# Déformations de coefficients binomiaux de mots

**Auteur :** Mélot, Robin
**Promoteur(s) :** Rigo, Michel
**Faculté :** Faculté des Sciences
**Diplôme :** Master en sciences mathématiques, à finalité didactique
**Année académique :** 2025-2026
**URI/URL :** http://hdl.handle.net/2268.2/25527

Faculté des Sciences
Département de Mathématique

# Déformations de coefficients binomiaux de mots

Mémoire de fin d'études présenté en vue de l'obtention du titre de
*Master en Sciences Mathématiques, à finalité didactique*

Année académique 2025-2026

*Auteur :*
Robin Mélot

*Promoteur :*
Michel Rigo

# Remerciements

Lorsqu'un travail tel que le mémoire arrive à son terme, l'heure des remerciements arrive également. Je tiens à remercier un panel de personnes qui ont, de près ou de loin, contribué à l'élaboration de ce dernier ou m'ont accompagné tout au long de celui-ci.

Premièrement, je remercie mon formidable promoteur, Michel Rigo, de m'avoir accompagné durant les deux dernières années lors de l'élaboration de ce mémoire. Les nombreuses discussions entre nous m'ont permis non seulement de m'aider à avancer dans la matière lorsque nécessaire mais m'ont également permis de prendre beaucoup de plaisir à réaliser ce travail. Je le remercie également pour sa disponibilité.

Deuxièmement, j'aimerais remercier les personnes du B37 qui, de manière directe ou indirecte, m'ont permis de m'améliorer et de passer d'inoubliables moments lors de mes cinq années d'études. Je pense notamment à Sarah Paternotre et Endymion Piette que je remercie pour leur amitié sans faille et pour le soutien apporté tout au long de mes études. Je pense notamment à Tess Poulet qui a été ma camarade dans de nombreux cours et qui m'a permis de prendre beaucoup de plaisir à y assister. Je remercie également Marie Huart pour les nombreuses discussions et les nombreux fous rires que nous avons pu avoir lorsque nous en avions l'occasion. Je tiens à remercier par la même occasion Pauline David qui m'a permis de passer de nombreux beaux moments. Merci à Marie Théatre pour la touche d'humour qu'elle a su apporter dans les différentes pauses que nous pouvions avoir. Un merci particulier à Thomas Devos pour les nombreuses aides qu'il a pu m'apporter au fil des années. Je remercie aussi Lucy Andrien, Ophélie Gérard et Heidi Bauduin pour toutes les conversations que nous avons eues et pour les différents conseils donnés. Je remercie enfin mon groupe d'ami au sens large pour tous les moments passés ensemble, notamment d'inoubliables soirées, et pour le soutien dans les moments opportuns ! Merci à tous !

Un merci particulier à Tiago Oliveira Mota et Thomas Lamby pour leur relecture attentive de ce mémoire. Il est clair que vous m'avez permis de relever de petits détails qui font toute la différence ! Je vous remercie également tous les deux pour les nombreuses soirées passées ensemble et les rires que nous avons pu partager.

Je remercie l'ensemble des professeurs du B37 pour m'avoir transmis leurs connaissances dans leurs domaines respectifs. Bien que je me sois dirigé vers les mathématiques discrètes, je tiens à remercier Jean-Pierre Schneiders pour les cours donnés et Pierre Mathonet pour la compréhension dont il a pu faire preuve tout au long des études de chacun et chacune. Je remercie Julien Leroy de m'avoir donné le goût des mathématiques discrètes

avec son cours sur les langages formels ainsi qu'avec d'autres de ses cours par la suite, notamment le cours de Théorie ergodique. Je remercie Manon STIPULANTI pour les deux cours qu'elle m'a donnés en Master et pour l'ambiance qu'elle a su créer dans ses cours. Je remercie les trois points fixes des jurys de mémoire, à savoir Céline ESSER, Julien LEROY et Arnout VAN MESSEM. Enfin, merci à Antoine RENARD d'avoir également accepté de faire partie de ce jury.

J'aimerais également prendre le temps de remercier certains amis du basket qui sont à mes côtés depuis longtemps et qui me permettent de pratiquer ma passion. Je remercie Nicolas DIMACAS pour l'amitié qu'il m'apporte au quotidien et pour les conseils plus qu'avisés qu'il me transmet. Merci également à Arthur VAN DE VYVER pour les différents matchs que nous avons passés ensemble et pour les nombreux appels pour prendre des nouvelles. Un grand merci à Arnaud CAWEZ et Thibault BOUNAMEAU pour leur nombreux conseils, dans leur domaine respectif. Enfin, je remercie chaleureusement Alexandre DEPIREUX pour le travail que nous effectuons ensemble au quotidien !

Je remercie également mes parents, sans qui mes études n'auraient pas pu avoir lieu. Merci également d'avoir relu mon mémoire pour trouver quelques fautes de frappe. Un grand merci également à l'ensemble de ma famille qui a su me soutenir durant tous les moments importants.

Pour finir, j'aimerais remercier Marie COLAUX. Sa présence et son soutien dans mes différents projets, que ce soit dans le cadre des études, du basket ou prochainement du travail, sont indispensables. Merci de m'accompagner au quotidien dans les bons comme dans les mauvais moments !

# Table des matières

**Introduction** **v**

**1 Rappels et notations** **1**
1.1 Alphabets et mots . . . . . 1
1.2 Langages et automates . . . . . 2
1.3 Coefficients binomiaux de mots . . . . . 2

**2 Théorème d'Eilenberg** **7**
2.1 Congruences $\sim_u$ et groupes $G_u$ . . . . . 8
2.2 Congruences $\sim_k$ et groupes $G_{r,k}$ . . . . . 13
2.3 Idéal d'augmentation et indices de nilpotence . . . . . 15
2.4 Caractérisation des langages acceptés par un $p$-groupe . . . . . 23

**3 Déformations de coefficients binomiaux de mots** **29**
3.1 Premières définitions et exemples . . . . . 30
3.2 Interprétation combinatoire . . . . . 40
3.3 Analogue de formules classiques de combinatoire . . . . . 48
3.4 Généralisation du théorème d'Eilenberg . . . . . 55
3.4.1 Résultats préliminaires . . . . . 56
3.4.2 Déformations et langages acceptés par un $p$-groupe . . . . . 62

**Bibliographie** **81**

# Introduction

Pour tous naturels $m$ et $n$, le coefficient binomial $\binom{m}{n}$ donne le nombre de parties à $n$ éléments d'un ensemble de $m$ éléments. En combinatoire des mots, le coefficient binomial de deux mots finis $u$ et $v$, noté $\binom{u}{v}$, en constitue une généralisation. Il compte le nombre d'occurrences de $v$ comme sous-mot de $u$. Par exemple, $\binom{abbaba}{aba} = 6$. Ces objets mathématiques, bien connus et déjà bien étudiés, apparaissent dans divers domaines tels que la théorie des langages formels et l'étude des automates finis. Au-delà de leur interprétation combinatoire, ces coefficients jouent un rôle important dans l'étude des relations d'équivalences sur les mots, notamment au travers des congruences définies à partir de propriétés de comptage telle que l'équivalence $k$-binomiale

$$\sim_k = \bigcap_{\substack{u \in A^* \\ |u|=k}} \sim_u,$$

où $w_1 \sim_u w_2$ si et seulement si $\binom{w_1}{v} \equiv \binom{w_2}{v} \mod p$ pour tout facteur $v$ de $u$, qui sera étudiée en détail dans la suite. Ils permettent ainsi de construire des structures algébriques naturelles, comme des monoïdes quotients, qui interviennent dans la reconnaissance de langages. Ces coefficients ont notamment été étudiés en détail dans [7].

Les $q$-déformations sont un outil fondamental en mathématiques modernes. Elles consistent à introduire un paramètre $q$ dans des objets classiques afin d'obtenir davantage d'informations de sorte à ce que, en faisant tendre $q$ vers 1, on retombe sur la version classique. Par exemple, dans les $q$-déformations de coefficients binomiaux de mots, en calculant $\binom{u}{a}_q$, le paramètre $q$ introduit permet de connaître la position des occurrences de $a$ dans $u$. Un exemple central de déformations est donné par les coefficients binomiaux Gaussiens, qui généralisent les coefficients binomiaux classiques. De ce fait, ces coefficients sont, ce qu'on appelle des $q$-analogues des coefficients binomiaux. Le coefficient $q$-binomial est un polynôme en la variable $q$ à coefficients entiers défini par

$$\binom{m}{n}_q = \frac{(1-q^m)(1-q^{m-1})\cdots(1-q^{m-n+1})}{(1-q)(1-q^2)\cdots(1-q^n)},$$

où $m$ et $n$ sont deux naturels.

L'objectif de ce mémoire est d'étudier une version enrichie des coefficients binomiaux de mots, obtenue au travers d'une déformation dépendant d'un paramètre $q$, et d'analyser les structures algébriques ainsi que les langages associés. Ces derniers prennent la forme

de polynôme en la variable $q$ et permettent d'enrichir l'information combinatoire contenue dans les coefficients classiques. De plus, comme les coefficients binomiaux de mots sont des généralisations des coefficients binomiaux classiques, les $q$-déformations des coefficients binomiaux de mots sont aussi une généralisation des coefficients binomiaux Gaussiens. L'objectif est donc double. Nous nous intéressons à ces $q$-déformations dans un contexte général pour ensuite pouvoir généraliser un théorème de Eilenberg.

Le premier chapitre se concentre sur des notions élémentaires à avoir pour aborder ce travail ainsi que des résultats utiles pour s'approprier la matière. Nous faisons des rappels sur la théorie des automates, sur la théorie des langages formels ainsi que certaines propriétés des coefficients binomiaux de mots.

Le deuxième chapitre a pour objectif principal de donner une caractérisation des langages acceptés par un $p$-groupe. Soit $p$ un nombre premier. Nous montrons qu'un langage régulier $L$ sur un alphabet $A$ est accepté par un $p$-groupe si et seulement si $L$ est une combinaison booléenne finie de langages de la forme

$$L_{v,r,p} = \left\{ u \in A^* : \binom{u}{v} \equiv r \mod p \right\},$$

où $r \in \{0, \ldots, p-1\}$ et $v \in A^*$. Pour ce faire, nous introduisons plusieurs notions essentielles à la démonstration de ce théorème. Premièrement, nous introduisons une relation d'équivalence, notée $\sim_u$, qui permettra de définir un groupe quotient $G_u = A^*/\sim_u$. Nous montrons qu'il s'agit en réalité d'un $p$-groupe. Nous nous intéressons également aux idéaux engendrés par des éléments d'une certaine forme qui permettront de passer à l'indice de nilpotence d'un $p$-groupe. Suite à cela, nous démontrons un théorème de Eilenberg qui donne une caractérisation des langages acceptés par un $p$-groupe et donnons des exemples s'y rapportant qui permettent d'illustrer ce dernier. Ce chapitre est basé principalement sur le chapitre 6 du livre *Automata, languages and machines* de Samuel Eilenberg [3].

Le troisième et dernier chapitre a un double objectif. Le premier est, comme explicité ci-dessus, d'introduire une $q$-déformation des coefficients binomiaux de mots. Le deuxième objectif est de généraliser le théorème dû à Samuel Eilenberg. Les $q$-déformations étant des polynômes, l'analogue de ce théorème s'intéressera non pas à la congruence modulo un nombre mais bien modulo un polynôme. L'objectif est donc de montrer que si $p$ est un nombre premier, $A$ est un alphabet, $v \in A^*$ et que le polynôme $\mathfrak{M}(q) = a(q-1)^d$ où $a \in \mathbb{Z}_p[q]$ est non-nul, alors un langage $L$ sur $A$ est accepté par un $p$-groupe si et seulement si $L$ est une combinaison booléenne de langages de la forme

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* : \binom{u}{v}_q \equiv \mathfrak{R} \mod \mathfrak{M} \right\},$$

où $\mathfrak{R} \in \mathbb{Z}_p[q]$ est tel que $\deg(\mathfrak{R}) < \deg(\mathfrak{M})$. Pour ce faire, nous proposons une définition des $q$-déformations des coefficients binomiaux de mots [12], notée $\binom{u}{v}_q$, définie pour tous mots $u, v \in A^*$ et toutes lettres $a, b \in A$ par

$$\binom{u}{\varepsilon}_q = 1, \quad \binom{\varepsilon}{v}_q = 0 \text{ si } v \neq \varepsilon \quad \text{et} \quad \binom{ua}{vb}_q = \binom{u}{vb}_q \cdot q^{|vb|} + \delta_{a,b} \cdot \binom{u}{v}_q.$$

Nous nous intéressons ensuite à plusieurs propriétés préliminaires donnant des informations sur le degré de ces déformations. Ensuite, nous étudions un résultat fondamental de ce chapitre, nous permettant de calculer n'importe quelle $q$-déformation de manière directe. Ce résultat stipule que, en choisissant une occurrence précise de $v$ dans $u$, elle contribue dans $\binom{u}{v}_q$ au terme $q^\alpha$, où $\alpha$ est la somme, sur toutes les lettres de $v$, du nombre de lettres à leur droite qui ne font pas partie de cette occurrence spécifique du sous-mot $v$. Une fois cela fait, nous étudions les analogues de quelques formules classiques de combinatoire comme la formule de Manvel [8, Lemma 1] ou encore [15, Proposition 7.7]

$$\sum_{v \in A^n} \binom{u}{v} = \binom{|u|}{n}.$$

Nous passons dès lors à la généralisation du théorème d'Eilenberg. Comme pour le chapitre précédent, nous travaillons progressivement : nous commençons par quelques observations concernant les indices et périodes de polynômes. Ensuite, nous introduisons une relation d'équivalence, notée $\sim_{u,\mathfrak{M}}$, définie par $w_1 \sim_{u,\mathfrak{M}} w_2$ si et seulement si $\binom{w_1}{v}_q \equiv \binom{w_2}{v}_q \mod \mathfrak{M}$ pour tout facteur non vide $v$ de $u$. Cette relation précise ne sera pas une congruence. Nous cherchons donc un raffinement de celle-ci, qui est elle une congruence et qui est notée $\equiv_{u,\mathfrak{M}}$. De ce fait, nous montrons que $A^*/\equiv_{u,\mathfrak{M}}$ est un groupe. Enfin, nous généralisons le théorème d'Eilenberg, que nous illustrons également au moyen de divers exemples. Ce chapitre est basé principalement sur l'article *Introducing q-deformed binomial coefficients of words* de Antoine Renard, Michel Rigo et Markus Whiteland [12]. Pour les différentes notions de ce chapitre, un programme effectué sur Python a été créé permettant de les calculer directement. Ce programme peut être utilisé pour les calculer dans n'importe quel cadre. Le lecteur intéressé peut évidemment s'en servir.

# Chapitre 1

# Rappels et notations

Nous profitons de ce chapitre pour faire des rappels sur la théorie des langages formels, sur la théorie des automates ainsi que sur les coefficients binomiaux de mots. Ce chapitre a un deuxième objectif : au travers des rappels, nous en profitons pour fixer les notations.

## 1.1 Alphabets et mots

Nous nous intéressons ici à faire des rappels sur la théorie des langages formels [1, 14]. Rappelons qu'un *alphabet* est un ensemble fini d'éléments, appelés *lettres*. Il est dit *unaire* s'il ne contient qu'une seule lettre. Dans l'ensemble de ce document, nous noterons $A$ l'alphabet utilisé. De plus, un *mot fini* sur un alphabet $A$ est une suite finie de lettres de $A$. La longueur d'un mot $u$ sur $A$ est le nombre de lettres constituant ce mot. On la note $|u|$. L'unique mot de longueur nulle est le mot correspondant à la suite vide. C'est le *mot vide*, noté $\varepsilon$. L'ensemble des mots finis sur un alphabet $A$ est noté $A^*$ et $A^* \setminus \{\varepsilon\}$ est noté $A^+$. Enfin, si $n \in \mathbb{N}$, l'ensemble des mots de longueur $n$ (resp. l'ensemble des mots de longueur au plus $n$) est noté $A^n$ (resp. $A^{\leq n}$).

Si $u = u_1 \cdots u_n$ est un mot sur $A$, les mots

$$\varepsilon, u_1, u_1u_2, \ldots, u_1 \cdots u_{n-1}, u_1 \cdots u_n$$

sont les *préfixes* de $u$. De manière similaire, les mots

$$\varepsilon, u_n, u_{n-1}u_n, \ldots, u_2 \cdots u_n, u_1 \cdots u_n$$

sont les suffixes de $u$. De plus, si $i, j \in \{1, \ldots, n\}$ avec $i \leq j$, le mot $u_i \cdots u_j$ est un *facteur* de $u$. L'ensemble des facteurs de $u$ sera noté $\mathrm{Fac}(u)$.

On définit une opération de concaténation sur $A^*$ de la manière suivante. Pour tous les mots $u = u_1 \cdots u_n$ et $v = v_1 \cdots v_l$, la *concaténation de $u$ et $v$*, notée $uv$, est le mot $w = w_1 \cdots w_{n+l}$ où

$$\begin{cases} w_i = u_i & \text{si } i \in \{1, \ldots, n\}, \\ w_{k+i} = v_i & \text{si } i \in \{1, \ldots, l\}. \end{cases}$$

Ainsi, $A^*$ muni de l'opération de concaténation est un monoïde de neutre $\varepsilon$.

## 1.2 Langages et automates

Dans la suite, nous nous intéressons aux langages réguliers ainsi qu'aux langages acceptés par des $p$-groupes. Nous faisons donc des rappels sur les langages formels ainsi que sur les automates [1, 4, 5, 14]. Un *langage* sur un alphabet $A$ est un ensemble, fini ou infini, de mots sur $A$. En d'autres termes, un langage est une partie de $A^*$. Par exemple, si $A = \{a, b\}$, l'ensemble des mots contenant un nombre pair de $a$ est un langage sur $A$. Rappelons également qu'un *automate fini déterministe* est la donnée d'un quintuple $\mathcal{A} = (Q, q_0, F, A, \delta)$, où

- $Q$ est un ensemble fini dont les éléments sont appelés les *états* de $\mathcal{A}$,
- $q_0 \in Q$ est un état appelé *état initial*,
- $F \subseteq Q$ désigne l'ensemble des *états finals*,
- $A$ est l'alphabet de l'automate,
- $\delta : Q \times A \to Q$ est la *fonction de transition* de $\mathcal{A}$.

Il est à noter que la fonction $\delta$ est supposée totale, c'est-à-dire que $\delta$ est défini pour tout couple $(q, a) \in Q \times A$. Cette fonction est étendue à $Q \times A^*$ en définissant $\delta(q, \varepsilon) = q$ et $\delta(q, aw) = \delta(\delta(q, a), w)$ pour toute lettre $a \in A$ et tout mot $w \in A^*$. Le *langage accepté* par un automate fini déterministe $\mathcal{A}$ est l'ensemble des mots qui, à partir de l'état initial, aboutissent dans un des états finals, c'est-à-dire

$$L(\mathcal{A}) = \{w \in A^* : \delta(q_0, w) \in F\}.$$

Enfin, un langage $L$ est *régulier* s'il est accepté par un automate fini déterministe.

## 1.3 Coefficients binomiaux de mots

Dans cette dernière section, nous définissons et étudions un objet mathématique que nous utilisons tout au long de ce document. Nous étudions donc les coefficients binomiaux de mots [7].

**Définition 1.3.1.** Soit $u \in A^*$. Un *sous-mot* du mot $u$ est une suite de lettres qui est contenue dans $u$.

En d'autres termes, un mot $v$ est un sous-mot de $u$ si la suite de lettres composant $v$ est une sous-suite de la suite de lettres composant $u$. La différence entre un sous-mot et un facteur est qu'un facteur est constitué de lettres consécutives, tandis qu'un sous-mot peut contenir des lettres qui se suivent sans être nécessairement consécutives.

**Exemple 1.3.2.** Soit $A = \{a, b, c\}$. Le mot $aba$ est un sous-mot du mot $bacbcab$. De fait, en prenant la deuxième, la quatrième et la sixième lettre dans le mot $bacbcab$, on remarque que $aba$ en est bien un sous-mot. De la même manière, on peut remarquer que $aba$ est également un sous-mot du mot $aabbaa$.

**Définition 1.3.3.** Soient $u, v \in A^*$. Le *coefficient binomial de $u$ et $v$*, noté $\binom{u}{v}$, est le nombre de fois que $v$ apparaît comme sous-mot de $u$. Autrement dit, si $u = u_1 \cdots u_n$ et $v = v_1 \cdots v_l$, on a

$$\binom{u}{v} = \#\left\{(i_1, \ldots, i_l) \in \mathbb{N}^l : 1 \leq i_1 < \cdots < i_l \leq n \text{ et } u_{i_1} \cdots u_{i_l} = v\right\}.$$

Nous adoptons comme convention que $\binom{u}{\varepsilon} = 1$ pour tout mot $u \in A^*$.

**Exemple 1.3.4.** Soient $A = \{a, b\}$ et $u = abbabab \in A^*$. Dans ce cas, on a

$$\binom{u}{a} = 3, \binom{u}{b} = 4 \text{ et } \binom{u}{ab} = 7.$$

**Remarque 1.3.5.** Soient $u, v \in A^*$. Pour calculer le coefficient binomial des mots $u$ et $v$, on compte le nombre d'applications $\varphi : \{1, \ldots, |v|\} \to \{1, \ldots, |u|\}$ telles que $\varphi(1) < \cdots < \varphi(|v|)$ et $u_{\varphi(1)} \cdots u_{\varphi(|v|)} = v$.

Considérons à présent un cas particulier. Si $A = \{a\}$ est un alphabet unaire, le coefficient binomial de mots coïncide avec le coefficient binomial usuel, c'est-à-dire que

$$\binom{a^p}{a^q} = \binom{p}{q} = \frac{p!}{q!(p-q)!}.$$

En effet, obtenir $v = a^q$ comme sous-mot de $u = a^p$ revient exactement à choisir $q$ positions parmi les $p$ positions disponibles dans $u$. Le nombre de tels choix est précisément le coefficient binomial classique. Cette constatation justifie donc notre terminologie.

**Remarque 1.3.6.** Soient $u, v \in A^*$. Pour que $v$ soit un sous-mot de $u$, il faut que $|u| \geq |v|$. En effet, si $|u| < |v|$, alors il n'existe pas de décomposition $(i_1, \ldots, i_{|v|}) \in \{1, \ldots, |u|\}^{|v|}$ telle que $u_{i_1} \cdots u_{i_{|v|}} = v$. De cette manière, $v$ n'est pas un sous-mot de $u$.

La remarque précédente implique la proposition suivante.

**Proposition 1.3.7.** *Soient $u, v \in A^*$. Si $|u| < |v|$, alors*

$$\binom{u}{v} = 0.$$

On obtient le corollaire suivant.

**Corollaire 1.3.8.** *Si $v \in A^+$, alors*

$$\binom{\varepsilon}{v} = 0.$$

La convention $\binom{u}{\varepsilon} = 1$, le corollaire précédent et la proposition suivante permettent de calculer les coefficients binomiaux de mots de manières récursives.

**Proposition 1.3.9.** *Pour tous mots $u, v \in A^*$ et toutes lettres $a, b \in A$, on a*

$$\binom{ua}{vb} = \binom{u}{vb} + \delta_{a,b}\binom{u}{v}$$

*où $\delta_{a,b}$ est le symbole de Kronecker.*

*Démonstration.* Supposons que $a \neq b$. Dans ce cas, les mots $u$ et $ua$ contiennent exactement le même nombre de fois le sous-mot $vb$. Ainsi, on a $\binom{ua}{vb} = \binom{u}{vb}$.

Supposons que $a = b$ et montrons que $\binom{ua}{va} = \binom{u}{va} + \binom{u}{v}$. Les occurrences de $va$ dans $ua$ sont de deux types :

- ▷ les occurrences n'utilisent pas la dernière lettre de $ua$. Dans ce cas, les occurrences sont entièrement contenues dans $u$. Elles correspondent donc exactement aux occurrences de $va$ dans $u$, c'est-à-dire $\binom{u}{va}$.
- ▷ les occurrences utilisent la dernière lettre de $ua$. Dans ce cas, la dernière lettre de $va$, qui est $a$, est alignée avec la dernière lettre de $ua$. Ainsi, pour avoir une occurrence de $va$ dans $ua$, il faut que $v$ apparaisse dans $u$, c'est-à-dire qu'on compte le nombre d'occurrences de $v$ dans $u$.

□

Les relations que nous venons d'obtenir permettent de déterminer n'importe quel coefficient binomial de mots.

**Remarque 1.3.10.** La Proposition 1.3.9 est une généralisation de la formule de Pascal

$$\binom{p}{q} = \binom{p-1}{q} + \binom{p-1}{q-1}.$$

En effet, l'argument utilisé pour démontrer cette proposition est similaire à l'argument utilisé pour démontrer la formule de Pascal. Ce résultat apporte un argument supplémentaire montrant que les coefficients binomiaux de mots généralisent les coefficients binomiaux classiques.

Un programme effectué sur Python permettant de calculer n'importe quel coefficient binomial de mots à partir des entrées $u$ et $v$ est donné à la Figure 1.1.

La proposition suivante, dont une démonstration peut être trouvée dans [7, Corollaire 6.3.7.] pour le lecteur intéressé, est généralisée au Corollaire 3.2.6. Nous nous contentons donc de démontrer cette généralisation. La formule de Chu-Vandermonde pour les entiers s'écrit de la manière suivante :

$$\binom{m+n}{k} = \sum_{\substack{0 \leq i,j \leq k \\ i+j=k}} \binom{m}{i}\binom{n}{j}.$$

**Proposition 1.3.11** (Identité de Chu-Vandermonde). *Pour tous mots $v, w_1, w_2 \in A^*$, on a*

$$\binom{w_1 w_2}{v} = \sum_{\substack{v_1, v_2 \in A^* \\ v = v_1 v_2}} \binom{w_1}{v_1} \binom{w_2}{v_2}.$$

*Autrement dit, pour compter les occurrences de $v$ comme sous-mot de $w_1 w_2$, il suffit de décomposer $v$ en une concaténation $v_1 v_2$ de toutes les façons possibles et de compter indépendamment les occurrences de $v_1$ dans $w_1$ et de $v_2$ dans $w_2$.*

```
import sympy as sp

def coeffbin(u, v):
    if not v:
        return sp.Integer(1)
    if not u:
        return sp.Integer(0)

    u_prime, a = u[:-1], u[-1]
    v_prime, b = v[:-1], v[-1]
    terme_1 = coeffbin(u_prime, v)

    if a == b:
        terme_2 = coeffbin(u_prime, v_prime)
    else:
        terme_2 = sp.Integer(0)

    return terme_1 + terme_2
```

FIGURE 1.1 – Programme permettant de calculer le coefficient binomial des mots $u$ et $v$.

# Chapitre 2

# Théorème d'Eilenberg

Ce chapitre est consacré à l'étude des langages réguliers acceptés par des $p$-groupes, où $p$ est un nombre premier. L'objectif principal est de comprendre comment la structure combinatoire des mots peut être traduite en propriétés algébriques de groupes finis, et inversement, comment des $p$-groupes permettent de caractériser certains langages.

Nous commençons par utiliser les coefficients binomiaux de mots pour définir une relation d'équivalence $\sim_u$ par $w_1 \sim_u w_2$ si et seulement si $\binom{w_1}{v} \equiv \binom{w_2}{v} \mod p$ pour tout facteur $v$ de $u$. Une fois cela fait, nous montrons qu'il s'agit en réalité d'une congruence et que $G_u = A^*/\sim_u$ est un $p$-groupe. Nous nous intéressons à un exemple de tel groupe. Nous définissons ensuite une nouvelle congruence $\sim_k$ par

$$\sim_k = \bigcap_{\substack{u \in A^* \\ |u|=k}} \sim_u .$$

Nous traduisons l'équivalence $\sim_k$ en terme d'appartenance à des idéaux. Nous étudions également l'indice de nilpotence d'un $p$-groupe, ce qui permet de montrer qu'un morphisme de monoïdes $\varphi$ se factorise dans le quotient $G_{r,k} = A^*/\sim_k$ où $r$ est la taille de l'alphabet $A$. Ces différentes propriétés nous permettent enfin de passer au théorème principal, étudiée par Samuel Eilenberg, qui donne une caractérisation précise des langages acceptés par un $p$-groupe, à savoir qu'un langage $L$ est accepté par un $p$-groupe si et seulement si $L$ est une combinaison booléenne de langages de la forme

$$L_{v,r,p} = \left\{ u \in A^* : \binom{u}{v} \equiv r \mod p \right\}$$

où $v \in A^*$ et $r \in \{0, \ldots, p-1\}$.

Bien que d'autres sources ont pu contribuer pour certaines parties, l'ensemble de ce chapitre est principalement basé sur le livre *Automata, languages and machines* de Samuel Eilenberg [3]. Dans ce chapitre, le nombre $p$ est un nombre premier.

## 2.1 Congruences $\sim_u$ et groupes $G_u$

Les coefficients binomiaux de mots permettent de définir des relations d'équivalences naturelles entre les mots, en comparant leurs occurrences de facteurs. Ces relations forment la base de la construction des groupes qui interviennent dans la reconnaissance des langages.

**Notation 2.1.1.** Nous notons $\mathbf{G}_p$ la classe de tous les groupes finis dont l'ordre est une puissance de $p$, c'est-à-dire la classe de tous les groupes d'ordre $p^r$ où $r$ est un nombre entier. Autrement dit, ce sont exactement les $p$-groupes finis.

**Remarque 2.1.2.** Un groupe fini $G$ est un $p$-groupe si et seulement si l'ordre de chacun de ses éléments est une puissance de $p$. Or, si $G$ est fini d'ordre $p^r$, alors pour tout $x \in G$, on a $x^{p^r} = 1$. On peut donc écrire

$$\mathbf{G}_p = \bigcup_{k \geq 0} \mathbf{G}_{p,k},$$

où $\mathbf{G}_{p,k}$ est la classe des $p$-groupes d'ordre $p^k$. Autrement dit,$\mathbf{G}_{p,k}$ est la classe de tous les groupes finis d'ordre exactement $p^k$.

Nous définissons une congruence importante dans la suite de notre étude.

**Définition 2.1.3.** Soit $u \in A^*$. Pour tous mots $w_1, w_2 \in A^*$, on définit la relation d'équivalence $\sim_u$ sur $A^*$ par

$$w_1 \sim_u w_2 \iff \binom{w_1}{v} \equiv \binom{w_2}{v} \mod p$$

pour tout facteur $v$ de $u$. Autrement dit, deux mots $w_1$ et $w_2$ sont équivalents pour la relation $\sim_u$ si et seulement si, pour chaque facteur $v$ de $u$, le nombre de fois où $v$ apparaît comme sous-mots dans $w_1$ et dans $w_2$ est congru modulo $p$.

**Remarque 2.1.4.** Étant donné que $\binom{u}{\varepsilon} = 1$ pour tout mot $u \in A^*$, il est clair que

$$\binom{w_1}{\varepsilon} \equiv \binom{w_2}{\varepsilon} \mod p$$

pour tous mots $w_1, w_2 \in A^*$.

Illustrons cette relation d'équivalence.

**Exemple 2.1.5.** Soient $A = \{a, b\}$, $u = ab \in A^*$ et $p = 2$. Remarquons que l'ensemble des facteurs de $u$ est l'ensemble $\mathrm{Fac}(u) = \{\varepsilon, a, b, ab\}$. Considérons les mots $w_1 = abab$ et $w_2 = baba$. Dans ce cas,

- ◇ pour $v = a$ et pour $v = b$, on a directement la conclusion car $w_1$ et $w_2$ ont le même nombre de $a$ et de $b$.

◇ pour $v = ab$, on a

$$\binom{abab}{ab} = 3 \quad \text{et} \quad \binom{baba}{ab} = 1.$$

Les deux coefficients sont bien congrus modulo 2.

Ainsi, pour tous facteurs $v$ de $u$, on a

$$\binom{abab}{v} \equiv \binom{baba}{v} \mod 2,$$

c'est-à-dire que $abab \sim_{ab} baba$.

**Remarque 2.1.6.** Soit $u \in A^*$. La relation $\sim_u$ est bien une relation d'équivalence. Cela résulte du fait que la relation modulo est une relation d'équivalence.

**Notation 2.1.7.** Si $u \in A^*$, on note $G_u$ le quotient $A^*/\sim_u$.

**Proposition 2.1.8.** *Pour tout mot $u \in A^*$, la relation d'équivalence $\sim_u$ est une congruence. De plus, le quotient $G_u$ est un $p$-groupe dont l'ordre de chaque élément divise $p^{|u|}$.*

*Démonstration.* Montrons que $\sim_u$ est une congruence. Pour cela, il suffit de montrer que si $w \sim_u w'$ et que $t \sim_u t'$, où $w, w', t, t' \in A^*$, alors on a $wt \sim_u w't'$. Soit $v$ un facteur du mot $u$. Par la Proposition 1.3.11, on sait que

$$\binom{wt}{v} = \sum_{\substack{v_1, v_2 \in A^* \\ v = v_1 v_2}} \binom{w}{v_1}\binom{t}{v_2}. \tag{2.1}$$

De manière similaire, au travers de la Proposition 1.3.11, on obtient que

$$\binom{w't'}{v} = \sum_{\substack{v_1, v_2 \in A^* \\ v = v_1 v_2}} \binom{w'}{v_1}\binom{t'}{v_2}. \tag{2.2}$$

Étant donné que $v_1$ et $v_2$ sont des facteurs de $v$ et que $v$ est un facteur de $u$, on sait que $v_1$ et $v_2$ sont des facteurs de $u$. De cette manière, étant donné que $w \sim_u w'$ et que $t \sim_u t'$, on obtient par définition de $\sim_u$ que

$$\binom{w}{v_1} \equiv \binom{w'}{v_1} \mod p$$

et

$$\binom{t}{v_2} \equiv \binom{t'}{v_2} \mod p.$$

De cette manière, étant donné la relation (2.1), on obtient que

$$\begin{aligned}\binom{wt}{v} &\equiv \sum_{\substack{v_1, v_2 \in A^* \\ v = v_1 v_2}} \binom{w'}{v_1}\binom{t'}{v_2} \mod p \\ &\equiv \binom{w't'}{v} \mod p\end{aligned}$$

par la relation (2.2). On obtient par définition que $wt \sim_u w't'$, ce qui nous donne la conclusion que $\sim_u$ est une congruence.

Montrons que le quotient $G_u = A^*/\sim_u$ est un $p$-groupe dont l'ordre de chaque élément divise $p^{|u|}$. Premièrement, étant donné que $\sim_u$ est une congruence finie, remarquons que $G_u$ est un monoïde fini. Pour montrer que le quotient $G_u$ est un $p$-groupe dont l'ordre de chaque élément divise $p^{|u|}$, il suffit de montrer que $[w]^{p^{|u|}} = [\varepsilon]$ pour tout $w \in A^*$, c'est-à-dire que $w^{p^{|u|}} \sim_u \varepsilon$, ou de manière équivalente que

$$\binom{w^{p^k}}{v} \equiv \binom{\varepsilon}{v} \mod p$$

pour tout facteur $v$ de $u$ tel que $|v| \in \{1, \ldots, k\}$. Étant donné le Corollaire 1.3.8, ceci revient à montrer que

$$\binom{w^{p^k}}{v} \equiv 0 \mod p$$

pour tout facteur $v$ de $u$ tel que $|v| \in \{1, \ldots, k\}$ et tout mot $w \in A^*$. Procédons par récurrence sur $k \geq 1$.

- Supposons que $k = 1$. Dans ce cas, le résultat est trivialement vérifié. En effet, si $k = 1$, alors $v$ est une lettre sur $A$ et $w^{p^k} = w^p$. De plus, on sait que $\binom{w}{v}$ compte le nombre d'occurrences de $v$ dans le mot $w$. Il existe donc $m \in \{0, \ldots, |w|\}$ tel que $|w|_v = m$. Dans ce cas, étant donné que

  $$\binom{w^p}{v} = |w^p|_v,$$

  on obtient $\binom{w^p}{v} = p \cdot m$. Par conséquent, on a

  $$\binom{w^{p^k}}{v} = \binom{w^p}{v} \equiv 0 \mod p,$$

  ce qui nous donne la conclusion dans ce cas.

- Supposons que le résultat soit vrai pour tous les facteurs de longueur plus petite ou égale à $k$. Considérons maintenant les facteurs $v$ de longueur $k+1$. Par la Proposition 1.3.11, on a

  $$\binom{w^{p^{k+1}}}{v} = \sum_{\substack{v_1,\ldots,v_p \in A^* \\ v = v_1 \cdots v_p}} \binom{w^{p^k}}{v_1} \cdots \binom{w^{p^k}}{v_p}.$$

  S'il existe $i \in \{1, \ldots, p\}$ tel que $|v_i| \in \{1, \ldots, k\}$, alors par hypothèse de récurrence, on obtient que

  $$\binom{w^{p^k}}{v_i} \equiv 0 \mod p$$

et le terme entier est nul modulo $p$. Ainsi, il reste les termes avec $v_i = v$ et $v_j = \varepsilon$ pour $j \neq i$. Chacun des ces termes est égal à $\binom{w^{p^k}}{v}$ et il y a exactement $p$ tels termes. De cette manière, on a

$$\binom{w^{p^{k+1}}}{v} \equiv 0 \mod p,$$

ce qui nous donne la conclusion pour la récurrence.

De cette manière, on a la conclusion que le quotient $G_u$ est un $p$-groupe dont l'ordre de chaque élément divise $p^{|u|}$. □

**Exemple 2.1.9.** Soient $A = \{a, b\}$, $u = ab \in A^*$ et $p = 2$. Par la Proposition 2.1.8, on sait que le quotient $G_{ab} = \{a, b\}^*/\sim_{ab}$ est un 2-groupe dont l'ordre de chaque élément divise

$$2^{|ab|} = 2^2 = 4.$$

Deux mots $w_1, w_2 \in A^*$ sont équivalents pour la congruence $\sim_{ab}$ si et seulement si $\binom{w_1}{a} \equiv \binom{w_2}{a} \mod 2$, $\binom{w_1}{b} \equiv \binom{w_2}{b} \mod 2$ et $\binom{w_1}{ab} \equiv \binom{w_2}{ab} \mod 2$. Chaque classe d'équivalence est donc déterminée par un triplet

$$\left(\binom{w}{a} \mod 2, \binom{w}{b} \mod 2, \binom{w}{ab} \mod 2\right).$$

La relation $\sim_{ab}$ dépend de la parité du nombre de $a$, de la parité du nombre de $b$ et de la parité du nombre de $ab$. Les huit classes d'équivalences sont données par $C_1, C_2, \ldots, C_8$, formées de l'ensemble des mots $w \in \{a, b\}^*$ tels que la parité du nombre de $a$, de $b$ et de $ab$ dans $w$ est définie à la Figure 2.1 pour chaque classe d'équivalence.

| | $\binom{w}{a}$ mod 2 | $\binom{w}{b}$ mod 2 | $\binom{w}{ab}$ mod 2 |
|---|---|---|---|
| $C_1$ | 0 | 0 | 0 |
| $C_2$ | 0 | 0 | 1 |
| $C_3$ | 0 | 1 | 0 |
| $C_4$ | 0 | 1 | 1 |
| $C_5$ | 1 | 0 | 0 |
| $C_6$ | 1 | 0 | 1 |
| $C_7$ | 1 | 1 | 0 |
| $C_8$ | 1 | 1 | 1 |

FIGURE 2.1 – Définition des 8 classes d'équivalences du groupe $\{a, b\}^*/\sim_{ab}$.

L'opération de $G_{ab}$ est la concaténation modulo $\sim_{ab}$, c'est-à-dire que

$$[w_1] \cdot [w_2] := [w_1 w_2].$$

La table de multiplication pour cette concaténation est donnée à la Figure 2.2.

| $\cdot$ | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ | $C_6$ | $C_7$ | $C_8$ |
|---|---|---|---|---|---|---|---|---|
| $C_1$ | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ | $C_6$ | $C_7$ | $C_8$ |
| $C_2$ | $C_2$ | $C_1$ | $C_4$ | $C_3$ | $C_6$ | $C_5$ | $C_8$ | $C_7$ |
| $C_3$ | $C_3$ | $C_4$ | $C_1$ | $C_2$ | $C_7$ | $C_8$ | $C_5$ | $C_6$ |
| $C_4$ | $C_4$ | $C_3$ | $C_2$ | $C_1$ | $C_8$ | $C_7$ | $C_6$ | $C_5$ |
| $C_5$ | $C_5$ | $C_6$ | $C_8$ | $C_7$ | $C_1$ | $C_2$ | $C_4$ | $C_3$ |
| $C_6$ | $C_6$ | $C_5$ | $C_7$ | $C_8$ | $C_2$ | $C_1$ | $C_3$ | $C_4$ |
| $C_7$ | $C_7$ | $C_8$ | $C_6$ | $C_5$ | $C_3$ | $C_4$ | $C_2$ | $C_1$ |
| $C_8$ | $C_8$ | $C_7$ | $C_5$ | $C_6$ | $C_4$ | $C_3$ | $C_1$ | $C_2$ |

FIGURE 2.2 – Table de multiplication du groupe $\{a,b\}^*/\sim_{ab}$ avec 8 classes d'équivalences.

Chaque élément de ce tableau a été obtenu de la manière suivante :

- pour déterminer la parité du nombre de $a$ du produit de deux classes, il suffit d'additionner la parité de $a$ dans la première classe et de la parité de $a$ dans la deuxième classe.

  Par exemple, pour le produit entre $C_4$ et $C_5$, étant donné que $C_4$ a un nombre pair de $a$ et $C_5$ a un nombre impair de $a$, le produit a un nombre impair de $a$.

- pour déterminer la parité du nombre de $b$ du produit de deux classes, il suffit de procéder de la même manière que pour le parité du nombre de $a$.

  Par exemple, pour le produit entre $C_4$ et $C_5$, étant donné que $C_4$ a un nombre impair de $b$ et $C_5$ a un nombre pair de $b$, le produit a un nombre impair de $b$.

- pour déterminer la parité du nombre de $ab$, on utilise la Proposition 1.3.11, c'est-à-dire, dans ce cas-ci, l'égalité

$$\binom{uw}{ab} \mod 2 \equiv \binom{u}{ab} \mod 2 + \binom{w}{ab} \mod 2 + \binom{u}{a}\binom{w}{b} \mod 2,$$

  où $u \in C_i$ et $w \in C_j$ avec $i,j \in \{1,\dots,8\}$.

  Par exemple, pour le produit entre $C_4$ et $C_5$, étant donné que $C_4$ a un nombre impair de $ab$ et $C_5$ a un nombre pair de $ab$, alors si $u \in C_4$ et $w \in C_5$, on a

$$\binom{uw}{ab} \mod 2 \equiv \binom{u}{ab} \mod 2 + \binom{w}{ab} \mod 2 + \binom{u}{a}\binom{w}{b} \mod 2 = 1.$$

Ainsi, le produit entre $C_4$ et $C_5$ contient un nombre impair de $ab$. Au vu de ce qui précède, le produit entre $C_4$ et $C_5$ est exactement la classe $C_8$. On a procédé de la même manière pour les autres produits.

Montrons à présent que pour chaque représentant $w$ de $C_i$, avec $i \in \{1,\dots,8\}$, on a que $w^{2^2} \sim_{ab} \varepsilon$.

- ◇ Un représentant de la classe $C_1$ est $w = \varepsilon$. On remarque que $w^4 = \varepsilon^4 = \varepsilon$, ce qui donne que $w^4 \sim_{ab} \varepsilon$.

- ◇ Un représentant de la classe $C_2$ est $w = abab$. On a donc $w^4 = abababababababab$. On remarque que $\binom{w^4}{a} = 8 \equiv 0 \mod 2$, $\binom{w^4}{b} = 8 \equiv 0 \mod 2$ et $\binom{w^4}{ab} = 36 \equiv 0 \mod 2$. Ainsi, on a bien $w^4 \sim_{ab} \varepsilon$.
- ◇ Pour les classes $C_3, \ldots, C_8$, on procède de la même manière, en utilisant le fait qu'un représentant de la classe $C_3$ (resp. $C_4$, $C_5$, $C_6$, $C_7$, $C_8$) est $b$ (resp. $aba$, $a$, $bab$, $ba$, $ab$).

## 2.2 Congruences $\sim_k$ et groupes $G_{r,k}$

Après avoir étudié les congruences pour un mot particulier, nous passons à une vision plus globale. Nous combinons les informations sur tous les facteurs de longueur donnée pour créer des groupes $G_{r,k}$. Ces groupes synthétisent les propriétés combinatoires des mots et permettent de comprendre comment les mots peuvent être classés modulo les congruences.

**Définition 2.2.1.** Soit $k$ un naturel. On définit la congruence $\sim_k$ par

$$\sim_k = \bigcap_{\substack{u \in A^* \\ |u|=k}} \sim_u .$$

Dans la suite, $k$ est un nombre naturel.

**Remarque 2.2.2.** Soit $u \in A^*$ tel que $|u| = k$. Étant donné que $\sim_u$ est une congruence par la Proposition 2.1.8 et que l'intersection de congruences est une congruence, on obtient bien que $\sim_k$ est une congruence.

**Remarque 2.2.3.** Au vu de la définition de la congruence $\sim_k$, il est clair que si $w_1, w_2 \in A^*$ sont deux mots tels que $|w_1|, |w_2| \geq k$, alors on a $w_1 \sim_k w_2$ si et seulement si $w_1 \sim_u w_2$ pour tout mot $u \in A^*$ tel que $|u| = k$. De plus, si $w_1 \sim_k w_2$, alors on a

$$\binom{w_1}{v} \equiv \binom{w_2}{v} \mod p$$

pour tout facteur $v$ de $u$ tel que $|v| \leq k$.

Illustrons cette congruence avec un exemple.

**Exemple 2.2.4.** Soient $A = \{a, b\}$, $p = 2$ et $k = 2$. Remarquons que l'ensemble des mots de longueur 2 sur $A$ est donné par $\{aa, ab, ba, bb\}$. On obtient donc que

$$\sim_2 = \sim_{aa} \cap \sim_{ab} \cap \sim_{ba} \cap \sim_{bb} .$$

Considérons les mots $w_1 = aabb$ et $w_2 = bbaa$. Le tableau donnant les coefficients modulo 2 pour les mots de longueur égale à 2 est donné à la Figure 2.3. Tous les coefficients sont identiques modulo 2 pour tous les mots de longueur égale à 2. De cette manière, on obtient que $aabb \sim_2 bbaa$.

| $u$ | $\binom{aabb}{u}$ | $\binom{aabb}{u} \mod 2$ | $\binom{bbaa}{u}$ | $\binom{bbaa}{u} \mod 2$ |
|---|---|---|---|---|
| $aa$ | 1 | 1 | 1 | 1 |
| $ab$ | 4 | 0 | 0 | 0 |
| $ba$ | 0 | 0 | 4 | 0 |
| $bb$ | 1 | 1 | 1 | 1 |

FIGURE 2.3 – Coefficients modulo 2 pour les mots de longueur égale à 2 sur $A = \{a, b\}$.

**Notation 2.2.5.** Si $A$ est un alphabet de taille $r \geq 1$, le quotient $A^*/\sim_k$ est noté $G_{r,k}$.

**Remarque 2.2.6.** Il découle de ce qui a été fait précédemment que $G_{r,k}$ est un sous-groupe du produit

$$\prod_{\substack{u \in A^* \\ |u|=k}} G_u.$$

Étant donné que $G_u$ est un $p$-groupe dont l'ordre de chaque élément divise $p^{|u|}$ par la Proposition 2.1.8, on obtient que $G_{r,k}$ est un $p$-groupe dont l'ordre de chaque élément divise $p^k$.

**Proposition 2.2.7.** *Si $A$ est un alphabet de taille $r \geq 1$, on a $G_{r,0} = \varepsilon$ et $G_{r,1}$ est isomorphe à $\mathbb{Z}_p^r$.*

*Démonstration.* Montrons que $G_{r,0} = \varepsilon$. Par définition, on sait que $G_{r,0}$ est le quotient $A^*/\sim_0$ où

$$\sim_0 = \bigcap_{\substack{u \in A^* \\ |u|=0}} \sim_u = \sim_\varepsilon .$$

Ainsi, $G_{r,0} = G_\varepsilon$. Par la Proposition 2.1.8, on sait que $G_\varepsilon$ est un $p$-groupe d'ordre

$$p^{|\varepsilon|} = p^0 = 1.$$

De cette manière, le groupe $G_\varepsilon$ est le groupe trivial. Dès lors, le produit

$$\prod_{\substack{u \in A^* \\ |u|=0}} G_u$$

est trivial. Étant donné que le sous-groupe d'un groupe trivial est trivial, on obtient que le sous-groupe $G_{r,0}$ est également trivial, ce qui est équivalent à $G_{r,0} = \varepsilon$.

Montrons que $G_{r,1}$ est isomorphe à $\mathbb{Z}_p^r$. Nous considérons donc tous les mots $u$ de longueur égale à 1, c'est-à-dire les lettres de l'alphabet $A$. Pour toute lettre $a \in A$, le $p$-groupe $G_a$ est par la Proposition 2.1.8 d'ordre

$$p^{|a|} = p^1 = p.$$

De cette manière, on obtient que le $p$-groupe $G_a$ est isomorphe à $\mathbb{Z}_p$. Étant donné que l'alphabet est de taille $r$, le produit $\prod_{a\in A} G_a$ est isomorphe à $\mathbb{Z}_p^r$. Définissons l'application

$$\Phi : A^* \to \mathbb{Z}_p^r,\ w \mapsto (|w|_a \mod p)_{a\in A}.$$

Remarquons que pour toute lettre $a \in A$, la composante $|w|_a \mod p$ est exactement l'image de $w$ dans $G_a$ puisque $G_a$ encode les occurrences du facteur $a$ modulo $p$. De plus, on obtient par construction que $\Phi$ est un morphisme. En effet, si $w_1, w_2 \in A^*$, alors on a $|w_1w_2|_a = |w_1|_a + |w_2|_a$. En réduisant cette égalité modulo $p$, on obtient que

$$|w_1w_2|_a \mod p = |w_1|_a \mod p + |w_2|_a \mod p$$

pour tous $w_1, w_2 \in A^*$. Comme cela vaut pour toute lettre $a \in A$, on obtient que $\Phi(w_1w_2) = \Phi(w_1) + \Phi(w_2)$ pour tous mots $w_1, w_2 \in A^*$. Enfin, pour le mot vide $\varepsilon$, on a $|\varepsilon|_a = 0$, ce qui nous donne donc que $\Phi(\varepsilon) = (0, \dots, 0)$ qui est l'élément neutre de $\mathbb{Z}_p^r$. De cette manière, l'application $\Phi$ est un morphisme. Enfin, on remarque que le noyau de l'application $\Phi$ est exactement la relation $\sim_1$. En effet, deux mots sont équivalents modulo $\sim_1$ si et seulement s'ils ont le même nombre d'occurrences des différentes lettres modulo $p$. Par le premier théorème d'isomorphisme, on obtient que l'image de $\Phi$ est isomorphe au quotient $A^*/\sim_1$, c'est-à-dire que $\Phi(A^*)$ est isomorphe à $G_{r,1}$. Montrons que l'application $\Phi$ est surjective et nous aurons $\Phi(A^*) = \mathbb{Z}_p^r$. On pourra conclure que $G_{r,1}$ est isomorphe à $\mathbb{Z}_p^r$. Soit $x = (x_a)_{a\in A}$ un élément quelconque de $\mathbb{Z}_p^r$. Pour toute lettre $a \in A$, notons $n_a$ un représentant dans l'ensemble $\{0, \dots, p-1\}$ tel que $n_a \equiv x_a \mod p$. Construisons le mot

$$w = \prod_{a\in A} a^{n_a}.$$

Dans ce cas, pour toute lettre $a \in A$, on a $|w|_a = n_a$. De cette manière, la $a$-ième composante de $\Phi(w)$ est $n_a \mod p$, c'est-à-dire $x_a$. De cette manière, $\Phi(w) = x$. On obtient par définition que l'application $\Phi$ est surjective, ce qui nous donne la conclusion. □

## 2.3 Idéal d'augmentation et indices de nilpotence

Pour mieux manipuler ces congruences et les relier aux $p$-groupes, nous traduisons notre approche combinatoire en langage algébrique. L'étude des idéaux dans l'algèbre de mots et de leur puissance nous permet de définir l'indice de nilpotence des $p$-groupes, une notion clé pour factoriser tout morphisme de mots vers un $p$-groupe.
Soient $A = \{a_1, \dots, a_r\}$ un alphabet de taille $r$ et $p$ un nombre premier. Considérons l'algèbre du monoïde libre $\mathbb{Z}_p\langle A^*\rangle$. En tant qu'espace vectoriel sur $\mathbb{Z}_p$, une base est formée par tous les mots de $A^*$. De plus, un élément général s'écrit

$$x = \sum_{w\in A^*} x_w w,$$

où $x_w \in \mathbb{Z}_p$ et où seul un nombre fini de coefficients sont non nuls. La multiplication est obtenue en étendant linéairement la concaténation des mots, c'est-à-dire que

$$\left(\sum_{u\in A^*} x_u u\right)\left(\sum_{v\in A^*} y_v v\right) = \sum_{\substack{u\in A^*\\ v\in A^*}} x_u y_v (uv).$$

Cette algèbre est exactement l'anneau des polynômes non commutatifs $\mathbb{Z}_p\langle a_1, \ldots, a_r\rangle$. Définissons l'application

$$\alpha : \mathbb{Z}_p\langle A^*\rangle \to \mathbb{Z}_p, \sum_{w\in A^*} x_w w \mapsto \sum_{w\in A^*} x_w$$

et notons $I = \ker(\alpha)$, c'est-à-dire

$$I = \left\{ \sum_{w\in A^*} x_w w : \sum_{w\in A^*} x_w = 0 \text{ dans } \mathbb{Z}_p \right\}.$$

Montrons que $I = \langle 1 - w : w \in A^*\rangle$. Pour tout mot $w \in A^*$, on a

$$\alpha(1-w) = 1 - 1 = 0.$$

Ainsi, $1 - w$ appartient à $I$ pour tout $w \in A^*$. Supposons que $x \in I$. Écrivons $x = \sum_{w\in A^*} x_w w$ et supposons que $\sum_{w\in A^*} x_w = 0$. Dans ce cas, on a

$$\begin{aligned} x &= \sum_{w\in A^*} x_w w \\ &= \sum_{w\in A^*} x_w w - \sum_{w\in A^*} x_w \\ &= \sum_{w\in A^*} x_w (w-1) \\ &= -\sum_{w\in A^*} x_w (1-w). \end{aligned}$$

Les coefficients $x_w$, avec $w \in A^*$, appartiennent à $\mathbb{Z}_p \subseteq \mathbb{Z}_p\langle A^*\rangle$. Ainsi, on obtient que $x$ est une combinaison linéaire finie dans $\mathbb{Z}_p$ des éléments de la forme $1 - w$, avec $w \in A^*$. Cette écriture appartient donc à l'idéal engendré par les éléments de la forme $1 - w$, avec $w \in A^*$. On en conclut que l'idéal $I$ est exactement l'idéal engendré par les éléments de la forme $1 - w$ avec $w \in A^*$.

**Définition 2.3.1.** Soit $G$ un groupe. Une application $f : G \to G$ est une *involution* si $f(f(x)) = x$ pour tout $x \in G$.

La démonstration du lemme suivant est classique et est laissée au lecteur.

**Lemme 2.3.2.** *Soit $G$ un groupe. Si $f : G \to G$ est une involution, alors $f$ est une bijection.*

**Notation 2.3.3.** Pour tout naturel $n$, nous noterons

$$I^n = \{w^n : w \in I\}.$$

**Proposition 2.3.4.** *Soient $w_1, w_2 \in A^*$. Dans ce cas, on a $w_1 \sim_k w_2$ dans $A^*$ si et seulement si $w_1 - w_2 \in I^{k+1}$ dans $\mathbb{Z}_p\langle A^*\rangle$.*

*Démonstration.* Soit $A = \{a_1, \ldots, a_r\}$ un alphabet de taille $r$. Définissons le morphisme d'algèbres $\pi : \mathbb{Z}_p\langle A^*\rangle \to \mathbb{Z}_p\langle A^*\rangle$ en posant, pour toute lettre $a_i$,

$$\pi(a_i) = 1 - a_i. \tag{2.3}$$

Étant donné que $\mathbb{Z}_p\langle A^*\rangle$ est l'algèbre libre engendrée par les éléments $a_1, \ldots, a_r$, cette définition détermine un unique morphisme d'algèbre. Montrons que $\pi$ est une involution. Pour cela, montrons que $\pi(\pi(u)) = u$ en procédant sur la longueur de $u$.

- ◇ Supposons que $u$ est de longueur 1, c'est-à-dire que $u$ est une lettre. Pour tout $i \in \{1, \ldots, r\}$, on a $\pi(\pi(a_i)) = \pi(1 - a_i)$. Or, étant donné que $\pi$ est un morphisme d'algèbres, il est linéaire ce qui nous donne que $\pi(1 - a_i) = \pi(1) - \pi(a_i)$. Or, $\pi$ envoie l'unité sur l'unité, ce qui nous donne que $\pi(1) = 1$. De plus, par définition, on a $\pi(a_i) = 1 - a_i$. Ainsi, on obtient que

  $$\pi(\pi(a_i)) = 1 - (1 - a_i) = a_i$$

  pour tout $i \in \{1, \ldots, r\}$.

- ◇ Supposons que le résultat est vérifié pour un mot $u \in A^*$, c'est-à-dire que $\pi(\pi(u)) = u$ et montrons que $\pi(\pi(ua)) = ua$ pour une lettre $a \in A$. En effet, étant donné que $\pi$ est un morphisme, on a

  $$\begin{aligned} \pi(ua) &= \pi(u)\pi(a) \\ &= \pi(u)(1 - a) \\ &= \pi(u) - \pi(u)a. \end{aligned}$$

  De cette manière, on a

  $$\begin{aligned} \pi(\pi(ua)) &= \pi(\pi(u)) - \pi(\pi(u)) \cdot \pi(a) \\ &= u - u \cdot (1 - a) \\ &= u - u + ua \\ &= ua. \end{aligned}$$

Par définition, on obtient que $\pi$ est une involution. Par le Lemme 2.3.2, on obtient que l'application $\pi$ est une bijection. Or, étant donné que $\pi$ est un morphisme d'algèbres bijectif, on obtient que $\pi$ est un automorphisme. De cette manière, la condition $w_1 - w_2 \in I^{k+1}$ est équivalente au fait que

$$\pi(w_1) - \pi(w_2) \in J^{k+1},$$

où $J = \pi(I)$. En effet, étant donné que $\pi$ est un automorphisme, on sait que $\pi(I^{k+1}) = (\pi(I))^{k+1}$. De cette manière, on a

$$\begin{aligned} w_1 - w_2 \in I^{k+1} &\iff \pi(w_1 - w_2) \in \pi(I^{k+1}) \\ &\iff \pi(w_1) - \pi(w_2) \in (\pi(I))^{k+1} \\ &\iff \pi(w_1) - \pi(w_2) \in J^{k+1}. \end{aligned}$$

Montrons que l'idéal $J^{k+1}$ est engendré par les éléments $v$ de $A^*$ tel que $|v| > k$. L'idéal $I$ est engendré par les éléments de la forme $1 - w$ avec $w \in A^+$. L'égalité

$$1 - w_1 w_2 = (1 - w_1) + w_1(1 - w_2)$$

implique que $I$ est l'idéal engendré par les éléments de la forme $1 - a$ avec $a \in A$. De plus, étant donné que $J = \pi(I)$, l'idéal $J$ est l'idéal engendré par les éléments de la forme $\pi(1-a)$. Étant donné que $\pi$ est une involution et vu la relation (2.3), on sait que $\pi(1 - a) = a$. Ainsi, l'idéal $J$ est l'idéal engendré par les éléments de la forme $a$ avec $a \in A$. L'idéal $J^{k+1}$ est donc engendré par les produits de $k + 1$ lettres, c'est-à-dire par les mots $v$ de $A^*$ tel que $|v| > k$.

Montrons que

$$\pi(w) = \sum_{u \in A^*} (-1)^{|u|} \binom{w}{u} u \tag{2.4}$$

pour tout mot $w \in A^*$. Étant donné la Proposition 1.3.7 et le fait que $w$ est un mot fini, on remarque que la somme ci-dessus est finie. Procédons par récurrence sur la longueur de $w$.

- ◇ Supposons que $w$ est de longueur nulle, c'est-à-dire que $w = \varepsilon$. Pour tout mot $u \in A^*$, par le Corollaire 1.3.8, on a $\binom{\varepsilon}{u} = 0$ si $|u| > 0$. De plus, par convention, on sait que $\binom{\varepsilon}{\varepsilon} = 1$. De cette manière, dans le terme de droite de la relation (2.4), seul le terme $u = \varepsilon$ reste. De plus, on a

  $$(-1)^{|\varepsilon|} \binom{\varepsilon}{\varepsilon} \varepsilon = (-1)^0 \varepsilon = \varepsilon.$$

  Enfin, le fait que $\pi(\varepsilon) = \pi(1) = 1 = \varepsilon$ implique que la relation (2.4) est vérifiée pour $w = \varepsilon$.

- ◇ Supposons à présent que $w = a$ où $a \in A$. Par la Proposition 1.3.7, on sait que les seuls mots $u$ tels que $\binom{a}{u} \neq 0$ sont $u = \varepsilon$ et $u = a$. De plus, on a $\binom{a}{\varepsilon} = \binom{a}{a} = 1$. Le

terme de droite dans la relation (2.4) devient

$$\sum_{u\in\{\varepsilon,a\}}(-1)^{|u|}\binom{a}{u}u=(-1)^0\binom{a}{\varepsilon}\varepsilon+(-1)^1\binom{a}{a}a$$
$$=\varepsilon-a.$$

Enfin, étant donné que $\pi(a)=1-a$ et que $\varepsilon$ est l'unité 1 dans l'algèbre, on obtient la conclusion que la relation (2.4) est vérifiée si $w=a$ avec $a\in A$.

◇ Supposons à présent que la relation (2.4) est vérifiée pour les mots $w_1,w_2\in A^*$ et montrons qu'elle est vérifiée pour le mot $w_1w_2\in A^*$. Étant donné que $\pi$ est un morphisme, par hypothèse de récurrence et par la Proposition 1.3.11, on a

$$\begin{aligned}\pi(w_1w_2)&=\pi(w_1)\pi(w_2)\\&=\sum_{u_1\in A^*}(-1)^{|u_1|}\binom{w_1}{u_1}u_1\sum_{u_2\in A^*}(-1)^{|u_2|}\binom{w_2}{u_2}u_2\\&=\sum_{\substack{u_1\in A^*\\u_2\in A^*}}(-1)^{|u_1u_2|}\binom{w_1}{u_1}\binom{w_2}{u_2}u_1u_2\\&=\sum_{u\in A^*}(-1)^{|u|}\sum_{\substack{u_1,u_2\in A^*\\u=u_1u_2}}\binom{w_1}{u_1}\binom{w_2}{u_2}u\\&=\sum_{u\in A^*}(-1)^{|u|}\binom{w_1w_2}{u}u,\end{aligned}$$

ce qui donne la conclusion pour l'induction.

De cette manière, la relation (2.4) est vérifiée pour tout mot $w\in A^*$.

Montrons que la condition $w_1\sim_k w_2$ dans $A^*$ est équivalente à la condition $w_1-w_2\in I^{k+1}$ dans $\mathbb{Z}_p\langle A^*\rangle$. Pour faire cela, étant donné que la condition $w_1-w_2\in I^{k+1}$ est équivalente à la condition $\pi(w_1)-\pi(w_2)\in J^{k+1}$, on montre que les conditions $w_1\sim_k w_2$ et $\pi(w_1)-\pi(w_2)\in J^{k+1}$ sont équivalentes. En effet, de la relation (2.4), on remarque que

$$\begin{aligned}\pi(w)&=\sum_{u\in A^*}(-1)^{|u|}\binom{w}{u}u\\&=\sum_{\substack{u\in A^*\\|u|\le k}}(-1)^{|u|}\binom{w}{u}u+\sum_{\substack{u\in A^*\\|u|>k}}(-1)^{|u|}\binom{w}{u}u\\&\equiv\sum_{\substack{u\in A^*\\|u|\le k}}(-1)^{|u|}\binom{w}{u}u\mod J^{k+1}.\end{aligned}$$

Si $w_1\sim_k w_2$, alors par la Remarque 2.2.3, on sait que

$$\binom{w_1}{u}\equiv\binom{w_2}{u}\mod p$$

pour tout mot $u$ tel que $|u| \leq k$. Dans $\mathbb{Z}_p\langle A^*\rangle$, on obtient donc que

$$\begin{aligned}\pi(w_1) - \pi(w_2) &= 0 + \sum_{\substack{u\in A^*\\|u|>k}} (-1)^{|u|}\binom{w_1}{u}u - \sum_{\substack{u\in A^*\\|u|>k}} (-1)^{|u|}\binom{w_2}{u}u \\ &\in J^{k+1},\end{aligned}$$

ce qui nous donne la conclusion. □

**Proposition 2.3.5.** *Soit $G$ un $p$-groupe d'ordre $q$. Si $I_G$ est l'idéal dans $\mathbb{Z}_p\langle G\rangle$ engendré par les éléments de la forme $1-g$ avec $g \in G$, alors on a $I_G^q = 0$.*

*Démonstration.* Procédons par récurrence sur l'ordre du groupe $G$.

- Supposons que $|G| = q = 1$. Si $G = \{e\}$, ce qui veut dire que $G$ est le groupe trivial, l'anneau $\mathbb{Z}_p\langle G\rangle$ s'identifie naturellement à $\mathbb{Z}_p$ via l'isomorphisme qui envoie $x_e e$ sur $x_e$. Dans cette identification, l'élément $1-e$ vaut

  $$1 - e = 1 - 1 = 0.$$

  De cette manière, l'idéal $I_G$ engendré par les éléments de la forme $1-g$ avec $g \in G$ est l'idéal nul, c'est-à-dire que $I_G^1 = 0$.

- Supposons que le résultat soit vrai pour tous les $p$-groupes d'ordre strictement plus petit que $q$ et soit $G$ un groupe d'ordre $q > 1$. Étant donné que le centre d'un $p$-groupe non trivial est non trivial, le $p$-groupe $G$ a un centre non trivial. Il existe donc un élément central $c$ d'ordre $p$. Posons $C = \langle c\rangle$ et $H = G/C$. Par le Théorème de Lagrange, on a $|H| = \frac{q}{p}$.
  La projection de groupes $\pi : G \to H$ s'étend par linéarité en un morphisme d'algèbres $\pi : \mathbb{Z}_p\langle G\rangle \to \mathbb{Z}_p\langle H\rangle$. De plus, montrons que son noyau $K = \ker(\pi)$ est un idéal dans $\mathbb{Z}_p\langle G\rangle$. L'application $\pi$ étant un morphisme d'algèbres, le noyau

  $$K = \{x \in \mathbb{Z}_p\langle G\rangle : \pi(x) = 0\}$$

  est donc le noyau d'un morphisme d'anneaux. Or, pour tout morphisme d'anneaux $f$, le noyau $\ker(f)$ est un idéal, ce qui nous donne la conclusion que $K$ est un idéal de $\mathbb{Z}_p\langle G\rangle$.
  Montrons que

  $$K = (1-c)\,\mathbb{Z}_p\langle G\rangle. \tag{2.5}$$

  Étant donné que

  $$\pi(1-c) = 1 - 1 = 0,$$

  il est clair que l'inclusion $(1-c)\,\mathbb{Z}_p\langle G\rangle \subseteq K$ est vérifiée. Montrons l'autre inclusion. Considérons une fonction $\varphi : H \to G$ telle que $\pi(\varphi)$ soit l'identité. Nous étendons cette fonction en une transformation linéaire $\psi : \mathbb{Z}_p\langle H\rangle \to \mathbb{Z}_p\langle G\rangle$. Étant donné que tout élément $g \in G$ peut s'écrire

  $$g = c^i(\varphi(h))$$

pour un $i \in \{1, \ldots, p\}$ et $h \in H$, il s'ensuit que tout élément $x \in \mathbb{Z}_p\langle G\rangle$ est de la forme

$$x = \sum_{i=1}^{p} c^i(\psi(x_i))$$

pour des éléments $x_1, \ldots, x_p \in \mathbb{Z}_p\langle H\rangle$. Étant donné que

$$\pi(x) = \sum_{i=1}^{p} \pi(\psi(x_i)) = \sum_{i=1}^{p} x_i,$$

il s'ensuit que $x \in K$ si et seulement si $\sum_{i=1}^{p} x_i = 0$. Ainsi, pour $x \in K$, on a

$$x = \sum_{i=1}^{p} (c^i - 1)(\psi(x_i)).$$

Étant donné que $c^i - 1 \in (1-c)\,\mathbb{Z}_p\langle G\rangle$ pour tout entier $i \in \{1, \ldots, p\}$, on en tire que $x \in (1-c)\,\mathbb{Z}_p\langle G\rangle$. De cette manière, l'inclusion $K \subseteq (1-c)\,\mathbb{Z}_p[G]$ est vérifiée. On en tire que la relation (2.5) est vérifiée.
En notant $r = |H| = \frac{q}{p}$, on a

$$\begin{aligned} \pi(I_G^r) &= (\pi(I_G))^r \\ &= I_H^r \\ &= 0 \end{aligned}$$

par hypothèse de récurrence. Ainsi, on obtient que

$$I_G^r \subseteq K = (1-c)\,\mathbb{Z}_p\langle G\rangle$$

et il s'ensuit que

$$I_G^q = (I_G^r)^p \subseteq (1-c)^p\,\mathbb{Z}_p\langle G\rangle.$$

Pour avoir la conclusion, il suffit donc de montrer que $(1-c)^p = 0$. Remarquons que dans le binôme de Newton de $(1-c)^p$, tous les coefficients binomiaux $\binom{p}{i}$ avec $i \in \{1, \ldots, p-1\}$ sont divisibles par le nombre premier $p$. Ainsi, on a

$$\begin{aligned} (1-c)^p &= 1 - c^p \\ &= 1 - 1 \\ &= 0. \end{aligned}$$

De cette manière, on a $I_G^q = 0$, ce qui nous donne la conclusion.

□

**Exemple 2.3.6.** Soit $p = 2$ et considérons le groupe cyclique $G = \{e, g\}$ tel que $g^2 = e$. L'ordre de $G$ est donné par

$$q = |G| = 2.$$

Les éléments de $\mathbb{Z}_2\langle G\rangle$ sont donnés par $ae + bg$ avec $a, b \in \mathbb{Z}_2$. Les quatre éléments sont donc $0, e, g$ et $e + g$. On peut identifier $e$ à 1 et, dans ce cas, on a $g^2 = 1$. Par définition, on sait que

$$I_G = \langle 1 - g : g \in G\rangle.$$

Cependant, dans $\mathbb{Z}_2$, on a $1 - g = 1 + g$. On en tire que

$$I_G = \langle 1 + g : g \in G\rangle = \{0, 1 + g\}.$$

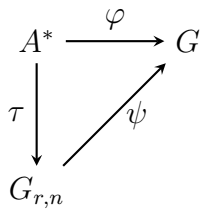
Montrons que $I_G^2 = \{(1 + g)^2 : g \in G\} = 0$. On sait que

$$(1 + g)^2 = 1 + 2g + g^2.$$

Or, dans $\mathbb{Z}_2$, on a $2g = 0$ et $g^2 = 1$. On obtient donc que $(1 + g)^2 = 0$, c'est-à-dire que $I_G^2 = 0$. Étant donné que $q = 2$, on a bien la conclusion que $I_G^q = 0$.

**Définition 2.3.7.** Soit $G$ un $p$-groupe. Le plus petit entier $n \geq 1$ tel que $I_G^{n+1} = 0$ est appelé l'*indice de nilpotence* du $p$-groupe $G$.

**Proposition 2.3.8.** *Soient $A$ un alphabet de taille $r$ et $G$ un $p$-groupe d'indice de nilpotence $n \geq 1$. Si $\varphi : A^* \to G$ est un morphisme de monoïdes, alors $\varphi$ se factorise à travers le quotient $G_{r,n} = A^*/\!\sim_n$. Autrement dit, il existe un morphisme de groupes $\psi : G_{r,n} \to G$ tel que le diagramme*




*commute, où $\tau$ est le morphisme quotient associé à la congruence $\sim_n$.*

*Démonstration.* Le morphisme de monoïdes $\varphi : A^* \to G$ s'étend par linéarité en un morphisme d'algèbres $\varphi : \mathbb{Z}_p\langle A^*\rangle \to \mathbb{Z}_p\langle G\rangle$. Soit $I$ l'idéal d'augmentation de $\mathbb{Z}_p\langle A^*\rangle$. Par définition, on a

$$I = \langle 1 - a : a \in A\rangle.$$

Pour toute lettre $a \in A$, on a $\varphi(1 - a) = 1 - \varphi(a)$. Étant donné que $\varphi(a) \in G$, l'élément $1 - \varphi(a)$ appartient à l'idéal d'augmentation $I_G$. On en tire que $\varphi(I) \subseteq I_G$. Cela implique que

$$\varphi(I^{n+1}) \subseteq I_G^{n+1}.$$

Or, puisque $G$ est d'indice de nilpotence $n$, on a $I_G^{n+1} = 0$. On obtient donc que $\varphi(I^{n+1}) = 0$. Soient deux mots $w_1, w_2 \in A^*$ tels que $w_1 \sim_n w_2$. Par la Proposition 2.3.4, on sait que $w_1 - w_2 \in I^{n+1}$. En particulier, en appliquant $\varphi$, on a

$$\varphi(w_1) - \varphi(w_2) \in \varphi(I^{n+1}) = 0.$$

De cette manière, on obtient que $\varphi(w_1) = \varphi(w_2)$. Le morphisme $\varphi$ est donc constant sur les classes d'équivalences de $\sim_n$. Il existe alors une application bien définie $\psi : G_{r,n} \to G$ telle que $\psi([w]) = \varphi(w)$ pour tout mot $w \in A^*$. Par construction, on a $\varphi = \psi \circ \tau$, ce qui nous donne la conclusion. □

**Proposition 2.3.9.** *Soit $G$ un $p$-groupe engendré par au plus $r$ éléments. Si $G$ est d'indice de nilpotence $n \geq 1$, alors $G$ est un groupe quotient de $G_{r,n}$.*

*Démonstration.* Étant donné que le groupe $G$ est engendré par au plus $r$ éléments, il existe des éléments $g_1, \ldots, g_r \in G$ qui engendrent $G$. Considérons un alphabet $A = \{a_1, \ldots, a_r\}$ et définissons un morphisme de monoïdes $\varphi : A^* \to G$ par $\varphi(a_i) = g_i$ pour tout $i \in \{1, \ldots, r\}$. Étant donné que les éléments $g_1, \ldots, g_r$ engendrent $G$, le morphisme $\varphi$ est surjectif. Par la Proposition 2.3.8, il existe un morphisme $\psi : G_{r,n} \to G$ tel que $\varphi = \psi \circ \tau$ où $\tau : A^* \to G_{r,n}$ est le morphisme quotient. Le morphisme $\tau$ étant surjectif car il s'agit d'un morphisme quotient, la surjectivité de $\varphi$ entraîne la surjectivité de $\psi$. Ainsi, $G$ est l'image homomorphe de $G_{r,n}$, c'est-à-dire que $G$ est isomorphe à $G_{r,n}/\ker(\psi)$. On conclut que $G$ est quotient du groupe $G_{r,n}$. □

**Corollaire 2.3.10.** *Tout $p$-groupe fini peut être obtenu comme quotient d'un groupe $G_{r,n}$ pour certains entiers $r \geq 1$ et $n \geq 1$.*

**Corollaire 2.3.11.** *Tout $p$-groupe fini peut être construit à partir des groupes $G_u$, avec $u \in A^*$, en utilisant seulement des produits directs finis, des sous-groupes et des quotients.*

*Démonstration.* On sait que chaque groupe $G_{r,n}$ est un sous-groupe d'un produit direct fini de groupes de la forme $G_u$, où $u$ parcourt les mots de longueur $n$. Or, par le Corollaire 2.3.11, tout $p$-groupe fini est quotient d'un certain groupe $G_{r,n}$. Par conséquent, tout $p$-groupe fini peut être obtenu à partir des groupes $G_u$, en utilisant uniquement des produits directs finis, des sous-groupes et des quotients. □

## 2.4 Caractérisation des langages acceptés par un $p$-groupe

Nous relions nos constructions à la théorie des langages. Le théorème dû à Eilenberg fournit une caractérisation remarquable des langages acceptés par des $p$-groupes en termes de combinaisons booléennes de certains ensembles.

Nous allons donc maintenant décrire la classe des langages acceptés par des $p$-groupes finis. Plus précisément, pour chaque alphabet fini $A$, nous considérons les langages $L \subseteq A^*$ pour lesquels il existe un morphisme de monoïdes $\varphi : A^* \to G$, où $G$ est un $p$-groupe fini, tel que $L = \varphi^{-1}(P)$ pour une certaine partie $P \subseteq G$.

Le théorème d'Eilenberg affirme que ces langages sont précisément les combinaisons booléennes d'ensembles définis à partir des coefficients binomiaux de mots modulo $p$. Pour pouvoir énoncer ce théorème, nous définissons un ensemble de mots jouissant d'une certaine propriété.

**Définition 2.4.1.** Soient $X$ un ensemble et $\mathcal{A}$ une famille de parties de $X$. Une *combinaison booléenne* d'éléments de $\mathcal{A}$ est tout ensemble de $X$ obtenu à partir des ensembles de $\mathcal{A}$ au moyen d'un nombre fini d'opérations d'union, d'intersection et de complémentaire.

**Définition 2.4.2.** La *clôture booléenne* d'une famille $\mathcal{A}$ de parties de $X$ est l'ensemble de toutes les combinaisons booléennes d'éléments de $\mathcal{A}$. Il s'agit de la plus petite famille de sous-ensembles de $X$ contenant $\mathcal{A}$ et stable par union, intersection et complémentaire.

La notation apparaissant dans la définition suivante est issue de [12]. Elle permettra de faire un lien avec le Chapitre 3.

**Définition 2.4.3.** Soient $v \in A^*$ et un entier $r \in \{0, \dots, p-1\}$. On définit le langage $L_{v,r,p}$ par

$$L_{v,r,p} = \left\{ u \in A^* : \binom{u}{v} \equiv r \mod p \right\}.$$

Autrement dit, le langage $L_{v,r,p}$ est l'ensemble des mots $u$ dont le nombre d'occurrences de $v$ comme sous-mot est congru à $r$ modulo $p$.

Illustrons cette définition au travers de deux exemples.

**Exemple 2.4.4.** Soient $A = \{a, b\}$, $v = a \in A$, $p = 2$ et $r = 1$. Dans ce cas, le langage

$$L_{a,1,2} = \left\{ u \in \{a, b\}^* : \binom{u}{a} \equiv 1 \mod 2 \right\}$$

est l'ensemble des mots $u \in \{a, b\}^*$ tels que le nombre de lettres $a$ dans $u$ est impair. L'automate minimal de ce langage est donné à la Figure 2.4. Ce langage est donc régulier.

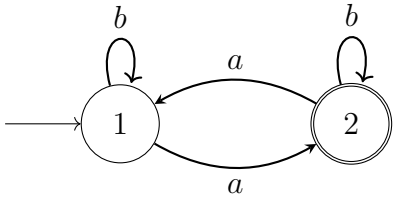



FIGURE 2.4 – Automate minimal du langage $L_{a,1,2}$.

**Exemple 2.4.5.** Soient $A = \{a, b\}$, $v = ab \in A^*$, $p = 3$ et $r = 2$. Dans ce cas, le langage

$$L_{ab,2,3} = \left\{ u \in \{a, b\}^* : \binom{u}{ab} \equiv 2 \mod 3 \right\}$$

contient les mots $u$ dont le nombre d'occurrences du sous-mot $ab$ est congru à 2 modulo 3. L'automate minimal de ce langage est donné à la Figure 2.5. Pour construire cet automate, il est nécessaire de mémoriser deux informations modulo 3 : le nombre de lettres $a$ déjà lues et le nombre d'occurrences du sous-mot $ab$ déjà rencontrées. Pour $x, y \in \{0, 1, 2\}$, l'état $q_{xy}$ représente donc l'ensemble des mots $u$ tels que

$$\binom{u}{a} \equiv x \mod 3 \quad \text{et} \quad \binom{u}{ab} \equiv y \mod 3.$$

La lecture d'une lettre $a$ augmente simplement le nombre de $a$ modulo 3, sans modifier le nombre d'occurrences de $ab$. En revanche, lorsqu'on lit une lettre $b$, chaque occurrence précédente de la lettre $a$ peut former un nouveau sous-mot $ab$. Ainsi, si un mot contient $x$ occurrences de $a$ modulo 3, alors la lecture d'un $b$ augmente le nombre d'occurrences de $ab$ de $x$ modulo 3. Les états finals sont donc les états $q_{x2}$ pour $x \in \{0, 1, 2\}$. Ce langage est donc régulier.

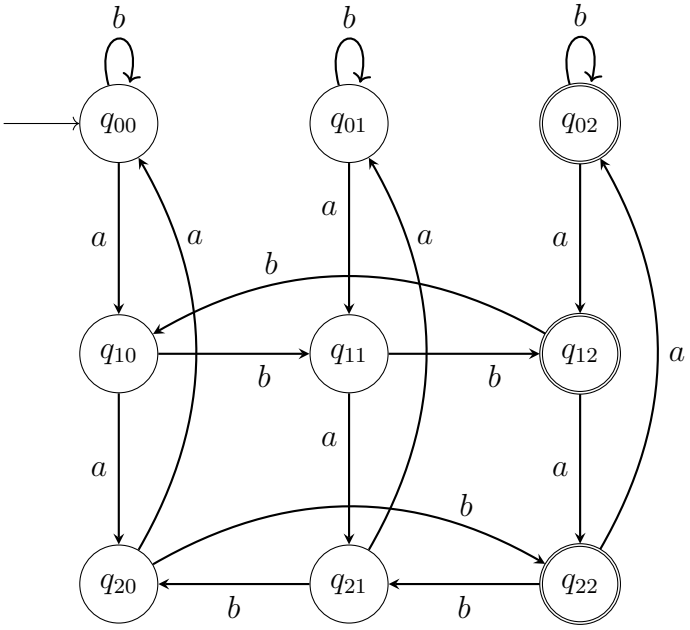



FIGURE 2.5 – Automate minimal du langage $L_{ab,2,3}$.

Nous pouvons maintenant énoncer le théorème principal.

**Théorème 2.4.6** (Théorème d'Eilenberg)**.** *Un langage $L$ sur $A$ est accepté par un $p$-groupe si et seulement si $L$ est une combinaison booléenne finie de langages de la forme $L_{v,r,p}$ où $v \in A^*$ et $r \in \{0, \ldots, p-1\}$.*

*Démonstration.* La condition est suffisante. Considérons un langage de la forme

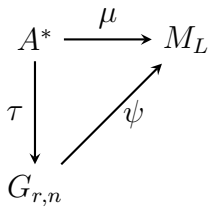
$$L_{v,r,p} = \left\{ u \in A^* : \binom{u}{v} \equiv r \mod p \right\}.$$

Par définition de la congruence $\sim_v$, on sait que

$$w_1 \sim_v w_2 \iff \binom{w_1}{x} \equiv \binom{w_2}{x} \mod p$$

pour tout facteur $x$ de $v$. En particulier, cela vaut pour $x = v$. Ainsi, deux mots équivalents pour la congruence $\sim_v$ ont le même coefficient $\binom{w}{v} \mod p$. Ainsi, l'appartenance d'un mot à $L_{v,r,p}$ dépend uniquement de la classe d'équivalence modulo $\sim_v$. De cette manière, l'ensemble $L_{v,r,p}$ est une union de classes d'équivalences de la congruence $\sim_v$. Cela signifie qu'il existe un ensemble $P \subseteq G_v$ tel que $L_{v,r,p} = \tau^{-1}(P)$ où $\tau : A^* \to G_v$. De plus, on sait, par la Proposition 2.1.8, que $G_v$ est un $p$-groupe. Par conséquent, l'ensemble $L_{v,r,p}$ est accepté par un $p$-groupe. Comme les langages acceptés par des groupes sont stables par union, intersection et complémentaire, toute combinaison booléenne de tels langages reste acceptée par un $p$-groupe, ce qui nous donne la conclusion.

La condition est nécessaire. Soit $L$ un sous-ensemble de $A^*$ accepté par un $p$-groupe fini. Soit $\mu : A^* \to M_L$ le morphisme syntaxique de $L$, où $M_L$ est le monoïde syntaxique de $L$. Étant donné que $L$ est accepté par un $p$-groupe, le monoïde $M_L$ est lui-même un $p$-groupe. Posons $r = \#A$ et soit $n$ l'indice de nilpotence du $p$-groupe $M_L$. Par la Proposition 2.3.8, le morphisme $\mu$ se factorise sous la forme




où $\tau$ est le morphisme quotient associé à la congruence $\sim_n$. Étant donné que $L = \mu^{-1}(\mu(L))$, on obtient que $L = \tau^{-1}(B)$ avec $B = \psi^{-1}(\mu(L))$. Ainsi, le langage $L$ est une union de classes d'équivalence de la congruence $\sim_n$. Or, par définition de $\sim_n$, deux mots sont équivalents si et seulement s'ils ont les mêmes coefficients binomiaux $\binom{w}{u} \mod p$ pour tout mot $u$ de longueur au plus $n$. Par conséquent, une classe d'équivalence de $\sim_n$ s'écrit comme l'intersection finie

$$\bigcap_{|v| \leq n} L_{v,r_v,p}.$$

Ainsi, une classe est une intersection finie d'ensembles $L_{v,r,p}$. Une union de classes d'équivalences est donc une combinaison booléenne de langage de la forme $L_{v,r,p}$. De cette manière, $L$ appartient à la combinaison booléenne des ensembles $L_{v,r,p}$, ce qui nous donne la conclusion. □

Nous terminons cette section par deux exemples illustrant concrètement le Théorème 2.4.6.

**Exemples 2.4.7.** (*a*) Considérons le langage

$$L = L_{a,1,2} \cap L_{b,1,2},$$

des mots $u \in \{a,b\}^*$ où le nombre de $a$ est impair et le nombre de $b$ est impair. Étant donné que $L$ est obtenu à partir des ensembles $L_{a,1,2}$ et $L_{b,1,2}$ par intersection, pour illustrer le Théorème 2.4.6, montrons que le langage $L$ est régulier et accepté par un 2-groupe.
Le langage est accepté par l'automate fini déterministe représenté à la Figure 2.6.

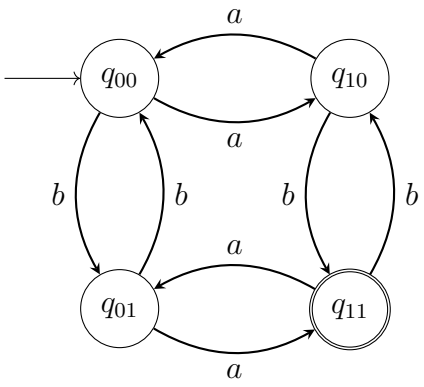



FIGURE 2.6 – Automate minimal du langage $L_{a,1,2} \cap L_{b,1,2}$.

Montrons que le langage $L$ est accepté par un 2-groupe. Considérons le groupe $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Il s'agit bien d'un 2-groupe. En effet, son cardinal est $4 = 2^2$. Définissons l'application

$$\varphi : \{a,b\}^* \to \mathbb{Z}_2 \times \mathbb{Z}_2,\ w \mapsto \left( \binom{w}{a} \mod 2, \binom{w}{b} \mod 2 \right).$$

Montrons que $\varphi$ est un morphisme de monoïdes. En effet, si $u, v \in A^*$, on a

$$\begin{aligned}
\varphi(uv) &= \left( \binom{uv}{a} \mod 2, \binom{uv}{b} \mod 2 \right) \\
&= \left( \binom{u}{a} + \binom{v}{a} \mod 2, \binom{u}{b} + \binom{v}{b} \mod 2 \right) \\
&= \left( \binom{u}{a} \mod 2, \binom{u}{b} \mod 2 \right) + \left( \binom{v}{a} \mod 2, \binom{v}{b} \mod 2 \right) \\
&= \varphi(u) + \varphi(v).
\end{aligned}$$

On remarque également qu'un mot $w$ appartient au langage $L$ si et seulement si $\varphi(w) = (1,1)$. Par conséquent, on a $L = \varphi^{-1}(\{(1,1)\})$. De cette manière, le langage $L$ est l'image réciproque d'un sous-ensemble de $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. On en conclut que le langage $L$ est accepté par le 2-groupe $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(*b*) Considérons à présent le langage

$$L' = L_{ab,1,2} \cup L_{b,1,2}$$

des mots $u \in \{a,b\}^*$ où le nombre d'occurrences du sous-mot $ab$ est impair ou le nombre de $b$ est impair. Étant donné que $L'$ est obtenu par union et complémentaire des ensembles $L_{ab,1,2}$ et $L_{b,1,2}$, pour illustrer le Théorème 2.4.6, montrons que le langage $L'$ est régulier et accepté par un 2-groupe.
Montrons que le langage $L'$ est régulier. Cela résulte du fait que ce langage est accepté par l'automate fini déterministe représenté à la Figure 2.7.

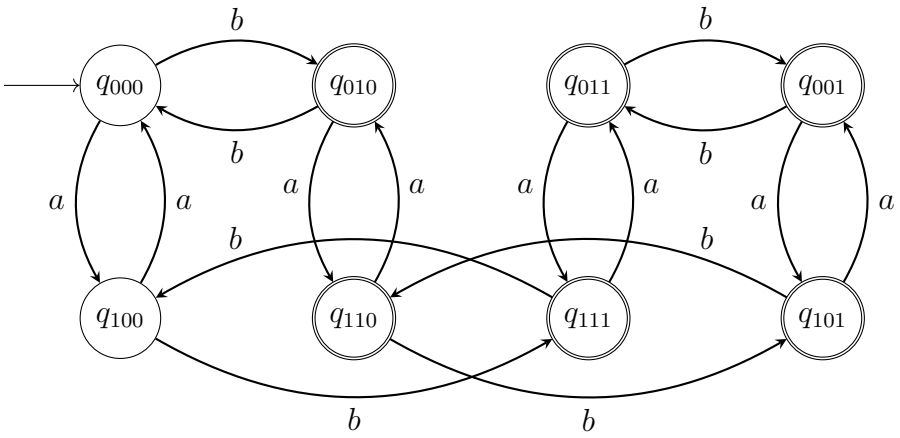



FIGURE 2.7 – Automate minimal du langage $L_{ab,1,2} \cup L_{b,1,2}$.

Montrons que le langage $L'$ est accepté par un 2-groupe. Considérons le groupe $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Il s'agit bien d'un 2-groupe. En effet, son cardinal est $8 = 2^3$. Définissons l'application

$$\varphi : \{a,b\}^* \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ w \mapsto \left( \binom{w}{a} \mod 2, \binom{w}{b} \mod 2, \binom{w}{ab} \mod 2 \right).$$

De la même manière que ci-dessus, on peut montrer que l'application $\varphi$ est un morphisme de monoïdes. On remarque également qu'un mot $w$ appartient au langage $L'$ si et seulement si

$$\varphi(w) \in \{(0,1,0),(0,1,1),(0,0,1),(1,0,1),(1,1,0),(1,1,1)\}.$$

Par conséquent, on a $L' = \varphi^{-1}(\{(0,1,0),(0,1,1),(0,0,1),(1,0,1),(1,1,0),(1,1,1)\})$. De cette manière, le langage $L'$ est l'image réciproque d'un sous-ensemble de $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. On en conclut que le langage $L'$ est accepté par le 2-groupe $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

# Chapitre 3

# Déformations de coefficients binomiaux de mots

Nous nous intéressons ici à une généralisation des coefficients binomiaux de mots sur un alphabet fini $A$. Étant donné deux mots $u, v \in A^*$, on définit une $q$-déformation du coefficient binomial de mots $\binom{u}{v}$, qui compte les sous-suites de $u$ égales à $v$, en enrichissant chaque occurrence par une contribution en puissance de $q$. L'objectif principal de cette construction est d'obtenir une information supplémentaire liée à la position des lettres dans les occurrences de $v$ dans $u$. Ainsi, la $q$-déformation, qui est notée $\binom{u}{v}_q$, ne se contente pas de compter les occurrences de $v$ dans $u$, mais encode également une statistique combinatoire à travers les puissances de $q$. La définition de ces coefficients repose sur une construction récursive, où chaque lettre ajoutée dans les mots modifie le polynôme selon une règle dépendant de la longueur des sous-mots considérés et du fait que les lettres soient les mêmes ou non. Cette récursion permet de construire un arbre de calcul où chaque branche correspond à un choix d'occurrence de $v$ dans $u$, pondéré par une puissance de $q$. Cette structure reflète une combinatoire enrichie, où les chemins dans l'arbre correspondent aux sous-suites possibles.

L'intérêt de ces $q$-déformations ne se limite pas à la combinatoire. Elles jouent également un rôle central dans l'étude de structures algébriques finies, notamment les $p$-groupes et les langages formels associés. En particulier, lorsqu'on considère ces polynômes modulo un polynôme $\mathfrak{M} \in \mathbb{Z}_p[q]$, on obtient une structure algébrique finie. Nous définissons des langages du type

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* : \binom{u}{v}_q \equiv \mathfrak{R} \mod \mathfrak{M} \right\},$$

qui relient directement la combinatoire des mots à la théorie des groupes finis. L'étude des $q$-déformations de coefficients binomiaux de mots permet ainsi de faire le lien entre la combinatoire des mots, l'arithmétique modulaire sur les polynômes et la théorie des $p$-groupes. Elle fournit un cadre où des propriétés combinatoires se traduisent en propriétés algébriques et où des congruences de polynômes contrôlent des langages formels.

Nous commençons donc avec la définition récursive des $q$-déformations de coefficients

binomiaux de mots. Nous étudions d'abord quelques propriétés les concernant, notamment sur le degré des polynômes obtenus. Ensuite, une interprétation combinatoire permet d'obtenir un point de vue différent sur ceux-ci et permet de les calculer de manière plus directe. Une fois cela fait, nous nous intéressons à quelques analogues de formules classiques de combinatoire. Nous procédons à une application concrète de ces $q$-déformations, à savoir la généralisation du théorème d'Eilenberg. Tout comme dans le Chapitre 2, nous avons un ordre logique permettant d'aboutir au théorème d'Eilenberg généralisé stipulant qu'un langage $L$ sur $A$ est accepté par un $p$-groupe si et seulement si $L$ est une combinaison booléenne de langages de la forme

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* : \binom{u}{v}_q \equiv \mathfrak{R} \mod \mathfrak{M} \right\},$$

où $\mathfrak{M}(q) = a(q-1)^d$ pour $a \in \mathbb{Z}_p^*$, $d \geq 1$ et $\mathfrak{R} \in \mathbb{Z}_p[q]$ est tel que $\deg(\mathfrak{R}) < \deg(\mathfrak{M})$.

L'ensemble de ce chapitre est basé sur l'article *Introducing q-déformed binomial coefficients of words* de Antoine Renard, Michel Rigo et Markus Whiteland [12]. Le lecteur intéressé pourra également trouver aux sources [9, 10, 11] des fichiers permettant d'avoir une vue globale sur la matière et permettant de résumer le tout.

## 3.1 Premières définitions et exemples

Nous nous intéressons à présent à définir des $q$-déformations de coefficients binomiaux de mots. L'objectif est donc de définir un polynôme dans $\mathbb{N}[q]$ qui généralise ce coefficient, de telle sorte que l'on retrouve le cas classique en évaluant $q = 1$. Nous en profitons également pour donner plusieurs exemples pour illustrer les propos. Pour ce faire, nous allons utiliser la Proposition 1.3.9 qui tient pour les coefficients binomiaux de mots pour définir ce nouvel objet : pour tous mots $u, v \in A^*$ et toutes lettres $a, b \in A$, on a

$$\binom{ua}{vb} = \binom{u}{vb} + \delta_{a,b} \cdot \binom{u}{v}.$$

**Définition 3.1.1.** Soient $u, v \in A^*$. On définit récursivement la *$q$-déformation du coefficient binomial* $\binom{u}{v}$ sur $A^* \times A^*$, notée $\binom{u}{v}_q$, qui est un élément de $\mathbb{N}[q]$, de la manière suivante. Pour tous mots $u, v \in A^*$ et toutes lettres $a, b \in A$,

$$\binom{u}{\varepsilon}_q = 1,$$

$$\binom{\varepsilon}{v}_q = 0 \text{ si } v \neq \varepsilon$$

et

$$\binom{ua}{vb}_q = \binom{u}{vb}_q \cdot q^{|vb|} + \delta_{a,b} \cdot \binom{u}{v}_q. \tag{3.1}$$

**Remarque 3.1.2.** Il est à noter que, en prenant $q = 1$, on retombe sur la Proposition 1.3.9.

Comme nous pourrons le remarquer à la section 3.3, cette définition permet d'obtenir des propriétés qui sont analogues à celles que nous connaissons déjà dans le cas des coefficients binomiaux de mots classiques. Cette définition étant introduite à l'aide d'une propriété elle-même déjà établie, il est naturel de travailler avec cette dernière.

Nous donnons un exemple de $q$-déformation.

**Exemple 3.1.3.** Soient $A = \{a, b\}$ et $u = aaabbb, v = ab \in A^*$. En utilisant la définition précédente, on obtient que

$$\begin{aligned}
\binom{aaabbb}{ab}_q =& \binom{aaabb}{ab}_q \cdot q^2 + \delta_{b,b} \cdot \binom{aaabb}{a}_q \\
=& \binom{aaab}{ab}_q \cdot q^2 \cdot q^2 + \delta_{b,b} \cdot \binom{aaab}{a}_q \cdot q^2 + \binom{aaab}{a}_q \cdot q + \underbrace{\delta_{b,a}}_{=0} \cdot \binom{aaab}{\varepsilon}_q \\
=& \binom{aaa}{ab}_q \cdot q^2 \cdot q^4 + \delta_{b,b} \cdot \binom{aaa}{a}_q \cdot q^4 + \binom{aaa}{a}_q \cdot q \cdot q^2 + \underbrace{\delta_{b,a}}_{=0} \binom{aaa}{\varepsilon}_q + \binom{aaa}{a}_q \cdot q \cdot q \\
&+ \underbrace{\delta_{b,a}}_{=0} \cdot \binom{aaa}{\varepsilon}_q \cdot q \\
=& \binom{aa}{ab}_q \cdot q^2 \cdot q^6 + \underbrace{\delta_{a,b}}_{=0} \cdot \binom{aa}{a}_q \cdot q^6 + \binom{aa}{a}_q \cdot q \cdot q^4 + \underbrace{\delta_{a,a} \binom{aa}{\varepsilon}_q}_{=1} \cdot q^4 + \binom{aa}{a}_q \cdot q \cdot q^3 \\
&+ \underbrace{\delta_{a,a} \cdot \binom{aa}{\varepsilon}_q}_{=1} \cdot q^3 + \binom{aa}{a}_q \cdot q \cdot q^2 + \underbrace{\delta_{a,a} \cdot \binom{aa}{\varepsilon}_q}_{=1} \cdot q^2 \\
=& \underbrace{\binom{a}{ab}_q}_{=0} \cdot q^2 \cdot q^8 + \underbrace{\delta_{a,b}}_{=0} \cdot \binom{a}{a}_q \cdot q^8 + \underbrace{\binom{a}{a}_q}_{=1} \cdot q \cdot q^5 + \underbrace{\delta_{a,a} \cdot \binom{a}{\varepsilon}_q}_{=1} \cdot q^5 + q^4 + \underbrace{\binom{a}{a}_q}_{=1} \cdot q \cdot q^4 \\
&+ \underbrace{\delta_{a,a} \cdot \binom{a}{\varepsilon}_q}_{=1} \cdot q^4 + q^3 + \underbrace{\binom{a}{a}_q}_{=1} \cdot q \cdot q^3 + \underbrace{\delta_{a,a} \cdot \binom{a}{\varepsilon}_q}_{=1} \cdot q^3 + q^2 \\
=& q^6 + q^5 + q^4 + q^5 + q^4 + q^3 + q^4 + q^3 + q^2 \\
=& q^6 + 2q^5 + 3q^4 + 2q^3 + q^2.
\end{aligned}$$

Un programme effectué sur Python permettant de calculer n'importe quelle $q$-déformation à partir des entrées $u$ et $v$ est donné à la Figure 3.1.

```
import sympy as sp

q = sp.Symbol('q')

def qbin(u, v):
    if not v:
        return sp.Integer(1)
    if not u:
        return sp.Integer(0)

    u_prime, a = u[:-1], u[-1]
    v_prime, b = v[:-1], v[-1]
    terme_1 = qbin(u_prime, v)*(q**len(v))

    if a == b:
        terme_2 = qbin(u_prime, v_prime)
    else:
        terme_2 = sp.Integer(0)
    return sp.expand(terme_1 + terme_2)
```

FIGURE 3.1 – Programme permettant de calculer une $q$-déformation de coefficients binomiaux de mots.

**Remarque 3.1.4.** Soient $k$ et $l$ deux naturels. Si $A$ est un alphabet unaire, alors on a

$$\binom{a^k}{a^l}_q = \binom{k}{l}_q.$$

En effet, en prenant $u = a^k$ et $v = a^l$ et en utilisant la définition, on a

$$\binom{a^{k+1}}{a^{l+1}}_q = \binom{a^k}{a^{l+1}}_q \cdot q^{l+1} + \binom{a^k}{a^l}_q.$$

Or, par définition, les coefficients binomiaux Gaussiens vérifient

$$\binom{k+1}{l+1}_q = \binom{k}{l+1}_q \cdot q^{l+1} + \binom{k}{l}_q. \tag{3.2}$$

Enfin, étant donné que

$$\binom{a^k}{\varepsilon}_q = 1, \quad \binom{a^k}{a^k}_q = 1,$$
$$\binom{k}{0}_q = 1 \quad \text{et} \quad \binom{k}{k}_q = 1,$$

les deux familles satisfont la même relation de récurrence, ce qui nous donne que

$$\binom{a^k}{a^l}_q = \binom{k}{l}_q.$$

Il existe également des conditions sur les longueurs des mots $u$ et $v$.

**Remarque 3.1.5.** Soient $u, v \in A^*$. Si $|u| < |v|$, alors on a

$$\binom{u}{v}_q = 0.$$

Cela résulte directement du fait que, dans la définition, on a que $\binom{\varepsilon}{v}_q = 0$ si $v \neq \varepsilon$. De plus, si $|u| = |v|$, alors on a

$$\binom{u}{v}_q = 0 \iff u \neq v.$$

Enfin, on a

$$\binom{u}{u}_q = 1$$

pour tout mot $u \in A^*$.

On en déduit le lemme suivant.

**Lemme 3.1.6.** *Soient $u, v \in A^*$. Dans ce cas, $\binom{u}{v}_q$ est le polynôme nul si et seulement si $v$ n'apparaît pas comme sous-mot de $u$.*

**Remarque 3.1.7.** Dans le choix de définition, nous avons décidé de nous intéresser aux lettres qui se trouvent à la droite de $u$ et de $v$. Nous aurions évidemment pu adopter une définition différente qui s'intéresse aux lettres qui se trouvent à gauche de $u$ et de $v$ :

$$\binom{au}{bv}_q = \binom{u}{bv}_q \cdot q^{|bv|} + \delta_{a,b} \cdot \binom{u}{v}_q.$$

Ce choix de définition mène à un autre polynôme avec des propriétés similaires. Par exemple, en prenant les mots $u = ababbab$ et $v = ba$, la $q$-déformation en utilisant la première définition est $q^8 + q^5 + q^3 + q^2$ et la $q$-déformation en utilisant la définition ci-dessus est $q^8 + q^7 + q^5 + q^2$.

En utilisant notre définition, un arbre de transitions peut être construit.

**Exemple 3.1.8.** Soient $A = \{a, b\}$ et $u = aaabbb, v = ab \in A^*$. En appliquant la première définition, on obtient que

$$\binom{aaabbb}{ab}_q = q^6 + 2q^5 + 3q^4 + 2q^3 + q^2.$$

L'arbre menant à cette égalité est explicité à la Figure 3.2. Si un sommet a deux enfants, ils correspondent aux deux termes du membre de droite dans la relation (3.1).

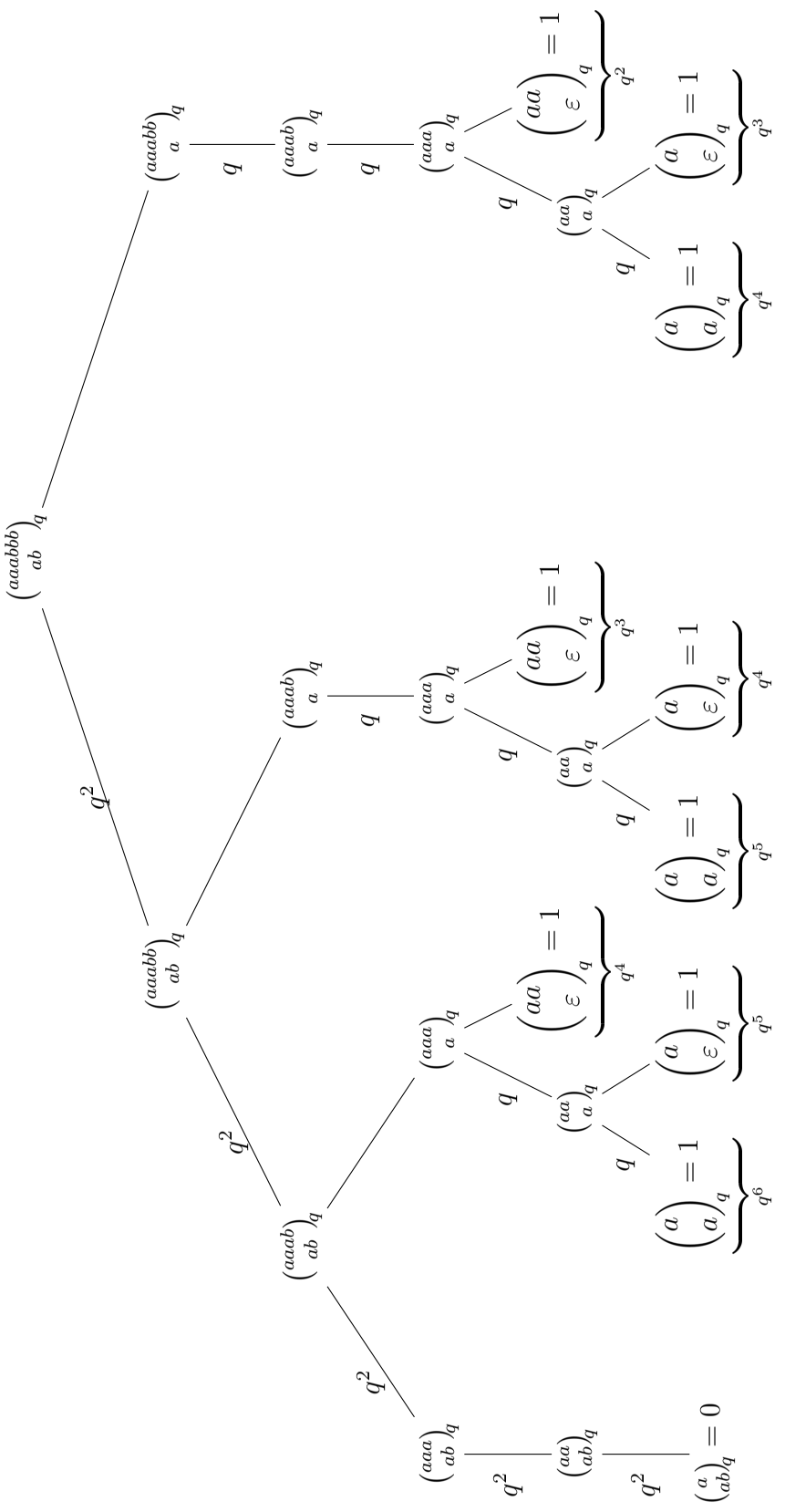



FIGURE 3.2 – Application récursive de la Définition 3.1.1 pour la $q$-déformation $\binom{aaabbb}{ab}_q$.

Dans ce cas, la multiplication par la puissance de la variable $q$ est l'étiquette de l'arrête de gauche. Si un sommet a un seul fils, cela veut dire que les deux dernières lettres sont identiques. Les accolades sur les feuilles sont obtenues en multipliant l'étiquette de chaque arrête jusqu'à la racine. Il est à noter que, en évaluant ce polynôme en $q = 1$, on retombe sur le fait que

$$\binom{aaabbb}{ab} = 9.$$

Nous introduisons à présent une notation nous permettant d'énoncer quelques résultats préliminaires sur les coefficients et les degrés des déformations de coefficients binomiaux de mots.

**Notation 3.1.9.** Si $P(q) = \sum_{i=0}^{d} c_i q^i$ est un polynôme en la variable $q$, on notera $P[q^m]$ le coefficient $c_m$ pour tout $m \in \{0, \dots, d\}$.

**Lemme 3.1.10.** *Soient $u, v \in A^*$. Les coefficients de la q-déformation $\binom{u}{v}_q$ sont bornés par les coefficients du coefficient Gaussien correspondant, c'est-à-dire*

$$\binom{u}{v}_q [q^m] \leq \binom{|u|}{|v|}_q [q^m].$$

*Démonstration.* Considérons le morphisme $\varphi : A^* \to \{\sigma\}^*$ qui encode toutes les lettres de $A$ sur une seule lettre $\sigma$. En appliquant la relation (3.1) avec les mots $u$ et $v$ d'un côté et avec les lettres $\varphi(u)$ et $\varphi(v)$ de l'autre, on remarque que toutes les branches ne menant pas à une configuration nulle dans l'arbre (comme dans la Figure 3.2) pour les mots $u$ et $v$ apparaissent également en considérant les lettres $\varphi(u)$ et $\varphi(v)$. De plus, sur un alphabet unaire, l'arbre peut éventuellement avoir plus de branches ne menant pas à une configuration nulle. En effet, $\delta_{a,b}$ peut être nul si l'alphabet $A$ est de taille plus grande ou égale à 2. Cependant, $\delta_{\varphi(a),\varphi(b)} = 1$ pour toutes les lettres $a, b \in A$, ce qui explique l'inégalité. □

Dans le Lemme 3.1.12, nous comparons le degré des deux termes apparaissant dans le membre de droite de la relation (3.1). Pour s'intéresser à celui-ci, nous procédons à un premier lemme.

**Lemme 3.1.11.** *Soit $u \in A^*$. Pour toute lettre $a \in A$, on a*

$$\deg \binom{ua}{u}_q = |u|.$$

*Démonstration.* Procédons par récurrence sur la longueur de $u$.

- Supposons que $u = \varepsilon$. Étant donné que $\varepsilon$ est de longueur nulle et que $\binom{a}{\varepsilon}_q = 1$ par définition, on a

  $$\deg \binom{a}{\varepsilon}_q = |\varepsilon|,$$

  ce qui nous donne la conclusion dans ce cas.

► Supposons à présent que

$$\deg \binom{va}{v}_q = |v|$$

pour tout mot $v \in A^{\leq n}$ et tout $a \in A$ et montrons que le résultat est satisfait pour tout mot de longueur $n+1$. Écrivons $u = vb$ où $v \in A^n$ et $b \in A$. Dans ce cas, par définition et en utilisant l'hypothèse de récurrence, on a

$$\begin{aligned}
\deg \binom{ua}{u}_q &= \deg \binom{vba}{vb}_q \\
&= \deg \left( \binom{vb}{vb}_q \cdot q^{|vb|} + \delta_{a,b} \cdot \binom{vb}{v}_q \right) \\
&= \max \{ |vb|, \delta_{a,b} \cdot |v| \} \\
&= \max \{ |u|, \delta_{a,b} \cdot (|u| - 1) \} \\
&= |u|,
\end{aligned}$$

ce qui nous donne la conclusion.

□

**Lemme 3.1.12.** *Soient $u, v \in A^*$ et $a \in A$. Si le coefficient binomial $\binom{u}{va}$ est non nul, alors*

$$\deg \left( \binom{u}{va}_q \cdot q^{|va|} \right) > \deg \binom{u}{v}_q.$$

*Démonstration.* Supposons que $v = \varepsilon$. Étant donné que $\binom{u}{\varepsilon}_q = 1$ et que $\binom{u}{a}_q \neq 0$ par hypothèse, on a

$$\deg \left( \binom{u}{a}_q \cdot q^{|a|} \right) > \deg \binom{u}{\varepsilon}_q,$$

ce qui nous donne la conclusion dans ce cas. Supposons à présent que $v \neq \varepsilon$. Étant donné que $\binom{u}{va}_q \neq 0$ par hypothèse, on sait par la Remarque 3.1.5 que $|u| \geq |va|$. Procédons par récurrence sur la longueur de $u$. Tout d'abord, supposons que $|u| = |va|$. Dans ce cas, on a $u = va$. Cela résulte du fait que, par la Remarque 3.1.5, si $|u| = |v|$, alors on a $\binom{u}{v}_q \neq 0$ si et seulement si $u = v$. En utilisant le Lemme 3.1.11, on a

$$\begin{aligned}
\deg \left( \binom{u}{va}_q \cdot q^{|va|} \right) &= \deg \binom{va}{va}_q + |va| \\
&> |v| \\
&= \deg \binom{va}{v}_q \\
&= \deg \binom{u}{v}_q,
\end{aligned}$$

ce qui nous donne la conclusion pour le cas de base. Soit $u \in A^*$ un mot tel que $|u| > |va|$. Dans ce cas, on peut noter $u = u'b$ où $u' \in A^*$ est un mot tel que $|u'| \geq |va|$ et où $b \in A$. Dans ce cas, remarquons que

$$\begin{aligned}\deg \binom{u}{va}_q &= \deg \binom{u'b}{va}_q \\ &= \deg \left( \binom{u'}{va}_q \cdot q^{|va|} + \delta_{a,b} \cdot \binom{u'}{v}_q \right).\end{aligned}$$

Montrons à présent que

$$\deg \binom{u}{va}_q + |va| \geq \deg \binom{u'}{v}_q + |va| \geq |va|. \tag{3.3}$$

Pour la deuxième des inégalités, cela résulte du fait que $\binom{u}{va}_q \neq 0$ implique que $\binom{u'}{v}_q \neq 0$. En ce qui concerne la première inégalité, pour qu'elle ne soit pas vérifiée, il faudrait que $\delta_{a,b} = 0$. Cependant, cela impliquerait

$$0 \neq \binom{u}{va}_q = \binom{u'}{va}_q \cdot q^{|va|}$$

dont le degré est donné par

$$\deg \binom{u'}{va}_q + |va| \geq 0.$$

Par hypothèse de récurrence, cette valeur est strictement plus grande que $\deg\left(\binom{u'}{v}_q\right)$. Par conséquent, on a la première inégalité. En utilisant la relation (3.3), on a

$$\begin{aligned}\deg \left( \binom{u}{va}_q \cdot q^{|va|} \right) &\geq \deg \binom{u'}{v}_q + |va| \\ &> \deg \left( \binom{u'}{v}_q \cdot q^{|v|} \right) \\ &= \deg \binom{u}{v}_q.\end{aligned}$$

La dernière égalité résulte du fait que, étant donné que $v \neq \varepsilon$, on peut écrire $v = v'c$ où $c \in A$ et $v' \in A^*$ est un mot tel que $|v'| < |v|$. Cela nous donne par définition que

$$\deg \binom{u}{v}_q = \deg \left( \binom{u'}{v}_q \cdot q^{|v|} + \delta_{b,c} \cdot \binom{u'}{v'}_q \right).$$

Comme montré précédemment, on sait que $\binom{u'}{v}_q \neq 0$. Ainsi, par hypothèse de récurrence, on a

$$\deg \left( \binom{u'}{v}_q \cdot q^{|v|} \right) > \deg \binom{u'}{v'}_q,$$

ce qui nous donne la conclusion. □

Dans la relation (3.1), le degré du terme de gauche est donc toujours strictement supérieur au degré du terme de droite.

**Exemple 3.1.13.** Soient $A = \{a, b\}$ et $u = aaabbb, v = ab \in A^*$. Par définition, on sait que

$$\binom{aaabbb}{ab}_q = \binom{aaabb}{ab}_q \cdot q^2 + \binom{aaabb}{a}_q.$$

Par le Lemme 3.1.12, le degré du terme de gauche est supérieur au degré du terme de droite. Ainsi, pour connaître le degré de $\binom{aaabbb}{ab}_q$, il suffit d'étudier le degré de $\binom{aaabb}{ab}_q \cdot q^2$. Le fait que le degré du terme de gauche est strictement supérieur au degré du terme de droite est également illustré à la Figure 3.2.

Le Lemme 3.1.12 permet de calculer de manière récursive le degré d'une $q$-déformation.

**Corollaire 3.1.14.** *Soient $u, v, x \in A^*$ et $a \in A$. Le degré de la $q$-déformation d'un coefficient binomial non nul est obtenu récursivement par*

$$\deg \binom{uax}{va}_q = |va| \cdot |x| + \deg \binom{u}{v}_q,$$

*où $ua$ est le préfixe le plus court de $uax$ dans lequel $va$ apparaît.*

*Démonstration.* Si $x = \varepsilon$, alors on a

$$\binom{ua}{va}_q = \binom{u}{va}_q \cdot q^{|va|} + \delta_{a,b} \cdot \binom{u}{v}_q = \binom{u}{v}_q.$$

Cela résulte du fait que, étant donné que $ua$ est le préfixe le plus court de $ua$ dans lequel $va$ apparaît, on sait que $va$ n'apparaît pas dans $u$. Ainsi, on a

$$\begin{aligned} \deg \binom{ua}{va}_q &= \deg \binom{u}{v}_q \\ &= |va| \cdot |\varepsilon| + \deg \left( \binom{u}{v}_q \right). \end{aligned} \tag{3.4}$$

Supposons à présent que $|x| \geq 1$. Dans ce cas, on peut écrire $x = x'c$ où $x' \in A^*$ est tel que $|x'| < |x|$ et où $c \in A$. En utilisant la définition, on a

$$\binom{uax}{va}_q = \binom{uax'c}{va}_q = \binom{uax'}{va}_q \cdot q^{|va|} + \delta_{a,c} \cdot \binom{uax'}{v}_q.$$

Étant donné que $va$ apparaît dans $ua$, on sait que $\binom{uax'}{va}_q \neq 0$. Par le Lemme 3.1.12, on obtient que

$$\deg \binom{uax}{va}_q = \deg \binom{uax'}{va}_q + |va|.$$

En réitérant cet argument, on obtient finalement que

$$\deg \binom{uax}{va}_q = \deg \binom{ua}{va}_q + |x| \cdot |va|.$$

On obtient la conclusion par la relation (3.4). □

**Exemple 3.1.15.** Soient $A = \{a, b\}$ et $u = aaabbb, v = ab \in A^*$. Dans ce cas, par le Corollaire 3.1.14, on a

$$\begin{aligned}\deg \binom{\underline{aaa}bbb}{ab}_q &= 2 \cdot 2 + \deg \binom{\underline{a}aa}{a}_q \\ &= 4 + 2 \cdot 1 + \underbrace{\deg \binom{\varepsilon}{\varepsilon}_q}_{=0} \\ &= 6,\end{aligned}$$

où les mots soulignés sont les plus courts préfixes $ua$ que nous considérons.

Pour finir cette section, nous donnons ce dernier corollaire.

**Corollaire 3.1.16.** *Soit $v = a_k \cdots a_1 \in A^*$ avec $a_i \in A$ pour tout $i \in \{1, \ldots, k\}$. Si $u = u_k a_k u_{k-1} \cdots u_1 a_1 u_0$, avec $u_i \in A^*$ pour tout $i \in \{0, \ldots, k\}$, où $u_k a_k \cdots u_j a_j$ est le préfixe le plus court de $u$ dans lequel $a_k \cdots a_j$ apparaît pour tout $j \in \{1, \ldots, k\}$, alors*

$$\deg \binom{u}{v}_q = \sum_{r=0}^{k-1} (k - r) \cdot |u_r|.$$

*Démonstration.* Étant donné que $u_k a_k \cdots u_1 a_1$ est le préfixe le plus court de $u_k a_k u_{k-1} \cdots u_1 a_1 u_0$ dans lequel $a_k \cdots a_1$ apparaît, on obtient par le Corollaire 3.1.14 que

$$\begin{aligned}\deg \binom{u}{v}_q &= \deg \binom{u_k a_k u_{k-1} \cdots u_1 a_1 u_0}{a_k \cdots a_1}_q \\ &= k \cdot |u_0| + \deg \binom{u_k a_k u_{k-1} \cdots a_2 u_1}{a_k \cdots a_2}_q.\end{aligned}$$

En itérant cet argument, on obtient finalement que

$$\begin{aligned}\deg \binom{u}{v}_q &= k \cdot |u_0| + (k-1) \cdot |u_1| + (k-2) \cdot |u_2| + \cdots + 1 \cdot |u_{k-1}| \\ &= \sum_{r=0}^{k-1} (k - r) \cdot |u_r|,\end{aligned}$$

ce qui nous donne la conclusion. □

## 3.2 Interprétation combinatoire

Nous nous intéressons à une interprétation combinatoire des $q$-déformations. L'exposant apparaissant dans une $q$-déformation apporte plus d'informations que les coefficients binomiaux de mots classiques. Toute occurrence de $v$ comme sous-mot de $u$ contribue à un terme de la forme $q^j$, où l'exposant $j$ est obtenu, à une constante additive près dépendant de $|v|$ – appelée *constante de normalisation* – comme la somme des indices des positions auxquelles les lettres de $v$ apparaissent dans $u$.

**Théorème 3.2.1.** *Soient $u = u_n \cdots u_1, v = v_k \cdots v_1 \in A^*$ avec $u_i \in A$ pour tout $i \in \{1, \ldots, n\}$ et $v_j \in A$ pour tout $j \in \{1, \ldots, k\}$. On a*

$$\binom{u}{v}_q = \sum_{Y \in A_{n,k}} q^{s(Y) - \frac{k(k+1)}{2}},$$

*où*

$$A_{n,k} = \{n \geq y_k > \cdots > y_1 \geq 1 : u_{y_k} \cdots u_{y_1} = v\}$$

*et pour tout $Y \in A_{n,k}$, on a*[1] $s(Y) := \sum_{y \in Y} y$.

*Démonstration.* Procédons par récurrence sur $n = |u|$ et sur $k = |v|$.

- ◇ Si $n = 1$, alors $u = a \in A$. Étant donné que $\binom{u}{v}_q = 0$ si $|u| < |v|$ par la Remarque 3.1.5, il suffit de considérer deux cas, celui où $k = 0$ et celui où $k = 1$.
  - ▶ Si $k = 0$, alors $v = \varepsilon$. Par définition, on a $\binom{a}{\varepsilon}_q = 1$. De plus, on sait que $Y = \emptyset$ est le seul sous-ensemble de $A_{1,0}$. De plus, on a $s(\emptyset) = 0$. Ainsi, on a

    $$\sum_{Y \in A_{1,0}} q^{s(Y) - \frac{k(k+1)}{2}} = q^{s(\emptyset) - \frac{0 \cdot 1}{2}} = 1,$$

    ce qui nous donne la conclusion dans ce cas.
  - ▶ Si $k = 1$, alors $v = b \in A$. Dans ce cas, étant donné que si $|u| = |v|$, alors $\binom{u}{v}_q = 0$ si et seulement si $u \neq v$ par la Remarque 3.1.5, on a $\binom{a}{b}_q = \delta_{a,b}$.
    - ○ Si $a \neq b$, alors $\binom{a}{b}_q = 0$. De plus, l'ensemble $A_{1,1}$ est vide. De cette manière, on a

      $$\sum_{Y \in A_{1,1}} q^{s(Y) - \frac{1 \cdot 2}{2}} = 0.$$

    - ○ Si $a = b$, alors $\binom{a}{b}_q = 1$. De plus, l'ensemble $A_{1,1}$ contient uniquement $Y = \{1\}$. Pour cet ensemble, on a $s(Y) = 1$, ce qui nous donne que

      $$\sum_{Y \in A_{1,1}} q^{s(Y) - \frac{k(k+1)}{2}} = q^{1 - \frac{1 \cdot 2}{2}} = 1.$$

1. Étant donné que la somme s'effectue sur tous les éléments de $Y$, notés $y_1, \ldots, y_k$, on peut également écrire $s(Y) = \sum_{i=1}^{k} y_i$.

Dans les deux cas, l'égalité est vérifiée.

◇ Supposons à présent que le résultat soit vérifié pour $m \in \{1, \dots, n-1\}$, avec $n \geq 2$, et montrons que le résultat est vérifié pour $n$.

▶ Si $k = 0$, alors le même raisonnement que précédemment permet de conclure. En effet, on sait par définition que $\binom{u}{\varepsilon}_q = 1$. De plus, $Y = \emptyset$ est le seul sous-ensemble de $A_{n,0}$, ce qui nous donne que

$$\sum_{Y \in A_{n,0}} q^{s(Y) - \frac{k(k+1)}{2}} = q^{s(\emptyset) - \frac{0 \cdot 1}{2}} = 1.$$

On a donc bien l'égalité dans ce cas.

▶ Soit $k \geq 1$ et posons $A_{n,k} = B \cup B'$, où

$$B = \{Y \in A_{n,k} : y_1 \neq 1\}$$

et

$$B' = \{Y \in A_{n,k} : y_1 = 1\}.$$

Ces deux ensembles forment une partition de $A_{n,k}$.

Si $Y \in B$, alors on sait que $Y \subseteq \{2, \dots, n\}$. Remarquons que l'ensemble $Y'$ défini par $Y' := Y - 1 := \{y - 1 : y \in Y\}$ est tel que $Y' \subseteq \{1, \dots, n-1\}$. De cette manière, on a $Y' \in A_{n-1,k}$. De plus, on a

$$s(Y') = \sum_{i=1}^{k} y'_i = \sum_{i=1}^{k} (y_i - 1) = s(Y) - k.$$

On obtient donc que $s(Y) = s(Y') + k$.

Si $Y \in B'$, alors on sait que $Y = Z \cup \{1\}$, où $Z$ est un ensemble tel que $Z \subseteq \{2, \dots, n\}$. Remarquons que l'ensemble $Z'$ défini par $Z' := Z - 1$ est tel que $Z' \subseteq \{1, \dots, n-1\}$ et est donc tel que $Z' \in A_{n-1,k-1}$. De cette manière, on a

$$s(Z') = \sum_{i=1}^{k-1} z'_i = \sum_{i=1}^{k-1} (z_i - 1) = s(Z) - k + 1.$$

Ainsi, on a

$$s(Y) = s(Z \cup \{1\}) = s(Z) + 1 = s(Z') + k.$$

Par définition de $A_{n,k}$, on sait que $B' \neq \emptyset$ si et seulement si $u_1 = v_1$. On en tire que

$$\begin{aligned}
\sum_{Y \in A_{n,k}} q^{s(Y) - \frac{k(k+1)}{2}} &= \sum_{Y \in B} q^{s(Y) - \frac{k(k+1)}{2}} + \delta_{u_1,v_1} \sum_{Y \in B'} q^{s(Y) - \frac{k(k+1)}{2}} \\
&= \sum_{Y' \in A_{n-1,k}} q^{s(Y') + k - \frac{k(k+1)}{2}} + \delta_{u_1,v_1} \sum_{Z' \in A_{n-1,k-1}} q^{s(Z') + k - \frac{k(k+1)}{2}} \\
&= q^k \sum_{Y' \in A_{n-1,k}} q^{s(Y') - \frac{k(k+1)}{2}} + \delta_{u_1,v_1} \sum_{Z' \in A_{n-1,k-1}} q^{s(Z') - \frac{k(k-1)}{2}}.
\end{aligned}$$

En appliquant l'hypothèse de récurrence, on obtient finalement que

$$\sum_{Y\in A_{n,k}} q^{s(Y)-\frac{k(k+1)}{2}} = q^k \binom{u_n\cdots u_2}{v}_q + \delta_{u_1,v_1}\binom{u_n\cdots u_2}{v_k\cdots v_2}_q = \binom{u}{v}_q.$$

Ceci nous donne la conclusion de la preuve. □

**Exemple 3.2.2.** Soient $A=\{a,b\}$ et $u=aaabbb, v=ab\in A^*$. Dans ce cas, on a

$$A_{6,2}=\{(6,3),(6,2),(6,1),(5,3),(5,2),(5,1),(4,3),(4,2),(4,1)\}.$$

De plus, en notant $Y_1=(6,3), Y_2=(6,2),\ldots,Y_9=(4,1)$, on a $s(Y_1)=6+3=9, s(Y_2)=6+2=8,\ldots,s(Y_9)=4+1=5$. Enfin, étant donné que $\frac{k(k+1)}{2}=\frac{2\cdot 3}{2}=3$, on obtient finalement par le Théorème 3.2.1 que

$$\begin{aligned}\binom{aaabbb}{ab}_q &= \sum_{Y\in A_{6,2}} q^{s(Y)-3}\\ &= q^{9-3}+q^{8-3}+q^{7-3}+q^{8-3}+q^{7-3}+q^{6-3}+q^{7-3}+q^{6-3}+q^{5-3}\\ &= q^6+2q^5+3q^4+2q^3+q^2.\end{aligned}$$

Il est commode de réécrire le Théorème 3.2.1 de la manière suivante.

**Corollaire 3.2.3.** *Soient $u=u_n\cdots u_1, v=v_k\cdots v_1\in A^*$ avec $u_i\in A$ pour tout $i\in\{1,\ldots,n\}$ et $v_j\in A$ pour tout $j\in\{1,\ldots,k\}$. Si $Y=\{n\geq y_k>\cdots>y_1\geq 1\}\in A_{n,k}$ correspond à une occurrence de $v$ dans $u$, alors cette occurrence contribue à $\binom{u}{v}_q$ avec un terme $q^\alpha$ où*

$$\alpha=\sum_{i=1}^{k} y_i - i,$$

*c'est-à-dire où $\alpha$ est la somme sur toutes les lettres de $v$ du nombre de lettres à leur droite qui ne font pas parties de cette occurrence spécifique du sous-mot $v$. Autrement dit, on a*

$$\binom{u}{v}_q = \sum_{\substack{u_{k+1}v_ku_k\cdots v_1u_1=u\\ u_i\in A^*}} \prod_{i=1}^{k} q^{|u_i\cdots u_1|}.$$

*Démonstration.* Nous montrons la dernière égalité.

Supposons que $v$ n'est pas un sous-mot de $u$. Dans ce cas, on sait par le Lemme 3.1.6 que $\binom{u}{v}_q=0$. De plus, étant donné qu'aucune factorisation de $v$ comme sous-mot de $u$ n'existe, la somme du membre de droite est faite sur le vide et est donc nulle. La formule est donc valide dans ce cas.

Supposons que $v$ est un sous-mot de $u$. Dans ce cas, on sait qu'on peut écrire $u$ sous la forme $u=u_{k+1}v_ku_k\cdots v_1u_1$, où $u_i\in A^*$ pour tout $i\in\{1,\ldots,k+1\}$. Pour calculer la $q$-déformation $\binom{u}{v}_q$, il suffit de faire la somme sur toutes les lettres de $v$ du nombre de

lettres à leur droite qui ne font pas partie de cette occurrence spécifique du sous-mot $v$. À la droite de la lettre $v_1$ se trouvent $|u_1|$ lettres ne faisant pas partie de cette occurrence. À la droite de la lettre $v_2$ se trouvent $|u_2| + |u_1| = |u_2u_1|$ lettres ne faisant pas partie de cette occurrence. En itérant cet argument, on remarque que, pour tout $i \in \{1, \dots, k\}$, à la droite de la lettre $v_i$ se trouvent $|u_i| + |u_{i-1}| + \cdots + |u_1| = |u_i \cdots u_1|$ lettres ne faisant pas partie de cette occurrence. Étant donné que, pour calculer la $q$-déformation $\binom{u}{v}_q$, il faut effectuer la somme sur toutes les factorisations possibles de $v$ comme sous-mot de $u$, on obtient finalement que

$$\binom{u}{v}_q = \sum_{\substack{u_{k+1}v_ku_k\cdots v_1u_1=u \\ u_i\in A^*}} q^{\sum_{i=1}^{k} |u_i\cdots u_1|} = \sum_{\substack{u_{k+1}v_ku_k\cdots v_1u_1=u \\ u_i\in A^*}} \prod_{i=1}^{k} q^{|u_i\cdots u_1|},$$

ce qui nous donne la conclusion. □

Illustrons ce corollaire au travers d'un exemple.

**Exemple 3.2.4.** Soient $A = \{a, b\}$ et $u = aaabbb, v = ab \in A^*$. Considérons l'occurrence rouge de $ab$ dans $aaabbb$. La lettre $a$ est suivie de 2 lettres noires à sa droite et la lettre $b$ est également suivie de 2 lettres noires à sa droite. Cette occurrence contribue donc pour $q^4$. Considérons à présent l'occurrence bleue de $ab$ dans $aaabbb$. La lettre $a$ est suivie de 4 lettres noires à sa droite et la lettre $b$ est suivie de 1 lettre noire à sa droite. Cette occurrence contribue donc pour $q^5$. En utilisant les autres occurrences de $ab$ dans $aaabbb$, on obtient que

$$\binom{aaabbb}{ab}_q = q^6 + 2q^5 + 3q^4 + 2q^3 + q^2.$$

**Corollaire 3.2.5.** *Soient $u, v \in A^*$. Si $\binom{u}{v}$ est non nul, alors le polynôme $\binom{u}{v}_q$ est monique et le coefficient non nul du terme de plus petit degré est égal à 1. En particulier, le terme indépendant de $\binom{u}{v}_q$ est égal à 1 si et seulement si $v$ est un suffixe de $u$ et est égal à 0 sinon. De même, on a*

$$\deg \binom{u}{v}_q \leq |v| \cdot (|u| - |v|).$$

*De plus, le coefficient de $q^{|v|\cdot(|u|-|v|)}$ est égal à 1 si et seulement si $v$ est un préfixe de $u$ et est égal à 0 sinon.*

*Démonstration.* Notons $u = u_n \cdots u_1$ avec $u_i \in A$ pour tout $i \in \{1, \dots, n\}$ et $v = v_k \cdots v_1$ avec $v_i \in A$ pour tout $i \in \{1, \dots, k\}$.

Montrons que le polynôme $\binom{u}{v}_q$ est monique. Par définition, il suffit de montrer que le coefficient du terme de plus haut degré est égal à 1. Procédons par l'absurde et supposons qu'il existe deux suites distinctes $Y$ et $Y'$ dans $A_{n,k}$ telles que $s(Y) = s(Y')$ soit maximal. Ces deux suites sont donc telles que le coefficient du terme de plus haut degré est augmenté. Soit $l \in \{1, \dots, k\}$ tel que $y_i = y'_i$ pour tout $i \in \{l+1, \dots, k\}$ et $y_l > y'_l$. Par définition, on sait que $u_{y_l} = u_{y'_l}$. En remplaçant $y'_l$ par $y_l$ dans la suite $Y'$, on obtient une nouvelle

suite $Z \in A_{n,k}$ telle que $s(Y') < s(Z)$, ce qui contredit la maximalité de $s(Y')$. De cette manière, le polynôme $\binom{u}{v}_q$ est monique.

Montrons que le coefficient non nul du terme de plus petit degré est égal à 1. Procédons par l'absurde et supposons qu'il existe deux suites distinctes $Y$ et $Y'$ dans $A_{n,k}$ telles que $s(Y) = s(Y')$ soit minimal. Soit $l \in \{1, \dots, k\}$ tel que $y_i = y'_i$ pour tout $i \in \{l+1, \dots, k\}$ et $y_l > y'_l$. Par définition, on sait que $u_{y_l} = u_{y'_l}$. En remplaçant $y_l$ par $y'_l$ dans la suite $Y'$ donnerait une nouvelle suite $Z \in A_{n,k}$ telle que $s(Y') > s(Z)$, ce qui contredit la minimalité de $s(Y')$. De cette manière, le coefficient non nul du terme de plus petit degré est égal à 1.

Montrons que le terme indépendant de $\binom{u}{v}_q$ est égal à 1 si et seulement si $v$ est un suffixe de $u$ et est nul sinon.

- La condition est nécessaire. Supposons que le terme indépendant de $\binom{u}{v}_q$ est égal à 1 et montrons que $v$ est un suffixe de $u$. Par le Corollaire 3.2.3, on sait que si $Y = \{n \geq y_k > \cdots > y_1 \geq 1 : u_{y_k} \cdots u_{y_1} = v\} \in A_{n,k}$ correspond à une occurrence de $v$ dans $u$, alors cette occurrence contribue à $\binom{u}{v}_q$ avec un terme $q^\alpha$ où $\alpha = \sum_{i=1}^k y_i - i$. Pour étudier la valeur du terme indépendant, il faut étudier quand $\alpha = 0$. Pour que $\alpha = 0$, étant donné que $y_i - i \geq 0$ pour tout $i \in \{1, \dots, k\}$, il faut que $y_i = i$ pour tout $i \in \{1, \dots, k\}$. De cette manière, on $v = u_k \cdots u_1$, c'est-à-dire que le sous-mot $v$ est un suffixe de $u$.
- La condition est suffisante. Supposons que $v$ est un suffixe de $u$ et montrons que le terme indépendant est égal à 1. Étant donné que $v$ est un sous-mot de $u$, on sait que $u = u_{k+1}v_k u_k \cdots v_1 u_1$ où $u_i \in A^*$ pour tout $i \in \{1, \dots, k+1\}$. Par le Corollaire 3.2.3, on a

$$\begin{aligned}
\binom{u}{v}_q &= \sum_{\substack{u_{k+1}v_k u_k \cdots v_1 u_1 = u \\ u_i \in A^*}} \prod_{i=1}^{k} q^{|u_i \cdots u_1|} \\
&= \sum_{\substack{u_{k+1}v_k u_k \cdots v_1 u_1 = u \\ u_i \in A^* \\ \exists i \in \{1,\dots,k\} : u_i \neq \varepsilon}} \prod_{i=1}^{k} q^{|u_i \cdots u_1|} + \sum_{\substack{u_{k+1}v = u \\ u_{k+1} \in A^*}} \prod_{i=1}^{0} q^{|u_i \cdots u_1|} \\
&= \sum_{\substack{u_{k+1}v_k u_k \cdots v_1 u_1 = u \\ u_i \in A^* \\ \exists i \in \{1,\dots,k\} : u_i \neq \varepsilon}} \prod_{i=1}^{k} q^{|u_i \cdots u_1|} + 1.
\end{aligned}$$

  S'il existe $i \in \{1, \dots, k\}$ tel que $u_i \neq \varepsilon$, on sait que $\prod_{i=1}^k q^{|u_i \cdots u_1|} = q^t$ où $t > 0$. De cette manière, le terme indépendant de $\binom{u}{v}_q$ est égal à 1.

Si $v$ n'est pas un suffixe de $u$, alors on sait que le terme indépendant est différent de 1. Cependant, étant donné que le coefficient non nul du terme de plus petit degré est égal à 1, on obtient que le terme indépendant est égal à 0.

Montrons que le degré de $\binom{u}{v}_q$ est plus petit ou égal à $|v| \cdot (|u| - |v|)$. Par le Théorème

3.2.1, on sait que

$$\binom{u}{v}_q = \sum_{Y \in A_{n,k}} q^{s(Y) - \frac{k(k+1)}{2}},$$

où $s(Y) = \sum_{i=1}^{k} y_i$. Étant donné que $y_k \leq |u|$, on obtient que $y_i \leq |u| - (k-i)$ pour tout $i \in \{1, \ldots, k\}$. De cette manière, on a $y_i - i \leq |u| - k$ pour tout $i \in \{1, \ldots, k\}$. Par conséquent, on a

$$\begin{aligned} s(Y) - \frac{k(k+1)}{2} &= \sum_{i=1}^{k} (y_i - i) \\ &\leq \sum_{i=1}^{k} (|u| - k) \\ &= k \cdot (|u| - k). \end{aligned}$$

Étant donné que cela vaut pour toutes les occurrences de $v$, on en tire que

$$\deg \binom{u}{v}_q \leq |v| \cdot (|u| - |v|).$$

Montrons que le coefficient de $q^{|v| \cdot (|u| - |v|)}$ est égal à 1 si et seulement si $v$ est un préfixe de $u$ et est égal à 0 sinon.

- La condition est nécessaire. Supposons que le coefficient de $q^{|v| \cdot (|u| - |v|)}$ est égal à 1 et montrons que $v$ est un préfixe de $u$. Par le Corollaire 3.2.3, on sait que si $Y = \{n \geq y_k > \cdots > y_1 \geq 1 : u_{y_k} \cdots u_{y_1} = v\} \in A_{n,k}$ correspond à une occurrence de $v$ dans $u$, alors cette occurrence contribue à $\binom{u}{v}_q$ avec un terme $q^{\alpha}$ où $\alpha = \sum_{i=1}^{k} y_i - i$. Pour étudier la valeur du coefficient du terme de plus haut degré, il faut étudier quand $\alpha = |v| \cdot (|u| - |v|)$. Pour satisfaire cette condition, il faut que $y_i - i = |u| - k$ pour tout $i \in \{1, \ldots, k\}$, c'est-à-dire que

  $$y_i = |u| - k + i$$

  pour tout $i \in \{1, \ldots, k\}$. Cela traduit exactement le fait que $v$ est un préfixe de $u$.

- La condition est suffisante. Supposons que $v$ est un préfixe de $u$ et montrons que le coefficient de $q^{|v| \cdot (|u| - |v|)}$ est égal à 1. Si $u = vu'$ avec $u' \in A^*$, alors si $Y = \{n \geq y_k > \cdots > y_1 \geq 1 : u_{y_k} \cdots u_{y_1} = v\} \in A_{n,k}$ est une occurrence de $v$ dans $u$, alors $y_k = n, y_{k-1} = n-1, \ldots, y_1 = n-k+1$. Ainsi, on a

  $$\sum_{i=1}^{k} (y_i - i) = k \cdot (n - k).$$

  De cette manière, le coefficient du terme $q^{|v| \cdot (|u| - |v|)}$ est plus grand ou égal à 1. Cependant, le polynôme $\binom{u}{v}_q$ étant monique et le terme $q^{|v| \cdot (|u| - |v|)}$ étant le terme de plus haut degré, on obtient que le coefficient de ce terme est égal à 1.

Si $v$ n'est pas un préfixe de $u$, alors on sait que le coefficient de $q^{|v|\cdot(|u|-|v|)}$ est différent de 1. Cependant, étant donné que le polynôme $\binom{u}{v}_q$ est monique, on sait que ce coefficient est donc nul, ce qui nous donne la conclusion. □

Dans le corollaire ci-dessous, dans le $q$-analogue de la relation donnée à la Proposition 1.3.11, une puissance de $q$ apparaît. Remarquons également qu'en faisant tendre $q$ vers 1, nous retombons bien sur cette proposition. Une telle puissance apparaît déjà dans le $q$-analogue de l'identité de Vandermonde :

$$\binom{m+n}{k}_q = \sum_j q^{j(m-k+j)} \binom{m}{k-j}_q \binom{n}{j}_q = \sum_{\substack{0\leq i,j\leq k \\ i+j=k}} q^{(m-i)j} \binom{m}{i}_q \binom{n}{j}_q,$$

où les contributions non nulles pour cette somme viennent des valeurs $j$ telles que

$$\max\{0, k-m\} \leq j \leq \min\{n, k\}.$$

**Corollaire 3.2.6.** *Pour tous mots $x, y, v \in A^*$, on a*

$$\binom{xy}{v}_q = \sum_{\substack{v_1,v_2\in A^* \\ v=v_1v_2}} q^{|v_1|(|y|-|v_2|)} \binom{x}{v_1}_q \binom{y}{v_2}_q.$$

*Démonstration.* Intéressons-nous à une occurrence du mot $v = v_1v_2$ comme sous-mot de $xy$ telle que $v_1$ apparaît dans $x$ et telle que $v_2$ apparaît dans $y$. Soit $\mathcal{V}_1 = \{j_{|v_1|} > \cdots > j_1\} \subset \{1, \ldots, |x|\}$ et $\mathcal{V}_2 = \{k_{|v_2|} > \cdots > k_1\} \subset \{1, \ldots, |y|\}$ les ensembles d'indices correspondants tels que

$$x_{j_{|v_1|}} \cdots x_{j_1} = v_1$$

et

$$y_{k_{|v_2|}} \cdots y_{k_1} = v_2.$$

Par le Théorème 3.2.1, cette occurrence spécifique de $v$ contribue à $\binom{x}{v_1}_q \binom{y}{v_2}_q$ avec

$$q^{s(\mathcal{V}_1) - \frac{|v_1|(|v_1|+1)}{2}} \cdot q^{s(\mathcal{V}_2) - \frac{|v_2|(|v_2|+1)}{2}}.$$

Étant donné que les positions des lettres sont comptées de droite à gauche, toute lettre de $v_1$ qui apparaît dans $x$ à la position $j$ apparaît dans $xy$ à la position $j+|y|$. Par conséquent, cette occurrence spécifique de $v$ contribue à $\binom{xy}{v}_q$ avec

$$q^{s(V) - \frac{|v|(|v|+1)}{2}},$$

où

$$V = (\mathcal{V}_1 + |y|) \cup \mathcal{V}_2 = \{j_{|v_1|} + |y| > \cdots > j_1 + |y| > k_{|v_2|} > \cdots > k_1\}.$$

En considérant un terme du membre de droite, on obtient que $s(V) = s(\mathcal{V}_1)+s(\mathcal{V}_2)+|v_1||y|$. De plus, on remarque que

$$\begin{aligned}\frac{|v|(|v|+1)}{2} &= \frac{(|v_1|+v_2|)(|v_1|+|v_2|+1)}{2} \\ &= \frac{|v_1|(|v_1|+1)}{2} + \frac{|v_2|(|v_2|+1)}{2} + |v_1||v_2|.\end{aligned}$$

On obtient finalement que

$$\begin{aligned}q^{s(V)-\frac{|v|(|v|+1)}{2}} &= q^{s(\mathcal{V}_1)+s(\mathcal{V}_2)+|v_1||y|-\frac{|v_1|(|v_1|+1)}{2}-\frac{|v_2|(|v_2|+1)}{2}-|v_1||v_2|} \\ &= q^{|v_1|(|y|-|v_2|)}q^{s(\mathcal{V}_1)-\frac{|v_1|(|v_1|+1)}{2}}q^{s(\mathcal{V}_2)-\frac{|v_2|(|v_2|+1)}{2}}.\end{aligned}$$

On en tire la conclusion. □

En itérant cet argument, on obtient le corollaire suivant.

**Corollaire 3.2.7.** *Soit $k \geq 2$. Si $x_1, \ldots, x_k, v \in A^*$, alors on a*

$$\binom{x_1 \cdots x_k}{v}_q = \sum_{\substack{v_1,\ldots,v_k \in A^* \\ v=v_1\cdots v_k}} q^{\sum_{i=1}^{k-1} |v_i|(|x_{i+1}\cdots x_k|-|v_{i+1}\cdots v_k|)} \binom{x_1}{v_1}_q \cdots \binom{x_k}{v_k}_q.$$

Nous finissons cette section avec un dernier corollaire liant les coefficients du polynôme $\binom{u}{v}_q$ avec ceux du polynôme $\binom{u^R}{v^R}_q$.

**Corollaire 3.2.8.** *Soient $u, v \in A^*$. Pour tout $i \in \{0, \ldots, |v|(|u|-|v|)\}$, on a*

$$\binom{u}{v}_q [q^i] = \binom{u^R}{v^R}_q [q^{|v|(|u|-|v|)-i}].$$

*En particulier, si $u$ et $v$ sont deux palindromes, alors la suite des coefficients de $\binom{u}{v}_q$ pour les degrés appartenant à $\{0, \ldots, |v|(|u|-|v|)\}$ est un palindrome.*

*Démonstration.* Soient $k = |v|$ et $n = |u|$. Soit $Y = \{n \geq y_k > \cdots > y_1 \geq 1 : u_{y_k} \cdots u_{y_1} = v\} \in A_{n,k}$ l'ensemble d'indices correspondant à une occurrence de $v$ dans $u$. Par le Théorème 3.2.1, cette occurrence spécifique contribue à $\binom{u}{v}_q$ avec un monôme de degré

$$s(Y) - \frac{k(k+1)}{2}.$$

Remarquons que l'ensemble

$$Y' = \{n - y_1 + 1 > \cdots > n - y_k + 1\}$$

est l'ensemble d'indices correspondant à l'occurrence de $v^R$ dans $u^R$. Par le Théorème 3.2.1, cette occurrence contribue à $\binom{u^R}{v^R}_q$ avec un monôme de degré

$$s(Y') - \frac{k(k+1)}{2}.$$

De plus, on a

$$s(Y') = \sum_{i=1}^{k}(n - y_i + 1) = kn + k - \sum_{i=1}^{n} y_i = k(n+1) - s(Y).$$

De cette manière, cette occurrence contribue à $\binom{u^R}{v^R}_q$ avec un monôme de degré

$$\begin{aligned} s(Y') - \frac{k(k+1)}{2} &= k(n+1) - s(Y) - \frac{k(k+1)}{2} \\ &= k(n+1) - k(k+1) - s(Y) - \frac{k(k+1)}{2} + k(k+1) \\ &= k(n+1) - k(k+1) - \left(s(Y) - \frac{k(k+1)}{2}\right) \\ &= k(n-k) - \left(s(Y) - \frac{k(k+1)}{2}\right). \end{aligned}$$

On en tire que, pour tout $i \in \{0, \ldots, k(n-k)\}$, on a

$$\binom{u}{v}_q [q^i] = \binom{u^R}{v^R}_q [q^{k(n-k)-i}],$$

ce qui permet de conclure.

Si $u$ et $v$ sont deux palindromes, on sait que $u^R = u$ et $v^R = v$. De cette manière, pour tout $i \in \{0, \ldots, |v|(|u| - |v|)\}$, on a

$$\binom{u}{v}_q [q^i] = \binom{u}{v}_q [q^{|v|(|u|-|v|)-i}].$$

On en tire donc que la suite des coefficients de $\binom{u}{v}_q$ pour les degrés appartenant à $\{0, \ldots, |v|(|u| - |v|)\}$ est un palindrome, ce qui nous permet de conclure. □

## 3.3 Analogue de formules classiques de combinatoire

Nous nous intéressons à présent à quelques analogues de formules classiques de la combinatoire. En faisant tendre $q$ vers 1 dans le théorème suivant, nous retombons sur la formule suivante de combinatoire : soient $u, x \in A^*$. Si $|u| \geq k \geq |x|$, alors

$$\binom{|u| - |x|}{k - |x|}\binom{u}{x} = \sum_{t \in A^k} \binom{u}{t}\binom{t}{x}.$$

**Théorème 3.3.1.** *Soient $u, x \in A^*$. Si $|u| \geq k \geq |x|$, alors*

$$\binom{|u|-|x|}{k-|x|}_q \binom{u}{x}_q = \sum_{t \in A^k} \binom{u}{t}_q \binom{t}{x}_q.$$

*Démonstration.* Supposons que $x$ ne soit pas un sous-mot de $u$. Dans ce cas, on sait par le Lemme 3.1.6 que le membre de gauche est nul. De plus, si $t$ est un sous-mot de $u$, alors $x$ n'est pas un sous-mot de $t$ car sinon $x$ serait un sous-mot de $u$. De cette manière, par le Lemme 3.1.6, le membre de droite est nul. Enfin, si $t$ n'est pas un sous-mot de $u$, alors on obtient également par le Lemme 3.1.6 que le membre de droite est nul, ce qui nous donne la conclusion dans ce cas.

Supposons que $x$ soit un sous-mot de $u$. Considérons [2] une occurrence spécifique de $x$ comme sous-mot de $u$ et un sous-mot spécifique $t$ de longueur $k$ de $u$ contenant cette occurrence de $x$. On va s'intéresser à la contribution de ces éléments comme puissance de $q$ dans les deux membres de la relation. Ainsi, si $u = u_{|u|} \cdots u_1$, il existe deux suites $|u| \geq i_k > \cdots > i_1 \geq 1$ et $k \geq j_{|x|} > \cdots > j_1 \geq 1$ telles que

$$t = u_{i_k} \cdots u_{i_1} \qquad et \qquad x = t_{j_{|x|}} \cdots t_{j_1}.$$

En particulier, on a

$$x = u_{i_{j_{|x|}}} \cdots u_{j_1}.$$

Par le Théorème 3.2.1, ces occurrences spécifiques contribuent respectivement à $\binom{u}{t}_q$ et $\binom{t}{x}_q$ dans le membre de droite avec

$$q^{\sum_{n=1}^{k} i_n - \frac{k(k+1)}{2}} \qquad et \qquad q^{\sum_{n=1}^{|x|} j_n - \frac{|x|(|x|+1)}{2}}.$$

De manière similaire, cette occurrence de $x$ contribue à $\binom{u}{x}_q$ dans le membre de gauche avec

$$q^{\sum_{n=1}^{|x|} i_{j_n} - \frac{|x|(|x|+1)}{2}}. \tag{3.5}$$

Pour construire un sous-mot spécifique $t$ de longueur $k$ de $u$ ayant cette occurrence particulière de $x$ comme sous-mot, on doit choisir $k-|x|$ nouvelles positions parmi les $|u|-|x|$ restantes. Il y a en effet une correspondance entre le choix des $k-|x|$ positions parmi $|u|-|x|$ et les sous-mots de $u$ de longueur $k$ ayant l'occurrence fixée de $x$ comme sous-mot. Étant donné que nous nous intéressons ici aux positions de lettres, on peut remplacer celles-ci par un symbole $\circ$. On interprète ainsi

$$\binom{|u|-|x|}{k-|x|}_q = \binom{\circ^{|u|-|x|}}{\circ^{k-|x|}}_q$$

2. Étant donné que $|u| \geq k$, il existe toujours un tel sous-mot $t \in A^k$. De plus, étant donné que $|x| \leq k$ et étant donné que $x$ est un sous-mot de $u$, on obtient bien que $x$ est un sous-mot de $t$.

et on veut que les contributions correspondent au choix des indices $i_k, \dots, i_1$ mais une fois que les indices $i_{j_{|x|}}, \dots, i_{j_1}$ ont été enlevés [3]. Par le Corollaire 3.2.3, la puissance est donnée par la somme sur toutes les lettres de $t$, exceptées celles de $x$, du nombre de lettres à leur droite qui ne font pas parties de cette occurrence spécifique du sous-mot $t$. Étant donné que $x$ fait partie de l'occurrence de $t$ dans $u$, on peut écrire la somme d'une autre manière. Il s'agit en fait de la contribution de tous les indices de $t$ dans $u$, à laquelle on soustrait les contributions qui viennent des indices de $x$ qui sont enlevés dans $u$, c'est-à-dire

$$q^{\sum_{n=1}^{k}(i_n-n)-\sum_{n=1}^{|x|}(i_{j_n}-j_n)} = q^{\sum_{n=1}^{k} i_n-\frac{k(k+1)}{2}-\sum_{n=1}^{|x|}(i_{j_n}-j_n)}.$$

En multipliant cette contribution avec la relation (3.5), on obtient que la contribution pour le membre de gauche est égale à

$$\begin{aligned} q^{\sum_{n=1}^{k} i_n-\frac{k(k+1)}{2}-\sum_{n=1}^{|x|}(i_{j_n}-j_n)} \cdot q^{\sum_{n=1}^{|x|} i_{j_n}-\frac{|x|(|x|+1)}{2}} &= q^{\sum_{n=1}^{k} i_n-\frac{k(k+1)}{2}-\sum_{n=1}^{|x|} i_{j_n}+\sum_{n=1}^{|x|} j_n+\sum_{n=1}^{|x|} i_{j_n}-\sum_{n=1}^{|x|}\frac{|x|(|x|+1)}{2}} \\ &= q^{\sum_{n=1}^{k} i_n-\frac{k(k+1)}{2}+\sum_{n=1}^{|x|} j_n-\frac{|x|(|x|+1)}{2}}. \end{aligned}$$

Les contributions pour le membre de gauche et le membre de droite étant égales, on en conclut finalement que

$$\binom{|u|-|x|}{k-|x|}_q \binom{u}{x}_q = \sum_{t\in A^k} \binom{u}{t}_q \binom{t}{x}_q.$$

□

Le corollaire suivant montre que les $q$-déformations contiennent plus d'informations que les coefficients obtenus avec $q = 1$.

**Corollaire 3.3.2.** *Soient $u \in A^*$ et $k \in \{1, \dots, |u|\}$. La suite $(\binom{u}{x}_q)_{x\in A^k}$ détermine de manière unique le mot $u$.*

*Démonstration.* La propriété est vraie pour $k = 1$. En effet, étant donné que le polynôme $\binom{u}{a}_q$, où $a \in A$, encode les positions de $a$ dans $u$, il détermine de manière unique le mot $u$.

Si $k \geq 2$, on utilise le Théorème 3.3.1 pour trouver le polynôme $\binom{|u|-1}{k-1}_q \binom{u}{a}_q$, où $a \in A$. De cette manière, on détermine le polynôme $\binom{u}{a}_q$. En particulier, on détermine de manière unique le mot $u$ comme expliqué précédemment, ce qui nous donne la conclusion. □

**Exemple 3.3.3.** Soit $A = \{a, b\}$. Considérons un mot $u = u_6 \cdots u_1$ de longueur 6 et soit $k = 2$. Supposons que la suite $(\binom{u}{x}_q)_{x\in A^2}$ soit donnée par

- $\binom{u}{aa}_q = q^6 + q^4 + q$,
- $\binom{u}{ab}_q = q^8 + q^7 + q^5 + q^2$,

3. Cela résulte du fait que les positions ne sont pas disponibles.

- $\binom{u}{bb}_q = q^6 + q^4 + q^3$,
- $\binom{u}{ba}_q = q^5 + q^4 + q^3 + q^2 + 1$.

Par le Théorème 3.3.1, on a

$$\begin{aligned}\binom{5}{1}_q\binom{u}{a}_q &= \sum_{t\in A^2}\binom{u}{t}_q\binom{t}{a}_q \\ &= \binom{u}{aa}_q\binom{aa}{a}_q + \binom{u}{ab}_q\binom{ab}{a}_q + \binom{u}{bb}_q\binom{bb}{a}_q + \binom{u}{ba}_q\binom{ba}{a}_q \\ &= (q^6+q^4+q)(q+1) + (q^8+q^7+q^5+q^2)\cdot q \\ &\quad + (q^6+q^4+q^3)\cdot 0 + (q^5+q^4+q^3+q^2+1)\cdot 1 \\ &= q^9+q^8+q^7+2q^6+2q^5+2q^4+2q^3+2q^2+q+1.\end{aligned}$$

Étant donné que

$$\binom{5}{1}_q = \frac{1-q^5}{1-q} = q^4+q^3+q^2+q+1,$$

on obtient que

$$\binom{u}{a}_q = \frac{q^9+q^8+q^7+2q^6+2q^5+2q^4+2q^3+2q^2+q+1}{q^4+q^3+q^2+q+1} = q^5+q^2+1.$$

Par définition, on obtient donc que $u_1 = a, u_3 = a$ et $u_6 = a$. Étant donné que $A$ ne contient que deux lettres, on en tire également que $u_2 = b, u_4 = b$ et $u_5 = b$. De cette manière, on obtient finalement que

$$u = abbaba.$$

**Remarque 3.3.4.** De manière générale, si $A$ est un alphabet de taille $k \geq 2$, il faut appliquer le procédé utilisé dans l'exemple précédent avec $k-1$ lettres de cet alphabet. Pour les positions de la dernière lettre, il suffit de déduire de ce qui a été fait précédemment que la dernière lettre se trouve aux positions manquantes dans le mot $u$.

En faisant tendre $q$ vers 1 dans la proposition suivante, nous retombons sur la formule suivante de combinatoire : soient $u, v \in A^*$. Si $n$ est un naturel, alors

$$\sum_{v\in A^n}\binom{u}{v} = \binom{|u|}{n}.$$

Observons que le $q$-analogue de cette formule ne dépend pas de la taille de l'alphabet $A$.

**Proposition 3.3.5.** *Soient $u, v \in A^*$. Si $n \geq 1$ est un naturel, alors*

$$\sum_{v\in A^n}\binom{u}{v}_q = \binom{|u|}{n}_q.$$

*Démonstration.* ◇ Supposons que $|u| < n$. Dans ce cas, on sait que $\binom{|u|}{n}_q = 0$. De plus, étant donné que la somme du membre de gauche se fait sur les mots $v \in A^n$, on sait que $|v| > |u|$. De cette manière, on obtient par la Remarque 3.1.5 que $\sum_{v\in A^n} \binom{u}{v}_q = 0$. L'égalité est donc vérifiée.

◇ Supposons que $|u| \geq n$. Procédons par double récurrence sur $n$ et sur $|u|$.

► Supposons que $n = 1$. Dans ce cas, on sait que

$$\sum_{a\in A} \binom{u}{a}_q = \sum_{i=0}^{|u|-1} q^i.$$

Cependant, par définition, on sait que

$$\binom{|u|}{1}_q = \frac{1-q^{|u|}}{1-q} = \sum_{i=0}^{|u|-1} q^i.$$

L'égalité est donc vérifiée dans ce cas.

► Supposons que $|u| = n$. Dans ce cas, on a par définition que $\binom{|u|}{n}_q = 1$. De plus, on a

$$\sum_{v\in A^n} \binom{u}{v}_q = \binom{u}{u}_q + \sum_{\substack{v\in A^n \\ v\neq u}} \binom{u}{v}_q = 1,$$

où l'on a utilisé la Remarque 3.1.5 pour dire que $\binom{u}{v}_q = 0$ si $v \neq u$. L'égalité est donc vérifiée dans ce cas.

► Supposons à présent que le résultat soit vérifié pour un $n \geq 1$ et pour tous les mots $u \in A^*$. Montrons que le résultat est vérifié pour $n+1$. Nous pouvons supposer que le résultat soit vérifié pour tous les mots dont la longueur est plus petite ou égale à $m$, où $m \geq n+1$. Considérons un mot $ub$ de longueur $m+1$, où $u \in A^m$ et $b \in A$. On remarque que

$$\begin{aligned}\sum_{v\in A^{n+1}} \binom{ub}{v}_q &= \sum_{a\in A}\sum_{v'\in A^n} \binom{ub}{v'a}_q \\ &= \sum_{a\in A}\sum_{v'\in A^n} q^{n+1}\binom{u}{v'a}_q + \sum_{a\in A}\sum_{v'\in A^n} \delta_{a,b}\cdot\binom{u}{v'}_q,\end{aligned}$$

où l'on a utilisé la définition de la $q$-déformation d'un coefficient binomial de

mots. En utilisant l'hypothèse de récurrence, on obtient que

$$\begin{aligned}\sum_{v\in A^{n+1}}\binom{ub}{v}_q &= q^{n+1}\sum_{v\in A^{n+1}}\binom{u}{v}_q+\sum_{v'\in A^n}\binom{u}{v'}_q\\ &= q^{n+1}\binom{|u|}{n+1}_q+\binom{|u|}{n}_q\\ &= q^{n+1}\binom{m}{n+1}_q+\binom{m}{n}_q\\ &= \binom{m+1}{n+1}_q\\ &= \binom{|ub|}{n+1}_q,\end{aligned}$$

où l'on a utilisé la relation (3.2).

La relation est donc vérifiée pour tout naturel $n\geq 1$, ce qui nous permet de conclure. □

**Exemple 3.3.6.** Par la Proposition 3.3.5, on obtient directement que

$$\begin{aligned}\sum_{v\in\{a,b,c\}^3}\binom{abcbac}{v}_q &= \binom{6}{3}_q\\ &= \frac{(1-q^6)(1-q^5)(1-q^4)}{(1-q)(1-q^2)(1-q^3)}\\ &= q^9+q^8+2q^7+3q^6+3q^5+3q^4+3q^3+2q^2+q+1.\end{aligned}$$

**Proposition 3.3.7.** *Soient $u,v\in A^*$. Si $n\geq 1$ est un naturel, alors*

$$\sum_{u\in A^n}\binom{u}{v}_q=(\#A)^{n-|v|}\binom{n}{|v|}_q.$$

*Démonstration.* Nous procédons par double récurrence sur $|v|$ et sur $n$.

- ◇ Supposons d'abord que $v=a\in A$ et que $n\geq 1$. Soit $i\in\{1,\dots,n\}$. Parmi les $(\#A)^n$ mots de longueur $n$, exactement $(\#A)^{n-1}$ mots ont une occurrence de $a$ en position $i$. Pour un tel mot $u$, en utilisant le Théorème 3.2.1, on obtient que

$$\binom{u}{a}_q[q^{i-1}]=1.$$

Par conséquent, le coefficient de $q^{i-1}$ dans le membre de gauche sera $(\#A)^{n-1}$. Remarquons que, pour le membre de droite, on a

$$\binom{n}{1}_q=\frac{1-q^n}{1-q}=q^{n-1}+\cdots+q+1,$$

ce qui nous permet de conclure dans ce cas.

◇ Supposons à présent que le résultat soit vérifié pour des mots de longueur plus petite ou égale à $m$ et tout $n \geq m$. Soit $va$ un mot de taille $m+1$ avec $v \in A^m$ et $a \in A$.

► Supposons que $n = m+1$. On remarque que les deux membres sont égaux à 1. En effet, on a

$$\sum_{u \in A^{m+1}} \binom{u}{v}_q = \binom{v}{v}_q + \sum_{\substack{u \in A^{m+1} \\ u \neq v}} \binom{u}{v}_q = 1,$$

où l'on a utilisé la Remarque 3.1.5 pour dire que $\binom{u}{v}_q = 0$ si $u \neq v$. De plus, on a

$$(\#A)^{m+1-(m+1)} \binom{m+1}{m+1}_q = 1.$$

La relation est donc vérifiée dans ce cas.

► Supposons à présent que le résultat soit vérifié pour $n \geq m+1$ et montrons qu'il est toujours vérifié pour $n+1$. On remarque que

$$\begin{aligned} \sum_{u \in A^{n+1}} \binom{u}{va}_q &= \sum_{b \in A} \sum_{u' \in A^n} \binom{u'b}{va}_q \\ &= \sum_{b \in A} \sum_{u' \in A^n} q^{n+1} \binom{u'}{va}_q + \sum_{b \in A} \sum_{u' \in A^n} \delta_{a,b} \binom{u'}{v}_q, \end{aligned}$$

où l'on a utilisé la définition de la $q$-déformation d'un coefficient binomial de mots. En utilisant l'hypothèse de récurrence, on obtient que

$$\begin{aligned} \sum_{u \in A^{n+1}} \binom{u}{va}_q &= q^{n+1}(\#A) \sum_{u' \in A^n} \binom{u'}{va}_q + \sum_{u' \in A^n} \binom{u'}{v}_q \\ &= q^{n+1}(\#A)(\#A)^{n-(|v|+1)} \binom{n}{|v|+1}_q + (\#A)^{n-|v|} \binom{n}{|v|}_q \\ &= (\#A)^{n-|v|} \cdot \left( q^{n+1} \binom{n}{|v|+1}_q + \binom{n}{|v|}_q \right) \\ &= (\#A)^{n-|v|} \binom{n+1}{m+1}_q \\ &= (\#A)^{n-|v|} \binom{n+1}{|va|}_q, \end{aligned}$$

où l'on a utilisé la relation (3.2).

La relation est donc vérifiée pour tout $n \geq 1$, ce qui nous permet de conclure. □

**Exemple 3.3.8.** Par la Proposition 3.3.7, on a

$$\begin{aligned}\sum_{u\in\{a,b\}^4}\binom{u}{ba}_q &= 2^{4-2}\cdot\binom{4}{2}_q\\ &= 4\cdot\frac{(1-q^4)(1-q^3)}{(1-q)(1-q^2)}\\ &= 4q^4+4q^3+8q^2+4q+4.\end{aligned}$$

## 3.4 Généralisation du théorème d'Eilenberg

Dans cette section, nous nous intéressons à une généralisation de ce qui a été fait au Chapitre 2, plus précisément à la section 2.4. Dans l'ensemble de cette section, $p$ est un nombre premier.

**Définition 3.4.1.** Une relation d'équivalence $\simeq$ est un *raffinement* d'une relation d'équivalence $\sim$ si pour tous mots $w_1, w_2 \in A^*$ vérifiant $w_1 \simeq w_2$, on a $w_1 \sim w_2$. On dira également que $\sim$ est *moins fine* que $\simeq$.

On introduit ce qui est appelé la $(u, \mathfrak{M})$-relation d'équivalence binomiale. En particulier, nous considérons les raffinements les plus grossiers $\equiv_{u,\mathfrak{M}}$ de ces relations qui sont des congruences. De cette manière, le quotient $A^*/\equiv_{u,\mathfrak{M}}$ est un monoïde. Dans la suite, nous étudions cette structure et déterminons lorsqu'elle est en plus un groupe. Nous obtenons également des informations sur l'ordre de celle-ci. Enfin, comme corollaire, nous généralisons le Théorème 2.4.6 caractérisant les langages acceptés par un $p$-groupe.

Rappelons la définition de langages reconnus par un monoïde.

**Définition 3.4.2.** Soient $L$ un langage sur $A$, $M$ un monoïde et $\mu : A^* \to M$ un morphisme de monoïdes. Le monoïde $M$ *reconnaît* le langage $L$ s'il existe un sous-ensemble $S$ de $M$ tel que $L = \mu^{-1}(S)$. Un langage est *reconnaissable* s'il est reconnu par un monoïde fini.

En particulier, un langage peut être accepté par un $p$-groupe.

**Définition 3.4.3.** Un langage $L$ sur $A$ est *accepté par un $p$-groupe* s'il est reconnu par un $p$-groupe.

Rappelons qu'un langage est reconnaissable si et seulement s'il est régulier, c'est-à-dire s'il existe un automate fini déterministe qui accepte le langage.

Soit $v \in A^*$. Nous allons suivre la procédure du Chapitre 2, dans lequel nous avons montré qu'un langage $L$ sur $A$ est accepté par un $p$-groupe si et seulement si $L$ est une combinaison booléenne de langages de la forme

$$L_{v,r,p} := \left\{u \in A^* : \binom{u}{v} \equiv r \mod p\right\}.$$

Soit $\mathbb{Z}_p$ le champ des entiers modulo $p$ et soit $\mathfrak{M}$ un polynôme non nul de degré $d \geq 1$ dans $\mathbb{Z}_p[q]$. Étant donné que les $q$-déformations de coefficients binomiaux de mots sont des polynômes dans $\mathbb{Z}[q]$, leurs coefficients entiers peuvent être réduits modulo $p$ pour obtenir un polynôme dans $\mathbb{Z}_p[q]$. De manière similaire à la définition des langages de la forme $L_{v,r,p}$, on définit les langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$.

**Définition 3.4.4.** Soient $v \in A^*$, $\mathfrak{M}$ un polynôme de degré $d \geq 1$ dans $\mathbb{Z}_p[q]$ et $\mathfrak{R} \in \mathbb{Z}_p[q]$ un polynôme tel que $\deg(\mathfrak{R}) < d$. On définit l'ensemble $L_{v,\mathfrak{R},\mathfrak{M}}$ par

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* : \binom{u}{v} \equiv \mathfrak{R} \mod \mathfrak{M} \right\}.$$

**Exemple 3.4.5.** Soient $A = \{a, b\}$, $v = a \in A$, $p = 2$ et les polynômes $\mathfrak{M}(q) = q + 1$ et $\mathfrak{R}(q) = 0$. Dans ce cas, on a

$$L_{a,0,q+1} = \left\{ u \in \{a, b\}^* : \binom{u}{a}_q \equiv 0 \mod q + 1 \right\}.$$

Dans le corps $\mathbb{Z}_2[q]/\langle q + 1 \rangle$, on sait que $q$ et 1 sont congrus. De cette manière, on a

$$L_{a,0,q+1} = \left\{ u \in \{a, b\}^* : \binom{u}{a} \equiv 0 \mod 2 \right\}$$

qui est l'ensemble des mots sur $A$ avec un nombre pair de $a$.

**Exemple 3.4.6.** Soient $A = \{a, b\}$, $v = ab \in A^*$, $p = 3$ et les polynômes $\mathfrak{M}(q) = q^2 + q + 1$ et $\mathfrak{R}(q) = q$. Dans ce cas, on a

$$L_{ab,q,q^2+q+1} = \left\{ u \in \{a, b\}^* : \binom{u}{ab}_q \equiv q \mod q^2 + q + 1 \right\}.$$

À l'aide de ces définitions, nous obtenons une généralisation du Théorème 2.4.6, à savoir qu'un langage est accepté par un $p$-groupe si et seulement s'il est une combinaison booléenne de langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$ où $\mathfrak{M}(q) = a(q-1)^d$ pour un entier $d \geq 1$ et pour un élément non nul $a \in \mathbb{Z}_p$.

### 3.4.1 Résultats préliminaires

De manière à clarifier la preuve du résultat principal, nous nous intéressons ici à plusieurs définitions et résultats préliminaires. Dans la suite, nous supposerons que $\mathfrak{M}$ est un polynôme non nul de degré $d \geq 1$ dans $\mathbb{Z}_p[q]$.

**Notation 3.4.7.** Nous notons $\mathbb{F}$ l'anneau fini $\mathbb{Z}_p[q]/\langle \mathfrak{M} \rangle$ d'ordre $p^d$ et nous notons $\mathbb{F}^*$ le groupe multiplicatif formé des éléments inversibles dans $\mathbb{F}$.

Il est à noter que $\mathbb{F}$ est un champ si et seulement si $\mathfrak{M}$ est irréductible sur $\mathbb{Z}_p$. Étant donné que $(\mathbb{F}, \cdot)$ est un semi-groupe fini dont l'identité est 1, on sait [4] que pour tout polynôme $\mathfrak{P} \in \mathbb{F}$, deux éléments de la suite $1, \mathfrak{P}, \mathfrak{P}^2, \ldots$ sont égaux, c'est-à-dire qu'il existe des entiers positifs $i \geq 0$ et $k \geq 1$ tels que

$$\mathfrak{P}^i = \mathfrak{P}^{i+k}. \tag{3.6}$$

**Définition 3.4.8.** Pour tout polynôme $\mathfrak{P} \in \mathbb{F}$, les deux entiers positifs $i \geq 0$ et $k \geq 1$ vérifiant l'équation (3.6) sont respectivement appelés *indice* et *période* de $\mathfrak{P}$. Ces deux entiers seront respectivement notés $\text{ind}(\mathfrak{P})$ et $\text{per}(\mathfrak{P})$.

L'illustration des notions d'indices et de périodes est donnée à la Figure 3.3. Il est à noter que, en règle générale, l'indice $i$ doit être tel que $i \geq 1$. Cependant, ici, étant donné que $\mathbb{F}$ possède un élément qui est l'identité, on peut prendre $i \geq 0$. De manière générale, l'élément $\mathfrak{P}^0$ n'est pas bien défini.

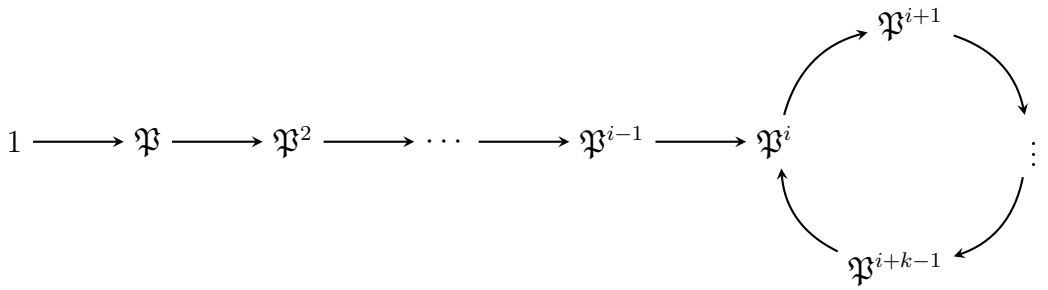



FIGURE 3.3 – Illustration de l'indice et de la période d'un élément $\mathfrak{P}$ de $\mathbb{F}$.

**Exemple 3.4.9.** Soient $p = 3$ et $\mathfrak{M}(q) = q^2 + q + 1 \in \mathbb{Z}_3[q]$. Dans ce cas, on a

$$\mathbb{F} = \{aq + b : a, b \in \mathbb{Z}_3\} = \{0, 1, 2, q, q+1, q+2, 2q, 2q+1, 2q+2\}.$$

De plus, étant donné que $q^2+q+1 \equiv 0 \mod q^2+q+1$, on a $q^2 \equiv -q-1 \mod q^2+q+1 \equiv 2q+2 \mod q^2+q+1$. Remarquons également que

$$\begin{aligned} q^3 &\equiv q \cdot (2q+2) \mod \mathfrak{M} \equiv 2q^2 + 2q \mod \mathfrak{M} \equiv 2(2q+2) + 2q \mod \mathfrak{M} \\ &\equiv 1 \mod q^2 + q + 1. \end{aligned}$$

De cette manière, on a $\text{per}(q) = 3$. De plus, étant donné que la suite $(q^n \mod q^2+q+1)_{n \geq 0}$ est donnée par

$$1, q, 2q+2, 1, q, 2q+2, 1, q, \ldots,$$

on obtient que $\text{ind}(q) = 0$.

4. Le théorème utilisé ici est le suivant [13, Théorème V.5.5.] : soit $(S, \cdot)$ un semi-groupe fini. Pour tout élément $a \in S$, il existe des entiers positifs $i$ et $p$ tels que $a, \ldots, a^i, \ldots, a^{i+p-1}$ soient disjoints mais tels que $a^{i+p} = a^i$.

Nous faisons la constatation directe suivante.

**Remarque 3.4.10.** Pour tous naturels $m$ et $n$, on a $\mathfrak{P}^m = \mathfrak{P}^n$ si et seulement si $m = n$ ou $m \equiv n \mod \mathrm{per}(\mathfrak{P})$ avec $m, n \geq \mathrm{ind}(\mathfrak{P})$. Il est également clair que $\mathrm{ind}(\mathfrak{P}) = 0$ si et seulement si $\mathfrak{P}$ est inversible.

L'indice et la période du polynôme $q$ ont un rôle central dans nos résultats. L'indice de $q$ est lui directement lié au polynôme $\mathfrak{M}$, comme nous le verrons par la suite.

Nous commençons avec un premier lemme technique qui nous donne des informations dans un cadre très précis.

**Lemme 3.4.11.** *Le polynôme $q$ est inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$ si et seulement si le polynôme $\mathfrak{M}$ a un terme constant non nul.*

*Démonstration.* On sait que $q$ est inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$, c'est-à-dire inversible modulo $\mathfrak{M}$, si et seulement s'il existe un polynôme $\mathfrak{D} \in \mathbb{Z}_p[q]$ tel que $\mathfrak{D}(q) \cdot q \equiv 1 \mod \mathfrak{M}$. Ainsi, $q$ est inversible modulo $\mathfrak{M}$ si et seulement s'il existe deux polynômes $\mathfrak{D}, \mathfrak{P} \in \mathbb{Z}_p[q]$ tels que

$$\mathfrak{D}(q) \cdot q + \mathfrak{P}(q) \cdot \mathfrak{M}(q) = 1.$$

Étant donné que $\mathbb{Z}_p$ est un champ, on sait que $\mathbb{Z}_p[q]$ est euclidien. De cette manière, le polynôme $q$ est inversible modulo $\mathfrak{M}$ si et seulement si le plus grand commun diviseur de $q$ et de $\mathfrak{M}$ est constant [5]. Étant donné que $q$ est un polynôme de degré 1, on sait que $\mathrm{pgcd}(q, \mathfrak{M}(q)) = q$ si $q$ divise $\mathfrak{M}$ et $\mathrm{pgcd}(q, \mathfrak{M}(q)) = 1$ sinon. Or, il est clair que $q$ divise $\mathfrak{M}$ si et seulement si le terme constant de $\mathfrak{M}$ est nul.

La condition est suffisante. Si le polynôme $\mathfrak{M}$ a un terme constant non nul, alors $q$ ne divise pas $\mathfrak{M}$. De cette manière, on a $\mathrm{pgcd}(q, \mathfrak{M}(q)) = 1$. On en tire que le polynôme $q$ est inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$.

La condition est nécessaire. Procédons par contraposition et montrons que si le terme constant de $\mathfrak{M}$ est nul, alors le polynôme $q$ n'est pas inversible. Étant donné que le terme constant de $\mathfrak{M}$ est nul, on sait que $q$ divise $\mathfrak{M}$. De cette manière, on a $\mathrm{pgcd}(q, \mathfrak{M}(q)) = q$. On en tire que le polynôme $q$ n'est pas inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$, ce qui nous donne la conclusion. □

Nous introduisons la valuation.

**Définition 3.4.12.** Si $\mathbb{K}$ est un champ, la *valuation* d'un polynôme $\mathfrak{P} \in \mathbb{K}[q]$, notée $\mathrm{val}(\mathfrak{P})$, est la plus grande puissance de $q$ qui divise $\mathfrak{P}$, c'est-à-dire

$$\mathrm{val}(\mathfrak{P}) = \max\{l \in \mathbb{N} : q^l \mid \mathfrak{P}(q)\}.$$

En particulier, on a $\mathrm{val}(0) = +\infty$.

5. En effet, le théorème de Bézout nous dit qu'il existe des polynômes $A$ et $B$ tels que $Aq + B\mathfrak{M}(q) = 1$ si et seulement si $\mathrm{pgcd}(q, \mathfrak{M}(q)) = 1$.

Le résultat suivant généralise le Lemme 3.4.11.

**Proposition 3.4.13.** *Dans* $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$, *on a* $\mathrm{ind}(q) = \mathrm{val}(\mathfrak{M})$.

*Démonstration.* Supposons que $\mathfrak{M}(q) = aq^d$ avec $a \neq 0$. Dans ce cas, la suite des puissances de $q$ modulo $\mathfrak{M}$ est de la forme

$$1, q, \ldots, q^{d-1}, 0, 0, \ldots,$$

où les $d$ premiers termes sont deux à deux distincts. Cela résulte du fait que les monômes $1, q, \ldots, q^{d-1}$ forment une base de $\langle q^d\rangle$. Par conséquent, on a $\mathrm{ind}(q) = d$. De plus, il est clair que $\mathrm{val}(\mathfrak{M}) = d$ également.

Supposons à présent que $\mathfrak{M}$ est de degré $d \geq 1$ et contient au moins deux termes non nuls. Dans ce cas, nous pouvons écrire

$$\mathfrak{M}(q) = a_d q^d + \cdots + a_1 q + a_0.$$

Soit $j$, avec $j < d$, le plus petit indice tel que $a_j \neq 0$.

- Montrons que $\mathrm{ind}(q) \leq j$. Définissons le polynôme

  $$\mathfrak{N}(q) = a_d q^{d-j} + \cdots + a_{j+1} q + a_j.$$

  Autrement dit, on a $q^j \mathfrak{N}(q) = \mathfrak{M}(q)$. Étant donné que $a_j \neq 0$, on obtient par le Lemme 3.4.11 que le polynôme $q$ est inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{N}\rangle$. En utilisant le même argument que ci-dessus, cela veut dire que l'indice de $q$ dans $\mathbb{Z}_p[q]/\langle\mathfrak{N}\rangle$ est nul. Par conséquent, il existe $i \geq 1$ et un polynôme $\mathfrak{B} \in \mathbb{Z}_p[q]$ tel que

  $$q^i = 1 + \mathfrak{B}(q)\mathfrak{N}(q).$$

  On en tire que

  $$q^{i+j} - q^j = \mathfrak{B}(q)\mathfrak{N}(q)q^j = \mathfrak{B}(q)\mathfrak{M}(q).$$

  Par conséquent, on a $q^{i+j} \equiv q^j \mod \mathfrak{M}$. Ceci nous donne finalement que $\mathrm{ind}(q) \leq j$.
- Montrons que $\mathrm{ind}(q) \geq j$. Procédons par l'absurde et supposons que $\mathrm{ind}(q) < j$. Par définition de l'indice et de la période, on sait que

  $$q^{\mathrm{ind}(q)+\mathrm{per}(q)} \equiv q^{\mathrm{ind}(q)} \mod \mathfrak{M}.$$

  Dans ce cas, on a

  $$q^{\mathrm{ind}(q)+\mathrm{per}(q)} - q^{\mathrm{ind}(q)} = \mathfrak{B}(q)\mathfrak{M}(q)$$

  pour un polynôme $\mathfrak{B} \in \mathbb{Z}_p[q]$. En divisant par $q^{\mathrm{ind}(q)}$, on obtient que

  $$q^{\mathrm{per}(q)} - 1 = \mathfrak{B}(q)\mathfrak{C}(q), \tag{3.7}$$

  où

  $$\mathfrak{C}(q) = \frac{\mathfrak{M}(q)}{q^{\mathrm{ind}(q)}} = a_d q^{d-\mathrm{ind}(q)} + \cdots + a_j q^{j-\mathrm{ind}(q)}.$$

  Vu la relation (3.7), on a $q^{\mathrm{per}(q)} \equiv 1 \mod \mathfrak{C}$. Ainsi, le polynôme $q$ est inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{C}\rangle$. Le terme constant de $\mathfrak{C}$ étant nul, on obtient par le Lemme 3.4.11 que le polynôme $q$ n'est pas inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{C}\rangle$, ce qui est absurde. Par conséquent, on a $\mathrm{ind}(q) \geq j$.

On en tire que $\mathrm{ind}(q) = j$. Enfin, étant donné que $\mathrm{val}(\mathfrak{M}) = j$, on obtient la conclusion. □

**Exemple 3.4.14.** Soient $p = 2$ et $\mathfrak{M}(q) = q^3 + q^5 \in \mathbb{Z}_2[q]$. Remarquons que $\mathfrak{M}(q) = q^3(1+q^2)$, c'est-à-dire que $q^3$ divise $\mathfrak{M}$. De plus, en effectuant la division euclidienne de $\mathfrak{M}$ avec $q^4$, on obtient que $q^3 + q^5 = q^4 \cdot q + q^3$ et en effectuant la division euclidienne de $\mathfrak{M}$ avec $q^5$, on obtient que $q^3 + q^5 = q^5 \cdot 1 + q^3$. De cette manière, $q^4$ et $q^5$ ne divise pas $\mathfrak{M}$. Ainsi, on obtient que $\mathrm{val}(\mathfrak{M}) = 3$. De plus, la suite $(q^n \mod \mathfrak{M})_{n\geq 0}$ est, étant donné que $q^5 \equiv q^3 \mod \mathfrak{M}$, que $q^6 \equiv q \cdot q^5 \equiv q^4 \mod \mathfrak{M}$, donnée par

$$1, q, q^3, q^3, q^4, q^3, q^4, q^3, q^4, \ldots.$$

Ainsi, on obtient que $\mathrm{ind}(q) = 3$, ce qui nous donne que $\mathrm{ind}(q) = \mathrm{val}(\mathfrak{M})$.

**Remarque 3.4.15.** La proposition précédente est bien une généralisation du Lemme 3.4.11. En effet, dans le cas particulier où $\mathrm{val}(\mathfrak{M}) = 0$, on a $\mathrm{ind}(q) = 0$. Par conséquent, le polynôme $\mathfrak{M}$ est inversible, ce qui nous donne que le polynôme $q$ est inversible. Ainsi, on retrouve bien que $q$ est inversible dans $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$ si et seulement si $\mathrm{val}(\mathfrak{M}) = 0$, c'est-à-dire si et seulement si $\mathfrak{M}$ a un terme constant non nul.

La proposition suivante est un élément clé dans notre étude des $p$-groupes à la sous-section 3.4.2.

**Proposition 3.4.16.** *Le polynôme $q$ est tel que* $\mathrm{ind}(q) = 0$ *et* $\mathrm{per}(q) = p^t$ *pour un $t > 0$ dans $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$ si et seulement si*

$$\mathfrak{M}(q) = a(q-1)^d$$

*pour un élément non nul $a \in \mathbb{Z}_p$ et un naturel $d \geq 1$.*

*Démonstration.* La condition est suffisante. Supposons que $\mathfrak{M}(q) = a(q-1)^d$ pour un naturel $d \geq 1$. Soit $n > 0$ tel que $p^n \geq d$. Étant donné que nous travaillons modulo $p$, on a

$$q^{p^n} - 1 = (q-1)^{p^n} = a^{-1}(q-1)^{p^n-d}a(q-1)^d = a^{-1}(q-1)^{p^n-d}\mathfrak{M}(q).$$

Par conséquent, on a $q^{p^n} \equiv 1 \mod \mathfrak{M}$. On en tire que le polynôme $q$ est inversible, c'est-à-dire que $\mathrm{ind}(q) = 0$. De plus, étant donné que $q^{p^n} \equiv 1 \mod \mathfrak{M}$, on obtient que $\mathrm{per}(q)$ divise $p^n$, c'est-à-dire qu'il existe $t > 0$ tel que $\mathrm{per}(q) = p^t$.

La condition est nécessaire. Supposons que $\mathrm{per}(q) = p^t$ pour un $t > 0$ et que $\mathrm{ind}(q) = 0$. Par définition, on sait que $q^{p^t} \equiv 1 \mod \mathfrak{M}$. Il existe donc un polynôme $\mathfrak{N} \in \mathbb{Z}_p[q]$ tel que

$$q^{p^t} = \mathfrak{N}(q)\mathfrak{M}(q) + 1.$$

Soit $\mathfrak{p}$ un facteur monique et irréductible de $\mathfrak{M}$. Étant donné que $\mathrm{ind}(q) = 0$, on sait que le polynôme $q$ est inversible. Par le Lemme 3.4.11, on obtient que le terme constant de $\mathfrak{M}$ est non nul. Ainsi, le terme constant de $\mathfrak{p}$ est également non nul. On obtient donc que $q^{p^t} \equiv 1 \mod \mathfrak{p}$. Le champ $\mathbb{Z}_p[q]/\langle\mathfrak{p}\rangle$ est d'ordre $p^{\deg(\mathfrak{p})}$. Ainsi, le groupe formé des inversibles de

$\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$ est d'ordre $p^{\deg(\mathfrak{p})}-1$. Étant donné que $\text{pgcd}(p^t, p^{\deg(\mathfrak{p})}-1)=1$ et que $q^{p^t}\equiv 1 \mod \mathfrak{p}$, on en déduit que $q\equiv 1 \mod \mathfrak{p}$. Ainsi, $q-1\equiv 0 \mod \mathfrak{p}$, ce qui revient à dire que $\mathfrak{p}$ divise $q-1$. De cette manière, il existe un polynôme $\mathfrak{B}\in\mathbb{Z}_p[q]$ tel que $q-1=\mathfrak{B}(q)\mathfrak{p}(q)$. Étant donné que $\mathfrak{p}$ est irréductible et que $q-1$ est irréductible (car il est de degré 1), on obtient que $\mathfrak{p}=q-1$ et $\mathfrak{B}=1$. Étant donné que $\mathfrak{p}$ était arbitraire, on en conclut que

$$\mathfrak{M}(q)=a(q-1)^d$$

pour un $d\geq 1$ et un élément non nul $a\in\mathbb{Z}_p$, ce qui nous donne la conclusion. □

**Exemple 3.4.17.** Soient $p=3$ et $\mathfrak{M}(q)=1\cdot(q-1)^2\in\mathbb{Z}_3[q]$. Dans ce cas, étant donné qu'on travaille modulo 3, on a $\mathfrak{M}(q)=q^2+q+1$. Comme nous l'avons vu à l'Exemple 3.4.9, on a $\text{ind}(q)=0$. De plus, on a $\text{per}(q)=3=3^1$.

**Exemple 3.4.18.** Soient $p=2$ et $\mathfrak{M}(q)=q^2+q\in\mathbb{Z}_2[q]$. Dans ce cas, on a

$$\mathfrak{M}(q)=q^2+q=q\cdot(q+1)\neq a(q-1)^d$$

pour un élément non nul $a\in\mathbb{Z}_2$ et un naturel $d\geq 1$. Étant donné que $q^2\equiv q \mod \mathfrak{M}$, on obtient que la suite $(q^n \mod \mathfrak{M})_{n\geq 0}$ est donnée par

$$1, q, q, q, \ldots.$$

De cette manière, on a $\text{ind}(q)=1$ et $\text{per}(q)=1$. Le polynôme $\mathfrak{M}$ n'est donc pas tel que $\text{ind}(q)=0$ et $\text{per}(q)=2^t$ pour un naturel $t\geq 1$.

Pour finir cette sous-section, nous nous intéressons à un dernier lemme portant sur l'arithmétique dans $\mathbb{Z}_p[q]/\langle\mathfrak{M}\rangle$.

**Lemme 3.4.19.** *Soit $\mathfrak{M}$ un polynôme non constant. Si $\mathfrak{P}\in\mathbb{Z}_p[q]$ est un polynôme de terme constant non nul et*

$$q^j\mathfrak{P}(q)\equiv q^{j+d\text{per}(q)}\mathfrak{P}(q) \mod \mathfrak{M}$$

*pour des entiers $j\geq 0$ et $d>0$, alors $j\geq ind(q)$.*

*Démonstration.* Supposons que $\text{ind}(q)=0$. Dans ce cas, étant donné que $j\geq 0$ par hypothèse, on obtient que $j\geq\text{ind}(q)$.

Supposons à présent que $\text{ind}(q)\geq 1$, c'est-à-dire, par la Proposition 3.4.13, le cas où $\text{val}(\mathfrak{M})\geq 1$. Procédons par l'absurde et supposons que $j<\text{ind}(q)$. Écrivons

$$\mathfrak{P}(q)\equiv c_nq^n+\cdots+c_1q+c_0 \mod \mathfrak{M}$$

avec $n<\deg(\mathfrak{M})$. De plus, remarquons que $c_0\neq 0$. En effet, étant donné que $\text{val}(\mathfrak{M})\geq 1$, on sait que $\mathfrak{M}(0)=0$. Par conséquent, on obtient que $c_0\neq 0$. Par hypothèse, on a

$$\sum_{i=0}^{n}c_iq^{i+j}\equiv\sum_{i=0}^{n}c_iq^{i+j+d\text{per}(q)} \mod \mathfrak{M}.$$

Étant donné que $j < \mathrm{ind}(q)$, il existe un entier positif $k$ tel que $j + k = \mathrm{ind}(q) - 1$. De plus, pour tout $m \in \{k+1, \ldots, n\}$, on a $c_m q^{m+j+d\mathrm{per}(q)} \equiv c_m q^{m+j} \mod \mathfrak{M}$. On en tire que

$$\sum_{i=0}^{k} c_i q^{i+j} \equiv \sum_{i=0}^{k} c_i q^{i+j+d\mathrm{per}(q)} \mod \mathfrak{M}.$$

En notant $\mathfrak{R}(q) := \sum_{i=0}^{k} c_i q^{i+j} - \sum_{i=0}^{k} c_i q^{i+j+d\mathrm{per}(q)}$, il existe un polynôme $\mathfrak{Q} \in \mathbb{Z}_p[q]$ tel que

$$\mathfrak{R}(q) = \mathfrak{Q}(q)\mathfrak{M}(q).$$

Étant donné que $c_0 \neq 0$, on sait que $\mathrm{val}(\mathfrak{R}) = j$. De plus, on a par hypothèse

$$\mathrm{val}(\mathfrak{R}) = j < \mathrm{ind}(q) = \mathrm{val}(\mathfrak{M}) \leq \mathrm{val}(\mathfrak{Q}\mathfrak{M}) = \mathrm{val}(\mathfrak{R}),$$

ce qui est absurde. De cette manière, on a $j \geq \mathrm{ind}(q)$. □

**Exemple 3.4.20.** Soient $p = 2$ et le polynôme non constant $\mathfrak{M}(q) = q^2 + q \in \mathbb{Z}_2[q]$. Au vu de l'Exemple 3.4.18, on sait que $\mathrm{ind}(q) = 1$ et $\mathrm{per}(q) = 1$. Considérons à présent le polynôme $\mathfrak{P}(q) = 1 \in \mathbb{Z}_2[q]$ dont le terme constant est non nul. En prenant $j = 0$, on a $q^j\mathfrak{P}(q) \equiv 1 \mod \mathfrak{M}$ et $q^{j+d\mathrm{per}(q)}\mathfrak{P}(q) \equiv q \mod \mathfrak{M}$. Or, étant donné que $1 \not\equiv q \mod \mathfrak{M}$, on a $q^0\mathfrak{P}(q) \not\equiv q^{d\mathrm{per}(q)}\mathfrak{P}(q) \mod \mathfrak{M}$. En prenant $j \geq 1$, on a $q^j\mathfrak{P}(q) \equiv q\mathfrak{P}(q) \mod \mathfrak{M}$. De plus, on a $q^{j+d\mathrm{per}(q)} \equiv q\mathfrak{P}(q) \mod \mathfrak{M}$. Ainsi, si $q^j\mathfrak{P}(q) \equiv q^{j+d\mathrm{per}(q)}\mathfrak{P}(q) \mod \mathfrak{M}$, alors $j \geq 1 = \mathrm{ind}(q)$.

### 3.4.2 Déformations et langages acceptés par un $p$-groupe

Nous faisons ici le lien entre les $q$-déformations de coefficients binomiaux de mots et les langages acceptés par un $p$-groupe. On définit une relation d'équivalence sur $A^*$.

**Définition 3.4.21.** Soient $u \in A^*$ et $\mathfrak{M} \in \mathbb{Z}_p[q]$. Deux mots finis $w_1, w_2 \in A^*$ sont $(u, \mathfrak{M})$-*binomiaux équivalents* si pour tout $v \in \mathrm{Fac}(u) \setminus \{\varepsilon\}$, on a

$$\binom{w_1}{v}_q \equiv \binom{w_2}{v}_q \mod \mathfrak{M}.$$

Dans ce cas, on note $w_1 \sim_{u,\mathfrak{M}} w_2$.

**Exemple 3.4.22.** Soient $A = \{a, b\}$, $u = ab \in A^*$ et $p = 3$. Considérons le polynôme $\mathfrak{M}(q) = q^2 + q + 1 \in \mathbb{Z}_3[q]$. Remarquons que $\mathrm{Fac}(u) \setminus \{\varepsilon\} = \{a, b, ab\}$. Les deux mots $w_1$ et $w_2$ sont $(ab, q^2 + q + 1)$-binomiaux équivalents si

- $\binom{w_1}{a}_q \equiv \binom{w_2}{a}_q \mod q^2 + q + 1$,
- $\binom{w_1}{b}_q \equiv \binom{w_2}{b}_q \mod q^2 + q + 1$,
- $\binom{w_1}{ab}_q \equiv \binom{w_2}{ab}_q \mod q^2 + q + 1$.

Montrons que les mots $w_1 = abba$ et $w_2 = baab$ sont $(ab, q^2+q+1)$-binomiaux équivalents. Les calculs suivants sont faits au moyen du Théorème 3.2.1.

- Remarquons qu'on a $\binom{abba}{a}_q = q^3 + 1 = (q^2+q+1)\cdot(q-1)+2$. De plus, on a $\binom{baab}{a}_q = q^2+q = (q^2+q+1)\cdot 1 - 1$. Ainsi, étant donné qu'on travaille dans $\mathbb{Z}_3$, on a
$$\binom{abba}{a}_q \equiv \binom{baab}{a}_q \mod q^2+q+1.$$
- Remarquons qu'on a $\binom{abba}{b}_q = q^2+q = (q^2+q+1)\cdot 1 - 1$. De plus, on a $\binom{baab}{b}_q = q^3+1 = (q^2+q+1)\cdot(q-1)+2$. Ainsi, étant donné qu'on travaille dans $\mathbb{Z}_3$, on a
$$\binom{abba}{b}_q \equiv \binom{baab}{b}_q \mod q^2+q+1.$$
- Remarquons qu'on a $\binom{abba}{ab}_q = q^4+q^3 = (q^2+q+1)\cdot(q^2-1)+q+1$. De plus, on a $\binom{baab}{ab}_q = q+1 = (q^2+q+1)\cdot 0 + q + 1$. Ainsi, on a
$$\binom{abba}{ab}_q \equiv \binom{baab}{ab}_q \mod q^2+q+1.$$

Par définition, on obtient que $abba \sim_{ab,q^2+q+1} baab$.

**Remarque 3.4.23.** Il faut considérer tous les facteurs de $u$ et calculer les $q$-déformations des coefficients binomiaux de mots réduits modulo $\mathfrak{M}$. Par conséquent, le nombre de classes d'équivalences est majoré par $\#\mathbb{F}^{(\#\mathrm{Fac}(u)-1)}$. En particulier, la relation d'équivalence $\sim_{u,\mathfrak{M}}$ est d'indice fini dans $A^*$.

**Remarque 3.4.24.** Soit $u \in A^*$. Si $t \in A^*$ est un facteur de $u$, on sait que $\mathrm{Fac}(t) \subseteq \mathrm{Fac}(u)$. Par conséquent, si $w_1, w_2 \in A^*$ sont tels que $w_1 \sim_{u,\mathfrak{M}} w_2$, alors $w_1 \sim_{t,\mathfrak{M}} w_2$.

**Exemple 3.4.25.** Soient $A = \{a, b\}$, $u = ab \in A^*$ et $p = 3$. Considérons le polynôme $\mathfrak{M}(q) = q^2+q+1 \in \mathbb{Z}_3[q]$. Étant donné que $\mathbb{F} = \mathbb{Z}_3[q]/\langle q^2+q+1\rangle$, on obtient directement que
$$\mathbb{F} = \{aq+b : a, b \in \mathbb{Z}_3\} = \{0, 1, 2, q, q+1, q+2, 2q, 2q+1, 2q+2\}.$$
De plus, on a $\mathrm{Fac}(u)\setminus\{\varepsilon\} = \{a, b, ab\}$. Par la Remarque 3.4.23, on sait qu'il y a au plus $9^{4-1} = 729$ classes d'équivalences. Cependant, en utilisant le programme annexe, on obtient directement qu'il y a 27 classes d'équivalences, avec des représentants de longueur au plus 6. Par exemple, le mot $w = aababb$ est le plus court tel que
$$\binom{w}{a}_q \equiv 2q+1 \mod q^2+q+1, \binom{w}{b}_q \equiv q+2 \mod q^2+q+1 \text{ et } \binom{w}{ab}_q \equiv 2q \mod q^2+q+1.$$
Notons ces classes d'équivalences dans l'ordre lexicographique, c'est-à-dire $C_1 = (0,0,0), C_2 = (0,1,0), C_3 = (0, q+1, 0), C_4 = (1,0,0), C_5 = (1,2,0), \ldots, C_{27} = (2q+2, 2q+2, 2)$. Pour $i \in \{1, \ldots, 27\}$, notons $w_i$ un représentant de la classe d'équivalence $C_i$. Dans ce cas, toujours au moyen du programme annexe, on peut remarquer que $w_1 = \varepsilon, w_2 = b, w_3 = bb, w_4 = a, w_5 = bba, \ldots, w_{26} = babb, w_{27} = aabaa$.

**Remarque 3.4.26.** Dans certains cas, le nombre maximal de classes d'équivalences peut être atteint. En effet, en considérant l'alphabet $A = \{a, b\}$, $u = ab \in A^*$, $p = 2$ et le polynôme $\mathfrak{M}(q) = q^2 + 1$, on obtient qu'il y a exactement $4^{4-1} = 64$ classes d'équivalences, le maximum possible, avec des représentants de longueur au plus 8 [12, Example 7.10.].

La relation d'équivalence $\sim_{u,\mathfrak{M}}$ n'est pas toujours une congruence.

**Remarque 3.4.27.** Soient $u \in A^*$ et $\mathfrak{M} \in \mathbb{Z}_p[q]$. La relation d'équivalence $\sim_{u,\mathfrak{M}}$ n'est pas toujours une congruence. Par exemple, en prenant $p = 2$ et $A = \{a, b\}$, on remarque que $a \sim_{a,q^2+1} abaa$ et $ba \sim_{a,q^2+1} a$ mais $aba \not\sim_{a,q^2+1} abaaa$. En effet,

- montrons que $a \sim_{a,q^2+1} abaa$. Remarquons que $\mathrm{Fac}(a)\setminus\{\varepsilon\} = \{a\}$. De plus, on a $\binom{a}{a}_q = 1 = (q^2+1)\cdot 0 + 1$. Enfin, on a $\binom{abaa}{a}_q = q^3 + q + 1 = (q^2+1)\cdot q + 1$. Au final, on obtient donc que
$$\binom{a}{a}_q \equiv \binom{abbbaa}{a}_q \mod q^2 + 1.$$
Ainsi, on a $a \sim_{a,q^2+1} abaa$.
- montrons que $ba \sim_{a,q^2+1} a$. Remarquons que $\binom{ba}{a}_q = 1$ et $\binom{a}{a}_q = 1$. Au final, on a
$$\binom{ba}{a}_q \equiv \binom{a}{a}_q \mod q^2 + 1.$$
Ainsi, on a $ba \sim_{a,q^2+1} a$.
- montrons que $aba \not\sim_{a,q^2+1} abaaa$. On a $\binom{aba}{a}_q = q^2 + 1 = (q^2+1)\cdot 1 + 0$. De plus, on a $\binom{abaaa}{a}_q = q^4 + q^2 + q + 1 = (q^2+1)\cdot q^2 + q + 1$. Étant donné qu'on travaille dans $\mathbb{Z}_2$, on obtient que
$$\binom{ab}{a}_q \not\equiv \binom{abbbaabb}{a}_q \mod q^2 + 1.$$
Ainsi, on a $aba \not\sim_{a,q^2+1} abaaa$.

La relation d'équivalence $\sim_{u,\mathfrak{M}}$ n'est donc pas une congruence.

Pour qu'un langage $L$ soit reconnaissable, il doit par définition être reconnu par un monoïde fini, c'est-à-dire qu'il doit exister un monoïde $M$ tel $L = \mu^{-1}(S)$ où $\mu : A^* \to M$ est un morphisme de monoïdes et où $S$ est un sous-ensemble de $M$. Par conséquent, nous cherchons une congruence $\equiv$ sur $A^*$ d'indice fini qui est un raffinement de $\sim_{u,\mathfrak{M}}$ de sorte que $A^*/\equiv$ est un monoïde fini. Pour ce faire, nous introduisons quelques notions dont l'utilité deviendra claire dans les résultats suivants.

**Définition 3.4.28.** Soient $l \geq 1$ un naturel et $w_1, w_2 \in A^*$. On définit la congruence [6] $\sim_l$ par $w_1 \sim_l w_2$ si et seulement si $|w_1| \equiv |w_2| \mod l$.

6. Montrons qu'il s'agit bien d'une congruence. Montrons que si $w_1 \sim_l w_2$, alors $xw_1y \sim_l xw_2y$ pour tous $x, y \in A^*$. Rappelons que $|xwy| = |x| + |w| + |y|$. Pour montrer que $xw_1y \sim_l xw_2y$, il faut montrer que $|xw_1y| - |xw_2y| \equiv 0 \mod l$. Or, on sait que $|xw_1y| - |xw_2y| = |w_1| - |w_2|$. Par hypothèse, on sait que $|w_1| - |w_2| \equiv 0 \mod l$. De cette manière, on obtient que $|xw_1y| - |xw_2y| \equiv 0 \mod l$, ce qui donne la conclusion que $\sim_l$ est une congruence.

**Exemple 3.4.29.** Soient $l = 3$ et $A = \{a, b\}$. Étant donné que $|abbab| = 5$ et que $|bb| = 2$, on obtient que $abbab \sim_3 bb$.

**Définition 3.4.30.** Soient $u \in A^*$ et $\mathfrak{M} \in \mathbb{Z}_p[q]$. Si $w \in A^*$ est un mot et $v \in \mathrm{Fac}(u)$ tel que $av \in \mathrm{Fac}(u)$ pour une lettre $a \in A$, on définit

$$l_{w,v} := \mathrm{val}\left(\binom{w}{v}_q \mod \mathfrak{M}\right).$$

On définit ensuite

$$l_w := \min\{l_{w,v} - |v| : \exists a \in A \text{ tel que } av \in \mathrm{Fac}(u)\}.$$

**Remarque 3.4.31.** On remarque que la quantité $l_{w,v}$ est la valuation du reste de la division euclidienne de $\binom{w}{v}_q$ par $\mathfrak{M}$. En particulier, on obtient que $l_{w,v} < \deg(\mathfrak{M})$.

Le lemme suivant donne des conditions nécessaires pour qu'une congruence soit un raffinement de la relation d'équivalence $\sim_{u,\mathfrak{M}}$.

**Lemme 3.4.32.** *Soient $u \in A^*$, $\mathfrak{M} \in \mathbb{Z}_p[q]$ et une congruence $\simeq$ qui est un raffinement de la relation d'équivalence $\sim_{u,\mathfrak{M}}$. Si $w_1, w_2 \in A^*$ sont deux mots tels que $w_1 \simeq w_2$, alors soit $|w_1| = |w_2|$, soit*

- $|w_1|, |w_2| \geq \mathrm{ind}(q)$,
- $w_1 \sim_{\mathrm{per}(q)} w_2$ *et*
- $\min\{l_{w_1} + |w_1|, l_{w_2} + |w_2|\} \geq \mathrm{ind}(q)$.

*Démonstration.* Soit $a \in A$ une lettre apparaissant dans le mot $u$. Étant donné que $\simeq$ est un raffinement de $\sim_{u,\mathfrak{M}}$ et que $w_1 \simeq w_2$, on sait que $w_1 \sim_{u,\mathfrak{M}} w_2$. En particulier, on a $\binom{w_1}{a}_q \equiv \binom{w_2}{a}_q \mod \mathfrak{M}$. Étant donné que $\simeq$ est une congruence et que $a \simeq a$, on obtient que $aw_1 \simeq aw_2$. Étant donné qu'il s'agit d'un raffinement de $\sim_{u,\mathfrak{M}}$, on a $aw_1 \sim_{u,\mathfrak{M}} aw_2$. En particulier, on a $\binom{aw_1}{a}_q \equiv \binom{aw_2}{a}_q \mod \mathfrak{M}$, c'est-à-dire, par le Théorème 3.2.1, que

$$q^{|w_1|} + \binom{w_1}{a}_q \equiv q^{|w_2|} + \binom{w_2}{a}_q \mod \mathfrak{M}.$$

Étant donné que $\binom{w_1}{a}_q \equiv \binom{w_2}{a}_q \mod \mathfrak{M}$, on obtient que

$$q^{|w_1|} \equiv q^{|w_2|} \mod \mathfrak{M}.$$

Par la Remarque 3.4.10, on obtient que soit $|w_1| = |w_2|$, soit

- $|w_1|, |w_2| \geq \mathrm{ind}(q)$ et
- $|w_1| \equiv |w_2| \mod \mathrm{per}(q)$, c'est-à-dire que $w_1 \sim_{\mathrm{per}(q)} w_2$.

Dans le deuxième cas, il reste à montrer que $\min\{l_{w_1}+|w_1|, l_{w_2}+|w_2|\} \geq \mathrm{ind}(q)$. Sans perte de généralité, supposons que $|w_2| > |w_1|$. Étant donné que $w_1 \sim_{\mathrm{per}(q)} w_2$, on sait que $|w_1| \equiv |w_2| \mod \mathrm{per}(q)$, c'est-à-dire que $|w_2| = |w_1| + d\mathrm{per}(q)$ où $d \geq 0$ est un naturel. Étant donné que $w_1 \simeq w_2$, pour tout $v \in \mathrm{Fac}(u)$, les restes de divisions euclidiennes de $\binom{w_1}{v}_q$ par $\mathfrak{M}$ et de $\binom{w_2}{v}_q$ par $\mathfrak{M}$ sont égaux. Notons le $R$. Ceci implique que $l_{w_1,v} = l_{w_2,v}$ pour tout mot $v$ tel que $av \in \mathrm{Fac}(u)$ pour une lettre $a \in A$. Procédons par l'absurde et supposons que $l_{w_1,v} + |w_1| - |v| < \mathrm{ind}(q)$ pour un mot $v$ tel que $av \in \mathrm{Fac}(u)$. Posons $l := \mathrm{val}(R) = l_{w_1,v} = l_{w_2,v}$. Il est à noter que $l \geq 0$ et que si $|w_1| - |v| < 0$, alors $\binom{w_1}{v}_q = 0$ par la Remarque 3.1.5 et $l_{w_1,v} = +\infty$. Ainsi, $l + |w_1| - |v|$ est toujours strictement positif. Par définition de $R$ et de $l$, on sait que $\frac{R}{q^l}$ est un polynôme. Soit $a \in A$ tel que $av \in \mathrm{Fac}(u)$. D'une part, par le Corollaire 3.2.6, on a

$$\begin{aligned}\binom{aw_1}{av}_q &= \sum_{\substack{v_1,v_2\in A^*\\ av=v_1v_2}} q^{|v_1|(|w_1|-|v_2|)}\binom{a}{v_1}_q\binom{w_1}{v_2}_q\\ &= \binom{w_1}{av}_q + q^{|w_1|-|v|}\binom{w_1}{v}_q\\ &\equiv \binom{w_1}{av}_q + q^{l+|w_1|-|v|}\frac{R}{q^l} \mod \mathfrak{M},\end{aligned}$$

où nous avons utilisé le fait que $\binom{a}{v_1}_q = 1$ si $v_1 = \varepsilon$ ou $v_1 = a$ et $\binom{a}{v_1}_q = 0$ sinon. D'autre part, en utilisant un argument similaire, on obtient que

$$\binom{aw_2}{av}_q \equiv \binom{w_2}{av}_q + q^{l+|w_2|-|v|}\frac{R}{q^l} \mod \mathfrak{M}.$$

Étant donné que $\simeq$ est une congruence et que $w_1 \simeq w_2$, on sait que $aw_1 \simeq aw_2$. La congruence $\simeq$ étant un raffinement de $\sim_{u,\mathfrak{M}}$, on sait également que $aw_1 \sim_{u,\mathfrak{M}} aw_2$. De cette manière, vu que $av \in \mathrm{Fac}(u)$, on obtient que $\binom{aw_1}{av}_q \equiv \binom{aw_2}{av}_q \mod \mathfrak{M}$. En utilisant les deux relations ci-dessus, étant donné que $\binom{w_1}{av}_q \equiv \binom{w_2}{av}_q \mod \mathfrak{M}$, on en tire que

$$q^{l+|w_2|-|v|}\frac{R}{q^l} = q^{l+|w_1|+d\mathrm{per}(q)-|v|}\frac{R}{q^l} \equiv q^{l+|w_1|-|v|}\frac{R}{q^l} \mod \mathfrak{M}.$$

Étant donné que $l + |w_1| - |v| < \mathrm{ind}(q)$, cela contredit le Lemme 3.4.19. Étant donné que $|w_1| < |w_2|$, on en tire que $\min\{l_{w_1}+|w_1|, l_{w_2}+|w_2|\} \geq \mathrm{ind}(q)$, ce qui nous donne la conclusion. □

**Notation 3.4.33.** Dans la suite, si $k$ est un entier, nous noterons $[k]_p$ la valeur de $k$ réduite modulo $p$.

La remarque suivante sera utile pour le lemme ci-dessous.

**Remarque 3.4.34.** Rappelons que, par la Proposition 3.4.13, on a $\mathrm{ind}(q) = \mathrm{val}(\mathfrak{M})$. En particulier, $\mathrm{ind}(q) \leq \deg(\mathfrak{M})$. De cette manière, si $|w| < \mathrm{ind}(q)$, alors $q^{|w|-1} + \cdots + q + 1$ est degré plus petit que $\deg(\mathfrak{M})$.

**Lemme 3.4.35.** *Soit $w \in A^*$.*

*(i) Si $|w| < \mathrm{ind}(q)$, alors*

$$\sum_{a\in A} \binom{w}{a}_q \equiv q^{|w|-1} + \cdots + q + 1 \mod \mathfrak{M}.$$

*(ii) Si $|w| = \mathrm{ind}(q) + k \cdot \mathrm{per}(q) + r$ pour un naturel $k \geq 0, r \in \{0, \ldots, \mathrm{per}(q) - 1\}$, alors*

$$\sum_{a\in A} \binom{w}{a}_q \equiv \sum_{j=\mathrm{ind}(q)+r}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} [k]_p q^j + \sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+r-1} [k+1]_p q^j + \sum_{j=0}^{\mathrm{ind}(q)-1} q^j \mod \mathfrak{M}.$$

*En particulier, la suite $(\binom{n}{1}_q \mod \mathfrak{M})_{n\geq 0}$ est périodique à partir de $\mathrm{ind}(q)$ et l'entier $\mathrm{per}(q) \cdot p$ est un multiple de la plus petite période.*

*Démonstration.* *(i)* Supposons que $|w| < \mathrm{ind}(q)$. Étant donné que la somme s'effectue sur toutes les lettres de $A$, on recouvrira le mot tout entier $w$. Par le Théorème 3.2.1, on obtient donc que

$$\sum_{a\in A} \binom{w}{a}_q = q^{|w|-1} + \cdots + q + 1.$$

Le polynôme obtenu est déjà réduit modulo $\mathfrak{M}$ car son degré est $|w| < \mathrm{ind}(q) \leq \deg(\mathfrak{M})$.

*(ii)* Soit $a \in A$. Supposons que la lettre $a$ possède $t$ occurrences dans $w$, données par les positions (en commençant par la droite) $i_t > \cdots > i_1 \geq 1$. Dans ce cas, par le Théorème 3.2.1, on a

$$\binom{w}{a}_q = \sum_{j=1}^{t} q^{i_j - 1}.$$

Étant donné que $q^{\mathrm{ind}(q)+\mathrm{per}(q)} \equiv q^{\mathrm{ind}(q)} \mod \mathfrak{M}$, on a

$$q^{\mathrm{ind}(q)+k\cdot\mathrm{per}(q)+r} \equiv q^{\mathrm{ind}(q)+r} \mod \mathfrak{M}. \tag{3.8}$$

Ainsi, on a

$$\binom{w}{a}_q = \sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} c_j q^j + \sum_{j=0}^{\mathrm{ind}(q)-1} d_j q^j, \tag{3.9}$$

où $c_i$ est le nombre réduit modulo $p$ de fois que $a$ apparaît dans $w$ dont les positions sont plus grandes que $\mathrm{ind}(q)$ et congruent à $i+1$ modulo $\mathrm{per}(q)$ pour tout $i \in \{\mathrm{ind}(q), \ldots, \mathrm{ind}(q) + \mathrm{per}(q) - 1\}$ et $d_i = \delta_{a,w_{i+1}}$ pour tout $i \in \{0, \ldots, \mathrm{ind}(q) - 1\}$. En effectuant la somme sur toutes les lettres de $a \in A$, on obtient la conclusion.

□

**Exemple 3.4.36.** Soient $p = 2$ et $\mathfrak{M}(q) = q^2 + q + 1$. Étant donné que $q^3 = (q-1) \cdot (q^2+q+1) + 1 \equiv 1 \mod \mathfrak{M}$, on obtient que $\mathrm{per}(q) = 3$. De plus, étant donné que $q^0 \equiv 1 \mod \mathfrak{M}$, on obtient que $\mathrm{ind}(q) = 0$. Soient $A = \{a, b, c\}$ et $w = abcbacba \in A^*$. Au vu de la relation (3.9), étant donné qu'il y a $2 \equiv 0 \mod 2$ lettres $a$ apparaissant dans $w$ dans les positions congruentes à $1 \mod 3$, qu'il y a $1 \equiv 1 \mod 2$ lettre $a$ apparaissant dans $w$ dans les positions congruentes à $2 \mod 3$ et qu'il y a $0 \equiv 0 \mod 2$ lettre $a$ apparaissant dans $w$ dans les positions congruentes à $3 \mod 3$, remarquons que

$$\begin{aligned}\binom{abcbacba}{a}_q &= q^7 + q^3 + 1 = (q^5 - q^4 + q^2 - 1) \cdot (q^2+q+1) + q + 2 \\ &\equiv q \mod q^2+q+1.\end{aligned}$$

De plus, toujours en utilisant la relation (3.9), on a

$$\begin{aligned}\binom{abcbacba}{b}_q &= q^6 + q^4 + q(q^4 - q^3 + q^2 - 1) \cdot (q^2+q+1) + 2q + 1 \\ &\equiv 1 \mod q^2+q+1.\end{aligned}$$

Enfin, en utilisant la relation (3.9), on a

$$\begin{aligned}\binom{abcbacba}{c}_q &= q^5 + q^2 = (q^3 - q^2 + 2) \cdot (q^2+q+1) - 2q - 2 \\ &\equiv 0 \mod q^2+q+1.\end{aligned}$$

Étant donné que $|w| = 0 + 2 \cdot 3 + 2$, on obtient par le Lemme 3.4.35 que

$$\begin{aligned}\sum_{\sigma \in A} \binom{abcbacba}{\sigma}_q &\equiv \underbrace{\sum_{j=2}^{2} [2]_2 \cdot q^j}_{=0} + \sum_{j=0}^{1} [3]_2 \cdot q^j + \underbrace{\sum_{j=0}^{-1} q^j}_{=0} \mod q^2+q+1 \\ &\equiv q+1 \mod q^2+q+1.\end{aligned}$$

Par le Lemme 3.4.35, on sait que la suite $(\binom{n}{1}_q \mod q^2+q+1)_{n \geq 0}$ est périodique d'indice $\mathrm{ind}(q) = 0$ et on sait que $\mathrm{per}(q) \cdot p = 3 \cdot 2 = 6$ est un multiple de la plus petite période. Pour les mots de longueurs plus grandes, la suite $(\binom{n}{1}_q \mod q^2+q+1)_{n \geq 0}$ est périodique de période 3

$$0, 1, 1+q, 0, 1, 1+q, \ldots.$$

**Proposition 3.4.37.** *Soient $u \in A^*$, $\mathfrak{M} \in \mathbb{Z}_p[q]$ et $\simeq$ une congruence qui est un raffinement de $\sim_{u,\mathfrak{M}}$. Si $q$ n'est pas inversible dans $\mathbb{F}$, alors le monoïde $A^*/\simeq$ n'est pas un groupe. En particulier, seul l'élément identité est inversible.*

*Démonstration.* Montrons que $A^*/\simeq$ possède des éléments qui ne sont pas inversibles, ce qui permettra de conclure qu'il ne s'agit pas d'un groupe. Étant donné que $\varepsilon$ est l'élément neutre de $A^*$, il est clair que $[\varepsilon]$ est l'identité du monoïde $A^*/\simeq$. Étant donné que $q$ n'est pas inversible, on sait par la Remarque 3.4.10 que $\mathrm{ind}(q) \geq 1$. Par le Lemme 3.4.32, étant donné que $\mathrm{ind}(q) \geq 1$, on obtient que l'élément $[\varepsilon]$ est un singleton. Pour tous mots $w \in A^+$ et $x \in A^*$, la classe $[w] \cdot [x] = [wx]$ est différente de $[\varepsilon]$. En effet, si $[wx] = [\varepsilon]$, alors $wx = \varepsilon$, ce qui est impossible car $w$ est non vide. De cette manière, il n'existe pas de mots $x \in A^*$ tel que $[w] \cdot [x] = [\varepsilon]$, ce qui permet de conclure que $w$ n'est pas inversible. Ainsi, $A^*/\simeq$ n'est pas un groupe, ce qui nous permet de conclure. □

Il est tout de même intéressant de se pencher sur la congruence la moins fine qui est un raffinement de $\sim_{u,\mathfrak{M}}$. Le résultat ci-dessous, combiné au Lemme 3.4.32 nous permet de dicter les conditions définissant cette congruence.

**Définition 3.4.38.** Soient $u \in A^*$ et $\mathfrak{M} \in \mathbb{Z}_p[q]$. Pour tous mots $w_1, w_2 \in A^*$, on définit la relation $\equiv_{u,\mathfrak{M}}$ par $w_1 \equiv_{u,\mathfrak{M}} w_2$ si $w_1 \sim_{u,\mathfrak{M}} w_2$ et soit $|w_1| = |w_2|$, soit

- $|w_1|, |w_2| \geq \mathrm{ind}(q)$,
- $w_1 \sim_{\mathrm{per}(q)} w_2$ et
- $\min\{l_{w_1} + |w_1|, l_{w_2} + |w_2|\} \geq \mathrm{ind}(q)$.

**Proposition 3.4.39.** *Soient $u \in A^*$ et $\mathfrak{M} \in \mathbb{Z}_p[q]$. Alors, la relation $\equiv_{u,\mathfrak{M}}$ est une congruence. De plus, elle est la moins fine qui est un raffinement de $\sim_{u,\mathfrak{M}}$.*

*Démonstration.* Montrons que $\equiv_{u,\mathfrak{M}}$ est une congruence. Soient $w_1, w_2, y_1, y_2 \in A^*$ des mots tels que $w_1 \equiv_{u,\mathfrak{M}} w_2$ et $y_1 \equiv_{u,\mathfrak{M}} y_2$. Montrons que $y_1 w_1 \equiv_{u,\mathfrak{M}} y_2 w_2$. Soit $v \in \mathrm{Fac}(u)$. Par le Corollaire 3.2.6, on a

$$\begin{aligned}\binom{xy}{v}_q &= \sum_{\substack{v_1,v_2 \in A^* \\ v = v_1 v_2}} q^{|v_1|(|w_1|-|v_2|)} \binom{y_1}{v_1}_q \binom{w_1}{v_2}_q \\ &= \binom{w_1}{v}_q + q^{|v||w_1|} \binom{y_1}{v}_q + \sum_{\substack{v_1,v_2 \in A^+ \\ v = v_1 v_2}} q^{|v_1|(|w_1|-|v_2|)} \binom{y_1}{v_1}_q \binom{w_1}{v_2}_q.\end{aligned}$$

Étant donné que $v_1$ et $v_2$ sont des facteurs de $v$, on sait qu'ils sont également des facteurs de $u$. De plus, le fait que $w_1 \equiv_{u,\mathfrak{M}} w_2$ et $y_1 \equiv_{u,\mathfrak{M}} y_2$ impliquent respectivement que $w_1 \sim_{u,\mathfrak{M}} w_2$ et $y_1 \sim_{u,\mathfrak{M}} y_2$. De cette manière, on a

$$\binom{y_1}{v_1}_q \equiv \binom{y_2}{v_1}_q \mod \mathfrak{M} \qquad \text{et} \qquad \binom{w_1}{v_2}_q \equiv \binom{w_2}{v_2}_q \mod \mathfrak{M}.$$

De plus, étant donné que $w_1 \equiv_{u,\mathfrak{M}} w_2$, on sait que soit $|w_1| = |w_2|$, soit $|w_1|, |w_2| \geq \mathrm{ind}(q)$ et $|w_1| \equiv |w_2| \mod \mathrm{per}(q)$. Ainsi, on a par la relation (3.8) que

$$q^{|v_1||w_1|} \equiv q^{|v_1||w_2|} \mod \mathfrak{M}.$$

Notons $R$ le reste de la division euclidienne de $\binom{w_1}{v_2}_q$ par $\mathfrak{M}$ de sorte que $\frac{R}{q^{l_{w_1,v_2}}}$ est un polynôme. On obtient donc que

$$\sum_{\substack{v_1,v_2\in A^+\\ v=v_1v_2}} q^{|v_1|(|w_1|-|v_2|)}\binom{y_1}{v_1}_q\binom{w_1}{v_2}_q \equiv \sum_{\substack{v_1,v_2\in A^+\\ v=v_1v_2}} q^{(|v_1|-1)(|w_1|-|v_2|)+l_{w_1,v_2}+|w_1|-|v_2|}\binom{y_1}{v_1}_q\frac{R}{q^{l_{w_1,v_2}}} \mod \mathfrak{M}.$$

Étant donné que $l_{w_1,v_2}+|w_1|-|v_2|\geq \mathrm{ind}(q)$, alors en supposant que $|w_2|=|w_1|+d\mathrm{per}(q)$, on a

$$\begin{aligned} q^{(|v_1|-1)(|w_1|-|v_2|)+l_{w_1,v_2}+|w_1|-|v_2|} &\equiv q^{(|v_1|-1)(|w_1|-|v_2|)+l_{w_2,v_2}+|w_1|-|v_2|+d|v_1|\mathrm{per}(q)} \mod \mathfrak{M}\\ &\equiv q^{|v_1|(|w_2|-|v_2|)+l_{w_2,v_2}} \mod \mathfrak{M}, \end{aligned}$$

où $l_{w_1,v_2}=l_{w_2,v_2}$ provient du fait que $w_1\equiv_{u,\mathfrak{M}} w_2$. Finalement, on obtient que

$$\sum_{\substack{v_1,v_2\in A^+\\ v=v_1v_2}} q^{|v_1|(|w_1|-|v_2|)}\binom{y_1}{v_1}_q\binom{w_1}{v_2}_q \equiv \sum_{\substack{v_1,v_2\in A^+\\ v=v_1v_2}} q^{|v_1|(|w_2|-|v_2|)}\binom{y_2}{v_1}_q\binom{w_2}{v_2}_q \mod \mathfrak{M}.$$

Par conséquent, on a $\binom{y_1w_1}{v}_q\equiv\binom{y_2w_2}{v}_q \mod \mathfrak{M}$ pour tout facteur $v$ de $u$. On obtient donc que $y_1w_1\equiv_{u,\mathfrak{M}} y_2w_2$, ce qui permet de conclure que $\equiv_{u,\mathfrak{M}}$ est une congruence.

Le fait que $\equiv_{u,\mathfrak{M}}$ est la congruence la moins fine qui est un raffinement de $\sim_{u,\mathfrak{M}}$ vient du Lemme 3.4.32. □

Soient $u\in A^*$ et $\mathfrak{M}\in\mathbb{Z}_p[q]$. Nous nous intéressons à présent à deux cas où la congruence $\equiv_{u,\mathfrak{M}}$ a une expression plus simple. Soient $w_1,w_2\in A^*$.

1. Le premier cas est celui où le polynôme $q$ est inversible dans $\mathbb{F}$. Par la Remarque 3.4.10, on sait que $\mathrm{ind}(q)=0$. De cette manière, les deux conditions
   - ◇ $|w_1|,|w_2|\geq\mathrm{ind}(q)$,
   - ◇ $\min\{l_{w_1}+|w_1|,l_{w_2}+|w_2|\}\geq\mathrm{ind}(q)$,

   sont toujours vérifiées. Cela résulte du fait que, pour tout mot $w\in A^*$, on a $|w|\geq 0$ et $l_w+|w|=l_{w,v}-|v|+|w|\geq 0$ pour un facteur $v$ de $u$. Par conséquent, on a
   $$w_1\equiv_{u,\mathfrak{M}} w_2 \iff w_1\sim_{u,\mathfrak{M}} w_2 \text{ et } w_1\sim_{\mathrm{per}(q)} w_2.$$
2. Le deuxième cas est celui où le mot $u$ contient toutes les lettres de $A$. Comme nous pourrons le remarquer ci-dessous, l'équivalence $w_1\sim_{u,\mathfrak{M}} w_2$ implique la congruence $w_1\sim_{\mathrm{per}(q)} w_2$. Dans ce cas, on peut remarquer que $w_1\equiv_{u,\mathfrak{M}} w_2$ si et seulement si $w_1\sim_{u,\mathfrak{M}} w_2$ et soit $|w_1|=|w_2|$, soit
   - ◇ $|w_1|,|w_2|\geq\mathrm{ind}(q)$ et
   - ◇ $\min\{l_{w_1}+|w_1|,l_{w_2}+|w_2|\}\geq\mathrm{ind}(q)$.

Montrons que l'équivalence $w_1 \sim_{u,\mathfrak{M}} w_2$ implique la congruence $w_1 \sim_{\mathrm{per}(q)} w_2$. Supposons que $w_1 \sim_{u,\mathfrak{M}} w_2$, c'est-à-dire que

$$\binom{w_1}{v}_q \equiv \binom{w_2}{v}_q \mod \mathfrak{M}$$

pour tout $v \in \mathrm{Fac}(u)$. Étant donné que toute lettre de $A$ apparaît dans $u$, on sait que pour toute lettre $a \in A$, on a $a \in \mathrm{Fac}(u)$. De cette manière, on a $\binom{w_1}{a}_q \equiv \binom{w_2}{a}_q \mod \mathfrak{M}$ pour tout $a \in A$. On en tire que

$$\sum_{a\in A} \binom{w_1}{a}_q \equiv \sum_{a\in A} \binom{w_2}{a}_q \mod \mathfrak{M}. \tag{3.10}$$

- Premièrement, supposons que le plus petit mot entre $w_1$ et $w_2$ soit tel que sa longueur est strictement plus petite que $\mathrm{ind}(q)$. Sans perte de généralité, supposons que $|w_1| < \mathrm{ind}(q)$. Par le Lemme 3.4.35, on obtient que

$$\sum_{a\in A} \binom{w_1}{a}_q \equiv q^{|w_1|-1} + \cdots + 1 \mod \mathfrak{M}.$$

  Remarquons que si $|w_2| > |w_1|$, alors $\sum_{a\in A} \binom{w_2}{a}_q$ contient plus de termes, ce qui contredit la relation (3.10). Ainsi, on a $|w_2| \leq |w_1|$. De la même manière, on obtient que $|w_1| \leq |w_2|$. Ainsi, on a $|w_1| = |w_2|$. Par conséquent, on a bien $w_1 \sim_{\mathrm{per}(q)} w_2$.
- Deuxièmement, supposons que $w_1$ et $w_2$ soient tels que leur longueur est au moins $\mathrm{ind}(q)$. Sans perte de généralité, supposons que $|w_1| < |w_2|$. Étant donné que $|w_1| \equiv |w_2| \mod 1$, il est clair que si $\mathrm{per}(q) = 1$, on a bien $w_1 \sim_{\mathrm{per}(q)} w_2$. Supposons donc que $\mathrm{per}(q) \geq 2$. Procédons par l'absurde et supposons que $w_1 \not\sim_{\mathrm{per}(q)} w_2$. Étant donné que $|w_1| \not\equiv |w_2| \mod \mathrm{per}(q)$, on a $|w_i| = \mathrm{ind}(q) + k_i \cdot \mathrm{per}(q) + r_i$, avec $k_i \geq 0$ et $r_i \in \{0, \ldots, \mathrm{per}(q) - 1\}$ pour $i \in \{1, 2\}$. Les deux cas étant similaires, supposons sans perte de généralité que $r_2 > r_1$. Par le Lemme 3.4.35, on sait que la différence $\sum_{a\in A} \binom{w_2}{a}_q - \binom{w_1}{a}_q$, est équivalente à

$$\sum_{j=\mathrm{ind}(q)+r_2}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} [k_2-k_1]_p q^j + \sum_{j=\mathrm{ind}(q)+r_1}^{\mathrm{ind}(q)+r_2-1} [k_2-k_1+1]_p q^j + \sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+r_1-1} [k_2-k_1]_p q^j \mod \mathfrak{M}.$$

  En utilisant la relation (3.10), on sait que cette différence est nulle modulo $\mathfrak{M}$. Par conséquent, on a

$$\begin{aligned} 0 &\equiv \sum_{a\in A} \binom{w_2}{a}_q - \binom{w_1}{a}_q \\ &\equiv [k_2 - k_1]_p \sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} q^j + \sum_{j=\mathrm{ind}(q)+r_1}^{\mathrm{ind}(q)+r_2-1} [1]_p q^j \mod \mathfrak{M}. \end{aligned} \tag{3.11}$$

En multipliant la première somme du membre de droite par $q-1$, on obtient [7]

$$(q-1)\sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} q^j = q^{\mathrm{ind}(q)}(q^{\mathrm{per}(q)}-1)$$
$$= q^{\mathrm{ind}(q)+\mathrm{per}(q)} - q^{\mathrm{ind}(q)} \equiv 0 \mod \mathfrak{M}. \tag{3.12}$$

Nous considérons deux sous-cas. Le premier est celui où $q-1$ n'est pas un facteur de $\mathfrak{M}$ et le deuxième est celui où $q-1$ est un facteur de $\mathfrak{M}$.

- ◇ Premièrement, supposons que $q-1$ n'est pas un facteur de $\mathfrak{M}$. Par conséquent, $q-1$ est inversible modulo $\mathfrak{M}$. On tire de la relation (3.12) que

$$\sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} q^j \equiv 0 \mod \mathfrak{M}.$$

Par conséquent, on tire de la relation (3.11) que

$$\sum_{a\in A}\binom{w_2}{a}_q - \binom{w_1}{a}_q \equiv \sum_{j=\mathrm{ind}(q)+r_1}^{\mathrm{ind}(q)+r_2-1} q^j \mod \mathfrak{M}. \tag{3.13}$$

En multipliant le membre de droite par $q-1$, on obtient

$$(q-1)\sum_{j=\mathrm{ind}(q)+r_1}^{\mathrm{ind}(q)+r_2-1} q^j = q^{\mathrm{ind}(q)+r_1}(q^{r_2-r_1}-1) = q^{\mathrm{ind}(q)+r_2} - q^{\mathrm{ind}(q)+r_1}$$

qui est, étant donné que nous avons supposé $r_1, r_2 \in \{0,\dots,\mathrm{per}(q)-1\}$ avec $r_1 < r_2$, non nul modulo $\mathfrak{M}$. Cela contredit la relation (3.11). De cette manière, on a $w_1 \sim_{\mathrm{per}(q)} w_2$.

- ◇ Deuxièmement, supposons que $q-1$ soit un facteur de $\mathfrak{M}$, c'est-à-dire que $\mathfrak{M}(q) = (q-1)^d \cdot \mathfrak{N}$ pour un polynôme $\mathfrak{N} \in \mathbb{Z}_p[q]$ et un naturel maximal $d \geq 1$. Il est à noter que $\deg(\mathfrak{N}) \geq 1$. En effet, si $\deg(\mathfrak{N}) = 0$, alors $q \equiv 1 \mod \mathfrak{M}$. Cela nous donnerait que $\mathrm{per}(q) = 1$, ce qui n'est pas possible car

7. Pour calculer cette somme, rappelons que, étant donné que $\sum_{j=0}^{n} q^j = \frac{q^{n+1}-1}{q-1}$, on obtient que

$$\sum_{j=a}^{b} q^j = \sum_{j=0}^{b} q^j - \sum_{j=0}^{a-1} q^j = \frac{q^{b+1}-1}{q-1} - \frac{q^a-1}{q-1} = \frac{q^{b+1}-q^a}{q-1} = \frac{q^a(q^{b+1-a}-1)}{q-1}.$$

Ainsi, on a

$$\sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} q^j = \frac{q^{\mathrm{ind}(q)}(q^{\mathrm{ind}(q)+\mathrm{per}(q)-1+1-\mathrm{ind}(q)})}{q-1} = \frac{q^{\mathrm{ind}(q)}(q^{\mathrm{per}(q)}-1)}{q-1}.$$

per$(q) \geq 2$. Remarquons que les relations (3.10) et (3.11) sont toujours valides modulo $\mathfrak{N}$. De la relation (3.12), on déduit que

$$\sum_{j=\mathrm{ind}(q)}^{\mathrm{ind}(q)+\mathrm{per}(q)-1} q^j \equiv 0 \mod \mathfrak{N}.$$

Il est donc clair que la relation (3.13) est valide modulo $\mathfrak{N}$. En multipliant par $q-1$, on obtient la même conclusion que dans le sous-cas précédent. Ainsi, on a $w_1 \sim_{\mathrm{per}(q)} w_2$.

On conclut en combinant les deux cas étudiés, c'est-à-dire quand $q$ est inversible et quand $u$ contient toutes les lettres de l'alphabet $A$. Dans ce cas, la congruence $\equiv_{u,\mathfrak{M}}$ est exactement la relation d'équivalence $\sim_{u,\mathfrak{M}}$. Il n'existe donc pas de raffinement moins fin.

Quand le polynôme $q$ est inversible dans $\mathbb{F}$, pour une congruence $\simeq$ qui est un raffinement de $\sim_{u,\mathfrak{M}}$, on est en droit de se demander quand le monoïde $A^*/\simeq$ est un groupe. Il est naturel de considérer la congruence la moins fine qui est un raffinement de $\sim_{u,\mathfrak{M}}$, qui est, par la Proposition 3.4.39, la congruence $\equiv_{u,\mathfrak{M}}$. En particulier, étant donné qu'on suppose que le polynôme $q$ est inversible dans $\mathbb{F}$, on a montré que cette congruence est exactement donné par l'intersection $\sim_{u,\mathfrak{M}} \cap \sim_{\mathrm{per}(q)}$ ou bien uniquement $\sim_{u,\mathfrak{M}}$ si le mot $u$ contient toutes les lettres de $A$. En considérant cette congruence précise, le quotient $A^*/\equiv_{u,\mathfrak{M}}$ est un groupe, comme montré dans le théorème suivant.

**Théorème 3.4.40.** *Soient $u \in A^*$ et $\mathfrak{M} \in \mathbb{Z}_p[q]$. Si le polynôme $q$ est inversible dans $\mathbb{F}$, alors le quotient $A^*/\equiv_{u,\mathfrak{M}}$ est un groupe dont l'ordre divise* $\mathrm{per}(q) \cdot p^{|u|}$.

*Démonstration.* Montrons pour tout mot $w \in A^*$ que $[w]^{\mathrm{per}(q)\cdot p^{|u|}} = [\varepsilon]$. Dans ce cas, tout élément du quotient est inversible et l'ordre de $A^*/\equiv_{u,\mathfrak{M}}$ divise $\mathrm{per}(q) \cdot p^{|u|}$, ce qui nous donnera la conclusion. Remarquons que la longueur de $w^{\mathrm{per}(q)\cdot p^{|u|}}$ est un multiple de per$(q)$. On obtient donc que $|w^{\mathrm{per}(q)\cdot p^{|u|}}| \equiv 0 \mod \mathrm{per}(q)$. Ainsi, étant donné que $|\varepsilon| = 0$, on a $w^{\mathrm{per}(q)\cdot p^{|u|}} \sim_{\mathrm{per}(q)} \varepsilon$. Montrons également que $w^{\mathrm{per}(q)\cdot p^{|u|}} \sim_{u,\mathfrak{M}} \varepsilon$. Étant donné que pour tout $v \in \mathrm{Fac}(u)\setminus\{\varepsilon\}$, on a $\binom{\varepsilon}{v}_q = 0$, on doit montrer que

$$\binom{w^{\mathrm{per}(q)\cdot p^{|u|}}}{v}_q \equiv 0 \mod \mathfrak{M}.$$

Soit $v \in \mathrm{Fac}(u)\setminus\{\varepsilon\}$. Montrons par récurrence sur $|v|$ que, pour tout mot $w \in A^*$ et tout $j \geq 0$, on a

$$\binom{w^{\mathrm{per}(q)\cdot p^{|v|+j}}}{v}_q \equiv 0 \mod \mathfrak{M}.$$

Il est suffisant de montrer cette relation pour $j = 0$. En effet, en remplaçant $w$ par le mot $w^p$, on a

$$(w^p)^{\mathrm{per}(q)\cdot p^{|v|}} = w^{\mathrm{per}(q)\cdot p^{|v|}\cdot p} = w^{\mathrm{per}(q)\cdot p^{|v|+1}}.$$

Pour le cas de base, supposons que $|v| = 1$, c'est-à-dire que $v = a \in A$. Par le Corollaire 3.2.7, on a

$$\binom{w^{\mathrm{per}(q)\cdot p}}{a}_q = \sum_{i=0}^{\mathrm{per}(q)\cdot p-1} q^{i|w|}\binom{w}{a}_q. \tag{3.14}$$

Étant donné que $q$ est inversible dans $\mathbb{F}$, on sait par la Remarque 3.4.10 que $\mathrm{ind}(q) = 0$. Ainsi, en utilisant la relation (3.8), on a

$$\sum_{i=0}^{\mathrm{per}(q)\cdot p-1} q^{i|w|} = \sum_{i=0}^{\mathrm{per}(q)-1}\sum_{j=0}^{p-1} q^{(\mathrm{per}(q)\cdot j+i)|w|} \equiv \sum_{i=0}^{\mathrm{per}(q)-1}\sum_{j=0}^{p-1} q^{i|w|} \equiv p\sum_{i=0}^{\mathrm{per}(q)-1} q^{i|w|} \equiv 0 \mod \mathfrak{M}.$$

Par la relation (3.14), on obtient que $\binom{w^{\mathrm{per}(q)\cdot p}}{a}_q \equiv 0 \mod \mathfrak{M}$. Supposons à présent que le résultat soit vérifié pour des mots de longueur $k \geq 1$ et considérons un mot $v$ de longueur $k+1$. Par le Corollaire 3.2.7, on a

$$\binom{w^{\mathrm{per}(q)\cdot p^{k+1}}}{v}_q = \sum_{\substack{v_1,\ldots,v_p\in A^*\\ v=v_1\cdots v_p}} q^{\sum_{i=1}^{p-1}|v_i|((p-i)\mathrm{per}(q)p^k|w|-|v_{i+1}\cdots v_p|)}\binom{w^{\mathrm{per}(q)\cdot p^k}}{v_1}_q\cdots\binom{w^{\mathrm{per}(q)\cdot p^k}}{v_p}_q.$$

Par hypothèse de récurrence, si un des mots $v_i$ dans la factorisation de $v$, avec $i \in \{1,\ldots,p\}$, est tel que $|v_i| \in \{1,\ldots,k\}$, alors on sait que

$$\binom{w^{\mathrm{per}(q)\cdot p^k}}{v_i}_q \equiv 0 \mod \mathfrak{M}.$$

Ainsi, les seuls termes non nuls modulo $\mathfrak{M}$ correspondent aux factorisations de $v$ où tous les $v_i$ sont égaux à $\varepsilon$ sauf un qui est égal à $v$. De cette manière, en utilisant la relation (3.8), on obtient que

$$\begin{aligned}\binom{w^{\mathrm{per}(q)\cdot p^{k+1}}}{v}_q &\equiv \sum_{j=0}^{p-1} q^{j|v|\mathrm{per}(q)p^k|w|}\binom{w^{\mathrm{per}(q)\cdot p^k}}{v}_q \equiv \sum_{j=0}^{p-1}\binom{w^{\mathrm{per}(q)\cdot p^k}}{v}_q \equiv p\binom{w^{\mathrm{per}(q)\cdot p^k}}{v}_q\\ &\equiv 0 \mod \mathfrak{M}.\end{aligned}$$

Ainsi, la récurrence est vérifiée et on a donc $w^{\mathrm{per}(q)\cdot p^{|u|}} \sim_{u,\mathfrak{M}} \varepsilon$. Ainsi, étant donné que $w^{\mathrm{per}(q)\cdot p|u|} \sim_{\mathrm{per}(q)} \varepsilon$ et que $q$ est inversible dans $\mathbb{F}$, on obtient que $w^{\mathrm{per}(q)\cdot p^{|u|}} \equiv_{u,\mathfrak{M}} \varepsilon$. Ainsi, le quotient $A^*/\equiv_{u,\mathfrak{M}}$ est un groupe dont l'ordre divise $\mathrm{per}(q)\cdot p^{|u|}$, ce qui nous permet de conclure. □

**Corollaire 3.4.41.** *Soient $v \in A^*$, $\mathfrak{M}(q) = a(q-1)^d$ pour un naturel $d \geq 1$ et un élément non nul $a \in \mathbb{Z}_p$. Si $\mathfrak{R} \in \mathbb{Z}_p[q]$ est un polynôme tel que $\deg(\mathfrak{R}) < \deg(\mathfrak{M})$, alors le langage $L_{v,\mathfrak{R},\mathfrak{M}}$ est accepté par un $p$-groupe.*

*Démonstration.* Montrons que le groupe $G = A^*/\equiv_{v,\mathfrak{M}}$ est un $p$-groupe. Étant donné que $\mathfrak{M}(q) = a(q-1)^d$ pour un naturel $d \geq 1$ et un élément non nul $a \in \mathbb{Z}_p$, on sait par la Proposition 3.4.16 que $\mathrm{ind}(q) = 0$ et $\mathrm{per}(q) = p^t$ pour un $t > 0$. Remarquons que $p^t \geq d$. Par le Théorème 3.4.40, l'ordre du groupe $G = A^*/\equiv_{v,\mathfrak{M}}$ est divisible par $p^{t+|v|}$. Ainsi, $G$ est un $p$-groupe.

Montrons que le langage $L_{v,\mathfrak{R},\mathfrak{M}}$ est accepté par un $p$-groupe. Considérons le morphisme de monoïdes $\pi : A^* \to G$ qui à chaque mot $x$ associe sa classe d'équivalence $[x]$. Soit $S \subseteq G$ l'ensemble des classes d'équivalences défini par $[y] \in S$ si et seulement si

$$\binom{y}{v}_q \equiv \mathfrak{R} \mod \mathfrak{M}.$$

Il est clair que $\pi^{-1}(S) = L_{v,\mathfrak{R},\mathfrak{M}}$. Étant donné que $S$ est un sous-ensemble d'un $p$-groupe et que $L_{v,\mathfrak{R},\mathfrak{M}}$ est l'image inverse de $S$ par un morphisme de monoïdes, on obtient que le langage $L_{v,\mathfrak{R},\mathfrak{M}}$ est accepté par un $p$-groupe, ce qui nous donne la conclusion. □

**Exemple 3.4.42.** Reprenons l'Exemple 3.4.25. Rappelons que $A = \{a, b\}$, $u = ab \in A^*$, $p = 3$ et $\mathfrak{M}(q) = q^2 + q + 1$. Dans $\mathbb{F} = \mathbb{Z}_3[q]/\langle q^2 + q + 1\rangle$, le polynôme $q$ est inversible. Étant donné que toutes les lettres de $A$ apparaissent dans $u$ et que le polynôme $q$ est inversible, on sait que les relations d'équivalences $\sim_{ab,q^2+q+1}$ et $\equiv_{ab,q^2+q+1}$ coïncident. De cette manière, le quotient $\{a, b\}^*/\sim_{ab,q^2+q+1}$ est, par le Théorème 3.4.40, un groupe. On peut donc construire la table de multiplication de ce groupe. Cette table est représentée à la Figure 3.4. Pour obtenir le produit entre les classes $C_i$ et $C_j$, avec $i, j \in \{1, \ldots, 27\}$, on prend les représentants $w_i$ de $C_i$ et $w_j$ de $C_j$. Ensuite, on étudie la signature

$$\left(\binom{w_iw_j}{a}_q \mod q^2+q+1, \binom{w_iw_j}{b}_q \mod q^2+q+1, \binom{w_iw_j}{ab}_q \mod q^2+q+1\right).$$

Si cette signature est la signature de la classe d'équivalence $C_k$, alors le produit de $C_i$ et $C_j$ est $C_k$ et on note $k$ dans la case correspondante.

**Remarque 3.4.43.** L'automate fini déterministe $\mathcal{A}$, dont l'ensemble des états est $G = A^*/\equiv_{v,\mathfrak{M}}$, dont la fonction de transition $\delta : G \times A \to G$ est définie par $\delta([y], a) = [ya]$, dont l'état initial est $[\varepsilon]$ et dont l'ensemble des états finals est $\pi^{-1}(S)$ comme dans la preuve précédente, accepte le langage $L_{v,\mathfrak{R},\mathfrak{M}}$. De plus, étant donné que $G$ est un groupe par le Théorème 3.4.40, cet automate fini déterministe est un automate de permutation, c'est-à-dire que le semi-groupe des transitions est un groupe. Le quotient d'un automate de permutation étant un automate de permutation, l'automate minimal du langage $L_{v,\mathfrak{R},\mathfrak{M}}$ est un automate de permutation.

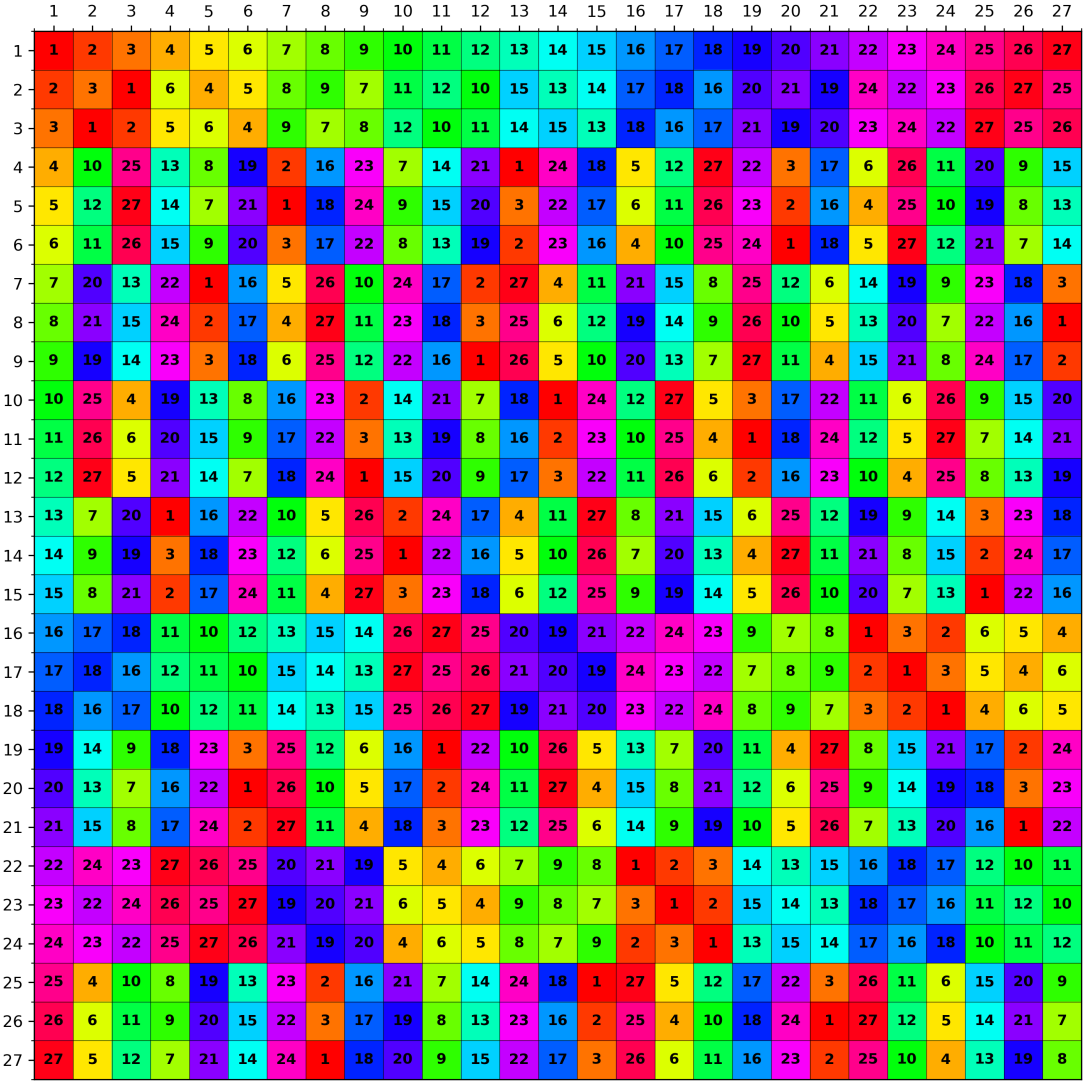


FIGURE 3.4 – Table de multiplication du groupe $\{a,b\}^*/\sim_{ab,q^2+q+1}$ avec 27 classes d'équivalences.

**Exemple 3.4.44.** Reprenons l'Exemple 3.4.42 en appliquant la procédure décrite ci-dessus. Une fois cet automate obtenu, on effectue la minimisation de ce dernier. L'automate minimal du langage $L_{ab,\mathfrak{R},q^2+q+1}$ est donné à la Figure 3.5, où les états finals sont $\{1,2,3\}$ (resp. $\{5\}$, $\{8\}$, $\{4\}$, $\{9\}$, $\{7\}$, $\{6\}$) si $\mathfrak{R}=0$ (resp. $\mathfrak{R}=1$, $\mathfrak{R}=2$, $\mathfrak{R}(q)=q$, $\mathfrak{R}(q)=q+1$, $\mathfrak{R}(q)=2q$, $\mathfrak{R}(q)=2q+2$). Dans la Figure 3.5, on voit également la manière dont $a$ et $b$ jouent un rôle de permutation dans cet automate minimal. Ces deux permutations peuvent être utilisées comme générateurs du groupe considéré.

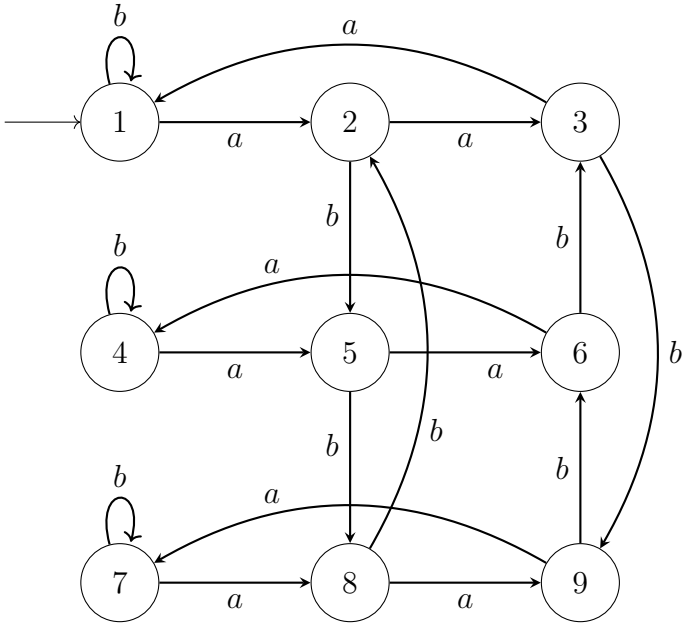



FIGURE 3.5 – Automate minimal du langage $L_{ab,\mathfrak{R},q^2+q+1}$.

Nous nous intéressons à présent à la généralisation du Théorème 2.4.6. Rappelons que le théorème d'Eilenberg donnait une caractérisation des langages acceptés par des $p$-groupes en termes de combinaisons booléennes de langages de la forme $L_{v,r,p}$.

**Théorème 3.4.45** (Théorème d'Eilenberg généralisé)**.** *Soient $v \in A^*$, $\mathfrak{M}(q) = a(q-1)^d$ pour un naturel $d \geq 1$ et un élément non nul $a \in \mathbb{Z}_p$ et $\mathfrak{R} \in \mathbb{Z}_p[q]$ tel que $\deg(\mathfrak{R}) < \deg(\mathfrak{M})$. Un langage $L$ sur $A$ est accepté par un $p$-groupe si et seulement si $L$ est une combinaison booléenne de langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$.*

*Démonstration.* Premièrement, remarquons que le reste $\mathfrak{R}(q)$ de la division euclidienne de $\mathfrak{P}(q)$ par $\mathfrak{M}$ et le polynôme $\mathfrak{P}(q)$ ont la même somme de coefficients modulo $p$. En effet, on a la division euclidienne

$$\mathfrak{P}(q) = \mathfrak{U}(q) \cdot a(q-1)^d + \mathfrak{R}(q)$$

où $\mathfrak{U}, \mathfrak{R} \in \mathbb{Z}_p[q]$ sont tels que $\deg(\mathfrak{R}) < d$. La conclusion suit en évaluant les deux membres en $q = 1$. En effet, on obtient que $\mathfrak{P}(1) \equiv \mathfrak{R}(1) \mod p$.

Par conséquent, pour les coefficients binomiaux de mots classiques, dont les valeurs sont des entiers, on a

$$\binom{u}{v} \equiv r \mod p$$

si et seulement si l'évaluation en $q = 1$ du polynôme dans $\mathbb{Z}_p[q]$ donné par

$$\binom{u}{v}_q \mod \mathfrak{M}$$

est également congrue à $r$ modulo $p$. En effet, si $\binom{u}{v}_q = \mathfrak{P}(q)$, alors les entiers $\mathfrak{P}(1)$ et $\binom{u}{v}$ sont égaux et la conclusion suit en considérant tous les coefficients dans $\mathbb{Z}_p$.

On obtient donc que tout langage $L_{v,r,p} = \{u \in A^* : \binom{u}{v} \equiv r \mod p\}$ est l'union disjointe des langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$ pour des polynômes $\mathfrak{R}$ tels que $\mathfrak{R}(1) \equiv r \mod p$. Plus précisément, on observe que parmi les $p^d$ polynômes $\mathfrak{R}(q)$ de degré plus petit que $d$ dans $\mathbb{Z}_p[q]$, il y en a exactement $p^{d-1}$ qui sont tels que $\mathfrak{R}(1)$ est un élément de $\mathbb{Z}_p$. La somme modulo $p$ dans un $d$-uple de coefficients de $\mathbb{Z}_p$ est complètement déterminée par un des coefficients quand les $d-1$ autres sont fixés.

La condition est nécessaire. Si le langage $L$ est accepté par un $p$-groupe, alors on sait par le Théorème 2.4.6 qu'il est combinaison booléenne de langages de la forme $L_{v,r,p}$ qui sont eux-mêmes des unions finies de langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$. De cette manière, si $L$ est accepté par un $p$-groupe, alors $L$ est une combinaison booléenne de langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$.

La condition est suffisante. Supposons que $L$ est une combinaison booléenne de langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$. Étant donné que toute combinaison booléenne d'ensembles acceptés par un $p$-groupe est acceptée par un $p$-groupe et que $L_{v,\mathfrak{R},\mathfrak{M}}$ est accepté par un $p$-groupe par le Corollaire 3.4.41, on obtient que le langage $L$ est accepté par un $p$-groupe, ce qui nous donne la conclusion. □

**Exemple 3.4.46.** Soient $v \in A^*$ et $p = 3$. Comme nous l'avons vu dans la preuve précédente, les langages de la forme $L_{v,r,p}$ sont des unions disjointes de langages de la forme $L_{v,\mathfrak{R},\mathfrak{M}}$ où le polynôme $\mathfrak{R}$ est tel que $\mathfrak{R}(1) \equiv r \mod p$. Ainsi, étant donné que $q+2$ évalué en $q=1$ est égal à 0 modulo 3 et que $2q+1$ évalué en $q=1$ est égal à 0 modulo 3, on obtient que

$$L_{v,0,3} = \left\{u \in A^* : \binom{u}{v}_q \equiv 0 \mod q^2+q+1\right\} \cup \left\{u \in A^* : \binom{u}{v}_q \equiv q+2 \mod q^2+q+1\right\} \cup \left\{u \in A^* : \binom{u}{v}_q \equiv 2q+1 \mod q^2+q+1\right\}.$$

De plus, étant donné que $q$ évalué en $q=1$ est égal à 1 modulo 3 et que $2q+2$ évalué en $q=1$ est égal à 1 modulo 3, on obtient que

$$L_{v,1,3} = \left\{u \in A^* : \binom{u}{v}_q \equiv 1 \mod q^2+q+1\right\} \cup \left\{u \in A^* : \binom{u}{v}_q \equiv q \mod q^2+q+1\right\} \cup \left\{u \in A^* : \binom{u}{v}_q \equiv 2q+2 \mod q^2+q+1\right\}.$$

Enfin, étant donné que $q+1$ évalué en $q=1$ est égal à 2 modulo 3 et que $2q$ évalué en $q=1$ est égal à 2 modulo 3, on obtient que

$$L_{v,2,3} = \left\{ u \in A^* : \binom{u}{v}_q \equiv 2 \mod q^2+q+1 \right\} \cup \left\{ u \in A^* : \binom{u}{v}_q \equiv q+1 \mod q^2+q+1 \right\} \cup \left\{ u \in A^* : \binom{u}{v}_q \equiv 2q \mod q^2+q+1 \right\}.$$

De cette manière, l'automate minimal du langage $L_{ab,r,3}$ est donné à la Figure 3.6, où les états finals sont $\{1,2,3\}$ (resp. $\{4,5,6\}$, $\{7,8,9\}$) si $r=0$ (resp. $r=1$, $r=2$).

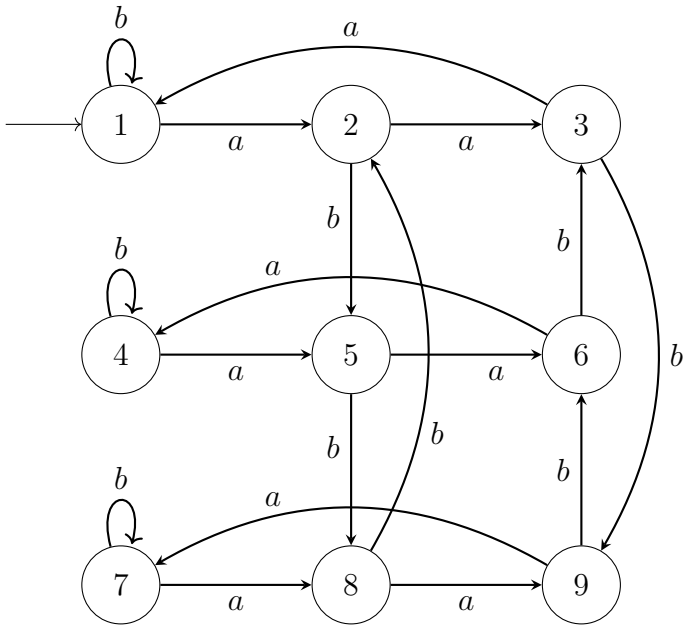



FIGURE 3.6 – Structure de l'automate minimal du langage $L_{ab,r,3}$.

Il est intéressant de noter que, dans le cas $r=2$, l'automate est le même que celui obtenu à la Figure 2.5.

Il est important de mentionner que, dans certains cas, l'automate minimal obtenu peut se projeter en un automate quotient. Dans l'exemple développé ci-dessus, cela n'est pas possible. Cependant, si $A=\{a,b\}$, si $u=ab \in A^*$, $p=2$ et $\mathfrak{M}(q)=q^2+1$, alors l'automate minimal se projette en un automate quotient [12, Figure 4].

# Bibliographie


[1] Jean Berstel, Dominique Perrin et Christophe Reutenauer, *Codes and automata*, Encyclopedia of mathematics and its applications, n°129, Cambridge University Press, 2010.

[2] Miroslav Dudík et Leonard J. Schulman, *Reconstruction from subsequences*, Journal of combinatorial theory Series A **103** (2003), n°2, 337-348.

[3] Samuel Eilenberg, *Automata, languages and machines* Vol B, Pure and Applied Mathematics, n°59, Academic Press, New-York, 1976.

[4] John E. Hopcroft, Rajeev Motwani et Jeffrey D. Ullman, *Introduction to automata theory, languages and computation*, 2$^{e}$ édition, Addison-Wesley, 2001.

[5] Mark V. Lawson, *Finite automata*, Chapman & Hall/CRC, Boca Raton, 2003.

[6] Julien Leroy, *Structures algébriques*, Notes provisoires du cours de 2$^{e}$ bachelier en sciences mathématiques, Université de Liège, 2023.

[7] M. Lothaire, *Combinatorics on words*, Cambridge Mathematical Library, Cambridge University Press, 1997.

[8] Bennet Manvel, Aaron Mayerowitz, Allen J. Schwenk, Kenneth W. Smith et Paul K. Stockmeyer, *Reconstruction of subsequences*, Discrete Mathematics **94** (1991), n°3, 209-220.

[9] Antoine Renard, *q-deformations of binomial coefficients of words*, Séminaire du laboratoire de mathématiques de Reims (Reims, 27 juin 2023), disponible via l'URL<`https://orbi.uliege.be/bitstream/2268/342183/1/seminaire_reims_q-coefficients.pdf`>.

[10] Antoine Renard, *q-deformations of binomial coefficients of words*, Journées Nationales d'Informatique Mathématique (Paris, 4 avril 2023), disponible via l'URL<`https://orbi.uliege.be/bitstream/2268/301678/1/Poster_JNIM2023%20_ARENARD.pdf`>.

[11] Antoine Renard, *Generalisations of the binomial coefficients of words*, CANT 2025 (Marseille, 29 septembre 2025 - 03 octobre 2025), disponible via l'URL<`https://orbi.uliege.be/bitstream/2268/339336/1/Poster_CANT_2025.pdf`>.

[12] Antoine Renard, Michel Rigo et Markus Whiteland, *Introducing q-deformed binomial coefficients of words*, Journal of Algebraic Combinatorics, **61** (2025), n°2.

[13] Michel Rigo, *Algèbre linéaire*, Notes du cours de 1er bachelier en sciences mathématiques, Université de Liège, 2009, disponible via l'URL <http://www.discmath.ulg.ac.be/cours/main_math.pdf>.

[14] Michel Rigo, *Théorie des automates et des langages formels*, Notes du cours de 3e bachelier en sciences mathématiques, Université de Liège, 2009, disponible via l'URL <http://www.discmath.ulg.ac.be/cours/main_autom.pdf>.

[15] Michel Rigo, Manon Stipulanti et Markus Whiteland, *Binomial coefficients of words and beyond*, en cours d'écriture.