HAL
open science

Les nombres de Catalan et le groupe modulaire PSL2(Z)

Christelle Guichard

To cite this version:

Christelle Guichard. Les nombres de Catalan et le groupe modulaire PSL2(Z). Théorie des nombres [math.NT]. Université Grenoble Alpes, 2018. Français. NNT : 2018GREAM057 . tel-02024805

HAL Id: tel-02024805

https://theses.hal.science/tel-02024805

Submitted on 5 Jan 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Communauté UNIVERSITÉ Grenoble Alpes

THÈSE

Pour obtenir le grade de

DOCTEUR DE LA COMMUNAUTÉ UNIVERSITÉ GRENOBLE ALPES

Spécialité : Mathématiques

Arrêté ministériel : 25 mai 2016

Présentée par

Christelle GUICHARD

Thèse dirigée par **Gérard BESSON**,

préparée au sein du **Laboratoire Institut Fourier**
dans **l'École Doctorale Mathématiques, Sciences et technologies de l'information, Informatique**

Les nombres de Catalan et le groupe modulaire PSL2(Z)

Catalan Numbers and the modular group PSL2(Z).

Thèse soutenue publiquement le **29 octobre 2018**,
devant le jury composé de :

M. Gérard BESSON
Directeur de recherche, CNRS Délégation Alpes, Directeur de thèse

M. François DAHMANI
Professeur, Université Grenoble Alpes, Président

Mme Theresia EISENKÖLBL
Maître de conférence, Université de Lyon 1, Examinateur

Mme Tatiana SMIRNOVA-NAGNIBEDA
Professeur, Université de Genève - Suisse, Rapporteur

M. Jean-Christophe AVAL,
Chargé de recherche, Délégation CNRS Aquitaine, Rapporteur

Résumé :

Dans ce mémoire de thèse, on étudie le morphisme de monoïde μ du monoïde libre sur l'alphabet des entiers $\mathbb{N}$, à valeurs dans le groupe modulaire $PSL_2(\mathbb{Z})$, considéré comme monoïde, défini pour tout entier a par $\mu(a) = \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}$. Les nombres de Catalan apparaissent naturellement dans l'étude de sous-ensembles du noyau de μ.

Dans un premier temps, on met en évidence deux systèmes de réécriture, l'un sur l'alphabet fini $\{0,1\}$, l'autre sur l'alphabet infini des entiers $\mathbb{N}$ et on montre que ces deux systèmes de réécriture définissent des présentations de monoïde de $PSL_2(\mathbb{Z})$ par générateurs et relations. Par ailleurs, on introduit le morphisme d'indice associé à l'abélianisé du revêtement universel de $PSL_2(\mathbb{Z})$, le groupe B_3 des tresses à trois brins. Interprété dans deux contextes différents, le morphisme d'indice est associé au nombre de "demi-tours". Ensuite, dans les quatrième et cinquième parties, on dénombre des sous-ensembles du noyau de $\mu_{|\{0,1\}}$ et du noyau de μ, bigradués par la longueur et l'indice. La suite des nombres de Catalan et d'autres diagonales du triangle de Catalan interviennent simplement dans les résultats. Enfin, on présente l'origine géométrique de cette étude : on explicite le lien entre l'objectif premier de la thèse qui était l'étude des polygones convexes entiers d'aire minimale et notre intéret pour le monoïde engendré par ces matrices particulières de $PSL_2(\mathbb{Z})$.

Summary :

In this thesis, we study a morphism of monoïd μ between the free monoïd on the alphabet of integers $\mathbb{N}$ and the modular group $PSL_2(\mathbb{Z})$ considered as a monoïd, defined for all integer a by $\mu(a) = \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}$. The Catalan Numbers arised naturally in the study of subsets of the kernel of the morphism μ.

Firstly, we introduce two rewriting systems, one on the finite alphabet $\{0,1\}$, and the other on the infinite alphabet of integers $\mathbb{N}$. We proove that both of these rewriting systems defines a monoïd presentation of $PSL_2(\mathbb{Z})$ by generators and relations. On another note, we introduce the morphism of loop associated to the abelianised of the universal covering group of $PSL_2(\mathbb{Z})$, the group B_3 of braid group on 3 strands. In two different contexts, the morphism of loop is associated to the number of "half-turns". Then, in the fourth and the fifth parts, we numerate subsets of the kernel of $\mu_{|\{0,1\}}$ and of the kernel of μ, bi-graduated by the morphism of length and the morphism of loop. The sequences of Catalan numbers and other diagonals of the Catalan triangle come into the results. Lastly, we present the geometrical origin of this research : we detail the connection between our first aim, which was the study of convex integer polygones of minimal area, and our interest for the monoïd generated by these particular matrices of $PSL_2(\mathbb{Z})$.

À mes enfants,
Trystan et Kylian.

Remerciements :

Je voudrais en premier lieu remercier tous ceux qui en ont cru en mon projet de thèse. Je pense notament Jean-Louis Verger-Gaugry, qui m'a particulièrement encouragée et a guidé mes premiers pas dans le monde de la recherche, et à Gérard Besson qui a accepté d'être mon directeur de thèse.

Je suis très reconnaissante à Jean-Christophe Aval et Tatiana Smirnova-Nagnibeda de l'intérêt qu'ils ont porté à mes recherches et d'avoir accepté d'en être les rapporteurs. J'ai expressément apprécié leurs commentaires, qui s'accordent étonnement avec mon point de vue général des mathématiques.

Je suis honorée que Roland Bacher, François Dahmani et Theresia Eisenkölbl aient accepté d'être membres de mon jury. Je remercie spécialement Roland, pour nos diverses échanges, toujours pertinents et bienveillants, à l'orée de mes recherches, entre musique, nature, (...) et science.

Je remercie tous les membres de l'Institut Fourier et les membres du DSDA de Valence pour leur accueil, et tous ceux avec qui m'ont soutenu dans mes recherches et mes enseignements, m'ont écouté et conseillé, parfois seulement le temps d'un café et d'un carreau de chocolat : Aurore Akoka, Roland Bacher, Marc Buonomo, Marie-Cécile Darracq, Philippe Eyssidieux, Takuji Kashiwabara, Benjamin Lespets, Hélène Maugendre, Hervé Pajot, Pierre Will, ... J'ai beaucoup appris sur moi-même de chacun de nos échanges.

Je remercie mes amis et je pense tout particulièrement à Fabien, qui a toujours été présent aussi bien dans mes meilleurs moments que dans mes meilleures galères, et ce, malgré la distance. Je remercie mon très cher voisin Yannick, sans qui la fin de la rédaction de mon mémoire aurait été particulièrement compromise.

Enfin, je remercie ma famille pour son soutien ; un grand merci à mon frangin Nicolas, le meilleur geek selon moi, toujours disponible et réactif en cas de contre-temps informatique. Et un grand merci à mes parents, qui ont toujours été là pour moi tout en me laissant une grande liberté dans mes choix.

Ma dernière pensée est pour mes enfants, Trystan et Kylian, qui ont su parfois être bien plus patients que moi. Je suis heureuse de vous avoir à mes cotés et très fière.

Table des matières

Introduction **3**

I Présentation de monoïde et système de réécriture. **7**

1 Monoïde et morphisme de monoïde. 7
2 Monoïde quotient. 11
3 Système de réécriture et monoïde quotient. 14
4 Morphisme d'un monoïde quotient dans un monoïde. 15
5 Propriété des systèmes de réécriture. 16
6 Le monoïde quotient $B^*/\sim_B$ sur $B = \{0, 1\}$. 20
7 Le monoïde quotient $\Sigma^*/\sim_\Sigma$. 21
8 Un isomorphisme de monoïde entre $B^*/\sim_B$ et $\Sigma^*/\sim_\Sigma$. 23
9 Les formes réduites de $B^*/\sim_B$ et de $\Sigma^*/\sim_\Sigma$. 24
10 Réductions maximales sur Σ^* et sur B^*. 27

II Deux présentations de $PSL_2(\mathbb{Z})$ et leurs formes réduites. **29**

1 Remarques préliminaires sur $PSL_2(\mathbb{Z})$ 29
2 Définitions - Morphismes de monoïdes 31
3 Les monoïdes $\Sigma^*/\sim_\Sigma$ et $B^*/\sim_B$ sont isomorphes à $PSL_2(\mathbb{Z})$. 33

III Morphisme d'indice et demi-tour. **37**

1 Définition et partition d'une partie de B^* ou de Σ^*. 38
2 Demi-tour d'un vecteur de $\mathbb{R}^2$ par un mot du noyau de μ. 40
2.1 Définitions de θ_e. 40
2.2 Invariance sous l'expansion V. 42
2.3 Comportement de θ_e avec l'expansion H. 43
2.4 Démonstration du théorème III.12. 45
2.5 Remarques et compléments. 45
3 Indice et tour d'une tresse de B_3. 46
3.1 Définitions. 46

3.2 De $B^* = \{0,1\}^*$ vers B_3^+. 47
3.3 Extension du morphisme $\tilde{\mu}^{B_3}$ sur Σ^*. 49
3.4 Indice et abélianisé de B_3. 49

IV Modèle binaire : du noyau K_B vers les nombres de Catalan 53

1 Définitions préliminaires et représentations. 56
1.1 Châteaux et partition $(\mathcal{C}_k)_{k\in\frac{\mathbb{N}}{6}}$ de l'ensemble des châteaux. 56
1.2 Digression : chemins, nombres et mots de Schröder 58
1.3 Douves, Donjons, chemins. 61
1.4 Factorisation DD (donjons/douves) des châteaux 64
2 Dénombrement des châteaux 65
2.1 Dénombrement des donjons 65
2.2 Dénombrement des châteaux 71
3 Mots maximaux - Nombres de Catalan 75
3.1 Châteaux maximaux 76
3.2 Permutation circulaire sur le noyau K_B et arbres 3-réguliers. 80
3.3 Arbres 3-réguliers plans finis décorés 82
3.4 Les châteaux maximaux du noyau via les arbres $3-$réguliers 87
3.5 Les châteaux maximaux de $[0]_B$ et $[00]_B$. 89
4 Permutation circulaire sur un sous-monoïde 90
4.1 Sous-monoïde libre 90
4.2 Permutations circulaires 92
4.3 Action de $W-$permutation sur l'ensemble $K_B^{\max}$ des châteaux maximaux du noyau. 94
4.4 Permutation circulaire par la famille libre $W_1 = \{0,1\}$ 96
4.5 Permutation circulaire par la famille libre $W_{01^*} = \{01^k, k \geq 0\}$ 105
4.6 Permutation circulaire par la famille libre $W_{10^*} = \{10^k, k \geq 0\}$ 106
4.7 Permutation circulaire par $W_{1(00^*1)^*} = \{1(00^{k_1}1)(00^{k_2}1)\cdots(00^{k_n}1), n, k_i \geq 0\}$ 107

V Modèle entier : dénombrement de K_Σ. 109

1 Le sous-ensemble $K_{\frac{1}{2}}$ associé au demi-tour. 110
2 Réductions et Expansions sur K_Σ. 111
2.1 Définitions des réductions et expansions élémentaires. 111
2.2 Propriétés. 112
3 Réduction maximale canonique. 115
3.1 Minimum global et minimums locaux de $K_{\frac{k}{2}}$. 115
3.2 Réductions et expansions canonique. 117

4 Le sous-ensemble K_1 associé au tour. 119
4.1 Les mots de K_1 obtenus avec le minimum global 000000. 120
4.2 Les minimums locaux non maximaux de K_1. 122
4.3 Les mots de K_1 obtenus avec les minimums locaux. 124
4.4 Dénombrement des mots de K_1. 126

VI Origine géométrique de l'étude 129
1 Espace affine et groupe affine 129
1.1 $\mathbb{R}^2$ en tant qu'espace affine et groupe affine $GA(\mathbb{R}^2)$ 129
1.2 Repères affines du réseau $\mathbb{Z}^2$ et groupe spécial affine $SA(\mathbb{Z}^2)$. 131
2 Polygones convexes entiers - Aires minimales 132
3 Lignes brisées convexes entières localement minimales 133
4 Chaînages positifs de repères affines directs 135
4.1 Définition 135
4.2 Décomposition d'un chaînage 138
4.3 Structure de monoïde et morphismes sur le monoïde Σ_2^* 139
4.4 Indice combinatoire et demi-tour sur les bases directes de $\mathbb{Z}^2$. 141

VII Problèmes ouverts. 145
1 Les mots non maximaux du noyau de $\mu_{|B^*}$. 145
2 Les mots du noyau de μ d'indice > 1. 146
3 D'autres images réciproques ? 146
4 Généralisation aux tresses à n brins, $n \geq 4$. 146
5 Les polygones convexes minimaux. 147

Introduction

Les nombres de Catalan $\{1, 1, 2, 5, 14, 42, 132, \ldots\}$ définis par

$$c_n = \frac{1}{n}\binom{2n}{n-1}$$

interviennent de multiples façons en combinatoire énumérative. Entre autre, le n-ième nombre de Catalan c_n compte le nombre :

- de triangulations d'un polygone convexe à $n+2$ cotés.
- de plusieurs types d'arbres planaires
- de façons différentes de placer des parenthèses autour de $n+1$ facteurs.
- de mots de Dyck de longueur $2n$.

Dans son traité intitulé *Catalan Number*, Richard Peter Stanley propose au lecteur de prouver l'équivalence de 214 objets combinatoires dénombrés par la suite des nombres de Catalan.

Dans ce travail de recherche, les nombres de Catalan s'insèrent dans deux nouveaux contextes en lien avec le groupe modulaire $PSL_2(\mathbb{Z})$ et son revêtement universel, le groupe des tresses à trois brins B_3.

Plus précisément, on considère l'application de $\mathbb{N}$ dans $PSL_2(\mathbb{Z})$ définie par

$$\mu(a) = \pm\begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}.$$

On pose $\Sigma = \mathbb{N}$ et on note Σ^* le monoïde libre sur l'alphabet Σ. L'application μ se prolonge en un morphisme surjectif du monoïde libre Σ^* dans $PSL_2(\mathbb{Z})$ et se relève de façon naturelle en une application $\tilde{\mu}_{B_3} : \Sigma \to B_3$ du monoïde libre Σ^* dans un sous-monoïde du monoïde des tresses positives.

On étudie deux présentations de monoïde, l'une sur l'alphabet $\Sigma = \mathbb{N}$, muni d'une relation d'équivalence $\sim_\Sigma$ et l'autre sur l'alphabet $\{0, 1\} \subset \Sigma$, muni de la relation d'équivalence

$\sim_B$ induite par $\sim_\Sigma$. On montre que ces deux présentations sont isomorphes au quotient $B_3/C \simeq PSL_2(\mathbb{Z})$ du groupe de tresse par son centre C.

Par ailleurs, l'extension naturelle de l'application $a \mapsto \frac{1-a}{12}$ définit le morphisme d'indice Ind sur Σ^*. Il correspond à l'abélianisé $B_3/D(B_3)$ du groupe des tresses à trois brins.

$$\begin{tikzcd}
\frac{1}{12}\mathbb{Z} \simeq B_3^{ab} \arrow[rr, leftrightarrow] & & B_3 \arrow[d] \\
\Sigma^* \arrow[u, "Ind"] \arrow[urr, "\tilde{\mu}_{B_3}"] \arrow[rr, "\mu"'] \arrow[dr] & & PSL_2(\mathbb{Z}) \simeq B_3/C \\
& \Sigma^*/\sim_{\Sigma^*} \arrow[ur, hook, two heads] &
\end{tikzcd}$$

Les nombres de Catalan apparaîssent en regardant le noyau de l'application μ, muni d'une bigradation associée à la longueur et à l'abélianisé de B_3.

Ils interviennent également dans le noyau de $\mu_{|B^*}$ et dans les images réciproques de U et de U^2 par $\mu_{|B^*}$.

Dans une première partie sont mis en place les outils utiles pour l'étude, notamment sur les systèmes de réécriture et les présentations de monoïde. On introduit les deux monoïdes quotients particuliers, $B^*/\sim_B$ sur l'alphabet $B = \{0, 1\}$ et $\Sigma^*/\sim_\Sigma$ sur l'alphabet $\Sigma = \mathbb{N}$.

Dans une deuxième partie, on montre que les morphismes induits par $\mu_{|B^*}$ et μ sur les monoïdes quotients $B^*/\sim_B$ et $\Sigma^*/\sim_\Sigma$ sont bijectifs.

Dans la troisième partie, on montre que l'indice défini combinatoirement par

$$\begin{array}{rcccc} Ind & : & \Sigma^* & \longrightarrow & \frac{1}{12}\mathbb{Z} \\ & & w & \longmapsto & \frac{1}{12}(2\lambda(w) - \sigma(w)) \end{array}$$

où $\lambda(w)$ désigne la longueur n d'un mot $w = a_1 a_2 \cdots w_n$ et $\sigma(w) = \sum_{i=1}^{n} a_i$ sa somme, s'interprète comme le nombre de tours d'un mot de Σ dans deux contextes différents.

On montre que, dans le plan euclidien usuel $\mathbb{R}^2$, l'indice d'un mot $w = a_n a_{n-1} \cdots a_2 a_1$ du noyau de $\mu_{|B^*}$ correspond au nombre de tours qu'effectue une demi-droite dirigée par un vecteur de $\mathbb{R}^2$ par les applications linéaires successives $\begin{pmatrix} 0 & -1 \\ 1 & a_i + 1 \end{pmatrix}$.

Aussi, dans le contexte des tresses à trois brins, l'indice d'un mot du noyau de μ évalue

le nombre de tours de la tresse associée par le morphisme $\tilde{\mu}_{B_3}$ défini par

$$\tilde{\mu}_{B_3}(a) = \sigma_1 \sigma_2^{1-a} \text{ , pour tout entier } a,$$

où σ_1 et σ_2 sont les générateurs de B_3. De plus, on met en évidence la corrrespondance entre l'indice d'un mot et l'abélianisé de sa tresse associée.

Dans une quatrième partie, on se concentre sur le noyau K_B de $\mu_{|B^*} \subset B^*$ et sur l'ensemble $K_B^{\max}$ des mots du noyau, d'indice fixé et de longueur maximale.

En introduisant une factorisation unique dont les facteurs premiers sont des mots de l'image réciproque $\mu_{|B^*}^{-1}(\langle U \rangle)$ du sous-groupe cyclique d'ordre 3 de $PSL_2(\mathbb{Z})$ engendré par $U = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, on dénombre les mots du noyau K_B à longueur et indice fixés.

Puis, on étudie les mots de longueur maximale d'indice donné de $K_B^{\max}$. On explicite une bijection entre les mots du noyau d'indice $\frac{n}{2}$ à permutation cyclique près et les arbres $3-$réguliers à $2n$ sommets. En rajoutant une décoration sur ces arbres $3-$réguliers précisant le début du mot associé, on montre que le cardinal de l'ensemble des mots maximaux du noyau d'indice $\frac{n}{2}$ est donné par la somme $c_{n-1} + c_n$ de deux nombres de Catalan consécutifs.

Enfin, en considérant les classes d'équivalence des mots maximaux à permutation cyclique près, on détermine trois types de mots maximaux dans le noyau : les mots simples, les mots carrés (de la forme p^2) et les mots cubes (de la forme p^3). On dénombre ainsi les orbites des mots simples, carrés et cubes de $K_B^{\max}$. Le nombre total d'orbite correspond au nombre d'arbres $3-$réguliers non-enracinés, dénombrés par la suite référncée $A001683$ dans l'OEIS [Sl], initialement introduite par W.G.Brown dans un contexte d'énumération de triangulation du disque dans [B].

Dans la cinquième partie, sur l'alphabet des entiers $\Sigma = \mathbb{N}$, on vise à dénombrer les mots du noyau $K_\Sigma \Sigma^*$ de μ, à indice et longueur fixés.

En particulier, on montre que l'ensemble des mots de longueurs $k+2$ d'indice $\frac{1}{2}$ est dénombré par la suite des nombres de Catalan $(c_k)_{k \geq 1}$.

Dans la sixième partie, on présente l'origine géométrique de cette étude. Initialement, on s'est interessé aux polygones convexes entiers à n sommets d'aire minimale. Ce problème est résolu pour seulement quelques petites valeurs de n. C'est dans ce contexe, en paramétrant un polygone d'aire minimale par un mot de longueur paire sur l'alphabet entier $\Sigma = \mathbb{N}$ qu'ont émergé les matrices de la forme $\begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}$, dans un premier temps dans $SL_2(\mathbb{Z})$.

Puis dans un second temps, on a étudié le noyau du morphisme $\mu : \Sigma^* \to PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\}$. Les mots du noyau de $\tilde{\mu} : \Sigma^* \to SL_2(\mathbb{Z})$ sont alors les mots du noyau de $\mu : \Sigma^* \to PL_2(\mathbb{Z})$ d'indice entier.

Enfin, la dernière partie contient quelques questions qui émanent de cette étude.

Chapitre I

Présentation de monoïde et système de réécriture.

1 Monoïde et morphisme de monoïde.

Définition I.1 *Un monoïde* $(\mathcal{M}, *, e)$ *est un ensemble* $\mathcal{M}$ *muni d'un produit associatif* $*$ *admettant un élément neutre* e *bilatéral.*

Exemple I.2

- *L'ensemble des entiers naturels* $(\mathbb{N}, +, 0)$ *est un monoïde (commutatif).*
- *L'ensemble des entiers pairs* $2\mathbb{N}$ *muni de la multiplication n'est pas un monoïde; il n'admet pas d'élément neutre.*
- *Un groupe* $(G, \times, e)$ *est un monoïde dont tous les éléments admettent un inverse à droite et un inverse à gauche.*

  En effet, si pour tout $x \in G$*, il existe* $d, g \in G$ *tel que* $xd = e$ *et* $gx = e$*, alors* $g = g(xd) = (gx)d = d$*. L'inverse à droite* d *et l'inverse à gauche* g *sont égaux. Donc l'élément* x *est inversible, d'inverse* $x^{-1} = d = g$*.*

Définition I.3 *Un morphisme de monoïde d'un monoïde* $(\mathcal{M}_1, *_1, e_1)$ *vers un monoïde* $(\mathcal{M}_2, *_2, e_2)$ *est une application* φ *de* $\mathcal{M}_1$ *vers* $\mathcal{M}_2$ *telle que*

- $\varphi(e_1) = e_2$.
- *pour tous* x, y *de* $\mathcal{M}_1$*, on a :* $\varphi(x *_1 y) = \varphi(x) *_2 \varphi(y)$

Définition I.4 *Un alphabet est un ensemble dont les éléments s'appellent les lettres.*

Définition I.5 *Le monoïde libre* Σ^* *sur un alphabet* Σ *est l'ensemble des mots finis composés*

de lettres de Σ. La loi interne est la concaténation

$$\begin{array}{rcccc} * & : & \Sigma^* \times \Sigma^* & \to & \Sigma^* \\ & & (w_1, w_2) & \mapsto & w_1 * w_2 = w_1 w_2 \end{array}$$

et l'élément neutre est le mot vide $\emptyset$.

Tout élément du monoïde libre Σ^* s'écrit de façon unique sur l'alphabet Σ.

Proposition I.6 *L'ensemble des morphismes d'un monoïde libre Σ^* sur un alphabet Σ vers un monoïde $(\mathcal{M}, *, e)$ est en bijection avec les applications de l'alphabet Σ dans le monoïde $(\mathcal{M}, *, e)$.*

L'extension naturelle d'une application $\varphi : \Sigma \to \mathcal{M}$ est l'unique morphisme de monoïde défini par :

$$\begin{array}{rccc} \varphi^* : & \Sigma^* & \longrightarrow & \mathcal{M} \\ & \emptyset & \longmapsto & e, \\ & a_1 \cdot a_2 \cdots a_n & \longmapsto & \varphi^*(a_1 \cdot a_2 \cdots a_n), = \varphi(a_1) * \varphi(a_2) * \cdots * \varphi(a_n). \end{array}$$

Preuve : Étant donné un mot w non vide du monoïde libre Σ^*, il s'écrit de façon unique sur l'alphabet Σ sous la forme $a_1 a_2 \cdots a_n$ où a_i sont des lettres de Σ. Le morphisme de monoïde φ^* coïncide avec φ sur Σ et on a : $\varphi^*(a_1 \cdot a_2 \cdots a_n) = \varphi^*(a_1) * \varphi^*(a_2) * \cdots * \varphi^*(a_n) = \varphi(a_1) * \cdots * \varphi(a_n)$. Ainsi, le morphisme φ^* est défini de manière unique sur Σ^*.

□

Pour simplifier, on notera $\varphi^* = \varphi$.

Exemple I.7 *Soit Σ un alphabet.*

- *Le morphisme longueur λ est l'extension naturelle de l'application constante $\Sigma \to \{1\} \subset \{\mathbb{N}, +, 0)$. Il est défini sur Σ^* par :*

$$\begin{array}{rccc} \lambda : & (\Sigma^*, \cdot, \emptyset) & \longrightarrow & (\mathbb{N}, +, 0), \\ & a_1 \cdot a_2 \cdots a_n & \longmapsto & \lambda(a_1 \cdot a_2 \cdots a_n) = n. \end{array}$$

- *Si l'alphabet Σ est un sous-ensemble d'un monoïde $(\mathcal{M}, *, e)$, l'extension naturelle de l'application identité sur Σ est le morphisme associé à la loi $*$:*

$$\begin{array}{rccc} \sigma : & (\Sigma^*, \cdot, \emptyset) & \to & (\mathcal{M}, *, e) \\ & w = a_1 \cdot a_2 \cdots a_n & \mapsto & \sigma(w) = a_1 * a_2 * \cdots * a_n. \end{array}$$

Dans le cas particulier où $\Sigma \subset (\mathbb{N}, +, 0)$, le morphisme σ est le morphisme "somme".

Pour $\Sigma = \{0,1\} \subset (\mathbb{N},+,0)$, l'extension naturelle de l'identité est le morphisme qui compte le nombre de 1 dans l'écriture d'un mot de $\{0,1\}^*$. Il est clair qu'il coïncide avec le morphisme "somme" par unicité de l'extension naturelle (voir proposition (I.6)).

- *Soit $(A,(+,0),(\times,1))$ un anneau commutatif unitaire. On se place dans le groupe quotient $PSL_2(A) = SL_2(A)/\{\pm I_2\}$ (muni du produit matriciel usuel et de l'élément neutre $I = \pm I_2$), considéré comme monoïde. Étant donné une matrice M de $SL_2(\mathbb{A})$, on note $\pm M$ sa classe d'équivalence dans $PSL_2(A)$.*

  Pour toute partie B de A, l'alphabet $P = \{\pm \begin{pmatrix} 0 & -1 \\ 1 & b+1 \end{pmatrix}, b \in B\}$, composé d'éléments du monoïde $(PSL_2(A),\cdot,\pm I_2)$ est en bijection avec le sous-ensemble B. L'extension naturelle de l'application $b \mapsto \pm \begin{pmatrix} 0 & -1 \\ 1 & b+1 \end{pmatrix}$ correspond au produit matriciel :

$$\begin{array}{rcl} \mu : (B^*,\cdot,\emptyset) \simeq (P^*,\cdot,\emptyset) & \longrightarrow & (PSL_2(\mathbb{Z}),\cdot,\pm I_2) \\ b_1 \cdots b_n & \longmapsto & \mu(b_1)\mu(b_2)\cdots\mu(b_n) = \pm \begin{pmatrix} 0 & -1 \\ 1 & b_1+1 \end{pmatrix} \cdots \begin{pmatrix} 0 & -1 \\ 1 & b_n+1 \end{pmatrix}. \end{array}$$

  On étudie ce morphisme μ dans la suite pour $B = \mathbb{N} \subset A = \mathbb{Z}$ (voir chapitre II).

Remarque I.8

- *L'ensemble des monoïdes forme une catégorie, notée $\mathcal{M}on$, dont les objets sont les monoïdes et les flèches sont les morphismes de monoïdes.*

  De même, l'ensemble des groupes forme une catégorie, notée $\mathcal{G}rp$, dont les objets sont les groupes et les flêches sont les morphismes de groupes.

- *Tout groupe peut être considéré comme un monoïde en "oubliant" les propriétés sur les inverses. On définit le foncteur d'oubli $M : \mathcal{G}rp \to \mathcal{M}on$ qui à tout groupe, associe le monoïde correspondant.*

  Étant donné un monoïde $(\mathcal{M},*,e)$, on note $I(\mathcal{M})$ l'ensemble des éléments inversibles à gauche et à droite de $\mathcal{M}$. Alors $I(M)$ forme un groupe. On dit que I est un foncteur de $\mathcal{M}on$ dans $\mathcal{G}rp$. C'est l'adjoint à droite du foncteur M :

$$\begin{tikzcd} \mathcal{G}rp \arrow[r] & \mathcal{M}on \arrow[r] & \mathcal{G}rp \\ (G,\times,e) \arrow[r, mapsto, "M"] \arrow[rr, bend right, "Id"'] & (G,\times,e) \arrow[r, mapsto, "I"] & (G,\times,e) \end{tikzcd}$$

  On a évidemment $I(M(G))) = G$ pour tout groupe G.

- *Dans le cas où $(\mathcal{M},\cdot,e)$ est un monoïde engendré par des générateurs inversibles, tous ses éléments sont inversibles et le monoïde $\mathcal{M}$ peut être considéré comme étant un*

groupe : $I(\mathcal{M}) = \mathcal{M}$. *En effet, si pour tout générateur* $g_i \in \mathcal{M}$, *il existe* $g_i^{-1} \in \mathcal{M}$ *tel que* $g_i g_i^{-1} = g_i^{-1} g_i = e$, *alors tout élément* w *du monoïde s'écrit sous forme d'un produit de générateurs* $w = g_1 \cdot g_2 \cdots g_n$ *et son inverse dans* $\mathcal{M}$ *est* $w^{-1} = g_n^{-1} \cdots g_2^{-1} \cdot g_1^{-1}$.

En particulier, tout monoïde engendré par des éléments d'ordre fini est un groupe.

2 Monoïde quotient.

Définition I.9

Une relation binaire R sur un ensemble E est une partie G de $E \times E$. Pour tout $(x, y) \in G$, on dit que x est en relation avec y et l'on note xRy.

La relation inverse R^{-1} d'une relation binaire R est l'ensemble des couples (y, x) tels que xRy.

Pour tout entier $k > 0$, on note R^k la relation binaire définie par $(xR^k y) \Leftrightarrow$ (il existe $x_0 = x, x_1, \ldots, x_k = y$ tels que $x_0 R x_1$, $x_1 R x_2$, $\ldots$, $x_{k-1} R x_k$).

Par convention, la relation binaire R^0 est la diagonale de $E \times E$.

Une relation d'équivalence $\sim$ sur un ensemble E est une relation binaire réflexive ($\forall x \in E$, $x \sim x$), symétrique ($\forall x$, $y \in E$, $x \sim y \Rightarrow y \sim x$), et transitive ($\forall x$, y, $z \in E$, $x \sim y$ et $y \sim z$ $\Rightarrow x \sim z$).

La relation d'équivalence $\sim_R$ (ou simplement $\sim$) engendrée par une relation binaire R sur un ensemble E, est la clôture réflexive et transitive de la relation symétrique $R \cup R^{-1}$: c'est $\bigcup_{k \geq 0} (R \cup R^{-1})^k$.

Exemple I.10 *Pour tout entier n, la relation inverse de la relation binaire sur $\mathbb{N}$ définie par $(xRy \Leftrightarrow y = x + n)$ est la relation binaire sur $\mathbb{N}$ définie par $(xR^{-1}y \Leftrightarrow y = x - n)$. La relation d'équivalence engendrée par cette relation binaire est la congruence modulo n, notée $\equiv_n$.*

Définition I.11 *Soit $\sim$ une relation d'équivalence sur un ensemble E.*

La classe d'équivalence $[x]_\sim$ (ou simplement $[x]$) d'un élément x de E est l'ensemble des éléments de E en relation avec x :

$$[x] = \{y \in E \mid x \sim y\}.$$

Un représentant de $[x]$ est un élément de la classe d'équivalence de x.

L'ensemble des classes d'équivalence de E forme une partition de E.

L'ensemble quotient de E par la relation R, noté E/R ou $E/\sim$, est le sous-ensemble des parties $\mathcal{P}(E)$ de E formé des classes d'équivalence :

$$E/\sim = E/R = \{[x] \in \mathcal{P}(E) \mid x \in E\}.$$

Étant donnée une famille de représentants $(x_i)_{i \in I}$ qui contient exactement un représentant par classe d'équivalence, on a $E/R \simeq (x_i)_{i \in I}$.

Exemple I.12 *La relation de congruence modulo 2, notée $\equiv_2$, partitionne l'ensemble des entiers en 2 classes d'équivalence : l'ensemble des entiers pairs et l'ensemble des entiers*

impairs. On représente canoniquement ces deux classes par leur plus petit élément 0 *et* 1. *Ainsi, l'ensemble quotient est* $\mathbb{N}/\equiv_2 \simeq \{[0];[1]\}$.

Proposition I.13 *La projection canonique* π *de* E *dans l'ensemble quotient* E/R, *qui à tout élément de* E *associe sa classe d'équivalence* $[x]_{\sim_R}$ *:*

$$\begin{array}{rccc} \pi : & E & \to & E/R \\ & x & \mapsto & [x] \end{array}$$

est surjective.

Preuve : Par construction, E/R est l'image de l'application $x \mapsto [x]$ dans $\mathcal{P}(E)$.

□

Définition I.14 *Soient* E *et* F *deux ensembles.*

Une relation binaire R *sur* E *est compatible avec une application* $f : E \to F$ *si et seulement si pour tous* x, y *de* E, *on a :*

$$xRy \Rightarrow f(x) = f(y).$$

Exemple I.15

- *La relation binaire* R_h *définie sur* $\{0,1\}^*$ *par* $(wR_hw' \Leftrightarrow (w = p000s$ *et* $w' = ps))$ *n'est pas compatible avec le morphisme longueur* $\lambda : B^* \to \mathbb{N}$ *car si* wR_hw' *alors* $\lambda(w') = \lambda(w) - 3 \neq \lambda(w)$.

  La relation binaire R_h *est compatible avec le morphisme somme* $\sigma : B^* \to \mathbb{N}$ *car si* wR_hw' *alors* $\sigma(w') = \sigma(p) + \sigma(s) = \sigma(w)$, *avec* $w = p000s$ *et* $w' = ps$.
- *La relation binaire* R_v *définie sur* $\{0,1\}^*$ *par* $(wR_vw' \Leftrightarrow (w = p101s$ *et* $w' = p00s))$ *n'est pas compatible avec les morphismes longueur et somme. En effet, si* wR_vw', *alors* $\lambda(w') = \lambda(w) - 1 \neq \lambda(w)$ *et* $\sigma(w') = \sigma(w) - 2 \neq \sigma(w)$.

Proposition I.16

Soient E *et* F *deux ensembles et* $\sim$ *une relation d'équivalence sur* E *compatible avec une application* $f : E \to F$. *Il existe une unique application* $\tilde{f} : E/\sim \to F$ *telle que* $f = \tilde{f} \circ p$ *:*

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "p"'] & F. \\ E/\sim \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

On dit que l'application f *passe au quotient* $E/\sim$.

Définition I.17 *Une relation d'équivalence $\sim$ sur un monoïde $(\mathcal{M}, *, e)$ est compatible avec la loi interne $*$ si pour tous éléments x, x', y et y' de $\mathcal{M}$, on a : $x \sim x'$ et $y \sim y' \Rightarrow x * y \sim x' * y'$.*

Exemple I.18 *On considère le monoïde $(\mathbb{Z}/4\mathbb{Z}, +, [0]_4)$.*

La relation d'équivalence $\sim_1$ engendrée par la relation $R_1 = \{(0,1),(2,3)\}$ n'est pas compatible avec la loi $+$.

La relation d'équivalence $\sim_2$ engendrée par la relation $R_2 = \{(0,2),(1,3)\}$ est compatible avec la loi de $\mathbb{Z}/4\mathbb{Z}$ et on a $(\mathbb{Z}/4\mathbb{Z})/\sim_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Proposition I.19 *Soit $\sim$ une relation d'équivalence sur un monoïde $(\mathcal{M}, *, e)$ compatible avec la loi $*$ de $\mathcal{M}$. La loi $*$ induit une unique loi $\star$ sur le quotient $\mathcal{M}/\sim$ telle que pour tout x, y de $\mathcal{M}$, on a :*

$$[x] \star [y] = [x * y].$$

L'ensemble quotient $\mathcal{M}/\sim$ muni de la loi induite $\star$ et de l'élément neutre $[e]$ est un monoïde.

On dit que $(\mathcal{M}/\sim, \star, [e])$ est le monoïde quotient.

Remarque I.20 *La projection canonique $\pi : \mathcal{M} \to \mathcal{M}/\sim$ est alors un morphisme de monoïde.*

Exemple I.21 *L'addition du monoïde $(\mathbb{N}, +, 0)$ est compatible avec la relation de congruence modulo n pour tout $n \geq 0$. Le monoïde quotient induit $(\mathbb{N}/\equiv_n, \star, [0])$ est isomorphe au monoïde $(\mathbb{Z}/n\mathbb{Z}, +, 0)$.*

Définition I.22 *Une présentation d'un monoïde $(\mathcal{M}, *, e)$ est la donnée d'un ensemble de générateurs $G \subset \mathcal{M}$ de $\mathcal{M}$ et d'une relation binaire R sur les générateurs, compatible avec la concaténation dans G^*, telle que le morphisme de G^* dans $\mathcal{M}$ associé à l'inclusion $G \subset \mathcal{M}$ passe au quotient et induit un isomorphisme entre G^*/R et $\mathcal{M}$:*

$$\begin{tikzcd} G^* \arrow[r, "Id"] \arrow[d, "p"'] & \mathcal{M}. \\ G^*/R \arrow[ur, "\simeq"'] & \end{tikzcd}$$

Une présentation de monoïde est notée $\langle G|R\rangle$, et on a : $\langle G|R\rangle \simeq G^*/R \simeq \mathcal{M}$.

Exemple I.23 *La relation R définie par $(xRy \Leftrightarrow y = x + 2)$ engendre la relation de congruence $\equiv_2$ modulo 2. Le monoïde quotient $(\mathbb{N}/\equiv_2, \star, [0])$ admet la présentation de monoïde $\langle \mathbb{N}|\equiv_2\rangle$ ou $\langle \mathbb{N}|R\rangle$.*

Deux autres exemples de monoïdes quotients décrits par une présentation de monoïde sont étudiés dans les sections (6) et (7) de ce chapitre.

3 Système de réécriture et monoïde quotient.

Définition I.24

Un mot w' est un facteur d'un mot w s'il existe deux mots w_1 et w_2 tels que $w = w_1 \cdot w' \cdot w_2$.

Un facteur w' de w est un préfixe si $w_1 = \emptyset$ et est un suffixe si $w_2 = \emptyset$.

Un facteur w' de w est un préfixe strict si $w_1 = \emptyset$ et $w_2 \neq \emptyset$ et est un suffixe strict si $w_2 = \emptyset$ et $w_1 \neq \emptyset$.

Définition I.25

Un système de réécriture est la donnée d'un alphabet Σ et d'un ensemble de règles d'écriture $(r_i)_{i \in I}$ de la forme $r_i : w_i \to t_i$, pour i dans un ensemble I, où w_i et t_i sont des mots du monoïde libre Σ^*.

Une règle $r : w \to t$ s'applique à un mot W de Σ^* si le mot w est un facteur de W. Ainsi, le mot W est de la forme $W = pws$ et il se réécrit $W' = pts$ et on note $W \to_R W'$ ou simplement $W \to W'$.

Ce système de réécriture est également noté $\langle \Sigma | r_i, i \in I \rangle$, $(\Sigma, \to)$ ou $\langle \Sigma | R \rangle$ avec $R = (r_i)_{i \in I}$.

Définition I.26

Soit $(\Sigma | \to)$ un système de réécriture.

- *On note $\to^k$ le $k-$ième itéré de la règle de réécriture $\to$. On a donc $w \to^k w'$ s'il existe une suite de $k+1$ mots $x_0 = w, x_1, \ldots, x_k = w'$ telle que $x_0 \to x_1 \to x_2 \to \cdots \to x_k$. Par convention $\to^0$ est la relation reflexive identité.*
- *On note $\to^*$ la relation binaire $\bigcup_{k \in \mathbb{N}} \to^k$.*

  La relation $\to^*$ est la clôture réflexive transitive de $\to$.
- *On note $\to^{-1}$ la relation inverse de $\to$ telle que $(w \to^{-1} w') \Leftrightarrow (w' \to w)$.*
- *On note $\leftrightarrow$ la relation binaire $(\to) \cup (\to^{-1})$: si $w \leftrightarrow w'$ alors $w \to w'$ ou $w' \to w$.*
- *On note $\leftrightarrow^*$, ou $\sim_{\to}$, ou simplement $\sim$, la relation d'équivalence engendrée par $\to$: si $w \leftrightarrow^* w'$ alors il existe une suite finie de mots $x_0 = w, x_1, \ldots, x_k = w'$ telle que $x_0 \leftrightarrow x_1 \leftrightarrow \cdots \leftrightarrow x_k$.*

Proposition I.27 *Un système de réécriture $\langle \Sigma | w_i \to t_i, i \in I \rangle$ définit une présentation de monoïde par générateurs et relations du monoïde quotient $(\Sigma^* / \sim, \cdot, \emptyset)$ où $\sim$ est la relation*

d'équivalence engendrée par la relation binaire

$$R = ((pw_i s, pt_i s), p, s \in \Sigma^*, i \in I) \subset \Sigma^* \times \Sigma^*$$

et la loi $\cdot$ est la loi induite sur le quotient.

Preuve : Il est clair que pour tous mots w, w', x, x' de Σ^*, si $\begin{cases} w \sim w' \\ x \sim x' \end{cases}$ alors $wx \sim w'x'$.

Donc la relation d'équivalence $\sim$ engendrée par R est compatible avec la loi de concatenation. Ainsi, $\langle \Sigma | R \rangle$ est une présentation par générateurs et relations du monoïde quotient $(\Sigma^*/\sim, \cdot, \emptyset)$ (voir proprosition (I.19)).

□

Exemple I.28

1. *Le groupe modulaire $PSL_2(\mathbb{Z})$ considéré comme monoïde, admet la présentation $\langle \{s,t\} | s^2 \to \emptyset, t^3 \to \emptyset \rangle$ (aussi noté par la présentation de groupe $\langle \{s,t\} | s^2, t^3 \rangle$). Il est étudié dans le chapitre (II).*
2. *Le monoïde quotient $B^*/\sim_B$ défini par le système de réécriture $\langle \{0,1\} | 000 \to \emptyset, 101 \to 00 \rangle$ est étudié dans la partie (6) de ce chapitre.*
3. *Le monoïde quotient $\Sigma^*/\sim_\Sigma$ défini par le système de réécriture $\langle \mathbb{N} | 000 \to \emptyset, a00b \to (a+b), (a+1)0(b+1) \to ab \rangle$ est étudié dans la partie (7) de ce chapitre.*

4 Morphisme d'un monoïde quotient dans un monoïde.

Proposition I.29 *Soit Σ un ensemble et $\mathcal{M}$ un monoïde. La relation d'équivalence $\sim$ engendrée par les règles d'un système de réécriture $\langle \Sigma | w_i \to t_i, i \in I \rangle$ est compatible avec l'extension naturelle f d'une application de Σ dans $\mathcal{M}$ si et seulement si pour tout $i \in I$, on a : $f(w_i) = f(t_i)$.*

Dans ce cas, l'extension naturelle $f : \Sigma^* \to \mathcal{M}$ passe au quotient $\Sigma^*/\sim = \langle \Sigma | w_i \to t_i, i \in I \rangle$: il existe un unique morphisme de monoïde $\hat{f}$ tel que

$$\begin{tikzcd} \Sigma^* \arrow[r, "f"] \arrow[d, "\pi"'] & \mathcal{M}. \\ \langle \Sigma / w_i \to t_i, i \in I \rangle \arrow[ur, "\hat{f}"'] & \end{tikzcd}$$

Preuve :

D'après la proposition (I.27), la relation d'équivalence $\sim$ engendrée par les règles de réécriture est compatible avec la loi de concatenation du monoïde libre Σ^* et le système de réécriture est une présentation du monoïde quotient $(\Sigma^*/\sim, \cdot, [\emptyset])$.

De plus, l'extension naturelle f est un morphisme de monoïde (voir proposition (I.6)), donc pour tous mots u, v tels que $u \sim v$, on a $f(u) = f(v)$.

Donc la relation d'équivalence $\sim$ est compatible avec l'extension f. Le morphisme f passe au quotient $\Sigma^*/\sim$ (voir proposition (I.19)).

Réciproquement, une fonction f qui passe au quotient vérifie $f(w_i) = f(t_i)$ pour tout $i \in I$.

□

5 Propriété des systèmes de réécriture.

Définition I.30

- *Un mot réduit (ou irréductible) d'un système de réécriture $\langle \Sigma | w_i \to t_i, i \in I \rangle$ est un mot de Σ^* qui ne contient pas de facteur dans l'ensemble $(w_i)_{i \in I}$.*
- *Un système de réécriture se termine s'il n'existe aucune suite infinie de mots $(x_n)_n$ telle que pour tout $i \in \mathbb{N}$, $x_i \to x_{i+1}$.*

Exemple I.31 *Pour les trois exemples suivants, on se place sur l'alphabet $\{a, b\}$.*

1. *Le système de réécriture $\langle \{a, b\} | a \to b \rangle$ se termine. En effet, étant donné un mot comportant des lettres a et b, on remplace les lettres a par des lettres b. Lorsqu'on obtient un mot qui ne contient que des lettres b, la règle de réduction ne s'applique plus. Il est alors écrit sous forme réduite. Le système de réécriture se termine dans l'ensemble $\{b\}^*$.*
2. *Le système de réécriture $\langle \{a, b\} | a \to b, b \to a \rangle$ ne se termine pas car il contient le cycle infini $\cdots \to a \to b \to a \to b \to \cdots$ (Le graphe associé au système de réécriture de la façon évidente possède une boucle).*
3. *Le système de réécriture $\langle \{a, b\} | a \to a^2 \rangle$ ne se termine pas, il possède des chaînes infinies. Par exemple : $a \to a^2 \to a^3 \to a^4 \to \cdots$*

Proposition I.32 *Tout mot w d'un monoïde quotient $\Sigma^*/\sim_R$ défini par un système de réécriture $\langle \Sigma | \to \rangle$ qui se termine admet au moins une forme réduite w_r telle que $w \to^* w_r$.*

Définition I.33 *Un bon ordre $<$ sur un ensemble X est une relation d'ordre pour laquelle tout sous-ensemble non vide de X admet un plus petit élément.*

Exemple I.34 *La relation d'ordre usuelle $<$ sur l'ensemble des entiers naturels $\mathbb{N}$ est un bon ordre.*

Définition I.35

Une relation d'ordre est bien fondée sur un ensemble s'il n'existe pas de suite infinie strictement décroissante.

Une relation d'ordre $<$ sur un ensemble X est totale si pour tous éléments $x \neq y$ de X, on a $x < y$ ou $y < x$.

Remarque I.36 *Tout bon ordre définit une relation d'ordre bien fondée.*

Une relation d'ordre bien fondée est un bon ordre si et seulement si c'est une relation d'ordre totale.

Définition I.37 *Un ordre $<$ sur un monoïde libre Σ^* est compatible avec la loi de concaténation si pour tous mots x, y, p, s de Σ^*, si $x < y$ alors $pxs < pys$.*

Exemple I.38

- *La relation d'ordre $<$ usuelle sur l'ensemble des entiers relatifs $\mathbb{Z}$ n'est pas un bon ordre car elle n'est pas bien fondée.*
- *La relation R définie sur $\mathbb{Z}$ par xRy si et seulement si $|x| < |y|$ est bien fondée. Mais ce n'est pas un ordre total : par exemple, les entiers -2 et 2 ne sont pas ordonnés.*
- *La longueur d'un mot sur un monoïde libre définit une relation d'ordre bien fondée compatible avec la loi de concaténation.*

  Si l'alphabet admet au moins deux lettres a et b, ce n'est pas un bon ordre car il n'est pas total. Par exemple, les mots a^2 et ab ne sont pas strictement ordonnés.

Proposition I.39 *Un système de réécriture $\langle \Sigma | w_i \to t_i, i \in I \rangle$ se termine s'il existe un ordre bien fondé $<$ sur le monoïde libre Σ^* compatible avec la loi de concaténation, tel que $t_i < w_i$ pour toute règle de réécriture $(w_i \to t_i)$.*

Preuve : On suppose que le système de réécriture ne se termine pas. Alors il existe une suite infinie $(x_n)_n$ telle que pour tout $n \in \mathbb{N}$, $x_n \to x_{n+1}$. Comme la relation d'ordre est compatible avec la loi de concaténation, pour tout $n \in \mathbb{N}$, on a $x_{n+1} < x_n$. Impossible car $<$ est un ordre bien fondé.

□

Exemple I.40 *L'ordre défini par la longueur d'un mot λ sur le monoïde libre $\{a, b\}^*$ est bien fondé : un mot w' est plus petit qu'un mot w si et seulement si $\lambda(w') < \lambda(w)$.*

Comme $\lambda(a) < \lambda(ab)$ et $\lambda(b) < \lambda(ba)$, le système de réécriture $\langle \{a, b\} | ab \to a, ba \to b \rangle$ se termine, généralement pas de façon unique : le mot aba par exemple admet deux mots réduits a^2 et a.

Définition I.41

- *Un système de réécriture est confluent si pour tous mots w, x_1 et x_2 tels que* $\begin{tikzcd} & x_1 \\ w \arrow[ur, "*"] \arrow[dr, "*"'] & \\ & x_2 \end{tikzcd}$ *, il existe un mot t tel que* $\begin{tikzcd} x_1 \arrow[dr, "*"] & \\ & t \\ x_2 \arrow[ur, "*"'] & \end{tikzcd}$.
- *Un système de réécriture vérifie la propriété de Church-Rosser si pour tout couple de mots (w, w') tel que $w \sim_R w'$, il existe un mot t tel que* $\begin{tikzcd} w \arrow[dr, "*"] & \\ & t \\ w' \arrow[ur, "*"'] & \end{tikzcd}$.

Exemple I.42

- *Le système de réécriture $\langle \{a, b\} | a \to b \rangle$ du premier exemple de (I.31) est confluent : l'unique forme réduite d'un mot de longueur n est b^n.*
- *Le système de réécriture $\langle \{a, b\} | a \to b, a^2 \to a \rangle$ n'est pas confluent. Le mot a^2 admet deux formes réduites distinctes : b et b^2.*
- *Le système de réécriture $\langle \{a, b, c, d\} | ab \to c, ba \to d, c \to ab, d \to ba \rangle$ est confluent mais ne se termine pas. Pour tout mot comportant les facteurs ab et ba, il existe au moins deux réductions distinctes. Il est toujours possible de le réécrire sous sa forme initiale.*

Proposition I.43 *Un système de réécriture est confluent si et seulement s'il vérifie la propriété de Church-Rosser.*

Preuve :

On suppose que le système de réécriture est confluent. On considère deux mots w, w' tels que $w \sim_r w'$: il existe une suite finie $(x_i)_{1 \leq i \leq n}$ telle que $w = x_1 \leftrightarrow x_2 \leftrightarrow \cdots \leftrightarrow x_n = w'$.

On montre par récurrence sur n qu'il existe un mot t tel que $x_i \to^* t$ pour tout $1 \leq i \leq n$.

Pour $n = 2$, on a $x_1 \leftrightarrow x_2$. Donc soit $\begin{tikzcd} & x_1 \\ x_1 \arrow[ur, "*"] \arrow[dr] & \\ & x_2 \end{tikzcd}$, soit $\begin{tikzcd} & x_1 \\ x_2 \arrow[ur] \arrow[dr, "*"'] & \\ & x_2 \end{tikzcd}$. Dans les deux cas, la confluence implique qu'il existe un mot t tel que $\begin{tikzcd} x_1 \arrow[dr, "*"] & \\ & t \\ x_2 \arrow[ur, "*"'] & \end{tikzcd}$.

Pour $n \geq 3$, par récurrence, il existe un mot t' tel que $\begin{tikzcd} x_1 \arrow[dr, "*"] & \\ x_2 \arrow[dr, "*"] & \\ \vdots \arrow[dr, "*"] & \\ x_{n-2} \arrow[dr, "*"] & t' \\ x_{n-1} \arrow[ur, "*"'] & \end{tikzcd}$.

Ainsi, si $x_n \to x_{n-1}$, alors on pose $t = t'$ et on a :

$$\begin{tikzcd}
x_1 \arrow[dr, "*"] & & \\
x_2 \arrow[dr, "*"] & & \\
\vdots \arrow[dr, "*"] & & \\
x_{n-2} \arrow[r, "*"] & t' = t & \\
x_n \arrow[r] & x_{n-1} \arrow[ur, "*"] &
\end{tikzcd}$$

Sinon, on a $x_{n-1} \to x_n$ et il existe t tel que

$$\begin{tikzcd}
x_1 \arrow[dr, "*"] & & & \\
x_2 \arrow[dr, "*"] & & & \\
\vdots \arrow[dr, "*"] & t' \arrow[dr, "*"] & & \\
x_{n-2} \arrow[r, "*"] & & t. & \\
x_{n-1} \arrow[r] & x_n \arrow[ur, "*"] & &
\end{tikzcd}$$

Donc le système vérifie la propriété de Church-Rosser.

L'implication (Church-Rosser) $\Rightarrow$ (confluence) est triviale car $\begin{tikzcd} & w \\ w \arrow[ur, "*"] \arrow[dr, "*"'] & \\ & w' \end{tikzcd}$ implique $w \sim_R w'$.

□

Proposition I.44 *Tout mot d'un système de réécriture confluent qui se termine admet une unique forme réduite.*

Dans ce cas, on dit que le système de réécriture est convergent.

Preuve : Tout mot d'un système de réécriture $\langle \Sigma | R \rangle$ qui se termine admet au moins une forme réduite.

On suppose qu'un mot w admet deux formes réduites : $\begin{tikzcd} & w_1 \\ w \arrow[ur, "*"] \arrow[dr, "*"'] & \\ & w_2 \end{tikzcd}$. Par confluence, il existe un mot t tel que $\begin{tikzcd} w_1 \arrow[dr, "*"] & \\ & t \\ w_2 \arrow[ur, "*"'] & \end{tikzcd}$. Comme w_1 et w_2 sont réduits, aucune règle de réécriture ne s'applique. Donc $w_1 = w_2 = t$.

□

Définition I.45 *Une réduction maximale d'un mot w par un système de réécriture $\langle \Sigma | w_i \to t_i, i \in I \rangle$ est une suite finie de règle de réécriture (ou réductions) de $\{w_i \to t_i, i \in I\}$ qui réduit un mot de Σ^* en un mot réduit w_r : il existe une suite d'indice $i_1, i_2, \ldots i_n$ avec $n \geq 0$ et une suite de mots $x_0, x_1, \ldots x_n \in \Sigma^*$ tels que $w = x_0 \to_{i_1} x_1 \to_{i_2} x_2 \cdots \to_{i_n} x_n = w_r$.*

Remarque I.46 *La confluence d'un système de réécriture qui se termine n'implique pas l'unicité d'une réduction maximale. Par exemple, le système de réécriture $\langle \{a, b, c\} | a \to_1 c, b \to_2 c \rangle$ se termine et est confluent. Le mot ab se réduit de deux façons différentes :*

$$ab \to_1 cb \to_2 c^2 \qquad \text{et} \qquad ab \to_2 ac \to_1 c^2.$$

6 Le monoïde quotient $B^*/\sim_B$ sur $B = \{0, 1\}$.

Définition I.47

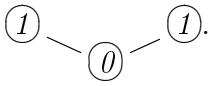
On appelle réduction "demi-tour" (half-turn) la règle de réécriture $\rightarrow_{\mathsf{h}}$ définie sur B^* par

$$\mathsf{h} = (000 \rightarrow \emptyset).$$

On appelle réduction "vallée" la règle de réécriture $\rightarrow_{\mathsf{v}}$ définie sur B^* par

$$\mathsf{v} = (101 \rightarrow 00).$$

Remarque I.48

- *Ces règles de réécriture sont appelées des réductions car elle réduisent strictement la longueur des mots. On appellera expansions H, et expansion V, les règles de réécriture inverses $H = \mathsf{h}^{-1}$ et $V = \mathsf{v}^{-1}$.*
- *La réduction h doit son nom "demi-tour" ("half-turn") de l'origine géométrique de l'étude (voir chapitre (VI)).*
- *La réduction v doit son nom au facteur* 101 *qui fait penser à une vallée :* 

.

Notation : Sur l'alphabet binaire $B = \{0, 1\}$, on note $\sim_B$ la relation d'équivalence engendrée par les règles de réécritures $R_B = (\mathsf{h}, \mathsf{v})$:

$$R_B = \{\mathsf{h} = (000 \rightarrow \emptyset), \mathsf{v} = (101 \rightarrow 00)\}.$$

Remarque I.49 *D'après la proposition (I.27), la relation d'équivalence $\sim_B$ est compatible avec la loi de concaténation du monoïde libre B^*. Le monoïde quotient $(B^*/\sim_B, \cdot, <\emptyset>)$ admet la présentation de monoïde $\langle\{0, 1\}|R_B\rangle = \langle\{0, 1\}|\mathsf{h}, \mathsf{v}\rangle$.*

Proposition I.50 *Le monoïde quotient $(B^*/\sim_B, \cdot, [\emptyset])$ est un groupe.*

Preuve : Les générateurs [0] et [1] du monoïde quotient sont inversibles (voir remarque (I.8)) :

comme $000 \sim_B \emptyset$ et $0101 \sim_B 1010 \sim_B \emptyset$, on a :

$$\begin{cases} [0]^{-1} = [00], \\ [1]^{-1} = [010]. \end{cases}$$

□

7 Le monoïde quotient $\Sigma^*/\sim_\Sigma$.

Dans cette partie, on se place sur le monoïde libre Σ^* sur l'alphabet des entiers $\Sigma = \mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

On rappelle que la réduction "demi-tour" définie au (I.47) est la réduction $\mathsf{h} = (000 \to \emptyset)$.

Définition I.51

On appelle réduction "vallée", notée $\mathsf{v}_{a,b}$ la règle de réécriture $\to_{\mathsf{v}_{a,b}}$ définie sur Σ^* pour deux entiers a et b par $\mathsf{v}_{a,b} = ((a+1)0(b+1)) \to ab)$.

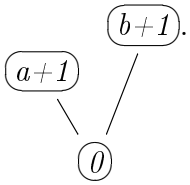
On note $\mathsf{v} = \bigcup_{a,b\in\mathbb{N}} \mathsf{v}_{a,b}$ l'ensemble des réductions $\mathsf{v}_{a,b}$.

On appelle réduction "goulet", notée $\mathsf{u}_{a,b}$, la règle de réécriture $\to_{\mathsf{u}_{a,b}}$ définie sur Σ^* pour deux entiers a et b par $\mathsf{u}_{a,b} = (a00b \to a+b)$.

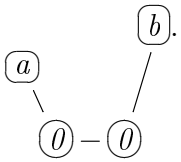
On note $\mathsf{u} = \bigcup_{a,b\in\mathbb{N}} \mathsf{u}_{a,b}$ l'ensemble des réductions $\mathsf{u}_{a,b}$.

Remarque I.52

- *La longueur des mots diminue strictement via les règles de réécriture h, u et v. D'où leur nom de réduction. On appellera expansion H, expansion U et expansion V, les relations inverses $H = \mathsf{h}^{-1}$, $U = \mathsf{u}^{-1}$ et $V = \mathsf{v}^{-1}$.*
- *Les réductions $\mathsf{v}_{a,b}$ étendent la réduction $\mathsf{v} = (101 \to 00)$ définie sur B^* au monoïde Σ^*. Le facteur $(a+1)0(b+1)$ fait aussi penser à une vallée :*



- *La rédcution u tient son nom du facteur $a00b$, qui fait penser à un goulet :*



Notation : Sur l'alphabet des entiers $\Sigma = \mathbb{N}$, on note $\sim_\Sigma$ la relation d'équivalence engendrée par les règles de réécritures $R_\Sigma = (\mathsf{h}, \mathsf{u}, \mathsf{v})$:

$$R_\Sigma = \{\mathsf{h} = (000 \to \emptyset), \mathsf{u} = (a00b \to a+b, a, b \in \mathbb{N}), \mathsf{v} = ((a+1)0(b+1) \to ab, a, b \in \mathbb{N})\}.$$

Remarque I.53 *D'après la proposition (I.27), la relation d'équivalence $\sim_\Sigma$ est compatible avec la loi de concaténation du monoïde libre Σ^*. Le monoïde quotient $(\Sigma^*/\sim_\Sigma, \cdot, [\emptyset])$ admet la présentation de monoïde $\langle \Sigma | R_\Sigma \rangle = \langle \Sigma | \mathsf{h}, \mathsf{u}, \mathsf{v} \rangle$.*

Proposition I.54 *Pour tous entiers a, b, la relation $\mathsf{u}_{a,b} = (a00b \to a+b)$ appartient à la relation d'équivalence engendrée par $\mathsf{h} = (000 \to \emptyset)$ et $\mathsf{v} = ((a+1)0(b+1) \to ab, a, b, \in \mathbb{N})$.*

Le monoïde quotient $(\Sigma^*/\sim_\Sigma, \cdot, [\emptyset])$ admet aussi la présentation $\langle \Sigma | \mathsf{h}, \mathsf{v} \rangle$.

Preuve :
Pour $a = 0$ ou $b = 0$, il est clair que la relation $\mathsf{u}_{a,b}$ est engendrée par la relation h.
Pour $a, b \geq 1$, la relation $\mathsf{u}_{a,b}$ est engendrée par h et v car on a :

$$\begin{array}{rcl} \underline{a0}0b & \sim_{\mathsf{v}} & \underline{(a+1)01}0b \\ & = & (a+1)0\underline{10b} \\ & \sim_{\mathsf{v}} & (a+1)0\underline{0(b-1)} \\ & = & \underline{(a+1)0}0(b-1) \\ & \vdots & \\ & \sim_{\mathsf{v}} & (a+b)\underline{000} \\ & \sim_{\mathsf{h}} & a+b. \end{array}$$

Ainsi, les présentations $\langle \Sigma | \mathsf{h}, \mathsf{u}, \mathsf{v} \rangle$ et $\langle \Sigma | \mathsf{h}, \mathsf{v} \rangle$ définissent le même monoïde quotient.

□

Lemme I.55 *Pour tout entier a, on a :*

$$a + 1 \sim_\Sigma 1(001)^a$$

où $(001)^0 = \emptyset$ par convention.

Preuve : Par récurrence sur a :
pour $a = 0$, il est clair que $1 \sim_\Sigma 1(001)^0$,
pour $a \geq 0$, on a :

$$\begin{array}{rcl} a+1 & \sim_{\mathsf{u}} & a001 \\ & \sim_\Sigma & 1(001)^{a-1}001 \\ & \sim_\Sigma & 1(001)^a. \end{array}$$

□

Proposition I.56 *Le monoïde quotient $(\Sigma^* / \sim_\Sigma, \cdot, [\emptyset])$ est un groupe.*

Preuve : Comme $000 \sim_\Sigma \emptyset$ et $1010 \sim_\Sigma 0101 \sim_\Sigma \emptyset$, les générateurs $[0]$ et $[1]$ admettent un inverse à gauche et à droite. Ils sont donc inversibles et on a :

$$\begin{cases} [0]^{-1} = [00], \\ [1]^{-1} = [010]. \end{cases}$$

Le sous-monoïde de $\Sigma^* / \sim_\Sigma$ engendré par les éléments inversibles $[0]$ et $[1]$ est un groupe (voir remarque (I.8)). Par le lemme (I.55), ce groupe contient les générateurs $[a]_\Sigma$ $(a \in \mathbb{N})$ du monoïde $\Sigma^* / \sim_\Sigma$.

□

8 Un isomorphisme de monoïde entre $B^*/\sim_B$ et $\Sigma^*/\sim_\Sigma$.

On rappelle les présentations

$$B^*/\sim_B = \langle B | \mathsf{h} = (000 \to \emptyset), \mathsf{v} = (101 \to 00) \rangle$$

et

$$\Sigma^*/\sim_\Sigma = \langle \Sigma | \mathsf{h} = (000 \to \emptyset), \mathsf{v} = ((a+1)0(b+1) \to ab, a, b \in \mathbb{N}) \rangle$$

des monoïdes quotients $B^*/\sim_B$ et $\Sigma^*/\sim_\Sigma$.

Dans cette partie, on démontre le résultat suivant :

Théoreme I.57 *Les monoïdes $B^*/\sim_B$ et $\Sigma^*/\sim_{\Sigma^*}$ sont isomorphes.*

Preuve : La preuve fait intervenir les résultats intermédiaires suivants et sera une conséquence directe de la proposition (I.60).

□

Proposition I.58

L'extension naturelle de l'inclusion $\iota : \begin{array}{ccc} B = \{0,1\} & \longrightarrow & \Sigma^*/\sim_\Sigma \\ 0 & \longmapsto & [0]_\Sigma \\ 1 & \longmapsto & [1]_\Sigma \end{array}$ *passe au quotient $B^*/\sim_B$.*

Le morphisme induit $\hat{\iota} : B^*/\sim_B \longrightarrow \Sigma^*/\sim_\Sigma$ est surjectif.

Preuve : Il est clair que $[000]_\Sigma = [\emptyset]_\Sigma$ car h est une relation de la présentation de monoïde $\langle \Sigma | \mathsf{h}, \mathsf{v} \rangle$ et que $[101]_\Sigma = [00]_\Sigma$ car $\mathsf{v} = \mathsf{v}_{0,0}$ est une relation de la présentation de monoïde $\langle \Sigma | \mathsf{h}, \mathsf{v} \rangle$.

Donc, d'après la proposition (I.29), l'extension de l'inclusion ι passe au quotient et il existe un unique morphisme de monoïde $\hat{\iota}$ tel que $\iota = \hat{\iota} \circ \pi$.

La surjectivité résulte du lemme (I.55).

□

Proposition I.59

L'extension naturelle de l'application κ définie par $\kappa : \begin{array}{ccc} \Sigma & \longrightarrow & B^*/\sim_B \\ 0 & \longmapsto & [0]_B \\ 1 \leq a & \longmapsto & [1(001)^{a-1}]_B \end{array}$ *passe au quotient $\Sigma^*/\sim_\Sigma$, avec la convention $1(001)^0 = 1$.*

Le morphisme induit $\hat{\kappa} : \Sigma^*/\sim_\Sigma \longrightarrow B^*/\sim_B$ est surjectif.

Preuve : Il est clair que $\kappa(000) = [000]_B = [\emptyset]_B = \kappa(\emptyset)$ et $\kappa(101) = [101]_B = [00]_B = \kappa(00)$ car h et v sont des relations de la présentation de monoïde $\langle B|\mathsf{h},\mathsf{v}\rangle$.

Pour tous entiers $a, b \geq 1$, on a :

$$\begin{aligned}
\kappa((a+1)0(b+1)) &= [1(001)^a01(001)^b]_B \\
&= [1(001)^{a-1}00101001(001)^{b-1}]_B \\
&= [1(001)^{a-1}0000001(001)^{b-1}]_B \\
&= [1(001)^{a-1}1(001)^{b-1}]_B \\
&= \kappa(ab).
\end{aligned}$$

Donc, d'après la proposition (I.29), l'extension κ passe au quotient et il existe un unique morphisme de monoïde $\hat{\kappa}$ tel que $\kappa = \hat{\kappa} \circ \pi$.

De plus, il est clair que les générateurs $[0]_B = \kappa(0)$ et $[1]_B = \kappa(1)$ de $B^*/\sim_B$ sont dans l'image de κ. Donc κ est surjective. Le morphisme induit $\hat{\kappa}$ est lui aussi surjectif.

□

Proposition I.60

Les morphismes $\hat{\iota} : \begin{array}{ccc} B^*/\sim_B & \longrightarrow & \Sigma^*/\sim_\Sigma \\ [0]_B & \longmapsto & [0]_\Sigma \\ [1]_B & \longmapsto & [1]_\Sigma \end{array}$ *et* $\hat{\kappa} : \begin{array}{ccc} \Sigma^*/\sim_\Sigma & \longrightarrow & B^*/\sim_B \\ [0]_\Sigma & \longmapsto & [0]_B \\ [a]_\Sigma & \longmapsto & [1(001)^{a-1}]_B \end{array}$ *sont réciproques l'un de l'autre.*

Preuve : Par définition des applications ι et κ, on a :

$$\begin{array}{ccccc}
\Sigma^*/\sim_\Sigma & \xrightarrow{\hat{\kappa}} & B^*/\sim_B & \xrightarrow{\hat{\iota}} & \Sigma^*/\sim_\Sigma \\
[0]_\Sigma & \longmapsto & [0]_B & \longmapsto & [0]_\Sigma \\
[a]_\Sigma & \longmapsto & [1(001)^{a-1}]_B & \longmapsto & [1(001)^{a-1}]_\Sigma = [a]_\Sigma \quad \text{(Voir lemme I.55).}
\end{array}$$

□

9 Les formes réduites de $B^*/\sim_B$ et de $\Sigma^*/\sim_\Sigma$.

Lemme I.61 *Le langage $\mathcal{L}'$ sur B^* composé de mots non vides commençant et terminant par 1, sans facteurs 0 isolé et sans facteur 000 est engendré par l'alphabet $\{1(001)^k, k \in \mathbb{N}\}$ et on a :*

$$\mathcal{L}' = \{\bigcup_{k\in\mathbb{N}} \{1(001)^k\}\}.\{\bigcup_{k\in\mathbb{N}} \{1(001)^k\}\}^*$$

avec la convention $1(001)^0 = 1$.

Preuve : Un mot de $\mathcal{L}'$ commence et termine par 1 et n'admet pas de facteur 0 isolé, ni de facteur 000. Donc $\{\bigcup_{k\in\mathbb{N}}\{1(001)^k\}\}.\{\bigcup_{k\in\mathbb{N}}\{1(001)^k\}\}^* \subset \mathcal{L}'$.

Réciproquement, on considère un mot w du langage $\mathcal{L}'$.

Si le mot w n'a que des facteurs 1 isolés, alors il est de la forme $1(001)^k$, avec $k \geq 0$.

Sinon, il est de la forme $w = u11v$ tels que les mots $u1$ et $1v$ sont dans le langage et commencent et terminent par 1, sans zéro isolés et sans facteurs 000. Par récurrence sur le nombre de 1 non isolés, $u1$ et $1v$ sont dans le langage $\mathcal{L}'$ et le mot w est dans l'ensemble $\{\bigcup_{k\in\mathbb{N}}\{1(001)^k\}\}\{\bigcup_{k\in\mathbb{N}}\{1(001)^k\}\}^*$.

Ainsi, un mot w du langage $\mathcal{L}'$ admet une unique factorisation de la forme

$$w = 1(001)^{k_1}1(001)^{k_2}\cdots 1(001)^{k_p}$$

avec $p \geq 1$ et $k_i \geq 0$ pour tout indice $1 \leq i \leq p$.

□

Remarque I.62 *Le monoïde $\mathcal{L} = \{\emptyset\} \cup \mathcal{L}'$ est le monoïde libre sur l'alphabet $\{1(001)^k, k \in \mathbb{N}\}$. Il est donc isomorphe à Σ^* (pour $\Sigma = \mathbb{N}$).*

Proposition I.63

Le système de réécriture $\langle B|\mathsf{h},\mathsf{v}\rangle$ se termine et l'ensemble de ses mots réduits est :

$$\textit{Réduit}_B = \{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\mathcal{L}'\{\emptyset, 0, 00\} \tag{I.1}$$

avec $\mathcal{L}' = \{\bigcup_{k\in\mathbb{N}}\{1(001)^k\}\}.\{\bigcup_{k\in\mathbb{N}}\{1(001)^k\}\}^*$.

Preuve : Le morphisme longueur $\lambda : B^* \longrightarrow \mathbb{N}$ définit une relation d'ordre bien fondée : un mot w' est plus petit qu'un mot w si et seulement si $\lambda(w') < \lambda(w)$. La longueur d'un mot diminue strictement avec les régles de réécriture h et v. Donc le système de réécriture se termine (voir proposition (I.39)).

Les mots réduits sont les mots du monoïde libre $\{0,1\}^*$ sans facteur 000 (sinon on peut appliquer la réduction $000 \to \emptyset$), et sans zéro intérieur isolé (sinon on peut appliquer la réduction $101 \to 00$).

Les mots réduits sans facteurs 1 sont $\emptyset$, 0 et 00.

Les mots avec au moins un facteur 1 sont les mots du langage $\mathcal{L}$ défini au lemme (I.61) avec éventuellement un ou deux zéro(s) au début et/ou à la fin. Ils sont donc de la forme

$$0^d \cdot 1(001)^{e_1} \cdot 1(001)^{e_2} \cdots 1(001)^{e_n} \cdot 0^f$$

avec $d, f \in \{0,1,2\}$, $n \geq 1$ et $e_i \geq 0$.

□

Corollaire I.64 *La projection canonique de Réduit$_B$ dans $B^*/\sim_B$ est surjective.*

Preuve : Tout mot de B^* admet au moins un représentant réduit pour $\sim_B$ dans Réduit$_B$.

□

Proposition I.65 *Le système de réécriture $\langle\Sigma|\mathsf{h},\mathsf{u},\mathsf{v}\rangle$ se termine et l'ensemble de ses mots réduits est :*

$$\textit{Réduit}_\Sigma = \{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\mathcal{K}'\{\emptyset, 0, 00\} \tag{I.2}$$

avec $\mathcal{K} = \big(\mathbb{N}\setminus\{0\}\big)^*$ et $\mathcal{K}' = \mathcal{K}\setminus\{\emptyset\}$.

Preuve : Comme sur l'alphabet binaire (voir proposition (I.63)), le morphisme longueur λ définit une relation d'ordre bien fondée sur Σ^* et la longueur d'un mot diminue strictement avec les réductions h, v et u. Donc le système de réécriture se termine vers des mots irréductibles de longueur minimale.

Les mots réduits sont les mots de Σ^* sans facteur 000, sans zéro isolé intérieur, ni facteur 00 isolé intérieur. Autrement dit, sans zéro intérieur et sans triplet de zéros.

Les mots réduits sans facteurs non nuls sont $\emptyset$, 0 et 00.

Ceux comportant au moins un facteur non nuls sont les mots non vides sur l'alphabet $\mathbb{N}\setminus\{0\}$ avec éventuellement 1 ou 2 zéros en début ou en fin de mot. Ce sont les mots de la forme

$$0^d a_1 a_2 \cdots a_n 0^f$$

avec d et f dans $\{0,1,2\}$ et $a_i \neq 0$ pour tout indice $1 \leq i \leq n$.

□

Corollaire I.66 *La projection canonique de Réduit$_\Sigma$ dans $\Sigma^*/\sim_\Sigma$ est surjective.*

Preuve : Tout mot de Σ^* admet au moins un représentant réduit pour $\sim_\Sigma$ dans Réduit$_\Sigma$.

□

Proposition I.67 *L'ensemble Réduit$_B$ des mots réduits pour la présentation de monoïde $\langle B|\mathsf{h},\mathsf{v}\rangle$ (voir proposition (I.63)) est en bijection avec l'ensemble Réduit$_\Sigma$ des mots réduits pour la présentation de monoïde $\langle\Sigma|\mathsf{h},\mathsf{u},\mathsf{v}\rangle$ (voir proposition (I.65)) :*

$$\textit{Réduit}_B \simeq \textit{Réduit}_\Sigma.$$

Preuve : C'est clair avec la remarque (I.62) et la proposition (I.65).

□

10 Réductions maximales sur Σ^* et sur B^*.

Dans la partie précédente, on a montré que les systèmes de réécriture $\langle B|\mathsf{h},\mathsf{v}\rangle$ et $\Sigma|\mathsf{h},\mathsf{u},\mathsf{v}\}$ se terminent dans leurs ensembles des mots réduits respectifs :

$$\text{Réduit}_B = \{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\mathcal{L}'\{\emptyset, 0, 00\} \text{ où } \mathcal{L}' = \mathcal{L} \setminus \{0\} \text{ avec } \mathcal{L} = \Big(\bigcup_{k\in\mathbb{N}} 1(001)^k\Big)^*$$

et

$$\text{Réduit}_\Sigma = \{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\mathcal{K}'\{\emptyset, 0, 00\} \text{ où } \mathcal{K}' = \mathcal{K} \setminus \{0\} \text{ avec } \mathcal{K} = \Big(\mathbb{N} \setminus \{0\}\Big)^*.$$

Et on a

$$\text{Réduit}_B \simeq \text{Réduit}_\Sigma.$$

Ainsi, tout mot de Σ^* (respectivement B^*) admet au moins un représentant réduit pour la relation d'équivalence $\sim_\Sigma$ (respectivement $\sim_B$) et se réduit par une suite de réductions h, u et v (respectivement h et v) à ce mot réduit de sa classe d'équivalence.

Exemple I.68 *Généralement, il existe plusieurs réductions maximales distinctes permettant de réduire un mot à un mot réduit.*

Par exemple, sur $B^* \subset \Sigma^*$, le mot $w = 001010110110$ se réduit par les réductions maximales suivantes au mot réduit $w_r = 0010010$:

- $w = 00\underset{\uparrow}{1}010110110 \to_{\mathsf{v}} 00000110\underset{\uparrow}{1}10 \to_{\mathsf{v}} \underline{000}0010010 \to_{\mathsf{h}} 0010010.$
- $w = 00101\underset{\uparrow}{0}110110 \to_{\mathsf{v}} 001\underline{000}10110 \to_{\mathsf{h}} 0011\underset{\uparrow}{0}10010 \to_{\mathsf{v}} 0010010.$
- $w = 00101011\underset{\uparrow}{0}110 \to_{\mathsf{v}} 00101\underset{\uparrow}{0}10010 \to_{\mathsf{h}} 001\underline{000}10010 \to_{\mathsf{v}} 0010010.$

Toutes ces réductions maximales sont composées de 2 réductions v et 1 réduction h.

Autre exemple, sur Σ^*, le mot $w = 1000102005$ se réduit par les réductions maximales suivantes (voir figure (1)) au mot réduit $w_r = 05$:

- $w = 1\underline{000}102005 \to_{\mathsf{h}} 1102\underline{00}5 \to_{\mathsf{u}} 11\underset{\uparrow}{0}7 \to_{\mathsf{v}} 1\underset{\uparrow}{0}6 \to_{\mathsf{v}} 05.$

  Cette réduction maximale comporte 1 réduction h, 1 réduction u et 2 réductions v .
- $w = 1000102\underline{00}5 \to_{\mathsf{u}} 1000\underset{\uparrow}{1}07 \to_{\mathsf{v}} 1\underline{000}06 \to_{\mathsf{h}} 1\underset{\uparrow}{0}6 \to_{\mathsf{v}} 05.$

  Cette réduction maximale comporte également 1 réduction h, 1 réduction u et 2 réductions v.
- *Aussi :* $w = 100\underset{\uparrow}{1}02005 \to_1 0\underline{000}1005 \to_{\mathsf{h}} 1\underset{\uparrow}{0}1005 \to_{\mathsf{v}} \underline{000}05 \to_{\mathsf{h}} 05.$

  Là, la réduction maximale comporte 2 réductions h et 2 réductions v (pas de réduction u).

Proposition I.69 *Le nombre n_{h} de réductions h et la somme $n_{\mathsf{u}}+n_{\mathsf{v}}$ du nombre de réductions u et du nombre de réductions v dans une réduction d'un mot w de Σ^* (respectivement de B^* avec $n_{\mathsf{u}}=0$) à un mot réduit w_r de Réduit$_\Sigma$ (repectivement de Réduit$_B$) ne dépendent pas du choix de la réduction maximale et on a :*

$$n_{\mathsf{v}} = \frac{1}{2}\left[\sigma(w) - \sigma(w_r)\right].$$

et

$$n_{\mathsf{h}} + n_{\mathsf{u}} = \frac{1}{6}\left[2\lambda(w) - \sigma(w)\right] - \frac{1}{6}\left[2\lambda(w_r) - \sigma(w_r)\right].$$

Preuve :

Seule la réduction v modifie la somme d'un mot, qui augmente de 2. Donc $\sigma(w)-\sigma(w_r) = 2n_{\mathsf{v}}$.

De plus, la longueur diminue de 3 par la réduction h et par la réduction u alors qu'elle diminue de 1 avec la réduction v. D'où $\lambda(w) - \lambda(w_r) = 3(n_{\mathsf{h}} + n_{\mathsf{u}}) + n_{\mathsf{v}}$.

□

Chapitre II

Deux présentations de $PSL_2(\mathbb{Z})$ et leurs formes réduites.

1 Remarques préliminaires sur $PSL_2(\mathbb{Z})$

Le groupe spécial linéaire $SL_2(\mathbb{Z})$ est l'ensemble des matrices 2×2 de déterminant 1 à coefficients entiers.

Le groupe modulaire $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I_2\}$ est le quotient du groupe spécial linéaire par son centre $\pm I_2 = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}$. Un élément de $PSL_2(\mathbb{Z})$ est une classe d'équivalence de $SL_2(\mathbb{Z})$ pour la relation $M \sim -M$ et on note $\pm M$ l'image d'une matrice M de $SL_2(\mathbb{Z})$ dans $PSL_2(\mathbb{Z})$:

$$\begin{array}{rcl} \pi : SL_2(\mathbb{Z}) & \longrightarrow & PSL_2(\mathbb{Z}), \\ M & \longmapsto & \pm M. \end{array}$$

Le produit de deux éléments $\pm A$ et $\pm B$ de $PSL_2(\mathbb{Z})$ est alors donné par $\pm AB$.

Soient $S = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $U = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ dans $PSL_2(\mathbb{Z})$. Le groupe modulaire $PSL_2(\mathbb{Z})$ est le produit libre

$$PSL_2(\mathbb{Z}) = \langle S | S^2 \rangle * \langle U | U^3 \rangle \qquad \text{(voir [Se])}. \tag{II.1}$$

Tout élément de $PSL_2(\mathbb{Z})$ admet un unique représentant réduit sur l'alphabet $\Gamma = \{S, U\}$ pour la relation d'équivalence $\sim_\Gamma$ engendrée par les règles de réécriture $R_\Gamma = \{S^2 \to \emptyset, U^3 \to \emptyset\}$. Les mots réduits sont formés d'une alternance d'éléments non vide de $\langle S | S^2 \to \emptyset \rangle \sim \mathbb{Z}/2\mathbb{Z}$ et d'éléments non vide de $\langle U | U^3 \to \emptyset \rangle \sim \mathbb{Z}/3\mathbb{Z}$:

$$PSL_2(\mathbb{Z}) \simeq \text{Réduit}_\Gamma = \{U^{\epsilon_1}SU^{\epsilon_2}\cdots SU^{\epsilon_n} \text{ pour } \begin{array}{l} n \geq 1, \\ \epsilon_1, \epsilon_n \in \{0,1,2\} \text{ et} \\ \epsilon_i \in \{1,2\} \text{ pour } 1 < i < n\}. \end{array} \tag{II.2}$$

Remarque II.1 *D'après la remarque (I.8) sur les catégories $\mathcal{M}on$ et $\mathcal{G}rp$, le groupe modulaire $PSL_2(\mathbb{Z})$ peut être considéré comme un monoïde, muni du produit matriciel usuel et de l'élément neutre $I = \pm I_2$. Dans la suite, le groupe $PSL_2(\mathbb{Z})$ sera spécifié par la présentation de groupe (ou de monoïde) $\langle \Gamma | R_\Gamma \rangle = \langle S, U | S^2 = I, U^3 = I \rangle$.*

Réciproquement, les générateurs S et U du monoïde $\langle S, U | S^2 \to \emptyset, U^3 = \emptyset \rangle$ sont d'ordre fini, donc inversibles. C'est bien un groupe.

Pour simplifier les notations, le groupe modulaire et le monoïde associé seront tous deux notés $PSL_2(\mathbb{Z})$.

Lemme II.2 *Le langage $\mathcal{J}'$ sur l'alphabet $\Gamma = \{U, S\}$ composé de mots non vides, commençant par US et terminant par SU, sans facteurs U^3 et sans facteur S^2 est engendré par l'alphabet $\{(US)^kU, k \geq 1\}$ et on a :*

$$\mathcal{J}' = \{\bigcup_{k\geq 1}\{(US)^kU\}\}.\{\bigcup_{k\geq 1}\{(US)^kU\}\}^*.$$

Preuve : Il est clair que pour tout entier $k \geq 1$, le mot $(US)^kU$ est dans le langage $\mathcal{J}'$. Donc

$$\{\bigcup_{k\geq 1}\{(US)^kU\}\}.\{\bigcup_{k\geq 1}\{(US)^kU\}\}^* \subset \mathcal{J}'.$$

Réciproquement, un mot W de $\mathcal{J}'$ s'écrit : $W = USU^{e_1}SU^{e_2}\cdots U^{e_n}SU$ avec $n \geq 1$, et $e_i \in \{1, 2\}$.

Si le mot W n'a que des facteurs U isolés, alors il est de la forme $(US)^kU$, avec $k \geq 1$.

Sinon, il est de la forme $W = W_1UUW_2$ tel que les mots W_1U et UW_2 sont dans le langage $\mathcal{J}'$. Par récurrence sur le nombre de facteur U^2, le mot W est dans l'ensemble $\{\bigcup_{k\geq 1}\{(US)^kU\}\}\{\bigcup_{k\geq 1}\{(US)^kU\}\}^*$.

Ainsi, un mot w du langage $\mathcal{J}'$ admet une factorisation de la forme

$$W = (US)^{k_1}U(US)^{k_2}U\cdots(US)^{k_p}U$$

avec $p \geq 1$ et $k_i \geq 1$ pour tout indice i. Il est facile de voir que cette factoristaion est unique.

□

Remarque II.3 *Le monoïde* $\mathcal{J} = \{\emptyset\} \cup \mathcal{J}'$ *est le monoïde libre sur l'alphabet* $\{(US)^k U, k \geq 1\}$. *Il est isomorphe à* Σ^* *(pour* $\Sigma = \mathbb{N}$*).*

Proposition II.4 *L'ensemble Réduit*$_\Gamma$ *des mots réduits pour la présentation* $\langle \Gamma | R_\Gamma \rangle$ *de* $PSL_2(\mathbb{Z})$ *est en bijection avec l'ensemble*

$$\{I, U, U^2\} \cup \{I, U, U^2\}\mathcal{J}'\{I, U, U^2\}$$

où $\mathcal{J}' = \{\bigcup_{k\geq 1}\{(US)^k U\}\}.\{\bigcup_{k\geq 1}\{(US)^k U\}\}^*$.

Preuve : Les mots réduits sans facteur S sont les mots de $\{I, U, U^2\}$.

Les mots réduits qui commencent et terminent par un facteur U sont les mots du langage $\mathcal{J}'$ avec éventuellement un facteur U en début et fin de mot. Ce sont les mots de l'ensemble $\{I, U\}\mathcal{J}'\{I, U\}$.

Un mot réduit W qui commence par S et termine par un facteur U est équivalent au mot $U^2(UW)$ avec UW dans le langage $\mathcal{J}'$ et avec éventuellement un facteur U en fin de mot. Donc l'ensemble des classes d'équivalences représentées par un mot réduit qui commence par S et termine par un facteur U est en bijection avec l'ensemble $\{U^2\}\mathcal{J}'\{I, U\}$.

Un mot réduit W qui commence par U et termine par un facteur S est équivalent au mot $(WU)U^2$ avec WU dans le langage $\mathcal{J}'$ et avec éventuellement un facteur U en début de mot. Donc, l'ensemble des classes d'équivalences représentées par un mot réduit qui commence par U et termine par un facteur S est en bijection avec l'ensemble $\{I, U\}\mathcal{J}'\{U^2\}$.

Enfin, un mot réduit W qui commence et termine par un facteur S est équivalent au mot $U^2(UWU)U^2$ avec UWU dans le langage $\mathcal{J}'$. Donc l'ensemble des classes d'équivalences représentées par un mot réduit qui commence et termine par un facteur S est en bijection avec l'ensemble $\{U^2\}\mathcal{J}'\{U^2\}$.

D'où le résultat.

□

2 Définitions - Morphismes de monoïdes

Dans cette partie, on considère le monoïde libre Σ^* sur l'alphabet $\Sigma = \mathbb{N}$ et on note

$$\begin{array}{rccc} \lambda : & \Sigma^* & \longrightarrow & \mathbb{N} \\ & a_1 \cdots a_n & \longmapsto & n \end{array} \quad \text{et} \quad \begin{array}{rccc} \sigma : & \Sigma^* & \longrightarrow & \mathbb{N} \\ & a_1 \cdots a_n & \longmapsto & \sum_{k=1}^n a_k \end{array}$$

les morphismes de monoïdes "longueur" et "somme" introduits dans l'exemple (I.7).

Définition II.5 *Le morphisme de monoïde $\mu : \Sigma^* \longrightarrow PSL_2(\mathbb{Z})$ est l'extension naturelle de l'application de Σ dans $PSL_2(\mathbb{Z})$ définie par :*

$$\mu(a) = \pm \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}, \text{ pour tout entier } a. \tag{II.3}$$

Remarque II.6 *En particulier, on a $\mu(0) = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = U$.*

On vérifie aisément que $\mu(1) = \pm \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} = USU$.

Ainsi, $\mu(00)\mu(1)\mu(00) = U^2USUU^2 = S$. Donc :

$$\begin{cases} U = \mu(0), \\ S = \mu(00100). \end{cases} \tag{II.4}$$

Proposition II.7 *Le morphisme de monoïde $\mu|_{\{0,1\}^*} : \{0,1\}^* \longrightarrow PSL_2(\mathbb{Z})$ est surjectif.*

Preuve : Les relations (II.4) montrent que les générateurs $S = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $U = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ de $PSL_2(\mathbb{Z})$ sont dans l'image de μ.

Comme S et U sont d'ordre fini, ils engendrent $PSL_2(\mathbb{Z})$ en tant que monoïde (voir remarque (I.8)).

□

Comme $\{0,1\} \subset \Sigma = \mathbb{N}$, on a :

Corollaire II.8 *Le morphisme de monoïde $\mu : \Sigma^* \longrightarrow PSL_2(\mathbb{Z})$ est surjectif.*

Lemme II.9 *Soit $a \geq 0$ un entier. Le représentant réduit de la matrice $\mu(a) = \pm \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}$ dans l'ensemble Réduit_Γ des mots réduits pour la présentation $\langle \Gamma | R_\Gamma \rangle$ de $PSL_2(\mathbb{Z})$ est :*

$$\mu(a) = (US)^a U. \tag{II.5}$$

Preuve : L'égalité se vérifie facilement par récurrence.

De plus, pour tout entier a, le produit $(US)^a U$ ne comporte pas de facteurs S^2, ni de facteurs U^3. C'est donc bien une forme réduite pour la présentation $\langle \Gamma | R_\Gamma \rangle$.

□

3 Les monoïdes $\Sigma^*/\sim_\Sigma$ et $B^*/\sim_B$ sont isomorphes à $PSL_2(\mathbb{Z})$.

Dans cette partie, on montre le résultat principal suivant :

Théoreme II.10 *Les groupes (ou monoïdes) $PSL_2(\mathbb{Z})$, $\Sigma^*/\sim_\Sigma$ et $B^*/\sim_B$ sont isomorphes.*

Un isomorphisme entre $B^*/\sim_B$ (respectivement $\Sigma^*/\sim_\Sigma$) et $PSL_2(\mathbb{Z})$ est donné par

$$\mu(a) = \pm \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}$$

pour a dans $B = \{0,1\}$ (respectivement pour a dans $\Sigma = \mathbb{N}$).

Preuve :

Le résultat pour $B^*/\sim_B$ est une conséquence des résultats intermédiaires suivants concernant la surjectivité du morphisme μ_{B^*} (proposition (II.11)) et l'injectivité du morphisme $\mu_{|\text{Réduit}_B}$ (proposition (II.13)).

Le résultat pour $\Sigma^*/\sim_\Sigma$ est une conséquence de l'isomorphisme $\hat{\iota}$ entre $\Sigma^*/\sim_\Sigma$ et $B^*/\sim_B$ (voir proposition (I.60)).

□

Proposition II.11 *La relation d'équivalence $\sim_B$ est compatible avec le morphisme $\mu_{|B^*}$.*

Le morphisme $\mu_{|B^*}$ passe au quotient $B^*/\sim_B$. Le morphisme induit $\hat{\mu} : B^*/\sim_B \longrightarrow PSL_2(\mathbb{Z})$ est surjectif.

Preuve : Comme on a $\mu(000) = \mu(\emptyset)$ et $\mu(101) = USUUUSU = USSU = UU = \mu(00)$, la relation d'équivalence $\sim_B$ engendrée par les règles de réécriture h et v est compatible avec le morphisme μ. On conclut avec la proposition (I.29).

Le morphisme induit est surjectif car $\mu_{|B^*} = \hat{\mu} \circ \pi$ l'est (voir proposition (II.7)).

□

Remarque II.12 *Pour tout entier a, on a :*

$$\mu(1(001)^a) = USU(UUUSU)^a = (US)^{a+1}U = \mu(a+1) = \pm \begin{pmatrix} 0 & -1 \\ 1 & a+2 \end{pmatrix}.$$

Proposition II.13 *L'application $\mu_{|\text{Réduit}_B} : \text{Réduit}_B \longrightarrow PSL_2(\mathbb{Z})$ est bijective.*

Preuve :

L'ensemble des mots réduits du système $\langle B|\mathsf{h},\mathsf{v}\rangle$ est $\text{Réduit}_B = \{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\mathcal{L}'\{\emptyset, 0, 00\}$ où $\mathcal{L}' = \mathcal{L} \setminus \{0\}$ avec $\mathcal{L} = \Big(\{1(001)^k, k \in \mathbb{N}\}\Big)^*$ (voir proposition (I.63)).

Le groupe modulaire $PSL_2(\mathbb{Z})$ est isomorphe à l'ensemble $\{I, U, U^2\} \cup \{I, U, U^2\}\mathcal{K}'\{I, U, U^2\}$ où $\mathcal{K}' = \mathcal{K} \setminus \{0\}$ avec $\mathcal{K} = \Big(\{(US)^k U, k \geq 1\}\Big)^*$ (voir proposition (II.4)).

On a $\mu_{|\text{Réduit}_B}(\{\emptyset, 0, 00\}) = \{I, U, U^2\}$ et l'application $\mu_{|\text{Réduit}_B}$ envoie les lettres de l'alphabet $\{1(001)^k, k \in \mathbb{N}\}$ sur les lettres de $\{(US)^k U, k \geq 1\}$ (voir remarque (II.12)). C'est clairement une bijection.

□

Corollaire II.14 *du théorème (II.10). Le système de réécriture $\langle B|\mathsf{h}, \mathsf{v}\rangle$ (respectivement $\langle \Sigma|\mathsf{h}, \mathsf{u}, \mathsf{v}\rangle$) est convergent : tout mot de B^* (respectivement Σ^*) admet un unique représentant réduit dans Réduit_B (respectivement dans Réduit_Σ) et*

$$\text{Réduit}_B \simeq \langle B|\mathsf{h}, \mathsf{v}\rangle \simeq B^*/\sim_B \simeq PSL_2(\mathbb{Z})$$

$$\Big(\textit{respectivement } \text{Réduit}_\Sigma \simeq \langle \Sigma|\mathsf{h}, \mathsf{u}, \mathsf{v}\rangle \simeq \Sigma^*/\sim_\Sigma \simeq PSL_2(\mathbb{Z})\Big).$$

Preuve : Voir proposition (I.44).

□

Remarque II.15 *Les systèmes de réécriture $\langle B|\mathsf{v}\rangle$ et $\langle \Sigma|\mathsf{v}\rangle$ ne sont pas convergents.*

Ces systèmes de réécriture se terminent car la longueur définit un ordre bien fondé et la réduction v sur B^* et sur Σ^* réduit strictement la longueur des mots (voir proposition (I.39)).

Mais ils ne sont pas confluents ; il n'y a pas unicité du mot réduit.

Par exemple, le mot 10101 *de $B^* \subset \Sigma^*$ qui n'est pas réduit pour la réduction $\mathsf{v} = \mathsf{v}_{0,0} = (101 \to 00)$, se réduit par $10101 \to_{\mathsf{v}} 1000$ et $10101 \to_{\mathsf{v}} 0001$. Les deux mots distincts* 1000 *et* 0001 *sont réduits pour la réduction v.*

Les mots réduits d'un même mot pour la réduction v, n'ont pas forcément la même longueur, ni la même somme. Par exemple, avec le mot 1010101 *de $B^* \subset \Sigma^*$, on a : $1010101 \to_{\mathsf{v}} 000101 \to_{\mathsf{v}} 00000$ et $1010101 \to_{\mathsf{v}} 100001$.*

Sur Σ^*, l'unicité du mot réduit (voir corollaire (II.14)) dans une classe d'équivalence pour $\sim_\Sigma$ implique le lemme suivant :

Lemme II.16 *Soit w_r un mot réduit pour $\sim_\Sigma$ dans l'ensemble $\{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\{1\}\{1\}^*\{\emptyset, 0, 00\} \subset \text{Réduit}_\Sigma$. Tout mot non réduit de la classe d'équivalence $[w_r]_\Sigma$ de w_r admet soit un zéro isolé intérieur, soit un facteur* 000.

Preuve : Par l'absurde, on suppose qu'il existe des mots non réduits dans la classe d'équivalence $[w_r]_\Sigma$ de w_r sans zéro isolé intérieur et sans facteur 000 et on considère un tel mot w de longueur minimal.

Comme w n'est pas réduit, il possède un couple de zéro isolé intérieur. Donc le mot w est de la forme $w = w_1.a.0.0.b.w_2$ où $a, b \geq 1$. Les facteurs $w_1.a$ et $b.w_2$ n'ont pas de zéro isolé intérieur et pas de facteur 000.

Le mot w se réduit via une réduction u au mot $w' = w_1.(a+b).w_2$. Le mot w' est aussi dans la classe d'équivalence $[w_r]_\Sigma$; il ne possède aucun zéro isolé intérieur et aucun facteur 000. Il ne comporte pas non plus de couple de zéro intérieur car cela contredirait l'hypothèse de minimalité de w.

Donc, le mot w' est réduit. Par uncité du mot réduit, on a $w = w_r$. Or, w admet un facteur $a + b \geq 2$; il n'est pas dans l'ensemble $\{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\{1\}\{1\}^*\{\emptyset, 0, 00\} \subset \text{Réduit}_\Sigma$. Contradiction.

□

Remarque II.17 *Le lemme précédent II.16 implique que l'on peut se passer de la réduction* u *dans les classes d'équivalence des mots réduits ne comportant pas de facteurs* $a \geq 2$. *C'est valable, en particulier, pour les mots de la classe* $[\emptyset]_\Sigma$.

Proposition II.18

Soit w_r *un mot réduit dans l'ensemble* $\{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\{1\}\{1\}^*\{\emptyset, 0, 00\} \subset$ *Réduit*$_\Sigma$.

Tout mot w *de* $[w_r]_\Sigma$ *se réduit via une réduction maximale composée de* $\frac{1}{2}\sigma(w)$ *réductions* v *et* $\frac{1}{6}[2\lambda(w) - \sigma(w)] - \frac{1}{6}[2\lambda(w_r) - \sigma(w_r)]$ *réductions* h.

Preuve : C'est une conséquence directe de la remarque (II.17) et de la proposition (I.69).

□

Chapitre III

Morphisme d'indice et demi-tour.

Soit $w \in \Sigma^*$ un mot qui se réduit vers l'unique mot réduit de sa classe d'équivalence w_r avec n_{h} réductions h, n_{v} réductions v et n_{u} réductions u. On a (voir proposition (I.69)) :

$$\left\{ \begin{array}{rcl} n_{\mathsf{h}} + n_{\mathsf{u}} & = & \frac{1}{6}\left[2\lambda(w) - \sigma(w)\right] - \frac{1}{6}\left[2\lambda(w_r) - \sigma(w_r)\right] \\ n_{\mathsf{v}} & = & \frac{1}{2}\left[\sigma(w) - \sigma(w_r)\right] \end{array} \right. \tag{III.1}$$

avec la possibilité de ne considérer que des réductions maximales sans réduction u pour les classes d'équivalences des mots réduits de l'ensemble $\{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\{1\}\{1\}^*\{\emptyset, 0, 00\}$ (voir proposition (II.18)).

Respectivement, sur l'alphabet B, on a montré que les nombres de réduction h et v dans une réduction maximale d'un mot $w \in B^*$ vers l'unique mot réduit w_r de sa classe d'équivalence vérifient les même relations (avec $n_{\mathsf{u}} = 0$).

Dans une première partie, on définit de façon combinatoire le morphisme d'indice sur le monoïde libre Σ^* où $\Sigma = \mathbb{N}$ (et sur le monoïde libre B^* où $B = \{0, 1\}$ par restriction) à partir du morphisme $\frac{1}{6}\left[2\lambda - \sigma\right]$ qui intervient dans la relation (III.1).

Dans la seconde partie, on définit le relèvement $\tilde{\mu} : \Sigma^* \to SL_2(\mathbb{Z})$, du morphisme $\mu : \Sigma^* \to PSL_2(\mathbb{Z})$, qui à tout entier a associe la matrice $\begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}$. On montre que l'application linéaire associée à la matrice $\tilde{\mu}(a)$ fait "tourner" une demi-droite dirigée par un vecteur de $\mathbb{Z}^2$ et que l'indice combinatoire d'un mot du noyau de $\mu_{|B^*}$ s'interprète en terme de demi-tours que fait une demi-droite quelconque par les applications successives associées aux lettres du mots.

Dans la troisième partie, on définit le relèvement $\tilde{\mu}^{B_3}$ du monoïde libre Σ^* dans le groupe des tresses à trois brins B_3 qui à tout entier a associe la tresse $\sigma_1\sigma_2^{1-a}$, où σ_1, σ_2 sont les générateurs d'Artin du groupe B_3. On montre que le morphisme d'indice Ind correspond à l'abélianisé B_3^{ab} de B_3.

1 Définition et partition d'une partie de B^* ou de Σ^*.

Définition III.1 *Soit Ind le morphisme d'indice défini sur Σ^* par :*

$$\begin{array}{rccl} Ind: & \Sigma^* & \longrightarrow & \mathbb{Z}/12 \\ & w & \longmapsto & Ind(w) = \dfrac{1}{12}\left[2\lambda(w) - \sigma(w)\right] \end{array} \tag{III.2}$$

On note $Ind_{|B^*}$ (ou simplement Ind) la restriction du morphisme d'indice à B^*.

Soit X une partie de Σ^*. On note X_n l'ensemble des mots de X d'indice n. Les sous-ensembles $(X_n), n \in \mathbb{Z}/12$ forment une partition de X et on a $X = \bigcup_{n\in\mathbb{Z}/12} X_n$.

Remarque III.2

- *Le nombre de réductions h et u (respectivement h) d'une réduction maximale d'un mot de Σ^* (respectivement B^*) vers l'unique mot réduit de sa classe d'équivalence est l'entier donné par :*

  $$n_{\mathsf{h}} + n_{\mathsf{u}} = 2(Ind(w) - Ind(w_r)) \text{ (voir proposition (I.69))}$$

  avec $n_{\mathsf{u}} = 0$ sur B^*.

  Ainsi, tout mot de la classe d'équivalence d'un mot réduit w_r a un indice dans $Ind(w_r) + \frac{1}{2}\mathbb{N}$. La classe d'équivalence $[w_r]_\Sigma$ (respectivement $[w_r]_B$) d'un mot réduit w_r est partitionnée en sous-ensembles

  $$[w_r]_\Sigma = \bigcup_{n\in\mathbb{N}} [w_r]_{\Sigma, Ind(w_r)+\frac{\mathbb{N}}{2}}$$

  (respectivement $[w_r]_B = \bigcup_{n\in\mathbb{N}} [w_r]_{B, Ind(w_r)+\frac{\mathbb{N}}{2}}$).

  Pour simplifier les notations, lorsqu'il n'y a pas de confusion possible, on notera $[w_r]_{\Sigma, Ind(w_r)+\frac{\mathbb{N}}{2}}$ ou $[w_r]_{B, Ind(w_r)+\frac{\mathbb{N}}{2}}$ par simplement $[w_r]_{Ind(w_r)+\frac{\mathbb{N}}{2}}$.

- *Deux mots non équivalents pour la relation d'équivalence $\sim_\Sigma$ peuvent avoir le même indice. Par exemple, les deux mots réduits 05 et 14 d'indice $\frac{-1}{12}$ ne sont pas équivalents pour $\sim_\Sigma$.*

Remarque III.3

1. *Le morphisme d'indice est l'extension naturelle de l'application définie pour tout $a \in \Sigma = \mathbb{N}$ par :*

   $$Ind(a) = \frac{2-a}{12}.$$

2. *On note n_0 le nombre de facteurs 0 et n_1 le nombre de facteurs 1 dans un mot w de B^*.*

Ainsi, l'indice de w est aussi donnée par :

$$Ind(w) = \frac{2n_0 + n_1}{12}.$$

Proposition III.4

1. *La réduction v est compatible avec le morphisme d'indice.*
2. *Les réductions h et u ne sont pas compatibles avec le morphisme d'indice.*

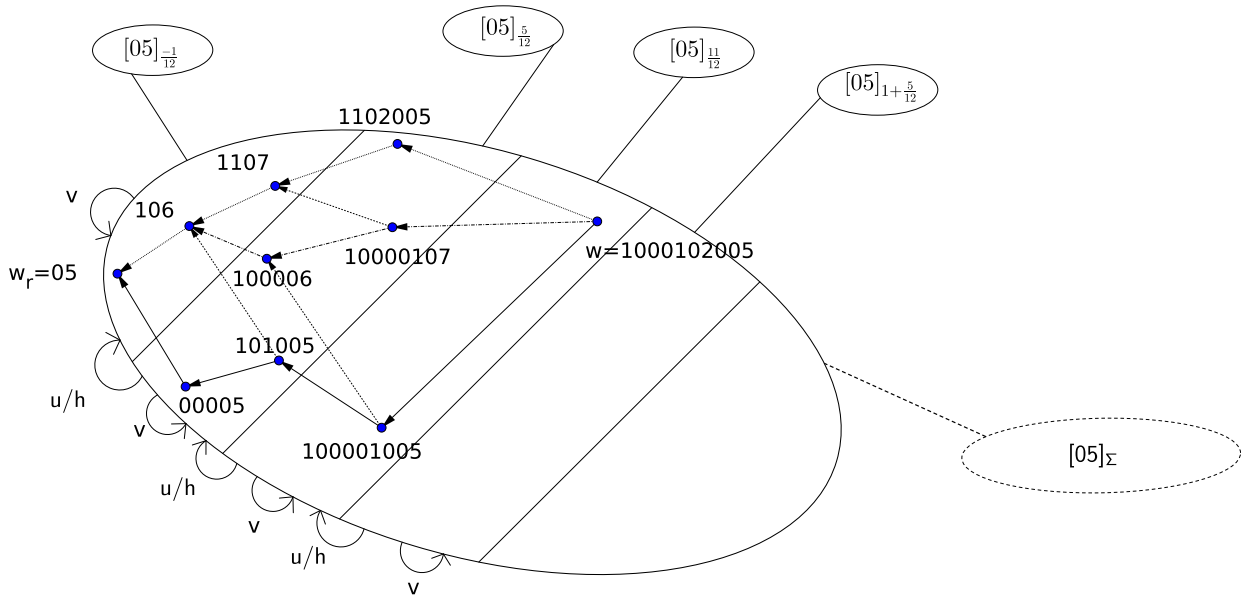
Preuve : C'est clair avec la proposition (I.69) et la définition du morphisme d'indice.
Pour tous w et w' de $\Sigma^* \supset B^*$, si $w \to_{\mathsf{v}} w'$ alors $Ind(w) = Ind(w')$.
Pour tous w et w' de $\Sigma^* \supset B^*$, si $w \to_{\mathsf{h}} w'$ ou $w \to_{\mathsf{u}} w'$ alors $Ind(w) = Ind(w') + \frac{1}{2}$.

□

Remarque III.5 *Un sous-ensemble $[w_r]_{\Sigma,n}$ (respectivement $[w_r]_{B,n}$) est stable par réduction v et par la relation d'équivalence $\sim_{\mathsf{v}}$ engendrée par v.*

La réduction $\mathsf{h}(w)$ ou $\mathsf{u}(w)$ d'un mot w de $[w_r]_{\Sigma,n}$ est un mot de $[w_r]_{\Sigma,n-\frac{1}{2}}$ et l'expansion $H(w)$ ou $V(w)$ d'un mot w de $[w_r]_{\Sigma,n}$ est un mot de $[w_r]_{\Sigma,n+\frac{1}{2}}$.

FIGURE III.1 – Partition de la classe $[05]_\Sigma$ en sous-ensembles $[05]_n$ pour $n \in \frac{-1}{12} + \frac{\mathbb{N}}{2}$.



Exemple III.6 *Plusieurs réductions maximales du mot $w = 1000102005$ d'indice $\frac{11}{12}$ au mot réduit $w_r = 05$ d'indice $\frac{-1}{12}$ sont proposées dans l'exemple(I.68). Elles sont illustrées sur la figure (1) et montrent différentes façons de réduire w vers w_r dans les sous-ensembles $[w_r]_n$, avec $n \in \frac{-1}{12} + \frac{1}{2}\mathbb{N}$.*

2 Demi-tour d'un vecteur de $\mathbb{R}^2$ par un mot du noyau de μ.

Dans ce chapitre, on donne une interprétation géométrique de l'indice pour les mots du noyau K_Σ (ou K_B).

Cela nécessite de travailler dans le plan euclidien dont la structure n'est évidemment pas préservée par le groupe $SL_2(\mathbb{Z})$.

On utilise la structure euclidienne. Le choix d'un vecteur non nul e de ce plan euclidien permet d'associer un angle $\theta_e(w)$ de $\mathbb{R}$ à un mot w de Σ^*. Cet angle $\theta_e(w)$ dépend généralement du choix du vecteur e, sauf pour les mots w du noyau où l'angle $\theta_e(w)$ ne dépend plus du choix du vecteur e. On obtient de cette façon une fonction $\theta = \theta_e : K_\Sigma \to \mathbb{R}$. Plus précisément, on obtient :

$$\theta(w) = 2\pi Ind(w),$$

pour tout mot w du noyau.

2.1 Définitions de θ_e.

Dans cette partie, on se place dans le plan euclidien usuel $\mathbb{R}^2$.

Définition III.7 *Soit $\tilde{\mu}$ l'application de $\Sigma^* = \mathbb{N}$ dans $SL_2(\mathbb{Z})$ définie par $\tilde{\mu}(a) = \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix}$.*

Remarque III.8

- *Pour tout entier a, l'inverse de $\tilde{\mu}(a)$ est donné par la matrice*

$$(\tilde{\mu}(a))^{-1} = \begin{pmatrix} a+1 & 1 \\ -1 & 0 \end{pmatrix}.$$

- *L'extension naturelle de l'application $\tilde{\mu}$ est l'application de Σ^* dans $SL_2(\mathbb{Z})$ donnée par :*

$$\begin{array}{rccc} \tilde{\mu} : & \Sigma^* & \longrightarrow & SL_2(\mathbb{Z}) \\ & w = a_1 a_2 \cdots a_n & \longmapsto & \tilde{\mu}(w) = \tilde{\mu}(a_1)\tilde{\mu}(a_2)\cdots\tilde{\mu}(a_n) \end{array}.$$

- *Le morphisme $\tilde{\mu}$ est un relèvement du morphisme μ défini de Σ^* dans $PSL_2(\mathbb{Z})$ (voir chapitre (II)).*

Pour tout vecteur non nul e de $\mathbb{R}^2$, o note $e^\perp = \begin{pmatrix} -y \\ x \end{pmatrix}$ le vecteur orthogonal à $e = \begin{pmatrix} x \\ y \end{pmatrix}$ tel que la base $(e, e^\perp)$ est directe.

Lemme III.9 *Soit $a \in \Sigma = \mathbb{N}$.*

L'angle orienté $\measuredangle(e, \tilde{\mu}(a)e)$ formé par un vecteur non nul e de $\mathbb{R}^2$ et son image par l'application linéaire $\tilde{\mu}(a)$ est dans l'intervalle $[-\frac{\pi}{2}, \frac{\pi}{2}]$.

Preuve :
Soit $e = \begin{pmatrix} x \\ y \end{pmatrix}$ un vecteur non nul de $\mathbb{R}^2$ et on note $e' = \tilde{\mu}(a)e = \begin{pmatrix} -y \\ x + (a+1)y \end{pmatrix}$.
Le produit scalaire $e' \cdot e = -xy + xy + (a+1)y^2 = (a+1)y^2$ est positif (éventuellement nul). Donc l'angle orienté $\measuredangle(e, e')$ est dans l'intervalle $[-\frac{\pi}{2}, \frac{\pi}{2}]$.

□

Définition III.10 *Soit e un vecteur non nul du plan vectoriel $\mathbb{R}^2$. On note θ_e l'application qui à un entier a associe l'angle algébrique $\theta_e(a)$ dans l'intervalle $[-\frac{\pi}{2}, \frac{\pi}{2}]$ défini par les vecteurs e et $\tilde{\mu}(a)e$:*

$$\begin{array}{rccl} \theta_e : & \Sigma & \longrightarrow & [-\frac{\pi}{2}, \frac{\pi}{2}] \\ & a & \longmapsto & \theta_e(a) = \measuredangle(e, \tilde{\mu}(a)e). \end{array}$$

Remarque III.11

1. *L'application θ_e est bien définie pour tout e non nul (voir lemme (III.9)).*
2. *L'extension naturelle de θ_e sur le monoïde libre est donnée par*

$$\begin{array}{rlcll} \theta_e : & \Sigma^* & \longrightarrow & \mathbb{R} & \\ & \emptyset & \longmapsto & 0 & \\ & w = (a_n, a_{n-1} \cdots a_1) & \longmapsto & \theta_e(w) = & \theta_e(a_1) + \theta_{\tilde{\mu}(a_1)e}(a_2) + \theta_{\tilde{\mu}(a_2 a_1)e}(a_3) \\ & & & & + \cdots + \theta_{\tilde{\mu}(a_{n-1} a_{n_2} \cdots a_1)e}(a_n) \end{array}.$$

3. *Le réel $\theta_e(w)$ est une mesure de l'angle $\measuredangle(e, \tilde{\mu}(w)e)$ (mod 2π).*
4. *Comme $\tilde{\mu}$ est linéaire, pour tout entier a et tout vecteur e de $\mathbb{R}^2$, on a :*

$$\theta_{-e}(a) = \theta_e(a).$$

Dans cette partie, on démontre le résutat principal suivant :

Théoreme III.12 *Pour tout mot w du noyau K_{Σ^*} et pour tout vecteur non nul e, on a :*

$$\theta_e(w) = 2\pi Ind(w).$$

En particulier, $\theta_e(w)$ ne dépend pas du vecteur e et l'angle $\theta(w) = \theta_e(w)$ est dans $\pi\mathbb{Z}$.

La démonstration du théorème est l'objet de la section (2.4).

2.2 Invariance sous l'expansion V.

Dans cette section, on montre que pour tout vecteur e de $\mathbb{R}^2$, l'angle θ_e est invariant par expansion $V = (ab \to (a+1)0(b+1))$ (et par réduction $\mathsf{v} = (a+1)0(b+1) \to ab)$).

Définition III.13 *Le demi-plan fermé positif déterminé par un vecteur non nul e est le demi-plan fermé formé des vecteurs e' dont le produit scalaire $e.e'$ avec e est positif ou nul.*

Pour tout vecteur e' dans le demi-plan fermé déterminé par e, l'angle $\measuredangle(e, e')$ est dans l'intervalle $[-\pi/2, \pi/2]$. On convient que $\measuredangle(e, 0) = 0$ et que le vecteur nul est dans le demi-plan fermé positif.

Le demi-plan ouvert positif déterminé par un vecteur non nul e est le demi-plan ouvert formé des vecteurs e' dont le produit scalaire $e.e'$ avec e est positif non nul.

Pour tout vecteur e' dans le demi-plan ouvert déterminé par e, l'angle $\measuredangle(e, e')$ est dans l'intervalle $]-\pi/2, \pi/2[$. Le vecteur nul n'est pas dans le demi-plan ouvert positif.

Proposition III.14 *Pour tout vecteur non nul e du plan $\mathbb{R}^2$, et tous entiers a et b, on a :*

$$\tilde{\mu}((a+1)0(b+1)) = \tilde{\mu}(ab) \qquad \text{et} \qquad \theta_e((a+1)0(b+1)) = \theta_e(ab).$$

Preuve : La démonstration n'est pas difficile, mais assez calculatoire.

1. Par simple calcul matriciel, on montre que

$$\tilde{\mu}((a+1)0(b+1)) = \tilde{\mu}(ab) = \begin{pmatrix} -1 & -(b+1) \\ a+1 & (a+1)(b+1)-1 \end{pmatrix}.$$

2. Soit $e = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$. On note $(e_0, e_1, e_2, e_3) = (e, \tilde{\mu}(b+1)e, \tilde{\mu}(0(b+1))e, \tilde{\mu}((a+1)0(b+1))e)$ et $(e_0, f_1, f_2) = (e, \tilde{\mu}(b)e, \tilde{\mu}(ab)e)$. Ainsi, on a :
   - $e_1 = \tilde{\mu}(b+1)e = \begin{pmatrix} -y \\ x+(b+2)y \end{pmatrix}$,
   - $e_2 = \tilde{\mu}(0(b+1))e = \tilde{\mu}(0)e_1 = \begin{pmatrix} -x-(b+2)y \\ x+(b+1)y \end{pmatrix}$,
   - $e_3 = \tilde{\mu}((a+1)0(b+1))e = \begin{pmatrix} -x-(b+1)y \\ (a+1)x+[(a+1)(b+1)-1]\,y \end{pmatrix} = \tilde{\mu}(ab)e = f_2$,
   - et $f_1 = \tilde{\mu}(b)e = \begin{pmatrix} -y \\ x+(b+1)y \end{pmatrix}$.

   On montre que le vecteur e_0 est dans le demi-plan fermé défini par le vecteur f_1 et les vecteurs e_1, e_2 et e_3 sont dans le demi-plan ouvert positif défini par le vecteur f_1 en calculant leurs produits scalaires avec f_1 :

- $f_1.e_0 = -xy + xy + (b+1)y^2 = (b+1)y^2 \geq 0$,
- $f_1.e_1 = y^2 + x^2 + (2b+3)xy + (b+1)(b+2)y^2 = (x + \frac{2b+3}{2}y)^2 + \frac{3}{4}y^2 > 0$,
- $f_1.e_2 = y^2 + x^2 + (2b+3)xy + (b+1)(b+2)y^2 = (x + \frac{2b+3}{2}y)^2 + \frac{3}{4}y^2 > 0$,
- $f_1.e_3 = (a+1)x^2 + 2(a+1)(b+1)xy = (a+1)(b+1)^2y^2 = (a+1)\big(x+(b+1)y\big)^2 > 0$.

Donc tous ces vecteurs sont dans un même demi-plan fermé, et seul le vecteur e_0 peut être sur la frontière du demi-plan.

Donc, les mesures de l'angle $\measuredangle(e_0, e_3)$ données par les sommes $\measuredangle(e_0, e_1) + \measuredangle(e_1, e_2) + \measuredangle_(e_2, e_3)$ et $\measuredangle(e_0, f_1) + \measuredangle(f_1, e_3))$ sont dans l'intervalle $]-\pi, \pi[$. Donc les réels $\theta_e((a+1)0(b+1))$ et $\theta_e(ab)$, représentant l'angle $\measuredangle(e_0, e_3)$, sont égaux.

□

Corollaire III.15 *Pour tout vecteur $e \in \mathbb{R}^2$, la réduction v (et l'expansion V) sur un mot w de Σ^* ne modifie pas l'angle $\theta_e(w)$: pour tous mots w et w' de Σ^*,*

$$\textit{si } w \to_{\mathsf{v}} w' \textit{ alors } \theta_e(w) = \theta_e(w').$$

Preuve : On note $w = pabs$ et $w' = p(a+1)0(b+1)s$. On a :

$$\begin{aligned}
\theta_e(w') = \theta_e(p(a+1)0(b+1)s) &= \theta_e(s) + \theta_{\tilde{\mu}(s)e}((a+1)0(b+1) + \theta_{\tilde{\mu}((a+1)0(b+1))\tilde{\mu}(s)e}(p) \\
&= \theta_e(s) + \theta_{\tilde{\mu}(s)e}(ab) + \theta_{\tilde{\mu}(abs)e}(p) \\
&= \theta_e(pabs) = \theta_e(w).
\end{aligned}$$

□

2.3 Comportement de θ_e avec l'expansion H.

Dans cette section, on montre que le mot 000 "fait tourner" d'un demi-tour positivement tout vecteur e du plan $\mathbb{R}^2$.

Ainsi, pour tout vecteur $e \in \mathbb{R}^2$, l'angle $\theta_e(w)$ d'un mot w augmente de π par l'expansion H. Le vecteur $\tilde{\mu}(H(w))e$ est obtenu en "ajoutant un demi-tour" au vecteur $\tilde{\mu}(w)e$.

Lemme III.16

Pour tout vecteur non nul e du plan vectoriel $\mathbb{R}^2$, on a :

$$\theta_e(0) \in]0, \frac{\pi}{2}].$$

Preuve : Soit $e = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$. On a et $e' = \tilde{\mu}e = \begin{pmatrix} -y \\ x+1y \end{pmatrix}$.

Le produit scalaire $e' \cdot e^{\perp} = y^2 + x^2 + xy = \frac{1}{2}((x+y)^2 + x^2 + y^2)$ est strictement positif.

Donc l'angle orienté $\measuredangle(e, e')$ est dans l'intervalle $]0, \pi[$. Donc $\theta_e(0) \in]0, \frac{\pi}{2}]$ (voir lemme (III.9)).

□

Proposition III.17 *Pour tout vecteur non nul e du plan $\mathbb{R}^2$, on a :*

$$\tilde{\mu}(000) = -I \qquad \text{et} \qquad \theta_e(000) = \pi.$$

Preuve : On note $(e_0, e_1, e_2, e_3) = (e, \tilde{\mu}(0)e, \tilde{\mu}(00)e, \tilde{\mu}(000)e)$.

- Par simple calcul matriciel, on obtient $\tilde{\mu}(000) = -I$. Donc $e_3 = \tilde{\mu}(000)e = -e$ et le réel $\theta_e(000)$, qui mesure l'angle $\measuredangle(e_0, e_3)$, est dans $\pi + 2\mathbb{Z}\pi$.
- D'après le lemme (III.16), les angles orientés $\theta_e(0) = \measuredangle(e_0, e_1)$, $\theta_{e_1}(0) = \measuredangle(e_1, e_2)$ et $\theta_{e_2}(0) = \measuredangle(e_2, e_3)$ sont dans l'intervalle $]0, \frac{\pi}{2}]$. Donc l'angle $\theta_e(000) = \measuredangle(e_0, e_3) = \measuredangle(e_0, e_1) + \measuredangle(e_1, e_2) + \measuredangle(e_2, e_3)$ est dans l'intervalle $]0, \frac{3\pi}{2}]$.

Finalement, $\theta_e(000) = \pi$.

□

Remarque III.18 *On peut réaliser l'application linéaire $\tilde{\mu}(000)$ par déformation continue d'un vecteur e de $\mathbb{R}^2$ dans le sens positif d'un angle π. On dit que le vecteur e tourne d'un demi-tour par le mot* 000.

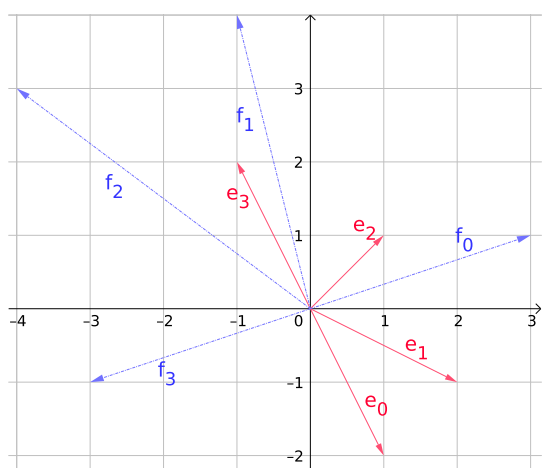


FIGURE III.2 – $(\tilde{\mu}_{e_0}(0), \tilde{\mu}_{e_0}(00), \tilde{\mu}_{e_0}(000)) = (e_1, e_2, e_3)$ avec $e_0 = (1, -2)$ et $(\tilde{\mu}_{f_0}(0), \tilde{\mu}_{f_0}(00), \tilde{\mu}_{f_0}(000)) = (f_1, f_2, f_3)$ avec $f_0 = (3, 1)$: les vecteurs e_0 et f_0 tournent d'un demi-tour par le mot 000.

Corollaire III.19 *Pour tout vecteur $e \in \mathbb{R}^2$ et tous mots w et w' de Σ^*, on a :*

$$\textit{si } w \to_H w' \textit{ alors } \theta_e(w') = \theta_e(w) + \pi.$$

Preuve : On note $w = ps$ et $w' = p000s$. On a :

$$\begin{aligned}\theta_e(w') = \theta_e(p000s) &= \theta_e(s) + \theta_{\tilde{\mu}(s)e}(000) + \theta_{\tilde{\mu}(000s)e}(p)\\ &= \theta_e(s) + \pi + \theta_{-\tilde{\mu}(s)e}(p)\\ &= \theta_e(s) + \pi + \theta_{\tilde{\mu}(s)e}(p)\\ &= \theta_e(ps) + \pi = \theta_e(w) + \pi.\end{aligned}$$

□

2.4 Démonstration du théorème III.12.

Les résultats intermédiaires des sections 2.2 et 2.3 sur les expansions V et H permettent de montrer simplement le théorème III.12 en comptant le nombre d'expansions H du mot vide vers un mot w du noyau K_Σ :

Preuve du théorème III.12 :

D'après les corollaires (III.15) et (III.19), pour tout vecteur e du plan $\mathbb{R}^2$, si un mot w est obtenu avec n_v expansions V et n_H expansion H sur un mot w' alors $\theta_e(w) = \theta_e(w') + n_H\pi$.

Or, pour tout vecteur e de $\mathbb{R}^2$, on a $\theta_e(\emptyset) = 0$ et tout mot w du noyau K_{Σ^*} s'obtient à partir du mot vide avec $2Ind(w)$ expansions H (voir poposition II.18)). D'où $\theta_e(w) = 2\pi Ind(w)$.

□

2.5 Remarques et compléments.

Sur l'alphabet B^*, l'effet de rotation par les applications $\tilde{\mu}(a)$ (avec $a \in \{0,1\}$), d'une demi-droite $e\mathbb{N}$, dirigée par un vecteur non nul e, est plus clair.

Dans cette section, on montre que sur l'alphabet B, pour toute lettre $a \in \{0,1\}$, une demi-droite dirigée par un vecteur non nul e tourne dans le sens positif d'un angle positif dans l'intervalle $]0, \frac{\pi}{2}]$, alors que sur l'alphabet Σ, parfois, la demi-droite tourne d'un angle négatif.

Par exemple, pour le vecteur $e = \begin{pmatrix}1\\-1\end{pmatrix}$, on a $e' = \tilde{\mu}(2)e = \begin{pmatrix}1\\-2\end{pmatrix}$ et $e^\perp.e' = -4 < 0$. Donc $\theta_e(2)$ est dans l'intervalle $[-\frac{\pi}{2}, 0[$. La demi-droite $e\mathbb{N}$ ne tourne pas dans le sens positif par l'application linéaire $\tilde{\mu}(2)$.

Le lemme (III.16) montre que pour tout vecteur e, la demi-droite $\tilde{\mu}(0)e\mathbb{N}$ est l'image de la demi-droite $e\mathbb{N}$ par une rotation d'angle $\theta_e(0) \in]0, \frac{\pi}{2}]$.

Pour la lettre 1, on a :

Lemme III.20

Pour tout vecteur non nul e du plan vectoriel $\mathbb{R}^2$, on a :

$$\theta_e(1) \in [0, \frac{\pi}{2}].$$

Preuve : On note $e = \begin{pmatrix} x \\ y \end{pmatrix}$ et $e' = \tilde{\mu}(1)e = \begin{pmatrix} -y \\ x+2y \end{pmatrix}$ de $\mathbb{R}^2 \setminus \{0,0\}$.

Le produit scalaire $e' \cdot e^{\perp} = y^2 + x^2 + 2xy = (x+y)^2$ est positif (éventuellement nul).

Donc l'angle orienté $\measuredangle(e, e')$ admet un représentant dans l'intervalle $[0, \pi]$.

Donc $\theta_e(1) \in [0, \frac{\pi}{2}]$ (voir lemme (III.9)).

□

Ainsi, pour tout mot w de B^*, et tout vecteur non nul e de $\mathbb{R}^2$, la demi-droite $e\mathbb{N}$ tourne dans le sens positif d'un angle $\theta_e(w)$.

Et d'après le théorème III.12, pour tout mot w du noyau K_{B^*}, et tout vecteur non nul e de $\mathbb{R}^2$, la demi-droite $e\mathbb{N}$ tourne dans le sens positif d'un angle $2\pi Ind(w)$.

3 Indice et tour d'une tresse de B_3.

Dans cette partie, l'indice d'un mot est interprété dans le groupe des tresses. On associe une tresse à trois brins aux générateurs $a \in \mathbb{N}$ de Σ^*. Dans ce contexte, l'indice d'un mot du noyau de $\mu_{|B^*}$ correspond au nombre de tours de la tresse centrale associée.

Plus généralement, on montre que l'indice d'un mot correspond à son image dans l'abélianisé $B_3^{ab} = B_3/D(B_3)$ du groupe des tresses à trois brins.

3.1 Définitions.

Définition III.21 *Soit $\mathcal{P} = \{P_1, \ldots, P_n\}$ un ensemble de n points du disque unité ouvert de $\mathbb{C}$.*

Un brin est le graphe d'une application b continue de $[0,1]$ dans le disque unité ouvert de $\mathbb{C}$, dont les extrémités $b(0)$ et $b(1)$ appartiennent à $\mathcal{P}$.

Une tresse géométrique à n brins est la réunion de n brins disjoints.

Une tresse est l'ensemble des tresses géométriques équivalentes par déformations des brins et de leurs extrémités sans décrocher leurs extrémités et sans que les brins ne se traversent.

Un diagramme de tresse (ou représentation) est la projection des brins de l'espace $\mathbb{R}^3$ d'une tresse sur le plan. On dit que deux diagrammes sont équivalents (ou isotopes) s'ils représentent la même tresse.

Dans la suite, on ne considérera que des tresses à 3 brins.

Définition III.22 *Le groupe des tresses à 3 brins, noté B_3, est donné par la présentation de groupe $\langle\{\sigma_1,\sigma_2\}|\sigma_1\sigma_2\sigma_1=\sigma_2\sigma_1\sigma_2\rangle$, où les générateurs σ_1 et σ_2 sont représentés par les diagrammes de tresse suivant :*

$\sigma_1 =$ et $\sigma_2 =$

Les inverses σ_1^{-1} et σ_2^{-1} des générateurs sont représentés par :

$\sigma_1^{-1} =$ et $\sigma_2^{-1} =$

Remarque III.23 *Une tresse désigne une classe d'équivalence de mots et un diagramme de tresse (ou représentation) désigne un mot de cette classe d'équivalence.*

Définition III.24 *La tresse unitée est la tresse triviale sans croisement.*

Une représentation de tresse est positive si elle ne comporte aucun σ_i^{-1}. Une tresse est positive si elle admet une représentation positive.

L'ensemble des tresses positives, dont l'élement neutre est la tresse triviale, forment un monoïde noté B_n^+. Le monoïde des tresses positives à trois brins admet la présentation de monoïde

$$B_3^+ = \langle\{\sigma_1,\sigma_2\}|\sigma_1\sigma_2\sigma_1=\sigma_2\sigma_1\sigma_2\rangle.$$

Définition III.25 *La tresse de Garside à trois brins, définie par $\Delta_3=\sigma_1\sigma_2\sigma_1$ correspond à un diagramme où les 3 brins font un demi-tour positif (voir figure III.3)).*

Le centre C du groupe des tresses B_3 est l'ensemble des tresses qui commutent avec les tresses de B_3. Le centre C est le sous-groupe engendré par Δ_3^2.

Une tresse centrale est une tresse de C.

3.2 De $B^*=\{0,1\}^*$ vers B_3^+.

Définition III.26 *Soit $\tilde{\mu}^{B_3}$ l'extension naturelle sur $B^*=\{0,1\}^*$ de l'application de $\{0,1\}$ dans le monoïde des tresses positives à trois brins B_3^+ définie par*

$$\begin{array}{rcccl} \tilde{\mu}^{B_3} & : & B^* & \longrightarrow & B_3^+ \\ & & 0 & \longmapsto & \sigma_1\sigma_2 \\ & & 1 & \longmapsto & \sigma_1 \end{array}.$$

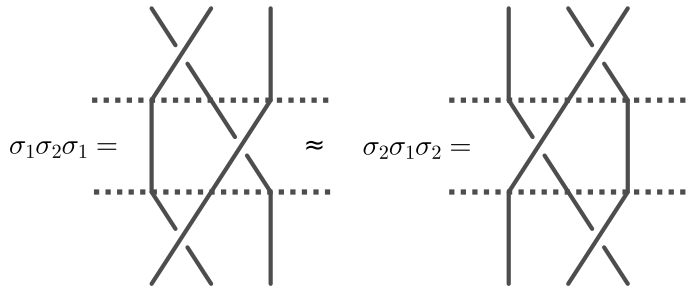
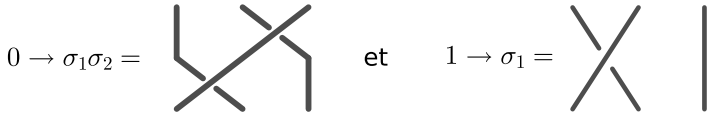


FIGURE III.3 – Les diagrammes de la tresse de Garside à 3 brins $\sigma_1\sigma_2\sigma_1$ et de la tresse $\sigma_2\sigma_1\sigma_2$ sont isotopes. Les trois brins font 1 demi-tour positif.



Remarque III.27 *L'image de $\tilde{\mu}^{B_3}$ est le sous-monoïde de B_3^+ engendré par σ_1 et $\sigma_1\sigma_2$.*

Proposition III.28 *La tresse $\tilde{\mu}^{B_3}(0^3) = (\sigma_1\sigma_2)^3$ associée au mot 000 est la tresse positive centrale Δ_3^2 qui fait 1 tour et qui engendre le centre C.*

Preuve : On a :

$$\tilde{\mu}^{B_3}(000) = (\sigma_1\sigma_2)^3 = (\sigma_1\sigma_2\sigma_1)(\sigma_2\sigma_1\sigma_2) = (\sigma_1\sigma_2\sigma_1)^2 = \Delta_3^2$$

où Δ_3 est la tresse de Garside à 3 trois brins (voir définition (III.3)).

La tresse fait deux demi-tours. Les brins reviennent à leurs positions initiales respectives.

□

Proposition III.29 *La réduction r est compatible avec le morphisme $\tilde{\mu}^{B_3}$.*

Preuve : On a : $\tilde{\mu}^{B_3}(101) = \sigma_1(\sigma_1\sigma_2)\sigma_1 = \sigma_1(\sigma_1\sigma_2\sigma_1) = (\sigma_1\sigma_2\sigma_1)\sigma_2 = (\sigma_1\sigma_2)^2 = \tilde{\mu}^{B_3}(00)$.

□

Proposition III.30 *La tresse à trois brins associée à un mot w du noyau de $\mu_{|B^*}$ est une tresse centrale.*

Le nombre de tour de la tresse associée est $2Ind(w)$.

Preuve : L'expansion H augmente le nombre de tours de 1 tour et l'expansion V ne modifie pas la tresse associée.

Le mot vide est associée à la tresse triviale à 0 tour.

Les mots du noyau sont obtenus à partir du mot vide avec $2Ind(w)$ expansions H et $\frac{1}{2}\sigma(w)$ expansions V (voir proposition (I.69)).

D'où le résultat.

□

3.3 Extension du morphisme $\tilde{\mu}^{B_3}$ sur Σ^*.

Le morphisme $\tilde{\mu}^{B_3}$ s'étend naturellement à Σ^* en posant

$$\tilde{\mu}^{B_3}(a) = \sigma_1\sigma_2^{1-a}.$$

La réduction v sur Σ^* est compatible avec le morphisme $\tilde{\mu}^{B_3}$. On a :

$$\tilde{\mu}^{B_3}((a{+}1)0(b{+}1)) = \sigma_1\sigma_2^{1-a-1}(\sigma_1\sigma_2)\sigma_1\sigma_2^{1-b-1} = \sigma_1\sigma_2^{1-a-1}(\sigma_2\sigma_1\sigma_2)\sigma_2^{1-b-1} = \sigma_1\sigma_2^{1-a}\sigma_1\sigma_2^{1-b} = \tilde{\mu}^{B_3}(ab).$$

La réduction u enlève un tour $(\sigma_1\sigma_2)^3$ à la tresse associée. En effet, on a :

$$\begin{aligned} \tilde{\mu}^{B_3}(a00b) &= \sigma_1\sigma_2^{1-a}(\sigma_1\sigma_2)(\sigma_1\sigma_2)\sigma_1\sigma_2^{1-b} = \sigma_1\sigma_2^{1-a}(\sigma_1\sigma_2)^3\sigma_2^{-b} \\ \text{et} \\ \tilde{\mu}^{B_3}(a+b) &= \sigma_1\sigma_2^{1-a-b}. \end{aligned}$$

Remarque III.31 *Pour tout mot w de Σ^*, la tresse $\tilde{\mu}^{B_3}$ appartient aux tresses positives au sens de P. Dehornoy (voir [D]).*

3.4 Indice et abélianisé de B_3.

Le morphisme d'indice de Σ^* dans $\frac{1}{12}\mathbb{Z}$ est donné par

$$Ind(w) = \frac{1}{12}\big(2\lambda(w) - \sigma(w)\big)$$

où λ est la longueur et σ est le morphisme somme. En particulier, pour tout générateur $a \in \Sigma = \mathbb{N}$, on a :

$$Ind(a) = \frac{2-a}{12}.$$

Dans cette partie, on explicite la relation entre le morphisme d'indice et l'abélianisé B_3^{ab} du groupe des tresses à 3 brins.

Définition III.32

Le commutateur de deux éléments g et h d'un groupe G est l'élément $[g,h] = ghg^{-1}h^{-1}$.

Le groupe dérivé d'un groupe G, noté $D(G)$ est le sous-groupe de G engendré par l'ensemble des commutateurs de G :

$$D(G) = \{ghg^{-1}h^{-1}, g, h \in G\}.$$

Le groupe dérivée est un sous-groupe normal et l'abélianisé d'un groupe G est le quotient $G/D(G)$.

L'image d'un élément g de G dans $G/D(G)$ est appelé l'abélianisé de g.

Définition III.33 *On note α le morphisme de groupe de B_3 dans $\mathbb{Z}$ défini sur les générateurs σ_1 et σ_2 de B_3 par*

$$\alpha(\sigma_1) = \alpha(\sigma_2) = 1.$$

Remarque III.34 *Le morphisme α est bien défini : la relation $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ du groupe des tresses B_3 est compatible avec le morphisme α.*

Il est clair que α est surjectif : pour tout entier $n \in \mathbb{Z}$, on a $\alpha(\sigma_1^n) = n$.

Proposition III.35

Le noyau de α est le groupe dérivé $D(B_3)$ du groupe des tresses à trois brins.

Le morphisme α est un morphisme d'abélianisation du groupe des tresses à 3 brins.

L'abélianisé $B_3^{ab} = B_3/D(B_3)$ du groupe des tresses à trois brins est isomorphe à $\mathbb{Z}$.

Preuve :

Il est clair que l'image d'un élément du commutateur par α est nul et $D(B_3) \subset Ker(\alpha)$.

D'après la relation du groupe B_3, on a : $\sigma_1\sigma_2^{-1} = \sigma_2^{-1}\sigma_1^{-1}\sigma_2\sigma_1$. Donc $\sigma_1\sigma_2^{-1}$ (et son inverse $\sigma_2\sigma_1^{-1}$) est dans le groupe dérivé. De même, $\sigma_1^{-1}\sigma_2$ et $\sigma_2^{-1}\sigma_1$ sont dans $D(B_3)$.

Une tresse W non triviale dans le noyau de α admet autant de facteurs de l'ensemble $\{\sigma_1, \sigma_2\}$ que de facteurs de l'ensemble $\{\sigma_1^{-1}, \sigma_2^{-1}\}$. Donc au moins deux facteurs de chacun de ces ensembles sont consécutifs. Ainsi, une tresse W de $Ker(\alpha)$ s'écrit sous la forme $W = pUs$ avec $ps \in Ker(\alpha)$ et $U \in \{\sigma_1\sigma_2^{-1}, \sigma_2\sigma_1^{-1}, \sigma_1^{-1}\sigma_2, \sigma_2^{-1}\sigma_1\} \subset D(G)$.

Par récurrence sur la longueur de W, on conclut que W est dans le groupe dérivé.

□

Remarque III.36

Comme $\sigma_1 = (\sigma_1\sigma_2^{-1})\sigma_2$, les deux générateurs σ_1 et σ_2 sont dans la même classe d'équivalence modulo le groupe dérivé $D(B_3)$.

Proposition III.37 *Pour tout mot w de Σ^*, l'entier $12Ind(w)$ correspond à l'abélianisé $\alpha \circ \tilde{\mu}^{B_3}(w)$ de la tresse $\tilde{\mu}^{B_3}(w)$.*

Preuve : Pour tout générateur a de Σ^*, on a :

$$\alpha \circ \tilde{\mu}^{B_3}(a) = \alpha(\sigma_1 \sigma_2^{1-a}) = 2 - a = 12Ind(a).$$

$\square$

Chapitre IV

Modèle binaire : du noyau K_B vers les nombres de Catalan

Dans ce chapitre, on étudie les mots du noyau K_B du morphisme surjectif $\mu_{|B^*}$ (voir proposition II.7) défini par :

$$\begin{array}{rccl} \mu_{|B^*}: & B^* & \longrightarrow & PSL_2(\mathbb{Z}) \\ & 0 & \longmapsto & U = \pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \\ & 1 & \longmapsto & USU = \pm\begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \quad \text{avec } S = \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in PSL_2(\mathbb{Z}). \end{array}.$$

Le noyau K_B est la classe d'équivalence $[\emptyset]_B$ (ou simplement $[\emptyset]$) du mot vide pour la relation d'équivalence $\sim_B$ engendrée par les réductions $\mathsf{v} = (101 \to 00)$ et $\mathsf{h} = (\emptyset \to 000)$ (voir proposition (II.14)).

Le noyau K_B est stable par concaténation, par réductions v et h (et par expansions $V = \mathsf{v}^{-1} = (00 \to 101)$ et $H = \mathsf{h}^{-1} = (000 \to \emptyset)$) et par permutations circulaires.

Il est partionné en sous-ensemble $[\emptyset]_{\frac{n}{2}}$, pour $n \in \mathbb{N}$, par le morphisme d'indice

$$\begin{array}{rccl} Ind_{|B^*}: & B^* = \{0,1\}^* & \longrightarrow & \mathbb{Z}/12 \\ & w & \longmapsto & Ind(w) = \dfrac{1}{12}\left[2\lambda(w) - \sigma(w)\right]. \end{array}$$

Sont répertoriés ci-dessous, les premiers mots du noyaux K_B à indice et longueur fixés :

Ind	λ	σ	Mots de K_B de longueur λ et d'indice Ind	Nombre de mots	$card([\emptyset]_{Ind})$
0	0	0	$\emptyset$	1	1
1/2	3	0	000	1	3
	4	2	$0101, 1010$	2	
1	6	0	$(000)^2$	1	21
	7	2	1010000, 0101000, 0010100, 0001010, 0000101, 0100001, 1000010	7	
	8	4	10110100, 10101010, 10100101, 01011010, 01010101, 00101101, 11010010, 10010110, 01101001, 01001011	10	
	9	6	$101101101, 1101101110, 011011011$	3	
3/2	9	0	$(000)^3$	1	191
	10	2	1010^7, 01010^6, 0^21010^5, 0^31010^4, 0^41010^3, 0^51010^2, 0^61010, 0^7101, 10^410^4, 010^410^3, $0^210^410^2$, 0^310^410 0^410^41, 10^710, 010^71	15	
	...	...	...	...	

Pour tout entier k, le mot $(000)^k$ est le mot du noyau K_B d'indice $\frac{k}{2}$ de somme minimale (et de longueur minimale $3k$). L'ensemble des mots du noyau d'indice $\frac{k}{2}$ est stable par réduction v et par expansion $V = \mathsf{v}^{-1}$. Mais la relation de réduction $\mathsf{v} = (101 \to 00)$ n'est pas confluente (voir remarque (II.15)) et les éléments d'indice $\frac{k}{2}$ ne sont généralement pas engendrés par l'expansion R sur le mot de longueur minimal. Ils sont obtenus récursivement à partir des mots d'indices inférieurs sur lesquels on effectue n expansions H, ce qui augmentent l'indice de $\frac{n}{2}$ et éventuellement d'autres expansions V.

Dans l'objectif de dénombrer les mots du noyau, on focalise sur les mots de B^* de l'image réciproque du sous-groupe cyclique d'ordre 3 engendré par $U = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. On appelle ces mots des châteaux. On définit une factorisation canonique DD des châteaux avec des facteurs "premiers" : la douve 0 et l'ensemble $\mathcal{D}$ des donjons.

Un donjon est un mot particulier de la forme $1v1$, d'indice dans $\frac{1}{6}(3\mathbb{N}+2)$. En remplaçant un facteur 101 d'un mot par un autre donjon, on construit des mots d'indices supérieurs qui ne sont pas équivalents modulo v au mot de longueur minimale $(000)^k$.

L'ensemble des châteaux d'indice donné $\frac{n}{6}$ est fini ; cet ensemble admet des mots maximaux de longueur maximale (et de somme maximale). On montre que les zéros des châteaux

maximaux sont isolés et on note, en notation condensée, les châteaux maximaux par la suite d'entiers donnant les longueurs des blocs de 1 consécutifs.

À permutation près, les châteaux maximaux d'indice $\frac{n}{6}$ sont en bijection avec l'ensemble des arbres $3-$réguliers à $2n+2$ sommets. Les mots du noyau peuvent alors être considérés comme des arbres $3-$réguliers muni d'une décoration servant à indiquer le début des mots circulaires correspondants. On montre que l'ensemble des mots maximaux du noyau d'indice $\frac{3k+3}{6}$ est dénombré par la somme $c_k + c_{k+1}$ des deux nombres de Catalan consécutifs c_k et c_{k+1}.

Ci-dessous sont énumérées les premiers mots maximaux dans le noyau K_B en notation condensée :

Indice	λ	σ	Mots Maximaux d'indice Ind	$card(K_{\frac{3k+3}{6}})$
$1/2$	4	2	$110, 011$	$C_0 + C_1 = 2$
1	9	6	$2220, 1221, 0222$	$C_1 + C_2 = 3$
$3/2$	14	10	32320, 23230, 22321 13231, 12322, 03232, 02323	$C_2 + C_3 = 7$
2	19	14	423320, 332420, 324230, 323321, 242330, 233240, 232421, 224231, 223322, 142331, 133241, 132422, 124232, 123323, 042332, 033242, 032423, 024233, 023324	$C_3 + C_4 = 19$
$5/2$	24	18	...	$C_4 + C_5 = 56$
$n/2$	$5n-1$	$4n-2$	...	$C_{n-1} + C_n$

Dans la dernière partie, on étudie des permutations circulaires selon une base W d'un sous-monoïde W^* du noyau K_B. On montre qu'un château maximal du noyau K_B est soit simple, soit un carré (de la forme p^2), soit un cube (de la forme p^3). Pour $W = B = \{0, 1\}$, On dénombre les orbites simples, les orbites carrées et les orbites cubes des sous-ensembles de mots d'indice $\frac{3k+3}{6}$, et on obtient pour $0 \leq k \leq 7$:

k	Ind	λ	Nombre d'orbites simples	Nombre d'orbites carrées	Nombre d'orbites cubes	Nombre total d'orbites	$card(K_{\frac{3k+3}{6}})$
0	1/2	4	0	1	0	1	2
1	1	9	0	0	1	1	3
2	3/2	14	0	1	0	1	7
3	2	19	1	0	0	1	19
4	5/2	24	1	2	1	4	56
5	3	29	6	0	0	6	164
6	7/2	34	14	5	0	19	561
7	4	39	47	0	2	49	1859

1 Définitions préliminaires et représentations.

Dans cette partie, on introduit l'ensemble $\mathcal{C}$ des châteaux. Cette ensemble $\mathcal{C}$ contient le noyau K_B. On définit, dans l'ensemble $\mathcal{C}$ des châteaux, des mots particuliers, appelés douves et donjons. Ces mots jouent le rôle de facteurs premiers dans une factorisation unique appelée factorisation DD.

1.1 Châteaux et partition $(\mathcal{C}_k)_{k\in\frac{\mathbb{N}}{6}}$ de l'ensemble des châteaux.

Définition IV.1

L'ensemble des châteaux $\mathcal{C}$ est la pré-image $\mathcal{C} = \mu^{-1}_{|B^*}(\langle U\rangle)$ par le morphisme $\mu_{|B^*} : B^* \longrightarrow PSL_2(\mathbb{Z})$ du sous-groupe cyclique $\langle U\rangle$ d'ordre 3 de $PSL_2(\mathbb{Z})$.

Remarque IV.2

1. *Tous les sous-groupes cycliques d'ordre 3 de $PSL_2(\mathbb{Z})$ sont conjugués à $\langle U\rangle$.*
2. *Le système de réécriture $\langle 0, 1|\mathsf{h}, \mathsf{v}\rangle$ est convergent (voir corollaire (II.14)). L'unique forme réduite d'un mot de $\mathcal{B}^*$ est dans l'ensemble :*

$$\textit{Réduit}_B = \{\emptyset, 0, 00\} \cup \{\emptyset, 0, 00\}\mathcal{L}'\{\emptyset, 0, 00\}$$

où $\mathcal{L}' = \bigcup k \in \mathbb{N}\{1(001)^k\}\Big(\bigcup_{k\in\mathbb{N}}\{1(001)^k\}\Big)^*$.

Les mots réduits s'écrivent sur l'alphabet $\{0, 00, 1(001)^k, k \in \mathbb{N}\}$. Leurs images par μ dans $PSL_2(\mathbb{Z})$ sont : $\mu(0) = \pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, $\mu(00) = \pm\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ et $\mu(1(001)^k) =$

$\pm\begin{pmatrix}0 & -1\\ 1 & k+2\end{pmatrix}$ *(voir remarque (II.12)).*

L'ensemble Réduit_B *des mots réduits est en bijection avec* $PSL_2(\mathbb{Z})$ *(voir proposition (II.13)).*

3. *L'ensemble* $\{[\emptyset],[0],[00]\}$ *est l'image réciproque de l'ensemble* $\{I,U,U^2\}$ *par l'isomorphisme* $\hat{\mu} : B^*/\sim_B \longrightarrow PSL_2(\mathbb{Z})$ *(voir proposition (II.10)). On a donc :*

$$\mathcal{C} = [\emptyset] \cup [0] \cup [00].$$

Les mots $\emptyset$, 0 *et* 00 *sont les seuls mots réduits qui sont des châteaux.*

4. *Tout château admet une réduction maximale à un mot de l'ensemble* $\{\emptyset, 0, 00\}$ *avec* n_{v} *réductions* v *et* n_{h} *réductions* h *(voir proposition (I.69)).*

La somme d'un château est paire, égale à $2n_{\mathsf{v}}$.

On rappelle que le morphisme d'indice Ind est défini par (voir au chapitre (III)) :

$$\begin{array}{rccl} Ind: & B^* & \longrightarrow & \frac{1}{12}\mathbb{Z} \\ & w & \longmapsto & Ind(w) = \dfrac{1}{12}\left[2\lambda(w) - \sigma(w)\right]. \end{array}$$

Le nombre de réduction h *d'un mot* w *vers l'unique mot réduit* w_r *de sa classe d'équivalence est* $n_{\mathsf{h}} = 2Ind(w) - 2Ind(w_r)$. *Le morphisme d'indice partitionnne une classe d'équivalence* $[w_r]_B$, *représentée par son unique mot réduit* w_r, *en sous-ensembles* $[w_r]_{Ind(w_r)+\frac{n}{2}}$ *avec* $n \in \mathbb{N}$.

Pour les châteaux, comme $Ind(\emptyset) = 0$, $Ind(0) = \frac{1}{6}$ *et* $Ind(00) = \frac{1}{3}$, *on a :*

$$[\emptyset] = \bigcup_{k\in\mathbb{N}} \mathcal{C}_{\frac{0+3k}{6}} = \mathcal{C}_{\frac{0+3\mathbb{N}}{6}}, \quad [0] = \bigcup_{k\in\mathbb{N}} \mathcal{C}_{\frac{1+3k}{6}} = \mathcal{C}_{\frac{1+3\mathbb{N}}{6}} \quad \text{et} \quad [00] = \bigcup_{k\in\mathbb{N}} \mathcal{C}_{\frac{1+3k}{6}} = \mathcal{C}_{\frac{2+3k}{6}}.$$

On obtient la partition de l'ensemble des châteaux suivante :

$$\mathcal{C} = \mathcal{C}_{\frac{1}{6}(0+3\mathbb{N})} \cup \mathcal{C}_{\frac{1}{6}(1+3\mathbb{N})} \cup \mathcal{C}_{\frac{1}{6}(2+3\mathbb{N})} = \bigcup_{n\in\mathbb{N}} \mathcal{C}_{\frac{n}{6}} = \mathcal{C}_{\frac{\mathbb{N}}{6}}.$$

Chaque ensemble $\mathcal{C}_{\frac{n}{6}}$ *est stable par réductions* v *(et expansions* V*).*

La réduction $\mathsf{h}(w)$ *d'un château* w *de* $\mathcal{C}_{\frac{n}{6}}$ *est un château du sous-ensemble* $\mathcal{C}_{\frac{n-3}{6}}$, *et l'expansion* $H(w)$ *d'un château* w *de* $\mathcal{C}_{\frac{n}{6}}$ *est un château du sous-ensemble* $\mathcal{C}_{\frac{n+3}{6}}$.

Proposition IV.3 *Pour tout entier* n, *l'ensemble* $\mathcal{C}_{\frac{n}{6}}$ *est fini.*

Preuve : Sur l'alphabet binaire $\{0,1\}$, la somme $\sigma(w)$ d'un mot w est majorée par sa longueur $\lambda(w)$. Or $Ind(w) = \frac{1}{12}\left[2\lambda(w) - \sigma(w)\right]$, donc $2\lambda(w) = 12Ind(w) + \sigma(w) \leq 12Ind(w) + \lambda(w)$.

Donc, à indice $Ind(w) = \frac{n}{6}$ fixé, la longueur est majorée par

$$\lambda(w) \leq 12 Ind(w) = 2n.$$

□

Exemple IV.4 *Pour $n \leq 4$, les sous-ensembles $\mathcal{C}_{\frac{n}{6}}$ sont :*
$\mathcal{C}_{\frac{0}{6}} = \{\emptyset\}$, *de cardinal* 1,
$\mathcal{C}_{\frac{1}{6}} = \{0\}$, *de cardinal* 1,
$\mathcal{C}_{\frac{2}{6}} = \{00, 101\}$, *de cardinal* 2,
$\mathcal{C}_{\frac{3}{6}} = \{000, 1010, 0101\}$, *de cardinal* 3,
$\mathcal{C}_{\frac{4}{6}} = \{0000, 10100, 01010, 00101, 101101\}$, *de cardinal* 5.

Remarque IV.5 *La classe $\mathcal{C}_{\frac{n}{6}}$ est stable par réductions v et par expansions V. Mais tous les mots de la classe $\mathcal{C}_{\frac{n}{6}}$ ne s'obtiennent généralement pas par des expansions V sur le mot 0^n de longueur minimal de la classe, du fait que la réduction v n'est pas confluente sur la classe $\mathcal{C}_{\frac{n}{6}}$ (voir remarque II.15)).*

Par exemple, le mot $10101010^{n-5} \in \mathcal{C}_{\frac{n}{6}}$ se réduit vers les deux mots distincts suivants, tous deux réduits pour la réduction v :

$$\begin{tikzcd}
 & 1010000^{n-5} \arrow[r, "\mathsf{v}"'] & 0^n \\
10101010^{n-5} \arrow[ur, "\mathsf{v}"'] \arrow[dr, "\mathsf{v}"'] & & \\
 & 1000010^{n-5} &
\end{tikzcd}$$

Le château 1000010^{n-5} du sous-ensemble $\mathcal{C}_{\frac{n}{6}}$ est construit à partir d'un château du sous-ensemble d'indice inférieur $\mathcal{C}_{\frac{n-3}{6}}$.

Pour construire les châteaux de façon unique, on définit, dans la section (1.4), une factorisation unique sur $\mathcal{C}$, appelée factorisation DD (Donjons/Douves), dont les facteurs "premiers" sont la douve simple et les donjons. Ces mots particuliers sont définis dans la section (1.3).

Sous forme factorisée, les châteaux sont représentés par des chemins de Schröder (cf digression suivante (1.2)).

1.2 Digression : chemins, nombres et mots de Schröder

Cette partie n'est pas indispensable pour la compréhension de la suite de l'étude.

Définition IV.6

- *Un chemin de Motzkin est un chemin du demi-plan supérieur reliant le point* $(0,0)$ *au point* $(n,0)$*, par des pas Nord-Est* $(1,1)$*, Sud-Est* $(1,-1)$ *ou Est* $(1,0)$ *(voir [WM]).*
  L'ensemble des chemins de Motzkin de longueur n *est noté* $\mathcal{M}_n$ *et l'ensemble des chemins de Motzkin est* $\mathcal{M} = \bigcup_{n\in\mathbb{N}} \mathcal{M}_n$.
- *Un chemin de Schröder est un chemin de Motzkin avec des pas horizontaux double : dans le demi-plan supérieur, il relie le point* $(0,0)$ *au point* $(2n,0)$ *par des pas Nord-Est* $(1,1)$*, Sud-Est* $(1,-1)$ *ou double Est* $(2,0)$ *(voir [WS]).*

Remarque IV.7

- *Le nombre de chemins de Motzkin de longueur* n *(i.e : reliant* $(0,0)$ *à* $(0,n)$*) est un nombre fini* M_n *appelé le nombre de Motzkin. La suite* $A001006$ *de l'OEIS des nombres de Motzkin commence par :*

n	0	1	2	3	4	5	6	7	8	9	10	11
Mn	1	1	2	4	9	21	51	127	323	835	2188	5798

  Un mot de Motzkin est un mot sur un alphabet $A = \{a, x, \bar{x}\}$ *à trois lettres tels que* x *et* $\bar{x}$ *interviennent dans le mot comme un parenthésage. L'ensemble des mots de Motzkin* $\mathcal{M}$ *vérifie l'équation*

$$\mathcal{M} = \varepsilon + a\mathcal{M} + x\mathcal{M}\bar{x}\mathcal{M}.$$

  Les chemins de Motzkin sont en bijection avec les mots de Motzkin. La correspondance entre mots de Motzkin et chemins de Motzkin s'obtient en notant un pas montant par la lettre x*, un pas descendant par la lettre* $\bar{x}$ *et un pas horizontal par la lettre* a.
  Ainsi, le nombre de Motzkin M_n *est égal au nombre de mots de Motzkin de longueur* n.
  Les premiers mots du langage de Motzkin sont :

n	M_n	
0	1	$\emptyset$
1	1	a
2	2	$aa, x\bar{x}$
3	4	$aaa, ax\bar{x}, xa\bar{x}, x\bar{x}a$
4	9	$aaaa, x\bar{x}aa, xaa\bar{x}, aax\bar{x}, axa\bar{x}, ax\bar{x}a, xa\bar{x}a, x\bar{x}x\bar{x}, xx\bar{x}\bar{x}$

  Le nombre de Motzkin Mn *est aussi le nombre d'arbres unaires-binaires à* n *arcs, c'est-à-dire d'arbres planaires enracinés où chaque nœud a soit un enfant (correspondant à la lettre* a*), soit deux enfants (correspondant à une paire de parenthèses* $x, \bar{x}$*).*
- *Pour tout entier* n*, le nombre de chemin de Schröder de longueur* $2n$ *est fini et le nombre de Schröder* r_n *est le nombre de chemin de Schröder de longueur* $2n$*. Les nombres de Schröder correspondent à la suite* $A006318$ *de l'OEIS et les premiers de ces nombres sont :*

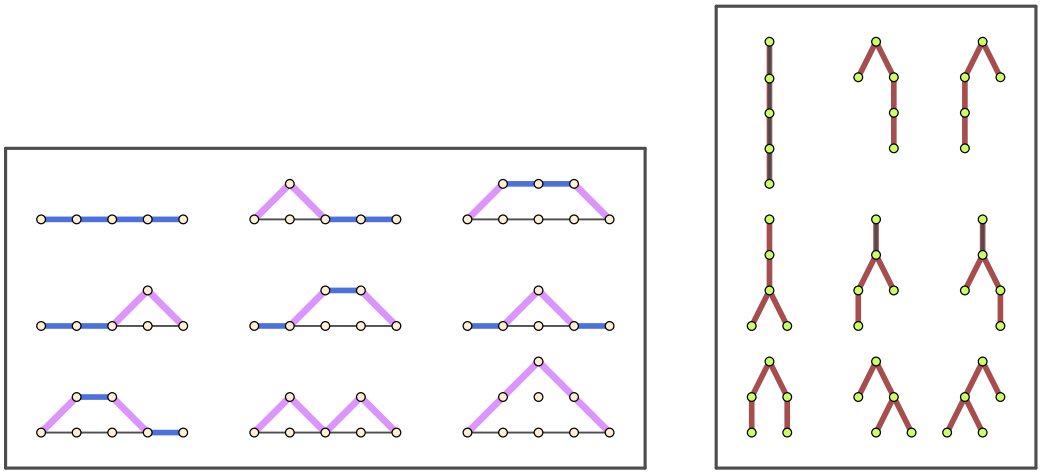


FIGURE IV.1 – Les $M_4 = 9$ chemins de Motzkin de longueur 4 et les $M_4 = 9$ arbres unaires-binaires pour 4 arcs correspondants aux $M_4 = 9$ mots de Motzkin $\{aaaa, x\bar{x}aa, xaa\bar{x}, aax\bar{x}, axa\bar{x}, ax\bar{x}a, xa\bar{x}a, x\bar{x}x\bar{x}, xx\bar{x}\bar{x}\}$.

n	0	1	2	3	4	5	6	7
r_n	1	2	6	22	90	394	1806	8558

Tout comme les chemins de Motzkin, les chemins de Schröder peuvent être représentés par des mots de longueurs $2n$ sur un alphabet à trois lettre $\{y, x, \bar{x}\}$ où les lettres x et $\bar{x}$ viennent par paires et la lettre y vient par couple yy. Le langage de Schröder R est l'ensemble de mots défini par l'équation récursive

$$R = \emptyset + yyR + xR\bar{x}R.$$

Les premiers mots du langage rangés par longueur sont :

n	R_n	
0	1	ε
1	2	$yy, x\bar{x}$
2	6	$yyyy, yyx\bar{x}, x\bar{x}yy, xyy\bar{x}, x\bar{x}x\bar{x}, xx\bar{x}\bar{x}$

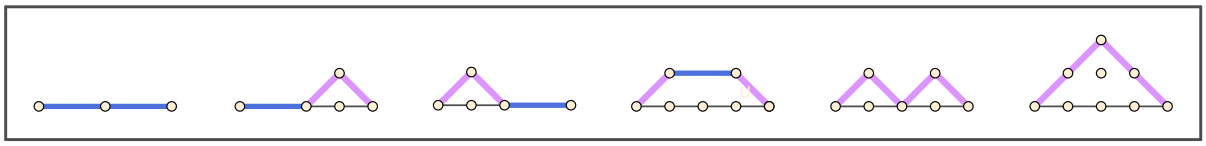


FIGURE IV.2 – Les $R_2 = 6$ chemins de Schröder de longueur 4 correspondants aux $R_2 = 6$ mots de Schröder $\{yyyy, yyx\bar{x}, x\bar{x}yy, xyy\bar{x}, x\bar{x}x\bar{x}, xx\bar{x}\bar{x}.\}$

La correspondance entre mots de Schröder et chemin de Schröder s'obtient en notant un

pas montant par la lettre x, un pas descendant par la lettre $\bar{x}$ et un pas horizontal double par le facteur yy.

1.3 Douves, Donjons, chemins.

Les facteurs "premiers" qui interviennent dans la factorisation unique DD des châteaux définie dans la partie suivante (1.4) sont la douve simple 0, et les donjons. Ces mots sont définis par :

Définition IV.8

- *Le mot* 0 *est appelée une douve.*
- *Un donjon est un château de somme non nulle dont aucun préfixe strict n'est un château. On note $\mathcal{D}$ l'ensemble des donjons.*

Lemme IV.9 *Soit w un mot de $\mathcal{B}^*$ et $\tilde{w} \in$ Réduit$_B$ le mot réduit de sa classe d'équivalence. S'il existe deux mots réduits $\tilde{p}$ et $\tilde{s}$ de Réduit$_B$ tels que $\tilde{w} = \tilde{p}1\tilde{s}$, alors il existe deux mots p et s de $\mathcal{B}^*$ tels que* $\begin{cases} w = p1s \\ p \sim_B \tilde{p} \\ s \sim_B \tilde{s} \end{cases}$.

Preuve : L'idée est que les réductions v et h ne produisent pas de facteur 1 et ne modifient pas leur place dans un mot. Ainsi, si la forme réduite $\tilde{w}$ du mot w comporte un facteur 1, alors le mot w lui-même comporte ce même facteur 1 et seuls les suffixes et préfixes ont été réduits. On le montre par récurrence sur $k = \lambda(w) - \lambda(\tilde{w}) \geq 0$.

- Si $k = \lambda(w) - \lambda(\tilde{w}) = 0$, alors le mot w est réduit. On a $w = \tilde{w}$ et on prend $p = \tilde{p}$ et $s = \tilde{s}$.
- Si $k > 0$, alors le mot w n'est pas réduit : il se réduit soit par une réduction v, soit par une réduction h, en un mot équivalent w' de longueur strictement inférieur qui satisfait les même hypothèses que w. Donc, il existe deux mots p' et s' tels que $\begin{cases} w' = p'1s' \\ p' \sim_B \tilde{p} \\ s' \sim_B \tilde{s} \end{cases}$.

  Enfin, le mot w s'obtient par une expansion $V : (00 \to 101)$ ou une expansion $H : (\emptyset \to 000)$ sur w'. Elle s'applique
  - soit sur le préfixe p'. Dans ce cas on obtient un préfixe p de w tel que $p \sim_B p' \sim_B \tilde{p}$ et on garde le suffixe $s = s' \sim_B \tilde{s}$.
  - soit sur le suffixe s'. Dans ce cas on obtient un suffixe s de w tel que $s \sim_B s' \sim_B \tilde{s}$ et on garde le préfixe $p = p' \sim_B \tilde{p}$.

Remarque IV.10 *Ce lemme est spécifiquement lié au modèle binaire et au fait que les expansions H et V ne s'appliquent pas sur les facteurs 1. Les facteurs 1 sont comme des "barrières" : une expansion H ou V s'applique sur un mot $p1s$, soit sur le facteur p situé avant un facteur 1, soit sur le facteur s situé après.*

Cette propriété de relèvement n'est plus vraie pour des mots irréductibles factorisés sous la forme $\tilde{w} = \tilde{p}\tilde{s}$. Il n'existe pas toujours de mots p et s qui "relèvent" le produit $\tilde{w} = \tilde{p}\tilde{s}$ vers un produit $w = ps$ dans $\mathcal{B}^*$ tel que $p \sim_B \tilde{p}$ et $s \sim_B \tilde{s}$. Par exemple, le mot $w = 11011$ est équivalent au mot réduit $\tilde{u} = 10.01$. Ni le préfixe $\tilde{p} = 10$, ni le suffixe $\tilde{s} = 01$ ne se retrouve dans l'écriture de w, quelque soit la factorisation de w.

Proposition IV.11 *Un donjon est un château de $\mathcal{C}_{\frac{1}{6}(2+3\mathbb{N})}$ de la forme $1u1$ où u est un château de $\mathcal{C}_{\frac{1}{6}(1+3\mathbb{N})}$.*

Preuve : Un donjon est un château : il est équivalent à 0^k, avec $k \in \{0, 1, 2\}$.

Un donjon est un château de somme non nulle et de somme paire (voir remarque (IV.2-4)) : il s'écrit sous la forme $w = 0^d 1u10^f$, avec $d, f \in \mathbb{N}$.

Si $d \neq 0$ ou si $f \neq 0$, les préfixes stricts 0^d et $0^d 1u1$ sont respectivement équivalents à 0^d et 0^{k+2f}, ce qui contredit la définition d'un donjon. Donc $d = f = 0$ et le donjon w est de la forme $w = 1u1$.

$$\begin{array}{llcll} \text{Ainsi,} & 1u1 & \sim_B & 0^k & \\ \Rightarrow & 0101u1010 & \sim_B & 0100^k010 & \\ \Rightarrow & u & \sim_B & 010^l10 & \text{pour } l \in \{0,1,2\}. \end{array}$$

Si $l = 0$ ou $l = 2$, alors le facteur u est équivalent au mot réduit 0110 ou au mot réduit 010010. D'après le lemme précédent (IV.9), il existe deux mots p et s de B^* tel que $u = p1s$ avec $p \sim_B 0$ et $s \sim_B 10$ ou $s \sim_B 0010$. Ainsi, le préfixe $1p1$ de $w = 1u1$ est équivalent au château $101 \sim_B 00$. Impossible.

Donc $l = 1$. Le facteur intérieur u est équivalent à la douve 0 et le donjon $w = 1u1$ est équivalent au mot réduit 00.

□

Remarque IV.12

- *Soit $w = 1u1$ un donjon. De la définition d'un donjon, aucun préfixe strict du facteur intérieur u n'est équivalent à 01 pour $\sim_B$.*
- *D'après la proposition précédente, tous les donjons sont des châteaux de $\mathcal{C}_{\frac{1}{6}(2+3\mathbb{N})}$.*
  Mais généralement, les châteaux de $\mathcal{C}_{\frac{1}{6}(2+3\mathbb{N})}$ ne sont pas des donjons. Par exemple, le château 1010101 de $\mathcal{C}_{\frac{1}{6}(2+3\times1)}$ n'est pas un donjon puisqu'il admet un préfixe strict 101

équivalent à 00. *D'où :*

$$\mathcal{D} \subsetneq \mathcal{C}_{\frac{1}{6}(2+3\mathbb{N})}.$$

- *L'ensemble des donjons d'indice donné n'est pas stable par expansions V. Par exemple : les expansions V permettent de construire trois nouveaux donjons (représentés dans l'exemple IV.16) à partir du donjon* 100001.

  Mais en appliquant l'expansion V sur les 2 *zéros au centre du mot, on obtient le château* $10\underline{10}1$01, *qui n'est pas un donjon.*

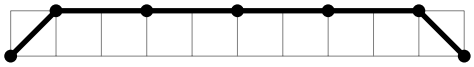
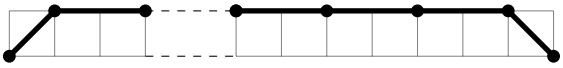
- *Le préfixe* 1 *et le suffixe* 1 *d'un donjon $w = 1u1$ sont couplés : aucun préfixe de u n'est équivalent à* 01 *; le préfixe* 1 *du donjon w ne peut pas se réduire avec un facteur* 1 *de u. La réduction v : $(101 \to 00)$ ne s'applique avec le premier* 1 *uniquement après réduction du facteur u en* 0 *et avec le suffixe* 1, *pour finalement réduire le donjon* $1u1$ *à* 00.

  Le préfixe 1 *et le suffixe* 1 *d'un donjon $w = 1u1$ sont complémentaires, comme des parenthèses.*

Dans la suite, les donjons $1u1$ sont représentés par des chemins de Schröder (voir section (1.2)) avec un pas horizontonal double pour les facteurs 0, un pas nord-est pour le premier facteur 1 et un pas sud-est pour le dernier facteur 1.

De manière équivalente, on note les donjons $1u1$ par des mots sur l'alphabet à trois lettres $\mathcal{T} = \{0, +, -\}$ où les lettres 0 restent inchangés et la lettre $+$ pour le premier facteur 1 et la lettre $-$ pour le second facteur 1 couplé.

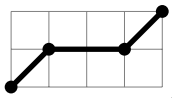
Exemple IV.13 *Les donjons de somme* 2 *sont :*

$\mathcal{D}$	*Ind*	$\mathcal{T} = \{0+, -1\}$	*Chemin de Schröder*
101 *(le plus petit)*	$\frac{2}{6}$	$+0-$	*de longueur* 4
100001	$\frac{5}{6}$	$+0000-$	 *de longueur* 10
$10(000)^k1$, $k \in \mathbb{N}$	$\frac{2+3k}{6}$	$+0(000)^k-$	 *de longueur* $6k+4$

Remarque IV.14 *Tous les chemins de Schröder ne correspondent pas à des donjons. Par exemple :*

1). les chemins qui commencent (et ceux qui se terminent) par un pas horizontal ne sont pas des représentations de donjons. En effet, les donjons commencent par un facteur 1 *(et se terminent par un facteur* 1*).*

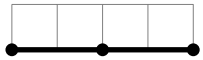
2). Les chemins comportant des pics *(noté* $+-$*) ne sont pas des représentations de donjons. En effet, entre deux facteurs* 1 *couplés, se trouve un facteur* $u \sim_B 0$ *non vide.*

3). Les chemins de Schröder commençant par  *, correspondants à des mots de Schröder avec un préfixe strict* $+0+$*, ne sont pas non plus des représentations de donjons. Un tel chemin serait codé par un mot de préfixe strict* 101*, qui est un donjon.*

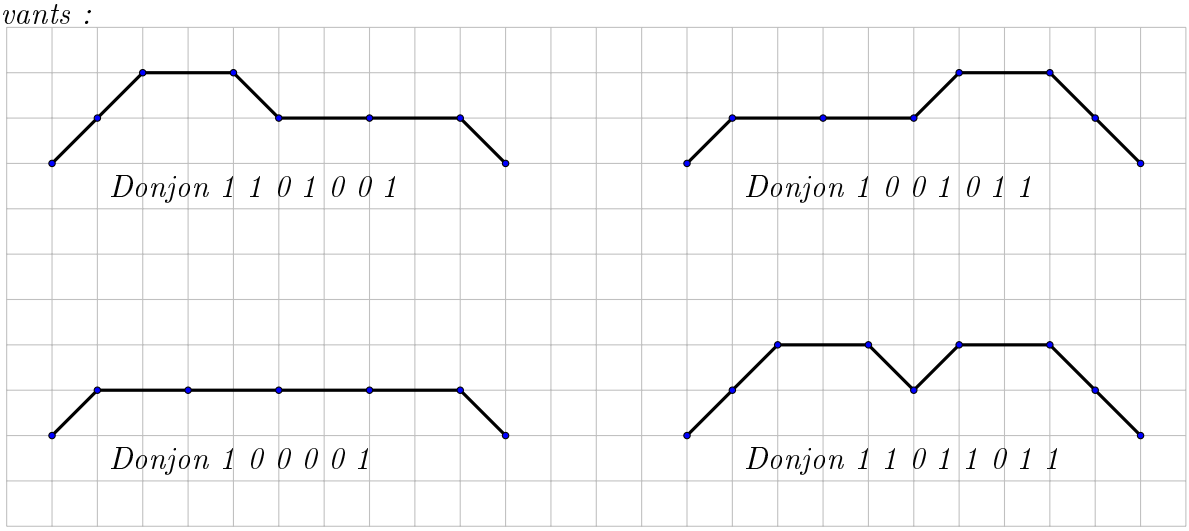
Remarque IV.15 *Le choix du pas double pour les facteurs* 0 *permet de représenter des mots d'indice* $\frac{n}{6}$ *donné par des chemins de Schröder de même longueur* $2n$*.*

En effet, l'indice d'un mot est $Ind(w) = \frac{1}{12}(2n_0 + n_1)$ *(voir remarque (III.3)), d'où* $2n_0 + n_1 = 12Ind = 2n$*.*

Exemple IV.16

Les facteurs 00 *et* 101 *d'indice* $\frac{2}{6}$ *sont représentés par les chemins de Schröder de longueur* 4 *:*  *et* *.*

Les 4 *donjons d'indice* $\frac{5}{6}$ *sont représentés par les chemins de Schröder de longueur* 10 *suivants :*



1.4 Factorisation DD (donjons/douves) des châteaux

Les facteurs "premiers", la douve simple et les donjons, permettent de définir une factorisation unique des châteaux, appelée factorisation DD :

Lemme IV.17 *Tout château w admet une unique factorisation DD en donjons/douves de la forme*

$$w = 0^{e_0} D_1 0^{e_1} D_2 0^{e_2} \cdots 0^{e_{n-1}} D_n 0^{e_n}$$

où $D_1, D_2, ...D_n$ est une suite de $n \geq 0$ donjons et $e_0, e_1, ...e_n$ sont des entiers naturels.

Preuve : Par récurrence sur la somme paire $2s, s \in \mathbb{N}$ du château (voir remarque (IV.2-4)).

Pour $s = 0$, la factorisation DD de w est immédiate et unique : $w = 0^{e_0}$.

Pour $s > 0$, le château s'écrit sous la forme $w = 0^d 1 w' 1 0^f$ où $1w'1$ est un château de somme paire $2s > 0$. Alors :

- si le facteur $1w'1$ est un donjon, alors $1w'$ n'admet pas de préfixe strict qui soit un château (en particulier, pas de préfixe strict qui soit un donjon). Le château w admet l'unique factorisation $w = 0^d D_1 0^f$ avec le donjon $D_1 = 1w'1$.
- sinon, le château $1w'1$ admet un préfixe strict C_1 qui est un château de somme paire $0 < 2s_1 < 2s$. On note $1w'1 = C_1 C_2$. Le suffixe C_2 de $1w'1$ est un château de somme $0 < \sigma(C_2) = 2(s - s_1) < 2s$.

  Par récurrence, le château C_1, qui commence par un facteur 1 et le château C_2, qui termine par un facteur 1, admettent les uniques factorisations DD :

  $$C_1 = D_1 0^{d_1} \cdots 0^{d_{n-1}} D_n 0^{d_n} \qquad \text{et} \qquad C_2 = 0^{e_0} E_1 0^{e_1} \cdots 0^{e_{m-1}} E_m$$

  Ainsi, l'unique factorisation DD du château w est :

  $$w = 0^d D_1 0^{d_1} \cdots 0^{d_{n-1}} D_n 0^{d_n + e_0} E_1 0^{e_1} \cdots 0^{e_{m-1}} E_m 0^f$$

□

Remarque IV.18 *Un château w écrit sous forme factorisée $w = 0^{e_0} D_1 0^{e_1} D_2 0^{e_2} \cdots 0^{e_{n-1}} D_n 0^{e_n}$ est équivalent à $0^{2n+e_0+e_1+...e_n \pmod 3}$. Il est dans l'ensemble $\mathcal{C}_{\frac{1}{6}((2n+e_0+e_1+...e_n)+3\mathbb{N})}$.*

Corollaire IV.19 *Soit $w = 0^{e_0} D_1 0^{e_1} D_2 0^{e_2} \cdots D_n 0^{e_n}$ un château de $\mathcal{C}_{\frac{k}{6}}$ sous forme factorisée, où n et $(e_0, e_1, ...e_n)$ sont des entiers et $D_1, \ldots, D_n$ sont des donjons. Pour toute suite $(f_i)_{0 \leq i \leq n}$ telle $\sum_{i=0}^n f_i = \sum_{i=0}^n e_i$ et toute permutation σ de $[0, n]$, le mot $0^{f_0} D_{\sigma(1)} 0^{f_1} D_{\sigma(2)} 0^{f_2} \cdots D_{\sigma(n)} 0^{f_n}$ est un château de l'ensemble $\mathcal{C}_{\frac{k}{6}}$.*

2 Dénombrement des châteaux

2.1 Dénombrement des donjons

Équivalents au plus petit donjon 101 pour la relation d'équivalence $\sim_B$, les donjons sont construits via des expansions $V : 00 \to 101$ et $H : \emptyset \to 000$ sur le mot 101. Mais on

n'exploitera pas ce point de vue car l'ensemble des donjons n'est pas stable par expansion V (voir remarque (IV.12)).

Pour construire récursivement l'ensemble des donjons, on utilise l'unique factorisation DD du facteur intérieur u d'un donjon $1u1$ de la forme $u = 0^{e_1}D_1 \cdots D_n 0^{e_n}$. Et on regarde les possibilités pour les puissances des douves 0^{e_i} pour que tous les facteurs stricts de $1u1$ ne soient pas des châteaux.

On obtient ainsi une équation ensembliste de l'ensemble des donjons (voir proposition (IV.20)). On en déduit la série génératrice du nombre de donjons à indice et somme donnés. Puis, on explicite la fonction algébrique associée à cette série génératrice.

Proposition IV.20 *L'ensemble $\mathcal{D}$ des donjons satisfait l'équation ensembliste récursive :*

$$\mathcal{D} = \left\{ \quad 101 \quad \right\} \cup \left\{ 1 \cdot \quad \{00 \cup \mathcal{D}\} \cdot \{000 \cup 0\mathcal{D} \cup \mathcal{D}0\}^* \cdot \{00 \cup \mathcal{D}\} \quad \cdot 1 \right\} \tag{IV.1}$$

Lemme IV.21 *Pour tout entier k, l'unique donjon de somme 2 et d'indice $\frac{2+3k}{6}$ est $10^{3k+1}1$.*

Preuve : Si D est un donjon de somme $\sigma(w) = 2$, alors il s'écrit $w = 1u1$ avec $\sigma(u) = 0$ et $u \sim_B 0$. Donc il est clair que w est de la forme $10^{3k+1}1$.

□

Lemme IV.22 *Soit $n \geq 1$ et soient $e_0, e_1, \ldots, e_n$ des entiers et $D_1, D_2, \ldots, D_n$ des donjons.*

Le mot $10^{e_0}D_1 0^{e_1} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$ est un donjon si et seulement si la puissance de la première douve $e_0 \neq 1 \pmod 3$ et le mot $10^{e_0+e_1+2} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$ est un donjon. .

Preuve :

Comme $D_1 \sim_B 00$, il est clair que le mot $w = 10^{e_0}D_1 0^{e_1} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$ est équivalent pour $\sim_B$ au mot $w' = 10^{e_0+e_1+2} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$. Donc le mot w est équivalent à 00 si et seulement le mot w' l'est aussi.

On note $D_1 = 1d_1 1$ le donjon D_1. Si $e_0 = 1 \pmod 3$, alors $0^{e_0} \sim_B 0$ et le mot w n'est pas un château. Donc $e_0 \neq 1 \pmod 3$.

De plus, comme aucun préfixe strict de w n'est pas un château, il est clair qu'aucun préfixe strict du mot $w' = 10^{e_0+e_1+2} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$ n'est un château.

Ainsi, si w est un donjon, alors $w' = 10^{e_0+e_1+2} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$ est un donjon.

Réciproquement, on suppose que le mot $w' = 10^{e_0+e_1+2} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$ est un donjon avec $e_0 \neq 1 \pmod 3$. Soit $D_1 = 1d_1 1$ un donjon.

Les préfixes stricts du mot $w = 10^{e_0}D_1 0^{e_1} D_2 0^{e_3} \cdots D_n 0^{e_n} 1$ sont de trois sortes :

1. les préfixes stricts de la forme 10^k avec $k \leq e_0$. Ces préfixes sont de somme 1. Clairement, ce ne sont pas des châteaux.
2. les préfixes stricts de la forme $10^{e_0}1p$ où $1p$ est un préfixe strict du donjon D_1. Comme $e_0 \neq 1 \pmod 3$, le premier facteur 1 ne se réduit pas avec le préfixe 1 du donjon D_1. Comme D_1 est un donjon, le préfixe 1 du facteur $1p$ ne se réduit pas par une réduction v. Donc le préfixe $1^{e_0}1p$ n'est pas un château.
3. les préfixes de la forme $10^{e_0}D_1p$. Ils sont équivalents aux préfixes stricts $10^{e_0+2}p$ du donjon w'. Donc ce ne sont pas des châteaux.

Donc le mot $w = 10^{e_0}D_10^{e_1}D_20^{e_3}\cdots D_n0^{e_n}1$ est un donjon.

□

Preuve de la proposition (IV.20) : On procède par récurrence sur le nombre de donjon dans la factorisation DD du facteur intérieur u d'un donjon $w = 1u1$. L'hérédité est assez fastidieuse, avec de multiples cas (et sous-cas) à considérer.

Si w est un donjon de somme $\sigma(w) = 2$, soit $w = 101$, soit $w = 100(000)^{k-1}001$ pour $k \geq 1$ (voir lemme (IV.21)).

Si $w = 1u1$ est un donjon de somme $\sigma(w) \geq 4$: la factorisation DD de son facteur intérieur u admet au moins 1 donjon. On note $u = 0^{e_0}D_10^{e_1}\cdots 0^{e_n}$.

D'après le lemme (IV.22), le mot w est un donjon si et seulement si $w' = 10^{e_0+e_1+2}D_2\cdots 0^{e_n}1$ est un donjon.

Par récurrence, comme $e_0 + e_1 + 2 \geq 2$, le donjon w' n'est pas le donjon 101. Le donjon w' est dans l'ensemble

$$\{1\cdot\ \{00 \cup \mathcal{D}\}\cdot\{000 \cup 0\mathcal{D} \cup \mathcal{D}0\}^*\cdot\{00 \cup \mathcal{D}\}\ \cdot 1\}.$$

On considère alors trois situations distinctes possibles : soit le facteur intérieur u' de $w' = 1u'1$ n'admet pas de donjon dans sa factorisation DD, alors le mot w' est de la forme $100(000)^k001$ avec $3k + 4 = e_0 + e_1 + 2$, soit u' est de la forme $100(000)^k.0D_2.\cdots 1$ avec $3k+3 = e_0+e_1+2$, enfin soit u' est de la forme $100(000)^k.D_20.\cdots 1$ avec $3k+2 = e_0+e_1+2$.

1. Pour $w' = 100.(000)^k.001$, on a :
   - si $e_0 = 3k_1 = 0 \pmod 3$ alors $\begin{cases} \text{soit } w = 1.D_1.(000)^k.00 \text{ si } e_0 = 0, \\ \text{soit } w = 1.00.(000)^{k_1-1}.0D_1.(000)^{k-k_1}.00.1. \end{cases}$
   - si $e_0 = 3k_1 + 2 = 2 \pmod 3$ alors $\begin{cases} \text{soit } w = 1.00.(000)^{k_1}.D_1.1 \ \text{ si } \ k_1 = k, \\ \text{soit } w = 1.00.(000)^{k_1}.D_10.(000)^{k-k_1-1}.00.1. \end{cases}$

2. Pour $w' = 100(000)^k.0D_2.\cdots 1$, on a :

   - si $e_0 = 3k_1 = 0 \pmod 3$ alors $\begin{cases} \text{soit } w = 1.D_1.(000)^k.0D_2.\cdots 1 \text{ si } e_0 = 0, \\ \text{soit } w = 1.00.(000)^{k_1-1}.0D_1.(000)^{k-k_1}.0D_2.\cdots 1. \end{cases}$
   - si $e_0 = 3k_1 + 2 = 2 \pmod 3$ alors $w = 100.(000)^{k_1}.D_1 0.(000)^{k-k_1-1}.0D_2.\cdots .1$.

3. Pour $w' = 100(000)^k.D_2 0.\cdots 1$, on a :

   - si $e_0 = 3k_1 = 0 \pmod 3$ alors $\begin{cases} \text{soit } w = 1.D_1.(000)^k.D_2 0.\cdots 1 \text{ si } e_0 = 0, \\ \text{soit } w = 1.00.(000)^{k_1-1}.0D_1.(000)^{k-k_1}.D_2 0.\cdots 1. \end{cases}$
   - si $e_0 = 3k_1 + 2 = 2 \pmod 3$ alors $w = 100.(000)^{k_1}.D_1 0.(000)^{k-k_1-1}.D_2 0.\cdots .1$.

Donc w est un donjon si et seulement si $w \in \{1\cdot\ \{00 \cup \mathcal{D}\} \cdot \{000 \cup 0\mathcal{D} \cup \mathcal{D}0\}^* \cdot \{00 \cup \mathcal{D}\}\ \cdot 1\}$.

□

Proposition IV.23

Pour tout entier i, j, on note $d_{i,j}$ le nombre de donjons de somme $2i$ et d'indice $\frac{j}{6}$. La série génératrice $\mathbf{D}(x,y) = \sum_{i,j\geq 0} d_{i,j} x^i y^j$ associée à $(d_{i,j})_{i,j}$ vérifie la relation de récurrence :

$$\mathbf{D} = x\Big(y^2 + y\frac{(y^2+\mathbf{D})^2}{1-y(y^2+2\mathbf{D})}\Big). \tag{IV.2}$$

Preuve :

Comme $2\sigma(0) = 0$ et $6Ind(0) = 1$, un facteur 0 compte pour y dans la série génératrice. Comme $\frac{1}{2}\sigma(1) = \frac{1}{2}$ et $6Ind(1) = \frac{1}{2}$, un facteur 1 compte pour $x^{1/2}y^{1/2}$. Avec l'équation de récurrence (IV.1)

$$\mathcal{D} = \left\{\ 101\ \right\} \cup \left\{1\cdot\ \{00 \cup \mathcal{D}\} \cdot \{000 \cup 0\mathcal{D} \cup \mathcal{D}0\}^* \cdot \{00 \cup \mathcal{D}\}\ \cdot 1\right\},$$

on obtient la série génératrice

$$\mathbf{D} = x^{\frac{1}{2}}y^{\frac{1}{2}} \cdot y \cdot x^{\frac{1}{2}}y^{\frac{1}{2}} + x^{\frac{1}{2}}y^{\frac{1}{2}} \cdot (y^2+\mathbf{D}) \cdot (\sum_{k\in\mathbb{N}}(y^3 + 2\cdot y\mathbf{D}))^k \cdot (y^2+\mathbf{D}) \cdot x^{\frac{1}{2}}y^{\frac{1}{2}}$$

$$\Leftrightarrow \qquad \mathbf{D} = xy^2 + xy \cdot (y^2+\mathbf{D})^2 \cdot \frac{1}{1-y^3-2y\mathbf{D}}.$$

□

Corollaire IV.24 *La série génératrice* $\mathbf{D}(x,y) = \sum_{i,j\geq 0} d_{i,j}x^iy^j$ *associée à la famille* $(d_{i,j})_{i,j}$ *est la fonction algébrique :*

$$\mathbf{D}(x,y) = \frac{1-y^3-\sqrt{(y^3-1)^2-4xy^3(2+x)}}{2y(2+x)} \tag{IV.3}$$

Preuve :

D'après la proposition précédente, la série génératrice vérifie l'équation polynomiale du second degré :

$$D^2(xy+2y)+D(y^3-1)+xy^2=0.$$

$$\text{Donc} \quad D(x,y) = \frac{1-y^3\pm\sqrt{\Delta}}{2y(2+x)}, \quad \text{avec} \quad \begin{array}{rcl} \Delta & = & (y^3-1)^2-4xy^3(2+x) \\ \text{et} \quad \sqrt{\Delta} & = & 1-y^3-2xy^3(2+x)+o(y^3). \end{array}$$

Avec le signe + devant la racine, on a :

$$D(x,y) = \frac{2-2y^3-2xy^3(2+x)+o(y^3)}{2y(2+x)} = \frac{1}{y(2+x)} - y^2(\frac{1}{2+x}-x)+o(y^2).$$

Ce qui ne correspond pas à notre cas. En effet, un donjon commmence et termine par un 1. Donc il n'y a pas de donjon de somme 0 et les coefficients de x^0y^j sont tous nuls.

Avec le signe − devant la racine, on a :

$$D(x,y) = \frac{2xy^3(2+x)+o(y^3)}{2y(2+x)} = xy^2+o(y^2).$$

On a bien un unique donjon d'indice $\frac{2}{6}$, c'est le donjon 101 de somme 2. Les autres donjons sont d'indice strictement supérieur à $\frac{2}{6}$ dans l'ensemble $\frac{2+3\mathbb{N}\setminus\{0\}}{6}$.

□

Le développement à l'ordre 26 par rapport à la variable y (la puissance est égale à $6Ind$) est :

$$
\begin{aligned}
\mathbf{D}(x,y) &= x\mathbf{y^2} \\
&+ (x^3+2x^2+x)\mathbf{y^5} \\
&+ (\mathbf{2}x^5+8x^4+11x^3+6x^2+x)\mathbf{y^8} \\
&+ (\mathbf{5}x^7+30x^6+70x^5+80x^4+46x^3+12x^2+x)\mathbf{y^{11}} \\
&+ (\mathbf{14}x^9+112x^8+371x^7+658x^6+674x^5+400x^4+130x^3+20x^2+x)\mathbf{y^{14}} \\
&+ (\mathbf{42}x^{11}+420x^{10}+1806x^9+4368x^8+6524x^7 \\
&\quad +6216x^6+3766x^5+1400x^4+295x^3+30x^2+x)\mathbf{y^{17}} \\
&+ (\mathbf{132}x^{13}+1584x^{12}+8382x^{11}+25740x^{10}+50790x^9 \\
&\quad +67344x^8+60948x^7+37464x^6+15260x^5+3920x^4+581x^3+42x^2+x)\mathbf{y^{20}} \\
&+ (\mathbf{429}x^{15}+6006x^{14}+37752x^{13}+140712x^{12}+345972x^{11}+590568x^{10}+717222x^9 \\
&\quad +624624x^8+388074x^7+168924x^6+49812x^5+9408x^4+1036x^3+56x^2+x)\mathbf{y^{23}} \\
&+ (\mathbf{1430}x^{17}+22880x^{16}+166595x^{15}+730730x^{14}+2154152x^{13}+4508504x^{12} \\
&\quad +6898892x^{11}+7830680x^{10}+6619250x^9+4146384x^8+1898358x^7+620004x^6 \\
&\quad +139020x^5+20160x^4+1716x^3+72x^2+x)\mathbf{y^{26}} \\
&+ o(y^{26}).
\end{aligned}
$$

Ci-dessous, un extrait des premières valeurs $d_{i,j}$ des nombres de donjons de somme $2i$ et d'indice $\frac{j}{6}$:

						1						
					1	2	**1**					
				1	6	11	8	**2**				
			1	12	46	80	70	30	**5**			
		1	20	130	400	674	658	371	112	**14**		
	1	30	295	1400	3766	6216	6524	4368	1806	420	**42**	
1	42	581	3920	15260	37464	60948	67344	50790	25740	8382	1584	**132**.

On observe que les coefficients devant les plus grandes puissances de x sont les premiers nombres de Catalan. Il est démontré dans la partie suivante que les donjons maximaux (de somme maximale) sont dénombrés par la suite des nombres de Catalan.

Remarque IV.25

- *Les coefficients $d_{0,j}$ sont tous nuls : il n'y a pas de donjon de somme nulle.*
- *Les coefficients $d_{i,3k}$ et $d_{i,3k+1}$ sont tous nuls. En effet, les donjons sont équivalents au mot réduits 00 et sont dans le sous-ensemble $I_{2+3\mathbb{N}}$.*
- *Les coeffcients $d_{1,2+3k}$ valent 1 (voir lemme (IV.22)).*
- *Les coefficients $d_{2,2+3k}$ pour $k \geq 1$ valent $k(k+1)$.*

En effet, un donjon de somme 4 est de la forme $w = 10^d 10^{3l+1} 10^f 1$. *Une fois choisi le donjon de intérieur d'indice* $\frac{3l+2}{6}$ *pour* $0 \leq l \leq k-1$, *on choisit une place parmi les* $d + f = 3(k-l) - 1$ *zéros.*

Si $d = 0 \pmod 3$ *alors* $f = 2 \pmod 3$, *c'est bien un donjon. Si* $d = 2 \pmod 3$ *alors* $f = 0 \pmod 3$, *c'est bien un donjon. Si* $d = 1 \pmod 3$ *alors* $f = 1 \pmod 3$, *ce n'est pas un donjon. Donc 2 places sur 3 sont possibles. Donc parmi les* $3(k-1)$ *places, il y a* $2(k-l)$ *possibilités.*

Donc, $d_{2,2+3k} = \sum_{l=0}^{k-1} 2(k-l) = 2\sum_{j=1}^{k} j = k(k+1)$.

Remarque IV.26 *Au cumulé, les premières valeurs des nombres de donjons d'indice* $\frac{j}{6}$ *obtenus avec* $0 \leq j \leq 10$ *expansions* H *sont :*

$$\begin{aligned}\mathbf{D}(1,y) &= 1y^2 + 4y^5 + 28y^8 + 244y^{11} + 2380y^{14} + 24868y^{17} + 272188y^{20} \\ &+ 3080596y^{23} + 35758828y^{27} + 423373636y^{30} + 5092965724y^{33} + O(y^{35}).\end{aligned}$$

On obtient la série génératrice algébrique suivante :

$$\mathbf{D}(1,y) = \frac{1 - y^3 - \sqrt{y^6 - 14y^3 + 1}}{6y} \tag{IV.4}$$

La suite des coefficients $\{1, 4, 28, 244, 2380, 24868, \ldots\}$ *est référencée A103211 dans l'OEIS et est associée à la même série génératrice avec* $y^3 = u$ *(à un facteur* y^2 *près) (cf [Sl]).*

Ainsi, le nombre de donjons d'indice $\frac{3i+2}{6}$ *est* $\sum_{k=0}^{i} \binom{i+k}{2k} 3^k c_k$, *où* c_k *est le* $k-$*ième nombre de Catalan.*

Remarque IV.27 *À indice fixé différent de* $\frac{2}{6}$, *la somme des coefficients de degré pair en la variable* x *est égale à la somme des coefficients degré impair. En effet, on a :*

$$D(-1,y) = \frac{(1-y^3) - \sqrt{y^6 - 2y^3 + 1 + 4y^3}}{2y} = -y^2$$

Donc, pour tout indice $\frac{k}{6} \neq \frac{2}{6}$, *il y a autant de donjons de somme* $\sigma = 0 \pmod 4$ *que de donjons de somme* $\sigma = 2 \pmod 4$.

2.2 Dénombrement des châteaux

On rappelle que tout château w s'obtient à partir du mot réduit $w_r \in \{\emptyset, 0, 00\}$ de sa classe d'équivalence, avec $n_R = \frac{1}{2}\sigma(w)$ expansions R et $n_H = 2(Ind(w) - Ind(w_r))$ expansions H (voir proposition (I.69)).

L'ensemble des châteaux $\mathcal{C}$ est partitionné par le morphisme d'indice en sous-ensemble $\mathcal{C}_{\frac{k}{6}}$, pour $k \in \mathbb{N}$ (voir chapitre (III)). Plus précisément, les pré-images de I, U et U^2 par le

morphisme $\mu : B^* \to PSL_2(\mathbb{Z})$ sont partitionnées en sous-ensemble :

$$\begin{array}{rcl} \mu^{-1}(I) & = & \bigcup_{k\in\mathbb{N}} \mathcal{C}_{\frac{0+3k}{6}} \\ \mu^{-1}(U) & = & \bigcup_{k\in\mathbb{N}} \mathcal{C}_{\frac{1+3k}{6}} \\ \mu^{-1}(U^2) & = & \bigcup_{k\in\mathbb{N}} \mathcal{C}_{\frac{2+3k}{6}} \end{array}$$

La factorisation DD permet d'écrire de façon unique les châteaux de $\mathcal{C}$ comme produit de donjons de $\mathcal{D}$ et de la douve 0 (voir lemme (IV.17)).

Proposition IV.28 *L'ensemble des châteaux vérifie la relation :*

$$\mathcal{C} = 0^*\{\mathcal{D}0^*\}^* \tag{IV.5}$$

Preuve : Tout château admet une unique factorisation DD : $0^{e_0}D_1 0^{e_1}...0^{e_{n-1}}D_n 0^{e_n}$ où $n \geq 0$, $(e_i) \in \mathbb{N}$ et $D_i \in \mathbb{D}$. Donc l'ensemble des châteaux $\mathcal{C}$ s'injecte dans l'ensemble $0^*\{\mathcal{D}0^*\}^*$.

Réciproquement, comme tout donjon de $\mathcal{D}$ est un château équivalent à 00, il est facile de vérifier que tout mot de l'ensemble $0^*\{\mathcal{D}0^*\}^*$ est un château.

□

Proposition IV.29 *La série génératrice* $\mathbf{C}(x,y) = \sum_{i,j\geq 0} c_{i,j}x^i y^j$ *associée au nombre* $d_{i,j}$ *de châteaux de somme* $2i$ *et d'indice* $\frac{j}{6}$ *vérifie la relation :*

$$\mathbf{C}(x,y) = \frac{1}{1-y-\mathbf{D}(x,y)}.$$

Preuve : D'après la relation (IV.5), comme $\sigma(0) = 0$ et $6Ind(0) = 1$, on a :

$$\mathbf{C}(x,y) = \frac{1}{1-y}\frac{1}{1-\dfrac{\mathbf{D}(x,y)}{1-y}}.$$

D'où le résulat.

□

Corollaire IV.30 *La série génératrice* $\mathbf{C}(x,y) = \sum_{i,j\geq 0} c_{i,j}x^i y^j$ *associée au nombre* $d_{i,j}$ *de châteaux de somme* $2i$ *et d'indice* $\frac{j}{6}$ *est algébrique et on a :*

$$\mathbf{C}(x,y) = \frac{2y(x+2)}{2y(1-y)(x+2)+y^3-1+\sqrt{(y^3-1)^2-4xy^3(x+2)}}. \tag{IV.6}$$

Proposition IV.31 *La série génératrice* $\mathbf{C}(x,y) = \sum_{i,j\geq 0} c_{i,j} x^i y^j$ *associée au nombre* $c_{i,j}$ *de châteaux de somme* $2i$ *et d'indice* $\frac{j}{6}$ *vérifie la relation :*

$$\mathbf{C}(x,y) = \sum_{n\geq 0}\sum_{s\geq 0}\binom{n+s}{n}\mathbf{D}^n(x,y)y^s \tag{IV.7}$$

Preuve : Étant donné un château w, il admet une unique factorisation DD de la forme $w = 0^{e_0}D_1 0^{e_1}...0^{e_{n-1}}D_n 0^{e_n}$ où $n \geq 0$, $(e_i) \in \mathbb{N}$ et $D_i \in \mathbb{D}$. Donc un tel donjon comporte n donjons et $s = \sum_{i=0}^{n} e_i$ douves, soit $n+s$ facteurs premiers.

Parmi $n+s$ emplacements possibles, il y a $\binom{n+s}{n}$ possibilités de choisir les places des n donjons, les autres places étant complétés par les s douves 0. D'où le résultat.

□

Avec la fonction algébrique (IV.6) ou avec la relation (IV.7) de la proposition précédente, on obtient le développement et le développement au cumulé à indice donné suivant :

$$\begin{aligned}
\mathbf{C}(x,y) &= 1 \\
&+y \\
&+(1+x)y^2 \\
&+(1+2x)y^3 \\
&+(1+3x+x^2)y^4 \\
&+(1+5x+5x^2+x^3)y^5 \\
&+(1+7x+10x^2+3x^3)y^6 \\
&+(1+9x+18x^2+11x^3+2x^4)y^7 \\
&+(1+12x+35x^2+37x^3+15x^4+2x^5)y^8 \\
&+(1+15x+55x^2+74x^3+39x^4+7x^5)y^9 \\
&+(1+18x+81x^2+142x^3+111x^4+39x^5+5x^6)y^{10} \\
&+O(y^{11}).
\end{aligned}
\qquad
\begin{aligned}
\mathbf{C}(1,y) = \; & 1 \\
& +y \\
& +2y^2 \\
& +3y^3 \\
& +5y^4 \\
& +12y^5 \\
& +21y^6 \\
& +41y^7 \\
& +120y^8 \\
& +191y^9 \\
& +397y^{10} \\
& +O(y^{11})
\end{aligned}$$

Remarque IV.32 *Les premières valeurs* $c_{i,j}$ *des nombres de châteaux, de somme* $2i$ *et d'indice* $\frac{j}{6}$ *sont listées ci-dessous.*

$i =$	1	2	3	4	5	6	7	*total*
$\mathcal{C}_{\frac{0}{6}}$	**1**							1
$\mathcal{C}_{\frac{1}{6}}$	**1**							1
$\mathcal{C}_{\frac{2}{6}}$	1	**1**						2
$\mathcal{C}_{\frac{3}{6}}$	1	**2**						3
$\mathcal{C}_{\frac{4}{6}}$	1	3	**1**					5
$\mathcal{C}_{\frac{5}{6}}$	1	5	5	**1**				12
$\mathcal{C}_{\frac{6}{6}}$	1	7	10	**3**				21
$\mathcal{C}_{\frac{7}{6}}$	1	9	18	11	**2**			41
$\mathcal{C}_{\frac{8}{6}}$	1	12	35	37	15	**2**		120
$\mathcal{C}_{\frac{9}{6}}$	1	15	55	74	39	**7**		191
$\mathcal{C}_{\frac{10}{6}}$	1	18	81	142	111	39	**5**	397

Remarque IV.33

1. *Conformément à la remarque (IV.3), les premières classes d'équivalences $\mathcal{C}_{\frac{n}{6}}$ sont finies et on peut extraire le nombre de donjons de somme maximale à indice fixé $\frac{n}{6}$. Les premières valeurs sont rangées dans le tableau suivant, selon le reste de n modulo 3 :*

	$k=$	*0*	*1*	*2*	*3*	*4*	*5*
nombres de châteaux de longueur maximale dans $\mathcal{C}_{\frac{n}{6}}$	$n = 3k$	*1*	*2*	*3*	*7*	*19*	*56*
	$n = 3k+1$	*1*	*1*	*2*	*5*	*14*	*42*
	$n = 3k+2$	*1*	*1*	*2*	*5*	*14*	*42*

2. *L'ensemble des châteaux de somme maximale à indice fixé, appelés châteaux maximaux, est étudié à la partie suivante. On montrera que le nombre de châteaux maximaux d'indice $\frac{3k+1}{6}$ et le nombre de châteaux maximaux d'indice $\frac{3k+2}{6}$ est le k-ième nombre de Catalan et le nombre de châteaux maximaux d'indice $\frac{3k+3}{6}$ est la sommme $c_k + c_{k+1}$ de deux nombres de Catalan consécutifs.*

3. *À partir de la série génératrice des châteaux, on extrait la série génératrice d'un des ensembles $\mathcal{C}_{\frac{1}{6}(0+3\mathbb{N})}$, $\mathcal{C}_{\frac{1}{6}(1+3\mathbb{N})}$ ou $\mathcal{C}_{\frac{1}{6}(2+3\mathbb{N})}$.*
   Dans le premier cas, la série génératrice $\mathbf{C}_0$ des châteaux du noyau $K_B = \mathcal{C}_{\frac{1}{6}(0+3\mathbb{N})}$ s'obtient avec l'expression $\mathbf{C}_0(x,y) = \frac{1}{3}(\mathbf{C}(x, j_0^2 y) + \mathbf{C}(x, j_0 y) + \mathbf{C}(x,y))$ où j_0 est la racine troisième de l'unité $\frac{-1+i\sqrt{3}}{2}$, racine du polynôme $z^2 + z + 1$.
   De même, la série génératrice $\mathbf{C}_1$ des châteaux de $\mathcal{C}_{\frac{1}{6}(1+3\mathbb{N})}$ est : $\mathbf{C}_1(x,y) = \frac{1}{3}(\mathbf{C}(x, j_0^2 y) j_0 + \mathbf{C}(x, j_0 y) j_0^2 + \mathbf{C}(x,y))$.
   Et la série génératrice C_2 des châteaux de $\mathcal{C}_{\frac{1}{6}(2+3\mathbb{N})}$ est : $\mathbf{C}_2(x,y) = \frac{1}{3}(\mathbf{C}(x, j_0^2 y) j_0^2 + \mathbf{C}(x, j_0 y) j_0 + \mathbf{C}(x,y))$.

3 Mots maximaux - Nombres de Catalan

L'ensemble des châteaux est partitionné en sous-ensembles $\mathcal{C}_{\frac{n}{6}}, n \in \mathbb{N}$. Pour tout entier n, l'ensemble $\mathcal{C}_{\frac{n}{6}}$ est finie (voir proposition (IV.3)) et admet des mots de somme maximale.

Dans cette partie, on étudie, les châteaux maximaux d'indice $\frac{n}{6}$ fixé. En particulier, on montre que pour tout entier k, l'ensemble $\mathcal{C}^{\max}_{\frac{3k+2}{6}}$ des châteaux maximaux d'indice $\frac{3k+2}{6}$ sont les donjons maximaux.

Définition IV.34 *Soit $n \in \mathbb{N}$.*

Un château d'indice $\frac{n}{6}$ est dit maximal s'il est de somme maximale $\sigma_n = \max\limits_{w \in \mathcal{C}_{n/6}} (\sigma(w))$ dans l'ensemble fini $\mathcal{C}_{\frac{n}{6}}$.

On note $\mathcal{C}^{\max}_{\frac{n}{6}}$ l'ensemble des châteaux maximaux d'indice $\frac{n}{6}$ et on note $\mathcal{C}^{\max} = \bigcup_{n \in \mathbb{N}} \mathcal{C}^{\max}_{\frac{n}{6}}$ l'ensemble des châteaux maximaux.

Un donjon d'indice $\frac{3k+2}{6}$ est dit maximal s'il est de somme maximale $\max\limits_{D \in \mathcal{D} \cap \mathcal{C}_{(3k+2)/6}} (\sigma(D))$ dans l'ensemble fini $\mathcal{D} \bigcap \mathcal{C}_{(3k+2)/6}$.

On note $\mathcal{D}^{\max}_{\frac{3k+2}{6}}$ l'ensemble des donjons maximaux d'indice $\frac{3k+2}{6}$ et on note $\mathcal{D}^{\max} = \bigcup\limits_{k \in \mathbb{N}} \mathcal{D}^{\max}_{(3k+2)/6}$ l'ensemble des donjons maximaux.

Remarque IV.35

1. *Le morphisme d'indice est défini par $Ind = \frac{1}{12}(2\sigma - \lambda)$. Donc les mots de somme maximale d'indice $\frac{n}{6}$ fixé sont aussi les mots de longueur maximale d'indice $\frac{n}{6}$.*

   On note λ_n la longueur des châteaux maximaux et σ_n la somme des châteaux maximaux de $\mathcal{C}_{\frac{n}{6}}$. On a :
$$\sigma_n = 2\lambda_n - 2n.$$

2. *Il est clair qu'on a l'inégalité :*
$$\max_{D \in \mathcal{D} \cap \mathcal{C}_{(3k+2)/6}} (\sigma(D)) \leq \sigma_{3k+2} = \max_{w \in \mathcal{C}_{(3k+2)/6}} (\sigma(w)).$$

   L'égalité est démontrée dans la proposition (IV.41).

Dans un premier temps, on étudie les propriétés des châteaux maximaux et on montre que les châteaux maximaux sont engendrés par l'expansion $(0 \to 101101)$ sur les châteaux maximaux d'indice $\frac{3\times0+1}{6}$, $\frac{3\times0+2}{6}$ et $\frac{3\times0+3}{6}$.

Ensuite, on montre qu'il existe une bijection naturelle des orbites de l'action de permutation sur l'ensemble des châteaux maximaux du noyau d'indice $\frac{3k+3}{6}$ et l'ensemble des arbres $3-$ réguliers à $2k+2$ sommets.

Puis, on définit l'ensemble $\mathcal{T}^{\mathrm{d}}$ des arbres $3-$ réguliers décorés (par une feuille ou par une arête orientée) et on montre que l'ensemble $\mathcal{T}^{\mathrm{d}}_k$ des arbres décorés à $2k+2$ sommets est

dénombré par la somme $c_k + c_{k+1}$ de deux nombres de Catalan consécutifs et est en bijection avec l'ensemble $\mathcal{C}^{\max}_{3k+3/6}$ des châteaux maximaux du noyau d'indice $\frac{3k+3}{6}$.

Dans une dernière partie, on dénombre les orbites de l'action de permutation sur des sous-ensembles de châteaux du noyau selon trois types : les orbites des mots simples, les orbites des mots carrés (de la forme p^2) et les orbites des mots cubes (de la forme p^3). La suite du nombre total d'orbites d'indice fixé est la suite du nombre d'arbres 3−réguliers référencée $A001683$ dans l"encyclopédie OEIS en ligne [Sl].

3.1 Châteaux maximaux

L'ensemble des châteaux est partitionné en sous-ensembles finis $\{\mathcal{C}_{\frac{n}{6}}, n \in \mathbb{N}\}$ (voir proposition (IV.3)). Pour tout entier n, le sous-ensemble $\mathcal{C}_{\frac{n}{6}}$ admet des mots de somme maximale. Ces mots sont également de longueur maximale.

Exemple IV.36 *Les premiers châteaux maximaux d'indice* $\frac{0}{6}$, $\frac{1}{6}$, $\frac{2}{6}$ *et* $\frac{3}{6}$ *sont :*

$$\mathcal{C}^{\max}_{0/6} = \{\emptyset\} \qquad \mathcal{C}^{\max}_{1/6} = \{0\} \qquad \mathcal{C}^{\max}_{2/6} = \{101\} \qquad \mathcal{C}^{\max}_{3/6} = \{0101, 1010\}$$

Comme 101 *est un donjon, il est clair que* $\mathcal{C}^{\max}_{\frac{2}{6}} = \mathcal{D}^{\max}_{\frac{2}{6}}$.

Dans cette section, on montre le résultat principal suivant :

Proposition IV.37 *L'ensemble des châteaux maximaux* $\mathcal{C}^{\max}$ *est l'ensemble des châteaux obtenus par l'expansion* $0 \to 101101$ *sur les premiers châteaux maximaux* $\{0, 101, 0101, 1010\}$ *et on note :*

$$\mathcal{C}^{\max}_{\frac{3\mathbb{N}+1}{6}} = \langle 0, 0 \to 101101 \rangle,$$
$$\mathcal{C}^{\max}_{\frac{3\mathbb{N}+2}{6}} = \langle 101, 0 \to 101101 \rangle,$$
$$\mathcal{C}^{\max}_{\frac{3\mathbb{N}+3}{6}} = \langle 0101, 1010, 0 \to 101101 \rangle.$$

Lemme IV.38 *Les zéros intérieurs d'un château maximal sont isolés : un château maximal non vide est soit le château* 0*, soit un mot de la forme* $0^d 1^{\alpha_1} 0 1^{\alpha_2} 0 \cdots 0 1^{\alpha_n} 0^f$ *avec* $n \geq 2$*,* $d, f \in \{0, 1\}$ *et* $\alpha_1, \cdots, \alpha_n \geq 2$.

Preuve : Il est clair que si un château comporte un facteur 00, l'expansion $V : 00 \to 101$, qui ne modifie pas l'indice, s'applique. Donc un tel château n'est pas maximal.

Un mot de la forme $0^d 1^\alpha 0^f$, avec $d, f \in \{0, 1\}$ et $\alpha \geq 1$ est réduit pour les réductions v et h. Il n'est pas dans l'ensemble $\{\emptyset, 0, 00\}$, donc ce n'est pas un château. Donc un château maximal non vide, différent du château maximal 0, admet au moins un facteur 0 isolé intérieur.

□

Lemme IV.39 *Un château maximal d'indice* $\geq \frac{2}{3}$ *admet un facteur* 101101.

Plus précisément, un château maximal d'indice $\geq \frac{2}{3}$ *est de la forme* $0^d1^{\alpha_1}01^{\alpha_2}0\cdots01^{\alpha_n}0^f$ *avec* $n \geq 3$, $d, f \in \{0,1\}$, $\alpha_1, \alpha_n \geq 1$ *et* $\alpha_2, \cdots, \alpha_{n-1} \geq 2$, *avec au moins un cas d'égalité.*

Preuve :

D'après le lemme précédent (IV.38), les zéros d'un château maximal w d'indice $\geq \frac{4}{6}$ sont isolés. Un château maximal d'indice $\geq \frac{4}{6}$ est un mot de la forme

$$w = 0^d1^{\alpha_1}01^{\alpha_2}0\cdots01^{\alpha_n}0^f \qquad \text{avec } n \geq 2, d, f \in \{0,1\} \text{ et } \alpha_i \geq 1.$$

Le facteur intérieur $1^{\alpha_1}01^{\alpha_2}0\cdots01^{\alpha_n}$ est aussi un château.

On montre par disjonction des cas, selon le nombre n de 0 intérieurs isolés qu'un tel château maximal admet un facteur intérieur 0110.

- Pour $n = 2$, le mot $0^d1^{\alpha_1}01^{\alpha_2}0^f$ est un château si et seulement si $\alpha_1 = \alpha_2 = 1$.

  Si $d = f = 1$, le château $0^d1010^f = 01010$, d'indice $\frac{2}{3}$ n'est pas maximal car le château 101101, également d'indice $\frac{2}{3}$, est de longueur strictement supérieur. Donc les châteaux maximaux de la forme $0^d1^{\alpha_1}01^{\alpha_2}0^f$ sont les châteaux de l'ensemble $\{0101, 101, 1010\}$, d'indices $< \frac{3}{2}$. Impossible.

  Donc $n \geq 3$.

- Si $\alpha_i \geq 3$, pour tout indice $2 \leq i \leq n-1$, alors le facteur intérieur $1^{\alpha_1}01^{\alpha_2}0\cdots01^{\alpha_n}$ est équivalent au mot réduit $1^{\alpha_1-1}001^{\alpha_2-2}001^{\alpha_3-2}00\cdots1^{\alpha_{n-1}-2}001^{\alpha_n-1} \notin \{\emptyset, 0, 00\}$. Donc ce n'est pas un château. Impossible.

  Donc il existe $i \in [2, n-1]$ tel que $\alpha_i \leq 2$.

- S'il existe $i \in [2, n-1]$ tel que $\alpha_i = 1$: sans perdre de généralité, on considère que $\alpha_2 = 1$.

  Pour $n = 3$, le facteur intérieur $1^{\alpha_1}0101^{\alpha_3}$ est équivalent au mot réduit $1^{\alpha_1+\alpha_3-1} \notin \{\emptyset, 0, 00\}$. Donc ce n'est pas un château. Impossible.

  Pour $n \geq 4$, le facteur intérieur $1^{\alpha_1}0101^{\alpha_3}$ est équivalent à :

  $$1^{\alpha_1-1}0001^{\alpha_3} \sim_B 1^{\alpha_1-1}1^{\alpha_3}000 \sim_B 1^{\alpha_1+\alpha_3}010.$$

  Le château $w' = 0^d1^{\alpha_1+\alpha_3}01\underline{00}1^{\alpha_4}\cdots1^{\alpha_n}0^f$ est équivalent à w, de même indice que w et de même longueur que w. Mais w' n'est pas maximal (voir proposition (IV.38)). Donc le château w n'est pas maximal. Impossible.

  Donc pour tout $i \in [2, n-1]$, on a : $\alpha_i \geq 2$.

Finalement, un château maximal d'indice $\geq \frac{4}{6}$ est un mot de la forme $0^d 1^{\alpha_1} 0 1^{\alpha_2} 0 \cdots 0 1^{\alpha_n} 0^f$ avec $n \geq 3$, $d, f \in \{0,1\}$, $\alpha_1, \alpha_n \geq 1$ et $\alpha_2, \cdots, \alpha_{n-1} \geq 2$, avec au moins un cas d'égalité.

D'où le résultat.

□

Preuve de la proposition (IV.37) : Soit $i \in \{1,2,3\}$.

- Par récurrence sur $k \geq 0$, on montre que $\mathcal{C}^{\max}_{\frac{3k+i}{6}}$ est l'ensemble image de $\mathcal{C}^{\max}_{\frac{i}{6}}$ par k expansions $0 \to 101101$.

  Pour $k = 0$, c'est clair.

  Soit w un château maximal d'indice $\frac{3k+i}{6}$ pour $k \geq 1$. D'après le lemme (IV.39), le château w admet un facteur 101101. On note $w = p101101s$ et $\lambda(w) = l$.

  Si le château $v = p0s$, d'indice $\frac{3(k-1)+i}{6}$ et de longueur $l-5$, n'est pas maximal, alors il existe un château v' de même indice de longueur strictement supérieur $> l-5$. Appliquant l'expansion $(0 \to 101101)$ sur un zéro du château v', on obtient un château w' d'indice $\frac{3k+i}{6}$ de longueur $l' > l$, strictement supérieur au château maximal w. Absurde. Donc v est maximal.

  Par récurrence, v est dans l'image de $\mathcal{C}^{\max}_{\frac{i}{6}}$ par $k-1$ expansions $0 \to 101101$. Or, par construction, $v \underset{0\to 101101}{\longrightarrow} w$. Donc w est dans l'image de $\mathcal{C}^{\max}_{\frac{i}{6}}$ par k expansions $0 \to 101101$.

- Réciproquement, on considère un château w, d'indice $\frac{3k+i}{6}$, obtenu par k expansions $0 \to 101101$ sur un mot de $\mathcal{C}^{\max}_{\frac{i}{6}}$. Il existe un château v obtenu par $k-1$ expansions $0 \to 101101$ sur un mot de $\mathcal{C}^{\max}_{\frac{i}{6}}$ tel que $v \underset{0\to 101101}{\longrightarrow} w$.

  Par récurrence, v est un château maximal d'indice $\frac{3(k-1)+i}{6}$.

  Si w n'est pas maximal de longueur $l = \lambda(w)$ alors il existe un château maximal w' d'indice $\frac{3k+i}{6}$ et de longueur $l' > l$. D'après le lemme (IV.39), le château w' admet un facteur 101101. Notons $w' = p'101101s'$. Le château $v' = p'0s'$ est de même indice que v et de longueur $l'-5$ strictement supérieur à la longueur $l-5$ du château maximal v. Absurde. Donc w est maximal.

□

Corollaire IV.40 *Soit k un entier ≥ 0. Les sommes et longueurs des châteaux maximaux sont :*

$$\begin{array}{lll} \sigma_{\frac{3k+1}{6}} = 4k & \textit{et} & \lambda_{\frac{3k+1}{6}} = 5k+1 \\ \sigma_{\frac{3k+2}{6}} = 4k+2 & \textit{et} & \lambda_{\frac{3k+2}{6}} = 5k+3 \\ \sigma_{\frac{3k+3}{6}} = 4k+2 & \textit{et} & \lambda_{\frac{3k+3}{6}} = 5k+4 \end{array}$$

Preuve :

Il est clair que la somme d'un mot augmente de 4 par expansion ($0 \to 101101$) et la longueur augmente de 5.

□

Corollaire IV.41 *Les châteaux maximaux d'indice* $\frac{3\mathbb{N}+2}{6}$ *sont des donjons. Et pour tout entier* k*, on a :*

$$\mathcal{C}^{\max}_{\frac{3k+2}{6}} = \mathcal{D}^{\max}_{\frac{3k+2}{6}}$$

Preuve :

Tous les zéros des donjons sont intérieurs et tous les zéros des donjons maximaux sont intérieurs et isolés par des 1.

Une expansion ($0 \to 101101$) sur un zéro isolé intérieur remplace un facteur 101 (qui est un donjon) par le donjon 11011011. D'après l'équation récursive des donjons (IV.1), on obtient un donjon.

□

Corollaire IV.42 *On a :*

$$\mathcal{C}^{\max}_{\frac{3\mathbb{N}+1}{6}} = \{0\} \cup (D^{\max})^2,$$
$$\mathcal{D}^{\max} = 1\mathcal{C}^{\max}_{\frac{3\mathbb{N}+1}{6}}1$$

et

$$K_B^{\max} = \mathcal{C}^{\max}_{\frac{3\mathbb{N}}{6}} = \{\emptyset\} \sqcup 0\mathcal{D}^{\max} \sqcup \mathcal{D}^{\max}0 \cup (\mathcal{D}^{\max})^3.$$

Preuve :

Les deux premiers points sont clairs par la proposition (IV.37).

Pour la troisième relation, on a $K_B^{\max} = \{\emptyset\} \cup \mathcal{C}^{\max}_{\frac{3\mathbb{N}+3}{6}}$ et selon le facteur 0 sur lequel on applique l'expansion $0 \to 101101$ dans les mots 0101 et 1010, on a :

$$\begin{aligned} \mathcal{C}^{\max}_{\frac{3\mathbb{N}+3}{6}} &= \langle 101101101, 0 \to 101101\rangle \cup 01\langle 0, 0 \to 101101\rangle 1 \cup 1\langle 0, 0 \to 101101\rangle 10 \\ \text{D'où :}\quad K_B^{\max} &= \mathcal{C}^{\max}_{\frac{3\mathbb{N}+3}{6}} = (\mathcal{D}^{\max})^3 \cup 0\mathcal{D}^{\max} \cup \mathcal{D}^{\max}0. \end{aligned}$$

Les unions sont disjointes car les châteaux de $0\mathcal{D}^{\max}$ sont les châteaux qui commencent par 0 et terminent par 1. Ceux de $\mathcal{D}^{\max}0$ sont ceux qui commencent par 1 et terminent par 0. Enfin, ceux de $(\mathcal{D}^{\max})^3$ sont ceux qui commencent et terminent par 1.

□

Remarque IV.43 *En notation condensée, l'expansion* $0 \to 101101$ *s'écrit* $\lceil ab \rceil \to (a+1)2(b+1)$ *et on a :*

$$\mathcal{C}^{\max}_{\frac{3\mathbb{N}+1}{6}} = \lceil 0 \rceil \cup \langle \lceil 121 \rceil, \lceil ab \rceil \to (a+1)2(b+1) \rangle,$$

$$\mathcal{C}^{\max}_{\frac{3\mathbb{N}+2}{6}} = \langle \lceil 11 \rceil, \lceil ab \rceil \to (a+1)2(b+1) \rangle,$$

$$\mathcal{C}^{\max}_{\frac{3\mathbb{N}+3}{6}} = \langle \lceil 01 \rceil, \lceil 10 \rceil, \lceil ab \rceil \to (a+1)2(b+1) \rangle.$$

L'indice d'un mot de B^* *augmente de* $1/2$ *via l'expansion* $0 \to 101101$ *et la longueur du mot augmente de* 5*. En notation condensée, la longueur du mot augmente de* 1*.*

3.2 Permutation circulaire sur le noyau K_B et arbres 3-réguliers.

La somme $\sigma(w)$, la longueur $\lambda(w)$ et l'indice $Ind(w)$ d'un mot w de B^* sont invariants par permutation circulaire.

Comme $PSL_2(\mathbb{Z})$ est un groupe, le noyau K_B de $\mu_{|B^*}$ est stable par permutations circulaires. En effet, si un mot ps est dans le noyau, alors $\mu(ps) = \mu(p)\mu(s) = I$ donc $\mu(sp) = \mu(s)\mu(p) = I$ et sp est dans le noyau K_B.

Dans cette partie, tous les arbres sont des arbres finis (un arbre est un graphe simple sans cycle). On montre le résultat principal suivant :

Proposition IV.44 *Les orbites des mots maximaux du noyau* K_B *pour l'action de permutation circulaire est en bijection avec l'ensemble des arbres* $3-$*réguliers.*

Définition IV.45 *Un arbre plan est un arbre plongé dans le plan orienté.*

Un sommet de degré 1 *est une feuille. Un sommet de degré* > 1 *est un sommet intérieur.*

Définition IV.46 *Un arbre* $n-$*régulier plan est un arbre plan dont les sommets sont soit des feuilles (de degré* 1*), soit des sommets intérieurs de degré* n*.*

Un arbre $3-$*régulier plan à* k *sommets intérieurs est un arbre* $3-$*régulier plan à* $2k+2$ *sommets. Un tel arbre possède* $k+2$ *feuilles et* $2k+1$ *arêtes.*

On note $\mathcal{T}_k$ *l'ensemble des arbres* $3-$*réguliers plans à* k *sommets intérieurs (*$2k+2$ *sommets) et* $\mathcal{T} = \bigcup_{k \geq 0} \mathcal{T}_k$ *l'ensemble des arbres* $3-$*réguliers plans finis.*

Dans la suite, on considérera des arbres $3-$réguliers plans finis.

Définition IV.47 *L'expansion "pousse" de l'ensemble* $\mathcal{T}_k$ *des arbres* $3-$*réguliers à* $2k+2$ *sommets dans l'ensemble* $\mathcal{T}_{k+1}$ *des arbres* 3*-réguliers à* $2k+4$ *sommets remplace une feuille d'un arbre* $3-$*régulier par un sommet intérieur à deux fils de degré* 1 *(deux feuilles) :*

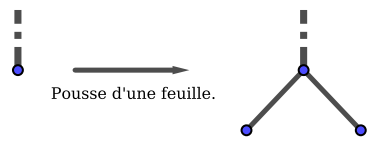
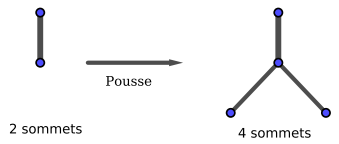


FIGURE IV.3 – Pousse d'une feuille d'un arbre.

Proposition IV.48 *L'ensemble des arbres plans finis* $3-$*réguliers* $\mathcal{T}$ *est engendré par l'expansion "pousse" sur l'arbre* $3-$*régulier à* 2 *sommets (2 feuilles reliées par* 1 *arête).*

Preuve :

L'unique arbre $3-$régulier à $2 \times 1 + 2$ sommets est composé d'un sommet intérieur relié par trois arêtes à 3 feuilles. C'est la pousse de l'unique arbre $3-$régulier à 2 sommets :



Par récurrence, pour tout entier $k \geq 0$, un arbre $3-$régulier plan fini à $2(k+1)+2$ sommets admet un sommet intérieur relié à deux feuilles : c'est la pousse d'un arbre $3-$régulier plan fini à $2k + 2$ sommets.

□

Preuve de la proposition (IV.44) : On associe un mot de B^* à un arbre 3-régulier par lecture anti-horaire en associant 0 à une feuille et 1 à une arête. Ainsi, l'expansion pousse d'un arbre $3-$régulier correspond à l'expansion $(0 \to 101101)$ (voir figure (IV.4)).

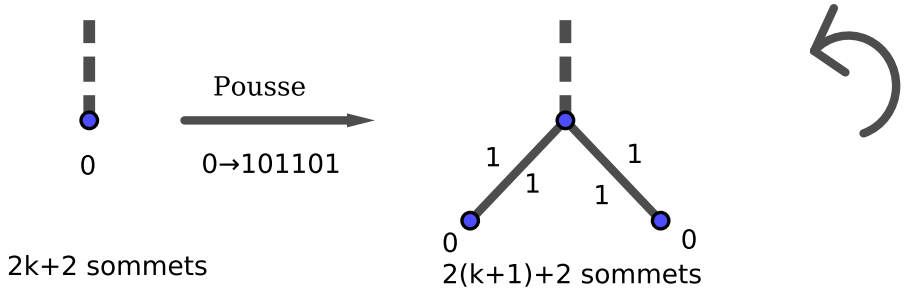


FIGURE IV.4 – L'expansion "pousse" d'un arbre est associée à l'expansion $(0 \to 101101)$ sur $K_B \subset B^*$.

Les deux mots 0101 et 1010 sont dans la même orbite pour l'action de permutation circulaire. Leur orbite est associée à l'arbre 3-régulier à 2 sommets. Par lecture anti-horaire, selon si on commence par une feuille ou une arête, on obtient le mot 0101 ou le mot 1010.

Comme le noyau K_B est engendré par l'expansion $(0 \to 101101)$ sur les mots $\{0101, 1010\}$ (voir proposition (IV.37)), à permutation près, les châteaux du noyaux K_B est en bijection avec l'ensemble des arbres engendrés par l'expansion pousse sur l'arbre $3-$régulier à 2 sommets (voir proposition (IV.48)).

□

3.3 Arbres 3-réguliers plans finis décorés

Dans cette section, on définit et on dénombre des arbres $3-$réguliers particuliers, appelés les arbres décorés.

Définition IV.49 *Un arbre enraciné est la donné d'un arbre et d'un sommet de l'arbre, appelé la racine de l'arbre.*

Les arêtes sont orientés dans le sens de la racine vers les feuilles.

La racine est l'unique sommet n'admettant pas de parent. Tous les autres sommets admettent un unique parent.

La racine et les sommets intérieurs admettent des fils (ses sommets adjacents).

Dans un arbre enraciné et ordonnée, les fils sont ordonnés : on parle du $j-$ième fils d'un sommet intérieur. On parle aussi de sous-arbre adjacent et du $j-$ième sous-arbre d'un sommet intérieur.

Un arbre décoré est la donné d'un arbre planaire et d'une décoration, à savoir soit une feuille de l'arbre, distinguée par une croix, soit une arête orientée, distinguée par une flêche sur l'arête.

Pour tout entier $k \geq 1$, on note $\mathcal{T}_k^d$ l'ensemble des arbres $3-$réguliers plans finis décorés à $2k+2$ sommets.

On note $\mathcal{T}^d = \bigcup_{k\geq 1} \mathcal{T}_k^d$ l'ensemble des arbres $3-$réguliers décorés.

On montre le résultat principal suivant :

Proposition IV.50 *Pour tout entier $k \geq 0$, l'ensemble $\mathcal{T}_k^d$ des arbres $3-$réguliers plans finis décorés à $2k+2$ sommets est dénombré par la somme de deux nombres de Catalan consécutifs :*

$$card(\mathcal{T}_k^d) = c_{k+1} + c_k.$$

Preuve : La démonstration fait intervenir les résultats partiels suivants sur les sous ensembles disjoints $\mathcal{T}^\times$ et $\mathcal{T}^\uparrow$, des arbres $3-$réguliers décorés par une feuille (proposition (IV.54)) et des arbres $3-$réguliers décorés par une arête orientée (proposition (IV.63)).

□

Définition IV.51 *On note $\mathcal{O}_{\mathcal{T}}$ l'injection canonique d'oubli qui à un arbre $3-$régulier décoré associe le même arbre $3-$régulier pour lequel on oublie la notion de décroration :*

$$\mathcal{O}_{\mathcal{T}} : \mathcal{T}^d \longrightarrow \mathcal{T}$$

Remarque IV.52 *Dans le plan orienté, les arbres $3-$réguliers décorés sont de 3 types :*

- *Soit l'arbre est décoré par une feuille. Cette feuille admet un unique fils et les sommets intérieurs admettent 2 fils ordonnés.*

  Ainsi, un arbre décoré par une feuille est un arbre $3-$régulier enraciné par cette feuille (ou arbre binaire enraciné).
- *Soit l'arbre est décoré par une arête orientée dont l'origine est une feuille. Dans ce cas, il est clair que l'arbre admet au moins 1 arête et au moins 2 feuilles.*
- *Soit l'arbre est décoré par une arête orientée dont l'origine est un sommet intérieur. Le sommet intérieur admet trois sous-arbres ordonnés. On représentera un tel arbre en plaçant ce sommet intérieur en haut et ses sous-arbres adjacents au dessous, le premier sous-arbres déterminé par l'arête ordonnée situé à gauche, le second sous-arbre au milieu et le troisième sous-arbre à droite.*

L'ensemble $\mathcal{T}^{\times}$ des arbres décorés par une feuille.

Définition IV.53 *L'ensemble $\mathcal{T}_k^{\times}$ est l'ensemble des arbres $3-$réguliers plans finis décorés par une feuille à $2k+2$ sommets (ou arbres **f-décorés** à $2k+2$ sommets).*

On note $\mathcal{T}^{\times} = \bigcup_{k\geq 0} \mathcal{T}_k^{\times}$ l'ensemble des arbres $3-$réguliers f-décorés.

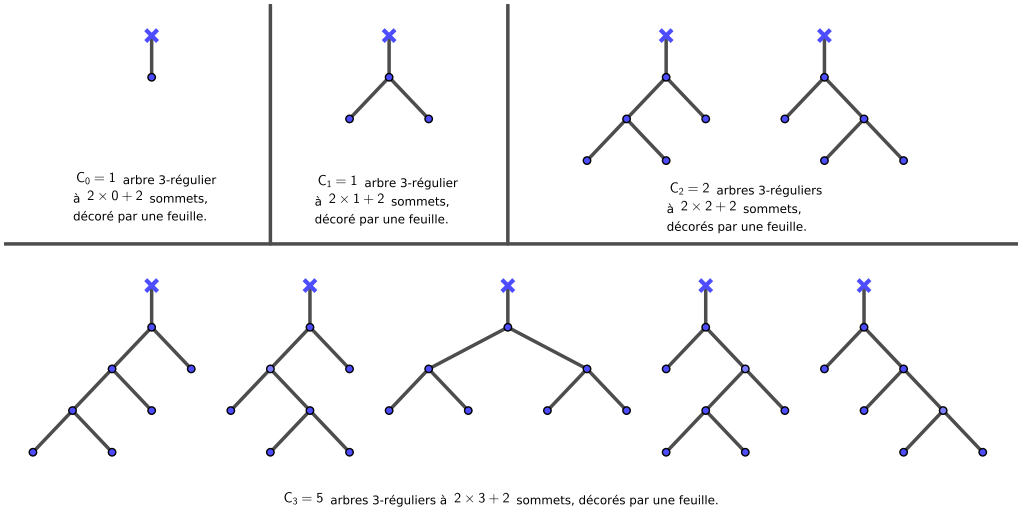


FIGURE IV.5 – Les arbres $3-$ réguliers f-décorés à 2, 4, 6 et 8 sommets de $\mathcal{T}_0^{\times}$, $\mathcal{T}_1^{\times}$, $\mathcal{T}_2^{\times}$ et $\mathcal{T}_3^{\times}$.

Proposition IV.54 *L'ensemble $\mathcal{T}^{\times}$ des arbres 3−réguliers plans finis f-décorés est dénombré par la suite des nombres de Catalan et pour tout entier k, on a :*

$$card(\mathcal{T}_k^{\times}) = c_k$$

où c_k est le $k-$ième nombre de Catalan : $c_k = \dfrac{1}{k+1}\dbinom{2k}{k}$.

Preuve : Notons f_k le nombre d'arbres 3−réguliers f-décorés.

L'unique arbre 3−régulier f-décoré à 2 sommets est l'arbre . Donc $f_0 = 1$.

Pour tout entier $k \geq 0$, l'unique fils de la racine d'un arbre 3−régulier f-décoré à $2(k+1)+2$ sommets admet deux sous-arbres ordonnés, un sous-arbre droit à $2k_1+2$ sommets et un sous-arbre gauche à $2k_2+2$ sommets tels que $2(k+1)+2 = 2k_1+2+2k_2+2-1+1$. Donc $k = k_1+k_2$.

Donc $f_{k+1} = \sum\limits_{k_1+k_2=k} f_{k_1}f_{k_2} = \sum\limits_{k_1=0}^{k} f_{k_1}f_{k-k_1}$.

La suite f_k satisfait la même relation de récurrence que la suite des nombres de Catalan

$$\begin{cases} c_{n+1} & = & \sum_{k=0}^{n} c_k c_{n-k} \\ c_0 & = & 1 \end{cases}.$$

□

Remarque IV.55 *L'ensemble des arbres 3−réguliers f-décorés est clairement en bijection avec l'ensemble des arbres trivalents plantés appelés "planted trivalent plane trees" dans [St2].*

L'ensemble $\mathcal{T}^{\uparrow}$ des arbres décorés par une arête orientée.

Définition IV.56

- *Pour tout entier $k \geq 1$, on note $\mathcal{T}_k^{\uparrow}$ l'ensemble des arbres 3−réguliers plans finis à $2k+2$ sommets, décorés par une arête (ou arbres 3−réguliers **a-décorés**).*
  On note $\mathcal{T}^{\uparrow} = \bigcup_{k\geq 1}\mathcal{T}_k^{\uparrow}$ l'ensemble des arbres 3−réguliers a-décorés.
- *Pour tout entier $k \geq 1$, on note $\mathcal{T}_k^{\uparrow f}$ l'ensemble des arbres 3−réguliers plans finis à $2k+2$ sommets, décorés par une arête sortant d'une feuille (ou arbres 3−réguliers **af-décorés**).*
  On note $\mathcal{T}^{\uparrow f} = \bigcup_{k\geq 1}\mathcal{T}_k^{\uparrow f}$ l'ensemble des arbres 3−réguliers af-décorés.
- *Pour tout entier $k \geq 1$, on note $\mathcal{T}_k^{\uparrow i}$ l'ensemble des arbres 3−réguliers plans finis à $2k+2$ sommets, décorés par une arête sortant d'un sommet intérieur (ou arbres 3−réguliers **ai-décorés**).*
  On note $\mathcal{T}^{\uparrow i} = \bigcup_{k\geq 1}\mathcal{T}_k^{\uparrow i}$ l'ensemble des arbres 3−réguliers ai-décorés.

Remarque IV.57 *Il est clair que* $\mathcal{T}_k^{\uparrow} = \mathcal{T}_k^{\uparrow f} \sqcup \mathcal{T}_k^{\uparrow i}$ *pour tout entier* $k \geq 1$ *et* $\mathcal{T}^{\uparrow} = \mathcal{T}^{\uparrow f} \sqcup \mathcal{T}^{\uparrow i}$.

Proposition IV.58 *L'ensemble* $\mathcal{T}^{\uparrow f}$ *des arbres* $3-$*réguliers af-décorés est en bijection avec l'ensemble* $\mathcal{T}^{\times}$ *des arbres* $3-$*réguliers f-décorés. Et pour tout entier* k*, on a :*

$$\mathcal{T}_k^{\uparrow f} \simeq \mathcal{T}_k^{\times}.$$

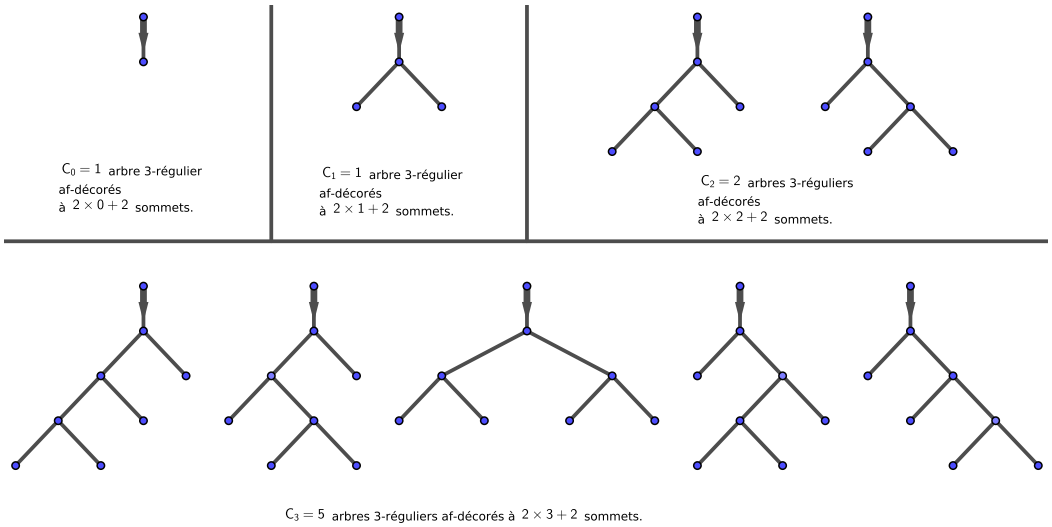


FIGURE IV.6 – Les arbres $3-$ réguliers af-décorés à 2, 4, 6 et 8 sommets de $\mathcal{T}_0^{\uparrow \mathrm{f}}$, $\mathcal{T}_1^{\uparrow \mathrm{f}}$, $\mathcal{T}_2^{\uparrow \mathrm{f}}$ et $\mathcal{T}_3^{\uparrow \mathrm{f}}$.

Preuve : Il est clair que l'application de $\mathcal{T}^{\times}$ dans $\mathcal{T}^{\uparrow \mathrm{f}}$ qui a un arbre décoré par une feuille associe l'arbre décoré par l'arête sortante de cette feuille est une bijection. L'application réciproque est l'application de $\mathcal{T}^{\times}$ dans $\mathcal{T}^{\uparrow \mathrm{f}}$ qui à un arbre décoré par une arête sortante d'une feuille associe l'arbre décoré par cette feuille.

□

Corollaire IV.59 *Pour tout entier* k*, l'ensemble* $\mathcal{T}^{\uparrow f}$ *des arbres* $3-$*réguliers af-décorés est dénombré par la suite des nombres de Catalan : Pour tout entier* k*, on a :*

$$card(\mathcal{T}_k^{\uparrow f}) = c_k$$

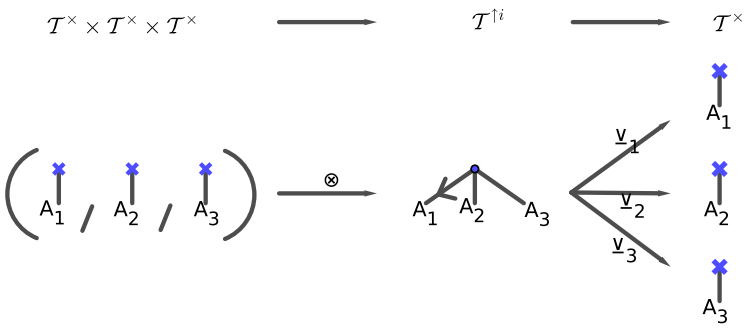
où c_k *est le* $k-$*ième nombre de Catalan.*

Preuve : C'est une conséquence directe de la bijection mis en évidence à la proposition (IV.58) et du cardinal de $\mathcal{T}_k^{\times}$ donné à la proposition (IV.54).

□

Définition IV.60 *Soient k_1, k_2 et k_3 des entiers ≥ 0. Soit $k = k_1 + k_2 + k_3 + 1 \geq 1$.*

On appelle "greffe" l'application $\otimes : \mathcal{T}_{k_1}^{\times} \times \mathcal{T}_{k_2}^{\times} \times \mathcal{T}_{k_3}^{\times} \longrightarrow \mathcal{T}_k^{\uparrow i}$ qui assemble trois arbres $3-$réguliers f-décorés (A_1, A_2, A_3), en faisant coïncider leurs racines de sorte que A_1 soient le sous-arbre gauche, A_2 soit le sous-arbre central et A_3 soit le sous-arbre droit de l'arbre ai-décoré $\otimes(A_1, A_2, A_3)$:



On note $\underline{\vee}_1$, $\underline{\vee}_2$ et $\underline{\vee}_3$ les applications de $\mathcal{T}_k^{\uparrow i}$ dans $\mathcal{T}^{\times}$ qui a tout arbre $3-$régulier ai-décoré A associe réciproquement le premier, deuxième et troisième sous-arbre de A.

Proposition IV.61 *L'ensemble des arbres $3-$réguliers ai-décorés est en bijection avec l'ensemble des arbres $3-$réguliers f-décorés au cube :*

$$\mathcal{T}^{\uparrow i} \simeq (\mathcal{T}^{\times})^3.$$

Et pour tous entiers k, k_1, k_2 et k_3 tels que $k = k_1 + k_2 + k_3 + 1 \geq 1$, on a :

$$\mathcal{T}_k^{\uparrow i} \simeq \bigcup_{k_1+k_2+k_3=k-1} \mathcal{T}_{k_1}^{\times} \times \mathcal{T}_{k_2}^{\times} \times \mathcal{T}_{k_3}^{\times}$$

Preuve : Pour tout arbre $3-$régulier ai-décoré A, on a : $\otimes(\underline{\vee}_1(A), \underline{\vee}_2(A), \underline{\vee}_3(A)) = A$.

Et pour tous arbres $3-$réguliers f-décorés A_1, A_2, A_3, on a : $(\underline{\vee}_1, \underline{\vee}_2, \underline{\vee}_3)(\otimes(A_1, A_2, A_3)) = (A_1, A_2, A_3)$.

Considérant qu'une greffe de 3 arbres f-décorés à $2k_1 + 2$, $2k_2 + 2$ et $2k_3 + 2$ sommets enlève la feuille de chacun de ces arbres f-décorés et crée un sommet intérieur, on obtient un arbre ai-décoré à $(2k_1 + 2 - 1) + (2k_2 + 2 - 1) + (2k_3 + 2 - 1) + 1 = 2(k_1 + k_2 + k_3 + 1) + 2$ sommets.

□

Corollaire IV.62 *Pour tout entier k, l'ensemble $\mathcal{T}_k^{\uparrow i}$ des arbres $3-$réguliers ai-décorés est dénombré par la suite des différences de deux nombres de Catalan consécutifs :*

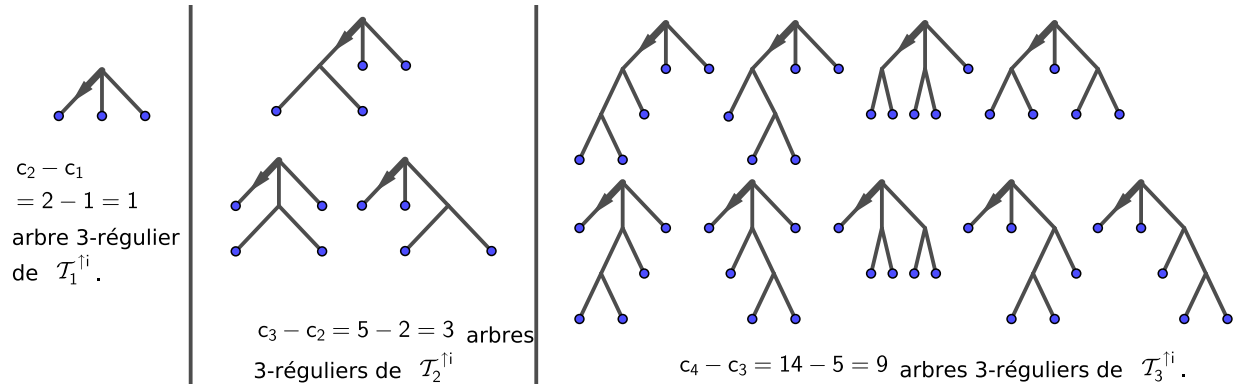


FIGURE IV.7 – Les arbres 3− réguliers ai-décorés de $\mathcal{T}_1^{\uparrow \mathrm{i}}$, $\mathcal{T}_2^{\uparrow \mathrm{i}}$ et $\mathcal{T}_3^{\uparrow \mathrm{i}}$.

$$card(\mathcal{T}_k^{\uparrow i}) = c_{k+1} - c_k$$

où c_k est le $k-$ième nombre de Catalan.

Preuve : Il est clair qu'un arbre 3−réguliers à 2 sommets n'a pas de sommet intérieur. D'où $card(\mathcal{T}_0^{\uparrow \mathrm{i}}) = 0$.

Pour $k \geq 1$, d'après les propositions (IV.54) et (IV.61), on a $card(\mathcal{T}_k^{\uparrow \mathrm{i}}) = \sum\limits_{k_1+k_2+k_3=k-1} c_{k_1} c_{k_2} c_{k_3}$.

$$\begin{aligned}
\text{D'où :} \quad card(\mathcal{T}_k^{\uparrow \mathrm{i}}) &= \sum_{k_1=0}^{k-1} c_{k_1} \sum_{k_2=0}^{k-1-k_1} c_{k_2} c_{(k-1-k_1)-k_2} \\
&= \sum_{k_1=0}^{k-1} c_{k_1} c_{k-k_1} \qquad \text{car } c_{n+1} = \sum_{i=0}^{n} c_i c_{n-i} \text{ pour } n = k - k_1 - 1 \geq 0. \\
&= \sum_{k_1=0}^{k} c_{k_1} c_{k-k_1} - c_k c_0 \\
&= c_{k+1} - c_k \qquad \text{car } c_{n+1} = \sum_{i=0}^{n} c_i c_{n-i} \text{ pour } n = k \geq 0.
\end{aligned}$$

□

Proposition IV.63 *Pour tout entier $k \geq 1$, l'ensemble $\mathcal{T}_k^{\uparrow}$ des arbres 3−réguliers plans finis a-décorés à $2k+2$ sommets est dénombré par la suite des nombres de Catalan :*

$$card(\mathcal{T}_k^{\uparrow}) = c_{k+1}.$$

Preuve : On a : $\mathcal{T}_k^{\uparrow} = \mathcal{T}_k^{\uparrow \mathrm{i}} \sqcup \mathcal{T}_k^{\uparrow \mathrm{f}}$. On conclut avec les propositions (IV.62) et (IV.59).

□

3.4 Les châteaux maximaux du noyau via les arbres 3−réguliers

Dans cette section, met en évidence une bijection entre l'ensemble $\mathcal{T}^{\uparrow}$ des arbres 3−réguliers décorés et l'ensemble K_B des mots maximaux du noyau. On dénombre ainsi l'ensemble des

mots maximaux du noyau en réinvestissant les résultats sur les arbres décorés de la partie (3.3).

On associe à un arbre 3−régulier décoré, un mot maximal du noyau K_B en associant à une arrête la lettre 1 et à une feuille la lettre 0 et en contournant l'arbre dans le sens anti-horaire à partir de la décoration, sans tenir compte des sommets intérieurs.

En notation condensée, on code un arbre binaire par des mots sur l'alphabet des entiers non nuls $\{1, 2, 3, \cdots\}$ en comptant le nombre d'arêtes entre deux feuilles, en partant de la décoration, dans le sens anti-horaire.

La notation binaire et la notation condensée d'un arbre 3−régulier décoré est illustrée sur la figure (IV.8) avec l'exemple d'un arbre 3−régulier f-décoré à 2 noeuds et 3 feuilles.

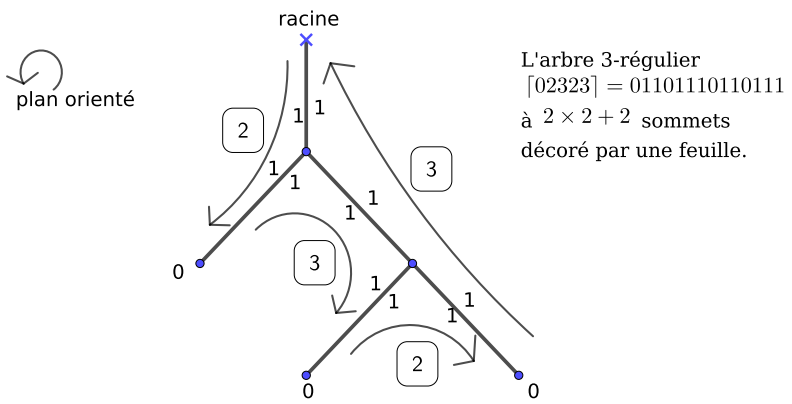


FIGURE IV.8 – Lecture anti-horaire d'un arbre 3−régulier décoré par une feuille.

Exemple IV.64

L'unique arbre 3−*régulier décoré par une feuille à* $2 \times 0 + 2$ *sommets est l'arbre* , *associé au château* 0101.

L'unique arbre 3−*régulier décoré par une arête (sortant d'une feuille) à* $2 \times 0 + 2$ *sommets est l'arbre* , *associé au château* 1010.

Proposition IV.65 *Soit* k *en entier* ≥ 0.

1. *L'ensemble des châteaux maximaux d'indice* $\frac{3k+3}{6}$ *commençant par un* 0 *(et terminant par un* 1*) est en bijection avec l'ensemble* $\mathcal{T}_k^{\times}$ *des arbres* 3−*réguliers f-décorés à* $2k + 2$ *sommets.*
2. *L'ensemble des châteaux maximaux d'indice* $\frac{3k+3}{6}$ *terminant par un* 0 *(et commençant par un* 1*) est en bijection avec l'ensemble* $\mathcal{T}_k^{\uparrow f}$ *des arbres* 3−*réguliers af-décorés à* $2k+2$ *sommets.*

3. *L'ensemble des châteaux maximaux d'indice* $\frac{3k+3}{6}$ *commençant et terminant par un* 1 *est en bijection avec l'ensemble* $\mathcal{T}_k^{\uparrow i}$ *des arbres* $3-$*réguliers ai-décorés à* $2k+2$ *sommets.*

Preuve : C'est une conséquence de la bijection entre les arbres $3-$réguliers et les orbites des châteaux maximaux du noyau à permutation près de la proposition (IV.44) et la définition des arbres décorés dont la décoration détermine le début du mot de K_B associé.

□

Corollaire IV.66 *Soit* k *en entier* ≥ 0. *On a :*

$$\begin{array}{rcccccl} card(\mathcal{C}^{\max}_{\frac{3k+3}{6}} \bigcap 0\{0,1\}^*1) & = & card(\mathcal{C}^{\max}_{\frac{3k+3}{6}} \bigcap 1\{0,1\}^*0) & = & card(\mathcal{T}_k^{\times}) & = & c_k, \\ et & & card(\mathcal{C}^{\max}_{\frac{3k+3}{6}} \bigcap 1\{0,1\}^*1) & = & card(\mathcal{T}_k^{\uparrow}) & = & c_{k+1} - c_k \end{array}$$

où c_k *est le* $k-$*ième nombre de Catalan.*

Preuve : C'est une conséquence de la proposition (IV.65), de la proposition (IV.54) et des corollaires (IV.59) et (IV.62).

□

Corollaire IV.67 *L'ensemble* K_B^{max} *des châteaux maximaux du noyau est en bijection avec l'ensemble des arbres décorés et on a, pour tout entier* $k \geq 0$ *:*

$$card(\mathcal{C}^{\max}_{\frac{3k}{6}}) = c_{k-1} + c_k$$

où c_k *est le* $k-$*ième nombre de Catalan avec* $c_{-1} = 0$.

Preuve : L'union suivante est disjointe :

$$\mathcal{C}^{\max}_{\frac{3k}{6}} = \{\emptyset\} \sqcup \big(\mathcal{C}^{\max}_{\frac{3k+3}{6}} \bigcap 0\{0,1\}^*1\big) \sqcup \big(\mathcal{C}^{\max}_{\frac{3k+3}{6}} \bigcap 1\{0,1\}^*0\big) \sqcup \big(\mathcal{C}^{\max}_{\frac{3k+3}{6}} \bigcap 1\{0,1\}^*1\big).$$

□

3.5 Les châteaux maximaux de $[0]_B$ et $[00]_B$.

Avec les relations ensemblistes entre $K_B^{\max} = \mathcal{C}^{\max}_{\frac{3\mathbb{N}}{6}}$, $\mathcal{C}^{\max}_{\frac{3\mathbb{N}+1}{6}}$ et $\mathcal{D}^{\max} = \mathcal{C}^{\max}_{\frac{3\mathbb{N}+2}{6}}$ de la proposition (IV.42) de la section (3.1), et les résultats combinatoires sur l'ensemble des châteaux maximaux du noyau K_B de la section (3.5), on en déduit des propriétés sur l'ensemble des châteaux maximaux de $[0]_B$ et de $[00]$.

Proposition IV.68 *Soit k en entier ≥ 0.*

1. *L'ensemble des châteaux maximaux d'indice $\frac{3k+2}{6}$ (l'ensemble des donjons maximaux) est en bijection avec l'ensemble $\mathcal{T}_k^{\times}$ des arbres $3-$réguliers enracinés par une feuille à k noœuds.*
2. *L'ensemble des châteaux maximaux d'indice $\frac{3k+1}{6}$ est en bijection avec l'ensemble $\mathcal{T}_k^{\times}$ des arbres $3-$réguliers enracinés par une feuille à k noœuds.*

Preuve : C'est une conséquence du corollaire (IV.42) et de la proposition (IV.65).

□

Corollaire IV.69 *Soit k en entier ≥ 0.*

$$card(\mathcal{C}^{\max}_{\frac{3k+1}{6}}) = card(\mathcal{C}^{\max}_{\frac{3k+2}{6}}) = c_k$$

Preuve : C'est une conséquence directe de la proposition (IV.68) et du corollaire (IV.66).

□

Le lemme suivant qui se déduit du corollaire IV.69, n'est pas nécessaire dans cette partie. Il est utile pour le chapitre (V) sur le modèle entier sur lequel l'expansion $V = (ab \to (a+1)0(b+1))$ est très proche de l'expansion en notation condensée $ab \to (a+1)2(b+1)$ sur les châteaux maximaux.

Lemme IV.70 *Soit δ un entier.*

L'ensemble des mots de longueur $l \geq 3$, engendrés par l'expansion $ab \to (a+1)\delta(b+1)$, sur le mot $\delta\delta\delta$, est de cardinal c_{l-2}, où c_k est le $k-$ième nombre de Catalan.

On a, avec la notation condensée (voir remarque (IV.43)) :

$$\mathcal{C}_{\frac{3k+2}{6}} = \langle \lceil 11 \rceil | ab \to (a+1)2(b+1) \rangle = \{\lceil 11 \rceil\} \cup \langle \lceil 222 \rceil | ab \to (a+1)2(b+1) \rangle.$$

Par le corollaire (IV.69), le lemme est vérifié pour $\delta = 2$.

Pour $\delta \neq 2$, le résultat découle de la une bijection évidente entre l'ensemble $\langle \lceil 222 \rceil | ab \to (a+1)2(b+1) \rangle$ et l'ensemble $\langle \lceil \delta\delta\delta \rceil | ab \to (a+1)\delta(b+1) \rangle$ par translation de $\delta - 2$.

4 Permutation circulaire sur un sous-monoïde

4.1 Sous-monoïde libre

Dans cette partie, on étudie des sous-monoïdes engendrés par des familles $W = (w_i)_{i \in I}$ de mots sur l'alphabet binaire B^* indéxées par un ensemble I dénombrable.

Plus précisément, si le sous-monoïde engendré est libre, tout mot de B^* admet au plus une factorisation dans W^* et la famille W est une base du sous-monoïde engendré W^*. Le sous-monoïde engendré W^* s'identifie au monoïde libre I^*.

Définition IV.71 *Soit Σ un alphabet.*

- *Le monoïde $\mathcal{M}_W$ engendré par une famille de mots $W = (w_i)_{i\in I}$ de Σ^* indéxée par un ensemble I, est l'image du morphisme de monoïde*

$$\begin{array}{rccc} \varphi_W : & I^* & \longrightarrow & \mathcal{M}_W \subset \Sigma^* \\ & i_1, i_2, ...i_n & \longmapsto & w_{i_1} w_{i_2} ... w_{i_n}. \end{array}$$

- *Une famille $W = (W_i)_{i\in I}$ est génératrice d'un sous-monoïde $\mathcal{M}$ de Σ^* si $Im(\varphi_W) = \mathcal{M}$.*
- *Un famille $W = (W_i)_{i\in I}$ est libre si le morphisme de monoïde φ_W est injectif.*

Proposition IV.72 *Soit $W = (w_i)_{i\in I}$ une famille de mots sur un alphabet Σ^*.*

Le sous-monoïde $\mathcal{M}_W$ engendré par W est libre de base W si et seulement si la famille génératrice W de $\mathcal{M}_W$ est libre. Dans ce cas, on note $\mathcal{M}_W = W^*$.

Remarque IV.73 *En théorie des langages, une famille libre est appelée un code. Les mots du code sont les facteurs premiers du monoïde engendré W^* : tout mot de W^* admet une unique écriture dans la base W.*

Le mot vide est dans le monoïde engendré car $\emptyset = \varphi_W(\emptyset)$. Mais le mot vide n'appartient jamais à une famillle libre (un code). Autrement, le mot vide aurait plusieurs factorisations $\emptyset = \emptyset.\emptyset$.

Définition IV.74 *Soit W une famille libre sur un alphabet Σ. Soit w un mot du sous-monoïde W^* de Σ^*.*

On appelle $W-$factorisation de w l'unique factorisation de w sur la famille libre W :

$$w = w_1 w_2 ... w_n \text{ avec } w_i \in W.$$

On appelle $W-$longueur de w le nombre de facteur w_i dans sa $W-$factorisation, notée $\lambda_W(w)$.

Exemple IV.75

1. *Le famille $W = \{w_1, w_2\} = \{00, 000\}$ n'est pas libre. Le morphisme φ_W n'est pas injectif, on a : $\varphi_W(1.1.1) = w_1^3 = 000000 = w_2^2 = \varphi_W(2, 2)$.*
2. *Soit $k \in \mathbb{N}$. Les mots de longueur nk, $n \in \mathbb{N}$, sur un alphabet Σ forment un sous-monoïde libre de Σ^*, engendré par les mots de longueur k.*

   Un mot w de longueur nk sur l'alphabet Σ est de W_k-longueur n ($\lambda_{W_k}(w) = n$).

Si l'alphabet Σ est fini, la famille libre W_k des mots de longueur k est finie.

Pour $k = 1$, la famille libre W_1 est l'alphabet Σ.

3. *L'ensemble des mots $W_{10^*} = \{10^k, k \geq 0\}$ sur l'alphabet $B = \{0, 1\}$ est une famille libre infini dénombrable. Le monoïde libre engendré est l'ensemble des mots de Σ^* qui commencent par 1 (et le mot vide).*

   Preuve : Si un mot admet deux écritures $10^{i_1}10^{i_2}\cdots 10^{i_n}$ et $10^{j_1}10^{j_2}\cdots 10^{j_m}$ sur la famille W_{10^*}, avec $i_k, j_k \in \mathbb{N}$, par unicité de la décomposition sur la base $\{0, 1\}$ du monoïde libre B^*, on a : $n = m$ et $i_k = j_k$ pour tout indice $1 \leq i \leq n$. Ainsi le morphisme $\varphi_{W_{10^*}}$ est injectif.

   Donc la famille W_{10^*} est libre et on a : $W^*_{10^*} = 1B^* \cup \{\emptyset\}$.

□

4. *Par permutation des lettres 0 et 1, il est clair que l'ensemble des mots $W_{01^*} = \{01^k, k \geq 0\}$ sur l'alphabet $B = \{0, 1\}$ est une famille libre. Le monoïde libre engendré est l'ensemble des mots qui commencent par 0 (et le mot vide) et on a : $W^*_{10^*} \simeq W^*_{01^*} = 0B^* \cup \{\emptyset\}$.*

5. *L'ensemble $W_{11^*0^*0} = \{1^k0^l, k, l \geq 1\}$ est une base infinie dénombrable de l'ensemble des mots de B^* qui commencent par 1 et qui terminent par 0 (et le mot vide) et on a : $W^*_{11^*0^*0} = 1B^*0 \cup \{\emptyset\}$.*

   Par permutation des lettres 0 et 1, l'ensemble $W_{00^*1^*1} = \{0^k1^l, k, l \geq 1\}$ est une base de l'ensemble des mots de B^* qui commencent par 0 et qui terminent par 1 (et le mot vide) et on a : $W_{11^*0^*0} \simeq W_{00^*1^*1} = 0B^*1 \cup \{\emptyset\}$.

4.2 Permutations circulaires

Étant donné une famille libre $W = \{w_i)_{i\in I}$, le groupe des entiers relatifs $(\mathbb{Z}, +, 0)$ agit par permutation circulaire sur les mots de $W-$longueur donné :

Définition IV.76 ($W-$Permutation circulaire) *Soit $(W_i)_{i\in I}$ une famille libre indéxée par un ensemble $I \subset \mathbb{N}$. L'action de permutation circulaire du groupe additif $(\mathbb{Z}, +, 0)$ sur le monoïde libre I^* induit une action de permutation sur le monoïde $\mathcal{M}_W$ par décalage circulaire à droite (translation à droite) :*

$$\begin{array}{rlcl} \tau_W : & \mathbb{Z} \times W^* & \longrightarrow & W^* \\ & (1, w_1w_2...w_n) & \longmapsto & 1 \cdot_W (w_1w_2...w_n) = (w_nw_1w_2...w_{n-1}) \end{array}$$

Remarque IV.77 *Sur l'alphabet $B = \{0, 1\}$, il est clair que le nombre de 0 et de 1 dans un mot ne changent pas par permutation circulaire. Donc la somme $\sigma(w)$, la longueur $\lambda(w)$ et l'indice $Ind(w)$ d'un mot w de B^* sont invariants par permutation circulaire.*

Proposition IV.78 *Soit W une famille libre sur un alphabet Σ.*

L'ensemble des mots de W^* de $W-$longueur donné est stable par l'action de permutation circulaire.

Preuve : Comme $1 \cdot_W (w_1 w_2 ... w_n) = (w_n w_1 w_2 ... w_{n-1})$, par unicité de la $W-$factorisation sur W^*, il est clair que $\lambda_W(1 \cdot_W (w)) = \lambda_W(w)$.

□

Définition IV.79 (Orbite et Stabilisateur d'un mot par une $W-$permutation circulaire)

Soit W une famille libre sur un alphabet Σ.

L'orbite $\mathbb{Z} \cdot_W w$ (ou simplement $\mathbb{Z}w$) d'un mot w par une $W-$ permutation circulaire est l'ensemble des mots $k \cdot_W w$ pour tout $k \in \mathbb{N}$.

Le stabilisateur $St_W(w)$ d'un mot w par une $W-$ permutation circulaire est l'ensemble des entiers $k \in \mathbb{N}$ tel que $k \cdot_W w = w$.

Notation : Pour simplifier les notations, lorsqu'il n'y a pas d'ambiguïté sur la famille libre W considérée, on notera $\tau_W(k, w) = k \cdot w$ l'image d'un mot w par la $W-$permutation circulaire, $\mathbb{Z}w$ l'orbite d'un mot w, et $St(w)$ le stabilisateur d'un mot w.

Proposition IV.80 *Soit W une famille libre sur un alphabet Σ. Pour tout mot w du sous-monoïde W^*, l'orbite de w sous l'action de permutation circulaire est finie et on a :*

$$St(w) = card(\mathbb{Z}w)\mathbb{Z}.$$

Preuve : Considérant la $W-$factorisation $w = w_1 w_2 \cdots w_n$ d'un mot w, l'orbite de w est composée de mots de longueur finie $\lambda_W(w)$ sur l'ensemble fini $\{w_1, w_2, \cdots, w_n\}$. Donc l'orbite de w est finie.

L'application $\begin{array}{rccc} \tau_w : & \mathbb{Z}/St(w) & \rightarrow & \mathbb{Z}w \\ & k & \longmapsto & k \cdot w \end{array}$ est une bijection, d'où le résultat.

□

Proposition IV.81 *Soit W une famille libre sur un alphabet Σ. Le cardinal de l'orbite d'un mot w de W^* par une $W-$permutation circulaire divise sa $W-$longueur :*

$$card(\mathbb{Z}w) \mid \lambda_W(w).$$

Preuve : Il est clair que $\lambda_W(w) \cdot w = w$: le mot $\lambda_W(w)$ est dans le stabilisateur $St(w) = card(\mathbb{Z}w).\mathbb{Z}$ de w (voir proposition (IV.80)).

□

Corollaire IV.82 *Soit W une famille libre sur un alphabet Σ.*

Pour tout mot w de W^*, il existe un mot p de W^* tel que

$$w = p^{\frac{\lambda_W(w)}{card(\mathbb{Z}w)}}.$$

Preuve : On note $m = card(\mathbb{Z}w)$. Comme $m \mid \lambda_W(w)$, on note $\lambda_W(w) = km$ et la $W-$factorisation de w est de la forme $w = (w_1w_2\cdots w_m)(w_{m+1}w_{m+2}\cdots w_{2m})\cdots(w_{(k-1)m+1}w_{(k-1)m+2}\cdots w_{km})$.

Comme $m.w = w$, on a :

$$\begin{array}{lllll} & (w_{(k-1)m+1}w_{(k-1)m+2}\cdots w_{km}) & (w_1w_2\cdots w_m) & \cdots & (w_{(k-2)m+1}w_{(k-2)m+2}\cdots w_{(k-1)m}) \\ = & (w_1w_2\cdots w_m) & (w_{m+1}w_{m+2}\cdots w_{2m}) & \cdots & (w_{(k-1)m+1}w_{(k-1)m+2}\cdots w_{km}). \end{array}$$

Par unicité de la $W-$factorisation, on a :

$$w_{(k-1)m+1}w_{(k-1)m+2}\cdots w_{km} = w_1w_2\cdots w_m = \cdots = w_{(k-2)m+1}w_{(k-2)m+2}\cdots w_{(k-1)m}.$$

D'où : $w = (w_1w_2\cdots w_m)^k$, avec $k = \dfrac{\lambda_W(w)}{card(\mathbb{Z}w)}$.

□

4.3 Action de $W-$permutation sur l'ensemble $K_B^{\max}$ des châteaux maximaux du noyau.

Dans cette partie, on considère des familles libres particulières $W = (W_i)_{i\in I}$ sur l'alphabet binaire $B = \{0,1\}$ et on étudie les orbites des mots du noyau K_B du morphisme $\mu_B : B^* \longrightarrow PSL_2(\mathbb{Z})$ par $W-$permutation circulaire.

De manière générale, le noyau K_B est stable par décalage circulaire. Ainsi, pour toute famille libre W, l'ensemble $W^* \cap K_B^{\max}$ est stable par $W-$permutation circulaire (voir proposition (IV.78)).

En particulier, l'ensemble des châteaux maximaux du noyau, d'indice fixé $\frac{3k+3}{6}$ (et de longueur fixée) est stable par $W-$permutation circulaire.

Comme l'ensemble des châteaux maximaux est en bijection avec l'ensemble $\mathcal{T}^{\mathrm{d}}$ des arbres décorés (voir proposition (IV.67)), l'action de W-permutation sur les châteaux de $W^* \cap K_B^{max}$ induit une action de permutation circulaire sur les l'ensemble des arbres trivalents décorés. L'ensemble des orbites des châteaux de $W^* \cap K_B^{max}$ pour l'action de $W-$permutation circulaire s'injecte dans l'ensemble $\mathcal{T}$ des arbres $3-$réguliers :

$$\begin{tikzcd}
W^* \cap K_B^{max} \arrow[r, hook] \arrow[d, hook] & \mathcal{T}^{\mathrm{d}} \arrow[d, hook] \\
\{W - \text{orbites des mots de } W^* \cap K_B^{max}\} \arrow[r, hook] & \mathcal{T}
\end{tikzcd}$$

L'étude des orbites sous-l'action de W-permutation circulaire pour des familles W particulières génère une suite d'entiers particulière $\{1, 1, 6, 14, 47, \ldots\}$ définie à partir des nombres de Catalan.

Lemme IV.83 *Soit w un mot maximal dans le noyau K_B.*
Si $w = ps$ avec p ou $s \in K_B$ alors $p = \emptyset$ ou $s = \emptyset$.

Preuve : Il est clair que si un mot du noyau s'écrit $w = ps$ avec l'un des facteurs p ou s dans le noyau alors l'autre facteur s ou p est aussi dans le noyau K_B car $\mu_B(p) = \mu_B(p)\mu_B(s)$. Donc les deux facteurs p et s sont des châteaux.

L'ensemble des châteaux maximaux vérifie l'équation récursive (voir corollaire (IV.42)) :

$$K_B^{\max} = \mathcal{C}^{\max}_{\frac{3\mathbb{N}}{6}} = \{\emptyset\} \sqcup 0\mathcal{D}^{\max} \sqcup \mathcal{D}^{\max}0 \cup (\mathcal{D}^{\max})^3.$$

On suppose que $w = ps$ avec $p, s \neq \emptyset$. Comme un donjon n'admet pas de préfixe strict qui soit un château, on a :

- si $w = ps$ est dans l'ensemble $0\mathcal{D}^{\max}$, alors $p = 0$ et $s \in \mathcal{D}^{\max}$. Donc $p, s \notin K_B$.
- si $w = ps$ est dans l'ensemble $\mathcal{D}^{\max}0$, alors $p \in \mathcal{D}^{\max}$ et $s = 0$. Donc $p, s \notin K_B$.
- si $w = ps$ est dans l'ensemble $(\mathcal{D}^{\max})^3$, alors $p, s \in \mathcal{D}^{\max} \cup (\mathcal{D}^{\max})^2$. Donc $p, s \notin K_B$.

Donc, soit p, soit s, est égale au mot vide.

□

Lemme IV.84 *Soit W une famille libre sur l'alphabet $B = \{0, 1\}$. Soit w un mot de $K_B^{\max}$.*
S'il existe $p \neq w \in W^*$ et $k \in \mathbb{N} \setminus \{0\}$ tel que $w = p^k$, alors $k \in \{2, 3\}$.

Preuve :

Soit $p \neq w \in W^*$ et $k \in \mathbb{N} \setminus \{0\}$ tel que $w = p^k$. On a : $\mu_B(w) = \mu_B(p^k) = \mu_B(p)^k = I$.

Donc, $\mu_B(p)$ est d'ordre fini dans le produit libre $PSL_2(\mathbb{Z}) = \langle S | S^2 \rangle * \langle U | U^3 \rangle$, conjugué à I, à S, à U ou à U^2. Donc, $\mu_B(p)$ est soit trivial et p est dans le noyau K_B, soit d'ordre 2 et p^2 est dans le noyau K_B, soit d'ordre 3 et p^3 est dans le noyau K_B.

On note $k_0 \in \{1, 2, 3\}$ l'ordre de p. Ainsi, $k \geq k_0$ et le mot w s'écrit $w = p^{k-k_0}p^{k_0}$. D'après le lemme (IV.83), on a : $p^{k-k_0} = \emptyset$. D'où $k = k_0 \in \{1, 2, 3\}$ et soit $w = p$ (impossible), soit $w = p^2$, soit $w = p^3$.

□

Proposition IV.85 *Soit W une famille libre sur l'alphabet $B = \{0, 1\}$. Pour tout mot maximal w du noyau K_B, il existe un mot p tel que*

- *soit $w = p^2$ et $Card(\mathbb{Z}w) = \frac{1}{2}\lambda_W(w)$.*
  On dit que w est un carré. On note W^{car} l'ensemble des carrés du monoïde W^*.
- *soit $w = p^3$ et $Card(\mathbb{Z}w) = \frac{1}{3}\lambda_W(w)$.*
  On dit que w est un cube. On note W^{cub} l'ensemble des cubes du monoïde W^*.
- *soit $w = \emptyset$ et $Card(\mathbb{Z}w) = 1$,*
- *soit $Card(\mathbb{Z}w) = \lambda_W(w)$.*

Dans les deux derniers cas, on dit que w est simple. On note W^{sim} l'ensemble des mots simples du monoïde W^*.

Preuve :

Le cardinal de l'orbite $\mathbb{Z}w$ d'un mot w divise sa $W-$longueur $\lambda_W(w)$ (voir proposition (IV.81)). D'après le corollaire (IV.82), il existe un mot q tel que $w = q^{\frac{\lambda_W(w)}{card(\mathbb{Z}w)}}$.

Si $card(\mathbb{Z}w) < \lambda_W(w)$ alors, d'après le lemme (IV.84), comme w est un mot maximal du noyau, soit $w = p^2$ et $card(\mathbb{Z}w) = \frac{\lambda_W(w)}{2}$, soit $w = p^3$ et $card(\mathbb{Z}w) = \frac{\lambda_W(w)}{3}$.

Sinon, $card(\mathbb{Z}w) = \lambda(w)$.

□

Remarque IV.86 *Il est clair que tout mot de l'orbite d'un mot simple est simple, tout mot de l'orbite d'un mot carré est un carré et tout mot de l'orbite d'un mot cube est un cube.*

On dit que l'orbite d'un mot simple est une orbite simple, l'orbite d'un mot carré est une orbite carrée et l'orbite d'un mot cube est une orbite cubique.

4.4 Permutation circulaire par la famille libre $W_1 = \{0, 1\}$

Dans cette partie, on considère l'action de permutation circulaire par la famille libre $W_1 = \{0, 1\}$ sur les mots maximaux du noyaux K_B. La W_1-longueur λ_{W_1} est identique à la longueur $\lambda(w)$.

Comme $W_1 = B$, la famille W_1 est génératrice de B^* et tous les mots maximaux du noyau K_B^m sont dans le sous-monoïde W_1^* engendré par W_1 :

$$W_1^* \cap K_B^{max} = K_B^{max}.$$

L'ensemble des mots maximaux du noyau d'indice non nul est engendré par l'expansion $0 \to 101101$ sur les deux châteaux maximaux 1010 et 0101 d'indice $\frac{3}{6}$ (voir proposition

(IV.37)). L'ensemble des mots du noyau à permutation près est en bijection avec l'ensemble des arbres 3−réguliers $\mathcal{T}$ (voir proposition (IV.44)). Les arbres 3−réguliers sont engendrés par l'expansion "pousse" (qui remplace une feuille par un sommet intérieur relié à deux nouvelles feuilles) sur l'unique arbre 3−régulier à 2 sommets (une arête et pas de sommets intérieur) (voir proposition (IV.48)).

Ainsi, l'ensemble des orbites des mots maximaux du noyau pour la W_1−permutation circulaire est en bijection avec l'ensemble des arbres 3−réguliers. L'ensemble des mots de $W_1^* = K_B^{max}$ est en bijection avec l'ensemble des arbres 3−réguliers décorés (soit pas une feuille, soit par une arête orientée).

Les orbites des mots maximaux du noyau sous l'action de W_1permutation sont de trois types : les orbites de mots simples, les orbites de carrés et les orbites de cubes (voir proposition (IV.85)). On montre que l'arbre 3−régulier associé à une orbite carrée admet une symétrie par rapport à une arête centrale et l'arbre 3−régulier associé á une orbite cubique admet une symétrie par rapport à un sommet intérieur (son centre).

En considérant séparément ces trois types d'orbites et les arbres 3−réguliers associés, on dénombre les orbites simples, les orbites carrés et les orbites cubes des châteaux maximaux du noyau sous l'action de W_1 permutation circulaire.

On obtient les premières valeurs des suites des nombres d'orbites simples, carrées et cubiques $N_k^{\mathrm{orb}^i}$ pour $i \in \{1, 2, 3\}$ d'indice $\frac{k+1}{2}$ et de la suite $(S_k)_k$ du nombre total d'orbites, pour $0 \leq k \leq 7$ suivantes :

k	Ind	λ	Nombre d'orbites simples $N_k^{\mathrm{orb}^1}$	Nombre d'orbites carrées $N_k^{\mathrm{orb}^2}$	Nombre d'orbites cubes $N_k^{\mathrm{orb}^3}$	Nombre total d'orbites S_k	$card(K^{\max}_{\frac{k+1}{2}})$
0	1/2	4	0	1	0	1	2
1	1	9	0	0	1	1	3
2	3/2	14	0	1	0	1	7
3	2	19	1	0	0	1	19
4	5/2	24	1	2	1	4	56
5	3	29	6	0	0	6	164
6	7/2	34	14	5	0	19	561
7	4	39	47	0	2	49	1859
k	$(k+1)/2$	$5k+4$	...	...	...	...	$c_k + c_{k+1}$

Exemple IV.87

1. *Le sous-ensemble* $K^{max}_{\frac{0}{6}} = \{\emptyset\}$ *a une orbite simple, pas d'orbite carrée, pas d'orbite cube.*

2. *Le sous-ensemble* $K^{max}_{\frac{3}{6}} = \{1010, 0101\}$ *n'a pas d'orbite simple, une orbite carré et pas d'orbite cube.*
3. *Le sous-ensemble* $K^{max}_{\frac{6}{6}} = \{110110110, 101101101, 011011011\}$ *n'a pas d'orbite simple, pas d'orbite carré et une orbite cube.*
4. *Le sous-ensemble* $K^{max}_{\frac{9}{6}} = \{11101101110110, 01110110111011, 10111011011101, 11011101101110, 01101110110111, 10110111011011, 11011011101101\}$ *n'a pas d'orbite simple, une orbite carré et pas d'orbite cube.*

Les carrés.

Dans cette partie, on étudie les orbites des carrés de $K^{\max}$. Les mots maximaux du noyau $K^{\max}$ à permutation près sont en bijection avec les arbres $3-$réguliers. En particulier, pour les carrés, on montre que les arbres $3-$réguliers sont symétriques par rapport à une arête :

Définition IV.88

Un arbre $3-$*régulier est symétrique par rapport à une arête s'il existe une arête (l'arête centrale) telle que les deux sous-arbres binaires enracinés par les deux sommets de cette arête sont identiques.*

Deux feuilles d'un arbre $3-$*régulier symétrique par rapport à une arête sont conjuguées si elles sont situ'ees à la même place dans les deux sous-arbres binaires enracinés issus des deux sommets de l'arête centrale.*

La "double expansion pousse" d'un arbre symétrique remplace 2 *feuilles conjuguées par la pousse de chacune de ces deux feuilles (une feuille est remplacée par un sommet intérieur avec* 2 *arêtes supplémentaires, reliées chacune à une nouvelle feuille).*

Remarque IV.89

1. *Un arbre* $3-$*régulier symétrique par rapport à une arête a un nombre pair* $2k \geq 0$ *de sommets intérieurs.*
2. *Un arbre* $3-$*régulier symétrique par rapport à une arête admet* $4k+2$ *sommets. Les sous-arbres binaires enracinés issus d'une arête centrale admettent chacun* $2k+1$ *sommets.*
3. *L'arête centrale d'un arbre symétrique est unique. En effet, si un arbre symétrique admet deux arêtes centrales distinctes* A_1 *et* A_2*, l'arête* A_2 *est dans un sous-arbre* SA_1 *issu de l'arête* A_1*. Ce sous-arbre* SA_1 *contient un sous-arbre issu de l'arête* A_1 *et admet donc plus de* $2k+2$ *sommets. Absurde.*

Lemme IV.90 *Pour tout entier* k *et tous châteaux maximaux* p *et* q *de* $\mathcal{C}^{\max}_{\frac{3k+1}{6}}$ *on a :*

les orbites des mots du noyau $(1p)^2$ *et* $(1q)^2$ *sont égales si et seulement si* $p = q$.

Preuve : Les mots p et q sont obtenus par une successions d'expansions $0 \to 101101$ sur le mot 0.

Les arbres 3−réguliers associés aux carrés $(1p)^2$ et $(1q)^2$ sont obtenus par une succession de "doubles expansions pousse" sur l'arbre 3−réguliers à 2 sommets associé au mot 1010.

Si les orbites des mots $(1p)^2$ et $(1q)^2$ sont égales, alors leurs arbres 3−réguliers associés sont égaux.

Par unicité de l'arête centrale, les sous-arbres binaires enracinés associés aux mots p et q sont identiques. Donc $p = q$.

La réciproque est triviale.

□

Lemme IV.91 *Tout carré de $K^{\max}$ d'indice $\geq \frac{3}{2}$ est dans l'orbite d'un carré de la forme $(1p101101s)^2$ avec $p, s \in B^*$.*

Preuve : Tout château maximal d'indice $\geq \frac{3}{2}$ est un mot de longueur $5k + 9 \geq 14$ (voir corollaire IV.40)) et admet un facteur 101101 (voir proposition (IV.39)).

Donc un carré w d'indice ≥ 1 est dans l'orbite d'un carré w' de la forme $w' = 101101s'$ avec $\lambda(s') \geq 14 - 6 = 8 > 6$. Donc le carré w' est de la forme $w' = (101101t)^2$ avec $s' = t101101t$.

Comme $K^{\max}$ est stable par réduction $101101 \to 0$, le mot $(0t)^2$ est un château maximal du noyau. Si $t = \emptyset$, le mot $(0t)^2$ n'est pas dans le noyau. Si t n'admet pas de facteur 1, le mot $(0t)^2$ n'est pas maximal. Donc le facteur t admet un facteur 1.

Finalement, le mot w est dans l'orbite d'un carré de la forme $(1p101101s)^2$, avec $s1p = t$.

□

Proposition IV.92 *L'ensemble des orbites carrés de $K^{\max}$ est en bijection avec l'ensemble des châteaux $\mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$.*

Preuve : Dans un premier temps, on montre par deux récurrences que tout mot carré de $K^{\max}_{k+\frac{1}{2}}$ est dans l'orbite d'un carré de la forme $(1u)^2$, avec $u \in \mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$ et qu'il n'y a pas de carrés d'indice entier :

D'après les exemples (IV.87), le sous-ensemble $K^{max}_{\frac{1}{2}}$ admet une unique orbite carrée, l'orbite de $(10)^2$ (et $0 \in \mathcal{C}_{\frac{3\times 0+1}{6}}$).

Soit w un carré de $K^{\max}_{k+\frac{1}{2}}$ avec $k \geq 1$. D'après le lemme (IV.91), w est dans l'orbite d'un carré de la forme $w' = (1p101101s)^2$. Comme $K^{\max}$ est stable par réduction $101101 \to 0$, le carré w' est obtenu par deux expansions $0 \to 101101$ sur le carré $(1p0s)^2$ d'indice $k - 1 + \frac{1}{2}$. Par récurrence sur k, le carré $(1p0s)^2$ est dans l'orbite d'un carré de la forme $(1u)^2$ avec $u \in \mathcal{C}_{\frac{3(k-1)+1}{6}}$.

Ainsi, w est dans l'orbite d'un mot $(1u')^2$ où u' est obtenu via l'expansion $0 \to 101101$ sur un facteur 0 de u et $u \in \mathcal{C}_{\frac{3k+1}{6}}$.

Pour les carrés d'indice entier : d'après les exemples (IV.87), les sous-ensembles K_0^{max} et K_1^{max} n'ont pas de carré.

Étant donné un carré $w \in K^{\max}$ d'indice $k \geq 1$, d'après le lemme (IV.91), le carré w est dans l'orbite d'un carré de la forme $w' = (1p101101s)^2$. Comme $K^{\max}$ est stable par réduction $101101 \to 0$, le mot $(1p0s)^2$ est un carré de $K_{k-1}^{\max}$. Par récurrence, le sous ensemble $K_{k-1}^{\max}$ n'admet pas de carré. Absurde.

Par ailleur, deux châteaux p et q distincts de $\mathcal{C}^{\max}$ déterminent deux orbites carrées $(1p)^2$ et $(1q)^2$ distinctes (voir lemme (IV.90)). Ainsi, une orbite carré de $K^{\max}$ admet un unique représentant de la forme $(1u)^2$ où u est un château de $\mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$.

Réciproquement, tout mot maximal de la forme $(1u)^2$ où u est un château de $\mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$ est un carré de $K^{\max}$.

D'où le résultat.

□

Corollaire IV.93 *Le nombre $N_k^{orb^2}$ d'orbites carrés de $K^{\max}$, d'indice $\frac{k+1}{2}$, est :*

$$N_k^{orb^2} = c_{\frac{k}{2}} = \begin{cases} 0 & \textit{si } k \textit{ est impair,} \\ c_{\frac{k}{2}} & \textit{si } k \textit{ est pair,} \end{cases}$$

où c_n est le $n-$ième nombre de Catalan si n est entier et $c_n = 0$ si $n \notin \mathbb{N}$.

Preuve : C'est une conséquence directe de la bijection de la proposition (IV.92) et du corollaire (IV.69) sur le cardinal de $\mathcal{C}^{\max}_{\frac{3k+1}{6}}$.

□

Corollaire IV.94 *Le nombre de carrés dans $K_B^{\max}$ d'indice $\frac{k+1}{2}$ est*

$$card(W^{car}_{\frac{k+1}{2}}) = \frac{5k+4}{2} c_{\frac{k}{2}}.$$

Preuve : L'orbite d'un mot carré w est de cardinal $\frac{\lambda(w)}{2}$.

La longueur d'un mot maximal w d'indice $\frac{k+1}{2}$ est $5k+4$ (voir corollaire (IV.40)).

□

Les cubes.

Dans cette partie, on étudie les orbites des cubes de $K^{\max}$. Les arbres $3-$réguliers associés aux carrés sont symétriques par rapport à une arête centrale. On montre que les arbres $3-$réguliers associés aux cubes sont symétriques par rapport à un sommet :

Définition IV.95

Un arbre $3-$régulier est symétrique par rapport à un sommet intérieur s'il existe un sommet intérieur (le centre) tel que les trois sous-arbres de ce sommet sont identiques.

Trois feuilles d'un arbre $3-$régulier symétrique par rapport à un sommet sont conjuguées si elles sont situées à la même place dans les trois sous-arbres binaires enracinés issus du centre.

La "triple expansion pousse" d'un arbre symétrique par rapport à un sommet remplace 3 feuilles conjuguées par la pousse de chacune de ces trois feuilles (une feuille est remplacée par un sommet intérieur avec 2 arêtes supplémentaires, reliées chacune à une nouvelle feuille).

Remarque IV.96

1. *Un arbre $3-$régulier symétrique par rapport à un sommet admet $3k+1$ sommets intérieurs $k \geq 0$.*
2. *Un arbre $3-$régulier symétrique par rapport à un sommet admet $6k+4$ sommets, $k \geq 0$. Les sous-arbres binaires enracinés issus du centre admettent chacun $2k+1$ sommets, $k \geq 0$.*
3. *Le centre d'un arbre symétrique est unique. En effet, si un arbre symétrique admet deux centres distincts C_1 et C_2, le centre C_2 est dans un sous-arbre issu du centre C_1. Ce sous-arbre contient un sous-arbre issu du centre C_1 et admet donc plus de $2k+2$ sommets. Absurde.*

Lemme IV.97 *Soit k un entier et p et q deux châteaux maximaux de $\mathcal{C}^{\max}_{\frac{3k+1}{6}}$.*

Les orbites des mots du noyau $(1p1)^3$ et $(1q1)^3$ sont égales si et seulement si $p = q$.

Preuve : Les mots p et q sont obtenus par une successions d'expansions $0 \to 101101$ sur le mot 0.

Les arbres $3-$réguliers associés aux cubes $(1p1)^3$ et $(1q1)^3$ sont obtenus par une succession de "triples expansions pousse" sur l'arbre $3-$réguliers à 4 sommets associé au mot 101101101.

Si les orbites des mots $(1p1)^3$ et $(1q1)^3$ sont égales, leurs arbres $3-$réguliers associés sont égaux.

Par unicité du centre, les sous-arbres binaires enracinés associés aux mots $1p1$ et $1q1$ sont identiques. Donc $p = q$.

La réciproque est triviale.

□

Lemme IV.98 *Tout cube de $K^{\max}$ d'indice ≥ 2 est dans l'orbite d'un cube de la forme $(1p101101s1)^3$ avec $p, s \in B^*$.*

Preuve : Tout château maximal d'indice ≥ 2 est un mot de longueur $5k+9 \geq 19$ (voir corollaire IV.40)) et admet un facteur 101101 (voir proposition (IV.39)).

Donc un cube w d'indice ≥ 2 est dans l'orbite d'un cube w' de la forme $w' = 101101s'$ avec $\lambda(s') \geq 19 - 6 = 13 > 12$. Donc le cube w' est de la forme $w' = (101101t)^3$ avec $s' = t101101t101101t$.

Comme $K^{\max}$ est stable par réduction $101101 \to 0$, le mot $(0t)^3$ est un château maximal du noyau.

Si $t = \emptyset$, le mot $(101101)^3$ n'est pas maximal.

Si t n'admet pas de facteur 1 le mot $(0t)^3$ n'est pas maximal.

Si le facteur t commence par 0 alors le château $(0t)^3$ n'est pas maximal. Donc $(0t)^3$ est un château est la forme $01^\alpha v01^\alpha v01^\alpha v$ avec $\alpha \geq 1$.

D'après le lemme (IV.39), on a : $\alpha \geq 2$. Donc t admet au moins un facteur 11.

Finalement, le mot w est dans l'orbite d'un carré de la forme $(1p101101s1)^3$, avec $s11p = t$.

□

Proposition IV.99 *L'ensemble des orbites cubes de $K^{\max}$ est en bijection avec l'ensemble des châteaux $\mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$.*

Preuve : La démonstration est semblable à celle de la proposition (IV.92) pour les carrés.

Dans un premier temps, on montre par deux récurrences que tout mot cube de $K^{\max}_{\frac{3k+2}{2}}$, $k \geq 1$ est dans l'orbite d'un carré de la forme $(1u1)^3$, avec $u \in \mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$ et qu'il n'y a pas de cube d'indice $\frac{3k}{2}$, ni d'indice $\frac{3k+1}{2}$ pour $k \geq 0$.

D'après les exemples (IV.87), le sous-ensemble K_1^{max} admet une unique orbite carrée, l'orbite de $(101)^3$ (et $0 \in \mathcal{C}_{\frac{3\times 0+1}{6}}$).

Soit w un cube de $K^{\max}_{\frac{3k+2}{2}}$ avec $k \geq 1$. D'après le lemme (IV.98), w est dans l'orbite d'un carré de la forme $w' = (1p101101s1)^3$. Comme $K^{\max}$ est stable par réduction $101101 \to 0$, le cube w' est obtenu par deux expansions $0 \to 101101$ sur le cube $(1p0s1)^3$ de $K^{\max}$ d'indice $\frac{3k-1}{2}$. Par récurrence sur k, le cube $(1p0s1)^3$ est dans l'orbite d'un cube de la forme $(1u1)^3$ avec $u \in \mathcal{C}_{\frac{3(k-1)+1}{6}}$.

Ainsi, w est dans l'orbite d'un mot $(1u'1)^3$ où u' est obtenu via l'expansion $0 \to 101101$ sur un facteur 0 de u et $u' \in \mathcal{C}_{\frac{3k+1}{6}}$.

Pour les cubes d'indice $\frac{3k+i}{2}$ avec $i \in \{0, 1\}$: d'après les exemples (IV.87), les sous-ensembles K_0^{max}, $K_{\frac{1}{2}}^{max}$ et $K_{\frac{3}{2}}^{max}$ n'ont pas de cube.

Étant donné un cube $w \in K^{\max}$ d'indice $\frac{3k+i}{2} \geq 2$. D'après le lemme (IV.98), w est dans l'orbite d'un cube de la forme $w' = (1p101101s1)^3$. Comme $K^{\max}$ est stable par réduction $101101 \to 0$, le mot $(1p0s1)^3$ est un cube de $K_{k-1}^{\max}$. Par récurrence, le sous ensemble $K_{k-1}^{\max}$ n'admet pas de carré. Absurde.

Par ailleurs, deux châteaux p et q distincts de $\mathcal{C}^{\max}$ déterminent deux orbites cubes $(1p1)^3$ et $(1q1)^3$ distinctes (voir lemme (IV.97)).

Ainsi, une orbite cube de $K^{\max}$ admet un unique représentant de la forme $(1u1)^3$ où u est un château de $\mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$.

Réciproquement, tout mot maximal de la forme $(1u1)^3$ où u est un château de $\mathcal{C}_{\frac{3\mathbb{N}+1}{6}}$ est un cube de $K^{\max}$.

D'où le résultat.

□

Corollaire IV.100 *Le nombre $N_k^{orb^3}$ d'orbites cubes des mots maximaux du noyau, d'indice $\frac{k+1}{2}$, est :*

$$N_k^{orb^3} = c_{\frac{k-1}{3}} = \begin{cases} 0 & si\ k \equiv_3 2\ ou\ k \equiv_3 0, \\ c_{\frac{k-1}{3}} & si\ k \equiv_3 1, \end{cases}$$

où c_n est le $n-$ième nombre de Catalan si n est entier et $c_n = 0$ si $n \notin \mathbb{N}$.

Preuve : C'est une conséquence directe de la bijection de la proposition (IV.99) et du corollaire (IV.69) sur le cardinal de $\mathcal{C}_{\frac{3k+1}{6}}^{\max}$.

□

Corollaire IV.101 *Le nombre de cubes dans $K_B^{\max}$ d'indice $\frac{k+1}{2}$ est*

$$card(W_{\frac{k+1}{2}}^{cub}) = \frac{5k+4}{3} c_{\frac{k-1}{2}}.$$

Preuve : L'orbite d'un cube w est de cardinal $\frac{\lambda(w)}{3}$.

La longueur d'un mot maximal w d'indice $\frac{k+1}{2}$ est $5k+4$ (voir corollaire (IV.40)).

□

Les mots simples.

Remarque IV.102 *On utilsera la propriété suivante sur deux nombres de Catalan pour simpifier les expressions :*

$$c_{k+1} = \frac{(2k+2)!}{(k+1)!(k+2)!} = \frac{2(k+1)(2k+1)}{(k+1)(k+2)} \frac{(2k)!}{k!(k+1)!} = \frac{4k+2}{(k+2)} c_k.$$

Proposition IV.103 *Le nombre de mots simples d'indice* $\dfrac{k+1}{2}$ *dans* K^{max} *est :*

$$card(W^{sim}_{\frac{k+1}{2}}) = (5k+4)\big(\frac{1}{k+2}c_k - \frac{1}{2}c_{\frac{k}{2}} - \frac{1}{3}c_{\frac{k-1}{3}}\big)$$

où c_n *est le* $n-$*ième nombre de Catalan si* $n \in \mathbb{N}$ *et* $c_n = 0$ *si* $n \notin \mathbb{N}$.

Preuve :

L'ensemble des mots maximaux dans le noyau d'indice $\frac{k+1}{2}$ est de cardinal $c_k + c_{k+1}$ (voir proposition (IV.63)).

Comme les ensembles disjoints $W^{sim}_{\frac{k+1}{2}}$, $W^{car}_{\frac{k+1}{2}}$ et $W^{cub}_{\frac{k+1}{2}}$ partitionne le noyau (voir proposition (IV.85)), on obtient avec les propositions (IV.94) et (IV.101) sur les carrés et les cubes du noyau :

$$card(W^{sim}_{\frac{k+1}{2}}) = c_k + c_{k+1} - \frac{5k+4}{2}c_{\frac{k}{2}} - \frac{5k+4}{3}c_{\frac{k-1}{3}}.$$

Or, $c_k + c_{k+1} = c_k + \dfrac{4k+2}{(k+2)}c_k = \dfrac{5k+4}{(k+2)}c_k$ (voir remarque (IV.102)), d'où le résultat.

□

Corollaire IV.104 *Le nombre* $N_k^{orb^1}$ *d'orbites simples de château maximaux du noyau d'indice* $\frac{k+1}{2}$ *est :*

$$N_k^{orb^1} = \frac{1}{k+2}c_k - \frac{1}{2}c_{\frac{k}{2}} - \frac{1}{3}c_{\frac{k-1}{3}}$$

où c_n *est le* $n-$*ième nombre de Catalan si* $n \in \mathbb{N}$ *et* $c_n = 0$ *si* $n \notin \mathbb{N}$.

Preuve : L'orbite d'un mot simple w est de cardinal $\lambda(w)$.

La longueur d'un mot maximal w d'indice $\frac{k+1}{2}$ est $5k+4$ (voir corollaire (IV.40)).

□

Remarque IV.105 *Les premières valeurs de la suite* $(N_k^{orb^1})_{k\geq 0}$ *sont :*

$$(N_k^{orb^1})_{k\geq 0} = \{0, 0, 0, 1, 1, 6, 14, 47, 136, 442, 1377, 4522, \ldots\}.$$

Les orbites pour la W_1-permutation et les arbres $3-$réguliers.

Proposition IV.106 *Le nombre* N_k^{orb} *d'orbites de château maximaux du noyau d'indice* $\frac{k+1}{2}$ *est :*

$$N_k^{orb} = \frac{1}{k+2}c_k + \frac{1}{2}c_{\frac{k}{2}} + \frac{2}{3}c_{\frac{k-1}{3}},$$

où c_n *est le* $n-$*ième nombre de Catalan si* $n \in \mathbb{N}$ *et* $c_n = 0$ *sinon.*

Preuve : C'est une conséquence des propositions (IV.93), (IV.100) et (IV.104) sur les ensembles disjoints des orbites simples, carrées et cubes.

□

Remarque IV.107 *Les premières valeurs de la suite* $(N_k^{orb})_{k\geq 0}$ *sont*

$$(N_k^{orb})_{k\geq 0} = \{1, 1, 1, 1, 4, 6, 19, 49, 150, 442, 1424, \ldots\}.$$

Cette suite correspond à la suite référencée A001683 dans l'OEIS [Sl] correspondant au nombre d'arbre $3-$*régulier à* $2k+2$ *sommets définie par la même expression.*

Pour tout entier k*, le nombre* $\dfrac{6}{k+2}c_k$ *est un entier. Les entiers de la suite* $(\dfrac{6}{k+2}c_k)_{k\geq 0}$ *sont appelées les "super ballot numbers", référencée A007054 dans l'OEIS [Sl].*

4.5 Permutation circulaire par la famille libre $W_{01^*} = \{01^k, k \geq 0\}$

Dans cette partie, on considère l'action de permutation circulaire par la famille libre $W_{01^*} = \{01^k, k \geq 0\}$ sur les mots maximaux du noyaux K_B.

Comme $W_{01^*}^*$ est l'ensemble des mots de B^* qui commence par 0, avec la proposition (IV.42), on a :

$$W_{01^*}^* \cap K_B^{\max} = O\mathcal{D}^{\max}.$$

D'après la proposition (IV.66), l'ensemble des mots de $W_{01^*}^* \cap K_B^{\max}$ d'indice $\frac{k+1}{2}$ est de cardinal c_k où c_k est le $k-$ième nombre de Catalan.

Tout mot non vide maximum du noyau $K^{\max}$ admet un facteur 0. Donc l'ensemble des orbites pour la W_{01^*}-permutation est l'ensemble des orbites pour la W_1-permutation circulaire.

Ainsi, les nombres d'orbites simples $(N_k^{\mathrm{orb}^1})_{k\geq 0}$, carrées $(N_k^{\mathrm{orb}^2})_{k\geq 0}$ et cubes $(N_k^{\mathrm{orb}^3})_{k\geq 0}$ et le nombre total d'orbites $(S_k)_{k\geq 0}$ de châteaux maximaux de noyau d'indice $\frac{k+1}{2}$ pour la W_{01^*}-permutation sont :

$$\begin{cases} N_k^{\mathrm{orb}^1} & = & \frac{1}{k+2}c_k - \frac{1}{2}c_{\frac{k}{2}} - \frac{1}{3}c_{\frac{k-1}{3}}, \\ N_k^{\mathrm{orb}^2} & = & c_{\frac{k}{2}}, \\ N_k^{\mathrm{orb}^3} & = & c_{\frac{k-1}{3}}, \\ S_k & = & \frac{1}{k+2}c_k + \frac{1}{2}c_{\frac{k}{2}} + \frac{2}{3}c_{\frac{k-1}{3}}, \end{cases}$$

où c_n est le $n-$ième nombre de catalan si n est entier et $c_n = 0$ sinon.

La $W_{01^*}-$longueur d'un mot w de $W_{01^*}^*$, notée $\lambda_{01^*}(w)$ est égale au nombre de facteur 0 dans un mot. Plus précisément, pour tout mot maximal w du noyau d'indice $\frac{k+1}{2}$ (voir

corollaire (IV.40)), on a :

$$\lambda_{01^*}(w) = \lambda_{\frac{k+1}{2}} - \sigma_{\frac{k+1}{2}} = 5k + 4 - (4k + 2) = k + 2.$$

Ainsi, les nombres de mots simples, carrés et cubes pour la $W_{01^*}-$permutation sont :

Proposition IV.108

$$\begin{array}{rcl} card(W_{01^*}^{sim} \bigcap K_{\frac{K+1}{2}}^{\max}) & = & c_k - \frac{k+2}{2} c_{\frac{k}{2}} - \frac{k+2}{3} c_{\frac{k-1}{3}} \\ card(W_{01^*}^{car} \bigcap K_{\frac{K+1}{2}}^{\max}) & = & \frac{k+2}{2} c_{\frac{k}{2}} \\ card(W_{01^*}^{cub} \bigcap K_{\frac{K+1}{2}}^{\max}) & = & \frac{k+2}{3} c_{\frac{k-1}{3}} \end{array}$$

On a bien :

$$card(W_{01^*}^{*} \bigcap K_{\frac{k+1}{2}}^{\max}) = c_k - \frac{k+2}{2} c_{\frac{k}{2}} - \frac{k+2}{3} c_{\frac{k-1}{3}} + \frac{k+2}{2} c_{\frac{k}{2}} + \frac{k+2}{3} c_{\frac{k-1}{3}} = c_k.$$

4.6 Permutation circulaire par la famille libre $W_{10^*} = \{10^k, k \geq 0\}$

Dans cette partie, on considère l'action de permutation circulaire par la famille libre $W_{10^*} = \{10^k, k \geq 0\}$ sur les mots maximaux du noyaux K_B.

Comme $W_{10^*}^*$ est l'ensemble des mots de B^* qui commence par 1 (qui ne commence pas par 0), avec la proposition (IV.42), on a :

$$W_{10^*}^* \cap K_B^{\max} = \mathcal{D}^{\max} 0 \cup (D^{\max})^3.$$

Les châteaux maximaux sont des mots sans facteurs 00 Donc les mots de $W_{10^*}^* \cap K_B^{\max}$ se factorisent avec les facteurs premiers 1 et 10 de la famille W_{10^*}.

D'après la proposition (IV.66), l'ensemble des mots de $W_{10^*}^* \cap K_B^{\max}$ d'indice $\frac{k+1}{2}$ est de cardinal $c_{k+1} - c_k + c_k = c_{k+1}$ où c_n est le $n-$ième nombre de Catalan.

Tout mot non vide maximum du noyau $K^{\max}$ admet un facteur 1. Donc l'ensemble des orbites pour la W_{10^*}-permutation est l'ensemble des orbites pour la W_1-permutation circulaire.

Ainsi, les nombres d'orbites simples $(N_k^{\mathrm{orb}^1})_{k\geq 0}$, carrées $(N_k^{\mathrm{orb}^2})_{k\geq 0}$ et cubes $(N_k^{\mathrm{orb}^3})_{k\geq 0}$ et le nombre total d'orbites $(S_k)_{k\geq 0}$ de châteaux maximaux de noyau d'indice $\frac{k+1}{2}$, pour la W_{10^*}-permutation, sont :

$$\left\{ \begin{array}{rcl} N_k^{\mathrm{orb}^1} & = & \frac{1}{k+2} c_k - \frac{1}{2} c_{\frac{k}{2}} - \frac{1}{3} c_{\frac{k-1}{3}}, \\ N_k^{\mathrm{orb}^2} & = & c_{\frac{k}{2}}, \\ N_k^{\mathrm{orb}^3} & = & c_{\frac{k-1}{3}}, \\ S_k & = & \dfrac{1}{k+2} c_k + \dfrac{1}{2} c_{\frac{k}{2}} + \dfrac{2}{3} c_{\frac{k-1}{3}}, \end{array} \right.$$

où c_n est le $n-$ième nombre de catalan si n est entier, et $c_n = 0$ sinon.

La $W_{10^*}-$longueur d'un mot w de $W^*_{10^*}$, notée $\lambda_{10^*}(w)$ est égale au nombre de facteur 1 dans un mot. Plus précisément, on a, pour tout mot maximal w du noyau d'indice $\frac{k+1}{2}$ (voir corollaire (IV.40)) :

$$\lambda_{10^*}(w) = \sigma_{\frac{k+1}{2}} = 4k+2.$$

Ainsi, les nombres de mots simples, carrés et cubes pour la $W_{10^*}-$permutation sont :

Proposition IV.109

$$\begin{aligned}
card(W^{sim}_{00^*} \bigcap K^{\max}_{\frac{K+1}{2}}) &= \frac{4k+2}{k+2}c_k - \frac{4k+2}{2}c_{\frac{k}{2}} - \frac{4k+2}{3}c_{\frac{k-1}{3}} \\
card(W^{car}_{00^*} \bigcap K^{\max}_{\frac{K+1}{2}}) &= \frac{4k+2}{2}c_{\frac{k}{2}} \\
card(W^{cub}_{00^*} \bigcap K^{\max}_{\frac{K+1}{2}}) &= \frac{4k+2}{3}c_{\frac{k-1}{3}}
\end{aligned}$$

On a bien, avec la formule (IV.102) :

$$card(W^*_{10^*} \bigcap K^{\max}_{\frac{k+1}{2}}) = \frac{4k+2}{k+2}c_k - \frac{4k+2}{2}c_{\frac{k}{2}} - \frac{4k+2}{3}c_{\frac{k-1}{3}} + \frac{4k+2}{2}c_{\frac{k}{2}} + \frac{4k+2}{3}c_{\frac{k-1}{3}} = c_{k+1}.$$

4.7 Permutation circulaire par $W_{1(00^*1)^*} = \{1(00^{k_1}1)(00^{k_2}1)\cdots(00^{k_n}1), n, k_i \geq 0\}$

Dans cette partie, on considère l'action de permutation circulaire par la famille libre

$$W_{1(00^*1)^*} = \{1(00^{k_1}1)(00^{k_2}1)\cdots(00^{k_n}1), n, k_i \geq 0\}$$

sur les mots maximaux du noyaux K.

Le sous-monoïde $W^*_{1(00^*1)^*}$ est l'ensemble des mots de B^* qui commence par 1 et termine par 1. D'après la proposition (IV.42), on a :

$$W^*_{1(00^*1)^*} \cap K^{\max} = (D^{\max})^3.$$

D'après la proposition (IV.66), l'ensemble des mots de $W^*_{1(00^*1)^*} \cap K^{\max}$ d'indice $\frac{k+1}{2}$ est de cardinal $c_{k+1} - c_k$ où c_n est le $n-$ième nombre de Catalan.

Tout mot non vide maximum du noyau $K^{\max}$ admet un facteur 101101 (voir proposition (IV.39). Donc l'ensemble des orbites pour la $W_{1(00^*1)^*}$-permutation est l'ensemble des orbites pour la W_1-permutation circulaire.

Ainsi, les nombres d'orbites simples $(N^{\text{orb}^1}_k)_{k\geq 0}$, carrées $(N^{\text{orb}^2}_k)_{k\geq 0}$ et cubes $(N^{\text{orb}^3}_k)_{k\geq 0}$ et le nombre total d'orbites $S_{k\geq 0}$ de châteaux maximaux de noyau d'indice $\frac{k+1}{2}$, pour la $W_{1(00^*1)^*}$-permutation, sont :

$$\begin{cases} N_k^{\text{orb}^1} &= \frac{1}{k+2}c_k - \frac{1}{2}c_{\frac{k}{2}} - \frac{1}{3}c_{\frac{k-1}{3}}, \\ N_k^{\text{orb}^2} &= c_{\frac{k}{2}}, \\ N_k^{\text{orb}^3} &= c_{\frac{k-1}{3}}, \\ S_k &= \dfrac{1}{k+2}c_k + \dfrac{1}{2}c_{\frac{k}{2}} + \dfrac{2}{3}c_{\frac{k-1}{3}}, \end{cases}$$

où c_n est le $n-$ième nombre de catalan si n est entier, et $c_n = 0$ sinon.

Un château maximal n'admet pas de facteur 00. Donc les mots de $W^*_{1(00^*1)^*} \cap K_B^{\max}$ admettent uniquement des facteurs 1, $1(01)^n$. De plus, d'après la proposition (IV.39), les châteaux maximaux admettent uniquement des facteurs 1 et 101.

Le nombre de facteur 101 dans la $W_{1(00^*1)^*}$ factorisation d'un mot w de $W^*_{1(00^*1)^*} \cap K_B^{\max}$ est égal au nombre de facteur 0 dans w, c'est $\lambda(w) - \sigma(w)$. La somme $\sigma(w)$ d'un mot w est la somme du nombre de facteur 1 dans la $W_{1(00^*1)^*}$ factorisation d'un mot w et du double du nombre de facteur 101. Donc la $W_{1(00^*1)^*}-$longueur d'un mot w de $W^*_{1(00^*1)^*}$ est : $\lambda_{1(00^*1)^*}(w) = \sigma(w) - \big(\lambda(w) - \sigma(w)\big) = 2\sigma(w) - \lambda(w) = 2(4k+2) - (5k+4) = 3k$ (voir corollaire (IV.40)). Donc :

$$\lambda_{1(00^*1)^*}(w) = 3k.$$

Ainsi, les nombres de mots simples, carrés et cubes pour la $W_{1(00^*1)^*}-$permutation sont :

Proposition IV.110

$$\begin{aligned} card(W^{sim}_{1(00^*1)^*} \bigcap K^{\max}_{\frac{k+1}{2}}) &= \frac{3k}{k+2}c_k - \frac{3k}{2}c_{\frac{k}{2}} - \frac{3k}{3}c_{\frac{k-1}{3}} \\ card(W^{car}_{01(00^*1)^*} \bigcap K^{\max}_{\frac{K+1}{2}}) &= \frac{3k}{2}c_{\frac{k}{2}} \\ card(W^{cub}_{1(00^*1)^*} \bigcap K^{\max}_{\frac{K+1}{2}}) &= \frac{3k}{3}c_{\frac{k-1}{3}} \end{aligned}$$

On vérifie aisément avec la formule (IV.102) qu'on a bien :

$$card(W^*_{1(00^*1)^*} \bigcap K^{\max}_{\frac{k+1}{2}}) = \frac{3k}{k+2}c_k = c_{k+1} - c_k.$$

Chapitre V

Modèle entier : dénombrement de K_Σ.

Dans ce chapitre, on étudie les mots du noyau K_Σ (noté simplement K) du morphisme surjectif μ (voir corollaire (II.8)) défini par :

$$\begin{array}{rccl} \mu : & \Sigma^* & \longrightarrow & PSL_2(\mathbb{Z}) \\ & 0 & \longmapsto & U = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \\ & a & \longmapsto & (US)^a U = \pm \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix} \quad \text{avec } S = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in PSL_2(\mathbb{Z}). \end{array}.$$

Le noyau K est la classe d'équivalence du mot vide pour la relation d'équivalence $\sim_\Sigma$ engendrée par les règles de réécriture (ou réductions) $\mathsf{v} = ((a+1)0(b+1) \to ab)$, $\mathsf{u} = (a00b \to a+b)$ et $\mathsf{h} = (000 \to \emptyset)$ (voir proposition (II.14)). Cette relation d'équivalence est également engendrée par les réductions v et h. Dans la classe d'équivalence du mot vide (le noyau K), tout mot se réduit au mot vide uniquement avec des réductions v et h. (voir remarque (II.17)). Dans ce chapitre, on ne considérera pas la réduction u.

Le noyau K est partitionné en sous-ensembles $(K_{\Sigma,\frac{k}{2}})_{k\in\mathbb{N}}$ (ou simplement $K_{\frac{k}{2}}$) par le morphisme d'indice

$$\begin{array}{rccl} Ind : & \Sigma^* = \{0,1,2,3,...\}^* & \longrightarrow & \mathbb{Z}/12 \\ & w & \longmapsto & Ind(w) = \dfrac{1}{12}\left[2\lambda(w) - \sigma(w)\right] \end{array}.$$

Tout mot w du noyau se réduit au mot vide par des réductions maximales composées de $\frac{1}{2}\sigma(w)$ réductions v et $2Ind(w)$ réductions h (voir proposition (II.18)). Réciproquement, tout mot w du noyau s'obtient à partir du mot vide avec $\frac{1}{2}\sigma(w)$ expansions $V = \mathsf{v}^{-1}$ et $2Ind(w)$ expansions $H = \mathsf{h}^{-1}$.

Un sous-ensemble $K_{\frac{k}{2}}$ est stable par réduction v et expansion V. Et si w est un mot du sous-ensemble $K_{\frac{k}{2}}$, alors $\mathsf{h}(w)$ est dans le sous-ensemble $K_{\frac{k-1}{2}}$ et $H(w)$ est dans le sous-

ensemble $K_{\frac{k+1}{2}}$.

Sont répertoriés ci-dessous, les premiers mots du noyaux K à indice et longueur fixés :

Ind	λ	σ	Mots du noyau	Nombre de mots
0	0	0	$\emptyset$	1
1/2	3	0	000	1
	4	2	$\{0101, 1010\}$	2
	5	4	$\{20110, 11020, 10201, 02011, 01102\}$	5
	6	6	301110, 210210, 202020, 201201, 120120, 111030, 110301, 103011, 101102, 030111, 021021, 020202, 012012, 011103	14
	l	$2l-6$	...	...
1	6	0	000000	1
	7	2	1010000, 0101000, 0010100, 0001010, 0000101, 0100001, 1000010	7
	8	4	20000110, 11000020, 02000011, 01100002, 201010010, 11010010, 10010110, 10001020, 10000201, 10200001, 02010001, 01101001, 01001011, 01000102, 20110000, 11020000, 10201000, 10110100, 10101010, 10100101, 02011000, 01102000, 01020100, 01011010, 01010101, 00201100, 00110200, 00102010, 00101101, 00020110, 00011020, 00010201, 00002011, 00001102	34
	l	$2l-12$	...	...
$k/2$	$3k$	0	0^{3k}	1
	l	$2l-6k$	...	...

1 Le sous-ensemble $K_{\frac{1}{2}}$ associé au demi-tour.

Dans cette partie, on dénombre les mots du noyau d'indice $\frac{1}{2}$ à longueur donné :

Théoreme V.1 *Le sous-ensemble $K_{\frac{1}{2}}$, formé des mots du noyau K du morphisme $\mu : \Sigma^* \to PSL_2(\mathbb{Z})$, d'indice $\frac{1}{2}$, admet c_{l-2} mots de longueur $l \geq 3$, où $c_n = \frac{1}{n+1}\binom{2n}{n}$ est le $n-$ième nombre de Catalan.*

Preuve : Un mot w du sous-ensemble $K_{\frac{1}{2}}$ est obtenu avec $2Ind(w) = 1$ expansion H et $\frac{1}{2}\sigma(w)$ expansions $V = (ab \to (a+1)0(b+1))$ sur le mot vide.

Il est clair que l'expansion V ne s'applique pas sur le mot vide et on commence par l'unique expansion H.

Ainsi, le sous-ensemble $K_{\frac{1}{2}}$ est engendré par l'expansion V sur le mot 000.

On conclut avec le lemme (IV.70) du chapitre (IV) sur le modèle binaire.

□

2 Réductions et Expansions sur K_Σ.

Les sous-ensembles $K_{\frac{k}{2}}$, avec $k \in \mathbb{N}$, du noyau K sont stables par réductions v.

Comme pour le modèle binaire, le système de réécriture $\langle \Sigma | \mathsf{v} \rangle$ termine mais n'est pas confluent : un sous ensemble $K_{\frac{k}{2}}$ peut contenir plusieurs mots réduits pour v distincts.

Par exemple, le mot $w = 01010101(000)^{k-2}$ de la classe $K_{\frac{k}{2}}$, pour $k \geq 2$, se réduit vers les deux mots réduits pour la réduction v $(000)^k$ et $0100001(000)^{k-2}$.

Ainsi, pour tout $k \geq 2$, le sous-ensemble $K_{\frac{k}{2}}$ admet au moins deux mots réduits distincts pour la réduction v.

Dans cette section, on spécifie les réductions et les expansions en ajoutant en indice la position dans le mot du facteur sur lequel la règle de réécriture s'applique, afin de choisir un chemin canonique dans les sous-ensembles $K_{\frac{k}{2}}$ reliant un mot du noyau au mot vide.

Ainsi, on peut choisir une réduction maximale canonique d'un mot du noyau et réciproquement une expansion canonique, dans l'objectif de dénombrer les mots du noyau à indice et longueur donnés.

2.1 Définitions des réductions et expansions élémentaires.

Définition V.2 *(Réductions et expansions élémentaires.)*

- *Une réduction élémentaire* h *("half-turn") d'indice* $i \geq 1$ *enlève à un mot un facteur* 000 *situé en positions* $(i, i+1, i+2)$ *: Pour tous mots* p *et* s *de* Σ^**, on a :*

$$h_i(p\underset{\substack{\uparrow \\ i}}{000}s) = ps \text{ avec } \lambda(p) = i - 1 \geq 0. \tag{V.1}$$

- *Une expansion élémentaire* H_i *pour* $i \geq 1$ *est l'inverse d'une réduction élémentaire* h_i*. L'expansion* H_i *insère un facteur* 000 *dans un mot de longueur supérieur à* $i - 1$ *en positions* $(i, i+1, i+2)$ *: Pour tous mots* p *et* s*, on a :*

$$H_i(ps) = h_i^{-1}(ps) = p\underset{\substack{\uparrow \\ i}}{000}s \text{ avec } \lambda(p) = i - 1 \geq 0. \tag{V.2}$$

- *Une réduction élémentaire* v *("vallée") d'indice* $i \geq 1$ *remplace un facteur* $(a+1)0(b+1)$ *situé en positions* $(i, i+1, i+2)$ *par un facteur* ab *en positions* $(i, i+1)$. *Pour tous mots* p *et* s *et tous entiers* a *et* b, *on a*

$$\mathsf{v}_i(p\underset{\substack{\uparrow \\ i}}{(a+1)}0(b+1)s) = pabs \text{ avec } \lambda(p) = i-1 \geq 0 \tag{V.3}$$

- *Une expansion élémentaire* V *d'indice* $i \geq 1$ *est l'inverse d'une réduction élémentaire* v *d'indice* i. *L'expansion* V_i *remplace un facteur* ab *en positions* $(i, i+1)$ *par un facteur* $(a+1)0(b+1)$ *en positions* $(i, i+1, i+2)$ *: Pour tous mots* p *et* s *et tous entiers* a *et* b, *on a*

$$V_i(pabs) = v_i^{-1}(pabs) = p\underset{\substack{\uparrow \\ i}}{(a+1)}0(b+1)s \text{ avec } \lambda(p) = i-1 \geq 0. \tag{V.4}$$

Exemple V.3 *Avec le mot* $w = 100101001$ *du noyau* K *de longueur* $\lambda(w) = 7$, *on a :*

$V_1(w) = 2010101001$ $\qquad$ $V_3(w) = 1010201001$

$H_1(w) = 000100101010$ $\qquad$ $H_2(w) = 100000101001 = H_3(w) = H_4(w)$

Étant donné une suite de n *expansions élémentaires* $(E_{i_1}, E_{i_2}, \ldots, E_{i_{n-1}}, E_{i_n})$ *avec* $E \in \{V, H\}$, *on note simplement* $[E_{i_1}, E_{i_2}, \ldots, E_{i_{n-1}}, E_{i_n}]$ *l'expansion composée* $E_{i_n} \circ E_{i_{n-1}} \circ \cdots \circ E_{i_2} \circ E_{i_1}$.

2.2 Propriétés.

Dans cette partie, on regarde localement des propriétés de composées d'expansions élémentaires simples. Seul le corollaire (V.5) (et donc le lemme (V.4)) est utilisé dans la suite du chapitre.

Les autres propriétés sont toutefois intéressantes pour comprendre le choix de la réduction maximale canonique définie dans la section (3).

Lemme V.4 *Soient deux entiers* i *et* j *tels que* $1 \leq i < j$. *On a :*

$$[V_j, V_i] = [V_i, V_{j+1}].$$

De plus, pour tout mot w *de* $\mathcal{A}^*$, *le mot* $[V_i, V_{j+1}](w)$ *admet au moins deux zéros intérieurs isolés.*

Preuve : En notant $w = \{a_1...., a_n\}$, on a :

$$\begin{array}{llcl}
\text{Si } j > i+1 \text{ alors} & [V_j, V_i](w) & = & V_i(a_1 \cdots a_i \cdots (a_j+1)0(a_{j+1}+1)\cdots a_n) \\
 & & = & a_1 \cdots (a_i+1)0(a_{i+1}+1)\cdots(a_j+1)0(a_{j+1}+1)\cdots a_n \\
 & & = & [V_i, V_{j+1}](w). \\
\text{Si } j = i+1 \text{ alors} & [V_j, V_i](w) & = & V_i(a_1....a_i.a_{i+1}+1.0.a_{i+2}+1....a_n) \\
 & & = & a_1....a_i+1.0.a_{i+1}+2.0.a_{i+2}+1....a_n \\
 & & = & [V_i, V_{i+2}](w).
\end{array}$$

□

On dit que l'on "permute" deux expansions V même si un des deux indices change lorque que l'on remplace une expansion $[V_j, V_i]$ par l'expansion d'indice croissant $[V_i, V_{j+1}]$.

Corollaire V.5 *Soit $p \in \mathbb{N}$. La composée de p expansions V est égale à la composée de p expansions V d'indice croissant.*

La suite d'expansions V d'indices croissants permettant d'obtenir un mot w' à partir d'un mot w est unique.

Preuve :

Étant donnée une suite de p expansions $(V_{i_j})_{1\leq j\leq p}$, on peut "trier" les expansions en les "permutant" deux à deux de sorte que si $i_{j-1} > i_j$, on a :

$$\left[V_{i_1}, ..., V_{i_{j-1}}, V_{i_j}, ...V_{i_p}\right] = \left[V_{i_1}, ..., V_{i_j}, V_{i_{j-1}+1}, ..., V_{i_p}\right].$$

L'algorithme de tri consiste alors à placer la première occurence de l'expansion d'indice le plus petit i_m au début et à itérer le processus sur la suite $(V_{i_1+1}, V_{i_2+1}, \ldots, V_{i_{m-1}+1}, V_{i_{m+1}}, \cdots, V_{i_p})$ de sorte que :

$$tri(V_{i_1}, V_{i_2}, \ldots V_{i_p}) = (V_{i_m}, (tri(V_{i_1+1}, V_{i_2+1}, \ldots V_{i_{m-1}+1}, V_{i_{m+1}}, \ldots, V_{j_p})).$$

Ce processus de tri termine vers une suite expansions d'indices croissants : l'indice le plus petit de la famille $(V_{i_1+1}, V_{i_2+1}, \ldots V_{i_{m-1}+1}, V_{i_{m+1}}, \ldots, V_{j_p})$ est supérieur ou égal à i_m.

S'il existe deux suites distinctes d'indices croissants telles que $w' = (V_{i_1}, V_{i_2}, \ldots, V_{i_p})(w) = (V_{j_1}, V_{j_2}, \ldots, V_{j_p})(w)$, quitte à changer le mot w par le mot $(V_{i_1}V_{i_2}, \ldots V_{i_{m-1}})(w)$, on peut considérer que les premiers indices i_1 et j_1 sont différents. On suppose que $i_1 < j_1$. De plus, quitte à considérer le mot $a_{i_1}a_{i_1+1}\cdots a_n$ à la place du mot $a_1a_2\cdots a_n$, on peut supposer que $i_1 = 1 < j_1$.

On a alors $F_1(w) = (a_1+1)0(a_2+1)a_3\cdots a_n$

et $F_{j_1}(w) = a_1\cdots a_{j_1-1}(a_{j_1}+1)0(a_{j_1+1}+1)a_{j_1+2}\cdots a_n$.

Les suites d'indices étant croissantes, la première lettre du mot $[V_{j_1}, V_{j_2}, \ldots, V_{j_p}](w)$ située en position i_1 est a_1 alors que celle de du mot $[V_{i_1}, V_{i_2}, \ldots, V_{i_p}](w)$ est $\geq a_1+1$. Absurde. D'où l'unicité.

□

Lemme V.6 *Soient i et j deux entiers non nuls. On a :*

$$[V_j, H_i] = \begin{cases} [H_i, V_{j+3}] & si \quad i \leq j \\ [H_{i-1}, V_j] & si \quad i \geq j+3 \\ [V_j, H_{j+1}] & si \quad i = j+2 \end{cases}.$$

Preuve : En notant $w = \{a_1 \cdots a_n\}$, on a :

$$\begin{array}{llrcl}
\text{Si} & i \leq j & \text{alors} \quad [V_j, H_i](w) & = & H_i(a_1 \cdots a_{i-1} \cdots (a_j+1)0(a_{j+1}+1) \cdots a_n) \\
 & & & = & a_1 \cdots a_{i-1}000 \cdots (a_j+1)0(a_{j+1}+1) \cdots a_n \\
 & & & = & V_{j+3}(a_1 \cdots a_{i-1}000 \cdots a_j \cdots a_n) \\
 & & & = & [H_i, V_{j+3}](w). \\
\text{Si} & i \geq j+3 & \text{alors} \quad [V_j, H_i](w) & = & H_i(a_1 \cdots (a_j+1)0(a_{j+1}+1) \cdots a_{i-1} \cdots a_n) \\
 & & & = & a_1 \cdots (a_j+1)0(a_{j+1}+1) \cdots a_{i-1}000 \cdots a_n \\
 & & & = & V_j(a_1 \cdots a_j a_{j+1} \cdots a_{i-1}000 a_i \cdots a_n) \\
 & & & = & [H_{i-1}, V_j](w). \\
\text{Si} & i = j+2 & \text{alors} \quad [V_j, H_{j+2}](w) & = & H_{j+2}(a_1 \cdots (a_j+1)0(a_{j+1}+1) \cdots a_n) \\
 & & & = & a_1 \cdots (a_j+1)0000(a_{j+1}+1) \cdots a_n \\
 & & & = & [V_j, H_{j+1}](w).
\end{array}$$

□

Lemme V.7 *Soit i un entier non nul. On a :*

$$[V_i, H_{i+1}, V_{i+2}] = [H_{i+1}, V_i, V_{i+4}].$$

Preuve : Soit $w = a_1..a_n$ un mot de Σ^* et $n > i$. On a :

$$\begin{array}{rcl}
[V_i, H_{i+1}, V_{i+2}](w) & = & [H_{i+1}, V_{i+2}](a_1 \cdots (a_i+1)0(a_{i+1}+1) \cdots a_n) \\
 & = & V_{i+2}(a_1 \cdots (a_i+1)0000(a_{i+1}+1) \cdots a_n) \\
 & = & a_1 \cdots (a_i+1)01010(a_{i+1}+1) \cdots a_n \\
 & = & V_{i+4}(a_1 \cdots (a_i+1)0100(a_{i+1}) \cdots a_n) \\
 & = & [V_i, V_{i+4}](a_1 \cdots a_i 000 a_{i+1} \cdots a_n) \\
 & = & [H_{i+1}, V_i, V_{i+4}](a_1 \cdots a_i a_{i+1} \cdots a_n)
\end{array}$$

Lemme V.8 *Soient i et j deux entiers non nuls. Si $j \leq i+3$, on a :*

$$[H_i, H_j] = \left| \begin{array}{lll} [H_i, H_i] & si & j \in \{i, i+1, i+2, i+3\} \\ [H_j, H_{i+3}] & si & j < i \end{array} \right.$$

Preuve : En notant $w = a_1, ..., a_n$ avec $n \leq i$, on a :

$$\begin{array}{llrcl}
\text{Si} & i \leq j \leq i+3 & \text{alors} \quad [H_i, H_j](w) & = & H_j(a_1 \cdots a_{i-1}000 \cdots a_n) \\
 & & & = & a_1 \ldots a_{i-1}000000 \ldots a_n \\
 & & & = & [H_i, H_i](w). \\
\text{Si} & j < i & \text{alors} \quad [H_i, H_j](w) & = & H_j(a_1 \cdots a_{j-1} \cdots a_{i-1}000 \cdots a_n) \\
 & & & = & a_1 \ldots a_{j-1}000 \ldots a_{i-1}000 \ldots a_n \\
 & & & = & [H_j, H_{i+3}](w).
\end{array}$$

□

3 Réduction maximale canonique.

Dans cette partie, on définit une réduction maximale canonique d'un mot w du noyau K vers le mot vide. Inversement, on définit une expansion canonique du mot vide vers un mot w du noyau.

On a fait le choix de commencer par réduire un mot w d'un sous-ensemble $K_{\frac{k}{2}}$ vers un mot "réduit pour la réduction v" de $K_{\frac{k}{2}}$, puis de "descendre" dans le sous-ensemble $K_{\frac{k-1}{2}}$ en enlevant un demi-tour 000. On itère ce procédé dans les sous-ensembles des mots d'indice strictement inférieur à $\frac{k}{2}$ jusqu'à obtenir le mot 000, qui se réduit uniquement par la réduction h_0 au mot vide.

Généralement, un mot réduit pour v n'est pas le mot de longueur minimal de l'ensemble $K_{\frac{k}{2}}$.

On a là deux choix encore à faire : vers quel mot "réduit pour v" de $K_{\frac{k}{2}}$ réduit-on un mot non-réduit ? Et vers quel mot de $K_{\frac{k-1}{2}}$ réduit-on un mot "réduit pour v" de $K_{\frac{k}{2}}$?

On commence par étudier les mots réduits pour la réduction v d'un sous-ensemble $\frac{k}{2}$:

3.1 Minimum global et minimums locaux de $K_{\frac{k}{2}}$.

Proposition V.9 *Pour tout entier k, le mot de l'ensemble $K_{\frac{k}{2}}$ de longueur minimale est le mot $(000)^k$. C'est également le mot de $K_{\frac{k}{2}}$ de somme minimale.*

Ce mot est appelé le minimum global du sous-ensemble $K_{\frac{k}{2}}$.

Définition V.10 *Soit k un entier. Un minimum local non global (appelé simplement minimum local dans la suite) de l'ensemble $K_{\frac{k}{2}}$ est un mot distinct du minimum global qui est réduit pour la réduction v.*

Remarque V.11 *La somme d'un minimum local est un entier pair (voir proposition (I.69)) strictement positif.*

Il est clair qu'un minimum local dans $K_{\frac{k}{2}}$ n'admet pas de zéro isolé intérieur, sinon, la réduction v s'appliquerait.

Le sous-ensemble $K_0 = \{\emptyset\}$ n'admet pas de minimum local .

Comme tout mot de $K_{\frac{1}{2}}$ se réduit au mot 000 par des réductions v, le sous-ensemble $K_{\frac{1}{2}}$ n'admet pas de minimum local non plus.

Pour $k \geq 2$, un minimum local de $K_{\frac{k}{2}}$ est un mot non réduit pour le système de réécriture $\langle \Sigma \mid \mathsf{v}, \mathsf{h} \rangle$ sans zéro isolé intérieur. Donc il admet au moins un facteur 000 (voir proposition (II.16)). Plus précisément, on a :

Proposition V.12 *Soit k un entier ≥ 2. Un minimum local d'un sous-ensemble $K_{\frac{k}{2}}$ admet au moins un facteur intérieur isolé 0^p avec $p \geq 4$ et $p \equiv 1$ mod (3).*

Si un minimum local w, de somme non nulle, n'admet aucun zéro intérieur, alors il est de la forme $0^{d+3e}a_1 \cdots a_k 0^{f+3g}$ avec d et $f \in \{0,1,2\}$, $e, g \in \mathbb{N}$ et les $a_j \in \mathbb{N} \setminus \{0\}$. Donc le mot w se réduit au mot réduit $0^d.a_1...a_k.0^f$ de Réduit$_\Sigma$. Donc w n'est pas dans le noyau K_Σ. Absurde.

Donc un minimum local admet des facteurs intérieurs isolés de la forme 0^p avec $p \geq 2$.

Si tous les facteurs intérieurs isolés d'un minimum local de la forme 0^p ont une puissance $p \neq 1$ (mod 3), alors le minimum local se réduit par la réduction h à un mot sans zéro isolé intérieur, sans facteur 000, avec éventuellement des facteurs 00 isolés intérieurs. Or, un tel mot n'est pas dans le noyau (voir lemme (II.16)).

D'où le résultat.

□

Proposition V.13 *Soient i, j et k trois entiers non nuls.*

Si un mot w du sous-ensemble $K_{\frac{k}{2}}$ admet un unique zéro isolé intérieur en position i alors le mot $H_j(w)$ est un minimum local de $K_{\frac{k+1}{2}}$ si et seulement si $j \in \{i-1, i\}$.

Preuve : Insérer un facteur 000 juste avant ou juste après un 0 produit le même mot.

Il est clair que le mot $H_{i-1}(w) = H_i(w)$ est dans le sous-ensemble $K_{\frac{k+1}{2}}$ et n'admet pas de zéro isolé intérieur.

Si $j \notin \{i-1, i\}$, l'expansion H_j "conserve" le zéro isolé intérieur de w et $H_j(w)$ n'est pas un minimum local.

□

Remarque V.14 *Pour $k \geq 2$, la réciproque n'est pas vraie. Par exemple, le mot $w = 1000010$ de $K_{\frac{2}{2}}$ n'admet pas de zéro intérieur isolé et le mot $H_2(w) = 1000000010$ est un minimum local de $K_{\frac{3}{2}}$.*

Pour $k = 1$, on montre que la réciproque est vraie :

Proposition V.15 *Un mot de K_1 est un minimum local de K_1 si et seulement si il est de la forme $pa0000bs$ avec $p, s \in \Sigma^*$ et $a, b \in \Sigma \setminus \{0\}$ et le mot $pa0bs$ est un mot de $K_{\frac{1}{2}}$ ayant un unique zéro intérieur isolé (celui situé entre les facteurs a et b).*

Preuve : Un minimum local de K_1 admet au moins un facteur 0^k intérieur (voir proposition (V.12)) avec $k \geq 4$ et $k = 1 \pmod 3$. Si $k > 4$, l'indice est strictement supérieur à 1. Donc un minimum local de K_1 admet un facteur 0000 intérieur isolé.

Il est de la forme $pa0000bs$ avec $pa0bs \in K_{\frac{1}{2}}$.

Un mot w de $K_{\frac{1}{2}}$ est obtenu par des expansions $V = ab \to (a+1)0(b+1)$ sur le mot 000. Donc le mot w n'admet pas de facteur 00 et n'a que des zéros isolés avec au moins un zéro isolé intérieur.

Si le mot w admet plus de deux zéros isolés intérieurs, quelque soit l'endroit i où on applique une expansion H, le mot $H_i(w)$ admet au moins un zéro isolé intérieur et n'est pas un minimum local. Ainsi, si $pa0000bs$ est un minimum alors $w = pa0bs$ admet un unique zéro intérieur isolé.

La réciproque est donnée par la proposition (V.13).

□

3.2 Réductions et expansions canonique.

En général, pour $k \geq 2$, un mot w d'un sous-ensemble $K_{\frac{k}{2}}$ se réduit vers différents minimums locaux de $K_{\frac{k}{2}}$.

Alors comment définir une réduction canonique parmi l'ensemble des réductions maximales ?

Par exemple, le mot $w = 10101010$ se réduit par v aux minimaux locaux $w_1 = 1000010$ et $w_2 = 000000$. Ce mot $w = 10101010$ admet 4 réductions maximales distinctes vers le mot vide :

1). la réduction $[\mathsf{v}_1, \mathsf{h}_1, \mathsf{v}_1, \mathsf{h}_1]$, inverse de l'expansion $[H_1, V_1, H_1, V_1]$:
$w = 10101010 \to_{\mathsf{v}_1} 0001010 \to_{\mathsf{h}_1} 1010 \to_{\mathsf{v}_1} 000 \to_{\mathsf{h}_1} \emptyset$,

2). la réduction $[\mathsf{v}_1, \mathsf{v}_4, \mathsf{h}_1, \mathsf{h}_1]$, inverse de l'expansion $[H_1, H_1, V_4, V_1]$:
$w = 10101010 \to_{\mathsf{v}_1} 0001010 \to_{\mathsf{v}_4} 000000 \to_{\mathsf{h}_1} 000 \to_{\mathsf{h}_1} \emptyset$,

3). la réduction $[\mathsf{v}_3, \mathsf{h}_2, \mathsf{v}_1, \mathsf{h}_1]$, inverse de l'expansion $[H_1, V_1, H_2, V_3]$:
$w = 10101010 \to_{\mathsf{v}_3} 1000010 \to_{\mathsf{h}_2} 1010 \to_{\mathsf{v}_1} 000 \to_{\mathsf{h}_1} \emptyset$,

4). et la réduction $[\mathsf{v}_5, \mathsf{v}_1, \mathsf{h}_1, \mathsf{h}_1]$, inverse de l'expansion $[H_1, H_1, V_1, V_5]$:
$w = 10101010 \to_{\mathsf{v}_5} 1010000 \to_{\mathsf{v}_1} 000000 \to_{\mathsf{h}_1} 000 \to_{\mathsf{h}_1} \emptyset$.

Cette dernière réduction est la réduction canonique maximale de w. Elle est définie par :

Définition V.16 *(Réduction canonique et réduction canonique maximale)*

1. *Pour tout entier $k \geq 1$, la réduction canonique d'un mot w du noyau K_Σ dans un sous-ensemble $K_{\frac{k}{2}}$ est la suite de n réductions $\mathsf{v}_{i_1}, \mathsf{v}_{i_2}, \ldots \mathsf{v}_{i_n}$ telle que la suite $w_1, w_2, \ldots w_n, w_{n+1}$ de mots de $K_{\frac{k}{2}}$ définie par $w = w_1 \to_{v_{i_1}} w_2 \to_{v_{i_2}} w_3 \to \ldots w_n \to_{v_{i_n}} w_{n+1}$ vérifie*

- *le mot* w_j *est de la forme* $w_j = p_j a_j 0 b_j s_j$ *où* $a_j, b_j \in \Sigma \setminus \{0\}$ *et* $\lambda(p_j a_j) = i_j$
- *le suffixe* $b_j s_j$ *de* w_j *n'admet pas de zéro isolé intérieur.*
- *le mot* w_{n+1} *est un minimum (local ou global) de* $K_{\frac{k}{2}}$.

Autrement dit, la réduction canonique dans un sous-ensemble $K_{\frac{k}{2}}$ *est la famille de réductions* v *qui enlèvent successivement le dernier zéro isolé intérieur d'un mot, celui situé le plus à droite.*

2. *Pour* $k = 1$, *l'unique réduction de l'unique minimum* 000 *de* $K_{\frac{1}{2}}$ *dans* K_0 *est* h_0.

   Pour $k \geq 2$, *la réduction canonique d'un minimum (local ou global)* w *d'un sous-ensemble* $K_{\frac{k}{2}}$ *dans le sous-ensemble* $K_{\frac{k-1}{2}}$ *est l'expansion* h *d'indice* i *tel que pour* w *de la forme* $w = pa0^k s$ *avec* $a \in \Sigma \setminus \{0\}$ *et* $k \geq 3$, *on a :*

   - $i = \lambda(pa) + 1$
   - *le suffixe* s *de* w *n'admet pas de facteur* 000.

   Autrement dit, la réduction canonique d'un sous-ensemble $K_{\frac{k}{2}}$ *dans le sous-ensemble* $K_{\frac{k-1}{2}}$ *est la réduction* h *qui enlève le facteur* 000 *le plus à gauche du facteur* 0^k *avec* $k \geq 3$ *situé le plus à droite dans la mot.*

3. *Pour tout entier* $k \geq 1$, *la réduction maximale canonique d'un mot* w *de* $K_{\frac{k}{2}}$ *est définie récursivement par la composée des réductions canoniques dans* $K_{\frac{k}{2}}$ *de* w *vers un minimum* w_m *de* $K_{\frac{k}{2}}$, *de la réduction canonique du minimum* w_m *vers un mot* w' *de* $K_{\frac{k-1}{2}}$ *et de la réduction maximale canonique du mot* w' *du sous-ensemble* $K_{\frac{k-1}{2}}$.

Exemple V.17

1. *La réduction maximale canonique du mot* 2021010020 *est la suite donnée par les réductions successives suivantes :*

$$2021\underline{0}10020 \to_{\mathsf{v}_4} 2\underline{0}2000020 \to_{\mathsf{v}_1} 11\underline{000}020 \to_{\mathsf{h}_3} 11\underline{0}20 \to_{\mathsf{v}_2} 1\underline{0}10 \to_{\mathsf{v}_1} \underline{000} \to_{\mathsf{h}_1} \emptyset.$$

   Son expansion canonique est alors $(H_1, V_1, V_2, H_3, V_1, V_4)$.

2. *La réduction maximale canonique du mot* 021020001000 *est la suite des réductions suivantes :*

$$021\underline{0}20001000 \to_{\mathsf{v}_3} 02\underline{0}10001000 \to_{\mathsf{v}_2} 0100001\underline{000} \to_{\mathsf{h}_8} 01\underline{00}001 \to_{\mathsf{h}_3} 01\underline{0}1 \to_{\mathsf{v}_2} \underline{000} \to_{\mathsf{h}_1} \emptyset.$$

   Son expansion canonique est alors $(H_1, V_2, H_3, H_8, V_2, V_3)$.

Remarque V.18 *La réduction canonique dans un sous-ensemble* $K_{\frac{k}{2}}$ *est une suite de réductions* v *d'indices décroissants.*

Inversement, une expansion canonique dans un sous-ensemble $K_{\frac{k}{2}}$ *est une suite d'expansions* V *d'indices croissants.*

Pour $k = 1$, toute suite d'expansions V d'indices croissants sur un minimum de $K_{\frac{1}{2}}$ est une expansion canonique dans $K_{\frac{1}{2}}$: le sous-ensemble $K_{\frac{1}{2}}$ admet un unique minimum 000 *(voir proposition (V.5)).*

Pour $k \geq 2$, la réciproque n'est pas vraie : le sous-ensemble $K_{\frac{k}{2}}$ admet différents minimums et il existe des suites expansions $(V_{i_1}, V_{i_2}, \ldots V_{i_n})$ d'indices croissants qui ne sont pas canoniques. Par exemple, la suite d'expansions d'indices croissants $[V_3]$ sur le mot réduit 1000010 *de K_1 n'est pas canonique. On a $V_3(1000010) =$* 10101010 *alors que la réduction canonique de* 10101010 *dans $K_{\frac{2}{2}}$ est $[v_5, v_1]$ et son expansion canonique dans $K_{\frac{2}{2}}$ est $[V_1, V_5]$.*

4 Le sous-ensemble K_1 associé au tour.

Dans cette partie, on étudie les réductions et expansions canoniques des mots de K_1 dans l'objectif de dénombrer le nombre de mots de K_1 de longueur fixée.

Le cas général des sous-ensembles $K_{\frac{k}{2}}$ pour $k \geq 3$ n'est pas résolu dans cette recherche.

Deux points principaux, valables dans le sous-ensemble K_1, simplifient le problème par rapport aux sous-ensembles d'indice > 1 :

- Sans compter la première expansion H évidente $\emptyset \to_{H_1}$ 000, il n'y a qu'une seule expansion H supplémentaire à effectuer pour obtenir les mots de K_1. De ce fait, il n'y a pas plusieurs cas à considérer : selon si les demi-tours 000 supplémentaires sont rajoutés au même endroit ou s'ils sont séparées par d'autres facteurs dans le mot, et selon s'ils sont rajoutés au même moment ou s'il y a des expansions V intermédiaires.
- Les minimums locaux se caractérisent simplement avec leur nombre de zéros isolés intérieurs.

Selon leurs expansions maximales canoniques, on classe les mots de K_1 en 3 catégories :

1. Si le mot se réduit par sa réduction canonique au mot de longueur minimal 000000 de K_1, alors son expansion maximale canonique est de la forme $[H_1, H_1, V_{i_1}, V_{i_2}, \ldots, V_{i_n}]$ où la suite des indices $(i_j)_j$ est croissante.
2. Si le mot est un minimum local de K_1, alors son expansion maximale canonique est de la forme $[H_1, V_{i_1}, V_{i_2}, \ldots, V_{i_n}, H_{i_n+1}]$ où la suite des indices $(i_j)_{1 \leq j \leq n}$ est croissante. Et le mot est de la forme $0^d p0000s0^f$ (voir proposition (V.12)) où le mot $0^d 0ps0^f$ est un mot de $K_{\frac{1}{2}}$ avec un unique zéro isolé.
3. Si le mot se réduit par une suite non vide de réductions v d'indices décroissants à un minimum local de K_1 alors son expansion maximale canonique est de la forme $[H_1, V_{i_1}, V_{i_2}, \ldots, V_{i_n}, H_{i_n+1}, V_{k_1}, V_{k_2}, \ldots, V_{k_m}]$ où les suites des indices $(i_j)_{1 \leq j \leq n}$ et $(k_j)_{1 \leq j \leq m}$ sont croissantes.

4.1 Les mots de K_1 obtenus avec le minimum global 000000.

L'ensemble K_1 contient un unique mot de longueur 6, c'est le minimum global 000000.

Les mots de K_1, de longueur $l \geq 7$ dont la réduction canonique dans K_1 se termine au minimum global 000000 sont construits par une suite de $k = l - 6$ expansions $V_{i_1}, V_{i_2}, \ldots, V_{i_k}$ d'indices croissants. On a :

Proposition V.19 *La série génératrice associée aux nombres de mots de K_1 de longueur $k + 6 \geq 6$ dont la réduction canonique dans K_1 se termine au minimum global* 000000*, est :*

$$\sum_{k \geq 0} T_{k+4,k} X^{k+6}$$

où $T_{n,m} = \binom{n+m}{n} \frac{n-m+1}{n+1}$ *est le triangle de Catalan.*

Lemme V.20 *Soient m, n deux entiers.*

Le nombre $\delta_{m,n}$ de suite croissante finie $(i_j)_{1 \leq j \leq n}$ telles que $1 \leq i_j \leq j + m$ pour tout indice $1 \leq j \leq n$ est donné par :

$$\delta_{m,n} = T_{n+m,n} = \binom{2n+m}{n+m} \frac{m+1}{n+m+1}$$

où $T_{n,m} = \binom{n+m}{n} \frac{n-m+1}{n+1}$ *est le triangle de Catalan référencé A*009766 *dans l'OEIS [Sl].*

Preuve :

- Les conditions initiales sont triviales :
  Pour $n = 0$, l'unique suite est $\emptyset$. D'où $\delta_{m,0} = 1$.
  Pour $n = 1$, comme $1 \leq i_1 \leq m + 1$, on a $\delta_{m,1} = m + 1$.
- Pour $m = 0$, on a $1 \leq i_1 \leq 1 + m = 1$. Donc le nombre de suite finie $(i_1, ...i_n)$ telle que $i_j \leq j + 0$ est égale au nombre de suite finie croissante $(k_1, .., k_{n-1}) = (i_2, ...i_n)$ telle que $k_j = i_{j+1} \leq j + 1$ pour tout $1 \leq j \leq n - 1$. D'où la relation de récurrence :

$$\delta_{0,n} = \delta_{1,n-1}. \tag{V.5}$$

- Pour $m \geq 1$, on distingue deux cas disjoints :
  Si $i_1 = 1$, alors le nombre de suite finie $(i_1, ..., i_n)$ possibles est égale au nombre de suite finie croissante $(k_1, .., k_{n-1}) = (i_2, ..., i_n)$ telle que $k_j = i_{j+1} \leq j + 1 + m$ pour tout $1 \leq j \leq n - 1$. Donc il y a $\delta_{m+1,n-1}$ possibilités.

Sinon, $i_1 > 1$, pour tout indice $1 \leq j \leq n$, on a : $2 \leq i_j \leq j + m$. Cela revient à choisir une suite croissante de n entiers k_j tels que $i_j = k_j + 1$ et $1 \leq k_j \leq j - 1 + m$. Donc il y a $\delta_{m-1,n}$ possibilités.

Finalement, on obtient la relation de récurence :

$$\delta_{m,n} = \delta_{m+1,n-1} + \delta_{m-1,n}. \tag{V.6}$$

En posant $T_{m,n} = \delta_{m-n,n}$ avec $0 \leq n \leq m$, (équivalent à $\delta_{m,n} = T_{n+m,n}$), on obtient :

$$\begin{cases} T_{m,0} &= \delta_{m,0} = 1, \\ T_{m,1} &= \delta_{m-1,1} = m, \\ T_{m,m} &= \delta_{0,m} = \delta_{1,m-1} = T_{m,m-1}, \\ T_{m,n} &= \delta_{m-n,n} = \delta_{m-n+1,n-1} + \delta_{m-n-1,n} = T_{m,n-1} + T_{m-1,n}. \end{cases}$$

Ainsi, $(T_{n,k})_{0 \leq k \leq n}$ est le triangle de Catalan référencé $A009766$ (voir [Sl]).

□

Les premières valeurs de $\delta_{m,n} = T_{n+m,n}$ sont :

$\delta_{m,n}$:	$n=0$	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$
$m=0$	1	1	2	5	14	42	132	429
$m=1$	1	2	5	14	42	132	429	
$m=2$	1	3	9	28	90	297		
$m=3$	1	4	14	48	165			
$m=4$	1	5	20	75				
$m=5$	1	6	27					
$m=6$	1	7						

Preuve de la proposition (V.19) :

L'expansion canonique permettant d'obtenir un tel mot à partir du mot 000000 est une suite $(V_{i_1}, V_{i_2}, \ldots V_{i_k})$ de $k = l - 6$ expansions V d'indices croissants.

Réciproquement , les images du mot 000000 par deux suites distinctes de k expansions d'indices croissants sont deux mots distincts (voir corollaire (V.5)).

On note $w_j = [V_{i_1}, V_{i_2}, \ldots V_{i_j}](000000)$. L'indice i_{j+1} de l'expansion $V_{i_{j+1}}$ est un entier compris entre 1 et $\lambda(w_j) - 1$, avec $\lambda(w_j) = \lambda(w_{j-1}) + 1 = \lambda(000000) + j = 6 + j$.

Donc les mots du noyau qui se réduisent canoniquement au minimum global 000000 de K_1 sont en bijection avec l'ensemble des suites croissantes $(i_j)_{1\leq j\leq k}$ telles que $1 \leq i_{j+1} \leq 5+j = 4+(j+1)$. On conclu avec le lemme (V.20) avec $m = 4$.

□

Remarque V.21

Pour tout entiers $n, m \geq 0$, on montre aisément que le nombre $\delta_{m,n}$ de suite croissante finie $(i_j)_{1\leq j\leq n}$ telles que $1 \leq i_j \leq j+m$ vérifie

$$\delta_{m,n} = \frac{(m+1)(2n+m)!}{n!(n+m+1)!}.$$

*À m fixé, la suite $(\delta_{m,n})_n$ est la $(m+1)-$ième ligne du triangle associée à la famille $\delta_{m,n}$. C'est aussi la $(m+1)-$ième diagonale du triangle de Catalan [**?**].*

La fonction génératrice de cette suite $(\delta_{m,n})_{n\geq 0}$ est donnée par (A. C. Robin - 2007) :

$$C(x)^{m+1}$$

où $C(x) = \dfrac{1-\sqrt{1-4x}}{2x}$ est la fonction génératrice de la suite des nombres de Catalan.

Par exemple, les premières valeurs de la suite $(\delta_{4,n})_n$ sont $\{1, 5, 20, 75, \ldots\}$.

4.2 Les minimums locaux non maximaux de K_1.

Dans cette partie, on étudie et dénombre les minimums locaux de K_1.

Un minimum local de K_1 est un mot de la forme $pa0000bs$ où, $a, b \in \Sigma \setminus \{0\}$ et $pa0bs$ est un mot de $K_{\frac{1}{2}}$ qui admet un unique zéro isolé (voir proposition V.15)).

Comment obtient-on tous les mots de $K_{\frac{1}{2}}$ avec un unique zéro isolé ?

Proposition V.22 *Soit $k \geq 1$.*

Le sous-ensemble $K_{\frac{1}{2}}$ contient 2^k mots de longueur $k+3$ ayant un unique zéro intérieur isolé.

Preuve : On note n_k le nombre de mots de longueur k ayant un unique zéro isolé intérieur.

Le sous-ensemble $K_{\frac{1}{2}}$ est $\{1010, 0101\}$; il contient 2 mots ayant un unique zéro intérieur isolé. Donc $n_{3+1} = 2$.

Soit w un mot de $K_{\frac{1}{2}}$ de longueur $p \geq 4$.

L'expansion V augmente le nombe de zéros intérieurs isolés :

- Si on applique l'expansion V sur un facteur ne contenant pas un zéro isolé intérieur, alors le mot $V(w)$ a un zéro isolé intérieur de plus que le mot w.

- Si on applique l'expansion sur un facteur contenant un zéro isolé intérieur, le mot $V(w)$ a le même nombre de zéro isolé intérieur que le mot w.

Ainsi, si un mot w admet au moins deux zéros intérieurs isolés, pour tout expansion V, le mot $V(w)$ a plus de deux zéros isolés intérieurs.

Donc les mots ayant un unique zéro isolé intérieur de longueur k sont obtenus par une expansion V sur le zéro isolé (en position i) des mots ayant un unique zéro isolé de longueur $k-1$. Deux expansions sont possibles : V_i et V_{i+1}, et on obtient deux mots distincts (voir proposition (V.5)).

D'où $n_k = 2n_{k-1}$.

□

Remarque V.23 *L'expansion canonique d'un mot de $K_{\frac{1}{2}}$ ayant un unique zéro isolé intérieur est une suite d'expansions V d'indices $i_1, i_2, \ldots, i_n$ tels que $i_{j+1} - i_j \in \{0, 1\}$ pour tout $1 \leq j \leq n-1$.*

Pour $1 \leq j \leq n-1$, si l'expansion V_{i_j} remplace le facteur $a0$ où 0 est l'unique zéro isolé intérieur du mot alors $i_{j+1} = i_j$. Et si l'expansion V_{i_j} remplace le facteur $0b$ où 0 est l'unique zéro isolé intérieur du mot alors $i_{j+1} = i_j + 1$.

Corollaire V.24 *Soit $k \geq 1$.*

Le sous-ensemble K_1 contient 2^k minimums locaux non globaux de longueur $k + 6 \geq 7$.

Preuve : C'est une conséquence directe des propositions (V.15) et (V.22).

□

Exemple V.25 *Les premiers minimums locaux de K_1 sont :*

Longueur	*Minimums locaux de K_1*	*Nombres*
7	1000010 0100001	*2*
8	20000110 11000020 02000011 01100002	*4*
9	300001110 120000120 021000021 011100003 210000210 111000030 030000111 012000012	8
10	4000011110 3100002110 0112000013 0111100004 2200001210 2110000310 0130000112 0121000022 1300001120 1210000220 0220000121 0211000031 1120000130 1111000040 0400001111 0310000211	16
$k+6$	...	2^k

4.3 Les mots de K_1 obtenus avec les minimums locaux.

Dans cette partie, on considère les mots non minimaux canoniquement obtenus par une suite d'expansions d'indices croissants sur les minimums locaux (non globaux).

Toutes les expansions d'indices croissants dans K_1 ne sont pas canoniques (voir remarque (V.18)). Dans cette partie, on étudie sous quelles conditions une expansion d'indice croissant est canonique et on dénombre les mots non minimaux obtenus par une suite d'expansions sur les minimums locaux.

On rappelle qu'un minimum local est un mot de la forme $w = pa0000bs$ où $a, b \in \Sigma \setminus \{0\}$ et les mots pa et bs n'ont pas de zéro intérieur isolé (voir proposition (V.15)).

Proposition V.26 *Soit $pa0000bs$ un minimum local de K_1 avec $a, b \in \Sigma \setminus \{0\}$ et $p, s \in \Sigma^*$.*

Une suite de k expansions sur le minimum local $pa0000bs$ est canonique si et seulement si c'est la réunion d'une suite de k_1 expansions d'indices croissants sur le préfixe $pa00$ et k_2 expansions d'indices croissants sur le suffixe $00bs$ avec $k_1 + k_2 = k$.

Preuve : Une suite d'expansions V que l'on applique sur un mot w, d'indices croissants $(i_1, i_2, \dots i_k)$ est canonique si pour tout indice $1 \leq j \leq k$, le zéro isolé le plus à doite du mot $[V_{i_1}, V_{i_2}, \dots V_{i_j}](w)$ est à la position $i_j + 1$, de sorte que l'inverse de l'expansion soit la réduction canonique de w.

Toute suite d'expansions d'indices croissants qui s'applique uniquement sur le facteur $pa00$ du mot w ne produit pas de zéro isolé à droite de l'indice de la dernière expansion. Ces expansions sont bien canoniques.

Après avoir effectué une telle suite d'expansions, on obtient un mot de la forme $p'c00bs$, avec $c \in \Sigma$ et $p' \in \Sigma^*$.

Comme $b \neq 0$, l'expansion $V_{\lambda(p'c)}$ n'est pas canonique. On obtient le mot $p'(c+1)010b$. Ce mot possède un zéro isolé d'indice strictement supérieur à $\lambda(p'c)+1$. La réduction canonique de ce mot commence par $\mathsf{v}_{\lambda(p'c)+2}$. Ce n'est pas l'inverse de l'expansion $V_{\lambda(p'c)}0$. Une telle expansion n'est pas possible dans une suite d'expansions canonique.

Sur le mot $p'c00bs$, toute expansion d'indices croissants supérieurs à $\lambda(p'c0)$ qui modifie uniquement le facteur $00bs$ ne produit pas de zéro isolé intérieur à droite de la dernière expansion. Ces expansions sont bien canoniques.

Finalement, les suites de k expansions canoniques sur un mot de la forme $pa0000bs$ correspondent aux suites de k_1 expansions d'indices croissants sur le facteur $pa00$ et k_2 expansions d'indices croissants sur le facteur $00bs$ avec $k = k_1 + k_2$.

□

Proposition V.27 *Soit w un minimum local de longueur l de K_1. La série génératrice du nombre de mots de longueur $l+k$ qui se réduisent canoniquement au minimum local w est :*

$$\sum_{k\geq 0} T_{k+l-3,k} X^{l+k}$$

où $(T_{n,m})_{n,m\geq 0}$ est le triangle de Catalan.

Preuve : D'après la proposition (V.26), l'ensemble des expansions canoniques sur un mot $pa0000bs$ est la réunion d'une suite de k_1 expansions d'indices croissants sur le préfixe $pa00$ et k_2 expansions d'indices croissants sur le suffixe $00bs$ avec $k_1+k_2=k$. On note $l_1=\lambda(pa00)\geq 3$ et $l_2=\lambda(00bs)\geq 3$ avec $l=\lambda(w)=l_1+l_2$.

Le nombre d'expansions canoniques de k expansions V sur le mot w est alors (voir lemme (V.20)) :

$$\sum_{k_1+k_2\geq 0} \delta_{l_1-2,k_1} X^{k_1} \delta_{l_2-2,k_2} X^{k_2} X^l.$$

Avec la remarque (V.21), on obtient la fonction génératrice :

$$C(x)^{l_1-1} C(x)^{l_2-1} x^l = C(x)^{l-2} x^l$$

associée à la série génératrice $\sum_{k\geq 0} \delta_{k,l-3} X^{l+k} = \sum_{k\geq 0} T_{k+l-3,k} X^{l+k}$.

□

Lemme V.28 *Pour tous entiers $0\leq l\leq k$ et $n\geq 0$, on a :*

$$\sum_{i=0}^{l} 2^{k-i} T_{n,i} = 2^{k-l} \binom{n+l+1}{n+1}.$$

Preuve :

On le montre par récurrence sur l en constatant que $T_{n,m} = \binom{n+m}{n} - \binom{n+m}{n+1}$ avec $\binom{n+m}{n+1} = 0$ si $m=0$.

$$\begin{array}{lrcl}
\text{Pour } l=0, \text{ on a :} & \sum_{i=0}^{0} 2^{k-i}T_{n,i} & = & 2^kT_{n,0} = 2^k\left(\binom{n}{n} - \binom{n}{n+1}\right) = 2^k\binom{n+l+1}{n+1}. \\
\text{Pour } 1\leq l\leq k, \text{ on a :} & \sum_{i=0}^{l} 2^{k-i}T_{n,i} & = & 2^{k-l}T_{n,l} + \sum_{i=0}^{l-1} 2^{k-i}T_{n,i} \\
 & & = & 2^{k-l}\left(\binom{n+l}{n} - \binom{n+l}{n+1}\right) + 2^{k-l+1}\binom{n+l}{n+1} \\
 & & = & 2^{k-l}\left(\binom{n+l}{n} - \binom{n+l}{n+1} + 2\binom{n+l}{n+1}\right) \\
 & & = & 2^{k-l}\left(\binom{n+l}{n} + \binom{n+l}{n+1}\right) \\
 & & = & 2^{k-l}\binom{n+l}{n+1}.
\end{array}$$

□

Proposition V.29 *La série génératrice du nombre de mots de longueur $k+6$ qui se réduisent canoniquement à un minimum local non global de K_1 est :*

$$2\sum_{k\geq 0}\binom{2k+3}{k+4}X^{k+6}.$$

Preuve : Pour $l\geq 1$, il a y 2^l minimums locaux de longueurs $l+6$ dans K_1 (voir proposition (V.24)).

Chaque minimum local permet de construire canoniquement $\delta_{k,l+6-3}$ mots distincts de longueur $l+6+k$ avec $k\geq 0$ (voir proposition (V.27)).

On obtient, en applicant le lemme (V.28) avec $n=j+3$, $k=j$ et $l=j-1$:

$$\sum_{k\geq 0, l\geq 1} 2^l T_{l+k+3,k}X^{l+k+6} = \sum_{j\geq 1}\sum_{i=0}^{j-1} 2^{j-i}T_{j+3,i}X^{j+6} = \sum_{j\geq 1} 2\binom{2j+3}{j+4}X^{j+6} = 2\sum_{j\geq 0}\binom{2j+3}{j+4}X^{j+6}$$

avec $\binom{2j+3}{j+4} = 0$ pour $j=0$.

□

4.4 Dénombrement des mots de K_1.

En regroupant les résultats partiels des parties précédentes, on dénombre l'ensemble des mots de K_1 à longueur fixé :

Théoreme V.30 *La série génératrice G_{K_1} du sous-ensemble K_1 des mots du noyau K du morphisme $\mu : \Sigma^* \to PSl_2(\mathbb{Z})$ est :*

$$G_{K_1}(X) = \sum_{k\geq 0} \big(T_{k+4,k} + 2\binom{2k+3}{k+4}\big) X^{k+6}$$

où $(T_{n,m})_{n,m\geq 0}$ est le triangle de Catalan.

Preuve : Par définition de la réduction maximale canonique, l'ensemble des mots de K_1 engendrés par des suites d'expansions V sur le minimum global 000000 et l'ensemble des mots de K_1 engendrés par des suites d'expansions V sur un minimum local non global de K_1 sont disjoints.

On conclut avec les propositions (V.19) et (V.29).

□

Exemple V.31 *Les premières valeurs des nombres de mots dans le sous-ensemble K_1 du noyau K du morphisme $\mu : \Sigma^* \to PSL_2(\mathbb{Z})$ sont :*

longueur	6	7	8	9	10	11	12	13	14	15
Nombre de mots de K_1	1	7	34	147	605	2431	9646	38012	149226	584630

Chapitre VI

Origine géométrique de l'étude

Cette partie présente la motivation initiale de cette recherche. C'est le problème d'optimisation d'aire de polygones convexes entiers suivant qui nous a mené à introduire et à étudier l'ensemble des matrices de la forme $\begin{pmatrix} 0 & -1 \\ 1 & (a+1) \end{pmatrix}$ de $SL2(\mathbb{Z})$.

L'objectif de recherche de polygones d'aire minimaux n'a pas été poursuivi.

1 Espace affine et groupe affine

1.1 $\mathbb{R}^2$ en tant qu'espace affine et groupe affine $GA(\mathbb{R}^2)$

On se place dans le plan affine $\mathbb{R}^2_{aff}$ sous-jacent au $\mathbb{R}-$espace vectoriel $E_0 = \mathbb{R}^2$, orienté et muni de la structure euclidienne usuelle.

Parmi l'ensemble des applications affines de $\mathbb{R}^2_{aff}$ dans $\mathbb{R}^2_{aff}$, l'ensemble $T(\mathbb{R}^2)$ des translations de $\mathbb{R}^2_{aff}$ dans $\mathbb{R}^2_{aff}$ s'identifie à l'espace vectoriel E_0 par l'isomorphisme naturelle

$$\begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & T(\mathbb{R}^2) \\ v & \longmapsto & \left(\begin{array}{cccc} \tau_v : & E & \longrightarrow & E \\ & p & \longmapsto & \tau_v(p) = p + v \end{array} \right). \end{array}$$

Toute application affine $f : \mathbb{R}^2_{aff} \longrightarrow \mathbb{R}^2_{aff}$ est la composée d'une application linéaire L et d'une translation τ : il existe une matrice $L \in M_2(\mathbb{R})$ et un vecteur $\tau \in \mathbb{R}^2$ tels que pour tout point p de $\mathbb{R}^2_{aff}$ on a $f(p) = \tau \circ L(p) = L.p + \tau$.

L'application linéaire L ne dépend pas du choix de l'origine de l'espace affine ; L est appelée l'application linéaire associée à f.

Le vecteur τ est l'image de l'origine $O(0,0)$ de l'espace vectoriel E_0 par f.

La translation dépend du choix de l'origine. Si on fixe un autre point m_0 de l'espace affine $\mathbb{R}^2_{aff}$ comme origine, pour tout point p de l'espace affine, il existe un vecteur v tel que

$p = m_0 + v$ et on a : $L(p) = L.v + (L.m_0 + \tau)$. La translation devient $f(m_0) = L.m_0 + \tau$.

Définition VI.1

L'ensemble des applications linéaires bijectives de $\mathbb{R}^2$ dans $\mathbb{R}^2$ muni de la loi de composition forme un groupe appelé le groupe linéaire, noté $GL(\mathbb{R}^2)$.

L'ensemble des applications affines bijectives de $\mathbb{R}^2_{aff}$ dans $\mathbb{R}^2_{aff}$ muni de la loi de composition forme un groupe appelé le groupe affine, noté $GA(\mathbb{R}^2)$.

Proposition VI.2 *Soit f une application affine de $GA(\mathbb{R}^2)$ et $L \in GL(\mathbb{R}^2)$ son application linéaire associée.*

f est bijective si et seulement si L l'est. C'est à dire :

$$f \in GA(\mathbb{R}^2) \Leftrightarrow L \in GL(\mathbb{R}^2).$$

On obtient la suite exacte :

$$\begin{array}{ccccccccc} 1 & \to & T(\mathbb{R}^2) \approx \mathbb{R}^2 & \to & GA(\mathbb{R}^2) & \to & GL(\mathbb{R}^2) & \to & 1 \\ & & \tau & \mapsto & f = \tau \circ L & \mapsto & L & & \end{array}$$

Le groupe quotient $GA(\mathbb{R}^2)/\mathbb{R}^2$ est isomorphe au groupe $GL(\mathbb{R}^2)$ et le groupe affine $GA(\mathbb{R}^2)$ se décompose en produit semi-direct :

$$GA(\mathbb{R}^2) = \mathbb{R}^2 \rtimes GL(\mathbb{R}^2)$$

avec la loi produit $(\tau, L).(\tau', L') = (L.\tau' + \tau, L.L')$ pour tout τ et $\tau' \in \mathbb{R}^2$ et pour tout L et $L' \in GL(\mathbb{R}^2)$.

Dans la suite, on décrira le groupe affine du plan par des matrices 3×3 :

$$GA(\mathbb{R}^2) = \mathbb{R}^2 \rtimes GL_2(\mathbb{R}) = \{ \begin{pmatrix} L & \tau \\ 0 & 1 \end{pmatrix} \text{ avec } L \in GL_2(\mathbb{R}) \text{ et } \tau \in \mathbb{R}^2 \}$$

muni de la loi $\begin{pmatrix} L & \tau \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} L' & \tau' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} L.L' & L\tau' + \tau \\ 0 & 1 \end{pmatrix}$.

Proposition VI.3 *Soient f une application affine de $GA(\mathbb{R}^2)$ et $L \in GL(\mathbb{R}^2)$ son application linéaire associée.*

- *f préserve l'orientation si et seulement si $det(L) > 0$.*
- *f préserve l'aire si et seulement si $det(L) = \pm 1$.*

Définition VI.4

L'ensemble des applications linéaires bijectives de $\mathbb{R}^2$ *dans* $\mathbb{R}^2$ *de déterminant* 1 *est appelé le groupe spécial linéaire, noté* $SL_2(\mathbb{R})$.

L'ensemble des applications affines bijectives de $\mathbb{R}^2_{aff}$ *dans* $\mathbb{R}^2_{aff}$ *telles que l'application linéaire associée* L *est de déterminant* 1 *forme un groupe appelé le groupe spécial affine de* $\mathbb{R}^2$, *noté* $SA(\mathbb{R}^2)$.

1.2 Repères affines du réseau $\mathbb{Z}^2$ et groupe spécial affine $SA(\mathbb{Z}^2)$.

Dans la suite, on se place dans le réseau $\mathbb{Z}^2$ des points à coordonnées entières du plan euclidien orienté usuel $\mathbb{R}^2$.

L'ensemble des translations de vecteurs de $\mathbb{Z}^2$ est isomorphe au réseau $\mathbb{Z}^2 \simeq \mathbb{Z}[i]$. On considérera parfois implicitement les points du réseau, les vecteurs entiers et les translations du plan comme des entiers de Gauss.

Comme le déterminant d'une application linéaire bijective entière est inversible dans $\mathbb{Z}$, il est égale à ± 1. Donc, l'ensemble des applications affines entières de $GA(\mathbb{Z}^2)$ est l'ensemble des applications spéciales linéaires entières $SA(\mathbb{Z}^2)$. L'aire est conservée par $GA(\mathbb{Z}^2) = SA(\mathbb{Z}^2)$.

Dans la suite, on considère l'ensemble $SA(\mathbb{Z}^2)$ des applications spéciales affines sur $\mathbb{Z}^2_{aff} \subset \mathbb{R}^2_{aff}$ muni de la loi induite par celle de $GA(\mathbb{R}^2)$. Toute application spéciale affine entière se décompose sous la forme d'une somme d'une application spéciale linéaire entière $L \in SL_2(\mathbb{Z})$ et d'une translation entière $\tau \in \mathbb{Z}^2$, de la forme $\begin{pmatrix} p \\ 1 \end{pmatrix} \longmapsto \begin{pmatrix} L & \tau \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} p \\ 1 \end{pmatrix}$ et

$$SA(\mathbb{Z}^2) = \mathbb{Z}^2 \rtimes SL_2(\mathbb{Z}) = \{ \begin{pmatrix} L & \tau \\ 0 & 1 \end{pmatrix} \text{ avec } L \in SL_2(\mathbb{Z}) \text{ et } \tau \in \mathbb{Z}^2 \}.$$

Définition VI.5 *Un repère affine de l'espace affine* $\mathbb{Z}^2_{aff}$ *dans le plan orienté* $\mathbb{R}^2$ *est la donnée d'une* $\mathbb{Z}-$*base* (v, w) *du réseau* $\mathbb{Z}^2$ *et d'une origine* t *de l'ensemble affine* $\mathbb{Z}^2$.

On note $\mathcal{R}$ *l'ensemble des repères affines.*

Un repère affine (v, w, t) *est direct si la base* (v, w) *est direct.*

On note $\mathcal{R}^+ \subset \mathcal{R}$ *l'ensemble des repères affines directs.*

Étant donné un repère affine (v, w, t) de $\mathbb{Z}^2_{aff}$, tout point P du plan $\mathbb{Z}^2_{aff}$ admet un unique couple de coordonnées entières $(x, y) \in \mathbb{Z}^2$ déterminé par

$$P = t + xv + yw.$$

L'ensemble $\mathcal{R}$ des repères affines du réseau entier $\mathbb{Z}^2$ s'identifie à

$$\begin{aligned} \mathcal{R} &\simeq \{(v, w, t), v, w \text{ et } t \in \mathbb{Z}^2 \text{ tel que } \mathbb{Z}^2 = t + \mathbb{Z}v + \mathbb{Z}w\} \\ &\simeq \{(v, w, t), v, w \text{ et } t \in \mathbb{Z}[i] \text{ tel que } \mathbb{Z}[i] = t + \mathbb{Z}v + \mathbb{Z}w\} \end{aligned}$$

.

Dans la suite, on rappelle quelques propriétés élémentaires sur les $\mathbb{Z}-$bases de sorte que :

Proposition VI.6 *L'ensemble des repères affines $\mathcal{R}$ et l'ensemble des repères affines positifs $\mathcal{R}^+$ s'identifient à :*

$$\mathcal{R} = \{(u, v, t) \in (\mathbb{Z}^2)^3 / det(u, v) = \pm 1\}$$

et

$$\mathcal{R}^+ = \{(u, v, t) \in (\mathbb{Z}^2)^3 / det(u, v) = 1\}.$$

Définition VI.7 *Un vecteur $V = (x, y)$ du réseau des entiers $\mathbb{Z}^2$ est dit primitif si $pgcd(x, y) = 1$.*

Remarque VI.8

1. *Étant donnés A et B deux points du réseau des entiers $\mathbb{Z}^2$. Un vecteur $V = B - A$ est primitif si et seulement si l'intérieur du segment $[AB]$ n'admet pas de point du réseau : $[AB] \bigcap \mathbb{Z}^2 = \{A, B\}$.*
2. *Réciproquement, si le vecteur v (respectivement w) n'est pas primitif, le couple (v, w) n'est pas une $\mathbb{Z}-$base de $\mathbb{Z}^2$. Pour toute origine t du plan entier, un point intérieur au segment $[t, t + v]$ (respectivement $[t, t + w]$) n'a pas de coordonnées entières.*

Proposition VI.9 *L'aire du parallélogramme défini par deux vecteurs u et v du plan est donnée par la valeur absolue de leur déterminant : $A_{u,v} = |det(u, v)|$.*

Proposition VI.10 *Soient u et v deux vecteurs entiers du plan. On a :*

- *Les vecteurs u et v sont colinéaires si et seulement si $A_{u,v} = 0$.*
- *La famille (u, v) est une base du réseau des entiers si et seulement si $A_{u,v} = 1$.*
- *Dans le plan orienté, la famille (u, v) est directe si et seulement si $det(u, v) > 0$.*
- *Dans le plan orienté, la famille (u, v) est une base directe du réseau des entiers si et seulement si $det(u, v) = 1$.*

2 Polygones convexes entiers - Aires minimales

Définition VI.11

Un polygone entier (ou $n-$gone) est la classe d'équivalence pour les permutations cycliques d'une suite de n points distincts $\mathcal{P} = \{(P_j)_{0 \leq j \leq n-1}\}$ du réseau $\mathbb{Z}^2 \simeq \mathbb{Z}[i]$ tel que trois points consécutifs ne sont pas alignés.

Les points sont appelés les sommets du polygone. On considérera l'ensemble des indices j modulo n.

Un polygone convexe entier est un polygone entier dont les angles intérieurs $\measuredangle(P_{j+1} - P_j, P_{j-1} - P_j)$ *sont strictement inférieurs à* π *(c'est à dire que le déterminant* $det(P_{j+1} - P_j, P_{j-1} - P_j)$ *est strictement positif).*

Dans le plan affine euclidien orienté usuel, les translations de vecteurs à coefficients entiers sont des isométries et conservent les angles, les distances et les aires. On s'intéresse aux classes d'équivalence des $n-$gones convexes entiers modulo les translations. Ainsi, une classe est définie par la suite des vecteurs (côtés) $\{(V_j)_{0\leq j\leq n-1}\}$, avec $V_j \in (\mathbb{Z}^2) \setminus (0,0) \simeq \mathbb{Z}[i]^*$ tels que $\sum_{j=0}^{n-1} V_j = 0$.

Le théorème de Pick permet de calculer l'aire d'un polygone entier à partir du nombre de points intérieurs et du nombre de points sur le bord :

Théoreme VI.12 *[Théorème de G. Pick - 1899] L'aire d'un polygone entier* $\mathcal{P}$ *est donné par la formule*

$$i + \frac{b}{2} - 1$$

où i *est le nombre de points entiers intérieurs du polygone* $\mathcal{P}$ *et* b *est le nombre de points entiers sur le bord* $\partial\mathcal{P}$ *du polygone* $\mathcal{P}$.

On cherche à minimiser l'aire d'un polygone convexe entier :

Définition VI.13 *On considère la fonction* $a(n)$ *qui à un entier* n *associe la plus petite aire possible d'un* $n-$*gone entier.*

Un $n-$*gone d'aire* $a(n)$ *est appelé polygone minimal.*

Les valeurs de $a(n)$ sont connues jusqu'à $n = 14$:

n	3	4	5	6	7	8	9	10	11	12	13	14
a(n)	0,5	1	2,5	3	6,5	7	10,5	14	21,5	24	32,5	40

$a(11)$ a été déterminé en 2006 par D. Olsezewska [O]. Au delà, seules quelques valeurs de $a(n)$ pour des entiers pairs sont connues :

n	16	18	20	22	24	26	28	30	32	34	36
a(n)	59	87	121	164	210	274	345	430	523	632	749

3 Lignes brisées convexes entières localement minimales

Dans le but de rechercher les $n-$gones minimaux, on définit les $n-$lignes brisées localement minimales.

Définition VI.14

- *Une $n-$ ligne brisée entière (ou $n-$ligne brisée, ou simplement ligne brisée) l est une suite de $n+1 \geq 1$ points du plan affine $\mathbb{Z}^2$.*

  On note $l = (t_0, t_1, ..., t_n)$ pour $n \geq 0$ avec $t_j \in \mathbb{Z}^2 \approx \mathbb{Z}[i]$.

- *Une ligne brisée $l = (t_0, t_1, ..., t_n)$ est fermée si $t_n = t_0$.*

- *On note $\Delta(l) = \Delta(t_0, t_1, ..., t_n)$ le $n+1$-gone délimité par la ligne brisée fermée $l = (t_0, t_1, ..., t_n, t_0)$.*

Définition VI.15

- *Une $n-$ligne brisée $l = (t_0, t_1, ..., t_n)$ est localement convexe si pour tout $1 \leq j \leq j-1$, l'angle algébrique $\measuredangle(t_{j+1} - t_j, t_{t-1} - t_j)$ est dans l'intervalle $]0, \pi[$.*

  Autrement dit, le déterminant $det(t_j - t_{t-1}, t_{j+1} - t_j)$ est strictement positif.

- *Une $n-$ligne brisée $(t_0, t_1, ..., t_n)$ est $1-$minimale si pour tout $1 \leq j \leq n-1$, les points t_{j-1}, t_j, t_{j+1} ne sont pas alignés et pour tout $0 \leq j \leq n-1$, le segment $t_{j+1} - t_j$ n'a pas de points entiers intérieurs (c'est à dire que le vecteur $t_{j+1} - t_j$ est primitif).*

- *Une $n-$ligne brisée $l = (t_0, t_1, ..., t_n)$ avec $n \geq 2$ est $2-$minimale si*

  i) l est $1-$minimale,

  ii) et pour tout $0 \leq j \leq n-1$, le triangle défini par deux segments consécutifs $\Delta(t_{j-1}, t_j, t_{j+1})$ n'a pas de point intérieur.

Remarque VI.16

- *Étant donnée une ligne brisée localement convexe $1-$minimale $l = (t_0, t_1, ..., t_n)$ avec $n \geq 2$, pour tout $1 \leq i \leq n-1$, le couple $(t_j - t_{j-1}, t_{j+1} - t_j)$ forme une base directe du réseau $\mathbb{Z}^2$ et le triplet $(t_j - t_{j-1}, t_{j+1} - t_j, t_{j-1})$ forme un repère affine direct du réseau $\mathbb{Z}^2$.*

- *D'après le théorème de Pick (VI.12), une ligne brisée $l = (t_0, t_1, ..., t_n)$ est $2-$minimale si pour tout indice $1 \leq j \leq n-1$, l'aire $A_j = |det(t_j - t_{j-1}, t_{j+1} - t_j)|$ délimitée par le triangle $\Delta(t_{j-1}, t_j, t_{j+1})$ est $\frac{1}{2}(\alpha_j - 1)$ où α_j est le nombre de points entiers sur le segment $t_{j+1} - t_{j-1}$.*

Remarque VI.17

- *Un $n-$gone $\mathcal{P} = (P_j)_{0 \leq j \leq n-1}$ est localement convexe si la ligne brisée $(P_0, P_1, \ldots, P_{n-1}, P_0, P_1)$ l'est.*

- *Un $n-$gone $\mathcal{P} = (P_j)_{0 \leq j \leq n-1}$ est convexe s'il est localement convexe et si la ligne brisée $(P_0, P_1, \ldots, P_{n-1}, P_0, P_1)$ ne fait pas de boucle (autrement dit, le polygone est simple : deux segments non consécutifs $[P_j, P_{j+1}]$ et $[P_k, P_{k+1}]$ sont disjoints).*

- *Un $n-$gone $\mathcal{P} = (P_j)_{0\leq j\leq n-1}$ est $1-$minimal si la ligne brisée $(P_0, P_1, \ldots, P_{n-1})$ l'est.*
  La propriété de $1-$minimalité est une condition nécessaire pour qu'un polygone convexe soit minimal. En effet, si un polygone convexe $\mathcal{P}$ n'est pas $1-$minimal, alors il existe un point P'_{j+1} à coordonnées entières sur un des cotés $[P_j, P_{j+1}]$ du $n-$gone.
  Le polygone $\mathcal{P}' = \{P_0, P_1, \ldots, P_j, P'_{j+1}, P_{j+2}, \ldots, P_{n-1})$ est un $n-$gone convexe entier d'aire inférieur à celle de $\mathcal{P}$.

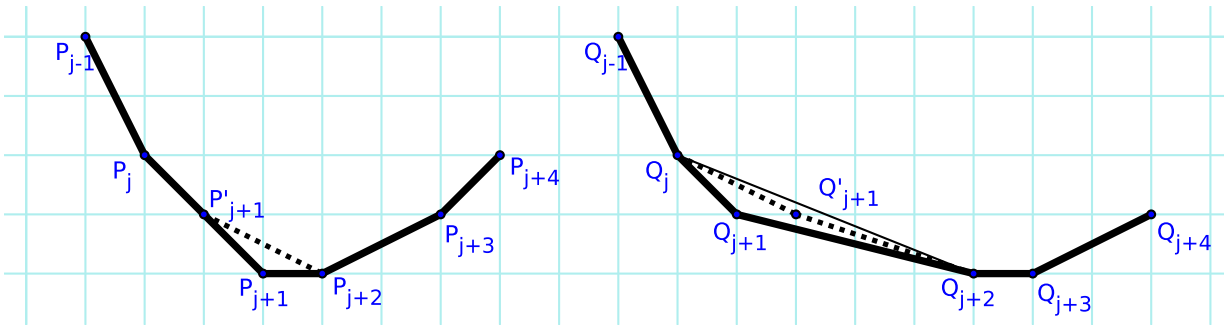


FIGURE VI.1 – Propriété locale de minimalité : la ligne brisée $\mathcal{P} = (P_j)_{1\leq j\leq n}$ n'est pas $1-$minimal. la ligne brisée $1-$minimal $\mathcal{Q} = (Q_j)_{1\leq j\leq n}$ n'est pas $2-$minimal.

- *Un $n-$gone $\mathcal{P} = (P_j)_{0\leq j\leq n-1}$ est $2-$minimal si la ligne brisée fermée $(P_0, P_1, dots, P_{n-1}, P_0, P_1)$ l'est.*
  Avec la propriété locale de $2-$minimalité, on affine la condition nécessaire pour qu'un $n-$gone soit minimal (voir proposition suivante (VI.18)).

Proposition VI.18 *Un polygone convexe entier minimal est $2-$minimal.*

Preuve : On considère un polygone $\mathcal{Q} = \{(Q_j)_{0\leq j\leq n-1}\}$ (voir figure (VI.17)) qui vérifie la propriété de $1-$minimalité et qui n'est pas $2-$minimal. Il existe une corde $[Q_jQ_{j+2}]$ telle que le triangle Δ_j délimité par cette corde admet un point intérieur Q'_{j+1}.

Le polygone $\mathcal{Q}' = \{Q_0, Q_1, \ldots, Q_j, Q'_{j+1}, Q_{j+2}, \ldots, Q_{n-1})$ est un $n-$gone convexe entier d'aire inférieur à celle de $\mathcal{Q}$ (voir figure (VI.17)).

□

4 Chaînages positifs de repères affines directs

4.1 Définition

L'ensemble $\mathcal{R}$ des repères affines du réseau entier $\mathbb{Z}^2$ dans le plan orienté $\mathbb{R}^2$ et l'ensemble $\mathcal{R}^+$ des repères affines positifs s'identifie à (voir proposition (VI.6)) :

$$\mathcal{R} = \{(u, v, t) \in (\mathbb{Z}^2)^3 / det(u, v) = \pm 1\}$$

et

$$\mathcal{R}^+ = \{(u,v,t) \in (\mathbb{Z}^2)^3 / det(u,v) = 1\}.$$

Définition VI.19 *Soient α et β deux entiers.*

Un chaînage positif est une application affine

$$\begin{array}{rccl} C_{\alpha,\beta}: & \mathcal{R} & \longrightarrow & \mathcal{R} \\ & (v,w,t) & \longmapsto & (v',w',t') = (v,w,t).\,[\alpha.\beta] \end{array}$$

où on considère les vecteurs entiers v, w et t comme des entiers de Gauss et $[\alpha.\beta]$ est la matrice

$$[\alpha.\beta] = \begin{pmatrix} -1 & -(\beta+1) & 1 \\ \alpha+1 & (\alpha+1)(\beta+1)-1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{VI.1}$$

On note $\mathcal{C}h_+$ l'ensemble des chaînages positifs.

Remarque VI.20 *Pour tous entiers α et β, le déterminant de la matrice $[\alpha.\beta]$ est 1. Donc un chaînage positif conserve l'orientation et $C_{\alpha,\beta}(\mathcal{R}^+) \subset \mathcal{R}^+$.*

Il est clair que la matrice $[\alpha.\beta]$ est inversible et que le déterminant de son inverse est 1. Donc $C_{\alpha,\beta}(\mathcal{R}^+) = \mathcal{R}^+$.

En particulier, les vecteurs v' et w' sont primitifs et (v',w') est une base du réseau $\mathbb{Z}^2$.

Proposition VI.21 *Étant donnés deux repères affines directs $R = (v,w,t)$ et $R' = (v',w',t')$ du plan affine $\mathbb{Z}^2$, il existe un unique chaînage positif $C_{\alpha,\beta}$ tel que $(v',w',t') = C_{\alpha,\beta}(v,w,t)$ si et seulement si $t' = t+v$ et la ligne brisée $l = (t, t+v, t+v+v', t+v+w')$ est localement convexe et $2-$minimale.*

On dit que les repères R et R' sont chaînés par le chaînage C_{α_β}.

Lemme VI.22 *Soient v, v' et w trois vecteurs entiers tels que $v+v' = (\alpha+1)w$ où α est un entier.*

Si (v,w) est une base du réseau $\mathbb{Z}^2$ alors pour toute origine t, la ligne brisée $(t, t+v, t+v+v')$ est $2-$minimale.

De plus, si (v,w) est une base directe alors la ligne brisée est localement convexe.

Preuve : D'après la relation, il est clair que les vecteurs primitifs v et v' ne sont pas colinéaires. Donc pour toute origine t, la ligne brisée $(t, t+v, t+v+v')$ est 1-minimale.

De plus, comme w est primitif, le nombre de point sur le segment $[t, t+v+v']$ est $\alpha+2$. Or, l'aire du triangle $\Delta(t, t+v, t+v+v')$ est donnée par $\frac{1}{2}|det(v,v')| = \frac{1}{2}|det(v, v+(\alpha+1)w)| = \frac{1}{2}(\alpha+1)|det(v,w)| = \frac{1}{2}(\alpha+1)$.

Donc le triangle $\Delta(t, t+v, t+v+v')$ n'a pas de point intérieur (voir remarque (VI.16)).

Donc la ligne brisée $(t, t+v, t+v+v')$ est $2-$minimale.

De plus, comme $det(v, v') = (\alpha+1)det(v, w)$, si la base (v, w) est directe, alors $det(v, w) > 0$ et la ligne brisée est convexe.

□

Preuve de la proposition VI.21 : Si $(v', w', t') = C_{\alpha,\beta}(v, w, t)$, alors

$$v' = -v + (\alpha+1)w, \tag{VI.2}$$

$$w' = -(\beta+1)v + [(\alpha+1)(\beta+1) - 1]w, \tag{VI.3}$$

$$t' = t + v. \tag{VI.4}$$

Par le lemme (VI.22), la relation (VI.2) implique que la ligne brisée $(t, t+v, t+v+v')$ est convexe et $2-$minimale.

D'après les relations (VI.2) et (VI.3), on a $w+w' = (\beta+1)v'$. Donc par le lemme (VI.22), avec l'origine $t+v$, la ligne brisée $(t+v, t+v+v', t+v+w')$ est convexe et $2-$minimale.

Réciproquement, si la ligne brisée $(t, t+v, t+v+v', t+v+w')$ est convexe et $2-$ minimale, les repères $R = (v, w, t)$ et $R' = (v', w', t+v)$ sont chaînés par l'unique chaînage $C_{\alpha,\beta}$ donné par :

- α est le nombre de points intérieurs au segment $[t, t+v+v']$,
- β est le nombre de points intérieurs au segment $[t+v-w, t+v+w']$.

Ainsi, on a bien les relations (VI.2), (VI.3) et (VI.4).

□

Exemple VI.23

Pour toute origine t, les deux repères affines directes $R = (v, w, t) = (\begin{pmatrix} 2 \\ -3 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}, t)$ et $R' = (v', w', t') = (\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix}, t + \begin{pmatrix} 2 \\ -3 \end{pmatrix})$, représentés sur la figure (VI.2), sont chaînés par le chaînage $C_{2,3}$.

Définition VI.24 *On appelle un $n-$chaînage positif une suite de n chaînages positifs $(C_{\alpha_1,\beta_1}, ..., C_{\alpha_n,\beta_n})$, avec $(\alpha_j)_{1\leq j\leq n}$ et $(\beta_j)_{1\leq j\leq n}$ dans $\mathbb{N}$. On note $\mathcal{C}h_+^*$ l'ensemble des $n-$chaînages positifs.*

Remarque VI.25 *L'ensemble des $n-$chaînages positifs muni de la loi de compostition et du neutre I_3 forme un monoïde libre isomorphe à $\mathbb{N}^2$.*

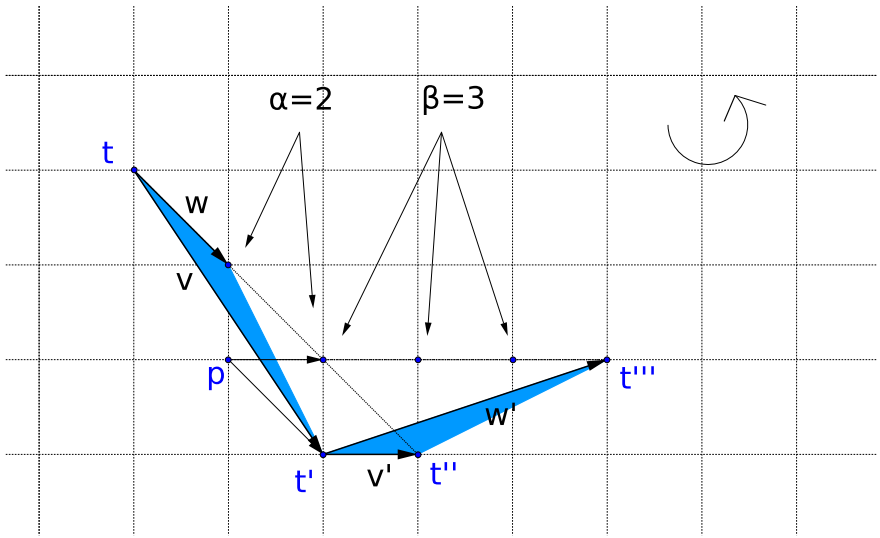


FIGURE VI.2 – Chaîne de deux repères positifs $R = (v, w, t)$ et $R' = (v', w', t')$ telle que $v + v' = 3w$ $(\alpha = 2)$, $w + w' = 4v'$ $(\beta = 3)$, donc de chaînage $C_{2,3}$.

Corollaire VI.26 *de la proposition (VI.21)*

Étant donnés $n+1$ repères affines directs $R_0 = (v_0, w_0, t_0)$, $R_1 = (v_1, w_1, t_1)$, ... et $R_n = (v_n, w_n, t_n)$ du plan affine $\mathbb{Z}^2$, il existe un unique n-chaînage positif $(C_{\alpha_1,\beta_1}, C_{\alpha_2,\beta_2}, \ldots, C_{\alpha_n,\beta_n})$ tel que $(v_j, w'_j, t'_j) = C_{\alpha,\beta}(v_{j-1}, w_{j-1}, t_{j-1})$ pour tout indice $1 \leq j \leq n$ si et seulement si $t_j = t_{j-1} + v_{j-1}$ et la ligne brisée $l = (t_0, t_1, t_2, \dot{t}_n, t_n + w_n)$ est convexe et $2-$minimale.

On dit que les repères R_1, R_2 ...R_n forment une chaîne positive de repères directs. Ils sont chaînés par le chaînage $(C_{\alpha_1,\beta_1}, ..., C_{\alpha_n,\beta_n})$.

Corollaire VI.27 *du corollaire (VI.26)*

L'ensemble des chaînages positifs $\mathcal{C}h^*_+$ est isomorphe à l'ensemble des $n-$lignes brisées $2-$minimales directes modulo le groupe affine $GA(\mathbb{Z}^2)$.

Exemple VI.28 *D'après la proposition (VI.27), étant donné un repère affine direct, un élement du monoïde $\mathcal{C}h^*_+$ peut être représenté par une ligne brisée convexe $2-$minimale, comme dans l'exemple de la figure VI.3.*

4.2 Décomposition d'un chaînage

Pour tout entier a, on note $\tilde{\mu}(a)$ l'application linéaire de $\mathbb{N}$ dans $SL_2(\mathbb{Z})$ définie par :

$$\tilde{\mu}(a) = \begin{pmatrix} 0 & -1 \\ 1 & a+1 \end{pmatrix} \tag{VI.5}$$

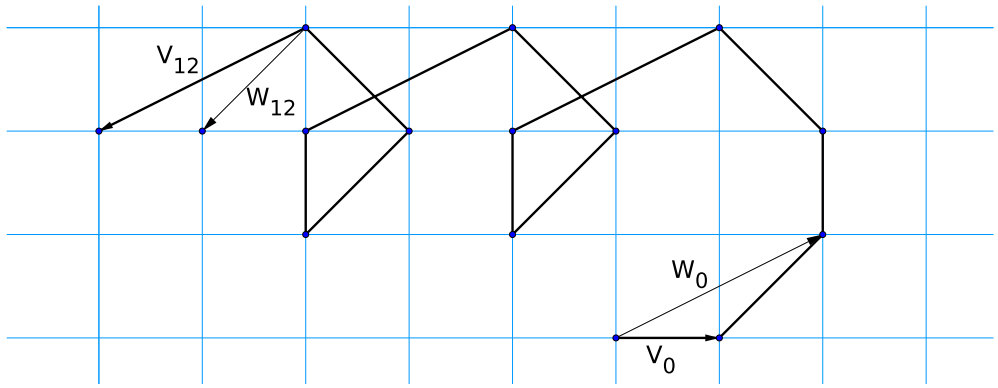


FIGURE VI.3 – Exemple d'un chaînage comportant des boucles. La ligne brisée représentée est l'image de la base $(v_0, w_0) = (1, 2+i)$ par le chaînage $C_{0,2}C_{0,3}C_{0,1}C_{2,0}C_{1,0}C_{0,0}C_{1,0}C_{2,0}C_{1,0}C_{0,0}C_{1,0}C_{2,0}C_{2,0}$.

et on considère les applications affines $(I_2, (1,0))$ et $(\tilde{\mu}(a), (0,0))$ de $GA(\mathbb{Z}^2) = SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ associées aux matrices T_3 et $[a]$ suivantes :

$$T_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{et} \qquad [a] = \begin{pmatrix} 0 & -1 & 0 \\ 1 & a+1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Étant donnés deux entiers α et β, la matrice $[\alpha.\beta]$ d'un chaînage $C_{\alpha,\beta}$ se factorise sous la forme :

$$[\alpha.\beta] \;=\; T_3.\,[\alpha]\,[\beta] \;=\; \begin{pmatrix} & I_2 & 1 \\ & & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} & \tilde{\mu}(\alpha) & 0 \\ & & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} & \tilde{\mu}(\beta) & 0 \\ & & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{VI.6}$$

Cette décomposition d'un chaînage $C_{\alpha,\beta}$ confère deux repères directs intermédiaires entre un repère R et son image R' par le chaînage $C_{\alpha,\beta}$:

$$R = (v, w, t) \underset{T_3}{\longmapsto} (v, w, t') \underset{[\alpha]}{\longmapsto} (w, v', t') \underset{[\beta]}{\longmapsto} R' = (v', w', t').$$

Les bases des repères intermédiaires sont adjacentes et directes.

4.3 Structure de monoïde et morphismes sur le monoïde Σ_2^*

On considère sur l'alphabet $\Sigma = \mathbb{N}$ le monoïde libre Σ^* muni de la loi de concaténation et de l'élément neutre $\emptyset$.

On considère le sous-monoïde libre Σ_2^* de Σ^* composés des mots de longueur paire. On note ι l'injection canonique $\Sigma_2^* \overset{\iota}{\hookrightarrow} \Sigma^*$.

L'ensemble des $n-$chaînages $\mathcal{C}h_+^* = \{(C_{\alpha_1,\beta_1}, ..., C_{\alpha_n,\beta_n}),\ n \geq 0, \alpha_j \text{ et } \beta_j \in \mathbb{N}\}$ est iso-

morphe à Σ_2^*. C'est un monoïde libre. Il est naturel de noter un $n-$chaînage $C_{\alpha_1,\beta_1},...,C_{\alpha_n,\beta_n}$ par un mot sur l'alphabet $\Sigma = \mathbb{N}$ de longueur pair de la forme $\alpha_1\beta_1...\alpha_n\beta_n$.

On note C le morphisme de monoïde défini sur les générateurs de $\mathcal{C}h_+^* \simeq \Sigma_2^*$ par :

$$\begin{array}{rccl} C: & \mathcal{C}h_+ & \longrightarrow & GA(\mathbb{Z}^2) \simeq Sl_2(\mathbb{Z}) \ltimes \mathbb{Z}^2 \\ & \emptyset & \longmapsto & I_3 \\ & \alpha.\beta & \longmapsto & C(\alpha,\beta) = [\alpha,\beta] \quad = \begin{pmatrix} -1 & -(\beta+1) & 1 \\ \alpha+1 & (\alpha+1)(\beta+1)-1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

Ainsi, pour un $n-$chaînage, on a : $C(\alpha_1.\beta_1,...,\alpha_n.\beta_n) = [\alpha_1.\beta_1]...[\alpha_n.\beta_n] = T_3.[\alpha_1].[\beta_1]...T_3.[\alpha_n].[\beta_n]$ où $T_3 = \begin{pmatrix} & I_2 & & 1 \\ & & & 0 \\ 0 & 0 & & 1 \end{pmatrix}$, $[\alpha] = \begin{pmatrix} \tilde{\mu}(\alpha) & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $[\beta] = \begin{pmatrix} \tilde{\mu}(\beta) & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (voir décomposition (VI.6)).

Proposition VI.29 *Le morphisme $C : \mathcal{C}h_+^* \to GA(\mathbb{Z}^2) = SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ est surjectif.*

Preuve : D'une part, les générateurs $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de $SL_2(\mathbb{Z})$ (voir [Se]) et la matrice $U = ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ sont dans l'image de C ; par exemple :

- $C(0.0, 1.0, 0.0, 0.0) = (S, (0,0))$,
- $C(0.0, 0.0, 0.1) = (T, (0,0))$,
- $C(0.0, 1.0, 0.0, 0.1) = (U, (0,0))$.

D'autre part, les pures translations dans chacune des directions canoniques sont dans l'image de M ; par exemple :

- $C(1.0, 0.0, 0.2, 0.1) = (I, (1,0))$,
- $C(1.0, 1.0, 0.1, 0.1) = (I, (0,1))$,
- $C(0.1, 0.2, 0.1, 0.0) = (I, (-1,0))$,
- $C(0.1, 0.1, 1.0, 1.0) = (I, (0,-1))$.

Donc $SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ est engendré par $M(\mathcal{C}h_+^*)$.

□

Remarque VI.30 *On note $K_C \subset \Sigma_2^*$ le noyau de $C : \mathcal{C}h_+^* \to GA(\mathbb{Z}^2)$.*

Géométriquement, étant donné un repère direct R_0 de $\mathcal{R}^+$ et un chaînage $(\alpha_1.\beta_1, \cdots \alpha_n.\beta_n)$ du noyau K_C, la ligne brisée convexe $2-$minimale définie par les origines des repères chaînés

$\{R_0, R_1, ...R_n\}$ se referme "parfaitement" : l'origine t_n du dernier repére R_n est l'origine t_0 du repère initial R_0, et la base (v_n, w_n) du repère final R_n est égale à la base (v_0, w_0) du repère initial R_0.

L'ensemble des polygones convexes correspond, modulo le groupe affine $\mathbb{Z}^2_{aff}$, à l'ensemble des mots non vide du noyau K_C qui ne font pas de boucles.

Remarque VI.31 *Soit π la projection canonique de $GA(\mathbb{Z}^2)$ dans $SL_2(\mathbb{Z})$. On a :*

$$\begin{array}{rccc} \pi \circ C : & \mathcal{C}h^*_+ \simeq \Sigma^*_2 & \longrightarrow & SL_2(\mathbb{Z}) \\ & \alpha.\beta & \longmapsto & \tilde{\mu}(\alpha)\tilde{\mu}(\beta) \end{array}$$

Le noyau de $\pi \circ C$ est l'ensemble des mots de longueur pair dans le noyau de $\tilde{\mu}$.

Étant donné un repère direct R_0 de $\mathcal{R}^+$, un mot du noyau de $\pi \circ C$ correspond à une ligne brisée convexe $2-$minimale définie par les origines des repères chaînés $\{R_0, R_1, ...R_n\}$ telle que la base (v_n, w_n) du repère final R_n est égale à la base (v_0, w_0) du repère initial R_0. Généralement, le ligne brisée ne se referme pas : l'origine du dernier repère R_n est différent de l'origine du repère initial R_0.

L'ensemble des mots de Σ^*_2 associés aux polygones convexes est inclu dans le noyau de $\tilde{\mu}$. Ce sont des mots non nuls du noyau de $\tilde{\mu}$ de longueur pair qui font exactement 1 tour.

Remarque VI.32 *Toujours dans l'objectif d'étudier les polygones convexes entiers, on s'est intéressé au morphisme μ de Σ^* dans $PSL_2(\mathbb{Z})$. Le noyau de μ contient le noyau de $\tilde{\mu}$.*

Les mots de longueur paire du noyau de μ correspondent aux repères chaîn'es tels que la base (v_n, w_n) du dernier repère R_n est soit égale à la base (v_0, w_0) du repère initiale R_0, soit l'opposé $(-v_0, -w_0)$.

4.4 Indice combinatoire et demi-tour sur les bases directes de $\mathbb{Z}^2$.

Dans la partie (IV), on montre que le noyau de $\mu : \Sigma^* \to$ est la classe d'équivalence du mot vide par la relation engendrée par les expansions $R : (ab \to a + 1.0.b + 1), H : (\emptyset \to 000)$ et $U : (a + b \to a000b)$.

En particulier, pour les mots du noyau, il n'est pas nécessaire de considérer l'expansion U.

Ces expansions ne conservent pas la parité d'un mot. On regarde localement les modifications sur les bases intermédiaires.

- Pour l'expansion H : étant donné une base directe $B_0 = (v, w)$ de $\mathbb{Z}^2$, on obtient, pour le mot 000, la suite de bases (B_j) suivante :

$$\begin{aligned} B_0 = (v,w) &\underset{[0]}{\rightarrow} B_1 = (w, -v+w) \\ &\underset{[0]}{\rightarrow} B_2 = (-v+w, -v) \\ &\underset{[0]}{\rightarrow} B_3 = (-v, -w). \end{aligned}$$

Ces bases sont directes et deux bases successives sont adjacentes. Les premiers vecteurs des bases (respectivement les seconds vecteurs) sont dans le demi-plan positif déterminé par v (respectivement w), rangés dans le même ordre. On peut réaliser l'application linéaire associée au mot 000 par déformation continue du vecteur v (respectivement w) d'un demi-tour dans le sens positif.

On dit que la base B_0 fait un demi-tour par le mot 000.

- Pour l'expansion V, étant donné une base directe $B_0 = (v,w)$ et deux entiers α, β, on obtient pour le mot $\alpha\beta$ la suite des bases suivante :

$$\begin{aligned} B_0 = (v,w) &\underset{[\alpha]}{\rightarrow} B_1 = (v_1, w_1) = (w, -v+(\alpha+1)w) \\ &\underset{[\beta]}{\rightarrow} B_2 = (v_2, w_2) = (-w+(\alpha+1)v, -(\beta+1)v + [(\alpha+1)(\beta+1)-1]w) \end{aligned}$$

Et pour le mot $(\alpha+1)0(\beta+1)$, on a :

$$\begin{aligned} B_0 = (v,w) &\underset{[\alpha+1]}{\rightarrow} B'_1 = (v'_1, w'_1) = (w, -v+(\alpha+2)w) \\ &\underset{[0]}{\rightarrow} B'_2 = (v'_2, w'_2) = (-v+(\alpha+2)w, -v-(\alpha+1)w) \\ &\underset{[\beta+1]}{\rightarrow} B'_3 = (v'_3, w'_3) = (-w+(\alpha+1)v, -(\beta+1)v + [(\alpha+1)(\beta+1)-1]w) \\ &= B_2 \end{aligned}$$

Ces bases sont directes et deux bases successives sont adjacentes. Les premiers vecteurs v, v_1, v_2 des bases d'une part et les seconds vecteurs v, v'_1, v'_2, v'_3 d'autre part sont rangés dans cet ordre. Comme $v'_1 = v_1$ et $v'3 = v_2$, le vecteur v'_2 est situé entre v_1 et v_2. Donc les vecteurs des bases sont rangés dans l'ordre suivant :

$$v, \quad w = v_1 = v'_1, \quad w'_1 = v'_2, \quad w_1 = w'_2 = v_2 = v'_3, \quad w_2 = w'_3.$$

On peut réaliser les applications linéaires associées aux mots $\alpha\beta$ et $(\alpha+1)0(\beta+1)$ par déformation continue du vecteur v (respectivement w) suivant le même angle de rotation.

Remarque VI.33 *L'indice conbinatoire d'un mot $\alpha_1\beta_1 \cdots \alpha_n\beta_n$ du noyau de μ de longueur pair compte le nombre d'expansion H et évalue le nombre de tour que que fait la ligne brisée définie par l'image d'un repère affine R_0 par le chaînage $(C_{\alpha_1\beta_1} \cdots C_{\alpha_n\beta_n})$.*

Si l'indice est demi-entier, la ligne brisée ne fait pas un nombre de tour complet. Le mot n'est pas dans le noyau de $\tilde{\mu}$.

Le noyau de $\tilde{\mu}$ *est l'ensemble des mots du noyau* μ *d'indice entier :* $Ker_{\tilde{\mu}} = [\emptyset]_{\mathbb{N}}$.

Les polygones convexes entiers sont les lignes brisées qui se referment, obtenues par des mots du noyau de μ*, de longueur pair et d'indice* 1.

Chapitre VII

Problèmes ouverts.

Ce travail de recherche suggère plusieurs approfondissements et ouvertures. Dans cette partie, on explicite quatre problèmes ouverts qui émanent de cette étude.

1 Les mots non maximaux du noyau de $\mu_{|B^*}$.

Dans le chapitre IV sur le modèle binaire lié à la présentation $\langle\{0,1\}|\mathsf{h} = (000 \to \emptyset, \mathsf{v} = 101 \to 00\rangle$ de $PSL_2(\mathbb{Z})$, l'étude est principalement orientée vers les mots maximaux du noyau de $\mu_{|B^*} : B^* \to PSL_2(\mathbb{Z})$ et plus généralement vers les châteaux maximaux de l'image réciproque $\mu_{|B^*}^{-1}(\langle I, U, U^2\rangle)$ avec $U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

La série génératrice des châteaux à somme $2i$ et indice $\frac{j}{6}$ fixé met en évidence trois triangles $(c_{i,3k+1})_{1\leq i\leq 2k}$, $(c_{i,2k+2})_{1\leq i\leq 2k+1}$ et $(c_{i,3k+3})_{1\leq i\leq 2k+1}$.

Les arbres 3-réguliers décorés ont permis d'expliciter les diagonales $c_{2k,3k+1}$ et $c_{2k+1,3k+2}$, égales à la suite des nombres de Catalan, ainsi que la diagonale $c_{2k+1,3k+3}$, égale à la suite des sommes de deux nombres de Catalan consécutifs.

Les premières valeurs des nombres de châteaux non vides du noyau K_B sont :

				1	2				
			1	7	10	3			
		1	15	55	74	39	7		
	1	26	175	485	650	442	147	19	
1	40	425	1947	4636	6252	4935	2255	552	56

Peut-on caractériser les suites de nombres associées aux autres diagonales, aux lignes, aux colonnes ?

Un sous-ensemble des mots du noyau K_B non maximaux peut-il s'interpréter simplement par d'autres objets combinatoires ?

2 Les mots du noyau de μ d'indice > 1.

Dans le chapitre V, on dénombre les mots du noyau du morphisme $\mu : \Sigma^* \to PSL_2(\mathbb{Z})$ d'indices $\frac{1}{2}$ et 1 à longueur fixée.

Le sous-ensemble $K_{\frac{1}{2}}$ est dénombré par la suite des nombres de Catalan $c_k = \frac{1}{n+1}\binom{2n}{n}$. Le $k-$ième nombre de Catalan est égal à la somme d'une ligne du triangle de Catalan, et on a : pour $k \geq 1$, le nombre de mots de longueur $k+2$ dans le sous-ensemble $K_{\frac{1}{2}}$ est

$$c_k = \sum_{i=0}^{k} T_{k,i}.$$

Le sous-ensemble K_1 est dénombré par une suite faisant intervenir le triangle de Catalan. Le nombre de mot de K_1 de longueur $k+6$ est :

$$T_{k+4,k} + 2\binom{2k+3}{k+4}.$$

Quand est-il pour les mots du noyau d'indice $\frac{k}{2} > 1$?

3 D'autres images réciproques ?

Dans cette étude, on s'est principalement intéressé aux mots des noyaux K_B et K_Σ. On a brièvement vu, sur l'alphabet B, que les mots des images réciproques $\mu^{-1}_{|B^*}(U)$ et $\mu^{-1}_{|B^*}(U^2)$ ont des propriétés simples.

Y a t'il d'autres sous-ensembles $A \subset PSL_2(\mathbb{Z})$ dont l'image réciproque $\mu^{-1}_{|B^*}(A)$ dans B^* ou $\mu^{-1}(A)$ dans Σ^* ait des propriétés remarquables ?

4 Généralisation aux tresses à n brins, $n \geq 4$.

Dans cette étude, on a déterminé deux présentations de monoïde, l'un sur l'alphabet $\Sigma = \mathbb{N}$ et l'autre sur l'alphabet $B = \{0, 1\}$, isomorphes au quotient du groupe de tresse par son centre $B_3/C \simeq PSL_2(\mathbb{Z})$.

L'ensemble des mots du monoïde libre Σ^* (respectivement B^*) est bi-gradué par les morphismes de longueur et d'indice, qui correspond à l'abélianisation du groupe des tresses.

Peut-on généraliser aux autres groupes de tresses B_n pour $n \geq 4$?

5 Les polygones convexes minimaux.

Dans le chapitre VI, on a paramétré un $n-$gone complexe par des mots sur l'alphabet $\Sigma = \mathbb{N}$ de longueur paire.

Réciproquement, existent-il des conditions simples pour que la ligne brisé associée à un mot de longueur paire sur l'alphabet $\Sigma = \mathbb{N}$ soit un polygone convexe.

La "rotation" d'une ligne brisée est donnée par l'étude du noyau de μ et par le morphisme d'indice : le mot associé à un polygone convexe entier est un mot du noyau de $\tilde{\mu}$ d'indice 1 (dans le sous-ensemble K_1).

Comment déterminer, simplement, si un mot de K_1 correspond à une ligne brisée qui se referme ?

Par ailleur, dans l'objectif de réduire le nombre de mots potentiellement associés à des polygones convexes minimaux, peut-on déterminer une (des) condition(s) nécessaire(s) pour qu'un mot de K_1 de longueur paire corresponde à un polygone d'aire minimale ?

Bibliographie

[B] W. G. Brown, *Enumeration of Triangulations of the Disk*, Proc. Lond. Math. Soc. s3-14 (1964) 746-768.

[BT] I. Barany and N. Tokushige, *The minimum area of convex lattice n-gons*, Combinatorica, **24**,No. 2, (2004), 171–185.

[C] T. X. Cai, *On the minimum area of convex lattice polygons*, Taiwanese Journal of Mathematics, **1**, No 4 (1997).

[CS] C. J. Colbourn and R. J. Simpson, *A note on bounds on the minimum area of convex lattice polygons*, Bull. Austral. Math. Soc. **45** (1992), 237–240.

[D] P. Dehornoy, *Le problème d'isotopie des tresses*, Leçons mathématiques de Bordeaux, Cassini, **vol 4**, (2011) 259-300.

[K] D. E. Knuth, *The Art of Computer Programming - Combinatorial Algorithms*, Addison-Wesley, **vol. 4A**, (2006), part 7.2.1.6.

[MKS] W. Magnus, A. Karrass, D. Solitar, *Combinatorial Group Theory - Presentations of Groups in Terms of Generators and Relations*, Courier Corporation,(2004)

[O] D. olszewska, *On the first unknown value of the function g(v)*, Electronic Notes in Discrete Mathematics, **24** (2006), 181-185.

[R1] S. Rabinowitz, *Convex Lattice Polygons*, Ph.D. Dissertation (Polytechnic University, Brooklyn, New York, 1986).

[R2] S. Rabinowitz, $O(n^3)$ *bounds for the area of a convex lattice* $n-gon$, Geombinatorics, vol.II, **4** (1993), 85–88.

[Se] J.P. Serre, *A course in arithmetic*, Springer Verlag, Graduate Texts in Mathematics, **7** (1973), 77–111.

[Si] R. J. Simpson, *Convex lattice polygons of minimum area*, Bull. Austral. Math. Soc. **42** (1990), 353–367.

[Sl] N. J. A. Sloane, *An On-Line Version of the Encyclopedia of Integer Sequences.*, published electronically at http ://oeis.org/, (since 1964).

[St1] R.P.Stanley, *Enumerative Combinatorics*, Cambridge University Press **vol 2** (1999), 219–229.

[St2] R.P.Stanley, *Catalan numbers*, Cambridge University Press (2015).

[WM] Wikipedia, *Nombre de Motzkin*, published electronically at https ://fr.wikipedia.org/wiki/Nombre_de_Motzkin

[WS] Wikipedia, *Nombre de Schröder*, published electronically at https ://fr.wikipedia.org/wiki/Nombre_de_Schröder

[WI] H. Wilf, *Generatingfunctionology*, Academic Press, Inc (1994)