a_{i_1}^{-\varepsilon_1}} = \overline{a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k} a_{i_k}^{-\varepsilon_k} \cdots a_{i_1}^{-\varepsilon_1}} = \overline{1}$$

car deux éléments sont dans la même classe si ils peuvent se simplifier de cette manière, et d'autre part,

$$\overline{m'} \bullet \overline{m} = \overline{a_{i_k}^{-\varepsilon_k} \cdots a_{i_1}^{-\varepsilon_1}} \bullet \overline{a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k}} = \overline{a_{i_k}^{-\varepsilon_k} \cdots a_{i_1}^{-\varepsilon_1} a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k}} = \overline{1}.$$

Cela prouve que $\overline{m}$ est inversible pour la loi $\bullet$ et donc que $(F(\mathcal{A}), \bullet)$ est un groupe.

Définition Soit $\mathcal{A}$ un ensemble fini. Le groupe $(F(\mathcal{A}), \bullet)$ est appelé **groupe libre** sur l'ensemble $\mathcal{A}$.

Notation De la même façon que dans les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$, $n \in \mathbb{N}^*$, on omettra la barre au dessus des éléments de $F(\mathcal{A})$ où $\mathcal{A}$ est un ensemble fini. De plus, et comme souvent dans un groupe abstrait, on n'écrira pas la loi $\bullet$ pour composer deux éléments de $F(\mathcal{A})$.

Moralement, $F(\mathcal{A})$ est l'ensemble des *classes de mots* sur l'*alphabet* $\mathcal{A}$ et l'opération $\bullet$ correspond à la concaténation des mots. Ces mots peuvent être simplifiés selon les règles définies par l'opération du groupe.

Définition Soit $\mathcal{A}$ un ensemble fini. Soit G un groupe.
On dit que G est **libre sur** $\mathcal{A}$ lorsqu'il est engendré par $\mathcal{A}$ et qu'il est isomorphe à $F(\mathcal{A})$.

Étant donné un mot, il est possible qu'il contienne des simplifications (une lettre suivie de son inverse). Un mot qui ne contient aucune simplification est dit *réduit*.

Définition Soit $\mathcal{A}$ un ensemble fini. Soit $m \in \mathcal{M}(\mathcal{A})$.
On dit que m est **réduit** lorsque l'une des deux propriétés suivantes est vérifiée :

1. $m = 1$.
2. $\exists n \in \mathbb{N}^*, \exists a_1, \cdots a_n \in \mathcal{A}, \exists \varepsilon_1, \cdots, \varepsilon_n \in \{-1, 1\}, m = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ avec $\forall i \in \{1, \cdots, n-1\}, a_{i+1}^{\varepsilon_{i+1}} \neq a_i^{-\varepsilon_i}$.

On note $F_{\mathcal{A}}$ l'ensemble des mots réduits sur $\mathcal{A}$.

Exemple : Tout mot de longueur 1 est réduit.

Théorème Soit $\mathcal{A}$ un ensemble fini.
Chaque classe d'équivalence de $\mathcal{M}(\mathcal{A})$ modulo $\mathbf{R}$ contient un unique mot réduit.

Preuve : Remarquons tout d'abord que si un mot $m \in \mathcal{M}(\mathcal{A})$ est non réduit, alors il est réductible au sens suivant :

$$\text{il existe } m' \in \mathcal{M}(\mathcal{A}) \text{ tel que } m \mathbf{A} m' \text{ et la longueur de } m' \text{ est strictement inférieure à celle de } m.$$

Tant que le mot adjacent ainsi défini n'est pas réduit, on peut répéter l'opération étant donné qu'à une telle suite de mots adjacents on associe une suite d'entiers strictement décroissante (la longueur des mots). Cela prouve qu'il existe un mot réduit dans toute classe d'équivalence de $\mathcal{M}(\mathcal{A})$ modulo $\mathbf{R}$. Il s'agit maintenant de prouver qu'il n'y en a qu'un seul. Pour cela, on se donne un mot $m = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ avec $a_1, \cdots, a_n \in \mathcal{A}$ et $\varepsilon_1, \cdots, \varepsilon_n \in \{-1, 1\}$, et on définit on définit $m_0, m_1, \cdots, m_n$ de la façon suivante :

$$m_0 = 1, m_1 = a_1^{\varepsilon_1} \text{ puis } m_2 = 1 \text{ si } a_1^{\varepsilon_1} = a_2^{-\varepsilon_2} \text{ et } m_2 = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \text{ sinon.}$$

Ensuite, si on dispose de m_i avec $i \in \{1, \cdots, n-1\}$, on définit m_{i+1} par $m_{i+1} = m_i a_{i+1}^{\varepsilon_{i+1}}$ si la dernière lettre de m_i (comptée avec la puissance) est différente de $a_{i+1}^{-\varepsilon_{i+1}}$ et on fait la simplification sinon. Cette définition de proche en proche assure que $\forall i \in \{0, \cdots, n\}$, le mot m_i est réduit et équivalent (au sens de la relation $\mathbf{R}$) à $a_1^{\varepsilon_1} \cdots a_i^{\varepsilon_i}$.
En particulier, m_n est réduit et équivalent à m. Cette construction de m_n montre que si m est réduit, alors $m = m_n$.
Dans la suite, m_n est appelé *forme réduite* de m et on note $r(m) = m_n$.
On montre sans difficulté que deux mots adjacents ont la même forme réduite. En effet, si deux mots sont adjacents, c'est que l'un des deux contient une simplification qui permet de retomber sur l'autre.
Plus formellement, si

$$u = a_1^{\varepsilon_1} \cdots a_k^{\varepsilon_k} a_{k+1}^{\varepsilon_{k+1}} \cdots a_n^{\varepsilon_n} \quad \text{et} \quad v = a_1^{\varepsilon_1} \cdots a_k^{\varepsilon_k} x x^{-1} a_{k+1}^{\varepsilon_{k+1}} \cdots a_n^{\varepsilon_n}$$

où $a_1, \cdots, a_n \in \mathcal{A}$, x ou x^{-1} appartient à $\mathcal{A}$ avec la convention $(x^{-1})^{-1} = x$ et $\varepsilon_1, \cdots, \varepsilon_n \in \{-1, 1\}$, on va montrer que $u_k = v_{k+2}$. Deux cas se présentent. Si la dernière lettre de u_k (comptée avec la puissance) est différente de x^{-1},

$$v_k = u_k, \quad v_{k+1} = v_k x \quad \text{et} \quad v_{k+2} = v_k = u_k$$

Sinon, la dernière lettre comptée avec puissance de u_k vaut x^{-1} et u_k se réécrit $u_k = t x^{-1}$. Comme u_k est réduit, on est désormais assurés que la dernière lettre de t est différente de x. Ainsi,

$$v_k = u_k, \quad v_{k+1} = t \quad \text{et} \quad v_{k+2} = v_k = u_k$$

À l'issue des deux cas précédents, on obtient $u_k = v_{k+2}$ et vu la forme de u et v, on obtient $u_n = v_{n+2}$ soit $r(u) = r(v)$.
Il ne reste plus qu'à prouver que deux mots réduits équivalents sont égaux. Par définition de l'équivalence des mots, on peut atteindre un mot à partir de l'autre par un nombre fini d'adjacences. Mais on vient de prouver que deux mots adjacents ont la même forme réduite. Les deux mots choisis étant déjà réduits, ils sont bien égaux. D'où l'unicité.

Corollaire Soit $\mathcal{A}$ un ensemble fini. On dispose d'une bijection

$$\begin{array}{rccc} \varphi & : & F(\mathcal{A}) & \longrightarrow & F_{\mathcal{A}} \\ & & \overline{m} & \longmapsto & r(m) \end{array}$$

Cela permet de définir une loi de composition interne

$$\begin{array}{rccc} \star & : & F_{\mathcal{A}} \times F_{\mathcal{A}} & \longrightarrow & F_{\mathcal{A}} \\ & & (u, v) & \longmapsto & r(u \cdot v) \end{array}$$

telle que $(F_{\mathcal{A}}, \star)$ est un groupe, engendré par $\mathcal{A}$ et isomorphe à $F(\mathcal{A})$. Ainsi, $F_{\mathcal{A}}$ est un groupe libre sur $\mathcal{A}$.

Définition On dit qu'un groupe G est **libre de type fini** si il admet une famille génératrice libre finie c'est-à-dire lorsqu'il existe un ensemble fini $\mathcal{A}$ tel que G est isomorphe à $F_{\mathcal{A}}$.

Remarque : De la même manière, on peut définir les groupes libres en remplaçant les ensembles finis par des ensembles quelconques et en prenant les mots finis sur cet ensemble.

L'intérêt des groupes libres de type fini réside dans la propriété universelle suivante.

Théorème Soient G un groupe non trivial et X une partie génératrice finie de G.
On note α l'injection canonique de X dans G. Alors, G est libre sur X si et seulement si pour tout groupe H et pour toute application $\sigma : X \to H$, il existe un unique morphisme $\varphi : G \to H$ tel que $\varphi \circ \alpha = \sigma$.
Cela revient à demander que le diagramme suivant commute.

$$\begin{array}{ccc} X & \xhookrightarrow{\alpha} & G \\ {\scriptstyle\sigma}\downarrow & \swarrow_{\exists! \varphi} & \\ H & & \end{array}$$

Preuve : On montre les deux implications successivement.
Quitte à supposer que G est libre sur X, on peut supposer $G = F_X$. Supposons donc que $G = F_X$.
Soient H un groupe et $\sigma : X \to H$ une application. On va définir un morphisme de F_X dans H en utilisant le fait que tout élément $m \neq 1$ de F_X s'écrit d'une unique manière sous la forme réduite

$$m = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$$

avec $x_1, \cdots, x_n \in X$ et $\varepsilon_1, \cdots, \varepsilon_n \in \{-1, 1\}$. Pour un tel mot m de F_X, on pose

$$\varphi(m) = (\sigma(x_1))^{\varepsilon_1} \cdots (\sigma(x_n))^{\varepsilon_n} \quad \text{et} \quad \varphi(1) = e_G.$$

On vérifie sans peine que φ est un morphisme de groupes et que $\forall x \in X, \varphi(x) = \sigma(x)$ donc que $\varphi \circ \alpha = \sigma$.
Réciproquement, supposons que pour tout groupe H et toute application $\sigma : X \to H$, il existe un unique morphisme de groupes $\varphi : G \to H$ tel que $\varphi \circ \alpha = \sigma$.
D'une part, en prenant $H = F_X$ et $\sigma = \alpha_X$ l'injection canonique, on obtient que le diagramme suivant commute :

$$\begin{array}{ccc} X & \xhookrightarrow{\alpha} & G \\ {\scriptstyle \alpha_X}\downarrow & \swarrow_{\exists ! \varphi} & \\ F_X & & \end{array}$$

D'autre part, part le sens direct qui précède, comme F_X est libre sur X, le diagramme qui suit commute également :

$$\begin{array}{ccc} X & \xhookrightarrow{\alpha_X} & F_X \\ {\scriptstyle \alpha}\downarrow & \swarrow_{\exists ! \psi} & \\ G & & \end{array}$$

On dispose ainsi de $\varphi : G \to F_X$ et de $\psi : F_X \to G$ qui vérifient les deux égalités suivantes :

$$\varphi \circ \alpha = \alpha_X \quad \text{et} \quad \psi \circ \alpha_X = \alpha.$$

En remplaçant α par $\psi \circ \alpha_X$ dans la première égalité et α_X par $\varphi \circ \alpha$ dans la deuxième, on obtient

$$\varphi \circ \psi \circ \alpha_X = \alpha_X \quad \text{et} \quad \psi \circ \varphi \circ \alpha = \alpha.$$

Ainsi, $\varphi \circ \psi|_X = id_X$ et $\psi \circ \varphi|_X = id_X$. Mais φ et ψ sont des morphismes de groupes et G et F_X sont engendrés par X donc G est isomorphe à F_X. Ainsi, G est libre sur X.

Corollaire Si X et Y sont deux ensembles finis non vides en bijection, alors F_X est isomorphe à F_Y.

Preuve : Notons $\beta : X \to Y$ une bijection.
Par le théorème précédent il existe un morphisme de groupes φ tel que le diagramme suivant commute :

$$\begin{array}{ccc} X & \xhookrightarrow{\alpha_X} & F_X \\ {\scriptstyle \beta}\downarrow & & \downarrow{\scriptstyle \varphi} \\ Y & \xhookrightarrow{\alpha_Y} & F_Y \end{array}$$

De même, il existe un morphisme de groupes ψ tel que le diagramme suivant commute :

$$\begin{array}{ccc} Y & \xhookrightarrow{\alpha_Y} & F_Y \\ {\scriptstyle \beta^{-1}}\downarrow & & \downarrow{\scriptstyle \psi} \\ X & \xhookrightarrow{\alpha_X} & F_X \end{array}$$

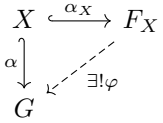
Comme ces diagrammes commutent, on a $\varphi \circ \alpha_X = \alpha_Y \circ \beta$ et $\psi \circ \alpha_Y = \alpha_X \circ \beta^{-1}$. Donc,

$$\psi \circ \varphi \circ \alpha_X = \psi \circ \alpha_Y \circ \beta = \alpha_X \quad \text{et} \quad \varphi \circ \psi \circ \alpha_Y = \varphi \circ \alpha_X \circ \beta^{-1} = \alpha_Y.$$

Ceci montre que $\psi \circ \varphi|_X = id_X$ et que $\varphi \circ \psi|_X = id_X$. Mais comme X engendre F_X et que Y engendre F_Y, on a bien l'isomorphisme annoncé.

Théorème Tout groupe de type fini est image homomorphe d'un groupe libre de type fini.

Preuve : Soit G un groupe de type fini. Soit X une partie génératrice finie de G.
Si G est trivial, alors G est libre sur l'ensemble vide (convention). Sinon, on note α l'injection canonique de X dans G et α_X l'injection canonique de X dans F_X. Par la propriété universelle, le diagramme suivant commute :



Ainsi, $\varphi \circ \alpha_X = \alpha$ et donc φ est surjectif (car X engendre G). Donc, $G = \varphi(F_X)$ et G est image homomorphe de F_X.

NOTATION Soient G un groupe et $A \subset G$. L'intersection des sous-groupes distingués de G contenant A est encore un sous-groupe distingué de G contenant A. C'est le plus petit par construction, et on le note $\langle\langle A \rangle\rangle$.

DÉFINITION Soit G un groupe de type fini. Soit X une partie génératrice finie de G.
On suppose que les éléments de X vérifient un ensemble de relations $\{r_\lambda = e_G, \lambda \in \Lambda\}$.
Notons $R = \{r_\lambda, \lambda \in \Lambda\}$, de sorte que $\langle\langle R \rangle\rangle$ soit un sous-groupe distingué de F_X.
On dit que $(X \mid R)$ est une **présentation** de G lorsque G est isomorphe à $F_X/\langle\langle R \rangle\rangle$.
Le groupe $F_X/\langle\langle R \rangle\rangle$ est alors *défini par générateurs et relations.*

EXEMPLES : On trouve facilement des exemples parmi les groupes bien connus.

1. Soit $n \in \mathbb{N}^*$. Une présentation du groupe cyclique d'ordre n engendré par x est $(\{x\} \mid \{x^n\})$.
2. Soit $n \in \mathbb{N}^* \setminus \{1\}$. Une présentation du groupe diédral D_n est $(\{s, r\} \mid \{s^2, r^n, rsrs\})$ avec $s \neq r$.
3. Une présentation du groupe des quaternions Q_8 est $(\{i, j\} \mid \{i^4, i^2j^{-2}, ijij^{-1}\})$.
4. Une présentation du groupe additif $\mathbb{Z}$ est $(\{1\} \mid \emptyset)$.

Bien entendu, une présentation d'un groupe n'est pas nécessairement unique.

REMARQUE : Tout groupe G de type fini admet une présentation. Effectivement, par le théorème précédent, G est image homomorphe d'un groupe libre de type fini donc par le premier théorème d'isomorphisme, G est isomorphe au quotient d'un groupe libre. Ainsi, G admet bien une présentation.

REMARQUE : Selon les cas, un groupe défini par générateurs et relations peut être fini ou infini. Moralement, moins il y a de relations, plus il y aura d'éléments dans le groupe. Quand il n'y a pas de relations, on obtient un groupe libre.

1.2 Groupes de cactus et représentation des éléments

Les groupes de cactus J_n sont définis par générateurs et relations pour tout entier $n \in \mathbb{N}^* \setminus \{1\}$.

DÉFINITION Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. On définit le **groupe de cactus** J_n par les générateurs

$$s_{p,q} \text{ pour tout } (p, q) \in \mathbb{N}^2 \text{ tel que } 1 \leqslant p < q \leqslant n$$

qui vérifient les trois relations suivantes : $\forall (p, q, m, r) \in \mathbb{N}^4$ tel que $1 \leqslant p < q \leqslant n$ et $1 \leqslant m < r \leqslant n$,

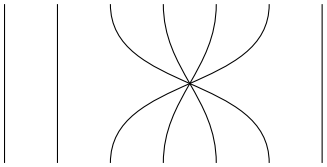
1. $s_{p,q}^2 = 1$.
2. si $[p, q] \cap [m, r] = \emptyset$, alors $s_{p,q}s_{m,r} = s_{m,r}s_{p,q}$.
3. si $[m, r] \subset [p, q]$, alors $s_{p,q}s_{m,r} = s_{p+q-r,p+q-m}s_{p,q}$.

EXEMPLE : Le groupe J_2 est engendré par $s_{1,2}$ qui vérifie $s_{1,2}^2 = 1$ donc $J_2 = \{1, s_{1,2}\}$. Ainsi, le groupe de cactus J_2 est fini d'ordre 2, donc isomorphe au groupe cyclique d'ordre 2.

REMARQUE : Parmi les groupes de cactus, J_2 est le seul groupe fini. En effet, si $n \in \mathbb{N}$ est tel que $n \geqslant 3$, le groupe J_n contient au moins $s_{1,2}$ et $s_{2,3}$ donc $s_{1,2}s_{2,3} \in J_n$ puis on obtient un élément distinct des précédents en considérant $s_{1,2}s_{2,3}s_{1,2}$, puis $s_{1,2}s_{2,3}s_{1,2}s_{2,3}$ et ainsi de suite.

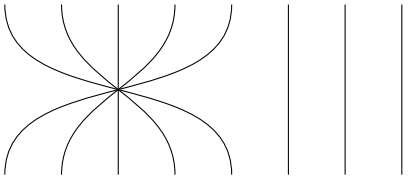
Pour comprendre les relations imposées aux générateurs des groupes de cactus, on introduit la représentation qui suit.

NOTATION Si $n \in \mathbb{N}$ est tel que $n \geqslant 2$, on visualise les générateurs de J_n par des **brins**.
Plus précisément, si $1 \leqslant p < q \leqslant n$, le générateur $s_{p,q}$ est constitué de n lignes verticales parallèles, sauf pour les lignes situées entre p et q (compris) qui sont courbées. Ainsi, pour $i \in \{0, q-p\}$, le "point du haut" $p+i$ est envoyé sur le "point du bas" $q-i$.
Par exemple, dans J_7, le générateur $s_{3,6}$ peut se représenter de la manière suivante.



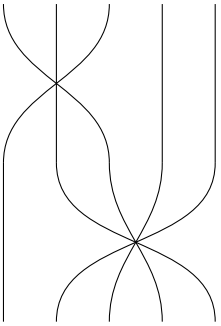
Le générateur $s_{3,6} \in J_7$.

Dans J_8, le générateur $s_{1,5}$ se visualise comme suit.



Le générateur $s_{1,5} \in J_8$.

Pour représenter un élément quelconque de J_n qui s'écrit comme un produit fini de générateurs, on met les brins ainsi construits les uns au dessus des autres.
Ainsi, dans J_5, le produit $s_{1,3}s_{2,5}$ se représente comme ci-dessous.

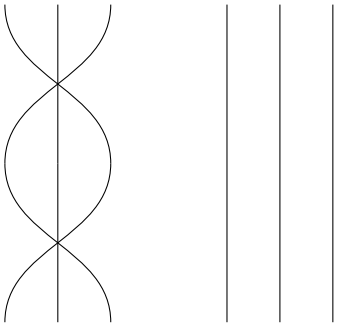


L'élément $s_{1,3}s_{2,5} \in J_5$.

Bien entendu, l'élément neutre est représenté par n lignes verticales parallèles sans aucune courbure.

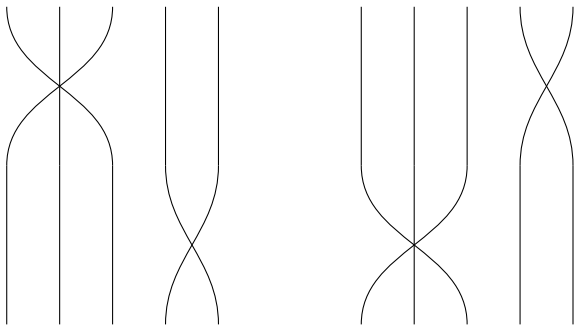
REMARQUE : Cette représentation justifie les relations qui définissent les groupes de cactus.

1. Les générateurs sont d'ordre 2, donc ces deux figures représentent le même élément des groupe de cactus.



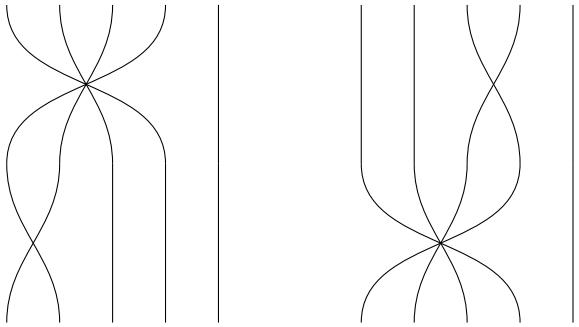
Les générateurs sont d'ordre 2.

2. Le deuxième point qui donne une condition pour que deux générateurs commutent se traduit par l'égalité des deux schémas suivants.



Deux générateurs commutent si ils ne se "croisent" pas.

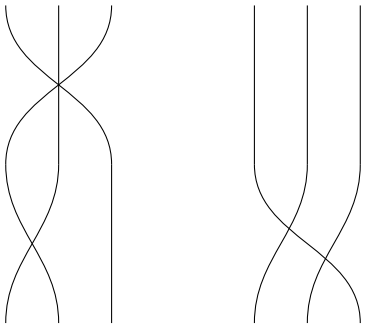
3. Enfin, la troisième relation qui nous donne une "fausse" commutativité se traduit par le passage d'un brin plus petit dans un brin plus grand. Par exemple, les deux diagrammes ci-dessous sont égaux.



La relation de "fausse" commutativité.

Ces trois relations qui semblaient arbitraires font sens à la lumière de la représentation en brins.

Remarque : Les relations imposées aux générateurs ne permettent pas de *simplifier* des brins pour obtenir l'égalité des deux schémas suivants par exemple.



On ne peut pas "démêler" les brins.

On insiste donc sur le fait qu'un produit de deux éléments d'un groupe de cactus ne peut pas se simplifier en général.

Le groupe J_3 fera l'objet d'une étude plus approfondie dans la partie sur les graphes de Cayley.

1.3 Groupes de cactus purs

La représentation des éléments des groupes de cactus nous fournit immédiatement un morphisme de J_n dans $\mathfrak{S}_n$ pour tout $n \in \mathbb{N}$ tel que $n \geqslant 2$. Précisément, à chaque générateur $s_{p,q}$ du groupe J_n, on envoie la permutation de $\mathfrak{S}_n$ qui laisse fixe les éléments en dehors de $\{p, p+1, \cdots, q-1, q\}$ et qui envoie $p+i$ sur $q-i$ pour tout $i \in \{0, \cdots, q-p\}$. Plus généralement, l'image d'un élément de J_n est la permutation obtenue en suivant les lignes verticales préalablement numérotées de 1 à n de la représentation en brins. Le noyau de ce morphisme est un sous-groupe de J_n (c'est même un sous-groupe distingué), appelé **groupe de cactus pur** et noté PJ_n.

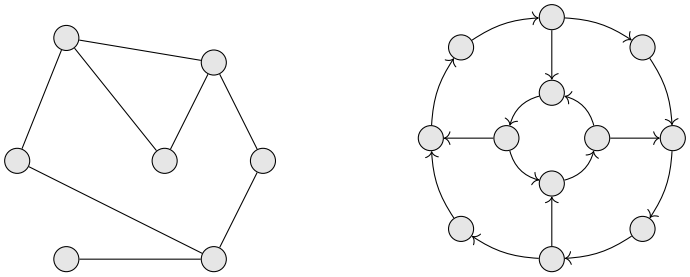
2 Graphes de Cayley et graphes médians

2.1 Graphe de Cayley d'un groupe de type fini

Cette partie est basée sur le livre en cours de rédaction d'Anthony Genevois (voir [3]) et sur [2].

DÉFINITION Un **graphe** est un couple $X = (V, \sim)$ où V est un ensemble et $\sim$ une relation binaire sur V.
Les éléments de V sont appelés **sommets** du graphe X. Une **arrête** de X est un couple de sommets $(x, y) \in X^2$ tel que $x \sim y$.
Si la relation $\sim$ est symétrique (i.e. $\forall x, y \in X, x \sim y \Rightarrow y \sim x$), le graphe sera dit **non orienté**. Dans ce cas, si $x, y \in X$ sont tels que $x \sim y$, nous dirons que x et y sont adjacents.
Si au contraire la relation $\sim$ n'est pas symétrique, le graphe sera dit **orienté**. On parlera dans ce cas d'arrête orientée.

On représente un graphe en dessinant des points pour les éléments de l'ensemble et en reliant ceux qui forment une arrête (orientée ou non). Donnons deux exemples.



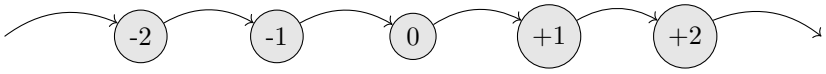
Un graphe non orienté et un graphe orienté.

L'objectif des graphes de Cayley est d'associer à tout groupe de type fini un graphe orienté.

DÉFINITION Soit G un groupe de type fini. Soit S une partie génératrice de G.
Le **graphe de Cayley** de G relatif à la partie S noté $\mathrm{Cayl}(G, S)$ est le graphe orienté dont les sommets sont les éléments de G et dont les arrêtes sont les couples (x, xs) pour tout $x \in G$ et tout $s \in S$.

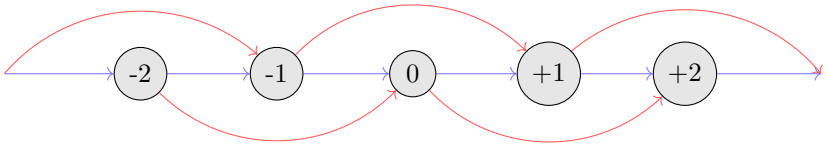
REMARQUE : Dès que la partie génératrice choisie a au moins deux éléments, on conviendra de distinguer les flèches selon le générateur auquel elles sont rattachées. Ainsi, deux flèches ayant la même couleur correspondent à une composition à droite par le même générateur.

EXEMPLES : Donnons la représentation de graphes de Cayley de $(\mathbb{Z}, +)$, de $(\mathbb{Z}^2, +)$, de $(\mathbb{Z}/8\mathbb{Z}, +)$ et de $(Q_8, \times)$.
Voici une partie du graphe de Cayley associé au générateur 1 (le graphe est infini).



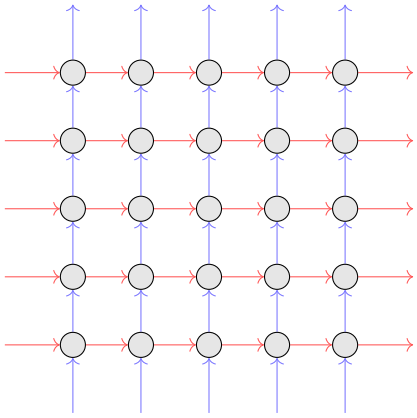
Le graphe $\mathrm{Cayl}(\mathbb{Z}, \{1\})$.

Si on ajoute 2 à la partie génératrice choisie, on obtient le graphe suivant.



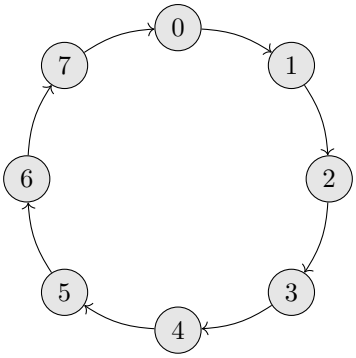
Le graphe $\mathrm{Cayl}(\mathbb{Z}, \{1, 2\})$.

Pour le graphe de Cayley de $\mathbb{Z}^2$, on choisit les deux générateurs $(1, 0)$ et $(0, 1)$ pour obtenir un quadrillage infini.



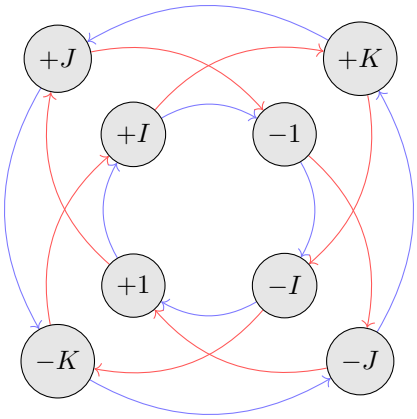
Le graphe $\mathrm{Cayl}(\mathbb{Z}^2, \{(1,0),(0,1)\})$.

Les graphes de Cayley des groupes cycliques forment des cycles.



Le graphe $\mathrm{Cayl}(\mathbb{Z}/8\mathbb{Z}, \{1\})$.

On trouve dans **[2]** un graphe de Cayley du groupe des quaternions Q_8, que l'on peut retrouver facilement à la main.



Le graphe $\mathrm{Cayl}(Q_8, \{I, J\})$.

Les graphes de Cayley permettent ainsi de visualiser les opérations pour se faire une idée de la "forme" du groupe. Il se trouve qu'un groupe de type fini agit de manière naturelle sur l'ensemble des sommets de son graphe de Cayley.

PROPOSITION Soit G un groupe de type fini. Soit S une partie génératrice de G.
Alors, G agit simplement transitivement sur $\mathrm{Cayl}(G, S)$ par l'action qui envoie un élément g de G et un sommet x du graphe de Cayley sur le sommet gx.

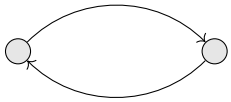
PREUVE : Tout d'abord, l'application qui envoie $g \in G$ et un sommet x sur le sommet gx est bien définie, puisque $gx \in G$ et les sommets de tout graphe de Cayley sont les éléments de G.
Cette application envoie l'élément neutre et un sommet x sur le même sommet x et l'image g et du sommet $g'x$ est le sommet $g(g'x) = (gg')x$ pour tout $g, g' \in G$. Il s'agit donc bien d'une action de groupe.

Cette action est transitive car si x et y sont deux sommets, l'élément yx^{-1} de G envoie x sur $yx^{-1}x = y$. De plus, si deux éléments g et g' de G envoient x sur y, on a $gx = g'x$ donc en multipliant par l'inverse de x à droite, on obtient $g = g'$. L'action est donc simplement transitive.
Sinon, on pouvait juste remarquer que cette action s'identifie à l'action de G sur G par translation à gauche.

Remarque : On peut montrer que si G et H sont deux groupes et que H agit simplement transitivement sur un graphe de Cayley de G, alors G et H sont isomorphes (voir par exemple [**2**]).

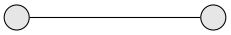
Donnons maintenant le graphe de Cayley des groupes de cactus J_2 et J_3 relatifs aux générateurs qui les définissent.

Proposition Le graphe de Cayley de J_2 relatif à la partie génératrice $\{s_{1,2}\}$ est le suivant.



Preuve : En effet, J_2 est monogène, engendré par un élément d'ordre 2.

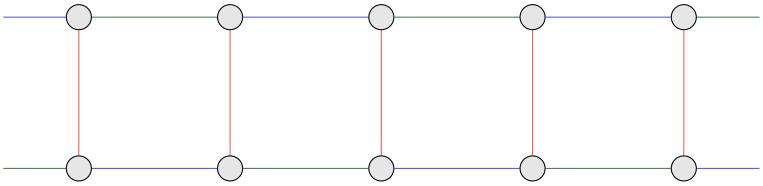
Remarque : Lorsqu'un générateur est d'ordre 2 dans un groupe, on conviendra de tracer un segment entre les deux sommets plutôt que de mettre deux flèches qui pointent l'une sur l'autre. Ainsi, on dessine plutôt le graphe de Cayley de J_2 comme ci-dessous.



Le graphe $\mathrm{Cayl}(J_2, \{s_{1,2}\})$.

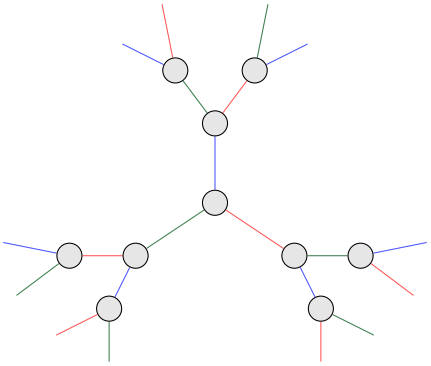
Le cas du groupe J_3 est moins facile étant donné que J_3 est infini.

Proposition Le graphe de Cayley de J_3 relatif à la partie génératrice $\{s_{1,2}, s_{2,3}, s_{1,3}\}$ est le suivant.



Le rouge correspond à $s_{1,3}$, le vert à $s_{2,3}$ et le bleu à $s_{1,2}$. Le graphe se poursuit à l'infini à gauche et à droite.

Preuve : On part du graphe de Cayley du groupe libre à trois générateurs d'ordre 2.

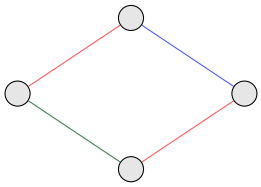


Le graphe de Cayley du groupe libre à trois générateurs d'ordre 2.

Ici, le graphe est tronqué, le groupe libre à trois générateurs d'ordre 2 est bien entendu infini. Dans la suite, on convient d'associer le rouge au générateur $s_{1,3}$, le vert à $s_{2,3}$ et le bleu à $s_{1,2}$. On ajoute alors les relations qui relient les générateurs dans le groupe de cactus J_3. Dans J_3 deux relations sont imposées :

$$s_{1,3}s_{1,2} = s_{2,3}s_{1,3} \text{ et}$$
$$s_{1,3}s_{2,3} = s_{1,2}s_{1,3}.$$

Dans le graphe de Cayley de J_3 les deux relations se traduisent de la façon suivante.



Suivre une arrête rouge puis une arrête bleue revient à suivre une arrête verte puis une arrête rouge.

En propageant cette relation dans le graphe de Cayley du groupe libre à trois générateurs d'ordre 2, le graphe se replie et donne bien le graphe annoncé.

Dans l'article **[0]**, Anthony Genevois prouve que pour tout entier $n \geqslant 2$, le graphe de Cayley du groupe J_n est *médian*. Cela permet une étude plus approfondie de la structure des groupes de cactus.

2.2 Rappels de théorie des graphes

Soit $X = (V, \sim)$ un graphe. Dans toute la suite, nous considérerons toujours que X est non orienté.
Nous préfererons également éviter le cas où un sommet est relié à lui-même. On demandera donc à la relation $\sim$ d'être anti-symétrique (i.e. $\forall x \in X, x \not\sim x$).
Afin de simplifier les notations, nous identifierons le graphe X avec l'ensemble de ses sommets. Ainsi, $x \in X$ signifiera que x est un sommet de X.

Rappelons quelques exemples de graphes élémentaires dont on aura besoin par la suite.
Exemples :

- Le *graphe complet* K_n à n sommets, dont tous les sommets sont deux à deux adjacents.
- Le *graphe complet biparti* $K_{n,m}$ avec n sommets de type 1 et m sommets de type 2, et tel que tout sommet de type 1 est adjacent à tous les sommets de type 2 et tous les sommets du même type ne sont pas adjacents.
- Le *cycle de longueur* n noté C_n dont l'ensemble des sommets est $\mathbb{Z}/n\mathbb{Z}$ et tel que deux sommets sont adjacents si et seulement si ils différent de ± 1 modulo n.

Définition Soit X un graphe. Soient x et y deux sommets de X.
On appelle **chemin** dans X toute suite finie de sommets $\gamma = x_0, \cdots, x_n$ telle que $\forall i \in \{0, \cdots, n-1\}$, x_i et x_{i+1} sont adjacents. La **longueur** du chemin notée $\text{long}(\gamma)$ est l'entier n associé.
Les sommets x_0 et x_n sont les **extrémités** du chemin. On dira aussi que x_0 et x_n sont **reliés** par γ.
Si les extrémités sont identiques on dira que le chemin est un **cycle**.
Un cycle de longueur n est appelé un **n-cycle**.
On dit que X est **connexe** si pour tout sommets $x, y \in X$, x et y sont les extrémités d'un chemin.
La relation "être reliés par un chemin" est une relation d'équivalence sur l'ensemble des sommets de X. Les classes d'équivalence de cette relation sont appelées **composantes connexes** de X.
La **distance** entre $x, y \in X$ est

$$d(x, y) = \min\{\text{long}(\gamma), \gamma \text{ chemin reliant } x \text{ et } y\}.$$

S'il n'existe aucun chemin reliant x et y, nous noterons $d(x, y) = \infty$.
Un chemin reliant x et y de longueur $d(x, y)$ est une **géodésique**.

Définition Soit X un graphe et $\alpha = (x_0, ..., x_r), \beta = (y_0, ..., y_s)$ deux chemins.
Si $x_r = y_0$, la **concaténation** de α et β, notée $\alpha \cup \beta$, est le chemin $(x_0, ..., x_r = y_0, ..., y_n)$.

Nous pouvons désormais démontrer que la distance naturelle sur un graphe définit bien une distance.

Proposition Soit X un graphe connexe. L'application d qui envoie deux sommets x et y du graphe X sur $d(x, y)$ est bien définie et est une distance sur l'ensemble des sommets de X.

Preuve : Comme X est connexe, l'application en question est bien définie (l'ensemble des longueurs des chemins qui relient deux sommets est une partie non vide de $\mathbb{N}$).

Soit $\gamma = (x = x_0, x_1, ..., x_{n-1}, x_n = y)$ une géodésique entre deux sommets $x, y \in X$. Posons $\delta = (y = x_n, x_{n-1}, ..., x_1, x_0 = x)$. De cette façon, δ est une géodésique entre y et x. Ainsi, d est symétrique.
De plus, si x et y sont deux sommets vérifiants $d(x, y) = 0$, alors il existe un chemin de longueur 0 reliant x à y. Donc $x = y$ et d vérifie l'axiome de séparation.
Enfin, soient $x, y, z \in X$, α (resp. β) une géodésique entre x et y (resp. entre y et z). Alors, $\alpha \cup \beta$ est un chemin entre x et z et donc

$$d(x, z) \leqslant \text{long}(\alpha \cup \beta) = \text{long}(\alpha) + \text{long}(\beta) = d(x, y) + d(y, z).$$

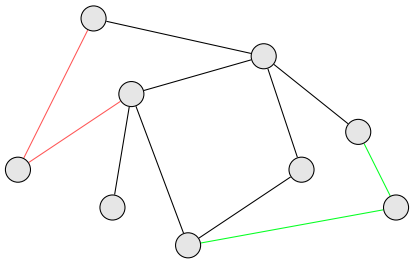
Ainsi l'inégalité triangulaire est bien vérifiée et d définit bien une distance.

Remarque : Par abus de langage, on dira que la distance définie précédemment est **la** distance sur X.

Définition Soit $X = (V, \sim_X)$ un graphe. Soit $Y = (U, \sim_Y)$ un graphe tel que $U \subset V$.
On dit que Y est un **sous-graphe** de X si $\forall x, y \in U,\ x \sim_Y y \Leftrightarrow x \sim_X y$.

Définition Soient X un graphe et Y un sous-graphe de X. On dit que Y est **convexe** lorsque toute géodésique dans X entre deux sommets de Y reste entièrement dans Y (i.e. si $x, y \in Y$ et $\gamma = (x = x_0, ..., x_n = y)$ est une géodésique entre x et y dans X, alors $\forall i \in \{0, ...n\},\ x_i \in Y$).

Exemples : Donnons un exemple de sous-graphe convexe et un exemple de sous-graphe non convexe.



Le sous-graphe vert est convexe et le sous-graphe rouge n'est pas convexe.

En effet, il manque une géodésique dans le sous-graphe rouge.

Définition Soient X et Y deux graphes. Un **isomorphisme** entre X et Y est une application $f : X \to Y$ bijective telle que $\forall x, y \in X,\ f(x) \sim_Y f(y) \Leftrightarrow x \sim_X y$. S'il existe un isomorphisme entre X et Y, on dira que X et Y sont **isomorphes**.

Lemme 1 Soient X et Y deux graphes isomorphes et f un isomorphisme entre X et Y.
Alors $\forall x, y \in X,\ d(x, y) = d(f(x), f(y))$.

Preuve : Soit $\gamma = (x = x_0, x_1, ..., x_{n-1}, x_n = y)$ une géodésique entre $x, y \in X$.
Notons $f(\gamma) = (f(x) = f(x_0), f(x_1), ..., f(x_{n-1}), f(x_n) = f(y))$ (ce chemin est bien défini au vu de la définition d'un isomorphisme). Si $f(\gamma)$ n'est pas une géodésique entre $f(x)$ et $f(y)$, alors il existe un chemin $\delta = (f(x) = y_0, y_1, ..., y_{r-1}, y_r = f(y))$ avec $r < n$. Mais alors $(x = f^{-1}(y_0), f^{-1}(y_1), ..., f^{-1}(y_{r-1}), f^{-1}(y_r) = y)$ est un chemin de longueur strictement plus petite que n entre x et y, ce qui est impossible.
Donc $f(\gamma)$ est une géodésique entre $f(x)$ et $f(y)$. D'où $d(x, y) = d(f(x), f(y))$.

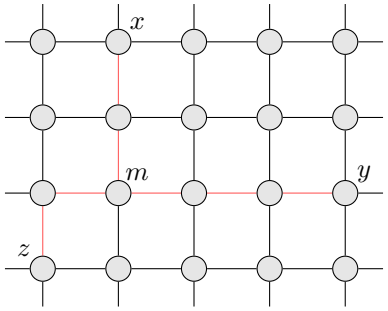
2.3 Graphes médians

Définition Soit X un graphe connexe. On dit que X est **médian** lorsque pour tout triplet de sommets x_1, x_2, x_3 du graphe X, il existe un unique sommet m qui vérifie

$$\forall i, j \in \{1, 2, 3\}, i \neq j, \quad d(x_i, x_j) = d(x_i, m) + d(m, x_j).$$

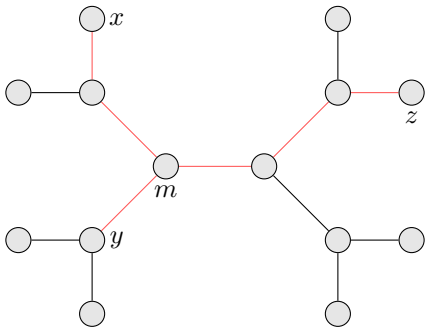
Le sommet m est appelé **point médian** de x_1, x_2, x_3.

Exemples : On se convaint facilement que le graphe de Cayley de $\mathbb{Z}^2$ donné précédemment est médian.



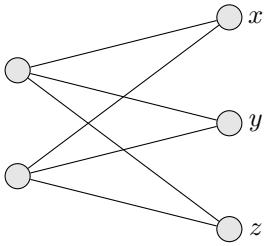
Le point médian de x, y, z est m.

Les arbres sont également des graphes médians. Par exemple, le graphe suivant est médian.



Le point médian de x, y, z est m.

Tous les graphes ne sont pas médians. Par exemple, $K_{2,3}$ n'est pas médian.



Les sommets x, y, z ont deux points médians.

Lemme 2 Soient X et Y deux graphes isomorphes. Alors X est médian si et seulement si Y est médian.

Preuve : Supposons Y médian. Soit f un isomorphisme entre X et Y. Soient $x, y, z \in X$. Comme Y est médian, il existe un unique point médian $m' \in Y$ de $f(x), f(y), f(z)$. Posons $m = f^{-1}(m')$. Alors $d(x, y) = d(f(x), f(y)) = d(f(x), m') + d(m', f(y)) = d(x, m) + d(m, y)$. De même pour x et z et pour y et z. Ainsi, X est médian.
On procède de même pour la réciproque.

Lemme 3 Un graphe médian ne contient pas de sous-graphe isomorphe à K_3 ou $K_{2,3}$.

Preuve : Soit X un graphe et Y un sous graphe de X isomorphe à K_3.
Par l'absurde, supposons que X est médian. Soient x, y, z les trois sommets de Y et m leur point médian. Alors $1 = d(x, y) = d(x, m) + d(m, y)$. Ainsi $d(x, m) = 0$ ou $d(m, y) = 0$. Donc $m = x$ ou $m = y$. Supposons par exemple $m = x$. Alors $1 = d(y, z) = d(y, m) + d(m, z) = 2$. Contradiction. De même pour $m = y$. Ainsi X n'est pas médian.
Supposons désormais que Y est un sous graphe de X isomorphe à $K_{2,3}$. Alors les trois sommets de type 2 admettent au moins deux points médians, à savoir les deux sommets de type 1. Ceci contredit l'unicité, donc X n'est pas médian.

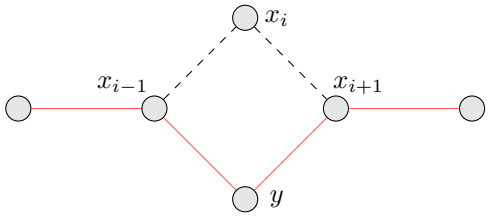
Définition Soit X un graphe médian et Y un sous graphe de X. On dit que Y est **localement convexe** lorsque tout 4-cycle dans X qui a deux arrêtes adjacentes dans Y est entièrement dans Y.

THÉORÈME Soit X un graphe médian et Y un sous graphe connexe de X.
Alors Y est convexe si et seulement si Y est localement convexe.

Nous commençons par introduire des opérations élémentaires sur les chemins.

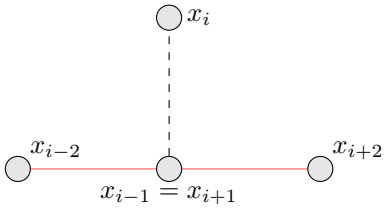
DÉFINITION Soit X un graphe et $\gamma = (x_1, ..., x_n)$ un chemin. Un chemin γ' est obtenu à partir de γ via :

— **retourner 4-cycle**, s'il existe $i \in \{1, ..., n-1\}$ tel que
$$\gamma' = (x_1, ..., x_{i-1}, y, x_{i+1}, ..., x_n)$$
où x_{i-1}, x_i, x_{i+1}, y forment un cycle de longueur 4.



Retourner un4cycle : passer par y au lieu de x_i.

— **retirer un retour en arrière**, s'il existe $i \in \{1, ..., n-2\}$ tel que
$$\gamma' = (x_1, ..., x_{i-1}, x_{i+2}, ..., x_n)$$
et $x_{i-1} = x_{i+1}$.



Retirer un retour en arrière : ne pas passer par x_i.

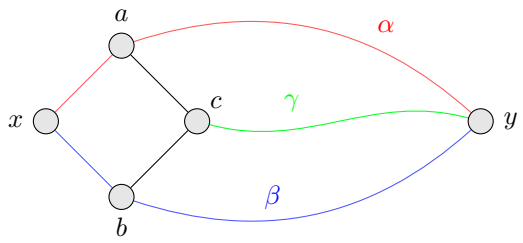
— **ajouter un retour en arrière** si γ peut être obtenu à partir de γ' en retirant un retour en arrière.

Avant de montrer le théorème, démontrons les lemmes suivants.

LEMME 4 Soit X un graphe médian. Soit $(x, y) \in X^2$.
Alors pour toutes géodésiques α, β dans X entre x et y, il existe des géodésiques
$$\alpha = \gamma_0, \gamma_1, ..., \gamma_{n-1}, \gamma_n = \beta$$
entre x et y telle que $\forall i \in \{0, ..., n-1\}, \gamma_{i+1}$ est obtenu via γ_i en retournant un 4-cycle.

PREUVE : On procède par récurrence sur $d(x, y)$.
Si $d(x, y) \leqslant 1$, alors il n'existe qu'une seule géodésique entre x et y. Le résultat est donc clair.
On suppose désormais $d(x, y) \geqslant 2$. Soient α, β deux géodésiques entre x et y, allant de x vers y (i.e. le premier sommet de α et β est x). Si la première arrête de α et β coïncident, alors on obtient le résultat en appliquant l'hypothèse de récurrence sur les deux sous-chemins de α et β commençant au second sommet (ce sont bien des géodésiques).
Sinon, soit a (resp. b) le second sommet de α (resp. β). Soit c le point médian de (a, b, y).
Montrons que a, c, b, x forment un 4-cycle. On remarque que $c \neq x$ car sinon
$$d(x, y) = 1 + d(a, y) = 1 + d(a, x) + d(x, y) > d(x, y).$$

On a également $c \neq a$ car sinon $d(b, y) = d(b, a) + d(a, y) = d(b, a) + d(b, y) > d(b, y)$. De même, $c \neq b$.
Enfin, on a $d(a, b) = 2$. En effet, comme on a un chemin de longueur 2 entre a et b ($[a, x] \cup [x, b]$), on a $d(a, b) \leqslant 2$. Si $d(a, b) = 1$, alors le sous-graphe de X défini par (x, a, b) serait isomorphe à K_3 (car on aurait $d(x, a) = d(a, b) = d(b, x) = 1$), ce qui est impossible d'après le lemme 3.
Ainsi $d(a, b) = d(a, c) + d(c, b) = 2$. Comme $c \neq a$ et $c \neq b$, il vient $d(a, c) = d(b, c) = 1$. Ainsi, $d(a, c) = d(c, b) = d(b, x) = d(x, a) = 1$, $a \neq b$ et $x \neq c$. On obtient bien que a, c, b, x forment un cycle de longueur 4.

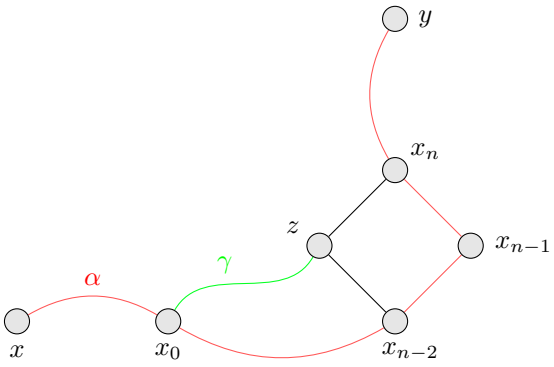


Les sommets a, c, b, x forment un 4-cycle.

Soit γ une géodésique entre c et y. Alors les chemins $\delta_1 := [x,a] \cup [a,c] \cup \gamma$ et $\delta_2 := [x,b] \cup [b,c] \cup \gamma$ sont des géodésiques de x à y. En effet, $\text{long}(\delta_1) = d(x,a) + d(a,c) + d(c,y) = d(x,a) + d(a,y) = \text{long}(\alpha)$ (de même pour δ_2).
Or, par hypothèse de réccurence, $[a,c] \cup \gamma$ peut être obtenu à partir de α' en retournant des 4-cycles, où α' désigne la géodésique obtenue en retirant l'arrête $[x,a]$ à α.
Ainsi, on peut passer de α à δ_1 via cette opération. De même, on peut passer de δ_2 à β en retournant des 4-cycles. Enfin, il est clair qu'on peut passer de δ_1 à δ_2 via cette opération.
Donc on peut obtenir β à partir de α en retournant des 4-cycles, ce qui conclut la preuve.

LEMME 5 Soient X un graphe médian, $x, y \in X$.
Alors tout chemin γ dans X entre x et y qui n'est pas une géodésique peut être réduit (au sens de diminuer sa longueur) en retournant des 4-cycles et en retirant des retours en arrière.

PREUVE : Soit α un chemin entre x et y qui n'est pas une géodésique. Soit $\sigma \subset \alpha$ un sous-chemin de longueur minimale tel que ce ne soit pas une géodésique. Notons $\sigma = (x_0, \cdots, x_n)$. Remarquons que, par définition de σ, $d(x_0, x_n) = d(x_0, x_{n-1}) - 1 = d(x_0, x_{n-2})$. Si $x_n = x_{n-2}$, alors on peut réduire σ (et donc α) en retirant un retour en arrière. On suppose dorénavant $x_n \neq x_{n-2}$.
Soit z le point médian de (x_0, x_{n-2}, x_n). On a $d(x_n, x_{n-2}) \neq 1$ car sinon le sous-graphe défini par les sommets (x_n, x_{n-1}, x_{n-2}) serait isomorphe à K_3. Donc $2 = d(x_0, x_{n-2}) = d(x_n, z) + d(z, x_{n-2})$. Or $z \neq x_{n-2}$ car sinon on aurait $d(x_0, x_n) = d(x_0, x_{n-2}) + d(x_{n-2}, x_n) > d(x_0, x_{n-2}) = d(x_0, x_n)$. De même, $z \neq x_{n-1}$ et $z \neq x_n$. Donc $d(x_n, z) = d(z, x_{n-2}) = 1$. Ainsi on a $z \neq x_{n-1}$ et $x_n \neq x_{n-2}$ et $d(x_n, x_{n-1}) = d(x_{n-1}, x_{n-2}) = d(x_{n-2}, z) = d(z, x_n) = 1$.
Donc x_n, x_{n-1}, x_{n-2}, z définissent un 4-cycle.



Les sommets x_n, x_{n-1}, x_{n-2}, z définissent un 4-cycle.

Soit γ une géodésique entre x_0 et z. Alors $\gamma \cup [z, x_n]$ peut être obtenu de $\gamma \cup [z, x_{n-2}] \cup [x_{n-2}, x_{n-1}] \cup [x_{n-1}, x_n]$ en retournant un 4-cycle et en retirant un retour en arrière. De plus, $\gamma \cup [z, x_{n-2}]$ et $[x_0, x_1] \cup \ldots \cup [x_{n-3}, x_{n-2}]$ sont deux géodésiques avec les mêmes extrémités. Par le lemme 4, on peut passer de l'une à l'autre en retournant des 4-cycles. Comme retirer un retour en arrière réduit la taille du chemin, on a bien démontré le résultat.

LEMME 6 Soient X un graphe médian, $x, y \in X$.
Alors pour tous chemins α, β dans X entre x et y, il existe des chemins

$$\alpha = \gamma_0, \gamma_1, ..., \gamma_{n-1}, \gamma_n = \beta$$

entre x et y tels que $\forall i \in \{0, ..., n-1\}, \gamma_{i+1}$ est obtenu via γ_i en retournant des 4-cycles, retirant des retours en arrière et ajoutant des retours en arrière.

Preuve : Soit α, β deux chemins entre x et y. Il est clair par le lemme 5 que α (resp. β) peut être transformé en une géodésique α' (resp. β') entre x et y en retournant des 4-cycles et en retirant des retours en arrière.
Or par le lemme 4, β' peut être obtenu via α' en retournant des 4-cycles. Ainsi, β peut être obtenu via α avec les trois opérations élémentaires.

Preuve du théorème :
$\Rightarrow$: Soit $a, b, c, d \in X$ formant un 4-cycle. Disons par exemple que $a \sim_X b \sim_X c \sim_X d \sim_X a$. Alors $d(a, c) \leqslant 2$.
Si $d(a, c) = 1$, alors le sous-graphe formé par a, b, c est isomorphe à K_3, ce qui est impossible par le lemme 3.
Donc $d(a, c) = 2$. Ainsi, $\text{long}([a, d] \cup [d, c]) = 2 = d(a, c)$.
Donc $[a, d] \cup [d, c]$ est une géodésique. Par convexité de Y, cette géodésique reste dans Y. Donc le cycle de longueur 4 est entièrement dans Y et Y est localement convexe.
$\Leftarrow$: Soient $x, y \in X$ et $\gamma \subset Y$ un chemin arbitraire entre x et y. D'après le lemme 5, γ peut être transformé en une géodésique γ' en retournant des 4-cycles et en retirant des retours en arrière. Comme Y est localement convexe, un chemin dans X obtenu à partir d'un chemin dans Y en retournant un 4-cycle est encore dans Y. Ainsi, $\gamma' \subset Y$. Soit γ'' une géodésique entre x et y dans X. Par le lemme 4, γ'' peut être obtenu via γ' en retournant des 4-cycles. Par le même argument que précédemment, on obtient bien que $\gamma'' \subset Y$. Donc Y est convexe.

2.4 Hyperplans

La principale notion permettant de mieux comprendre la structure des graphes médians est celle d'hyperplan. Elle nous invite à classer les arrêtes du graphe en mettant deux arrêtes dans la même classe si elles sont opposées dans un 4-cycle et à considérer la clôture transitive de cette relation.

Définition Soit X un graphe.
On définit les relations binaires $\mathcal{R}_X$ et $C(\mathcal{R}_X)$ sur les arrêtes par, pour toutes arrêtes $A, B \subset X$:
- $A \ \mathcal{R}_X \ B \Leftrightarrow A$ et B sont opposées dans un 4-cycle.
- $A \ C(\mathcal{R}_X) \ B \Leftrightarrow \exists A_1, ..., A_n \subset X$ des arrêtes tel que $A = A_1 \ \mathcal{R}_X \ A_2 \ \mathcal{R}_X \ ... \ \mathcal{R}_X \ A_{n-1} \ \mathcal{R}_X \ A_n = B$.

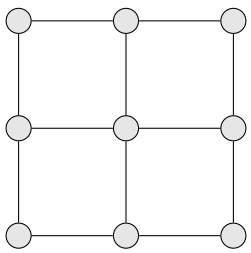
Quand il n'y aura pas d'ambiguité sur le graphe considéré, nous noterons ces relations $\mathcal{R}$ et $C(\mathcal{R})$.

Proposition Soit X un graphe. La relation $C(\mathcal{R})$ définie précédemment est une relation d'équivalence.

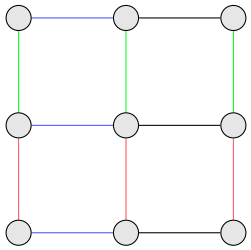
Preuve : La réflexivité et la transitivité sont claires. La symétrie découle de la symétrie de $\mathcal{R}$.

Définition Soit X un graphe médian. Un **hyperplan** est une classe d'équivalence pour la relation $C(\mathcal{R})$ (c'est donc un ensemble d'arrêtes). Soit J un hyperplan.
- Le **voisinage** de J, noté $N(J)$ est le sous-graphe de X défini par tous les sommets des arrêtes de J.
- Si $X \backslash\backslash J$ dénote le graphe obtenu en retirant à X toutes les arrêtes de J, alors un **demi-espace** est une composante connexe de $X \backslash\backslash J$.
- Une **fibre** est une composante connexe de $N(J) \cap X \backslash\backslash J$.
- Deux sous-ensembles de sommets $A, B \subset X$ sont **séparés par J** s'il existe deux demi-espaces distincts tels que A est inclus dans l'un et B est inclus dans l'autre. On notera $W(A|B)$ l'ensemble de tous les hyperplans qui séparent A et B.
- Deux hyperplans J_1 et J_2 sont **transverses** s'il existe deux arrêtes $e_1 \in J_1$ et $e_2 \in J_2$ tel que e_1 et e_2 appartiennent à un même 4-cycle.
- Deux hyperplans sont **tangents** s'il existe deux arrêtes $e_1 \in J_1$ et $e_2 \in J_2$ telles que e_1 et e_2 sont adjacents mais ne sont pas dans un même 4-cycle.

Exemple : On part d'une partie du graphe de Cayley de $\mathbb{Z}^2$.

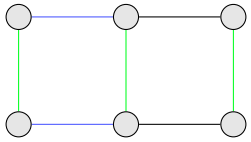


Représentons ses hyperplans en coloriant de la même couleur les arrêtes appartenant au même hyperplan.



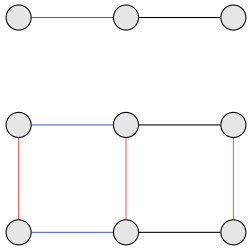
Les hyperplans sont coloriés de la même couleur.

On considère l'hyperplan colorié en vert. Le voisinage de cet hyperplan est le graphe suivant.



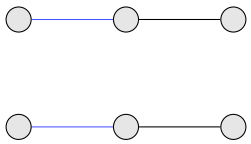
Le voisinage de l'hyper plan vert.

Dessinons les demi-espaces délimités par l'hyperplan vert.



Les demi-espaces de l'hyperplan vert.

On obtient alors les fibres de l'hyperplan vert en intersectant les deux graphes précédents.



Les fibres de l'hyperplan vert.

On remarque que les hyperplans vert et rouge sont tangents et que les hyperplans bleu et rouge sont transverses.

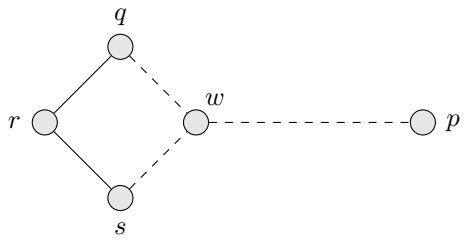
Nous allons désormais étudier les propriétés des hyperplans. Dans ce but, commençons par plusieurs lemmes.

LEMME 7 Soient X un graphe médian et $x, y, z \in X$. Si y et z sont adjacents, alors $d(x, y) \neq d(x, z)$

PREUVE : Soit m le point médian de (x, y, z). On a $1 = d(y, z) = d(y, m) + d(m, z)$. Ainsi, $d(y, m) = 0$ ou $d(m, z) = 0$, c'est à dire $m = y$ ou $m = z$. Supposons $m = y$. Alors $d(x, z) = d(x, y) + 1$. Si $m = z$, alors $d(x, y) = d(x, z) + 1$. Dans les deux cas, on a bien $d(x, y) \neq d(x, z)$.

LEMME 8 Soient X un graphe médian et $p, q, r, s \in X$. On suppose que r est adjacent à q et s.
Si $d(p, q) = d(p, s) = d(p, r) - 1$, alors il existe un unique sommet $w \in X$ qui vérifie $d(p, w) = d(p, r) - 2$ et qui est adjacent à q et s.

PREUVE : Si $q = s$, considérons γ une géodésique entre p et $q = s$ et posons w le sommet adjacent à $q = s$ dans γ (il n'y en qu'un car sinon ce ne serait pas une géodésique).
Alors on a $d(p, r) = d(p, q) + 1 = d(p, w) + 2$, ce qui est le résultat attendu.
On suppose dorénavant $q \neq s$. Soit w le point médian de (p, q, s).



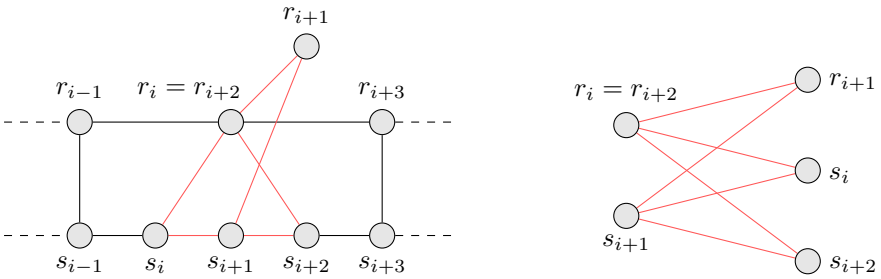
Le sommet w est le point médian de (p, q, s).

Si $w = q$, alors $d(p, q) = d(p, s) = d(p, q) + d(q, s) > d(p, q)$, contradiction. Donc $w \neq q$. De même, $w \neq s$.
De plus, si $d(q, s) = 1$ alors le sous-graphe défini par les sommets (q, r, s) est isomorphe à K_3, ce qui est impossible. Donc $2 = d(q, s) = d(q, w) + d(w, s)$. Comme ces deux distances sont non nulles, c'est que $d(q, w) = d(w, s) = 1$ et w est adjacent à q et s. De plus, $d(p, r) - 1 = d(p, q) = d(p, w) + 1$, ce qui est le résultat escompté.

DÉFINITION Soient X un graphe et $\alpha = (x_0, ...x_n), \beta = (y_0, ..., y_r) \subset X$ deux chemins.
On dit que α et β sont **parallèles** si $n = r$ et $\forall i \in \{0, ..., n\}$, les sommets x_i et y_i sont adjacents.

LEMME 9 Soient X un graphe médian et $[a, b], [x, y] \subset X$ deux arrêtes.
Soit r (resp. s) un chemin entre a et x (resp. b et y). On suppose que r et s sont parallèles.
Si r' est un chemin obtenu via r en retournant des 4-cycles (resp. en retirant des retours en arrières), alors il existe un chemin s' obtenu via s en retournant des 4-cycles (resp. en retirant des retours en arrières) et qui est encore parallèle à r'.

PREUVE : Notons $r = (a = r_0, r_1, ..., r_{n-1}, r_n = x)$ et $s = (b = s_0, s_1, ..., s_{n-1}, s_n = y)$.
Supposons que r' soit un chemin obtenu via r en retirant un retour en arrière.
Alors $\exists i \in \{0, ..., n-2\}$ tel que $r_i = r_{i+2}$ et $r' = (a = r_0, r_1, ..., r_i, r_{i+3}, ..., r_{n-1}, r_n = x)$. Par construction, r_{i+1} et s_i appartiennent à un même 4-cycle. Donc $r_{i+1} \neq s_i$. De même, $r_{i+1} \neq s_{i+2}$ et $r_{i+2} \neq s_{i+1}$. Si $s_i \neq s_{i+2}$ alors $s_i, s_{i+1}, s_{i+2}, r_{i+1}$ et $r_i = r_{i+2}$ définissent un sous-graphe de X isomorphe à $K_{2,3}$, ce qui est impossible.



Le graphe médian X contient un sous-graphe isomorphe à $K_{2,3}$.

Donc $s_i = s_{i+2}$. Ainsi, $s' := (b = s_0, s_1, ..., s_i, s_{i+3}, ..., s_{n-1}, s_n = y)$ peut être obtenu via s en retirant un retour en arrière et est parallèle à r'.
Supposons que r' est obtenu via r en retournant un 4-cycle. Alors $\exists i \in \{1, ..., n-1\}$ et $\exists c \in X$ tels que r_{i-1}, r_i, r_{i+1}, a forment un 4-cycle et $r' = (a = r_0, r_1, ..., r_{i-1}, c, r_{i+1}, ..., r_{n-1}, r_n = x)$.
Comme r_{i-1}, r_i, r_{i+1}, c forment un 4-cycle, on a $r_{i-1} \neq r_{i+1}$. Donc $[r_{i-1}, r_1] \cup [r_i, r_{i+1}]$ n'est pas un retour en arrière. On en déduit via la preuve du cas précédent que $[s_{i-1}, s_1] \cup [s_i, s_{i+1}]$ n'est pas non plus un retour en arrière, et donc que $s_{i-1} \neq s_{i+1}$. Ainsi, $r_{i-1}, r_i, r_{i+1}, s_{i-1}, s_i$ et s_{i+1} sont deux à deux distincts.
De plus, s_{i-1} n'est pas adjacent à r_{i+1} car sinon le sous-graphe défini par les sommets $s_{i-1}, r_{i-1}, r_i, r_{i+1}$ et s_i serait isomorphe au graphe $K_{2,3}$, ce qui est impossible. Donc $a \neq s_{i-1}$. De même, $a \neq s_{i+1}$. De plus, si $d(s_{i-1}, s_{i+1}) = 1$ alors le sous-graphe défini par les sommets s_{i-1}, s_i, s_{i+1} serait isomorphe à K_3, ce qui est impossible. Donc $d(s_{i-1}, s_{i+1}) = 2$.
De même, $d(s_{i-1}, c) = d(c, s_{i+1}) = 2$. On en déduit que le point médian de c, s_{i-1}, s_{i+1}, noté d, est adjacent à ces 3 sommets. Posons $s' = (b = s_0, s_1, ..., s_{i-1}, d, s_{i+1}, ..., s_{n-1}, s_n = y)$.
Alors, par construction, s' est obtenu via s en retournant un 4-cycle et est parallèle à r'.

LEMME 10 Soient X un graphe médian et $[a, b], [x, y] \subset X$ deux arrêtes.
Si $[a, b]$ et $[x, y]$ appartiennent au même hyperplan, alors pour toute géodésique p entre a et x, il existe une géodésique q entre b et y telle que p et q soient parallèles.

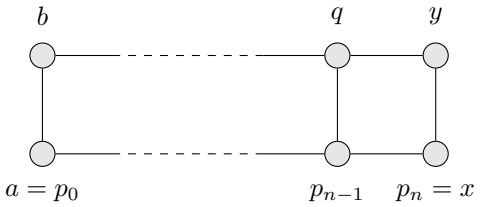
PREUVE : Tout d'abord, comme $[a, b]$ et $[x, y]$ appartiennent au même hyperplan, on a $[a, b]\ C(\mathcal{R})\ [x, y]$.
Par définition, $\exists [r_1, s_1], ..., [r_{n-1}, s_{n-1}]$ telles que $[a, b]\ \mathcal{R}\ [r_1, s_1]\ \mathcal{R}...\mathcal{R}\ [r_{n-1}, s_{n-1}]\ \mathcal{R}\ [x, y]$. Quitte à "retourner" les arrêtes, on peut supposer que $(a, r_1, ..., r_{n-1}, x)$ forme un chemin entre a et x. Notons le r.
Alors, par définition de $\mathcal{R}$, $(b, s_1, ..., s_{n-1}, y)$ forme aussi un chemin, que nous noterons s. Remarquons que r et s sont parallèles par construction.
Soit p une géodésique. D'après le lemme 5, on peut passer de r à une géodésique r' entre a et x en retournant des 4-cycles et retirant des retours en arrière. D'après le lemme 4, on peut passer de r' à p en retournant des 4-cycles. Ainsi, on peut passer de r à p en retournant des 4-cycles et en retirant des retours en arrières. D'après le lemme 9, il existe un chemin q entre b et y, parallèle à p et obtenu via s avec ces deux opérations. Il reste donc à montrer que q est une géodésique.
Par l'absurde, si q n'est pas une géodésique, alors il existe q' un chemin entre b et y obtenu via q et qui contient un retour en arrière. Or, d'après le lemme 9, il existe un chemin p' parallèle à q' obtenu à partir de p en retournant des 4-cycles. Comme cette opération ne modifie par la longueur du chemin, on a $\text{long}(p') = \text{long}(p)$ et donc p' est une géodésique. Or le lemme 9 implique que p' contient un retour en arrière et peut donc être raccourci. Contradiction.
Ainsi, q est une géodésique et le résultat est démontré.

COROLLAIRE Dans un graphe médian, deux arrêtes distinctes dans le même hyperplan sont disjointes (aucun des sommets de la première n'est égal à un sommet de la deuxième).

PREUVE : Soient X un graphe médian et $x, y, z \in X$ trois sommets tels que x est adjacent à y et z. Si $[x, y]$ et $[z, x]$ appartiennent au même hyperplan, alors d'après le lemme 10, les sommets x, y, x, z forment un 4-cycle, ce qui est absurbe.
Ainsi, si $[a, b]$ et $[c, d]$ sont deux arrêtes distinctes et que, par exemple, $a = c$, alors elles n'appartiennent pas au même hyperplan.

LEMME 11 Soient X un graphe médian et $[a, b], [x, y] \subset X$ deux arrêtes.
Si $d(a, x) < d(a, y)$ et $d(b, y) < d(b, x)$, alors $[a, b]$ et $[x, y]$ appartiennent au même hyperplan.

PREUVE : On a $d(a, x) < d(a, y) \leqslant d(a, b) + d(b, y) < 1 + d(b, x)$. De plus, $d(b, x) \leqslant 1 + d(a, x)$. Or, a et b étant adjacents, on a par le lemme 7 que $d(a, x) \neq d(b, x)$. D'où $d(b, x) = d(a, x) + 1$. Ainsi, $1 + d(a, x) < d(b, x) \leqslant d(b, y) + d(y, x) = d(b, y) + 1$. Donc $d(a, x) \leqslant d(b, y)$. Par symétrie, on peut également montrer que $d(b, y) \leqslant d(a, x)$. Ainsi, $d(a, x) = d(b, y)$.
Soit $p = (a = p_0, p_1, ..., p_{n-1}, p_n = x)$ une géodésique. On a $d(b, x) > d(b, y) = d(a, x)$ donc $d(b, x) = d(a, x) + 1$. D'où $[b, a] \cup p$ est une géodésique. On a donc $d(b, p_{n-1}) = 1 + d(a, p_{n-1}) = d(a, x) = d(b, y)$. On a montré que $d(b, y) = d(b, p_{n-1}) = d(b, x) - 1$. On peut alors appliquer le lemme 8. On obtient un sommet q adjacent à y et p_{n-1} tel que $d(b, q) = d(b, x) - 2$. De plus, $p_{n-1} \neq y$ car $d(a, p_{n-1}) = d(a, x) - 1 = d(a, y) - 2$. Ainsi, les sommets x, y, q et p_{n-1} forment un 4-cycle. Donc $[x, y]$ et $[p_{n-1}, q]$ sont dans le même hyperplan.



Les arrêtes $[x, y]$ et $[p_{n-1}, q]$ sont dans le même hyperplan.

Notons que

$$d(b, q) = d(b, x) - 2 = d(a, x) - 1 = d(a, p_{n-1}) = d(b, p_{n-1}) - 1 < d(b, p_{n-1}).$$

et que

$$d(a, p_{n-1}) = d(a, x) - 1 = d(a, y) - 2 \leqslant d(a, q) - 1 < d(a, q).$$

On peut donc itérer ce raisonnement en remplaçant $[x, y]$ par $[p_{n-1}, q]$ et ainsi de suite. On obtient alors bien que $[x, y]$ et $[a, b]$ sont dans le même hyperplan.

Nous sommes désormais en mesure de montrer que les graphes médians vérifient les propriétés suivantes :

Théorème Dans un graphe médian, nous avons les propriétés suivantes.

1. Tout hyperplan délimite exactement deux demi-espaces.
2. Les voisinnages, les demi-espaces et les fibres sont convexes.
3. Un chemin est une géodésique si et seulement s'il passe par chaque hyperplan au plus une fois.
4. La distance entre deux sommets coïncide avec le nombre d'hyperplans qui les séparent.

Preuve : Soit X un graphe médian.

1. Soit J un hyperplan et $[x,y] \in J$. On pose :
$$H(x,y) := \{z \in X \mid d(z,x) < d(z,y)\} \text{ et } H(y,x) := \{z \in X \mid d(z,y) < d(z,x)\}.$$
On va montrer que $H(x,y)$ et $H(y,x)$ sont les deux seules composantes connexes de $X\backslash\backslash J$.
Tout d'abord, par le lemme 7, tout sommet de X est dans l'un de ces deux ensembles.
Soit γ un chemin d'un sommet de $H(x,y)$ vers un sommet de $H(y,x)$. Alors $\exists [a,b] \subset \gamma$ une arrête tel que $a \in H(x,y)$ et $b \in H(y,x)$. Ainsi, $d(a,x) < d(a,y)$ et $d(b,y) < d(b,x)$. En appliquant le lemme 11, on obtient que $[a,b] \subset J$. Ainsi, $H(x,y)$ et $H(y,x)$ sont disjoints dans $X\backslash\backslash J$.
Il reste à montrer que $H(x,y)$ et $H(y,x)$ sont connexes. Soit $z \in H(x,y)$. On va montrer qu'il existe un chemin entre z et x qui ne passe pas par J. Soit $[u,v] \in \{[u,v] \in J \mid d(z,u) \text{ est minimal}\}$. Par construction, toute géodésique α entre z et u ne passe pas par J. Si $u = x$, c'est terminé. Sinon, soit β une géodésique entre u et x. Comme $[u,v]$ et $[x,y]$ appartiennent à J, le lemme 10 et son corollaire permettent d'affirmer que β ne passe pas par J. Ainsi, $\alpha \cup \beta$ est un chemin de z à x ne passant pas par J. Soit $w \in H(x,y)$. Alors en reliant z à x puis x à w avec des chemins ne passant pas par J, on obtient un chemin entre z et w dans $X\backslash\backslash J$.
Donc $H(x,y)$ est connexe. On montre de même que $H(y,x)$ est connexe.
2. Soient J un demi-espace et $x,y \in X$ dans une des deux fibres délimitées par J (il n'y en que 2 par le premier point). Soit $x' \in J$ (resp. $y' \in J$) le voisin de x (resp. y) tel que $[x,x'] \subset J$ (resp. $[y,y'] \subset J$). Comme x et y ne sont pas séparés par J, on a $y \in H(x,x')$. Ainsi, par le lemme 10, toute géodésique entre x et y reste dans la fibre. Donc les fibres sont convexes.
Soient $x,y \in N(J)$ et γ une géodésique entre x et y. Si x et y sont dans la même fibre, alors γ reste dedans car les fibres sont convexes et donc γ reste dans $N(J)$. Sinon, J sépare x et y. Donc J peut se décomposer en $\alpha \cup e \cup \beta$ où $e \in J$ et α et β sont chacun dans une fibre. Par convexité des fibres, $\alpha, \beta \subset N(J)$ et donc $\gamma \subset N(J)$. Donc les voisinnages sont convexes.
Soient $x,y \in X$ deux sommets dans un même demi-espace délimité par J. Soit γ une géodésique entre x et y. Si γ n'intersecte pas $N(J)$, alors γ reste dans le même demi-espace. Sinon, soit $p \in N(J)$ le premier sommet de γ qui est dans $N(J)$ et $q \in N(J)$ le dernier. Alors p et q sont dans la fibre située dans le même demi-espace que x et y. Par convexité des fibres, le sous-chemin de γ entre p et q reste dans le demi-espace. Ainsi γ reste dans le demi-espace de x et y. Donc les demi-espaces sont convexes.
3. 4. Soient $x,y \in X$. Un chemin entre x et y doit clairement passer par chaque hyperplan qui les sépare. De plus, par convexité des demi-espaces, une géodésique entre x et y passe au plus une fois par chaque hyperplan. Donc un chemin de x à y est une géodésique si et seulement si il passe une et une seule fois par chaque hyperplan qui sépare x et y. Ceci implique le point 4. Enfin, un chemin de x à y qui passe par un hyperplan qui ne sépare pas x et y doit le croiser au moins deux fois, ce qui permet d'en déduire le point 3.

3 Graphe de Cayley des groupes de cactus

3.1 Le théorème

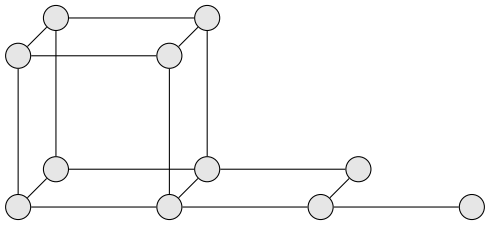
L'objectif de cette section est de prouver le théorème suivant.

Théorème Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$.
Alors, le graphe de Cayley de J_n relatif aux générateurs qui définissent J_n est médian.

Définissons tout d'abord les notions dont nous aurons besoin pour la preuve du théorème.

Définition Un **complexe cubique** est un espace métrique obtenu en recollant autant de 0-cubes que l'on souhaite, autant de 1-cubes que l'on souhaite, ... , et des n-cubes (c'est-à-dire des cubes de dimension n de coté 1) de façon isométrique, en identifiant des cubes de dimension k avec des cubes de dimension k.

Exemple : Donnons un exemple de complexe cubique, où on a recollé un 3-cube, un 2-cube et un 1-cube.



Un complexe cubique.

Définition Soit X un complexe cubique. Le **k-squelette** de X noté $X^{(k)}$ est la réunion des cubes de dimension inférieure ou égale à k.

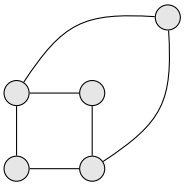
Remarque : Le 1-squelette d'un graphe est égal au graphe lui-même.

Définition Soit X un complexe cubique. On dit que X est **simplement connexe** lorsque pour tout sommet $x \in X$ et pour toute boucle combinatoire qui passe par x (un chemin qui boucle sur lui-même et qui passe par x), il existe une suite de chemins combinatoires qui passent par x telle que chaque chemin est obtenu à partir du précédent en retournant un carré ou en rajoutant un un retour en arrière ou en retirant un retour en arrière, et telle que le dernier chemin de cette suite finie est $\{x\}$.

Pour montrer le théorème, on va utiliser la proposition qui suit, dont on ne donne pas de preuve.

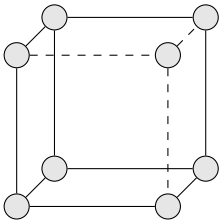
Proposition Soit X un complexe cubique. Supposons que les quatre assertions suivantes sont vérifiées.

1. Le complexe cubique X est simplement connexe.
2. Les carrés de X sont "embedded".
3. Deux carrés distincts ne partagent jamais deux arrêtes consécutives.



Cette situation est supposée impossible.

4. Un cycle de trois carrés s'étend en le 2-squelette d'un 3-cube.

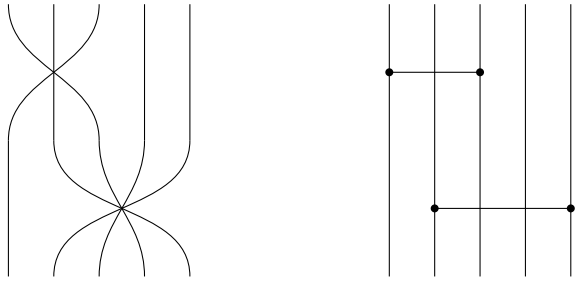


Un cycle de trois carrés s'étent en un 3-cube.

Alors, le 1-squelette de X est un graphe médian. De plus, tout 4-cycle dans $X^{(1)}$ délimite un carré dans X.

Avant d'appliquer ce critère au graphe de Cayley de J_n pour $n \geqslant 2$, nous introduisons une nouvelle représentation pour les éléments des groupes de cactus et donnons des noms aux relations imposées aux générateurs.

NOTATION On change l'ancienne notation des éléments des groupes de cactus en remplaçant les courbures par des *intervalles* (des lignes horizontales qui rejoignent les deux extrémités du générateur en question).

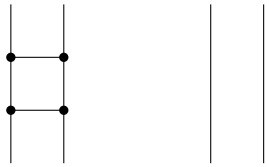


L'ancienne (à gauche) et la nouvelle (à droite) représentation de l'élément $s_{1,3}s_{2,5} \in J_5$.

Définissons deux opérations disponibles pour modifier un diagramme qui représente un élément d'un groupe de cactus.

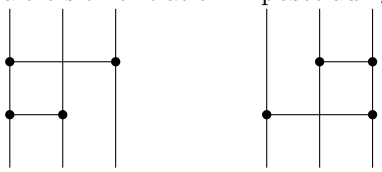
DÉFINITION Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Dans le groupe de cactus J_n,

— la relation qui consiste à retirer deux lignes horizontales successives et de même taille est une **réduction**.



On réduit le diagramme de gauche en celui de droite.

— la relation qui consiste à appliquer la troisième relation imposée aux générateurs est un **retournement**.



On retourne le diagramme de gauche pour obtenir celui de droite.

— la **longueur** d'un diagramme est égal au nombre de lignes horizontales qu'il contient.

— un diagramme est **réduit** quand on ne peut plus faire de réductions, même après des retournements.

Nous allons montrer qu'à partir d'un diagramme qui représente un élément d'un groupe de cactus, on peut trouver un diagramme sous forme *normale* en appliquant des réductions et des retournements à notre diagramme de départ, et que le diagramme normal ainsi obtenu est unique.

DÉFINITION Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. On dit qu'un diagramme qui représente un élément de J_n est **sous forme normale** lorsqu'il est réduit, et que l'on ne peut pas appliquer de réductions ou de retournements pour faire monter un intervalle (ligne horizontale) au dessus d'un intervalle plus petit.

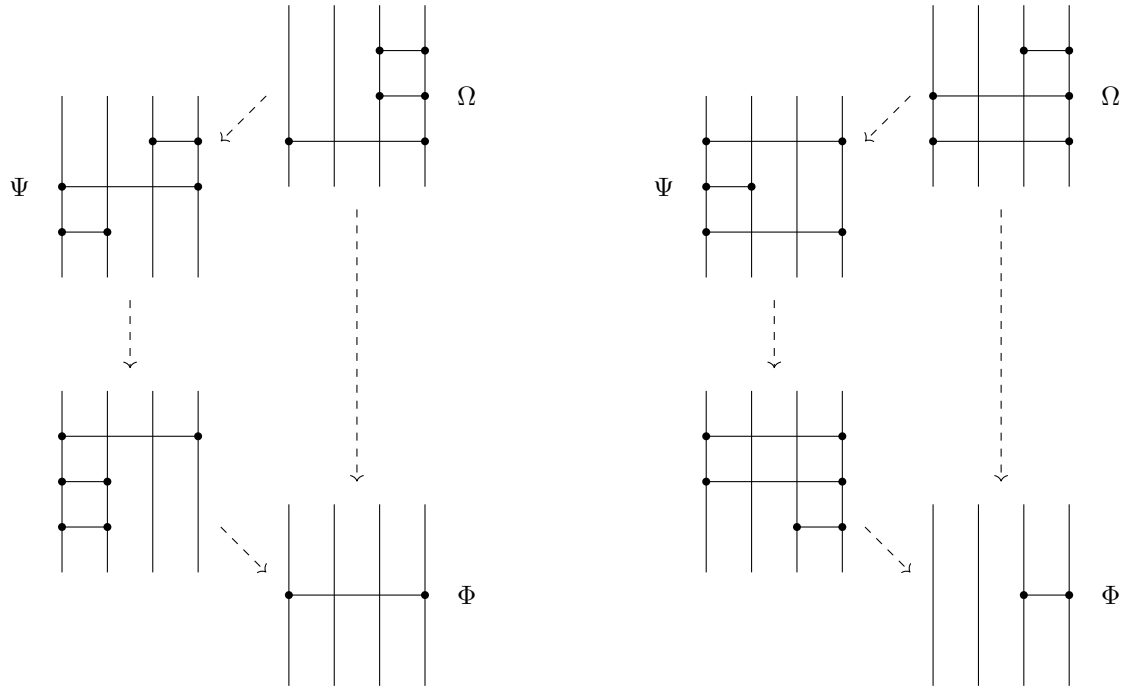
NOTATION On note $\equiv$ l'égalité des diagrammes modulo réductions et retournements.

PROPOSITION Soit Δ un diagramme qui représente un élément d'un groupe de cactus.
Alors, il existe un unique diagramme Δ_0 sous forme normale tel que $\Delta \equiv \Delta_0$.
De plus, Δ_0 peut être obtenu à partir de Δ en appliquant des réductions et des retournements de paires d'intervalles qui font monter un intervalle plus grand.

PREUVE : Notons $\mathcal{G}(\Delta)$ le graphe orienté dont les sommets sont tous les diagrammes qui sont $\equiv$-égaux à Δ et dont les arrêtes relient un diagramme Δ_1 à un autre diagramme Δ_2 lorsque Δ_2 peut être obtenu depuis Δ_1 par réduction ou bien en retournant une paire d'intervalles pour faire monter un intervalle plus grand.
Lorsque Δ_1 et Δ_2 sont deux sommets de $\mathcal{G}(\Delta)$, on note $\Delta_1 \to \Delta_2$ si une arrête a pour origine Δ_1 et pour cible Δ_2, et on note $\Delta_1 \hookrightarrow \Delta_2$ si il existe un chemin orienté de Δ_1 vers Δ_2 dans le graphe $\mathcal{G}(\Delta)$.

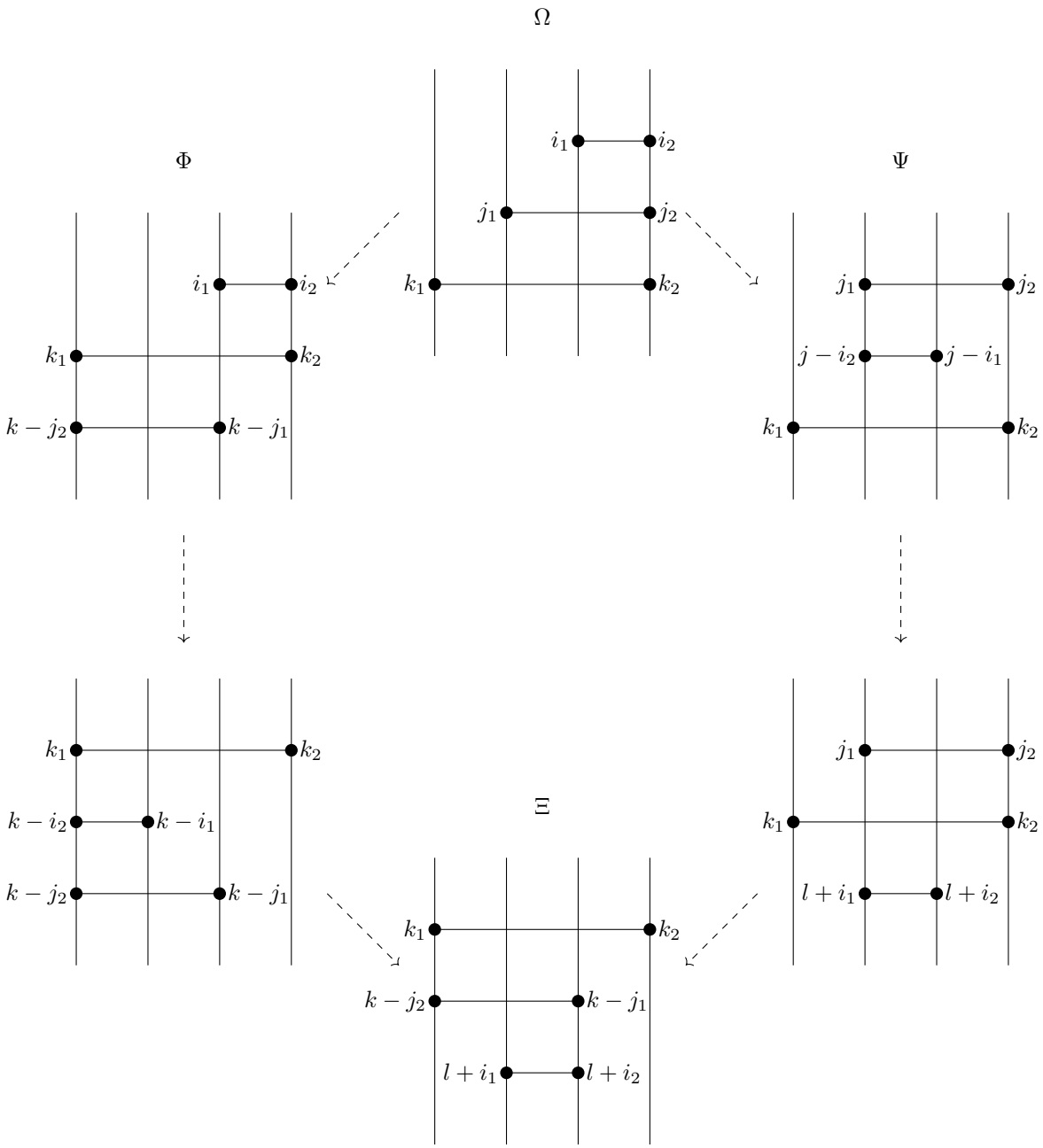
Tout d'abord, remarquons que le graphe non orienté induit par $\mathcal{G}(\Delta)$ est **connexe** par définition de l'égalité modulo réductions et retournements et par définition de $\mathcal{G}(\Delta)$.
De plus, $\mathcal{G}(\Delta)$ est "terminating", c'est-à-dire qu'il n'y a pas de chemin infini dans le graphe. Pour prouver cela, il suffit d'introduire une fonction de complexité χ qui à un diagramme du graphe $\mathcal{G}(\Delta)$ associe un entier et qui vérifie que si Ω et Φ sont deux diagrammes tels que $\Omega \to \Phi$, on a $\chi(\Omega) > \chi(\Phi)$. Pour tout diagramme Ω de $\mathcal{G}(\Delta)$, on pose $\chi(\Omega)$ qui vaut le nombre de couples (n, m) tels que tous les brins qui passent à travers n dans Ω passent aussi à travers m avec n au dessus de m. Ainsi, χ est à valeurs entières et si $\Omega \to \Phi$ avec Φ obtenu à partir de Ω par retournement, $\chi(\Omega) > \chi(\Phi)$ et si Φ est obtenu à partir de Ω par réduction, on a aussi $\chi(\Omega) > \chi(\Phi)$ car l'intervalle du haut des deux intervalles identiques passe en dessous du second.
Enfin, montrons que $\mathcal{G}(\Delta)$ est *localement confluent*, c'est-à-dire que si Ω, Φ, Ψ sont trois diagrammes distincts tels que $\Omega \to \Phi$ et $\Omega \to \Psi$, alors il existe un diagramme Ξ tel que $\Phi \hookrightarrow \Xi$ et $\Psi \hookrightarrow \Xi$. Soient donc Ω, Φ, Ψ trois diagrammes distincts tels que $\Omega \to \Phi$ et $\Omega \to \Psi$. Quatre cas se présentent.

1. Si Φ et Ψ sont tous les deux obtenus à partir de Ω par une réduction, les paires qui ont été réduites sont distinctes. Dans le cas contraire, on aurait nécessairement $\Phi = \Psi$ ce qui est impossible car les diagrammes sont supposés distincts. Comme les paires sont disjointes, on obtient peut poser Ξ le diagramme obtenu en réalisant les deux réductions successivement. On a alors $\Phi \to \Xi$ et $\Psi \to \Xi$ donc en particulier, $\Phi \hookrightarrow \Xi$ et $\Psi \hookrightarrow \Xi$.
2. Si Φ est obtenu par une réduction et Ψ par un retournement, deux sous-cas se présentent.
   Si les paires d'intervalles qui correspondent aux opérations $\Omega \to \Phi$ et $\Omega \to \Psi$ sont disjointes, il suffit de considérer Ξ le diagramme obtenu en faisant les deux opérations l'une après l'autre.
   Sinon, il suffit de poser $\Xi = \Phi$, comme justifié par les diagrammes ci-dessous.



Les deux configurations possibles dans le cas où les opérations ne sont pas disjointes.

   Les schémas montrent que l'on a bien $\Psi \hookrightarrow \Phi$ en un retournement suivi d'une réduction.
3. Le cas où Ψ est obtenu par une réduction et Φ par un retournement est symétrique au cas précédent.
4. Il ne reste que le cas où Φ et Ψ sont tous les deux obtenus par un retournement. Comme précédemment, si les paires d'intervalles des deux retournements sont disjointes, il suffit de réaliser les deux retournements successivement pour obtenir un diagramme Ξ qui convient. Sinon, on construit Ξ de la façon suivante.



Obtention du diagramme Ξ *avec* $k = k_1 + k_2$, $j = j_1 + j_2$ *et* $l = k - j$.

Ce schéma montre qu'on a $\Phi \hookrightarrow \Xi$ et $\Psi \hookrightarrow \Xi$, comme voulu.

Ainsi, $\mathcal{G}(\Delta)$ est localement confluent. On en déduit sans peine que $\mathcal{G}(\Delta)$ est **confluent**, c'est-à-dire que si Ω, Φ, Ψ sont trois diagrammes distincts tels que $\Omega \hookrightarrow \Phi$ et $\Omega \hookrightarrow \Psi$, alors il existe un diagramme Ξ tel que $\Phi \hookrightarrow \Xi$ et $\Psi \hookrightarrow \Xi$.
Un diagramme est normal si et seulement si aucune arrête ne sort de ce diagramme dans $\mathcal{G}(\Delta)$ par définition de diagramme normal. Donc comme $\mathcal{G}(\Delta)$ est "terminating", tout diagramme peut être réduit en un diagramme normal. Ce diagramme normal est unique car $\mathcal{G}(\Delta)$ est confluent.

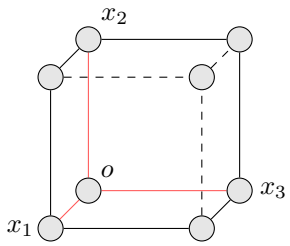
Nous pouvons maintenant prouver le théorème.
Preuve du théorème : Notons $\mathcal{C}_n$ le graphe de Cayley du groupe J_n.
Notons $\mathcal{SC}_n$ le complexe de Cayley de la présentation de J_n, c'est-à-dire le complexe cubique dont le 1-squelette est $\mathcal{C}_n$ et dont les carrés sont formés par les 4-cycles suivants : $\forall (p, q, m, r) \in \mathbb{N}^4$ tel que $1 \leqslant p < q \leqslant n$ et $1 \leqslant m < r \leqslant n$,

$$(1, s_{p,q}, s_{p,q}s_{m,r}, s_{p,q}s_{m,r}s_{p,q}, s_{p,q}s_{m,r}s_{p,q}s_{m,r} = 1) \text{ si } [p, q] \cap [m, r] = \emptyset$$

et

$$(1, s_{p,q}, s_{p,q}s_{m,r}, s_{p,q}s_{m,r}s_{p,q}, s_{p,q}s_{m,r}s_{p,q}s_{p+q-r,p+q-m} = 1) \text{ si } [m, r] \subset [p, q].$$

Les carrés de $\mathcal{SC}_n$ sont donc donnés par les relations vérifiées par les générateurs canoniques de J_n. Ainsi, $\mathcal{SC}_n$ est simplement connexe par définition. De plus, les carrés de $\mathcal{SC}_n$ sont "embedded" vu la proposition sur la forme normale des diagrammes (voir **[0]** pour plus de précisions).
Deux carrés distincts de $\mathcal{SC}_n$ ne peuvent pas partager deux arrêtes consécutives étant donné que les relations imposées aux générateurs canoniques de J_n contiennent deux générateurs à chaque fois.
Enfin, montrons que si o est un sommet de $\mathcal{C}_n$, et si x_1, x_2, x_3 sont trois voisins de o dans $\mathcal{C}_n$, si $[o, x_1], [o, x_2]$ et $[o, x_3]$ s'étendent en carrés par paires, alors ils s'étendent en le 2-squelette d'un 3-cube.



L'objectif est de prouver que les arrêtes pointillées sont en fait pleines.

Comme J_n agit transitivement sur l'ensemble des sommets de $\mathcal{C}_n$, on peut supposer sans perte de généralité que $o = 1$.
Pour $i \in \{1, 2, 3\}$, notons S_i l'intervalle "tressé" par x_i (le générateur par lequel on a multiplié 1 pour obtenir x_i s'écrit $s^i_{p,q}$ et on note $S_i = [p, q]$). Étant donné qu'on a supposé que les arrêtes s'étendent en carrés, les S_i sont disjoints ou imbriqués (on a imposé la forme des 4-cycles).
Pour $r \in \mathbb{N}$ tel que $r \leqslant 3$, et pour tout $1 \leqslant i_1 < \cdots < i_r \leqslant 3$, on note $x(i_1, \cdots, i_r)$ le diagramme obtenu en inversant les brins dans S_{i_1}, puis ceux dans S_{i_2}, et ainsi de suite. Quand $r = 0$, on obtient $o = 1$ et quand $r = 1$ avec $i_1 = i$, on obtient x_i. L'entier r représente la distance à $o = 1$. La bonne définition de $x(i_1, \cdots, i_r)$ résulte de la remarque que l'on a faite sur les S_i. De plus, les sommets du 3-cube que l'on cherche sont les $x(i_1, \cdots, i_r)$.
Finalement, par la première proposition de cette partie, le graphe $\mathcal{C}_n$ est médian.

Ne nous trompons pas sur les apparences, bien que ce théorème se situe à la fin de ce rapport, ce n'est que le début de l'histoire de la théorie géométrique des groupes. Les propriétés algébriques des groupes qui agissent sur des graphes médians sont riches et il faudrait bien plus de temps (et d'espace !) pour faire le tour du paysage (voir **[0]** et **[3]**).

3.2 Un mot sur le problème du mot dans les groupes de cactus

DÉFINITION Soit G un groupe de type fini. Le problème qui consiste à décider si deux mots en les générateurs de G représentent le même élément du groupe G est le **problème du mot**.

REMARQUE : C'est un problème algorithmique, l'objectif est donc de donner une solution explicite et avec la meilleure complexité possible.

Dans le cas des groupes de cactus, nous avons en fait déjà donné une solution au problème du mot pour prouver le théorème sur les graphes de Cayley des groupes de cactus. En effet, si $n \in \mathbb{N}$ est tel que $n \geqslant 2$, si x et y sont deux mots en les générateurs du groupe de cactus J_n, on peut former le diagramme représenté par xy^{-1}.
En faisant des réductions et des retournements pour faire monter des intervalles plus grands dans ce diagramme, on trouve la forme normale du diagramme de xy^{-1}. Si le diagramme sous forme normale obtenu ne contient aucun élément (si on obtient n lignes verticales), c'est que $x = y$. Par contre, si la forme normale contient au moins un intervalle, c'est que $x \neq y$. On a donc une méthode explicite. Est-elle efficace ?
Si on note $\text{long}(x)$ la longueur du mot x et $\text{long}(y)$ la longueur du mot y, on obtient un diagramme de départ de taille $m = \text{long}(x) + \text{long}(y)$. Dans le pire cas, notre diagramme contient des intervalles de taille croissante (le plus grand est tout en bas, et la taille décroit en montant) et on doit effectuer m retournements à la première étape, $m - 1$ à la deuxième et ainsi de suite. Au total, nous aurons effectué $m(m + 1)/2$ retournements, auxquels il faut ajouter $m/2$ réductions potentielles pour avoir une borne supérieure pour la complexité. Au final, la complexité de notre méthode est dans le pire cas en $O(m^2)$.

RÉFÉRENCES :

— **[0]** Anthony GENEVOIS, *Cactus groups from the viewpoint of geometric group theory*, 2022.
— **[1]** Josette CALAIS, *Éléments de théorie des groupes*, 1984.
— **[2]** Alain DEBREIL, *Groupes finis et treillis de leurs sous-groupes*, 2016.
— **[3]** Anthony GENEVOIS, *Algebraic properties of groups acting on median graphs*, 2023.